Research Doctorate in
Legal Sciences

European and Transnational Legal Studies

CYCLE XXXVIII

The protection of the right not to provide information c*ontra se* in financial investigations. Reconciling an apparent dichotomy

Academic Discipline (SSD) IUS/16

Doctoral Candidate
Dr. Costanza De Caro

Supervisor
Prof. Paola Felicioni
Co-supervisor
Serena Cacciatore

Coordinator
Prof. Maria Luisa Vallauri

The consultation of the thesis is free. Unless a specific authorization is obtained from the author, the thesis can be, however, downloaded and printed only for strictly personal purposes related to study, research and teaching, with the explicit exclusion of any use that has – even indirectly – a commercial nature.

Contents

Introduction **6**
1 Setting the scene: *securitization* as the main background 7
1.1 The role of the private sector in the security dogma 12
2 Financial investigations and their clashes with fundamental rights 13
3 Setting the limits: definition of the objectives and research questions 15
4 Methodology 17
5 Roadmap 18

I The legal framework on financial investigations **20**
1 Introduction 20
2 The international standards: the role of the Financial Action Task Force 21
2.1 The notion of financial investigations 27
2.2 The actors: Financial Intelligence Units and their network 33
3 The European Union's action against dirty money: a success story? 40
3.1 The EU AML/CTF system between prevention approaches and criminal prosecution 49
3.1.1 Financial Intelligence Units: network, cooperation, powers 61
3.2 Following the money through mutual recognition instruments 70

II *Nemo tenetur se detegere* principle from old to new paradigms **79**
1 Introduction 79
2 The manifold relevance of secrecy in financial investigations and its clash with procedural rights 80
3 An overview on the *nemo tenetur* principle in light of the right to a fair trial 85
3.1 Protecting the right to silence of suspects under human rights law: the European Convention of Human Rights . . 92
3.2 The EU legal framework on procedural safeguards: Directive (EU) 2016/343 on the presumption of innocence 98
4 The privilege against self-incrimination in the context of financial investigations: an intricate playing field 114

4.1 The applicability of the *nemo tenetur* principle 122
4.2 Evidential value of financial data: intelligence reports and their evidentiary use in criminal proceedings 127
5 Preliminary conclusions: looking for legal remedies 135

III The rise of Public-Private Partnerships for Information Sharing in AML/CTF legislation 140
1 Introduction 140
2 New challenges and old dilemmas: the private sector enters the scene 141
2.1 Untangling the concept of Public-Private Partnerhips . . . 150
2.2 Obliged entities within criminal proceedings: drawing lessons from the theory on horizontal effect of fundamental rights 156
3 The new legal basis for Public-Private Partnerships for Information Sharing 168
4 Do the fair trial rights apply? An attempt to sort it out 174
4.1 The subjective scope of application of the privilege against self-incrimination between *matière pénale* and de-risking practices 175
4.2 The material scope of application of the privilege: PPPs as *fishing expeditions* 180
5 Preliminary conclusions: towards the contractualization of criminal procedure 184

IV Drawing a conclusion: towards a comprehensive regulation of financial investigations 191
1 Key findings 191
2 What is still missing: data protection implications of financial investigations 195
2.1 Core principles: fairness of processing and purpose limitation 201
2.2 EU data protection frameworks and the never-ending discourse around the applicable regime 206
3 Contributions and recommendations for a prospective framework on financial investigations 216
3.1 Striving for silence: the protection of informational self-determination and control over self-incriminating data . . 219
3.2 Striving for remedies: the right to notification to ensure informed consent 223
3.3 Striving for accountability: the need to address the role of private actors 226

References 228

Introduction

1 Setting the scene: *securitization* as the main background

In recent years, the policies and legislative choices of the European Union and, consequently, those at the national level, have been inspired by the need to ensure greater internal and external security at the borders to avert (*i.e.*, prevent) the occurrence of, as well as to protect civil society from, new threats and particularly serious forms of crime[1]. No longer intended only as an objective of EU action[2], but also as a value worthy of attaining the rank of a subjective right[3], the concept

[1]U. Sieber, *The New Architecture of Security Law. Crime Control in the Global Risk Society*, in U. Sieber-V. Mitsilegas-C. Mylonopulos-E. Billis-N. Knust (eds), *Alternative Systems of Crime Control National, Transnational, and International Dimensions*, Berlin, 2018, pp. 3-38, observes that the shift in the crime control field from a repressive approach to a preventive one, is to ascribe, inter alia, to the rise of new criminal threats, including terrorism, organized crime and cybercrime.

[2]The reference goes to the institutional framework shaped by the Treaty of Amsterdam, one of the objectives was «to maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime». The idea of an Area of freedom, security and jsutice was maintained and strenghten by the Treaty of Lisbon under Title V of the Treaty on the Functioning of the European Union. Critical towards the terminilogy adopted in Art. 67 TFEU, whereby the criminal law field seems to be linked only to the principle of security, is V. Mitsilegas, *EU Criminal Law*, Oxford, 2009, p. 38.

[3]The Court of Justice of the EU has gradually recognised an autonomous *raison d'être* for the concept of security with respect to the similar – but evidently not equal – right to liberty, both enshrined in Article 6 of the Charter of Fundamental Rights of the European Union (hereinafter: CFREU). Recently, in the judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, para 42, the CJEU for instance stated that «Article 6 of the Charter lays down the right of any person

of security in a securitarian sense[4] has enjoyed renewed glory in the current "risk society"[5], in which the uncertainties brought about by modernity and the scientific and technological development necessitate an anticipation of the risk control mechanisms that these uncertainties entail[6]. Hence, the trend towards an erratic – and, according to some authors, political[7] – identification of these risks as threats to security, to be faced with extraordinary means, following the steps characteristic of that process of "securitization" which transcends criminal law and extends to all areas relevant to securitarian rhetoric[8].

---

not only to liberty, but also to security». The issue is closely connected to the debate concerning whether the right enshrined therein is unitary, the two terms thus operating as a hendiadys in which the latter represents an instrumental means for the achievement of the former, or whether the aforementioned principles pertain to two distinct normative dimensions. On this point, see F. Rossi dal Pozzo, M. Gialuz, *Articolo 6. Diritto alla libertà e alla sicurezza*, in S. Allegrezza-R. Mastroianni-F. Pappalardo-O. Pollicino-O. Razzolini (eds), *Carta dei diritti fondamentali dell'Unione europea*, Milan, 2017, p. 102 ff. and the literature cited therein.

[4]Namely, as the securitization of assets and legal interests deemed worthy of protection by means of criminal intervention, which is antithetical to liberal security. See D. Pulitanò, *Sicurezza e diritto penale*, in *Riv. it. dir. e proc. pen*, 2009, 2, p. 547 ff.

[5]The term was coined by da U. Beck, *Risk Society: Towards a New Modernity*, London, 1992.

[6]V. Mitsilegas, *Money Laundering Countermeasures in the European Union: a New Paradigm of Security Governance versus Fundamental Legal Principles*, The Hague, 2003, p. 12.

[7]T. Balzacq, *Securitization Theory: Past, Present, and Future*, in *Polity*, 2019, n. 2, p. 331-348.

[8]It is no coincidence that the Area of Freedom, Security and Justice, as revised by the Treaty of Lisbon, aims to establish appropriate measures with regard to border checks, migration policies, asylum, and the prevention and combating of crime, pursuant to Article 3(2) TEU. Furthermore, Title V TFEU lists the matters specifically falling within the Area, including judicial cooperation and mutual recognition in civil and criminal matters. Among these, the sector that arguably most suffers from the damage caused by securitarian and defensive policies is that of immigration, where security law, administrative criminal law, but also intelligence and civil law combine to form a risk prevention system. In the literature, see V. Mitsilegas, J. Monar, W. Rees, *The European Union and Internal Security. Guardian of the People?*, Houndmills, 2003; N. Vavoula, *Immigration and Privacy in the Law of the European Union. The Case of Information Systems* Leiden-Boston, 2022.

Therefore, the phenomenon of *securitization*[9] is closely linked to the inexorable paradigm shift that has occurred in the field of criminal law, moving from a logic of repression to one of prevention, which manifests itself both in its substantive aspect, with the criminalization of activities considered preparatory to the commission of crimes but which, upon closer inspection, do not harm any legally relevant public interest; and in its procedural aspect, with the deployment of procedural tools bent to purposes or assumptions external to them. Thus, one witnesses, for example, an alteration of the power dynamics between the judiciary and law enforcement authorities[10], or the admissibility of intelligence data as evidence into criminal proceedings, where the former nonetheless lacks the characteristics and safeguards that are attached to the latter[11]. The involvement of intelligence agencies responds to the need of investigative authorities to build a solid so-called "information position" to develop targeted strategies for combating serious forms of crime, as an integral part of an intelligence-led policing approach[12].

Regarding the latter aspect, namely the free access and collection of informa-

[9]Securitzation studies were conceptualized by the political scientists belonging to the School of Copenaghen, and the term refers to a rethoric «through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat» (B. Buzan, O. Waever, *Regions and Powers*, Cambridge, 2003, p. 481.). See also O. Waever, *Politics, security, theory*, in *Security Dialogue*, 2011, 4-5, p. 465 ff.

[10]D. Negri, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen.*, 2016, 1, p. 44 ff., where the Author, with regards to the new counter-measures adoptded in Italy in the aftermath of the jihadist terroristic attacks taking place across Europe starting from 2015, points to the minimal powers left in the hands of public prosecutors in favor of a greater involvement of the judicial police in the field of web electronic surveillance.

[11]On this point, M. Jimeno-Bulnes, *The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama*, in *New Journal of European Criminal Law*, 2017, n. 2, pp. 171-191. The Author reminds us of the fundamental difference between evidentiary material collected by police forces and that provided by intelligence agencies, namely the circumstance that the latter gather information in a condition of secrecy rather than transparency, making it impossible to verify its reliability, thus devaluing the right of the defence to an adversarial process. For a more in-depth discussion, see B. Vogel, *Balancing Procedural Fairness and Surveillance in Criminal Procedure Law. Between the Adversarial Principle and a Resurgence of the Inquisitorial Process*, in Id. (ed.), *Secret Evidence in Criminal Proceedings. Balancing Procedural Fairness and Covert Surveillance*, Berlin, 2021, pp. 1-52.

[12]Cf. L. Winter Bachmaier, *Section III–Criminal procedure. Information society and penal law: General Report*, in *Revue internationale de droit pénal*, 2014, 1, pp. 75-127.

tion to be used to guide or initiate criminal investigations, the securitization of criminal policies has always entailed[13] – and in recent years even more conspicuously[14] – the tendency of investigative authorities to seek the collaboration of the private sector, which notoriously holds a vast amount of data and technical knowledge, precisely with the aim of collecting information useful for investigative purposes. As a consequence, financial and banking institutions, airlines, legal professionals, and telecommunications service providers are "responsibilized"[15] by the judicial and police authorities, becoming their informants[16].

The anti-money laundering and counter-terrorism financing (AML/CTF) legislation perfectly fits in this scenario for two main reasons. In the first place, as human relations increasingly occur in a digital context and much of what we are, we do or aim at, passes through money flows and banking transactions, inquiries into the financial affairs of individuals have risen to the status of the privileged instrument for law enforcement and judicial authorities to prevent criminals from benefiting from the proceeds of their illicit conducts. Therefore, the analysis and monitoring of the financial system and the transactions conducted therein slowly shifted from a regulatory function aiming to preserve the well-functioning of financial and economic markets, to a distinctively crime control tool to detect, prevent, and eventually prosecute most serious forms of criminal conducts.

[13]As demonstrated by the figure of the private agent recording on behalf of the public prosecutor. See R. Del Coco, *Registrazioni audio-video effettuate da un privato su impulso dell'investigatore*, in A. Scalfati (ed), *Le indagini atipiche*, Turinn, 2019, pp. 3-29; A. Mangiaracina, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici ... e non solo*, in *Proc. pen. giust.*, 2021, 4, p. 741 ff.

[14]In light of the digitalization and technological development, as suggested by V. Mitsilegas, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law*, 2018, 3, pp. 263-265.

[15]Notable scholarship has identified the phenomenon by the term *responsibilization strategy*, in order to refer to the choice of the central state not to act directly through *ad hoc* governmental agencies, bu rather indirectly via private actors. See D. Garland, *The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society*, in *The British Journal of Criminology*, 1996, n. 4, p. 452. Similarly, M. Bergström, K. Svedeberg Kelgesson, U. Mörth, *A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management,* in *Journal of Common Market Studies*, 2011, 5, p. 1052.

[16]U. Sieber, *The New Architecture*, cit., p. 15, who refers to the role played by Financial Intelligence Units in conducting their activities in the AML/CTF field by calling them «data gatherers».

Secondly, the AML/CTF system encourages the massime involvement of private actors, insofar as "obliged entities", in the context of the analysis of banking and financial transactions, which are indispensable in investigations into financial crimes, are required to comply with a series of customer due diligence, risk assessment, reporting, and mitigation obligations for merely preventive purposes[17], which compels one to address the growing phenomenon of privatization of public policies.

[17]The rich AML/CTF legislative architecture will be addressed in the first chapter, where the main rationales and specific provisions will be analyzed. For the moment it will be sufficient to refer to the main legal instruments set out at the EU level: i) Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (First AML Directive); ii) 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 (Second AML Directive); iii) 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 (Third AML Directive); iv) 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 (Fourth AML Directive); v) 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 (Fifth AML Directive). Most recently, Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms that Member States must put in place to prevent the use of the financial system for the purposes of money laundering or terrorist financing repealed the Fourth AML Directive. In addition to that, Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on countering money laundering by criminal law addresses the substantial definition of moeny laundering. For a comprehensive analysis of the system, in the extensive literature, see E. Ioannides, *Fundamental principles of EU Law against money laundering*, Abingdon 2014; G. Stessens, *Money laundering: a new international law enforcement model*, Cambridge, 2000; B. Vogel-J.B. Maillart (eds.), *National and International Anti-Money Laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, Cambridge, 2022; V. Mitsilegas, N. Vavoula, *The Evolving EU Anti-Money Laundering Regime. Challenges For Fundamental Rights And The Rule Of Law*, in *Maastricht Journal of European and Comparative Law*, 2016, n. 2, p. 261-293; V. Mitsilegas, *Money laundering counter-measures in the European Union*, cit.

1.1 The role of the private sector in the security dogma

According to the "security dogma", security threats can be defined as «whatever significant actors may regard as such»[18]. This leads to an additional layer of complexity in the analysis of the financial investigations framework, as it cannot neglect the question as of who these "significant actors" are. Although the phenomenon of securitization has mostly occurred in the public security domain, it can nevertheless be framed within the broader social, economic, and political transformation that occurred starting from the mid-nineteenth century toward a regulatory model of governance set under the banner of a neoliberal approach[19]. Following the deregulation process and the related marketization of public services[20], the central state began opting for governing «at a distance»[21] through various contractual arrangements, thus "responsabilizing" the private sector for the delivery of state-controlled public services.

The *privatization* of public policies is also visible in the law enforcement field, where the the co-option of the private sector to carry out law enforcement tasks is increasingly resorted to. In view of the fact that all private actors involved in the financial system, be it banking institutions, financial intermediaries or even legal professionals, hold vast amounts of first-hand information about their customers which puts them in an "informational asymmetry" with law enforcement[22], their involvement in the fight against "dirty money" is in constant expansion.

The newly adopted provision of the AML/CTF legislation laying down the

[18] S. Guzzini, *Securitization as a causal mechanism*, in *Security Dialogue*, 42(4-5), 2011, p. 330.

[19] A. Amicelle, *Towards a 'new' political anatomy of financial surveillance*, in *Security Dialogue*, 2011, 42(2), p. 172; G. Majone, *From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance*, in *Journal of Public Policy*, 1997, 17(2), pp. 139-167.

[20] M. Djelic, *Marketization: From intellectual agenda to global policy-making*, in M. Djelic-K. Sahlin-Andersson, *Transnational Governance. Institutional Dynamics of Regulation*, Cambridge, 2006, pp. 53-73.

[21] N. Rose, P. Miller, *Political power beyond the state: Problematics of government*, in *The British Journal of Sociology*, 1992, 43(2), pp. 173-205.

[22] I. Deleanu, *Information flows and repressive enforcement*, in B. Unger-J. Ferwerda-M. Van Den Broek-I. Deleanu (eds), *The economic and legal effectiveness of the European Union's Anti-Money Laundering policy*, Cheltenham-Northampton, 2014. p. 130.

legal basis for the establishment of Public-Private Partnerships (PPPs) for information sharing envisaged by Regulation (EU) 2024/1624 attests to this trend. Overcoming the traditional rationale underpinning the AML/CTF preventive architecture, pursuant to which reporting entities share information with the authorities only when suspicious activities are detected, the new provision paves the way for a scenario in which, according to a bidirectional flow of information, competent authorities may transmit information — which does not yet necessarily amount to evidence — collected during preliminary investigations to be used by obliged entities to provide further details, on the financial activity and financial profile of targeted customers.

Against this backdrop, the fear is that the co-optation of the private sector will eventually break the boundaries of preventive regulation according to a risk-based approach, to land on the scene of crime prosecution. Specifically, we would witness the formalization of a mechanism of "outsourcing" or contracting out[23] of the powers and prerogatives of the criminal justice system, such as conducting investigations to prosecute criminal facts and ordering investigative measures, to private subjects driven by profit-oriented interests.

It stems from the above that financial investigations are placed at a crossroads of different cross-cutting phenomena, which are all interwoven and eventually raise concerns for the protection of fundamental rights. It is in this briefly described context that the present research grows its roots.

2 Financial investigations and their clashes with fundamental rights

While financial investigations are well-suited, and are indeed being used, to serve a preventive purpose, meaning that they are proactively conducted to anticipate the commission of crimes and heavily rely on intelligence gathering according to a risk-based approach, they have been increasingly drawn into the realm of crim-

[23] G. Lasagni, *Public private partnerships nell'antiriciclaggio e antiterrorismo: una nuova forma di outsourcing del processo penale?*, in *Dir. pen. cont.*, 2021, 3, p. 153 ff.

inal investigations for repressive purposes. When carried out in a judicial setting, they are supposed to comply with fundamental rights and the procedural safeguards stemming from criminal law. However, the blurring boundaries between prevention and prosecution, administrative and criminal, legislative and political, all of which occur in the subject at stake, do not allow for a clear-cut distinction between the two different spheres of intervention of public and private authorities. As a consequence, procedural safeguards might be irremediably downplayed, if not obviated, by resorting to the AML/CTF preventive framework to carry out law enforcement functions.

In fact, the analysis of the twin-track approach adopted by EU lawmakers shows that the two policies, although distinct *in abstracto*, often overlap and serve each other's purposes, with criminal law being used to enforce the regulatory financial framework, and risk management and CDD duties being used to identify criminals or traces of crime, with blurred and unclear lines being drawn between criminal law and administrative law in AML/CTF policy[24]. A salient feature of the AML/CTF preventive legislation is the imposition on obliged entities of a series of burdening obligations to report suspicious transactions, as well as to assess the risk profile of their customers and to operate according to due diligence. In sum, the preventive approach to tackle money laundering and terrorism financing relies on penetrating cooperation duties, which nevertheless appear to raise tensions with fundamental rights safeguarding both the position of suspects targeted by law enforcement *within* criminal proceedings (fair trial rights)[25] and their personal spheres threatened *by* them (right to privacy and data protection).

In this sense, it is self-evident that the surveillance logic underpinning financial investigations, which, similar to other intelligence-led approaches, aim to gather vast amounts of data in order for competent authorities to enhance their infor-

[24]M. Bergström, *Legal perspectives on money laundering*, in V. Mitsilegas-S. Hufnagel-A. Moiseienko (eds), *Research Handbook on Transnational Crime*, Cheltenham, 2019, p. 106.

[25]As is, for instance, the case of the presumption of innocence. See J.A.E. Vervaele, *Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?*, in S. Gutwirth-R. Leenes-P. De Hert (eds), *Reloading data protection. Multidisciplinary insights and contemporary challenges*, Cham, 2013, pp. 115-128.

mation position, is at odds with the right to informational self-determination of those engaging with the financial system. From a fair trial right perspective, the right to informational self-determination is understood as the right of suspects of crime to have control over the incriminating information gathered from them by public authorities, and the use to which such information is put. The privilege against self incrimination, which, according to the well-established ECtHR case law, lies at the heart of the notion of a fair procedure under Article 6 ECHR[26], perfectly encloses the concept behind informational self-determination insofar as it ensures individuals' free choice vis-à-vis abusive coercion by public authorities. Against the broader picture, the privilege, together with the right to silence, is drawn by the *nemo tenetur se detegere* principle, which protects individuals and their personal spheres from illicit intrusions of public powers, as it allows them to refuse to damage themselves at the request of the authority.

Furthermore, from a data protection perspective, informational self-determination refers to the authority of the individual to decide herself when and within what limits information about her private life should be communicated to others.

In light of the above, while financial investigation tools have been under in-depth scrutiny of eminent scholarship[27], although often neglected compared to other measures, their implications for fundamental rights through the lens of informational self-determination have not yet received much attention.

3 Setting the limits: definition of the objectives and research questions

The primary objective of this research is to lay the ground for future discussion about the opportunity to build a comprehensive framework on financial investigations in the EU scenario, which would account for the need to protect the informational self-determination of subjects vis-à-vis competent authorities

[26]ECtHR, [GC], 8 February 1996, *John Murray v. the United Kingdom*, Application n. 18731/91, § 45.

[27]For all, G. Lasagni, *Banking supervision and criminal investigation: comparing the EU and US experiences*, Cham, 2019.

and private actors engaged in the detection of economic crimes. The work will therefore focus on pre-trial investigations into financial transactions and movements suspected of being related to criminal activities, which usually take place in the first stage of the asset recovery process leading to the confiscation of illicit proceeds and which can be either initiated within the framework of traditional criminal investigations or in parallel with them.

Due to the complex theoretical framework in which financial investigations are conducted, intermediate steps are to be undertaken. A clear definition of financial investigations should be provided, which would consider the actors involved, their roles and powers. To that end, both the international and the European Union normative frameworks should be examined.

Subsequently, the research should explore the impact that banking and financial investigations have on the enjoyment of fundamental rights of those targeted, especially when such inquiries trigger the mechanisms of the justice system - and supposedly the safeguards thereof. In order to do that, attention will be focused on one specific fundamental right which represents a strong limit to public powers, that is the privilege against self-incrimination and the right to silence (*nemo tenetur se detegere*) whose protection is provided by Directive (EU) 2016/343 on the presumption of innocence as well as by a rich case law of the supranational Courts.

Thirdly, the research will address the challenge for fundamental rights represented by the newly adopted provision pursuant to Art. 75 Regulation (EU) 2024/1624, allowing the establishment of Public-Private Partnerships for information sharing in the context of money laundering and terrorism financing prevention.

Finally, because of the weight that data processing has in the subject at stake, the research should in conclusion include a reflection on data protection provisions, to evaluate whether they could provide for higher standards of protection of the right of those suspected or accused of crime not to provide self-incriminating information while exerting their economic liberty to engage with the financial system.

In sum, the research will be guided by the following question: Does the EU legislative and regulatory framework on financial investigations comply with the

right to self-determination of customers and suspects of crime, *i.e.*, to decide not to provide personal information that might jeopardize their position before law enforcement and judicial authorities?

In order to provide an answer, the main research question is divided into sub-issues, each focusing on a particular aspect of the problem at hand:

(i) What do we mean by financial investigations?

(ii) Can there be criminal financial investigations without the private sector?

(iii) How can financial investigations be consistent with the right of customers/-suspects of crime not to provide information *contra se* stemming from the criminal procedural framework?

(iv) What differences to the way financial investigations are conducted are brought about by the introduction of Public-Private Partnerships for information sharing?

(v) Does the EU legal framework on data protection provide for equivalent or higher safeguards against the abuse of personal data?

4 Methodology

A doctrinal research methodology appears to be the most appropriate to the study, as it aims to systematize different bodies of legal norms and understand the relationships between them in order to address the identified research questions.

As illustrated, the issues under examination are not confined to the field of criminal procedural law and EU law, as they also touch upon political science and security theorization backgrounds. However, the research does not engage with those methodologies, nor does it employ an empirical legal methodology. Instead, different doctrines or bodies of law are identified to provide an answer to the research questions. Firstly, the research analyzes the most obvious set of EU law provisions that is to be applied when it comes to criminal procedure law, *i.e.* the Procedural Rights Directives Package, and more specifically Directive (EU) 2016/343 on the presumption of innocence as interpreted by the case law of the

Court of Justice. With respect to the latter, since only a few decisions have been delivered on the Directive itself, the scope of the research needs to be extended so as to take into consideration other pieces of legislation addressing the protection of the self-determination of suspects, for instance competition law.

Yet another body of norms of paramount importance is international human rights law. Because of the rich case law developed so far and the impact that the Convention on Human Rights has in shaping national systems in the field of criminal procedure, the research focuses on cases decided by the European Corut of Human Rights (ECtHR).

Lastly, in order to assess whether the privatization of financial investigations represents a threat to the rule of law and in fact entails a shift in accountability in law enforcement towards the private sector, an analysis of the applicable legal frameworks will be carried out accompanied by relevant case law, which covers a wide range of issues that intermingle in the particular field of research at stake. In this sense, the jurisprudence of the ECtHR and the CJEU on data protection regimes, data retention for law enforcement purposes and surveillance case law will shed light on the requirements that public authorities should comply with for fair data processing.

Desk research into administrative and public management literature will be furthermore necessary to untangle the concept of PPPs for information sharing and to evaluate their impact on the EU public governance in crime control and security. Drawing from those bodies of literature and from the different theories on the radiating effects of fundamental rights (*e.g.*, Drittwirkung doctrine, State action doctrine, positive obligations doctrine) whose precise purpose is to justify holding private actors accountable for fundamental rights violations, the broader issue of accountability should be tackled.

5 Roadmap

The research takes its preliminary steps by delving into the legal framework on financial investigations, however scattered, currently in place at the international and European Union level. In the first chapter, the state of the art of the overall anti-money laundering and terrorism financing architecture addressing both its

preventive and repressive courses of action will be analyzed in order to set the theoretical frameworks, which will help us understand how unclear the prevention-repression divide actually is.

In the second chapter, the focus will be on the privilege against self-incrimination and the right to silence as enshrined in human rights law, especially in light of the case law of the Court of Strasbourg, and in the EU legal framework. This analysis will set the stage for further considerations on the existence within the AML/CTF legislative field of any leeway of protection of the privilege, to be understood as the control of suspects over their personal and potentially self-incriminating information.

The third chapter will be devoted to the privatization of financial investigations, as suggested by the newly adopted provision establishing PPPs for Information Sharing. Before addressing the case study, an overview of the literature addressing the concept and features of PPPs will be offered, and the issue of accountability of prive actors will be addressed by drawing from various declinations of the doctrine of horizontal effects of human rights.

In the last chapter, before laying down the results of the research and formulating a series of contributions and recommendations, the data protection implications of financial investigations will be explored, in order to assess whether that legislative provision might provide for higher levels of protection of informational self-determination.

Chapter I

The legal framework on financial investigations

1 Introduction

The present research revolves around the notion, *ratio* and effects of financial investigations carried out in the context of criminal proceedings. In particular, the aim of the thesis is to explore the impact that assets-oriented investigative measures have on fundamental rights that are to be respected during crimminal prosecution, paying particular attention to the right of suspects and defendants not to incriminate themselves vis-à-vis public authorities. It might seem like a difficult task to achieve in light of the lack of a uniform and agreed-upon definition of financial investigations in EU legislation as well as in international hard law. However, the research intends to make an attempt to systematically compile the relevant pieces of legislation in order to outline a gneral statute on criminal financial investigations.

To that end, Section 2 introduces the system to combat money laundering and terrorsim financing laid down by the Financial Action Task Force, which encourages the adoption of common standards to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and predicate offences. The subsections therein further elaborate on specific key concepts, namely what is to be understood by "financial investigations" and who are the actors involved with a main focus on Financial Intelligence

Units.

Section 3 delves into the legal framework currently in place at the European Union level. Starting from the influence that the international community was increasingly exerting at the regional level on the implementation of a strong system against the economic effects of crime, the research will provide an overview of the historical and political background against which the EU criminal law policy was developed (§3). Furthermore, following the "twin-track" approach adopted by EU lawmakers, it will present the state of the art of the overall anti-money laundering and terrorism financing architecture addressing both its preventive and repressive courses of action (§3.1). Finally, the picture will be integrated with an overview of the instruments of judicial cooperation in criminal matters that are relevant to the purpose of chasing illicit money.

The chapter does not aspire to provide an exhaustive overview of the state of the art on the regulation of financial investigations. It is neither forgotten nor deliberately neglected that fundamental initiatives on the matter, both at the international and supranational level, exist and are indeed relevant. While acknowledging the importance of instruments such as the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988 and the UN Convention against Transnational Organized Crime of 12 December 2000, as well as regional conventions like the 1990 and the 2005 Council of Europe Conventions on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, the scope of the research will be limited to the EU legislation, as influenced by the FATF standards. As limited as it may seem, it was nonetheless sufficient to address the research questions outlined above.

2 The international standards: the role of the Financial Action Task Force

Money laundering became a major policy issue in the late 1980s, when the international community feared that the magnitude of cross-border drug trafficking could reach massive proportions not only for the devastating consequences it would

have on health and society[1], but most importantly for its economic impact[2]. The 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[3], although not explicitly mentioning money laundering, ackowledged for the first time «the links between illicit traffic and other related organized criminal activities which undermine the legitimate economies and threaten the stability, security and sovereignty of State»[4] and showed commitment to the effort of depriving criminals of their illicit gains through confiscation measures. By introducing provisions on the substantive criminalization of the offence of money laundering[5] as well as on the confiscation of proceeds of crime, the basis for an international anti-money laundering system was thus created[6] and the calls for better controls to prevent the exploitation of financial markets and licit economies by criminals multiplied[7]. From that moment on, with the proliferation of global emerging threats and the extension of the anti-money laundering criminal policy to other forms of economic crimes[8], the number of international and supranational

[1]G. Stessens, *Money Laundering: a new international law enforcement model, Cambridge, 2000*, p. 10, notes that «[w]hereas drugs were originally seen as an almost exclusively medical problem of drug users, the scope of the production, use and trafficking of drugs is nowadays of such a nature that drugs have come to be seen as a problem for society as a whole».

[2]As M.T. Nance, *The regime that FATF built: an introduction to the Financial Action Task Force*, in *Crime, Law, and Social Change*, 2018, 69, p. 111, puts it, «[m]oney laundering lies at the nexus of the licit and illicit economies and intertwines the two in dangerous ways».

[3]United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.

[4]Recital 3) 1988 UN Convention.

[5]According to V. Mitsilegas, *Money laundering counter-measures in the European Union: a new paradigm of security governance versus fundamental legal principles*, Ph.D. dissertation, University of Edinburgh, 2000, p. 70, the Convention created the offence of drug-related money laundering.

[6]E. Ioannides, *Fundamental principles of EU law against money laundering*, London, 2014, p. 13. According to G. Stessens, *Money Laundering*, cit., p. 11, «[t]he fight against money laundering was not just a new strategy in the fight against crime, but also in the fight against drug trafficking».

[7]G. Pavlidis, *Financial action task force and the fight against money laundering and the financing of terrorism. Quo vadimus?*, in *Journal of financial crime*, 2020, 28(3), p. 771.

[8]E. Ioannides, *Fundamental principles*, cit., p. 44, asserts that «[t]oday's global anti-money laundering system comprises a uniform regulatory framework with common objectives for the prosecution and sanctioning of different forms of economic crimes», such as financing of terrorism, corruption, insider dealing, human trafficking, etc. V. Mitsilegas, *Current and prospective responses: Countering the chameleon threat of dirty money*, in A. Edwards-P. Gill, *Transnation organized crime. Perspectives on global security*, London, 2003, p. 200 ff. refers to the emergence of organized crime as the global threatening phenomenon urging the extension of the

initiatives addressing the need to trace and recovery proceeds of crime increased. Several hard law instruments prove this trend, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the proceeds of crime, whose criminalization obligation upon States Parties is not strictly concerned with drug-related crimes but extends to the laundering of proceeds of any predicate offence[9]. However, the intervention of the international community was not limited to legally binding obligations, for soft law instruments have been enacted in the forms of recommendations and principles to provide for guidelines and global standards which would «permittent la formulation consensuelle de valeurs par un processus dynamique»[10] and that oftentimes are transposed into domestic legislations. This is the case of the international standards set out by the Financial Action Task Force (hereafter: FATF), whose establishment in 1989[11] signalled the growing interest of the international community in addressing the threats posed by the laundering of proceeds from drug and other forms of serious crime. Such inter-governamental body was primarily set up with the view to develop international standards to protect the integrity of the financial system, *i.e.* to prevent its misuse for crimiminal purposes as well as to propose measures to detect, prevent and punish money laundering[12].

The FATF, from a temporary international task force with a mandate limited

anti-money laundering framework.

[9] V. Mitsilegas, *Current and prospective responses*, cit., p. 201.

[10] U. Cassani, *L'internationalisation du droit pénal économique et la politique criminelle de la Suisse: la lutte contre le blanchiment d'argent*, in *Revue de droit suisse*, 2008, 127, p. 236.

[11] The Financial Action Task Force was created during the G7 Economic Summit held in Paris. As a consequence, some authors contend that the FATF AML/CTF policies so far have been governed and influenced by the Great Powers, that is a group of states of global economic relevance such as the US and its allies, except for the growing role played by the private sector. Cf. I.S. de Oliveira, *The governance of the financial action task force: an analysis of power and influence throughout the years*, in *Crime, Law and Social Change*, 2017, 69, p. 154 ff. Similarly, *B.A. Simmons*, *International efforts against money laundering*, in D. Shelton (ed), *Commitment and compliance: The role of non-binding norms in the international legal system*, Oxford, 2000, p. 244 ff. To the contrary, G. Pavladis, *Financial action task force*, cit., p. 766, concludes that by gradually expanding its membership to other countries, the FATF did not lose its legitimacy but rather made sure that its standards are the result of the experience and expertise of all the jurisdictions taking part in it.

[12] Fatf, *25 Years and Beyond: The Financial Action Task Force setting the standards to combat money laundering and the financing of terrorism and proliferation*, 2014, p. 6.

in time[13] and in scope[14], ultimately evolved into an open-ended mandate body[15] focusing on other relevant threats to the financial system beyond money laundering, such as terrorism financing and mass proliferation of weapons[16]. In order to achieve those objectives, in 1990 the FATF issued a soft law document containing 40 recommendations[17] setting out the standards to which its members are required to adjust their legal and operational frameworks to effectively counter the misuse of the financial system.

The 40 Recommendations therefore aimed at fostering the international *consensus* over legal and regulatory measures specifically addressing for the first time the misuse of the financial system for illicit purposes. Notwithstanding the democratic deficit claimed by some in light of the lack of representativeness,these recommendations have been complied with by most states and have been influential in the development of a new design of the fight against money laundering, according to which not only states are called on to implement measures addressing the profits of economic crimes but also private entities are made responsible for such effort[18].

In fact, most of the principles set out in the recommendations turn to financial

[13]The activity of the FATF was originally supposed to last until 1990.

[14]The FATF mandate initially was «to assess the results of cooperation already undertaken in order to prevent the utilisation of the banking system and financial institutions for the purpose of money laundering, and to consider additional preventive efforts in this field, including the adaptation of the legal and regulatory systems so as to enhance multilateral judicial assistance» according to G7, *Economic Declaration*, Paris, 1989.

[15]The choice was driven by the will to consolidate its global governance in controlling and preventing money laundering. See FATF, *Mandate approved by the Ministers and Representatives of the Financial Action Task Force*, Washington, DC, 12 April 2019. In practical terms, this implies minor changes in the FATF governance processes and the extension of the terms of the FATF presidency to a two-year period.

[16]Indeed, the material mandate of the FATF was expanded in 2001 as to also encompass terrorism financing-related activities by enacting nine Special Recommendations specifically related to the such threat. As observed by V. MITSILEGAS, *Current and prospective responses*, cit., p. 2017, while money laundering and terrorism financing behaviors show similarities to a certain extent, they differ insofar as terroristic activities may well be funded with legitimate money, thus compelling obliged entities to monitor not only the sources, but also the destination of monetary flows.

[17]The 40 Recommendations raise to 49 if considering the IX Special Recommendations on terrorism financing threats.

[18]U. CASSANI, *L'internationalisation du droit pénal économique*, cit., p. 247.

and banking institutions in their capacity of private businesses and commercial activities to task them with various obligations[19]. Indeed, from that moment on, private entities are required to verify the identity and the financial profile of potential new clients before estabishing business relationships with them according to Costumer Due Diligence Measures (CDD) and to terminate the contractual relationship if suspicions of crime arise[20]. They are also prevented from dismissing records on transactions, account files and business correspondence which shall be maintained for at least five years so as to provide, if necessary, evidence for prosecution of criminal activity[21].

Notably, the FATF Recommendations introduced a proactive duty for obliged entities to report to the domestic FIU any banking transaction if reasonable grounds arise to suspect that such funds are the proceeds of a criminal activity, or are related to terrorist financing[22] while also being compelled not to disclose the fact that a suspicious transaction report (STR) or related information is being filed with the FIU[23].

---

[19] As a consequence, as V. Mitsilegas, *Current and prospective responses*, cit., p. 199 puts it, the FATF Recommendations permanently changed commercial relationships.

[20] FATF Recommendation 10. It shall be mentioned that the urge to attribute relevance to the so-called Know Your Customer rule had already been catered for by the Basel Committee in Banking Supervision (BCBS), *i.e.* an informal group founded by the central bank governors of the G10 countries in 1975 with the aim to provide for international standards on the prudential regulation of banks. According to Principle II contained in the Basel Committee Statement, «With a view to ensuring that the financial system is not used as a channel for criminal funds, banks should make reasonable efforts to determine the true identity of all customers requesting the institution's services. (...) All banks should institute effective procedures for obtaining identification from new customers. It should be an explicit policy that significant business transactions will not be conducted with customers who fail to provide evidence of their identity». On the BCBS and its principles, see G. Lasagni, *Banking Supervision and Criminal Investigation. Comparing the EU and US Experiences*, Cham, 2019, p. 100 ff.

[21] FATF Recommendation 11.

[22] FATF Recommendation 20.

[23] FATF Recommendation 21. All the measured mentioned above are also extended by the FATF Recommendations to designated non-financial businesses and professions (DNFBPs) such as lawyers, notaries, trusts and company service provideers, when they engage in a suspicious transaction. On this last note, it has been observed how the standards conceived at the international level inevitably marked the reconceptualization of the lawyer-client relationship which was previously based on strict confidentiality rules. On the implications that this approach has not only on privacy but also on the rights of defendents, see V. Mitsilegas, *Countering the chameleon threat of dirty money*, cit., p. 203. For the choice made of the EU lawmakers in this regard, see *infra* §3.1.

What emerged from the above is that the overarching logic behind the international AML/CTF regime in general and the one designed by the FATF Recommendations in particular is preventive in nature, that is, it is guided by the will to reduce the crime by reducing the risk[24]. In fact, they are essentially a compound of three different systems of provisions, namely the criminal law concerning the criminalization of money laundering offences and the cooperation mechanisms between the private and public actors involved in the investigations, the bank sector-inspired rules concerning the prudential activity of financial institutions such as identification and surveillance measures, and lastly a monitoring and mutual evaluation procedure mechanism[25]. However, this should not suggest that the international standards set out by the FATF do not concern the prosecutorial aspect of money laundering-related behaviors. Instead, the recommendations outline the role that the private sector as well as the FIUs shall also have in criminal investigations dealing with proceeds-generating cases. "follow the money" approaches have arguably become the most crucial tool in addressing transnational crimes[26], as was recently reaffirmed by the international community[27]. The drastic change in the global governance of ML/TF crimes control brought about by the Financial Action Task Force urged scholarship to reflect on whether and to what

[24]M.T. Nance, *The regime that FATF built*, cit., p. 113.

[25]M. Delmas-Marty, *Les forces imaginantes du droit. le relatif er l'universel*, La Couleur des idées, Seuil, 1999, p. 279. On the mutual evaluation model launched for the first time by the FATF, cf. M. Levi, W. Gilmore, *Terrorist Finance, Money Laundering and the Rise and Rise of Mutual Evaluation: A New Paradigm for Crime Control?*, in M. Pieth (ed.), *Financing terrorsim*, Dodrecht, 2003, p. 95 ff., who describes how such system of periodic peer-reviews operate through on-site monitoring procedures and casts doubt on the apparent voluntary nature of international relations and on the lack of democratic control.

[26]M.T. Nance, *The regime that FATF built*, cit., p. 110.

[27]The UN Resolution 10/4 adopted by the Conference of the Parties to the e United Nations Convention against Transnational Organized Crime to promote its effective implementation, reiterates the urge for States parties «to conduct proactive investigations, including by investigating the movements of proceeds of crime and using financial investigative tools, in order to identify and disrupt any possible linkages between existing and emerging manifestations of transnational organized crime, money-laundering and the financing of terrorism, and effectively prosecute those crimes, in accordance with their national legislation». On the importance of this resolution and its implications for the fight against transnational crime, see A. Balsamo, *Il contrasto internazionale alla dimensione economica della criminalità organizzata: dall'impegno di Gaetano Costa alla "risoluzione Falcone" delle Nazioni Unite*, in *Sistema Penale*, 2020, p. 3 ff.

extent criminal procedural law is affected by the appearence of new actors, *e.g.* the private sector, new powers and new dynamics.

2.1 The notion of financial investigations

As highlighted above, a common definition of financial criminal investigations is missing in any international or supranational binding piece of legislation. In most domestic legal frameworks, no mention is made of financial investigations but traditional investigative measures are usually employed to deal with criminal proceeds[28].

The need to implement financial investigations in the prosecution of certain crimes to the widest extent possible was first acknowledged at the international level by the FATF, whose interpretative note to Recommendation 30 reads that a financial investigation is «an enquiry into the financial affairs related to a criminal activity, with a view to identifying the extent of criminal networks and/or the scale of criminality; identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and developing evidence which can be used in criminal proceedings»[29]. According to the same FATF standard, countries should make sure that law enforcement or other competent authorities are in the position to conduct pro-active parallel investigations. "Pro-active" refers to the fact that financial investigations shall be initiated before the undertaking of a criminal investigation[30] as in they are not triggered by a *notitia criminis* but rather by intelligence information previously

[28] As a consequence, a fragmented approach can be observed throughout national legislations when it comes to regulating assets recovery systems. See M. Simonato,M. Lassalle, *A fragmented approach to asset recovery and financial investigations: a threat to effective international judicial cooperation?*, in Z. Durdevic-E. Ivicevic Karas (eds), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, 2016, p. 136

[29] Fatf, Interpretative note to Recommendation 30 (Responsibilities of law enforceemnt and investigative authorities).

[30] M.Jimeno-Bulnes, *The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama*, in *New Journal of European criminal law*, 2017, 8(2), p. 173, describes proactive measures as those that are enforced *ante-delictum* in the absence of a prosecution, a crime or criminal proceedings.

gathered[31].

On the other hand, "parallel financial investigations" means that they are conducted alongside, or in the context of, a traditional criminal investigation into money laundering, terrorist financing and predicate offences in order to collect and analyse all available information with a view towards assisting in the prosecution of crime and in the deprivation of proceeds and instrumentalities of crime[32].

In light of the above, it seems that financial investigations - when performed in connection with traditional criminal prosecution - can serve a two-fold purpose. They either aim at gathering pieces of evidence to substantiate the charges against the person under investigation or they are intended to trace and identify financial assets to put under forfeiture. In any event, given that targeting the proceeds of crime is the ultimate goal of both parallel financial investigations and AML/CTF preventive measures[33], the identification of proceeds of crime, terrorist funds and other proceeds subject to confiscation and the gathering of evidence that can be used in criminal proceedings does not only enhance the overall effectiveness of a country's AML/CFT regime[34] but it also supports traditional criminal investigations into allegations of money laundering, predicate offences and terrorism financing. It is clear that the reason behind the call for an integrated financial investigation model[35] lies in the assumption that the link between the origins of the money, beneficiaries, when the money is received and where it is stored or deposited can provide information about and proof of criminal activity, according to the well-known "follow the money approach" logic.

In sum, although the FATF Recommendations provide for a general definition of what falls within the notion of financial investigations, the terms remain too

[31]M. Simonato,M. Lassalle, *A fragmented approach*, cit., p. 137. define these types of financial investigations as "intelligence-led investigations".

[32]*Ibid.*, p. 6

[33]R. Golobinek, *Financial investigations and confiscation of proceeds from crime: training manual for law enforcement and judiciary*, Council of Europe, 2006, p. 28. By measures for the prevention and detection of money laundering, the Author refers to the composite system in which FIUs perform their tasks.

[34]Fatf, *Operational Issues. Financial Investigations Guidance*, 2012, p. 3.

[35]According to R. Golobinek, *Financial investigations*, cit., p. 7, this would mean «from the suspicion of a criminal offence to the assets».

broad to build an harmonized policy across national legal systems: suffice it to think that criminal procedure rules differ as to whether and under what conditions intelligence information can be employed for evidentiary purposes in criminal prosecution.

This is not the only problematic feature of this type of investigative measures, in light of the fact that the term "financial investigations" refers to an umbrella concept, for it encompasses a broad range of investigating measures that vary in nature and in terms of degree of intrusiveness into the personal sphere of those targeted. Such measures can be inferred by the Fourty Recommendations themselves, although they were later systematized in 2005 by the Council of Europe Criminal Asset Recovery Convention[36], whose aim was to update the 1990 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime in light of the «new developments [witnessed in other international *fora* such as EU, UN, FATF] to ensure mutual consistency with these standards and to make possible harmonized domestic responses in an appropriate legal format».

According to a fourfold categorization following an ascending order, investigations aimed at depriving criminals of illicit proceeds should primarily consist of retrieving banking information on specified bank accounts, that is, whether natural or legal persons hold or control accounts as well as basic and beneficial ownership information, information held by tax authorities, information held in asset registries, and information held in citizenship, residency, or social benefit registries[37].

The second investigative measure with a low degree of coerciveness, consists of requesting information on past banking transactions that have been performed during a specific period through one or more specified accounts[38]. This information

[36]Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198), 16 May 2005 (the 'Warsaw Convention').

[37]FATF Recommendation (31). See also Warsaw Convention, Artt. 7, § 2, *b* and 17, according to which the Parties are required to put in place any measure to determine whether a natural or legal person is a holder or beneficial owner of one or more accounts and obtain the particulars of such bank accounts.

[38]Warsaw Convention, Artt. 7, § 2, b) and 18.

is usually requested through production orders[39], «which represent the original core of investigating techniques in the matter of banking data»[40] and shall address information already in the possession of the requested bank, which is compelled to provide it accordingly.

Financial investigations reveal an increasing intrusive nature when they involve real-time monitoring of banking operations that are being carried out through one or more identified accounts[41]. Indeed, such measure allows authorities to simultaneously intercept financial movements, localization and personal information of the persons involved. The real-time monitoring of financial movements is a mechanism aiming at better determining the licit or illicit origin of tranferred fund and therefore to allow competent authorities to rapidly identify, trace and freeze criminal property[42].

Clearly, this measure implies a higher risk of encroachment on fundamental rights, not differently from the last investigative measure contemplated by international standards, *i.e.* the postponement of transactions and freezing of assets[43]. These are considered as provisional measures, insofar as they are limited in time and usually lead up to a more definitive action. In the former case, the consent to financial transactions reported by obliged entities is suspended or withheld by FIUs or other competent authorities[44] for a limited period to grant them addi-

[39]Production orders are understood as «the powers of the authorities to inspect, copy or order the production of data, documents or other objects, in whatever form (oral, written, digital)», M. Luchtman, J. Vervaele, *Comparison of the legal frameworks*, in Id. (eds), *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with other EU law enforcement authorities (ECN/ESMA/ECB)*, April 2017, p. 268.

[40]G. Lasagni, *The new frontiers of financial investigation: banking supervision and real-time monitoring of financial records. A comparative analysis between the EU and the US*, Ph.D. thesis, University of Bologna, 2016.

[41]Fatf Recommendations (16), (26) and (27). Cf. Warsaw Convention, Artt. 7, § 2, *c* and 19. On the real-time monitoring of financial records, see extensively G. Lasagni, *Banking Supervision*, cit.

[42]Moneyval, *The postponement of financial transactions and the monitoring of bank accounts*, April 2013, p. 6.

[43]They can be considered as «a two-step procedure, where the first is prodromal to the adoption of the second», according to M. Simonato, M. Lassalle, *A fragmented approach*, cit., p. 143.

[44]According to Moneyval, *The postponement*, cit., p. 34, in most countries, law enforcement agencies do not have postponement powers as they are generally part of FIUs prerogatives; but of course when LEAs are involved in the procedure, the suspension of transactions have a criminal

tional time to analyze the operations and potentially confirm the suspicions[45]. The postponement of the transaction, if implemented, can lead to the freezing of assets[46] which represents the peak of the ascending systematization of these investigative tools, as it implies the power of «temporarily prohibiting the transfer, destruction, conversion, disposition or movement of property or temporarily assuming custody or control of property on the basis of an order issued by a court or other competent authority»[47].

In sum, assets freezing is understood as a seizure measure[48] of a provisional nature, therefore usually performed during the pre-trial phase[49], and with preventive purposes, *i.e.* to prevent money to be reinvested into the legal economy or the consequences of the crime to be exacerbated, or to gather evidence that can be used in criminal proceedings[50].

Being a temporary measure, freezing orders pursue the objective to ensure the effective execution of a confiscation measure and are therefore usually followed by the final forfeiture of the criminal property and/or the property of corresponding value. Confiscation represents the cornerstone of the international and EU legislative assets recovery frameworks which have been developed over the years by means of legal instruments focused on countering criminal phenomena such as money laundering and related predicate offences[51], terrorism financing, and

---

procedure nature.

[45] FATF Recommendation 4). See also Warsaw Convention, Art. 14.

[46] Cf. Interpretative Note to FATF Recommendation 4), according to which the duration of the suspansion of the transaction should «allow sufficient time to analyse the transaction and for competent authorities to initiate, where appropriate, an action to freeze or seize».

[47] Warsaw Convention, Art. 1, lett. g). See FATF Recommendations 4), 16) and 30)

[48] As noted by O. CAHAN, J. TRICOT, *Procedural aspects of freezing in Europe. A comparative analysis (Belgium, France, Germany, Italy, Netherlands, Romania)*, in A. BERNARDI (ed.), *Improving confiscation procedures in the European Union*, Naples, 2019, p. 502, with reference to the EU legislative framework, «it is through the "seizure" procedures that Member States implement EU law requirements relating to the freezing».

[49] As such, it is usually regulated by the national codes of criminal procedure.

[50] *Ibid.*, p. 505, where the Authors observe that most of the legal orders studied are characterized by the distinction between evidentiary seizures and the seizures for the purpose of confiscation.

[51] Cf. for example, the UN Convention against Corruption (the 'Merida Convention') adopted on 31st October 2003 by resolution 58/4 which invites States Parties to put in place confiscation measures to deprive criminals of the values derived from bribery and other corruption offences linked to money laundering.

organized crime[52].

The reason why confiscation has gained such a pivotal role in the fight against the most serious forms of crime lies in the principle according to which offenders should not be left with the profits they made by committing the crime[53], according to the renowned saying that «crime does not pay».

The issue related to which types of assets and values in general can be subjected to freezing and confiscation measures holds a particular relevance for the present research, inasmuch as the property and values targeted by financial investigations determine the degree of intrusiveness of said investigations into the personal sphere of those interested, with clear consequences on the procedural safeguards that shall be granted to them. This holds all the more true when it comes to asset freezing measures in light of the impactful effects they have on the enjoyment of fundamental rights of those targeted, as well as the increasingly relevant role they have in tackling economic crimes both in a domestic and cross-border setting.

According to Art. 5 Warsaw Convention, competent authorities should be able to freeze or confiscate «the property into which the proceeds have been transformed or converted (...)», where "property" stands for «property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title to or interest in such property»[54] and "proceeds" encompass any economic advantage derived directly or indirectly ob-

[52]The most prominent international text on organized crime which deals with the illicit profits deriving therefrom is the UN Convention against transnational organized crime (the Palermo Convention) adopted on 15th November 2000 by Resolution 55/25, whose Art. 12 calls on States Parties to enable the confiscation of proceeds of crime or other benefits derived from organized crime. The Convention also addresses the issue of international cooperation through mutual legal assistance mechanisms for purposes of confiscation and that of the management of confiscated proceeds of crime, which is the final phase of the assets recovery procedure. On the Palermo Convention and its impact as the most widely ratified international covenant, see A. Balsamo, *Il contrasto internazionale*, cit.; R. Virzo, *La confisca nell'azione internazionale di contrasto ad attività criminali*, Naples, 2020.

[53]For a law and economics analysis of the confiscation of proceeds from crime, please refer to R. Bowles, M. Faure, N. Garoupa, *Forfeiture of illegal gain: an economic perspective*, in *Oxford Journal of Legal Studies*, 2005, 25(2), p. 276, in which the Authors challenge the idea according to which from a criminal policy perspective the removal of illegal gains is always considered to be a highly effective tool against crime due to its deterrence effects.

[54]Warsaw Convention, Art. 1, lett. *b*.

tained from criminal offences[55]. In light of the above, monetary funds held in bank accounts, as well as cash and financial instruments, may fall within the material scope of reach of freezing and confiscation measures when conducting a financial criminal investigation.

To preliminary conclude on the definition of financial investigations to adopt for the purposes of this work, it may be mantained that a financial investigation is an enquiry into the financial affairs allegedly related to a criminal activity with a view to prevent the abuse of the financial and banking system for illicit purposes or support the prosecution of money laundering, terrorism financing, and predicate offences, for the purpose of gathering evidence or removing assets for future confiscation. It may also be concluded that if financial investigations are conducted together with criminal investigations, and therefore involve both non-judicial and judicial authorities which are competent in prosecuting money-laundering and terrorsim financing, then they can be defined as "criminal financial investigations".

In the following paragraph, the analysis will focus on the key actor in conducting financial investigations, that is, the Financial Intelligence Units, in order to provide a picture of their role and their interaction with law enforcement and judicial authorities.

2.2 The actors: Financial Intelligence Units and their network

Among the recommended measures that need to be implemented by national lawmakers, one in particular stands out for the functioning of the AML/CTF architecture. Recommendation (29) calls on countries to establish central and independent units tasked with the specific mandate to receive and analyze reports on suspicious transactions filed by the private sector and to access information held in other sources to possibly disseminate them with law enforcement, judicial,

[55] Warsaw Convention, Art. 1, lett. *a*.

or other adminstrative autorities[56]. The Financial Intelligence Units (hereafter: FIUs) were consequently created, with the mandate to act as a filter or "buffer"[57] between the financial sector and law enforcement and judicial authorities that have jurisdiction over the investigation and prosecution of allegations of money laundering and related offenses[58].

The creation of an autonomous and centrilised body specifically tasked with the processing of extensive mole of information on financial movements has the advantage of unburdening the workload of the justice system as well as to support the action of competent authorities against wrongdoers. Concerning the latter point, law enforcement and judicial agencies often lack the necessary informational and operational background to trace illicit monetary flows and therefore reduce the information asymmetry that occurs in the prosecution of economic crimes[59].

This informational gap is bridged by the intelligence gathering activity performed by specialized agencies, *i.e.* the FIUs, whose expertise and dedicated channels allow public authorities to compensate for the information asymmetry occurring between justice and the illicit market where proceeds of crime flow freely.

In order to build a sustainable coordination between FIUs and competent authoritities in their exchange of financial data - both nationally and at the international level - the Egmont Group of Financial Intelligence Units (the Egmont Group) was established in 1995 to provide a forum for FIUs to improve support to their national AML programs, namely to foster better and more secure communi-

[56]According to G. Stessens, *Money Laundering*, cit., p. 184, FIUs serve a «repository function» as in they constitute the centralised venue where information on ML/TF are gathered and controlled, as well as an «analysis function» when they process the information received from reporting entities.

[57]M. Penna, *The 'pre-investigative' role of Fianncial Intelligence Units in recovering assets*, in K. Ligeti-M. Simonato (eds), *Chasing Criminal Money: Challenges and Perspectives on Asset Recovery in the EU*, Oxfor-Portland, 2017, p. 271.

[58]G. Stessens, *Money Laundering*, cit., p. 184, mentions the «clearing house function» of FIUs to refer to the role they play in conducting and facilitating the exchange of information between various actors such as domestic regulatory agencies, domestic judicial authorities, or foreign FIUs.

[59]I. Deleanu, *Information flows and repressive enforcement*, cit., p. 130., claims that when such an asymmetry is not reduced, the benefits deriving from laundering transactions exceed those of legal transactions and therefore foster the commission of money laundering-related crimes.

cations between them, improve their expertise, and expand the exchange of information. This informal organization[60], currently consisting of 177 FIUs members[61] and intergovernmental organizations as non-member observers such as Europol, the World Bank and the International Monetary Fund, not only helped fostering the international community's interest towards the swift and secure exchange of data[62], but it also strongly called for the establishment of an international cooperation network fostering «the widest possible cooperation and exchange of information with other Egmont Group FIUs on the basis of reciprocity or mutual agreement»[63].

Furthermore, the development of international cooperation mechanisms between FIUs represents the opportunity for competent authorities to use channels for the exchange of information that are faster than other mechanisms contemplated by mutual legal assistance instruments. In fact, when financial data ought to be retrieved abroad, law enforcement and judicial authorities might opt for the FIU channel to determine whether it is worth sending out a request for international cooperation[64]. In this regard, for the first time before the actione of the European Union [65], the Egmont Group established the Egmont secure Web (ESW), that is, an Internet encrypted system through which FIUs may exchange expertise and financial intelligence or send requests of cooperation[66].

[60]Countries that join the Egmont Group do not participate in any international treaty or convention, therefore there are no international sanction regimes in place in case of non-compliance. However, the body is developed according to a vertical structure whose peak is represented by a governance collegial body - the Heads of Financial Intelligence Units (HoFIU) which has the power to expel or suspend non-compliant FIUs.

[61]Updated data may bu found at https://egmontgroup.org/members-by-region/eg-member-fiu-information/.

[62]V. Mitsilegas, *New forms of transnational policing: The emergence of Financial Intelligence Units in the European Union and the challenges for human rights: Part 1*, in *Journal of Money Laundering Control*, 3(3), p. 156.

[63]Egmont Group, *Egmont Group of Financial Intelligence Units Charter*, October 2013, at 3.1), p. 8. FATF Recommendations had already encouraged countries to improve international cooperation with foreign FIUs according to the principles set out in the Interpretative Note to Recommendation 40.

[64]A. Amicelle, K. Chaudieu, *In search of transnational financial intelligence: questioning cooperation between Financial Intelligence Units*, in C. King-C. Walker-J. Gurulé (eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Cham, 2018, p. 652.

[65]See *infra* §3.1.1.

[66]Cf. Egmont Group, *Egmont Group of Financial Intelligence Units Charter*, cit., at. 3.3).

This FIU-to-FIU communication channel permits members to communicate with one another via secure e-mail requesting and sharing case information, which is however not limited to FIUs but it can also involve other authorities according to an indirect "diagonal coooperation" scheme[67], where FIUs operate as mediators between foreign law enforcement authorities asking each other relevant data[68].

The key role that an up-to-date and fast information sharing system between FIUs has gained throughout the years clearly accounts for the relevant position that intelligence agencies have been recognized. Regarding the FIUs, while it is known that they were originally established as the cornerstone of the international legal architecture on the prevention of risks of money laundering and terrorism financing, it should also be noted that other functions have been assigned to them beyond their core tasks - namely the receipt, analysis, and dissemination of financial intelligence - which may entail a more active role in the detection of crimes.

To start with, it should not be excluded that under the FATF framework FIUs may start an analysis regardless of the previous receipt of a report from the financial sector[69]. Suspicious transaction reports are not the only source of information that FIUs can pool relevant data from, insofar as their activity can also be triggered by public prosecutors and law enforcement, the press, or by foreign counterparts, as well as be initiated on their own accord. Furthermore, FIUs are entrusted with the power to obtain additional information from reporting entities as needed to perform their analysis properly, but also from entities which have not previously submitted a report[70].

See also V. Mitsilegas, *New forms of transnational policing*, cit., p. 156.

[67]G. Pavlidis, *Financial information in the context of anti-money laundering: broadening the access of law enforcement and facilitating information exchanges*, in *Journal of Money Laundering Control*, 2020, 23(2), p. 374. Cf. also A. Amicelle, K. Chaudieu, *In search of transnational financial intelligence*, cit., p. 652.

[68]However, indirect access to investigative information inevitably appears cumbersome to some as compared to the direct access of law enforcement to centralized bank account registries. EU legislator has addressed the issue as il will be see *infra* at § 3.1.1.

[69]J.B. Maillart, *The Anti-Money Laundering Architecture of the FATF*, in B. Vogel-J.B. Maillart (eds), *National and international Anti-Money Laundering Law. Developing the Architecture of Criminal Justice, Regulation and Data Protection*, Cambridge, 2022, p. 47.

[70]*Ibid.*, p. 45.

As seen in the preceding section, according to the FATF Recommendations FIUs should also be able to withhold consent to the execution of a financial transaction reported by the private sector, concretely blocking it for a limited period in order to have more time to determine whether it is related to criminal activity or not[71]. During this time - and in cases in which the FIU lacks the power to do it autonomously - judicial authorities are able to step in and judicially freeze or seize the transactions and the related bank accounts if the suspicion is well-founded.

Whether they exclusively belong to the Egmont Group or are also EU FIUs since they are established in an EU Member State, the institutional nature of FIUs can be referred to one of the four models that have been identified from the setting-up of such units in the early 1990s[72].

As a matter of fact, neither the FATF nor the Egmont Group outlined an internationally accepted model for the status and functions of FIUs, thus leaving a great margin to national systems[73]. According to this systematization, which has been primarily enforced by the Egmont Committee[74], FIUs may be established within an already existing or newly created police department[75], such as a financial crimes unit, in order to take advantage of the experience developed by law enforcement in processing and exchanging data.

As has been noted, police-type FIUs[76] appear to be the most efficient solution

[71]Cf. Fatf Recommendation (4)

[72]Cf. J.F. Thony, *Processing financial information in money laundering matters: the financial intelligence units*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 4(3), 1996, p. 264 ff. See also International Monetary Fund, *Financial Intelligence Units: an overview*, Washington D.C., 2004, p. 9 ff.

[73]G. Pavlidis, *Financial information*, cit., p. 372. The issue has neither been addressed by the European legislator in the so-called Anti-Money Laundering Directives. See V. Mitsilegas, *New forms of transnational policing*, cit, pp. 147 ff. See below at 3.1.1.

[74]I. Deleanu, *FIUs in the European Union - facts and figures, functions and facilities*, in B. Unger-J. Ferwerda-M. Van Den Broek- I. Deleanu, *The economic and legal effectiveness of the European Union's Anti-money laundering policy*, Cheltenham-Northampton, 2014, p. 100.

[75]In those countries where a law-enforcement FIUs was set up, it was created as part of a law enforcement agency so as to avoid having to design a new entity with a new legal framework from scratch.

[76]According to A. J. Marcus, *Financial intelligence units (FIUs): Effective institutional design, mandate and powers*, Transparency International, July 2019, law-enforcement-type FIUs are the second most common model among the members of the Egmont Group with a total

when there is a high risk of informational decay, *i.e.* when the dispersion of information deemed to be irrelevant in their transmigration to competent authorities might seriously compromise the effectinveness of the AML/CTF system, precisely because of the knowledge that police FIUs would have of what prosecution services need[77].

Under the law enforcement model, FIUs may have access to the entirety of information sources and databes already available to police forces; moreover, information flows can occur more freely between law enforcement agencies and those FIUs - both domestically and at the international level - on an informal basis. As far as their function is concerned, law enforcement-type FIUs usually have the same investigative powers as the law-enforcement authority and may therefore freeze funds and bank accounts as well as carry out searches and interrogation under the degree of judicial supervision provided for in that specific country[78]. However, police FIUs can have a discouraging effect for the reporting entities and their clients, since the proximity between the latter and prosecutorial services may prevent them from disclosing information that is a mere suspicion of crime but could nonetheless be further used in the investigation of any type of crime[79].

FIUs can also be established according to a judicial-type model when they are part of the judiciary, namely the prosecution services. This circumstance clearly guarantees a higher degree of independence of the units from political interference[80]. In this case, the FIU is integrated within the justice system and the public prosecutor serves as a filter in determining which information reveal serious suspicions of crime being committed and deserve further investigation and which ones

number of 19 jurisdictions.

[77] I. Deleanu, *Information flows and repressive enforcement*, cit., p. 136.

[78] M. Penna, *The 'pre-investigative' role*, cit., p. 272.

[79] «[W]hat may be no more than a suspicion on the part of a banker may become a clue for the police or even an assumption», J.F. Thony, *Processing financial information*, cit. p. 267.

[80] Such independence might inspire confidence with financial institutions but discourage them as well as the role of the judicial FIUs only substantiates in transmitting the reports to the police unit. Cf. G. Stessens, *Money Laundering: a new international law enforcement model*, cit., p. 187. On different notes, J.F. Thony, *Processing financial information*, cit., p. 268, where he points out that reporting entities would put more confidence in prosecutorial-type FIUs in that the public prosecutor should have the capacity to identify possible error of judgment and therefore not transmit the irrelevant report to the investigative bodies.

do not.

In the former case, an official investigation may be initiated under the supervision of the public prosecutor, with a low risk of losing the information disclosed by the financial sector[81]. Prosecutorial-type FIUs have the judicial powers that are usually attributed to prosecuting authorities, that can also be of a coercive nature, such as freezing of funds, searching, and questioning, which may be exercised more rapidly. However, while they share the same cons of the law enforcement model, namely the possible discouraging effect on the financial sector, judicial FIUs cannot share the information gathered with other authorities as freely as law-enforcement FIUs do.

Finally, FIUs can be designed as administrative authorities, which can be completely independent[82] or rather be subjected to the supervision of a Ministry[83] or other governamental bodies[84].

Administrative FIUs were established for preventive purposes, that is, to receive, analyze, and disseminate financial data that may reveal the commission of money laundering-related crimes. As a consequence, they do not have judicial powers. However, in some countries FIUs have gradually been given investigative powers in order to effectively support the action of law enforcement and judicial authorities. Indeed, they may be provided with the power to postpone the execution of a suspicious financial transaction for a limited period of time, or even freeze bank accounts linked to criminals or criminal groups.

Financial data so obtained are not intentended to be freely disseminated and used for any purpose, as according to the so-called «specialty principle», the information received by a FIU shall only be employed for the purpose it was originally

[81]Since criminal prosecution depends on the information gathered by investigative authorities and passed on to the public prosecutor's office, the establishment of the FIU within the office itself reduces information dispersion

[82]For instance, the Belgian FIU - *Cellule de Traitement des Information Financères* (CTIF) - enjoys a high degree of budgetary as well as organizational and decision making independence. It also has its own legal personality.

[83]As the case of France, where the TRACFIN (*Traitement du Renseignement et Action contre les Circuits Financiers Clandestins*) reports to the Ministry of Finance.

[84]The Italian experience belongs to this typology, as it is located within the Bank of Italy.

gathered for or for a specifically defined one[85]. Consequently, not only should this information not be shared for tax-related purposes, but its subsequent use as evidence in criminal proceedings shall not be presumed as it depends on national legislative provisions[86].

In conclusion, the presentation of the different typologies of FIUs that can be encountered across Egmont Group members suggests that criminal investigations that deal with proceeds-generating cases may involve a wide variety of authorities with different legal nature and constituent mandates interacting with each other. As will be shown below, the FIUs established in the Member States of the European Union lack a uniform regulation and thus reflect the same features as far as their institutional status and relation with the other public authorities are concerned. Before addressing this issue, the EU legsislative framework applicable to financial investigations will be presented.

3 The European Union's action against dirty money: a success story?

The growing interest of the international community in the challenges represented by illicit proceeds from crime and in the development of prevention and repression policies to address such threats is also reflected at the regional level. Not only did the European Community/European Union actively participate in several international initiatives addressing the regulation of money laundering and

[85]Nonetheless, as pointed out by G. Stessens, *Money Laundering*, cit., p. 187, judicial-type FIUs may be exempted from the limitation deriving from the principle at stake given that national public prosecutors are empowered to further investigate any report which comes to their attention even beyond ML/TF crime allegations. This is the internal relevance of the specialty principle, which also plays a role in the international cooperation between competent authorities, inasmuch as exchanged information should be used only for the purpose for which the information was sought or provided unless a prior authorization is requested. Cf. Fatf, Interpretative Note to Recommendation 40. Cf. also Egmont Group, *Principles for information exchange between Financial Intelligence Units*, July 2013, at 32), p.6.

[86]Indeed, FATF Recommendations do not address the issue. See J.B. Maillart, *The Anti-Money Laundering Architecture of the FATF*, cit. p. 56.

the use of the financial system for illicit purposes[87], but it also strived to adapt its framework to the new international standards. Hence, the inclusion within the European security agenda of measures addressing illicit financial flows from serious forms of crime.

The *ratio* behind the establishment of such a priority cannot be fully comprehended without taking into account the efforts put in place to address the emerging phenomen of organized crime. It was not until the 1990s[88] that organized criminal groups, and the particular crimes usually related to them, such as money laundering, terrorism, and drug trafficking[89], shaking civil society and justice systems across Europe urged EU institutions to underscore «the need for a coherent and coordinated approach by the Union»[90].

As the provisions set out by the Treaty of Maastricht informing the third pillar[91]

[87]The European Commission as well as the EU Member States were parties to the Financial Action Task Force and actively participated in the development of the 40 Recommendations. See W. Gilmore, *Dirty money: the evolution of international measures to counter money laundering and the financing of terrorism*, Strasbourg, 1999, p. 89.

[88]According to M. Fichera, *Organised crime: developments and challenges for an enlarged European Union*, in C. Eckes, T. Konstadinides, *Crime within the Area of Freedom, Security and Justice. A European Public Order*, Cambridge, 2011, p. 162 ff., the factors revealing the urge for EU institutions to strengthen their fight against organized crime are to be identified in the global governance following the fall of the Berlin Wall, where organized crime represented the most threatening non-military danger; moreover, in the free movement of persons, capitals and goods in the aftermath of the establishment of an internal market free from borders control; thirdly, in the globalization of criminal trafficks and trafficking routes.

[89]For a sociological overview over the modern structures of criminal groups and their elected illicit businesses, see A. La Spina, *The role of organized crime in illicit trades: drug trafficking, migrant smuggling, arms trafficking and cigarette smuggling*, in V. Militello-A. Spena-A. Mangiaracina-L. Siracusa (eds), *I traffici illeciti nel mediterraneo. Persone, Stupefacenti, Tabacco*, Torino, 2019, pp. 67-79.

[90]Dublin European Council, 13 and 14 December 1996, Presidency Conclusions

[91]It is widely known that the Maastricht Treaty construed the European Union according to a pillar structure, where the First Pillar concerned the European Communitites and was thus regulated according to a communitarian model; the Second Pillar was constituted by the common foreign and security policy (CFSP) which, together with the Third Pillar on the Justice and Home Affairs (JHA) policy, fashioned an intergovernmental set-up. For in-depth insights on the structure of the Union in the aftermath of the Treaty of Maastricht, see D. Curtin, *The constitutional structure of the Union: a Europe of bits and pieces*, in *Common Market Law Review*, 1993, 30, pp. 17-69. The Third Pillar was intuitively related by R. Morgan, *The Third Pillar: an introduction*, in J. Monar-R. Morgan (eds), *The Third Pillar of the European Union. Cooperation in the fields of justice and home affairs*, Bruxelles, 1994, p. 14, to the abolition of frontiers within the internal market, because «if the State authorities can no longer use the existence of a frontier to control what passes across, or control the activity, then

in general[92], and the field of police and judicial cooperation in criminal matters in particular, did not appear to be appropriate to cater for an effective and organic common criminal policy geared towards the long-craved-for European integration[93], nor did the Treaty expressly mention organized crime, the Treaty of the European Union was to undergo fundamental reforms as far as the Third Pillar was concerned[94].

Therefore, in 1996 an intergovernmental conference was tasked with preparing the reform of the Treaty of Maastricht[95], which led to the adoption of the Treaty of Amsterdam[96], signed on 2 October 1997 and entered into force on 1 May 1999. Although the amendments brought by the new Treaty entailed major changes to the institutional framework of the Union[97], the keystone for the EU criminal policy

other means, compensatory means of controlling these activities have to be found». Among the unlimited literature on the JHA, see S. Peers, *EU Justice and Home Affairs Law*, 5th edn, Oxford, 2024; R. Morgan, *The Third Pillar: an introduction*, cit.

[92]In the words of J. Monar, *Justice and Home Affairs: The Treaty of Maastricht as a decisive intergovernmental gate opener*, in *Journal of European Integration*, 2012, p. 718, «the old 'third pillar' introduced by the Treaty of Maastricht appears in retrospect a very 'thin' basis» for the creation of a solid Justice and Home Affairs policy.

[93]Differently than what had been established for first and second pillar law measures, as noted by V. Mitsilegas, *EU Criminal law*, cit., p. 10. The Author further explains how the marginalised role attributed by the Treaty to the European Parliament, the European Commission and more strikingly to the Court of Justice revealed the strong reluctance of Member States to hand over their control in criminal law matters. For an orverview of the flaws of the Maastricht Treaty, which nevertheless did not diminish the ground-breaking value it represented for further developments in the JHA policy, see J. Monar, *Justice and Home Affairs*, cit.

[94]Commission, *Reinforcing political union and preparing for enlargement*, COM(96) 90, 28.2.1996, pp. 5 ff., which identifies the main shortcomings of the Justice and Home Affairs policy in the lack of democratic and judicial review, as well as in the use of «outdated methods and resources», such as the unanimity rule for decision-making and the adoption of non-binding legal instruments.

[95]Art. N, par. 2, TEU provided for the establishment of a conference of representatives of the governments of the Member States to gather in 1996 to discuss the revisions to the Treaty.

[96]Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ C 340/01, 10 november 1997.

[97]The topic concerning the reforms brought about by the Amsterdam Treaty would require extensive further attention which is beyond the scope of this thesis. However, it should be here mentioned that the Amsterdam Treaty «commnunitarized» specific areas previously falling under the competence of the Union, namely visas, asylum, immigration, borders and cooperation in civil matters. To the contrary, the provisions on police and judicial cooperation in criminal matters were retained in the Third Pillar, namely in Title VI which is now renamed "provisions on police and judicial cooperation in criminal matters". Not only did it mark a step forward towards integration as, in the words of R. Barents, *Some observations on the Treaty of Amsterdam*,

development was represented by the creation of an Area of Freedom, Security and Justice where to ensure a high level of safety «by preventing and combating crime, organised or otherwise»[98]. Pursuant to the new Art. 29 EU Treaty, the EU third pillar competences in criminal law were thus expanded to encompass the prevention and repression of crime, organised or otherwise, in particular terrorism, trafficking in persons and offences against children, illicit drug trafficking and illicit arms trafficking, corruption and fraud, by means of strengthening the cooperation between enforcement agencies, judicial authorities and also through legislative approximation in criminal matters.

However, the strengthening of the provisions on police and judicial cooperation in criminal matters did not happen in a vacuum. Previous initiatives had indeed already shown signs of the urge to better address emerging phenomena

in *Maastricht Journal of European and Comparative Law*, 1997, 4(4), p. 341, «it is now clearly recognized that matters of criminal law, a sacred domain of national sovereignty, will become an explicit part of the Union's activities», but it also watered down the intergovernmental features that had characterized the JHA policy in the aftermath of Maastricht, by providing for greater democratic oversight. On that note, see C. Fijnaut, *A peaceful revolution: the development of police and judicial cooperation in the European Union*, Cambridge, 2019, pp. 216 ff. The Amsterdam Treaty also addressed other relevant aspects for the construction of a criminal law field, most importantly the new legislative instruments that could be adopted, the potential jurisdiction of the Court of Justice over the validity and interpretation of Thirs Pillar instruments and the role of the European Parliament and the Commission in the legislative procedure. For an overview, S. Miettinen, *Criminal law and policy in the European Union*, London, 2013, p. 30 ff. Among the wide scholarship addressing the different profiles touched upon by the Amsterdam Treaty, see G. Gaja, *How Flexible Is Flexibility Under the Amsterdam Treaty?*, in *Common Market Law Review*, 1998, 35(4), pp. 855-870 on the "closer cooperation" procedure; M. den Boer, *An Area of Freedom, Security and Justice: bogged down by compromise*, in P. Twomey-D. O'Keeffe (eds), *Legal Issues of the Amsterdam Treaty*, Oxford-Portland, 1999, pp. 303-322.

[98]The creation of an Area of Freedom, Security and Justice within which the Community would ensure that citizens could enjoy their right to free movement as well as provide them with a high level of safety, had already been substantially envisaged by the Maastricht Treaty of 1992, although not formally labeling it as such. In fact, what was at that time known as the third pillar concerning the field of Justice and Home Affairs, provided for a series of areas of *common interest* in which Member States were supposed to cooperate for the sake of achieving the objectives of the Union, «in particular the free movement of persons», such as asylum and immigration policy, judicial and police cooperation in criminal matters to prevent and combat drug-related crimes, terrorism, and other forms of international crime. Cf. Art. K.1 TEU. For an overview on the evolution of the third pillar law throughout the Treaties' amendements until the final abolition of the pillar structure by the Lisbon Treaty, see V. Mitsilegas, *EU Criminal Law*, Oxford, 2009, pp. 9-23; C. Fijnaut, *A peaceful revolution*, cit., pp. 143-438; S. Peers, *EU Justice and Home Affairs Law, Vol. II*, cit., pp. 5-58.

such as organized crime and cross-border criminality. In December 1996, during the European Council gathered in Dublin a High Level Group was created to work out a strategy to step up the fight against organized crime. It resulted in the development of the Action Plan to Combat Organized Crime[99] which mapped out political guidelines and recommendations to be adopted by Member States[100] to ensure legislative harmonization and stronger cooperation to the widest extent possible. The added value of the Action Plan lies in the attention that the European Council paid to the profit-driven interests of organized crime, thus calling for a stronger set of «legislation in the field of confiscation of the proceeds from crime and the laundering of such proceeds»[101], which was operatively transposed in the need to strengthen the legal basis to allow investigations into money laundering as well as the tracing and seizure procedures of illegal assets[102].

The approval of the Action Plan by the Amsterdam European Council marked a step forward in the gradual evolution of the EU criminal law framework, which had not been fructiferous under the framework set out by the Maastricht Treaty[103]

[99]Action Plan to Combat Organized Crime (OJ 97/C 251/1). The Action Plan was approved by the European Council during the Amsterdam summit on 16 and 17 June 1997 which preluded the adoption of the Amsterdam Treaty.

[100]A brief analysis of the recommendations set out in the Action Plan and the state of play on the fight against organized crime in several Member States is carried out by M. DE BOER, *The fight against organised crime in Europe: a comparative perspective*, in *European Journal on Criminal Policy and Research*, 9, 2001, pp. 259-272. See also M. FICHERA, *Organised crime*, cit. p. 164 ff., who points out the shortcomings of the Action Plan, although acknowledging the impetus it gave to the following initiatives in the field of EU criminal law such as legislation, policy recommendations, action plans, which resulted in a comprehensive strategy against organized crime headed *The prevention and control of organised crime: a strategy for the beginning of the new millennium* (OJ C 124 of 3 May 2000).

[101]Political Guideline 11) of the Action Plan.

[102]Recommendation 26(b) of the Action Plan. In the same paragraph, the Action Plan calls for the criminalisation of laundering of proceeds from crime to be as general as possible. How pointed out by V. MITSILEGAS, J. MONAR, W. REES, *The European Union and Internal Security: Guardian of the People?*, Houndmills, 2003, p. 100, this is due to the fact that while money laundering legislation had already been enacted, that was by means of internal market/free movement legal basis instruments which therefore could not constitute the ground for criminal law provisions. The reference is to the AML Directives that had been delivered prior to the Maastricht Treaty and the Action Plan, whose evolution and the contitutional issues they raised will be extensively addressed below in § 3.1.

[103]According to V. MITSILEGAS, J. MONAR, W. REES, *The European Union and Internal Security*, cit., p. 91, the Action Plan on organized crime represented a boosting initiative for EU measures in criminal law, also due to the tight deadlines provided for to take action.

and which, to the contrary, was fostered by the Treaty of Amsterdam in light of the institutional amendments it brought about[104].

While the commitment of EU institutions to set out a stronger and comprehensive criminal policy against serious forms of organized and eonomic crime had been reitered in several institutional circumstances[105], it was the Treaty of Lisbon to actually improve the fight against crime within the Area of Freedom, Security

[104]Based on the recommendations set out in the Action Plan, several third pillar initiatives in the form of Joint Actions were concluded with the aim to harmonize national legislations. For instance, Joint Action 98/699/JHA of 3 December 1998 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime was adopted, as well as Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union. Cf. L. Salazar, *La lotta alla criminalità nell'Unione: passi in avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il Programma dell'Aia*, in *Cass. pen.*, 2004, pp. 3522. These acts, while they had an inspiring effect on the subsequent outline of the Amsterdam Treaty, were repealed in the following years by the newly introduced legislative instruments, *i.e.* Framework Decisions. The Joint Action on participation in criminal groups was repealed by Framework Decision 2008/841/JHA. For an overview on the FD, see F. Calderoni, *Organized crime legislation in the European Union*, Springer, 2010. On the Joint Action on money laundering, see below § 3.2.

[105]How pointed out by C. Fijnaut, *A peaceful revolution*, cit., p. 221, the implementation process of the Amsterdam Treaty appeared fragmented in a set of overlapping frameworks. During the summit held in Cardiff in June 1998, the Heads of State and Governments called for an Action Plan on how best to implement the provisions of the Treaty of Amsterdam on an Area of Freedom, Security and Justice, which was subsequently adopted by the European Council on 3 December 1998 at the Vienna summit. Among the five priorities pointed out, the Vienna Action Plan called for the strenghtening of the action against money laundering. Interestinlgy, the European Council also submitted the need for the exchange, collection and storage of data «concerning dubious financial transactions, criminal records, cross-border crime or on-going investigations» to be developed to increase the effectiveness of the action. An important step towards the promotion of progress in the Area of Freedom, Security and Justice as set out by the Treaty of Amsterdam is represented by the Tampere European Council held in October 1999, in whose conclusions it is vividly explained that «[m]oney laundering is at the very heart of organised crime» and that it «should be rooted out wherever it occurs» by way of improving procedures to trace, freeze, seize and confiscate proceeds of crime as well as by implementing EU provisions on money laundering, the 1990 Strasbourg Convention and the Financial Action Task Force recommendations. The Tampere conclusions also hoped for the expedition of the exchange of information between FIUs on suspicious transactions, as well as for provisions allowing judicial authorities and FIUs to receive, *subject to judicial control*, relevant information from private businesses to investigate money laundering (emphasis added). For a comment on the Tampere Programme, see D. O'Keeffe, *The Tampere Summit: the ties that bind or the policemen's ball*, in *Common Market Law Review*, 36(6), 1999, pp. 1119-1126; J. Monar, *Justice and Home Affairs*, in *Journal of Common Market Studies*, 38, 2000, pp. 138-142; L. Salazar, *La costruzione di uno spazio penale comune europeo*, in G. Grasso-R. Sicurella (eds), *Lezioni di diritto penale europeo*, Milan, p. 414.

and Justice by providing for an appropriate legal basis for the EU to exercise the power - «by means of directives adopted in accordance with the ordinary legislative procedure»[106] - to adopt criminal law provisions[107].

In particular, not only did the Lisbon Treaty abolished the three pillar structure thus "communitarizing" the old third pillar on police and judicial cooperation in criminal matters which had been, so to speak, left behind post-Amsterdam, but it also expressely conferred upon the European Union the power to adopt minimum rules in order to approximate national legislations in substantive[108] as well

[106]Artt. 82(2) and 83(1) TFEU. As argued by V. Mitsilegas, *EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe*, Oxford, 2016, p. 7, the strategic deployment of Directives in shaping EU criminal law, a move replacing the former use of Framework Decisions, carries a significant legal consequence: the activation of the principle of direct effect for these provisions. This fundamentally empowers individuals by according them substantive and procedural rights «to claim these rights before national courts and ensuring thus the decentralised enforcement of EU criminal law».

[107]It would be misleading not to mention the contribution that the Court of Justice brought to the gradual integration of the European criminal law framework. While the Lisbon Treaty expressly and officialy created one institutional framework under the communitarian model, the Court's case law had played an important role in making these pillars converge, as noted by A. Klip, *European Criminal Law. An integrative approach*, Cambridge, 2016, p. 18. Just to mention a few of its seminal rulings, in case C-176/03, 13 september 2005, *Commission v. Council*, ECLI:EU:C:2005:542, the Court resolved the controversy between the European Commission and the Council concerning the appropriate legal basis to impose on Member States the obligation to criminalize certain illicit conducts. More specifically, the Court held that while «as a general rule, neither criminal law nor the rules of criminal procedure fall within the Community's competence», nonetheless it does not prevent «the Community legislature, when the application of effective, proportionate and dissuasive criminal penalties by the competent national authorities is an essential measure for combating serious environmental offences, from taking measures which relate to the criminal law of the Member States which it considers necessary in order to ensure the rules which it lays down an environmental protection are fully effective». As a consequence, the Court annulled the Framework Decision advanced by the Council and upheld the competence of the Community in criminal law to a certain extent. On the undefined limits of such extent and the implications of the ruling in general, see V. Mitsilegas, *EU Criminal Law*, cit., pp. 70-78; E. Aprile, *Diritto processuale penale europeo e internazionale*, Padua, 2007, p. 102 ff.; S. Miettinen, *Criminal Law and Policy*, cit., pp. 37-40. On the challenges that this ruling posed before the Lisbon Treaty, R. sicurella, *Il Corpus Juris come modello per la definizione di un sistema penale europeo*, in G. Grasso-R. Sicurella (eds), *Lezioni di diritto penale europeo*, Milan, 2007, p. 707 ff.; A. Klip, *European Criminal Law*, cit., pp. 160-164. In addition to such *implied* or *indirect* competence of the Community, in the case C-105/03, 16 June 2003, *Pupino*, ECLI:EU:C:2005:386, the Court held that the provisions on police and judicial cooperation had binding effects similar to Community law, recognizing an enforcement obligation for Member States also in criminal law matters.

[108]The legal basis for the adoption of substantive criminal law instruments is Art. 83 TFEU, whose para. 1 makes a non-exhaustive list of so-called "eurocrimes", that is, particularly serious

as procedural[109] criminal law issues, thus binding the competence in criminal law to the objective of the free movement of persons within the Area of Freedom, Security and Justice[110].

The inclusion of an express competence in criminal law to counter serious forms of crime, organized or otherwise, certainly fostered the debate around *how* to effectively tackle it. From that moment on, a growing number of EU acts acknowledged the connection between serious cross-border crime and the recovery of illicit assets[111]. In its communication on *Proceeds of organised crime: ensuring that "crime does not pay"*[112], the Commission stressed that financial investigations «are at the heart of the fight against organised crime and terrorism financing» and urged a wider use of financial investigation and financial criminal analysis as a law enforcement technique in all Member States to improve the freezing and confiscation framework.

Fast-forwarding to recent initiatives, in its conclusions on enhancing financial investigations to fight serious and organized crime, the Council called on Member States to ensure that financial investigations be initiated immediately and form part of all kinds of criminal investigations regarding organised crime, being a «hor-

---

crimes with a crossborder dimension on which the European Union may legiferate to provide for the definition and related sanctions; moreover, para. 2 allows EU institutions to adopt criminal law provisions if it proves essential to ensure the effective implementation of a common Union policy, that is for the safeguard of supranational or institutional interests. For this interpretation, see G. Grasso, *La competenza penale dell'Unione europea nel quadro del Trattato di Lisbona*, in G. Grasso-L. Picotti-R. Sicurella (eds), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milan, 2011, p. 694 ff.

[109] Art. 82 TFEU grants the power to adopt minimum rules in areas of criminal procedure, such as mutual admissibility of evidence, the rights of individuals in criminal procedure and the rights of victims of crime (par. 2), to the extent that it is necessary to facilitate mutual recognition of judgments and judicial decisions, which is now considered the basic principle of judicial cooperation in criminal matters (par. 1). More extensively on the principle of mutual recognition and the role of mutual recognition instruments in detecting proceeds of crime, see §3.2.

[110] S. Miettinen, *Criminal law and policy*, cit., p. 41.

[111] The European Parliament had already pointed out in its Report on the 1997 Action Plan on organized crime, that «(...) steps must also be taken to raise the probability of uncovering organized crime, (...) it is necessary to concentrate, in investigation and sentencing, more on the criminal organization itself, and on its most sensitive area - its money».

[112] COM(2008) 766 final.

izontal, cross-cutting priority in EMPACT[113]». Similarly, the strategy to tackle organized crime delivered by the European Commission identifies the strenghtening of fight against criminal finances as one of the priority work strands to better protect citizens and the economy from organized crime, calling for the improvement of the rate of financial investigations in practice as well as the freezing and confiscation framework[114].

Against this backdrop, it could be maintained that the development of a culture of financial investigations in the context of criminal proceedings, for which effective information sharing among all parties involved is essential, has become a policy and legislative priority for the European Union. However, the clear multidisciplinary nature[115] that investigations into economic and financial crimes have, as well as the sophistication that certain investigative techniques may reveal in terms of technological advancement, raise several doubts on the legitimacy of fi-

[113]EMPACT stands for *European Multidisciplinary Platform Against Criminal Threats* and refers to the EU multidisciplinary and multiagency operational cooperation to fight organised crime policy, which stretches over a 4-year period and set out the priorities for the fight against organized and serious crimes. EMPACT 2022-2025 identifies the priority to address financial crimes and the related aim to «combat and disrupt criminal networks and criminal individuals who are involved in criminal finances and money laundering, and facilitate asset recovery in view of effectively confiscating the criminal profits, especially by supporting the automatic launch of financial investigations and developing a culture of asset recovery through training and financial intelligence sharing». The cornerstone of the EMPACT policy cycle is represented by the Europol's Serious and Organized Crime Threat Assessment (SOCTA), which gives a complete picture of what forms of criminality constitute or are perceived by Member States as emerging threats. According to SOCTA 2021, «[s]ince financial gain is the primary motivation behind almost all forms of serious and organised crime, the laundering of illicit proceeds forms an integral part of criminal infrastructures», thus qualifying money laundering as both an enabler of profit-driven organized crime and the primary cause of public revenue's loss, corruption and distorting factor of free market mechanisms. Whilst not falling within the scope of the research, it should not be overlooked the role played by Europol in the fight against serious crimes in general and the protection of the financial system from criminal threats in particular. In 2020, Europol established the European Financial and Economic Crime Centre (EFECC) to provide support to Member States in the development and implementation of financial investigations.

[114]Communication from the commission to the European Parliament, the Cuncil, The European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025, COM/2021/170 final, par. 3 ff.

[115]As pointed out by K. Ligeti, V. Franssen, *Current Challenges in Economic and Financial Criminal Law in Europe and the US*, in Id., *Challenges in the Field of Economic and Financial Crime in Europe and the US*, Oxford-Portland, 2017, p. 9, "multi-disciplinary investigations" refers to investigations involving authorities of diverse nature, *e.g.* police, judicial, and administrative, both at national and supranational level.

nancial investigations *vis-à-vis* criminal procedure rules and principles. In the following subsections, the EU fragmented framework on financial investigations will be discussed in-depth, according to two parallel and, to some extent, interwoven limbs.

On the one hand, § 3.1 will address the origin, development, and *status quo* of AML/CTF legislation in light of the ongoing evolution of international standards and the architecture of Financial Intelligence Units networks. On the other hand, Section 3.2 will be dedicated to presenting the instruments based on the principle of mutual recognition enshrined in the Lisbon Treaty that may serve the purpose of chasing criminal money. The aim is to provide a comprehensive view of secondary legislation relevant to this work, thus setting the stage for further discussion on their implications for fundamental rights.

3.1 The EU AML/CTF system between prevention approaches and criminal prosecution

The previous section concerning the history behind the growing attention in EU policy towards the economic dimension of crime - be it organized or otherwise - should not mislead the reader to believing that the EU framework addressing money laundering threats is solely concerned with the repression of the criminal phenomenon. If anything, it has already been mentioned how the development of the EU AML regulatory framework went in parallel with international initiatives taken especially at the FATF level, setting standards for the preventive functions of the action against illicit money entering the financial system.

In other words, the framework developed by the European Union managed to merge different approaches[116] to money laundering, that is, a preventive model aiming to protect the integrity and transparency of the financial system, and a repressive one relying on (the harmonization of) criminalization. Whether they

[116] According to W. Gilmore, V. Mitsilegas, *The EU legislative framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards*, in *The International and Comparative Law Quarterly*, 1, 2007, p. 119, the EU strategy combines the approach of the UN and the Council of Europe, fostering the criminalization of certain conducts, and that of the FATF centered on prevention.

are cumulatively referred to as "twin-track fight"[117], "two-fold goal"[118] or "two-pronged approach"[119], such policies respond *in abstracto* to different objectives and therefore follow different (normative) paths.

Focusing on the preventive policy of the regulatory architecture, we should start by saying that the EU legislation is more composite and consolidated on this side than it is in the criminal law field, and the reasons for this are both the longer time frame in which it was developed and the particular interest that the European Union has always shown in protecting the stability of markets. In fact, while the development of the EU AML/CTF preventive framework had been initially pushed by external actors[120], it proved to be consistent with the original nature of the European Union, *i.e.*, an organization of States promoting the free movement of capitals and the integrity of markets. In this sense, «since money laundering and terrorist financing pose a clear risk to the integrity, proper functioning, reputation and stability of society»[121], a regulatory framework that aims to mitigate the risks of financial crimes to "pollute" international financial systems prevents consumer confidence in the market and in financial transactions from being undermined[122].

The favor of the EU legislator towards the regulation of financial threats by

[117]Cfr. G. Stessens, *Money laundering*, cit., p. 108; M. van der Broek, *Preventing money laundering: A legal study on the effectiveness of supervision in the European Union*, The Hague, 2015, p. 4.

[118]The words are used by V. Mitsilegas,*Counter-measures in the European Union: A new paradigm of security governance versus fundamental legal principles*, The Hague-Boston-London, 2003, p. 31, who distinguishes between an active goal connected to criminal policy justifications as it strives to increase the law enforcement and asset forfeiture risks for criminals, and a defensive goal striving to protect domestic and international financial markets from illicit flows which cause the malfunctioning of the legal economy.

[119]W. Gilmore, V. Mitsilegas, *The EU legislative framework*, cit., p. 119.

[120]The FATF playing a major role in this, but also tracing back the interest towards the earinings of crime to the United States' fight against European mafia, as highlighted by J. Vervaele, *Economic crimes and money laundering: a new paradigm for the criminal justice system*, in B. Unger-D. van der Linde (eds), *Research Handbook on Money Laundering*, Cheltenham-Northampton, 2013, p. 382.

[121]P. Godinho Silva, *Recent developments in EU legislation on anti-money laundering and terrorist financing*, in *New Journal of European Criminal Law*, 10(1), 2019, p. 58.

[122]E. Herlin-Karnell, *EU criminal law and its complicated relationship to the internal market*, in V. Mitsilegas-M. Bergström-T. Quintel (eds), *Research handbook on EU criminal law*, Chelthenam-Northempton, 2024, p. 255.

means of administrative procedures and sanctions can be clearly drawn from the choice of the legal basis for the adoption of the AML Directives. For the purposes of the present work, it is sufficient to mention that the AML/CTF Directives have been adopted under the internal market basis of Art. 114 TFEU, which provides EU institutions with the competence to adopt measures ensuring the establishment and functioning of the internal market[123]. While such choice grants wider participation by EU Member States to the provisions stemming from AML/CTF Directives, since otherwise the non-participation mechanisms featured in Area of Freedom, Security and Justice provisions would apply[124], it nonetheless raises doubts on the appropriateness of an internal market legal basis for the fight against money laundering and terrorism financing[125].

However, that being the case, the first legal instrument addressing the misues of the financial system for illegal purposes was Directive 91/308/EEC (first AML Directive)[126] which closely followed the 1990 FATF Recommendations in burdening the financial sector with identification and reporting duties, while also leaving a broad margin of discretion to Member States in prohibiting and sanctioning drug-related money laundering[127], as well as in setting up the competent authorities which should receive the suspicious transactions reports. Following the 1996 update of the FATF Recommendations, the first AML Directive was amended by Directive 2001/97/EC[128] in order to broaden the subjective scope of the preventive

[123]Cfr. Art. 26 TFEU.

[124]The reference goes to the "emergency brake" procedure designed by several provisions, as well as to the opt-out choice granted to Denmark and Ireland, and more generally to the possibility to establish enhanced cooperation procedures. On this picture of justice "*à-la-carte*", see V. Mitsilegas, *EU Criminal Law after Lisbon*, cit., p. 44 ff; Id, *EU Criminal Law*, cit., pp. 53-56; Id., *European Criminal Law and Resistance to Communautarisation after Lisbon*, in *New Journal of European Criminal Law*, 1(4), 2010, p. 458 ff.

[125]E. Herlin-Karnell, *The EU's Anti-Money Laundering Agenda: Built on Risks?*, in C. Eckes-T. Konstadinides (eds), *Crime Within the Area of freedom, security and justice: a European public order*, Cambridge, 2011, p. 79.

[126]Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, OJ L 166.

[127]The first AML Directive fulfilled the criminalization obligation pursuant to the 1998 UN Vienna Convention.

[128]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, OJ L 344.

obligations, now falling on other professions such as estate agents, lawyers, tax auditors, and extend the scope of predicate offences to "serious crimes"[129]. These steps forward nothwistanding, the actual improvement towards the strategy as designed nowadays was brought about by the third AML Directive of 2005[130]. First, it promoted a "risk-based approach" to money laundering threats which, as will be seen below, entails an evidence-based risk assessment and a proportionate allocation of resources according to a cost-effective logic[131].

Secondly, bringing in line the EU framework to the developments occurred within the FATF[132], the third AML Directive included terrorism financing in its scope beside the fight against money laundering. Consequently, it also prohibited terrorist financing, whose definition is consistent with that provided for by Framework Decision 2002/475/JHA on combating terrorism.

Thirdly, due diligence measures were intensified and differentiated in simplified and enhanced procedures depending on the seriousness of the risk. Moreover, reporting duties included FIUs as addressees.

The third AML/CTF Directive was repealed by Directive (EU) 2015/849 (fourth AML Directive)[133] to incorporate the latest version of the FATF Recommendations adopted in 2012 enhancing the effectiveness of the AML/CTF system. While the implementation deadline was pending, the Commission proposed to re-

[129]Revised Art. 1(4), lett. *e* first AMLD.

[130]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, OJ L 309. For a thorough analysis of the Directive, see W. Gilmore, V. Mitsilegas, *The EU legislative framework*, cit., p. 124-129; M. Bergström, *Money Laundering*, in V. Mitsilegas-M. Bergström-T. Konstadinides (eds), *Research Handbook on EU Criminal Law*, Cheltenham-Northampton, 2016, pp. 335-354.

[131]On the concept of "risk" and its implications, see E. Herlin-Karnell, *The EU's Anti-Money Laundering Agenda*, cit., pp. 76-96. Doubts on the cost-effectiveness of the risk-based approach are put forward by P. Costanzo, *The risk-based approach to anti-money laundering and counter-terrorist financing in international and EU standards: what it is, what it entails*, in B. Unger-D. van der Linde (eds), *Research Handbook on Money Laundering*, cit., p. 356 ff.

[132]Between 2001 and 2004, the FATF published nine Special Recommendations specifically addressing the financing of terrorism in respons to the 9/11 attacks, thus expanding its mandate.

[133]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, OJ 141.

vise the fourth AML Directive to improve specific aspects related to transparency and to keep pace with technological advancement in financial services[134]. Hence, the fifth AML Directive was adopted in 2018[135].

The regulatory framework that arises from the provisions currently in force is devoted to enhancing the effectiveness of the AM/CTF system by providing tougher and clearer rules on cash payments, simplified CDD procedures and access to beneficial ownership registers, while also paying attention to data protection implications[136]. Moreover, the improvement of cooperation mechanisms between national authorities and in a cross-border setting[137] is carried out.

Before delving into the nature and content of the AML/CTF preventive policy, the recently adopted legislative package addressing money laundering legislation should be presented, insofar as it is going to replace the current legal framework starting from 2027. In July 2021, the European Commission presented its package intended to revise and strengthen EU AML and CFT rules by means of four different legislative proposals, namely a directive replacing the fourth AML/CTF Directive (sixth AML Directive)[138]; a regulation establishing a EU single rulebook on AML/CFT[139] and compensating for the fragmanted implementation of

[134]P. Godinho Silva, *Recent developments*, cit. p. 60.

[135]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, OJ L 156.

[136]For example, it is prescripted that obliged entities shall store the information acquired through due diligence measures and record the transactions for at least five years after the end of the business relationship with their customer, with the possibility to extent such period for other five years. According to V. Mitsilegas, N. Vavoula, *The evolving EU anti-money laundering regime. Challenges for fundamental rights and the rule of law*, in *Maastricht Journal of European and Comparative Law*, 23(2), 2016, p. 281, such a provision raises proportionality concerns. For further analysis of the pitfalls of the provisions, see M. Bergström, *Money laundering*, in V. Mitsilegas-M.Bergström-T. Quintel (eds), *Research handbook on EU criminal law,* cit., p. 325 ff.

[137]On FIUs cooperation see further in § 3.1.1.

[138]Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849, OJ 2024, L 1640/1.

[139]Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ 2024, L 2024/1.

the fourth AML Directive; a regulation setting up a central body tasked with EU-level AML/CFT supervision[140]; and a directive amending the current provisions regulating the access and search centrilised bank account registers by competent authorities[141]. Moreover, a regulation on information accompanying transfers of funds and certain crypto-assets had already been approved in 2023[142].
In its communication, the Commission acknowledged the ineffectiveness and inadequacy of the implementation of AML/CTF provisions across Member States, resulting from the low rates of suspicious transactions detected and those of illicit assets seized, as well as the inconsistency of the supervision over obliged entities[143]. The goal of the Commission's initiative is therefore to advance harmonization of the AML/CTF regulatory system within the EU and strengthen the enforcement system[144].

This might appear to be at odds with the choice to transfer the provisions of the fourth AML Directive to two different instruments requiring national implementation [145], although according to the Commission it accounts for the idea to transfer all rules that apply to the private sector to a Regulation, whereas the organization of the institutional AML/CFT system at national level is left to a Directive[146]. Besides the reshuffling of the existing provisions, the package brings

[140]Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 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, OJ 2024, L 1620/1.

[141]Directive (EU) 2024/1654 of the European Parliament and of the Council of 31 May 2024 amending Directive (EU) 2019/1153 as regards access by competent authorities to centralised bank account registries through the interconnection system and technical measures to facilitate the use of transaction records, OJ 2024, L 1654/1.

[142]Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, OJ 2023, L 150/1.

[143]European Commission, Impact assessment accompanying the Anti-money laundering package, SWD(2021) 190 final, 20th July 2021.

[144]S. Allegrezza, G. Bruzzese, *Supervision and Enforcement of EU's Anti-Money-Laundering and Countering the Financing of Terrorism*, in F. Annunziata-M. Siri, (eds), *EU Banking and Capital Markets Regulation Open Issues of Vertical Interplay with National Law*, Cham, 2025, pp. 509.

[145]Ibid., where the Authors still see certain degrees of complexity due to the coexistence of a directive and a regulation.

[146]European Commission, Proposal for a Regulation of the EUropean Parliament and of the

about several novelties, such as the expansion of the scope of obliged entities to crypto-asset service providers, crowdfunding platforms and migration operators; specific enhanced due diligence measures for cross-border correspondent relationships for crypto-asset service providers; more harmonized rules on beneficial ownership and on the management of threats posed by third countries[147].

Most strikingly, the new provisions contained in Regulation (EU) 2024/1620 open to an increased role for private actors, whose cooperation in accessing personal data of their customers is fundamental for public authorities[148]. Art. 75 Regulation (EU) 2024/1620 provides the legal basis for the establishment of public-private partnerships (PPPs) for information sharing in the context of ML/TF CDD duties, which possibly paves the way for indiscrimate flows of information and blurring lines between what is administrative and what is criminal[149].

Although their involvement is *in abstracto* limited to the prevention money laundering and terrorism financing, the overreliance on their regulatory role challenges the traditional compartmentalization between prevention and repression.

With regard to the content of the provisions set out in the Directives, the overarching logic governing the AML/CTF preventive framework is represented by the shift from a rule-based approach to a risk-based one, which aims at a more efficient allocation of resources where risks of money laundering are higher[150], therefore pulling back resources where risks are lower[151].

Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, COM(2021) 420 final.

[147]For an in-depth analysis of the amendments, see 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*, 2022, 13(2), pp. 216-246; T. Wahl, *The EU's New AML Single Rulebook Regulation*, in *Eucrim*, 2024, 2, p. 117 ff.

[148]M. Bergström, *Money laundering*, cit., p. 339.

[149]Ibid., p. 340. The challenges posed to the procedural safeguards of those targeted by the privatization of financial investigations will be the object of extensive analysis and discussion in Chapter III.

[150]L. Dalla Pellegrina, D. Masciandro, *The risk-based approach in the new European anti-money laundering legislation: A law and economics view*, in *Review of Law and Economics*, 5, 2009, p. 932; P. Tonnara, *Risk Assessment*, in D. Siclari (ed.), *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive*, Cham, 2016, p. 58.

[151]EU provisions substantially incorporate the principle enshrined in the 40 FATF Recommendations, namely Recommendation 1) according to which «countries should apply a risk-based

In doing so, regulators seek the collaboration of the private sector by granting it broad leeways of discretion in identifying what these risks are and delegating to profit-driven actors the power to design and implement AML control mechanisms[152]. Against this backdrop of increasing deregulation[153], obliged entities, *i.e.*, firms, banking institutions and other professionals working in high-risk fields[154] have to comply with highly specific and sophisticated duties[155], which can be traced back to two main strategies[156].

Firstly, obliged entities are required - without exception[157] - to put in place due diligence measures designed to assess the risk profile of their costumers. By promoting a know-your-costumer (KYC) way of doing business, EU preventive provisions ensure that, when establishing business relationships or when carrying out a single transaction[158], private actors perform standardized checks on, *inter*

approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are proportionate to the risks identified. (...) Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they should allow and encourage simplified measures as appropriate».

[152]L. Dalla Pellegrina, D. Masciandro, *The risk-based approach*, cit., p. 934. As clearly exemplified by J. de Wit, *A risk-based approach to AML. A controversy between financial institutions and regulators*, in *Journal of Financial Regulation and Compliance*, 2007, 15, p. 157, «[t]aking into consideration that it will be impossible for financial institutions to implement a 100 percent CDD system, which cover all the customers and their transactions, the next question will be: which customers and which transaction has to be monitored? In other words, which risk-based approach is the most appropriate for a particular type of customer and type of transaction?».

[153]Regulation of risks equates deregulation, insofar as the state liberalizes the public sector transfering authority to private actors which are called on to actually provide the service. Cfr. M. Bergstrom, K. Svedberg Helgesson, U. Morth, *A new role for for-profit actors? The case of Anti-Money Laundering and risk management*, in *Journal of Common Market Studies*, 2017, 5, p. 1046.

[154]As noted by V. Mitsilegas, N. Vavoula, *The evolving EU anti-money laundering regime*, cit., p. 273, preventive policy has registered an extension of the list of professions subject to money laundering duties, with the personal scope of the legislation now including casinos, lawyers, notaries, real estate agents, and any trader in goods when accepting a payment of EUR 10,000 or more in cash.

[155]Ibid., p. 274.

[156]E. Herlin-Karnell, *The EU's Anti-Money Laundering Agenda*, cit., p. 85.

[157]Directive (EU) 2015/849 does not allow for exemptions from the preventive duties as did the repealed Directive 2005/60/EC, but it rather allows for the performance of simplified costumer due diligence (CDD) measures when the degree of risk is proven to be low. See. Art. 15 Directive (EU) 2015/849.

[158]The thresholds that trigger the application of CDD measures are provided for in the legislation.

alia, the identity of the costumer and the purpose and intended nature of the latter. Most notably, financial intermediaries shall conduct ongoing monitoring of the business relationship and the transactions undertaken throughout the course of that relationship[159].

When customers are not natural persons, obliged entities are required to identify the beneficial owners, *i.e.* those who ultimately own or control the customer legal entity or the natural pesons on whose behalf the transaction is conducted[160].

Following the above-mentioned risk-oriented-approach logic, according to which the rule of conduct is not determined *ex ante* but rather designed only after the facts are evaluated[161], the intensity and scope of CDD controls are determined by financial intermediaries in accordance with the ML/TF risk stemming from factual circumstances[162], but should also be proportionate to the nature and size of the obliged entities[163]. Private credit and financial institutions therefore develop their own internal policies and procedures according to the level of risk, as long as they are consistent with the objectives set out in the legislation[164], which as a consequence implies inevitable differences in the outcome of compliance[165].

Strictly related to the first category of duties, the second strategy featured in the preventive regulatory architecture concerns the reporting obligations falling on obliged subjects. All information they collect when identifying, verifying and

[159]Art. 13, par. 1, lett. *d* Directive (EU) 2015/849. As pointed out by M. Bergstrom, K. Svedberg Helgesson, U. Morth, *A new role for for-profit actors?* cit., p. 1051, «[t]he risk-based approach further emphasizes that monitoring is to be continuous. An evaluation of who is high or low risk is not to be done once and for all but surveillance and (re)categorization is to be a continuous process».

[160]For an overview of the literature on beneficial ownership, see P. M. Gilmour, *Lifting the veil on beneficial ownership Challenges of implementing the UK's registers of beneficial owners*, in *Journal of Money Laundering Control*, 2020, 23(4), pp. 717-734.

[161]P. Costanzo, *The risk-based approach to anti-money laundering*, cit., p. 352.

[162]«This means that intermediaries should thoroughly analyse the concrete case under management, assess the associated ML/TF risks, define a proper risk profile and, thus, the appropriate level of mitigation to be applied». P. Fratangelo, *The CDD obligations following a risk-based approach*, in D. Siclari (ed.), *The new anti-money laundering law*, cit., p. 13.

[163]Art. 8(1) Directive (EU) 2015/849.

[164]L. Borlini, F. Montanaro, *The evolution of EU law against criminal finance: the "hardening" of FATF standards within the EU*, in *Georgetown Journal of International Law*, 48, 2017, p. 1040.

[165]P. Costanzo, *The risk-based approach*, cit., p. 354.

monitoring their costumers' profile and transactions, is gathered, stored, analyzed and eventually passed on to the FIU if suspicions of money laundering or terrorism financing arise. More specifically, obliged entities are required to bring to the attention of the FIU, by means of Suspicious Activity Reports (SARs) or Suspicious Transactions Reports (STRs)[166], every case in which they know, suspect or have reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing[167]. Reporting duties must be complied with by all obliged entities encompassed by the AML Directive, although certain professional figures, namely notaries, lawyers, other independent legal professionals, auditors, external accountants and tax advisors, answer to specific provisions[168].

As for the role of the FIUs as addressees of the communications, it was envisaged for the first time by the third AML Directive, as previous directives required obliged entities to send their reports to the competent authorities[169]. FIUs' tasks are therefore to receive reports and process them so as to perform financial analysis which are destined to the competent authorities on one hand[170] and to obliged

[166]As noted by F.A. Siena, *The European anti-money laundering framework*, cit., p. 231, SARs take into account the overall financial activity of the targeted customer, while STRs usually focus on single transactions. However, the difference among the two is often blurred.

[167]Art. 33(1) Directive (EU) 2015/849.

[168]For the sake of completeness, it should be mentioned that the topic has received much attention among scholars and in jurispruence with specific regard to the reporting duties falling on lawyers. In its judgment of 26 June 2007, *Ordre des barreaux francophones and germanophone and Others*, case C-305/05, ECLI:EU:C:2007:383 the Court of Justice, interpreting the provision in the previous version of the AML Directive, delimited the scope of such obligations and ruled that they do not infringe upon the right to a fair trial pursuant to Art. 6 ECHR, namely the right to the attorney-client legal privilege, in as much as lawyers are under obligation only when «they advise their client in the preparation or execution of certain transactions — essentially those of a financial nature or concerning real estate, (...) — or when they act on behalf of and for their client in any financial or real estate transaction» (CJEU, *Ordre des barreaux*, cit., para. 33.). In other terms, the legal privilege is given a restricted scope of application in light of the prominent general interest represented by the fight against money laundering (Cf. Opinion of Advocate General Poiares Maduro, Case C-305/05, *Ordre des Barreaux Francophones et Germanophone v. Conseil des Ministres*, ECLI:EU:C:2006:788, para. 78) and is thus limited to cases in which lawyers receive information while performing their task of defending or representing their client in, or concerning, judicial proceedings. However, as pointed out by L. Borlini, F. Montanaro, *The evolution of EU law*, cit., p. 1045, «it is difficult in practice to draw a line between lawyers' activities related to a trial and lawyers' activities unrelated to the conduct of judicial proceedings».

[169]Cf. Art. 6 Directive 91/308/EEC as amended by Directive 2001/97/EC.

[170]This is the case when FIUs detect funded suspicions of crime. As a consequence, they

entities on the other[171].

For what the repressive policy of the EU AML framework is concerned, it should be said that such an approach comes from the urge to prevent criminals from misusing the financial system to conceal the proceeds of their illicit conducts, and the tool exerting higher deterrant effects is, of course, criminal law. As already pointed out, criminal provisions sanctioning serious forms of crime required some time to get to the scene, as the EU (non-exclusive) competence in criminal law was provided only in 2009 by the Lisbon Treaty, way after that proceeds from crime emerged as a threat.

Eventually, in the aftermath of the terrorist attacks that occurred in Europe in 2016, the European Commission urged Member States to strengthen the fight against terrorist financing and the need to counter money laundering by means of criminal law[172]. Consequently, in 2018, money laundering constituted the subject of the very first directive based on art. 83(1) TFEU[173], that is, Directive (EU) 2018/1673[174].

The Directive was adopted not only to complement the already existing EU

---

will draw an intelligence report and forward it to judicial authorities to trigger a criminal investigation, therefore providing them with the *notitia criminis*. See F.A. Siena, *The European anti-money laundering framework*, cit., p. 217.

[171]In order to improve the capacities of obliged entities to identify and prevent ML/TF conducts with updated risk parameters, FIUs disseminate typologies and similar strategic information explaining new criminal trends and *modi operandi* of money laundering or terrorism financing. See B. Vogel, M. Lassalle, *Developing Public-Private Information Sharing to Strengthen the Fight against Money Laundering and Terrorism Financing. Recommendations for the European Union*, Freiburg, 2024, p. 9.

[172]European Commission, Action Plan for strengthening the fight against terrorist financing, COM(2016) 50 final. The Action Plan further built on the European Agenda on Security, (COM(2015)185 final) published in 2015 which had called for additional measures in the area of terrorism financing and money laundering.

[173]It is here recalled that art. 83(1) TFEU provides for the legal basis to adopt minimum rules concerning the definition of criminal offences and sanctions of the so-called *eurocrimes*, whose particular seriousness and structure require a counteraction on a common basis

[174]Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ, L 284. The Directive is indeed the first EU act to explicitly make use of criminal provisions to sanction money laundering, although Member States had already implemented within their criminal law framework the AML Directives requiring them to *prohibit* money laundering. The blameworthy choice of the legislator was highlighted before 2018 by V. Mitsilegas, N. Vavoula, *The evolving EU anti-money laundering regime*, cit., p. 268.

preventive system by extensively criminalizing money laundering and self-laundering conducts[175], but it also aimed at reinforcing the criminal law framework on combating serious forms of crimes such as terrorism and organized crime[176].

All of the above casts doubts on the assumption that the preventive approach and the repressive approach have well-defined and distinct features and existences. This view could not be more distant from reality. In fact, the two policies often overlap and serve each other's purposes, with criminal law being used to enforce the regulatory financial framework, and risk management and CDD duties being used to identify criminals or traces of crime, with blurred and unclear lines being drawn between criminal law and administrative law in AML/CTF policy[177]. As for the former, an example can be the mentioned provision of the fourth AML Directive offering a EU-harmonized definition of money laundering and calling on Member States to *prohibit* such acts, thus leaving broad margin of appreciation to Member States as to whether it should be by means of administrative or criminal sanctions[178].

An example of CDD measures serving criminal justice's purpose might be possibly offered by the newly adopted provision on information sharing PPPs pursuant to Regulation (EU) 2024/1624, as competent authoritites responsible

[175]For an overview on the provisions of the criminal law AML Directive, see S. Allegrezza, G. Bruzzese, *Supervision and Enforcement*, cit., p. 497 ff.; J.B. Maillart, *The anti-money laundering architecture of the European Union*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laundering Law*, cit., pp. 81 ff.

[176]See European Commission, *Proposal for a Directive on countering money laundering by criminal law*, 21 December 2016, COM(2016) 826 final.

[177]M. Bergström, *Legal perspectives on money laundering*, in V. Mitsilegas-S. Hufnagel-A. Moiseienko (eds), *Research Handbook on Transnational Crime*, Cheltenham, 2019, p. 106.

[178]Whatever the case, the Directive further states in Art. 58, (2) that any resulting sanction on obliged entities shall be effective, proportionate and dissuasive and that, when administrative sanctions implementing the directive are laid down, they should be «[w]ithout prejudice to the right of Member States to provide for and impose criminal sanctions». In other words, Member States can opt for a dual regulation system, as long as the *ne bis in idem principle* is respected according to Recital 59 Directive (EU) 2015/849. See further M. Bergström, *Legal perspectives*, cit., p. 167 and E. Herlin-Karnell, *EU criminal law*, cit., p. 259, who envisages other examples of interaction between administrative law and criminal law provisions, such as market abuse and restrictive measures. However, combining criminal provisions with administrative sanctions does not necessarily lead to greater effectiveness, as pointed out by V. Mitsilegas, N. Vavoula, *The evolving EU anti-money laundering regime*, cit., p. 272.

for the prosecution of money laundering-related offences will be able to engage with obliged entities and receive sensitive information from them, which - not surprisingly - should be governed by «the applicable provisions of national criminal procedural law, including prior judicial authorisation or any other national procedural safeguard as required»[179].

The alarming consequences of this blurred line between prevention and repression are evident, especially in light of the effects it has on the possible deliberate circumvention of the principles and safeguards stemming from criminal and criminal procedural law. In light of the above, prior to focusing on what such procedural safeguards are and if and how they are being respected in the context of financial investigations, it is essential to shed light on some procedural aspects of the EU AML normative architecture.

3.1.1 Financial Intelligence Units: network, cooperation, powers

The EU AML/CTF provisions do not lay down a definition of Financial Intelligence Units (FIUs). They were first envisaged in 1991 by the First AML directive, although it only referred to «the authorities responsible for combating money laundering of the Member State in whose territory the institution or person forwarding the information is situated»[180]. No reference was made to the nature or function of such authorities, and this uncertainty led to a variety of authorities being established in Member States that were entrusted with the collection of financial reports submitted by financial institutions and, in certain cases, with the supervision of the said institutions[181]. It took the updating of the FATF Recommendations in 2003 for EU lawmakers to expressly mention FIUs in Art. 21 of the third AML Directive[182], but only in 2015 more detailed provisions were laid down regulating their status and powers.

According to Art. 32(1) Fourth AML Directive, Member States should establish FIUs «in order to prevent, detect and effectively combat money laundering

[179] Art. 75 (4), lett. *j* Regulation (EU) 2024/1624.
[180] See. Art. 6 Council Directive 91/308/EEC.
[181] V. Mitsilegas, *New forms of transnational policing*, cit., p. 147.
[182] W. Gilmore, V. Mitsilegas, *The EU legislative framework*, cit., p. 127.

and terrorist financing», and grant them operational independence and autonomy - that is, the capacity to perform their tasks freely and to autonomously decide to analyze, request and disseminate information[183]. To that aim, they should be provied with adequate financial, human and technical resources to fulfill their tasks[184].

The Fourth AML Directive attributes three core functions to FIUs. First, receiving suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing, in that sense representing a buffer between the financial sector and law enforcement and judicial authorities[185]; second, analyizing the information received and requesting additional information from obliged entities to establish links between suspicious transactions and criminal activity; third, disseminating the results of the analysis[186] to investigative and prosecuting authorities if actual grounds to suspect money laundering, associated predicate offences or financing of terrorism are substantiated[187].

Despite FIUs share the same core duties, the efficiency of their performances, as well as the extent to which FIUs are entrusted with additional duties and responsibilities[188], to a large extent depend on the legal nature of said bodies, that is, the institutional and organizational structure given to them by law. In fact,

[183]Recital 37 Directive (EU) 2015/849.

[184]Art 32(3) Directive (EU) 2015/849. According to I. Borrello, *Financial Intelligence Unit (FIU)*, in D. Siclari (ed.), *Italian Banking and Financial Law: Vol I, Supervisory Authorities and Supervision*, Houndmills, 2015, p. 265, operational and managerial autonomy is «required by the international standards in defence of the independence of FIUs, the effectiveness of their action, the specialty of the functions related to the financial analysis, and the heterogeneity of the information available in performing the analysis, that may be of a financial, administrative or investigative type». On the risk for FIUs as well as for financial supervision autorities to be subjected to polictical pressure and capture, see P. Demetriades, R. Vassileva, *Money laundering and Central Bank governance in the European Union*, in *Journal in International Economic Law*, 2020, 23(2), pp. 509-533.

[185]M. Penna, *The 'pre-investigative' role*, cit., p. 257.

[186]I. Borrello, *Financial Intelligence Unit (FIU)*, cit., p. 264, makes a distinction between operational analysis and strategic analysis, according to which the former concerns specific targets in order to determine links between those targets and possible proceeds of ML/TF while the latter aims at identifing new trends and patterns to increase the capacity of FIUs and obliged entities to determine and detect threats and vulnerabilities.

[187]Art. 32(3) Directive (EU) 2015/849

[188]On the additional tasks that EU FIUs are burdened with across Member States, see data provided by I. Deleanu, *FIUs in the EUropean Union*, cit., pp. 110-116.

as already mentioned, EU law does not provide details on the nature national FIUs should have, which led to three different types of FIUs being established both against the international framework and the EU legislation. For the categorization in broad terms, please refer to the specific section[189]. However, the topic requires further analysis.

The organizational status of FIUs is strictly related to the extent to which they can exchange information with the competent authorities for the prevention, detection, investigation and prosecution of certain criminal offences. It is therefore related to the ability of FIUs to access public authorities' databases where such information is held and *viceversa*, inasmuch as «the closer the FIU is to law enforcement agencies (in particular financial police or prosecutorial authorities), the easier it is for the FIU to access law enforcement data», whereas «the closer the FIU is to financial or banking supervisors, the easier the process is to directly access data related to financial transactions»[190].

The topic is particularly sensitive for several reasons. In the first place, because swift information exchange mechanisms play a key role in the degree of efficiency of AML/CTF systems. Secondly, the breadth of access powers granted to FIUs exerts influence over the criminal proceedings that might be subsequently initiated. Allowing FIUs to directly access sensitive data held by criminal justice authorities would, in fact, enhance their information position and empower them to trigger and steer the investigative action of the judiciary without any judicial scrutiny or external control in general[191]. As a consequence, criminal investigations would dangerously run the risk of being politically or arbitrarily driven, and this might prove all the more true for administrative FIUs that are subject to governmental

[189] See *supra* Section 2.2.

[190] S. Allegrezza, *The proposed Anti-Money Laundering Authority, FIU cooperation, powers and exchanges of information: A Critical Assessment*, Publication for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2022, p. 44

[191] B. Vogel, *Reinventing EU Anti-Money Laundering. Toward a Holistic Legal Framework*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laundering Law*, cit., p. 951.

ministries[192].

Within the already mentioned categorization into the three general headings, namely the administrative, the judicial and the law enforcement ones[193], a major distinction can be made, insofar as while some Member States accommodate their FIUs within the criminal justice system, either under an investigative or prosecutorial agency, others chose to keep the unit outside thereof. In the first case, FIUs operate as an additional tool for law enforcement authorities, in that they are entrusted with the same powers as those given to police and judicial authorities. To the contrary, in the latter case, *i.e.* when FIUs are embedded within an administrative agency, their natural role of "filter" or "buffer" between public authorities and the private sector is emphasized[194].

Against this backdrop, different scenarios arise. Although Art. 32(4) Fourth AML Directive provides that «Member States shall ensure that their FIUs have access (...) to the financial, administrative and law enforcement information that they require to fulfil their tasks properly», differences across national jurisdictions exist[195]. While law enforcement and judicial FIUs usually have better access to national police and judicial data, administrative-type FIUs are granted limited access to criminal databases and police records, which can be very cumbersome in practice[196]. The power to access law enforcement information is therefore par-

[192]P. Demetriades, R. Vassileva, *Money laundering*, cit., p. 519; G. Lasagni, *Banking Supervision*, cit., p. 95.

[193]Which had already been acknwoledged by Council Decision 2000/642/JHA pursuant to Art. 3, according to which Article 3 «Member States shall ensure that the performance of the functions of the FIUs under this Decision shall not be affected by their internal status, regardless of whether they are administrative, law enforcement or judicial authorities».

[194]M. Brewczynska, *Financial Intelligence Units: Reflections on the applicable data protection legal framework*, in *Computer Law and Security Review*, 2021, 43, p. 8.

[195]For a comparative analysis, cf. J.B. Maillart, *Anti-money laundering architectures. Between structural homogeneity and functional diversity*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laundering Law*, cit., p. 840.

[196]All the more so when law enforcement data is held by competent authorities of another Member State, as there is no legal basis allowing diagonal cooperation between them. See G. Pavlidis, *Financial information*, cit., p. 373. Cf. European Commission, *Impact assessment accompanying the document proposal for a directive of the European parliament and of the council on laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing council decision 2000/642/JHA*, Commission Staff Working Document, 17.4.2018 SWD(2018) 114, p. 17, where the Commission points out how EU FIUs do not have access to the same level of information

ticularly restricted when FIUs are built within an administrative authority[197], although a legal basis for such mechanisms has been laid out by in Art. 8 Directive (EU) 2019/1153[198]. The directive, which regulates information exchange between public authorities only for law enforcement purposes[199] provides that «each Member State shall ensure that its designated competent authorities are required to reply in a timely manner to requests for law enforcement information made by the national FIU on a case-by-case basis, where the information is necessary for the prevention, detection and combating of money laundering, associate predicate offences and terrorist financing». In addition to that, the newly adopted Sixth AML Directive partially harmonizes the types of information that FIUs can have direct or indirect access to pursuant to the new legal framework, since it lists data that can be accessed by FIUs[200] while also providing that it should occur «regardless of their organisational status»[201].

However, as has been acknowledged, the Directive does not oblige Member States to grant FIUs an *immediate and direct* access to law enforcement information, hence the persistence of dissimilarities across national systems[202].

---

and in particular «administrative and hybrid FIUs have more limited access to such information or, access that is subject to specific access procedures».

[197]Cf. F.A. Siena, *The European anti-money laundering framework*, cit., p. 236, who refers to the findings of the analysis conducted by the EU FIUs' Platform on the characteristics and shortcomings in FIUs' activities. See EU FIUs Platform, *Mapping Exercise and Gap Analysis on FIUs' Powers and Obstacles for Obtaining and Exchanging Information*, 2016.

[198]Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, OJ 2019, L 186.

[199]Which, as noted by M. Brewczynska, *Financial Intelligence Units*, cit., p. 12, is a sign of the shift towards a law enforcement-oriented FIUs system.

[200]According to Art. 2(6) Directive (UE) 2019/1153 law enforcement information is (i) any type of information or data which is already held by competent authorities in the context of preventing, detecting, investigating or prosecuting criminal offences; and (ii) any type of information or data which is held by public authorities or by private entities in the context of preventing, detecting, investigating or prosecuting criminal offences and which is available to competent authorities without the taking of coercive measures under national law. In a non-exclusive manner, the provision mentions criminal records, information on investigations, information on the freezing or seizure of assets, or on other investigative or provisional measures and information on convictions and on confiscations.

[201]Art. 21(1) Directive (EU) 2024/1640.

[202]S. Allegrezza, *The proposed Anti-Money Laundering Authority*, cit., p. 44.

Quite to the opposite, administrative or hybrid FIUs could, in practice, more easily retrieve financial data, such as information on bank accounts, financial assets, or business relationships, all of which are supposed to be held in the centralized automated mechanisms (central registries or central electronic data retrieval systems) that Member States must set up pursuant to the Fourth AML Directive[203]. According to the directive, FIUs should have immediate and unfiltered access to central registries[204] for the timely identification of persons holding or controlling payment and bank accounts identified by IBAN and safe-deposit boxes who are suspected of money laundering or terrorism financing[205].

Closely related to the issue of FIUs' access to financial and law enforcement data is the question of their cooperation with foreign counterparts. In order to grant FIUs more autonomy and efficiency, as well as to provide them with a broader pool of information, national FIUs can cooperate among each other for the sake of information exchange. Originally envisaged by the third pillar Decision 2000/642/JHA[206] on information exchange for law enforcement purposes, the rules governing the cooperation mechanisms between FIUs at the preventive

[203]Art. 32a Directive (EU) 2015/849 as amended by the Fifth AML Directive.

[204]As the AML Directive's legal basis is Art. 114 TFEU, it only grants access to FIUs, whereas the possibility for competent authorities for the prevention, detection, investigation or prosecution of criminal offences to access centralized bank registries was provided by Art. 4 Directive (EU) 2019/1153.

[205]It should be noted that the Sixth AML Directive provides that starting from 2029 the centralized mechanisms shall be interconnected via the bank account registers interconnection system ('BARIS'), to which access has been granted also to competent authorities by Directive (EU) 2024/154 amending Directive (EU) 2019/1153. The initiative was undertaken by the European Commission in accordance with Art. 32a(5) Directive (EU) 2015/849, as amended by the Fifth AML Directive, the initiative having already aroused doubts on the potential shift toward a real-time monitoring model of banking operations for criminal investigations purposes. See G. Pavlidis, *Financial information*, cit., p. 375. For early comments on the 2024 reform, see C. Murphy, *Proposal to amend Directive (EU) 2019/1153: Single access point to bank account registries*, European Parliament Research Service, PE 729.425, September 2024

[206]Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ L 271/4. As noted by W. Gilmore, V. Mitsilegas, *The EU legislative framework*, cit., p. 129 with regards to the Third AML Directive, the coexistance of a first-pillar instrument and Decision 2000/642/JHA until 2019, when the latter was repealed, raised doubts on their relationship, as several provisions overlapped. The Authors also suggest that the AML Directive, since it is based on an internal market provision, was not well suited to allow FIUs to access police data.

level are now laid down by the Fourth AML Directive[207], while the exchange of information between FIUs of different member states and FIUs and law enforcement authorities for prosecutorial purposes is regulated by the already mentioned Directive (EU) 2019/1153.

Therefore, the directive, whose legal basis is Art. 87(2) TFEU on police cooperation[208], aimed to complement the provisions set out in the Fourth AML Directive, thus building a bridge between the two enforcement frameworks[209]. According to Art. 53(1) Fourth AML Directive, FIUs should «exchange, spontaneously or upon request, any information that may be relevant for the *processing* or *analysis* of information by the FIU related to *money laundering or terrorist financing*»[210], regardless of their organizational status. Limited restrictions to FIU-to-FIU information flows are set up, as the only condition upon which data can be exchanged is that they be relevant for the recipient FIU. Moreover, FIUs can exert all powers available to them by law and that would be used in a domestic case, such as requesting information to obliged entities or even freezing suspected funds[211].

In order to ensure protected and secure communications between EU FIUs, the Fourth AML Directive encourages Member States to make use of the FIU.net or its successor, that is a decentralized network for information exchanges between EU FIUs[212]. Formerly embedded within Europol's technical infrastructures, it is now provided that FIU.net will be hosted and managed by AMLA[213], so as to overcome the data protection issues highlighted by the European Data Protection

[207]See Art. 53 Directive (EU) 2015/849.

[208]The legal basis was adopted although not all Member States have given police status to their FIUs, as highlighted by F. Mouzakiti, *Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive*, in *New Journal of European Criminal Law*, 2020, 11(3), p. 357.

[209]S. Allegrezza, G. Bruzzese, *Supervision and Enforcement*, cit., p. 504.

[210]Emphasis added. The wording suggests that the provision is in compliance with the principle of purpose limitation. Cf. F. Mouzakiti, *Cooperation between Financial Intelligence Units*, cit., p. 357. The principle as well as the question of the applicable data protection framework in the case at stake will be discussed in Chapter IV.

[211]F.A. Siena, *The European anti-money laundering framework*, cit., p. 242.

[212]For an in-depth look at the functioning of the FIU.net, see F. Mouzakiti, *Cooperation between Financial Intelligence Units*, cit., pp. 360-363.

[213]Art. 30(1) Directive (EU) 2024/1640; Art. 47 AMLA Regulation.

Supervisor (EDPS)[214].

Looking at the powers of EU FIUs according to AML/CTF legislation, they can be summarized as follows. As mentioned, FIUs shall be able to obtain additional information directly from obliged entities[215], without the need to rely upon a third party, such as the judicial authority[216]. The prior submission of SARs by obliged entities is no longer required [217], thus greatly extending the access powers of FIUs to almost all financial data that obliged entities possess and diminishing the role of the latter to assess whether the information could reveal suspicions of any relevance[218]. Moreover, it goes without saying that when FIUs are set up according to a prosecutorial or law enforcement model, the information retrieved, either by means of a SAR or on their own initiative, can be directly passed on to the judiciary[219].

FIUs also have the power to suspend or withhold consent to the execution of a transaction suspected to be related to money laundering or terrorism financing, but only insofar as the postponement is necessary to «analyse the transaction, confirm the suspicion and disseminate the results of the analysis»[220] In this regard, the Sixth AML Directive has brought about some novelties. First, it lays down detailed timeframes for the suspension of the transaction, requiring FIUs to notify the obliged entity within 3 working days from the report submission and to suspend or withhold consent to the transaction for a time not exceeding 10 working days[221].

[214]EDPS, *Annual Report*, 2019, p. 41. Cf. EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 23 July 2020.

[215]Art. 32(3) DFourth AML Directive; Art. 19(3) Directive (EU) 2024/1640

[216]J.B. Maillart, *The Anti-Money Laundering Architecture of the FATF*, in B. Vogel-J.B. Maillart (eds), *National and international Anti-Money Laundering Law*, cit., p. 121.

[217]Art. 32(9) Fourth AML Directive.

[218]B. Vogel, *Reinventing EU Anti-Money Laundering*, cit., p. 951, argues that this provision is apt to irrimediably change the relationship between FIUs and obiged entities, opening up for an uncontrolled intrusiveness of FIUs' action.

[219]I. Borrello, *Financial Intelligence Unit (FIU)*, cit., p. 267; M. Penna, *The 'pre-investigative' role*, cit., p. 273.

[220]Art. 32(7) DFourth AML Directive.

[221]Art. 24(1) Directive (EU) 2024/1640.

Second, the new directive introduces the power to generally suspend bank or payment accounts when these are concerned with several suspicious transactions and FIUs need to preserve the funds and carry out their analysis; in this case, the suspension cannot exceed 5 working days[222]. Interestingly and worryingly enough, the final version of the directive does not envisage any remedy for the suspension of the transaction or the account, except for one case. In fact, it is provided that the holder of the suspended account or the person whose transaction has been suspended has the right to challenge the decision before a court when longer periods for suspension are set out in national legislation, which can occur when «pursuant to national law, FIUs perform the function of tracing, seizing, freezing or confiscating criminal assets»[223]. That is to say, the existence of legal remedies is entirely deferred to the choice of national legislators and will be available only against the activity of law enforcement or prosecutorial-type FIUs, although administrative FIUs may as well be tasked with suspension powers of equivalent afflictive effects[224].

Finally, another noteworthy addition to the range of powers of FIUs concerns the power to instruct obliged entities to monitor the transactions or activities that are being carried out through one or more accounts related to persons who present a significant risk of ML/TF[225]. In so doing, EU lawmakers not only adjusted EU rules to the standards set out at the international level by the FATF, but they also acknowledged the *status quo* in most of the Member States, where FIUs already have such power[226].

[222] Art. 24(2) Directive (EU) 2024/1640.

[223] Art. 24(1) and (2) Directive (EU) 2024/1640.

[224] As noted by F.A. Siena, *The European anti-money laundering framework*, cit., p. 240 with regard to the directive proposal, a favor for the power of suspension is prioritized at the expense of the fundamental rights of those targeted.

[225] Art. 25 Directive (EU) 2024/1640.

[226] Cfr. Moneyval, *The postponement of financial transactions and the monitoring of bank accounts,* cit., p. 37 ff.

3.2 Following the money through mutual recognition instruments

For the sake of completeness, the research cannot neglect that in parallel with the complex AML/CTF architecture described above, the European Union strategy against financial crimes also relies on legal instruments grounded in police and judicial cooperation provisions. Profit-oriented approaches to crime control were initially promoted in the context of the third-pillar policy of the European Community - then replaced by the provisions set out in Title V on the Area of freedom, security and justice - insofar as more attention was being paid to asset recovery mechanisms aimed at depriving offenders of their illegally obtained gained, especially when illicit assets crossed national borders. Where «confiscation of the proceeds discovered is the main and final aim»[227] of a profit-oriented strategy, financial investigations represent the first step of the asset recovery proceedings[228] leading to confiscation, and for this reason Member States have been invited to resort to financial investigations from the very first steps of criminal proceedings according to a common approach[229].

Joint Action 98/699/JHA is an emblematic sign of the EU overall approach to illicit profits[230], as it included in essence the legislative priorities that the European Union developed in the following years, *i.e.* the harmonization of national laws, the facilitation of cooperation between national authorities, and the principle of mutual trust[231].

[227]M. Kilchling, *Tracing, Seizing and Confiscating Proceeds from Corruption (and other Illegal Conduct) Within or Outside the Criminal Justice System*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2001, 9(4), p. 264.

[228]M. Simonato, M. Lassalle, *A fragmented approach to asset recovery*, cit., p. 135.

[229]Council of the European Union, *Multidisciplinary Group on Organised Crime, Final report on the fifth round of mutual evaluation: Financial crime and financial investigations*, 2 August 2012, no. 12657/12, p. 21 ff.

[230]As seen above, the Joint Action, which was the first instrument addressing confiscation of crime proceeds, was adopted following the Action Plan to combat organized crime aopted by the Council on 28 April 1997. For an overview of the obligations set up therein, M.J. Borgers, *Confiscation of the Proceeds of Crime: The European Union Framework*, in C. King-C. Walker (eds), *Dirty Assets. Emerging Issues in the Regulation of Criminal and Terrorist Assets*, London, 2014, p. 28 ff.

[231]K. Ligeti, M. Simonato, *Asset Recovery in the EU: Towards a Comprehensive Enforce-*

Although an in-depth analysis of the Joint Action as well as of the instruments addressing the economic dimension of serious forms of crime that have been laid down over the years fall outside the scope of the present discussion, it is worth mentioning that obligations requiring Member States to comply with the requests of other Member States to identify, trace, freeze and confiscate suspected proceeds of crime were afterwards transposed into legal instruments based on the mutual recognition principle, which in the meantime was making his way in the field of criminal law[232].

First introduced by the Tampere conclusions of the Council of 1999 as the "cornerstone" of the new judicial cooperation mechanism in criminal matters replacing the mutual legal assistance model, the principle of mutual recognition should ensure faster and more effective cooperation channels between national authorities, simplifying the recognition and execution procedures of judicial decisions. In globalized and integrated economies where illegal assets easily flow from one jurisdiction to another to not be intercepted by judicial authorities, it is not uncommon that property deriving from crime is being held in, or transferred to, a state different than that in which the unlawful activity took place or in which the criminal investigation has been undertaken[233].

---

ment Model beyond Confiscation? An Introduction, in K. Ligeti-M. Simonato, *Chasing Criminal Money*, cit., p. 5.

[232]On the role of mutual recognition in criminal law, see V. Mitsilegas, *The constitutional implications of mutual recognition in criminal matters in the EU*, in *Common Market Law Review*, 2006, 43, p. 1277 ff.; S. Peers, *Mutual recognition and criminal law in the European Union: Has the Council got it wrong?*, in *Common Market Law Review*, 2004, 41(1), pp. 5-36; L. Winter Bachmaier, *Il principio del mutuo riconoscimento*, in R.E. Kostoris (ed.), *Manuale di Procedura Penale Europea*, Milan, 2025, pp. 407-415 and the bibliography referred to therein; C. Amalfitano, *Unione europea e principio del reciproco riconoscimento delle decisioni penali*, in H. Belluta-M. Ceresa-Gastaldo (eds), *L'ordine europeo di protezione. La tutela delle vittime di reato come motore della cooperazione giudiziaria*, Turin, 2016, pp. 21–61. Broadly on the principle within the Area of Freedom, Security and Justice, refer to C. Rizcallah, *Le principe de confiance mutuelle dans l'Union européenne: un principe en peril*, in *Le cahiers de la justice*, 2022, 3(3), pp. 447-460; *A. Di Stasi, A. Festa*, *Breaches of the Rule of Law in the EU: What Implications for the Principle of Mutual Trust in the Area of Freedom, Security and Justice?*, in T. Russo-A. Oriolo-G. Dalia (eds), *Solidarity and Rule of Law. The New Dimension of EU Security*, Cham, 2023, pp. 153-171.

[233]F. Gascón Inchausti, *Mutual Recognition and Transnational Confiscation Orders*, in S. Ruggeri (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, Berlin-Heidelberg, 2013, p. 263.

Therefore, the logic behind mutual recognition compensates for the abolition of borders within the EU insofar as it makes sure that criminals do not benefit from a borderless European Union[234] and also renders the asset recovery system more efficient.

Bearing in mind the definition of financial investigations featuring their various characteristics[235], the two legal instruments of judicial cooperation that come into play *vis-à-vis* financial investigations are Directive (EU) 2014/41 on the European Investigation Order (EIO Directive)[236] on the one hand, and Regulation (EU) 2018/1805 on the mutual recognition of freezing and confiscation orders[237] on the other, both based on Art. 82(a) TFEU.

Looking at the European Investigation Order, the aim of the EIO Directive is to harmonize the gathering of evidence within the Area of Freedom, Security and Justice by providing a comprehensive set of rules on invetigative measures to be carried out in the territory of a Member State ("executing Member State") different than that conducting the investigation ("issuing Member State")[238].

Therefore, the directive establishes a single regime for obtaining evidence in the EU, envisaging relationships built on dialogue and mutual trust[239] according to

[234] V. Mitsilegas, *The constitutional implications*, cit., p. 1281.

[235] See supra § 2.1.

[236] Directive (EU) 2014/41 of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130.

[237] 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, OJ L 303.

[238] For an overview on the Directive, in the vas literature, please refer to S. Allegrezza, *Collecting criminal evidence across the European Union: The European Investigation Order between flexibility and proportionality*, in S. Ruggeri (ed.), *Transnational Evidence and Multicultural Inquiries in Europe. Developments in EU Legis-lation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases*, Berlin-Heidelberg, pp. 51-67; A. Mangiaracina, *A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order*, in *Utrecht Law Review*, 2014, 10, pp. 113–133; T. Rafaraci, *General Considerations on the European Investigation Order*, in S. Ruggeri (ed.), *Transnational Evidence*, cit., pp. 37–44; M. Daniele, E. Calvanese, *Evidence Gathering*, in R. Kostoris, *Handbook of European Criminal Procedure*, Cham, 2018, pp. 353-368.

[239] «(...) and on the rebuttable presumption that other Member States comply with EU law and, in particular, fundamental rights», judgment of 8 December 2020,*Staatsanwaltschaft Wien (Falsified transfer orders)*, C-584/19, EU:C:2020:1002, para. 40. On the extent of this presumption in light of the recent CJEU case law, see A. Hernandez Weiss, *Effective protection of rights as a precondition to mutual recognition: Some thoughts on the CJEU's Gavanozov II de-*

which the issuing authorities are best placed to evaluate the necessity, proportionality and availability of the measure requested[240], and the executing authorities should not in principle challenge or go over their assessment - unless they decide to invoke one of the (limited) grounds for refusal[241].
After setting the general principles for the gathering of evidence, the EIO Directive lays down specific provisions for certain investigative measures, among which there are some serving the purposes of financial investigations[242]. Art. 26 and Art 27 EIO Directive allow judicial authority to ask for the execution of production orders aimed at retrieving banking or financial information[243].

Art. 26 EIO Directive transposes the first of the four measures identified when defining the concept of financial investigations, *i.e.* access to financial information concerning holds or accounts in possession of persons subject to criminal proceedings. According to the provision, the issuing authority shall indicate why such information is of substantial value to the proceeding and why it presumes that the banks in the executing territory might have that information[244].

Art. 27 further provides for the issuing of a production order to gather information on past transactions «which have been carried out during a defined period through one or more accounts» to be specified in the EIO. In both cases, should the

---

cision, in *New Journal of European Criminal Law*, 2022, 13(2), p. 187; S. Busillo, *Mutual Recognition in EU Judicial Criminal Cooperation and Its 'Conditional Application' to the European Investigation Order (EIO) Under ECJ Case Law*, in T. Russo-A. Oriolo-G. Dalia (eds), *Solidarity and Rule of Law*, cit., pp. 263-277.

[240] Art. 6 EIO Directive.

[241] Cf. Artt. 9-11 Directive (EU) 2014/14. This system entail a "jurisdictional split" between the two authorities, since the legal remedies against the substantive reasons underlying the adoption of the measure should be provided in the issuing Member State, whereas the execution of the measure and the possible harm to the guarantees of fundamental rights could also be challenged in the executing Member State. See judgment of 30 April 2024, *M.N.*, Case C-670/22, ECLI:EU:C:2024:372; Opinion of Advocate General Bobek, *Gavanozov II*, Case C-852/19, ECLI:EU:C:2021:346, para. 35.

[242] Although, as noted by G. Lasagni, *Banking Supervision*, cit., p. 303, the EIO Directive does not explicitely include a positive obligation for Member States to introduce these measures, but rather provides rules for those Member States which already have those measures in place.

[243] M. Panzavolta, *Ordine di indagine europeo e indagini bancarie: spunti di riflessione sul concetto di caso interno analogo e atto di indagine alternativo*, in M. Caianiello-A. Di Pietro (eds), *Indagini penali e amministrative in materia di frodi IVA e doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale*, Bari, p. 367 ff.

[244] Art. 26(3) Directive (EU) 2014/41. Cf. G. Lasagni, *Banking Supervision*, cit., p. 293.

bank in which the account is held not have the information requested, the order shall be refused. Where the investigating authority deems it necessary to gather evidence on banking transactions «in real time, continuously and over a certain period of time», it may request the executing authority to monitor one or more specified accounts[245]. Already envisaged by the First Protocol to the 2000 Convention on Mutual Assistance in Criminal Matters, real-time surveillance techniques of financial transactions represent a highly intrusive measure impinging on fundamental rights, not solely related to criminal procedure, especially when conducted digitally[246].

Real-time monitoring may serve several purposes, *inter alia* identifying suspicious financial transactions in order to apply freezing measures in a timely manner and not to disperse their evidentiary value. In this regard, the EIO Directive also allows national judicial authorities to order their counterpart to execute «any measure with a view to provisionally preventing the destruction, transformation, removal, transfer or disposal of an item that may be used as evidence»[247]. Given that assets freezing measures by nature target monetary funds held in bank accounts as well as cash and financial instruments, it can be contended that financial assets and bank accounts may fall within the material scope of reach of an EIO as it can address "any item" that may constitute a piece of evidence.

With regard to Regulation (EU) 2018/1805, the scenario is quite different. As mentioned, the Regulation lays down the rules to be followed by Member States in their territory for the recognition and execution of freezing and confiscation

[245]Art. 28(1), lett. *a* Directive (EU) 2014/41.

[246]G. Lasagni, *Banking Supervision*, cit., p. 298, mentions freedom of expression, secrecy of communications and private domicile, freedom of movement.

[247]Article 32 Directive (EU) 2014/41.

orders issued by another Member State[248]. As such, differently than what is provided under the EIO Directive, the Regulation specifically - but not exclusively - addresses the economic advantages deriving from the commission of crime and aims at depriving criminals of the proceeds of crime with the purpose to confiscate them and to provide adequate compensation to those affected[249].

In light of its nature and content, Regulation (EU) 2018/1805 is relevant to the objective of financial investigations only insofar as it contemplates the provisional measure of freezing orders, *i.e.* a judicial decision issued «in order to prevent the destruction, transformation, removal, transfer or disposal of property with a view to the confiscation thereof»[250]. Also in the case of the Regulation, bank accounts and financial assets arguably fall within the notion of "property" pursuant to art. 2(3) Regulation (EU) 2018/1805, that is «property of any description, whether corporeal or incorporeal, movable or immovable, and legal documents or instruments evidencing title or interest in such property», which is deemed to be the proceeds of a criminal offence, or its equivalent, or the instrumentalities of a criminal offence or their value[251].

All of the above offers an exhaustive overview of the strategy of the European Union in fighting profit-driven criminality. The reason why providing the whole picture is of paramount importance is two-fold.

---

[248]For a detailed overview of the Regulation, see A. M. Maugeri, *Il Regolamento (UE) 2018/1805 per il reciproco riconoscimento dei provvedimenti di congelamento e di confisca: una pietra angolare per la cooperazione e l'efficienza*, in *Dir. Pen. Cont.*, 2019, 1, pp. 1–40; S. Mirandola, *Borderless enforcement of freezing and confiscation orders in the EU: the first regulation on mutual recognition in criminal matters*, in *Era Forum*, 2019; F. Meyer, *Recognizing the unknown – the new confiscation regulation*, in *European Criminal Law Review*, 2022, 10(2), pp. 140-170; S. Oliveira e Silva, *Regulation (EU) 2018/1805 on the mutual recognition of freezing and confiscation orders: A headlong rush into Europe-wide harmonisation?*, in *New Journal of European Criminal Law*, 2022, 13(2), pp. 198–215.

[249]N. Brandão, *The right of defence under Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and confiscation orders*, in *New Journal of European Criminal Law*, 2022, 13(1), p. 30.

[250]Art. 2(1) Regulation (EU) 2018/1805. Cf. Art. 3(5) Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation, according to which "freezing" means «the temporary prohibition of the transfer, destruction, conversion, disposal or movement of property or temporarily assuming custody or control of property».

[251]Cf. Art. 3(2) Directive (EU) 2024/1260. The same conclusion is drawn by G. Lasagni, *Banking Supervision*, cit., p. 299, with reference to the equivalent provision previously included in Directive (EU) 2014/42.

To start with, it should be borne in mind that, while investigative measures based on mutual recognition take place at a judicial level, in that they are issued and executed in the context of criminal proceedings and in any event under the supervision of a judicial authority - also possibly subjected to prior or *ex post* judicial authorization depending on national legislation - it does not necessarily entail that fundamental rights are given sufficient consideration. As has been pointed out with reference to Regulation (EU) 2018/1805, the provisions specifically addressing the rights and procedural guarantees of those affected by the measures at stake are only «programmatic in nature» and clearly reveal an imbalance in favor of the efficiency of the cooperation mechanisms[252]. The scarcity of references to the rights of those affected by freezing and confiscation orders, whether it is the suspects and defendants or third parties involved, could be explained in the case of the Regulation in light of the harmonizing effect that the procedural rights Directives[253] should have brought about across Member States[254].

As for the EIO Directive, while Recital 15 acknowledges the Directives on procedural safeguards, because of its indirect applicability, the EIO Directive relies on the national legal frameworks under the law of the issuing state and the executing

[252]N. Brandão, *The right of defence*, cit., p. 31.

[253]These are Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings [2010] OJ L280, Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings [2012] OJ L 142, Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty [2013] OJ L 294, Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings [2016] OJ L 65, Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings [2016] OJ L 132, Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, [2016] OJ L 297. The origin and features of the EU legal framework on individual criminal procedural rights will be addressed below in §.

[254]The Directives in comment are solely mentioned in the recitels of the Regulation and the procedural safeguards stated therein are not therefore made applicable by the Regulation. See Ibid., p. 39.

state to provide adequate procedural rights. It follows that gaps may exist in the EU framework on fundamental rights when particularly intrusive investigations, as is the case for banking and financial inquiries, are not specifically regulated.

Second, the two facets of financial investigations, *i.e.* the intelligence-led approach promoted by the competent authorities in the prevention of risks of money laundering, namely FIUs, and traditional criminal investigation techniques, can complement each other revealing great potential in tackling serious crime, especially when it involves multiple jurisdictions and therefore requires the cooperation of different authorities according to the channels provided for by the system of mutual recognition shared by Member States. In fact, FIUs' expertise and specific tools allow public authorities to compensate for the exisiting information asymmetry and ensure a smoother and faster identification of criminal money as they focus on tracing illicit properties[255].

However, although the urgency to fight the most serious forms of economic and organized crime is strongly felt in light of the threats they pose on democratic society, the aim of "following the money" strategies cannot be pursued without any sort of constraint on the action of public authorities. Adequate procedural safeguards must be envisaged.

To that end, the following chapter will address the question as of whhether and to what extent the procedural safeguards provided by the EU legislative framework can find application to those targeted by criminal financial investigations. While attention will be paid in particular to the *nemo tenetur se detegere* principle, that is, the right of individuals not to incriminate themselves before the authority, and its relation to the presumption of innocence, it will be contended that fair trial standards should apply whenever financial ivestigations are initiated or, differently put, whenever information exchanges related to financial movements take place between public authorities and private actors. Hence, also

[255]For instance, it can occur that competent authorities in charge of investigating serious crimes with a cross-border dimension might need to rely on FIUs in order to gather useful information for the advancement of the investigations or identify the territory where the proceeds or the instrumentalities of the crime are held. Similarly, executing authorities authorities might need to gather information by their national FIUs in order to properly execute the measure requested.

in the context of prevention activities, whose bounderies are often blurred.

Chapter II

Nemo tenetur se detegere principle from old to new paradigms

1 Introduction

In the previous chapter, the architecture of financial investigations within the context of criminal prosecution was analyzed in light of both soft law and hard law instruments. The roles played by various actors throughout the proceedings leading to the identification of criminal assets were presented. In particular, the relationship between the AML/CTF preventive system and the criminal justice system was disentangled in order to grasp a sense of how their activities support each other in searching and identifying ill-derived money and to what extent information flows from one system to another.

It was suggested that the entire set of procedural safeguards that characterize criminal prosecution from the beginning of the investigations through the trial phase shall also be respected when financial investigations are being conducted in parallel or even within criminal investigations. Therefore, applicable fair trial rights should be offered to suspects and defendants when they are touched upon by particularly intrusive investigative measures. The present chapter will focus on the privilege against self-incrimination and the right to silence which, according to the well-established case law of The European Court of Human Rights (hereinafter:

ECtHR), lie at the heart of the notion of a fair procedure under Article 6 ECHR[1]. As noted in the introduction to the present work, the *nemo tenetur* principle guarantees civil society from illicit intrusions of public powers into the personal spheres of private citizens as it allows them to refrain from damaging themselves at the request of the authority. The chapter is divided as follows. After a necessary preliminary remark on the significance that secrecy has in the context of financial investigations, the privilege against self-incrimination will be thoroughly explored as enshrined in human rights law, especially in light of the case law of the Court of Strasbourg, and in the EU legal framework. Subsequently, the points made therin will be applied to, or their applicability will be verified against, the features of financial investigations.

2 The manifold relevance of secrecy in financial investigations and its clash with procedural rights

Before addressing the legal framework concerning the principle of *nemo tenetur se detegere*, how it is regulated and interpreted at the supranational level, and how it applies in the context of banking and financial investigations, a fundamental point shall be preliminarily made. In fact, the discussion concerning financial investigations and the actors involved therein - obliged entities, FIUs, and judicial authorities engaged in detecting and prosecuting economic crimes - cannot neglect the role that secrecy plays in shaping the dynamics between these actors. Secrecy, as obvious as it may seem, is vested with deeply significant value in (criminal) banking and financial law that is not exclusively related to the efficiency of the investigations, but is also intended to safeguard the interests of the parties involved. For the purposes of the present research, three different declinations of secrecy have been identified that require specific attention.

[1]ECtHR, [GC], 8 February 1996, *John Murray v. the United Kingdom*, Application n. 18731/91, § 45.

Firstly, the concept of secrecy is attached to the duty of banks and other credit institutions not to disclose their clients' information that they acquire in the course of their professional activity. This general duty is broadly referred to as "bank secrecy" or "bank confidentiality", and is usually based on private or contractual law provisions[2]. Initially conceived to guarantee the privacy of private individuals engaging in business relationships with credit institutions, bank secrecy has gradually lost its role of protecting confidentiality due to the increasing importance of financial information in combating serious forms of crime, including terrorism and terrorist financing, as well as the laundering of illicit proceeds. This process of erosion of bank secrecy in favor of the imposition of positive disclosure obligations was mostly triggered by the FATF Recommendations, which urged the widest extent possible of data sharing between obliged entities and authorities[3], preventing confidentiality from constituting a ground for refusing cooperation. It was also supported within the European regulatory framework, increasingly discouraging private businesses from resorting to professional secrecy when required by law to hand over confidential information[4]. As a consequence, banking secrecy law now retains only a residual role[5], given that the disclosure of customer information under compulsion of law frequently occurs in criminal and tax legislation as an exception to bank secrecy[6].

[2]D. Neo, *A conceptual overview of bank secrecy*, in S. Booysen-D. Neo (eds), *Can Banks Still Keep a Secret?: Bank Secrecy in Financial Centres Around the World*, Cambridge, 2017, p. 8 ff.

[3]FATF Recommendation 9 states that «[c]ountries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations», while for the sake of efficient transnational cooperation Recommendation 37 invites Member States not to resort to bank secrecy.

[4]For instance, the 2005 Council of Europe Convention on Laundering, Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS 198, Warsaw, 16.05.2005, provides under Art. 7(1) that «[a] Party shall not decline to act under the provisions of this article on grounds of bank secrecy». Similar terms are used in Art. 7 First Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, and Art. 18(2) Directive 2011/16/EU on administrative cooperation in the field of taxation.

[5]G. Lasagni, *Banking supervision and criminal investigation: comparing the EU and US experiences*, Cham, 2019, p. 286.

[6]Without going into detail, it should be noted that national systems differently regulate the strenght that bank secrecy holds before mandatory production orders of judicial authorities, but they mostly uniformingly provide that bank secrecy should be lifted to allow the advancement

The AML/CTF legislation is a clear example of the rebalancing of the competing interests of data protection and confidentiality on one hand, and the safeguard of financial markets on the other, in light of the duties upon financial institutions to submit suspicious transactions reports to FIUs and share Know Your Costumer (KYC) information to allow them to conduct preventive investigations. Along with what has been defined as the «death of bank secrecy»[7], the EU lawmaker has provided an exemption from liability of any kind for obliged entities or their employees that, in disclosing information to the FIU, are in breach of confidentiality obligations imposed by contract or by any legislative, regulatory, or administrative provision[8]. In sum, bank secrecy no longer represents an hurdle to preventive and, when national provisions envisage them, proactive investigations into financial transactions and therefore does not constitute a shield for customers data protection[9], clearly hampering the relationship between defense rights and

of criminal proceedings. For instance, in the French legal system, banks cannot refuse to comply with mandatory requests (*réquisitions*) from the police regarding bank information. However, when financial institutions are under criminal investigation, they should enjoy their right not to be compelled to cooperate with judicial authoritities and therefore to resort to their privilege. Nevertheless, claiming that legal entities enjoy a right not incriminate themselves is not a straightforward conclusion, since neither EU legal framework or most domestic legislations have a say on this. On the former, while representing a significant step forward in recognizing the right of individuals not to cooperate in their own incrimination during administrative but substantively criminal investigations, the aforementioned judgment *DB v. Consob* concerned a sanction imposed on a natural person and not on a legal entity and therefore it does not solve the question relating to the relation between the duty to disclose regardless of professional secrecy and the privilege against self-incrimination. Concerning specific national legislations, as highlighted by G. Lasagni, *Public-Private Cooperation in the Detection and Investigation of Criminal Offences in Italy*, in B. Vogel-E. Kosta-M. Lassalle (eds), *Law of Public-Private Cooperation against Financial Crime*, Cambridge-Antwerp-Chicago, 2024, p. 251, in the absence of an express reference in the Italian legislation on corporate liability (Legislative Decree 231/2001), legal scholarship deems that the privilege is also applicable to legal entities, although it may give rise to the administrative santiones for the violation of duties to cooperate. Cf. Art. 170-*bis* D.lgs. 24 february 1998, n. 58 and Art. 2638 CC.

[7]M. Levi, *Regulating Money Laundering: The Death of Bank Secrecy in the UK*, in *British Journal of Criminology*, 31(2), pp. 109-125.

[8]The disposition was set out in Art. 37 Dir. (EU) 2015/849, now repealed by Art. 72 Reg. (EU) 2024/1624. Cf. the Italian transposition pursuant to Art. 35(4) Legislative Decree 21 November 2007, n. 231.

[9]As put by D. Neo, *A conceptual overview*, cit., p. 27, «[p]rotection of the customer's privacy in financial matters is gradually being reduced and sacrificed. This might seem inconsistent with other aspects of privacy which seem to be enjoying increased protection, such as personal data protection, which has seen active development internationally. (...) This increased protection of

criminal prosecution.

Secondly, secrecy refers to the regime under which operational analysis is conducted by FIUs, with the cooperation of obliged entities. During their investigations, FIUs may require obliged entities to expand on the information submitted via their SARs or their CDD assessments, or act on their own initiative and ask to provide information without a prior report submission. When carrying out their inquiries, the communications between FIUs and obliged entities are marked by far-reaching confidentiality obligations, according to which neither FIUs nor obliged entities cooperating with them are abstractly allowed to share information concerning the analysis with the addressees of the investigation. More specifically, financial institutions are prevented from disclosing «to the customer concerned or to other third persons the fact that transactions or activities are being or have been assessed [for suspicious transaction reporting reasons], that information is being, will be or has been transmitted in accordance with [reporting obligations] or that a money laundering or terrorist financing analysis is being, or may be, carried out»[10]. The serious, repeated, or systemic violation of the so-called "tip-off" prohibition is punihed with pecuniary sanctions, either of criminal or administrative nature[11].

As for FIUs, the EU legal framework does not specify whether they can or have to inform the addressees of being subject to operational analysis, while some domestic legislations, such as the German one, leave it up to their FIUs to decide whether to disclose the data they retain upon request of the bank customer[12].

---

privacy in the sphere of data protection might appear diametrically opposed to the erosion of privacy that is happening in the sphere of bank secrecy (...)». The issues raised by financial investigations concerning data protection provisions will be addressed in Chapter IV.

[10]Art. 73 Reg. (EU) 2024/1624.

[11]Art. 55 Dir. (EU) 2024/1640. Cf. in the Italian legal system, Artt. 39(1) and 55 D.Lgs. n. 231/2007 providing criminal sanctions for natural persons in breach of their reporting obligations. To the contrary, the Spanish law on countering money laundering provides sanctions under administrative law, and the scope of the prohibition is also more limited than the Italian or European one, as it only covers the fact that a SAR has been submitted. See Artt. 50 Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.

[12]For a comparative analysis, see J.B. Maillart, *Anti-money laundering architectures. Between Structural Homogeneity and Functional Diversity*, in B. Vogel-J.B. Maillart (eds), *National and international Anti-money laundering law. Developing the architecture of criminal*

What can be drawn from the above is an overall framework that envisages the secret processing of information with very limited to no possibility for customers/suspects of even being aware that their financial profile is of interest to the FIU, and most likely to law enforcement authorities, and that their sensitive data is being shared with them. While the use of intelligence information is gradually making its way through criminal proceedings, insofar as intelligence agencies «are now increasingly also involved in the sphere of criminal justice, with information frequently being shared between intelligence agencies and police authorities with the aim of triggering or otherwise supporting criminal investigations»[13], the use of secret evidence impinges on the very essence of adversarial criminal proceedings, *i.e.* the possibility for the defense to challenge such evidence in the trial phase[14]. Insofar as the defendant cannot know the source of the information used against her, how such data have been collected, and what methods were used to analyze it, and in the absence of clear admissibility rules governing this type of evidence, fair trial rights are irremediably endangered[15].

Lastly, the secrecy requirement is entrenched in the investigations conducted during the pre-trial stage of criminal proceedings. In other terms, the urge to ensure the protection of the investigative objectives requires all initial acts of the proceedings to be covered by an obligation of confidentiality. As a rule, this means that all the parties involved in the investigations are bound by the secrecy requirement until the defendant is made aware of the investigations or when the full discovery of the activity carried out by the prosecutor is made to the de-

justice, regulation and data protection, Cambridge - Antwerp - Chicago, 2020, pp. 837-838.

[13]B. Vogel, *Balancing Procedural Fairness and Surveillance in Criminal Procedure Law*, in B. Vogel (ed.), *Secret Evidence in Criminal Proceedings*, Berlin, 2021, p. 2.

[14]M. Jimeno-Bulnes, *The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama*, in *New Journal of European Criminal Law*, 8(2), p. 178.

[15]The issue will be specifically addressed in Section 4.2. It should be just mention the case of the Spanish AML law, where it is explicitly stated that FIUs intelligence reports sent to competent authorities have no evidential value in criminal proceedings, which means that the information therein will have to be acquired according to criminal procedural law in order for judicial authorities to use it against the defendant. See A.C. Carlos de Oliveira, *The Anti-money laundering architecture in Spain*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laundering Law*, cit., p. 498.

fendant[16]. Thus, secrecy aims to protect the effectiveness of investigations and prevent anyone from tampering with evidence. However, this priority shall be balanced with the interests of the defence.

3 An overview on the *nemo tenetur* principle in light of the right to a fair trial

In adversarial legal systems, whose implementation in pure form, however, is ideal and hard-to-find in practice [17], criminal proceedings in general, and particularly tangibly the trial phase, are inspired by the dialectic principle as a form of reasoning and a method of argument[18], as opposed to the inquisitorial model centered around the principle of authority and the role of the judge gathering and assessing evidence in secret. This means that the parties are driven by opposite interests, but they nonetheless contribute equally to the finding of the truth[19] by

[16]In the Italian legal system, this occurs in the moment that the pre-trial stage is concluded and the defendant is informed that investigations have taken place against them. Cf. Artt. 329 and 415-*bis* CPP.

[17]M. R. Damaška, *The Faces of Justice and State Authority: A Comparative Approach to the Legal Process*, New Haven-London, 1986, p. 3, traces back the dicothomy between *processus per accusationem* and *processus per inquisitionem* to the 12th century, when it used to distinguish a process initiated by a private party and a process launched in her absence. It later acquired another meaning, as it was employed among comparativist scholars to differ between continental and Ango-american models of justice administration. Generally, it is used to refer to distinctive clusters of traits of specific modes of proceeding, insofar as the adversarial model «unfolds as an engagement of two adversaries before a relatively passive decision maker whose principal duty is to reach a verdict», whereas the nonadversarial model is an official inquiry mostly performed by public officials. However, as noted by the Author, such an opposition is not clear-cut, since various traits of one of the two models is incorporated into the other. On this latter point, see also J. D. Jackson, S. J. Summers, *The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions*, Cambridge, 2009, p. 39. This phenomenon of mixture between the two theoretical models is also noted by D. Negri, *Modelli e Concezioni*, in A. Camon-M. Daniele-D. Negri-C. Cesari-M.L. Di Bitonto-P.P. Paulesu, *Fondamenti di Procedura Penale*, Milan, 2025, p. 17, who identifies the harmonization process fostered by the European Union as one of the causal factors, as it paved the way towards a distinction based on the *fairness* of proceedings rather than their institutional organization.

[18]P. Tonini, C. Conti, *Manuale di Procedura Penale*, Milan 2025, p. 8; P. Tonini, C. Conti, *Il diritto delle prove penali nel sistema accusatorio contemporaneo*, Milan, 2025 p. 9; G. Illuminati, *Accusatorio e inquisitorio (sistema)*, in *Enc. giur. Treccani*, I, 1988, p. 5 ff.

[19]On the conceptualization of the truth in the context of criminal proceedings ("*verità processuale*"), as opposed to the material or historical truth, see G. Ubertis, *Prova, verità e processo*,

supporting their points of view before the judge, by producing and rebutting evidence, and by having the opportunity to challenge the counterpart's position[20]. Against this backdrop, the cultural and political choice[21] to abandon the sys-

in *Arch. Pen.*, 2020, 2, pp. 547-556; ID., *Profili di epistemiologia giudiziaria*, Milan, 2015, 1-32; M. TARUFFO, *La semplice verità. Il giudice e la costruzione dei fatti*, Rome-Bari, 2009; L. FERRAJOLI, *Diritto e Ragione. Teoria del garantismo penale*, Bari, 1989, p. 16 ff.

[20]As underlined by L. FERRAJOLI, *Diritto e Ragione*, cit., p. 621, the adversarial legal system is anchored to a criminal epistemology inspired by individual safeguards («*epistemologia garantista o accusatoria*»), which requires that the trial be carried out according to procedural guarantees that allow the verification and falsification of facts. Corollaries of the adversarial epistemology are therefore the existence of a triangular relationship between the parties and the impartial judge; the opportunity to object allegations; the burden of proof falling on the prosecution; defence rights; the principles of publicity of proceedings, orality and legality; and the reasoning of the judgment. See also the analysis conducted by B. VOGLER, *A World View of Criminal Justice*, Ashgate, 2005, p. 129 ff., where it is purported that «[the adversarial system] is based upon the premise that all people, including persons accused of criminal offences, enjoy rights and the freedom to express their legitimate independent perspectives. Since the state is so much more powerful than individuals, such perspectives can only be understood and safeguarded in a criminal trial by placing the state under certain structural restrictions».

[21]V. PATANÈ, *Nemo tenetur se detegere: coordinate europee e parametri costituzionali del diritto a non collaborare dell'imputato*, in *Cass. pen.*, 2024, p. 2001, points out that the regulation of the cognitive contribution to the trial of an individual, even more so when they are defendants, is strongly conditioned by the political structure and ideological characterization of the legal system at a given historical moment.

tem of legal evidence[22] and the imposition on suspects of a duty to cooperate[23] with the judicial authority that were valid throughout the Middle Ages is arguably one of the clearest manifestations of the dialectical approach in criminal proceedings[24]. Once the view according to which a person subjected to criminal

[22]The notion of system of legal proofs (*sistema di prove legali*) refers to the «fixed strict statutory rules» (J. D. Jackson, S. J. Summers, *The Internationalisation of Criminal Evidence*, cit., p. 90) that the Canon law-inpired inquisitorial legal systems between the XIII and XVI century employed to dictate how evidence should be admitted and assessed by judges, who were left with no discretion in determining the guilt or the innocence of the accused. While the system of legal proofs was conceived in contintental European countries as a safeguard against the abuse of power of judges during the Middle Ages, its rationale started to be challenged by Enlightement thinkers and philosphers, because of its unethical implications, its blind application regardless of any personal assessment by the judge and the pre-eminent role attributed to confession - even extorted by means of torture - as the most unambiguous piece of evidence (for a general overview, see M. Sbriccoli, *Giustizia criminale*, in M. Fioravanti (ed.), *Lo Stato moderno in Europa. Istituzioni e diritto*, Rome-Bari, 2007, p. 187 ff.; E. Dezza, *Accusa e inquisizione. Dal diritto comune ai codici moderni*, Milan, 1989, p. 24 ff.). The doctrines developed during the Age of the Enlightement largely anticipated the reforms occurred in the nineteenth century accross continental European legal systems, which paved the way to the principles of free proof and *intime conviction*, which are still valid today. As reminded by scholars, however, the principle of free proof «should not be misunderstood as requiring simply that the judge have an intuitive feeling for the truth. The conviction must be based on logical, comprehensible reasons» (J. D. Jackson, S. J. Summers, *The Internationalisation of Criminal Evidence*, cit., p. 98).

[23]In the common law tradition, an *ex officio* oath procedure was in place before the Court of Star Chamber and the Court of High Commission for ecclesiastical causes, under which accused persons were required to take an oath to answer all questions (see R. H. Helmolz, *The Privilege and the Ius Commune: The Middle Ages to the Seventeenth Century*, in R.H. Helmolz-C. M. Gray-J. H. Langbein-E. Moglen-H. E. Smith-A. W. Alschuler (eds), *The Privilege against Self-Incrimination: Its Origins and Development*, Chicago, 1997, p. 17 ff.). The Courts and the oath procedure were abolished in 1641. In continental European countries, systems of *judicial torture* were in place (J.H. Langbein, *Torture and the Law of Proof: Europe and England in the Ancien Régime*, Chicago-London, 1977, p. 3), in which physical coercions was used by officals of the state to gather evidence for judicial proceedings. The use of torture was a natural consequence of the system of legal proof, since coercing a confession would have made the search of full evidence and oblective standards of proof unnecessary. See extensively V. Grevi, *«Nemo tenetur se detegere». Interrogatorio dell'imputato e diritto al silenzio nel processo penale italiano*, Milan, 1972, p. 5 ff; R. Vogler, *A World View*, cit., p. 25 ff.

[24]In this sense, F. Cordero, *Procedura penale*, Milan, 1979, p. 19, who strongly links the adversarial logic to a specific understanding of society according to which the fight against crime always encounters a limit imposed by the psyche of suspects, and therefore their moral freedom. The Author reminds us how the adversarial model stands in opposition to the "leviathanic" inquisitorial logic, «secondo la quale l'imputato è depositario di una verità da spremere». More recently, from the same author, F. Cordero, *Procedura penale*, Milan, 2012, pp. 21-38. See also G. Di Chiara, *L'imputato e il diritto di difesa*, in G. Fiandaca, G. Di Chiara, *Una introduzione al sistema penale. Per una lettura costituzionalmente orientata*, Naples, 2003, p.

proceedings is nothing more than an object of proof to be tested with every type of coercion was abandoned, the idea that emerged was that of a trial *secundum naturam*, therefore conceived as an instrument «volto ad una decisione possibilmente giusta, ottenuta senza sacrificare troppo la dignità delle persone implicate nel gioco»[25]. In other words, the idea that no one can be forced to contribute to compromising their own position by incriminating themselves finds justification in the need to both balance the conflicting interests pursued by the various subjects of the criminal proceedings[26] and, in any case, to protect their moral freedom and self-determination[27].

The principle of *nemo tenetur se detegere* embodies a set of values that contribute to the fairness of the trial and lies, in fact, at the heart of fair trial[28]. As now attested by a plentiful jurisprudence of the Strasbourg Court on the matter, the right to silence and the privilege against self-incrimination — though not expressly mentioned in Article 6 of the Convention — guarantee the suspect's free choice vis-à-vis abusive coercion by the authorities[29]. This helps prevent miscarriages of justice and satisfy the rights guaranteed by Article 6 ECHR, particularly the principle of equality of arms.

287, with reference to the interrogation of the defendant, which is strongly marked by evidentiary purposes in inquisitorial systems, whereas it is understood as a defensive tool in adversary models.

[25] F. Cordero, *Procedura penale*, cit., p. 23.

[26] Consider the case of a witness who, liable to a criminal penalty if they don't answer truthfully, makes self-incriminating statements. This undermines their private interest in self-preservation for the sake of the public interest in the proper administration of justice. Cf. P. Tonini, C. Conti, *Manuale*, cit., p. 324-325.

[27] As noted by F.M.W. Billing, *The Right To Silence In Transnational Criminal Proceedings: Comparative law perspectives*, Cham, 2016, p. 4, the crux of the matter lies in finding the right balance between the effectiveness of law enforcement and respect for fair trial rights.

[28] «Although not specifically mentioned in Article 6 of the Convention, there can be no doubt that the right to remain silent under police questioning and the privilege against self-incrimination are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6». ECtHR [GC], 8 February 1996, *John Murray v. United Kingdom*, Appl. No. 18731/91, § 45.

[29] As will be seen below, the Court of Strasbourg has reitered this principle in several decisions, starting from judgment 25 February 1993, *Funke v. France*, Appl. No 10828/84. *Ex multis*, ECtHR [GC], 17 December 1996, *Saunders v. United Kingdom*, Appl. No 19187/91; ECtHR [GC] 11 July 2006, *Jalloh v. Germany*, Appl. No 54810/00; ECtHR [GC], 5 February 2003, *Allan v. United Kingdom*, Appl. No 48539/99; ECtHR, sec. II, 3 August 2001, *J.B. v. Switzerland*, Appl. No 31827

Furthermore, while it is accepted that the right to refrain from answering questions posed by the investigating authority, in which the principle is embodied, is recognized to all individuals involved in criminal proceedings, it is also true that the *nemo tenetur* safeguard gains greater traction when applied to the position of the suspect or defendant. This is because the latter can use her silence as a tool to exercise their right to defense. In this sense, silence is strongly related to the self-defense of suspects and defendants as a form of passive defense[30] throughout all the stages of the criminal process, from the preliminary investigations to the trial. Therefore, the right to silence can be understood not only as a "protective" right, aimed at upholding substantive values such as the dignity and the moral freedom of suspects[31], but also as an "enabling" or "participatory" right, as for instance the equality of arms or the right to rebut evidence, which allow the defendant to effectively defend herself on an informed and willing basis[32].

From this perspective, the intrinsic connection that the *nemo tenetur* principle have with the fairness of the proceedings is made even more evident in light of the essence of the presumption of innocence principle, guaranteed by Article 6, § 2 ECHR. In fact, the right to silence and the privilege against self-incrimination can be said to be a logical implication of the presumption[33], insofar as the presumption

[30]In the Italian literature, see extensively L. Marafioti, *Scelte autodifensive dell'indagato e alternative al silenzio*, Turin, 2000, p. 123 ff., who includes the *ius tacendi* of the defendant as a constitutionally protected "negative" expression of their right to self-defence. See also O. Mazza, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Turin, 2004, p. 42 ff.

[31]Procedural defensive rights in general are strongly anchored to moral freedom, as noted by P. Felicioni, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Milan, 2009, p. 34.

[32]F.M.W. Billing *The Right To Silence*, cit., p. 12; J. D. Jackson, *Re-Conceptualizing the right of silence as an effective fair trial standard*, in *International and Comparative Law Quarterly*, 2009, 58, p. 853, according to whom suspects should not be questioned until they have had the chance to prepare their defence; Id., *The Effect of Human Rights on Criminal Evidentiary Processes: Towards Convergence, Divergence or Realignment?*, in *The Modern Law Review*, 68(5), p. 737 ff.; in general terms on the distinction, see A. Roberts, *Pre-Trial Defence Rights and the Fair Use of Eyewitness Identification Procedures*, in *The Modern Law Review*, 2008, 71(3), p. 337, who nevertheless points out how these aspects overlap insofar as «rights which secure opportunities for participation provide a means of protecting the suspect's interest». For a distinction between substantive and procedural aspects of the privilege against self-incrimination, see S. Lamberigts, *The privilege against self-incrimination. A chameleon of criminal procedure*, in *New Journal of European Criminal Law*, 2016, 7(4, p. 426 ff.

[33]V. Grevi, *«Nemo tenetur se detegere»*, cit., p. 13, ft. 17, had already noted, with refer-

carries with it an evidentiary obligation on the state to prove the alleged offence against the accused[34], and the criminal justice system presumes that the individual under investigation is unaware of the facts to which they are called on to answer[35]. This connection can also be drawn from the EU Charter of the fundamental rights, insofar as the meaning and the scope of the rights enshrined therein that correspond to rights guaranteed by the ECHR must be interpreted as being the same as those laid down by the correlating articles of the ECHR, in accordance with the homogeneity clause in Art. 52(3) CFREU. More specifically, as provided for in the Explanations to the Charter[36], Art. 47(2) CFREU on fair trial[37] shall bear, as a minimum, the same meaning and protection as that stemming from Art. 6, § 1 ECHR, and similarly Art. 48 CFREU[38] is the same as Art. 6, § 2 and 3 ECHR, as interpreted by the European Court[39].

Art. 47 and Art. 48 CFREU are closely linked together, since Art. 48(2) guarantees the rights of the defence as being an element of the right to a fair trial stated in Art. 47(2), since «if a trial is to be considered fair, the proess must comply with specific requirements»[40].

---

ence to the European Enlightenment movement, which was the first to draw attention to the immorality inherent in forcing an accused person to incriminate themselves: «[è] chiaro, in altri termini, come il riconoscimento all'imputato della libertà di tacere presupponga un sistema processuale in cui l'imputato stesso non abbia alcun obbligo di "purgarsi" – e sia, cioè, presunto innocente, o comunque non colpevole». See also G. Illuminati, *La presunzione d'innocenza dell'imputato*, Bologna, 1979, p. 191 ff.

[34]J. D. Jackson, S. J. Summers, *The Internationalisation of Criminal Evidence*, cit., p. 290.

[35]In the words of G. Ubertis, *Principi di procedura penale europea. Le regole del giusto processo*, Milan, 2009, p. 59, «sarebbe contraddittorio pretendere un contributo alla ricerca della verità da parte di chi va presunto estraneo al fatto per cui si procede».

[36]Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007.

[37]«Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented».

[38]«Everyone who has been charged shall be presumed innocent until proved guilty according to law. Respect for the rights of the defence of anyone who has been charged shall be guaranteed».

[39]D. Sayers, *Article 48 (Criminal Law)*, in S. Peers-T. Hervey-J. Kenner-A. Ward, *The EU Charter of Fundamental Rights. A Commentary*, Oxford-Portland, 2021, p. 1323.

[40]D. Sayers, *Article 48 (Criminal Law)*, cit., p. 1309. For a recent reaffirmation of the meaning to be attributed to Articles 47 and 48 CFREU in regard with the right to silence, see the conclusions of Advocate General Pikamäe in Case C-481/19, *DB v. Consob*, ECLI:EU:C:2020:861, para. 50. The facts and the ruling of the Court will be analyzed in Section 2.2.

Before addressing in detail the regulation and interpretation of the principle of *nemo tenetur* in light of the case law of the Court of Strasbourg and within the EU legal framework, which will be dedicated the following sections, it should be outlined here, for the sake of clarification, what is to be understood by right to silence on one hand and privilege against self-incrimination on the other. As a consequence of the lack of clear legislative references or guidelines on the part of the courts, terminological confusion rules this topic[41] with different categorizations having been formulated in the literature. Some authors have identified three different aspects within the formulation "right to silence": the right not to be questioned by the judge; the privilege against self-incrimination, which is recognized to any person called to make statements; and the right to silence *strictu sensu* of the defendant[42]. Other teorizations understand the privilege against self-incrimination as an early protection of the right to silence, insofar as the former protects anyone from providing incriminating information «until the right to silence is triggered, that is, until the person becomes a suspect»[43]. In accordance with it, the protection afforded by the right to silence is stronger than, and its scope of application broader then, the one of the privilege, insofar as it covers any declarations and not just the incriminating ones[44].

[41] Which, however, might bring about certain advantages insofar as the guarantee stemming therefrom have certain felxibility that a fixed text would not allow, as noted by S. Trechsel, S. J. Summers, *Human Rights in Criminal Proceedings*, Oxford, 2005, p. 342.

[42] E. Amodio, *Diritto al silenzio o dovere di collaborazione?*, in *Riv. dir. proc.*, 1974, p. 412; L. Marafioti, *Scelte autodifensive*, cit., p. 115; V. Patanè, *Il diritto al silenzio dell'imputato*, Turin, 2006, p. 3.

[43] D. Marchesi, M. Panzavolta, *Keep silence for yourself: The protection of the right to silence in the Italian criminal justice system*, in *New Journal of European Criminal Law*, 2021, 3, p. 367. Similarly, P. Tonini, C. Conti, *Manuale*, cit., p. 324

[44] D. Marchesi, M. Panzavolta, *Keep silence for yourself*, cit., p. 368; S. Trechsel, *Human Rights*, cit., p. 342. However, cf. M.W. Billing, *The right to silence*, cit., p. 9 ff., while believing that the privilege against self-incrimination is a component of the broader right to silence, identifies greater protection in the former when considering the type of information source. This is because the privilege does not only concern self-incriminating statements but also any document or real evidence that exists independently of the accused's will. This leads to the author's criticism of the ECHR's case law, which will be discussed below, for failing to make any distinction between the right to silence and the right not to incriminate oneself.

3.1 Protecting the right to silence of suspects under human rights law: the European Convention of Human Rights

The discussion will focus on the European Convention of Human Rights (ECHR) as interpreted by the case law of the European Court of Human Rights (ECtHR), although no explicit reference to the privilege against self-incrimination can be found throughout the convention. Unlike other human rights law instruments that specifically mention the privilege and the right to silence[45], Art. 6 ECHR omits any guarantee in this regard. However, the longstanding take of the Court on the matter acknowledges that the right to remain silent and the privilege against self-incrimination are generally recognised international standards which lie at the heart of the notion of a fair trial under Article 6[46]. Starting from the decision in which the privilege was introduced in its jurisprudence for the first time, that is, *Funke v. France* in 1993[47], the Court has progressively shaped the contours of the privilege against self-incrimination, namely its rationale and its scope of application, although the understanding of the decisions of the Court is not straightforward. For instance, the very distinction between the two concepts of the right to silence on the one hand and the privilege against self-incrimination on the other is blurred, insofar as it refers to the "right not to incriminate oneself" but extends it beyond «statements of admissions of wrongdoings which are directly incriminating»[48], thus overlapping with the content of the right to silence[49].

[45]Article 14(3)(g) of the ICCPR states that everyone shall be entitled to the right '[n]ot to be compelled to testify against himself or to confess guilt' and Article 8(2) (g) of the ACHR refers in similar terms to 'the right not to be compelled to be a witness against himself or to plead guilty'

[46]ECtHR [GC], 8 February 1996, *John Murray v. United Kingdom*, Appl. No 18731/91, § 45;ECtHR [GC], 17 December 1996, *Saunders v. United Kingdom*, Appl. No. 19187/91, § 68.

[47]ECtHR, 25 February 1993, *Funke v. France*, Appl. No 10828/84. For an overview, see J. Jackson, S.J. Summers, *The Internationalisation of Criminal Evidence*, cit., p. 273.

[48]ECtHR [GC], 13 September 2016, *Ibrahim and Others v. United Kingdom*, Appl. No 50541/08, 50571/08, 50573/08 and 40351/09, § 268;

[49]See ECtHR, *Saunders*, cit., dissenting opinion of Judge Martens, §§ 4 and 12, where it is held that the majority has merged the broader concept of the privilege, which referes to the right not to cooperate in providing evidence against oneself, with the right to silence, *i.e.*, the right not to answer questions. As noted by F. M. W. Billing, *The Right to Silence*, cit. p. 11,

Regarding the rationale, Strasbourg judges have actually identified more than one rationale behind the privilege and the right to silence. As mentioned above, the Court connects the privilege against self-incrimination to the presumption of innocence as guaranteed by Art. 6(2) ECHR, inasmuch as it implies that «the prosecution in a criminal case seek[s] to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused»[50]. In other terms, if the defendant, who shall be presumed innocent throughout the criminal proceedings and therefore unaware of the facts, was compelled to provide evidence against herself on those facts, this would not only be contradictory on the part of the state[51], but would also debase the basic rule according to which the prosecution must prove the guilt beyond any reasonable doubt[52]. Putting the suspect under an obligation to cooperate with the authorities in building a case against her would shift the burden of proof from the prosecution to the defence, with the subsequent violation of the presumption of innocence[53].

Secondly and predominantly, the privilege is justified by the aim of protecting the suspect against improper compulsion exerted by the authorities, which may lead to unrieliable evidence[54]. However self-evident this argument might be[55], improper compulsion represents the decisive element in order for an issue to arise from the perspective of the privilege against self-incrimination[56], although the

while the privilege against self-incrimination indeed offers a broader protection than the right against self-incrimination in terms of the type of information it applies to (both oral statements and documentary production), the right to silence is broader in the sense that it protects from any kind of statement and not just incriminating ones.

[50]ECtHR, *Saunders*, cit., § 68.

[51]G. Ubertis, *Principi*, cit., p. 59.

[52]A. Ashworth, *Self-incrimination*, cit., p. 767. However, cf. M. Redmayne, *Rethinking the Privilege Against Self-Incrimination*, in *Oxford Journal of Legal Studies*, 2007, 27(2), p. 219 for clarifications on the meaning to be attributed to the standard of proof.

[53]ECtHR, Sec. III, 20 March 2001, *Telfner v. Austria*, Appl. No 33501/96, § 15. The Court reached a different conclusion in *John Murray*, cit., § 54, since it found that the adverse inferences derived from the silence of the suspect did not amount to shifting the burden of proof to the defendant.

[54]S. Lamberigts, *The privilege against self-incrimination. A chameleon of criminal procedure*, in *New Journal of European Criminal Law*, 2016, 7(4), ft. 65.

[55]S. Trechsel, *Human Rights*, cit., p. 347.

[56]As a matter of fact, the privilege against self-incrimination does not protect against the

Court never clarified what improper compulsion is. Instead, in addition to making a distinction between direct and indirect compulsion[57], the Court identified three different scenarios in which improper compulsion might be in breach of the privilege against self-incrimination, *i.e.* when the suspect is obliged to testify under threat of sanctions imposed in the same proceedings or in other parallel proceedings; where physical or psychological pressure, often in the form of torture or ill treatment which breaches Article 3 ECHR[58], is applied to obtain self-incriminating information; finally, when the authorities use subterfuge to elicit information that they were unable to obtain[59].

While improper compulsion is one of the conditions that need to be satisfied for the circumstance to be relevant for the freedom from self-incrimination[60], it is not *per se* sufficient for the protection therefrom to be triggered. In this regard, the Court clarified that the privilege is not an absolute right, as in the improper compulsion exerted by public authorities is incompatible with Article 6 where «it extinguishes the very essence of the privilege against self-incrimination». For this purpose, the Court usually has regard, in turn, to the following factors: the nature and degree of compulsion used to obtain the evidence; the existence of any relevant safeguards in the procedure; and the use to which any material so obtained is put[61]. In this sense, the Court reiterates its distinctive substantial

making of an incriminating statement *per se*, which may also occurr voluntarily or inadvertently, but only against the obtaining of evidence by coercion or oppression. See J. E. Veas, *A Comparative Analysis of the Case Law of the European Court of Human Rights on the Right against Self-Incrimination*, in *Revista Brasileira de Direito Procesual Penale*, 2022, 8, p. 878.

[57]The Court implies this distinction in the case *John Murray*, cit., § 50, insofar as it held that warning the suspect that adverse inferences may be drawn from her silence represents a form of indirect compulsion, which could nevertheless still be consistent with the spirit of Art. 6 ECHR as long as domestic legislations provide for adequate safeguards and the silence is not the only evidence on which a declaration of conviction relies.

[58]This was the case in ECtHR [GC], 11 July 2006, *Jalloh v. Germany* Appl. No 54810/00.

[59]Cf. ECtHR [GC], 5 February 2003, *Allan v. United Kingdom*, Appl. No. 48539/99, in which the Court found a violation of the applicant's right against self-incrimination because, while detained, he had made incriminating statements to his cellmate, who had been instructed by the police to record their conversations.

[60]J. Jackson-S.J. Summers, *The Internationalisation of Criminal Evidence*, cit., p. 277, together with incrimination and the defiance of the will of the accused.

[61]ECtHR, Sec. IV, 21 March 2001, *Heaney and McGuinness v. Ireland*, Appl. No. 34720/97, §§ 47-58; ECtHR, *Jalloh*, cit., §§117-122.

approach, according to which a violation of Art. 6 ECHR is found only where the overall fairness of the proceedings has been infringed by a procedural error and no other compensating factors can remedy such error[62].

Moreover, in close connection to the argument of compelled unreliable evidence, another rationale was identified by the Court which is more procedural in nature, as it consists in the avoidance of miscarriages of justice and wrongful convictions[63].

Finally, the Court mantains that the rationale for the privilege against self-incrimination is primarily concerned with respecting the will of an accused person to remain silent[64], thus suggesting that the contribution of the suspect to the criminal proceedings must occur on a voluntary basis[65]. However, starting from the *Saunders* case, Strasbourg judges have clarified that some type of material falls outside the scope of protection of the privilege as if its acquisition by coercive means was not in fact in defiance of the will of the accused. More specifically, the Court has drawn a distinction between evidence connected to the person's will, *i.e.*, oral statements made as a result of compulsion, and «evidence that has an existence independent of the will of the suspect». According to the Court, these *Saunders exceptions*, among which there are documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing, can be obtained from the accused through the use of compul-

[62]Cfr ECtHR [GC], 13 September 2016, *Ibrahim and Others V. United Kingdom*, Appl. Nos 50541/08, 50571/08, 50573/08 e 40351/09, §§ 250-251; ECtHR [GC], 29 June 2007, *O'Halloran and Francis v. the United Kingdom*, Appl. Nos. 15809/02 and 25624/02, § 55.

[63]Some scholars criticize the way in which the Court links together a strictly substantive rationale, *i.e.*, preventing the authorities to collect evidence from the suspect in defiance of their dignity and their will, to a procedural rationale which relates to the fair trial and the presumption of innocence, and the possibility for the suspect to build their defence. See J. Jackson, *Re-conceptualizing the right of silence as an effective fair trial standard*, in *International and Comparative Law Quarterly*, 2009, 4, p. 842. Cf. also A. Ashworth, *Self-incrimination in European human rights law - a pregnant pragmatism?*, in *Cardozo Law Review*, 30, p. 768, according to whom «the privilege against self-incrimination and the right to silence belong to a cluster of criminal justice rights, centering on the presumption of innocence and the principle of equality of arms, and reaching out to the right of confidential access to a legal adviser, the right to disclosure of evidence held by the prosecution, the right of confrontation and other rights expressed or implied in Article 6 of the Convention».

[64]ECtHR Jalloh, cit., § 100; ECtHR, *Saunders*, § 69.

[65]J. Jackson, *Reconceptualizing the Right of Silence*, cit., p. 842.

sory powers[66]. While the *ratio* supporting such a differentiation has never been addressed in the case law[67], the Court has not rejected in full the idea that real evidence can indeed be collected in violation of the privilege. In fact, not only does the guarantee apply when the improper compulsion to obtain material and pre-existing evidence amounts to torture or inhumane or degrading treatment[68], but also when public authorities do not have knowledge of the existence of the incriminating evidence, but nonetheless engage in *fishing expeditions* in the attempt to compel an individual to provide evidence of offences he or she has allegedly committed[69].

Whatever the rationale, the Court has argued that the improper compulsion must take place in circumstances that are strictly connected to a criminal proceeding. More specifically, this applies to «cases relating to the use of compulsion for the purpose of obtaining information which might incriminate the person concerned in pending or anticipated criminal proceedings», but also to cases in which evidence is collected outside of the criminal investigation but is used in subsequent criminal proceedings. In the first scenario, oral or real evidence is compulsorily obtained from a suspect who has already been charged or when the pre-trial is

[66]ECtHR, *Saunders*, cit., § 69.

[67]F. M. W. Billing, *The right to silence*, cit., p. 11, argues that real evidence «is tangible and capable of independent examination, such as forensic testing», and therefore «more trustworthy and less open to manipulation by physical or psychological compulsion». M. Redmayne, *Rethinking the Privilege*, cit., p. 215, suggests that the privilege is means-, and not material-based, meaning that it applies to certain means of obtaining information, those that require cooperation from the suspect, and not to specific type of information. It follows that the material evidence that is not created as a result of the compulsion of the authorities can be obtained without resorting to cooperation and is therefore not in breach of Art. 6 ECHR. In so reasoning, the Author maintains that the Saunders judgment would be consistent with the conclusions reached by the Court in *Funke*, where it found a violation of Art. 6 ECHR for the applicant had been compelled to hand over financial documents to the authorities.

[68]ECtHR, *Jallow*, cit., § 100-108; ECtHR [GC], 1° June 2010, *Gäfgen v. Germany*, Appl. No 22978/05, § 166-168; ECtHR., Sec. II, 25 September 2012, *El Haski v. Belgium*, Appl. No 649/08, § 85. See P. Hirvela, S. Heikkila, *Right to a fair trial. A practical guide to the article 6 case-law of the European Court of Human Rights*, Cambridge, 2021, pp. 142-144.

[69]ECtHR, *De Legé*, cit., § 76. However, it is not convincing how the degree of awareness of the authority about the existence of specific evidence should somehow affect the assessment as of whether the suspect has been improperly compelled to incriminate herself. On this note, J. Escobar Veas, *De Legé v. the Netherlands: The ECtHR adopts a line of reasoning similar to that of the United States Supreme Court on compelled production of real or physical evidence*, in *Maastricht Journal of European and Comparative Law*, 2023, 30(5), p. 664.

pending[70]. The notion of "charge" for the purposes of Art. 6 ECHR has been given an autonomous interpretation by the Court, which looks at whether the situation of the suspect has been «substantially affected»[71] or whether the suspect has been officially notified the she is suspected of an offense. Adopting a substantive approach, the Court acknowledges that in certain circumstances the privilege is applicable even before or in the absence of a formal allegation, insofar as «somebody is confronted with questions or with a request for documents which could result in self-incrimination» and is therefore considered *de facto* as a person charged for a criminal offense[72]. This point also answers the question as to the subjective scope of application of the privilege, insofar as the privilege against self-incrimination aims at protecting those who are subject to a criminal charge in light of the autonomous interpretation developed by the Court.

To the contrary, in the second scenario, a criminal proceeding has not yet been initiated and the self-incriminating information is collected in the course of non-criminal procedures, but is subsequently used in a criminal prosecution that is clearly and sufficiently connected to the first one[73]. This does not lead to suggest that Art. 6 prevents public authorities from seeking, even by means of coercion, information from citizens who are subject to forms of law enforcement investigations, especially when such information is connected to the functioning of regulatory systems «which are necessary if modern government is to function efficiently and fairly»[74]. Instead, according to the Court, Art. 6 ECHR is breached

[70]ECtHR, *J.B.*, cit., § 44-49; ECtHR, Sec. IV, 4 October 2005, *Shannon v. United Kingdom*, Appl. No 6563/03, §§ 34-39.

[71]ECtHR, 27 February 1980, *Deweer v. Belgium*, Appl. No 6903/75, § 42-46; ECtHR, Sec. III, 8 April 2014, *Blaj v. Romania*, Appl. No 36259/04, § 74; ECtHR, Sec. I, 18 February 2010, *Aleksandr Zaichenko v. Russia*, Appl. No 39660/02, § 42-45

[72]S. Trechsel, *Human Rights*, cit., p. 350, who, however, observes how contradictory the decisions of the Court on this point are.

[73]ECtHR, Sec. V, 5 April 2012, *Chambaz v. Switzerland*, Appl. No 11663/04, § 46

[74]A. Ashworth, *Self-incrimination in European human rights law*, cit., p. 772; F. Zacchè, *Gli effetti della giurisprudenza europea in tema di privilegio contro le autoincriminazioni e diritto al silenzio*, in A. Balsamo-R.E. Kostoris (eds), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, p. 188. It is no surprise that most of the cases in which the violation of the privilege has been acknowledged concern tax and he context of financial-law matters. Cf. ECtHr, *Chambaz*, cit., § 55; ECtHR, *J.B.*, cit., §§65-66; ECtHR, Sec. IV, 30 January 2023, *De Legé v. the Netherlands*, Appl. No 58342/15; ECtHR, *Allan*, cit.

when the evidence so obtained is used in criminal proceedings, thus putting the person «under statutory compulsion to contribute actively to the preparation of the case which was subsequently brought against him»[75]. It can therefore be drawn from the Court's case law that what should be deemed relevant for the applicability of the privilege against self-incrimination is the criminal nature of the proceedings in which the demand for information production occurs, regardless of the formal qualification according to domestic law[76], or else the nature of the proceedings for which the self-incrimination is sought[77].

3.2 The EU legal framework on procedural safeguards: Directive (EU) 2016/343 on the presumption of innocence

At the beginning of this section, the logic underpinning the connection between the principle of the *nemo tenetur* and the presumption of innocence was demonstrated, showing how it necessarily relates to the fundamental rule of criminal procedural law according to which the burden of proof of guilt lies with the prosecution. While the Court of Strasbourg rarely traced the privilege back to the presumption of innocence under Art. 6(2) ECHR, this is particularly evident within the EU legal framework, pursuant to which the right to silence and the privilege against self-incrimination are based on Article 47 and Article 48 CFREU[78].

[75]ECtHR, *Saunders*, cit., concurring opinion of Judge Morenilla. The *Saunders* case concerned the use in court of the transcript records of the interviews that the applicant was subjected to by the Department of Trade and Industry inspectors, whose answers had been passed on to the police to build the criminal case. According to M. Berger, *Europeanizing Self-Incrimination: The Right to Remain Silent in the European Court of Human Rights*, in *Columbia Journal of European Law*, 2006, 12(2), p. 362, the judgment in *Saunders* represents a "logical extension" of the privilege against self-incrimination and the right to silence, insofar as it extended their scope beyond the obtaining of evidence within the criminal proceedings.

[76]The reference goes to the *Engel* criteria developed by the Court to qualify the concept of "criminal offense". See *supra*, Ch. III, § 4.1. For an application of this reasoning in a case relevant for the protection against self-incriminations, see ECtHR, *J.B.*, cit., § 44-50.

[77]M. Berger, *Europeanizing Self-Incrimination*, cit., p. 351.

[78]See supra, Section 2. See also G. Caneschi, *La Corte di Gisutizia sul diritto al silenzio: un primo passo verso il "giusto procedimento" amministrativo punitivo*, in *Riv. it. Dir. Proc. Pen.*, 2021, 2, p. 581.

Therefore, it is not surprising that the provisions regulating the right to remain silent are mainly included in Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial (hereafter: the Presumption of Innocence Directive)[79], whose Art. 7 provides that «suspects and accused persons [shall] have the right to remain silent in relation to the criminal offence that they are suspected or accused of having committed».

The Presumption of Innocence Directive is one of the outputs achieved in the aftermath of the adoption of the Roadmap by the JHA Council in November 2009[80] and the Stockholm Program by the European Council[81], as a comprehensive action to promote the setting of common minimum standards on the procedural rights of suspected or accused persons in criminal proceedings[82]. Despite some initial disagreements about the actual necessity of an EU instrument or the legality of the Commission initiative[83], Directive (EU) 2016/343 was eventually adopted under the pressure of the Italian presidency, although the final version greatly differed from the proposal laid out by the Commission[84].

[79]Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016.

[80]Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings, OJ C 295, 4.12.2009, pp. 1–3.

[81]European Council, The Stockholm Programme — An open and secure Europe serving and protecting citizens, O.J. C 115, 4.5.2010, p. 1.

[82]Which, in turn, serves the baseline to achieve the ultima goal of fostering the application of the principle of mutual recognition.

[83]Ibid., p. 26. See also A. Pivaty, A. Beazley, Y. M Daly, L. Beckers, D. de Vocht, P. ter Vrugt, *Opening Pandora's box: The right to silence in police interrogations and the Directive 2016/343/EU*, in *New Journal of European Criminal Law*, 2021, 12(3), p. 331 ff. The Commission did not adequately justify the need for a directive on the presumption of innocence, being already protected by Art. 6(2) ECHR and at the domestic level. However, D. Sarmiento, *The April Revolution for European Human Rights Law*, 7 April 2018, available at https://despiteourdifferencesblog.wordpress.com/2018/04/17/the-april-revolution-for-european-human-rights-law/, notes that the added value of the Directive exactly lies in the fact that Member States will be under EU supervision when their criminal courts rule on how the accused is to be treated in the course of the proceedings, setting aside national standards that do not comply with EU law. Furthermore, the UK questioned the respect of the principle of subsidiarity by the Commission and therefore did not take part in the Directive.

[84]For an overview on the adoption of the Directive, see S. Cras, A. Erbežnik, *The Directive on the Presumption of Innocence and the Right to Be Present at Trial: Genesis and Description of the New EU Measure*, in *Eucrim*, 2016, 1, p. 25 ff; L. Camaldo, *Presunzione di innocenza*

Before addressing the content of the Presumption of Innocence Directive, which is «to a large extent, a codification of the case law of the ECtHR»[85], especially in relation to the right to silence, it should be underscored how peculiar the directive is compared to the other EU secondary instruments adopted pursuant to the Roadmap. While the other directives concern specific defendant's rights (*e.g.*, the right to information or to legal assistance), the Presumption of Innocence Directive focuses on general principles of criminal procedural law[86], such as the presumption of innocence, the burden of proof, the participation of accused persons in their own criminal proceedings, *in absentia* trials, and the right to silence[87], thus seeking a far-reaching legislative harmonization of human rights standards in criminal proceedings[88]. Moreover, with regard to the presumption of innocence, Directive (EU) 2016/343 does not limit its scope to setting either a general rule to be followed when assessing the guilt or innocence of defendants or a rule governing how defendants should be treated within the proceedings, but rather embraces both of them, in line with the twofold meaning traditionally attributed to it[89]. On the one hand, Art. 4 (Public references to guilt), Art. 5 (Presentation of suspects and accused persons), and Art. 7 (Right to remain silence) contribute to defining the rule of treatment that the criminal justice system should comply with in the course of criminal proceedings. The rationale, it is evident, is to prevent authorities from acting according to a preconceived idea and the accused from being treated as guilty before a definitive conviction is delivered[90]. Concerning the right

e diritto di partecipare al giudizio: due garanzie fondamentali del giusto processo in un'unica Direttiva dell'Unione europea, in *Dir. pen. cont.*, 23 March 2016; N. Canestrini, *La direttiva sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali. Un'introduzione*, in *Cass. pen*, 2016, 5, pp. 2214-2239.

[85]S. Cras, A. Erbežnik, *The Directive*, cit., p. 28.

[86]A. Pivaty, A. Beazley, Y. M Daly, L. Beckers, D. de Vocht, P. ter Vrugt, *Opening Pandora's box*, cit., p. 329

[87]Which, «[l]eaving the method of the defense in the hands of the defendant, is a manifestation of the subjective treatment of the defendant and of respect for his or her dignity». A. Sakowicz, *The Right to Silence in the EU Directive 2016/343 on the Strengthening of Certain Aspects of the Presumption of Innocence from the Perspective of Polish Criminal Proceedings*, in *Review of European and Comparative Law*, 2020, 41, p. 77.

[88]D. Sarmiento, *The April Revolution,* cit.

[89]M. L. Villamarín López, *The presumption of innocence in Directive 2016/343/EU of 9 March 2016*, in *ERA Forum*, 2017, 18, pp. 343-352.

[90]V. Manes, M. Caianiello, *Introduzione al diritto penale europeo: fonti, metodi, istituti,*

to silence and the privilege against self-incrimination, these safeguards guarantee the respect of the will of the suspect or the accused, by giving them the free choice not to contribute to their own incrimination.

On the other hand, Art. 6 Presumption of Innocence Directive sets a rule of judgment by placing the burden of proof for establishing the guilt on the prosecution, also providing that any doubt as to the question of guilt should be assessed to their benefit (*in dubio pro reo*). Admittedly, the right to silence and the privilege against self-incrimination also relate to the rule of judgment, insofar as forcing the suspect to provide information that might incriminate them or otherwise contribute to the case against them would equate a shift of the burden of proof on the defense.

According to Art. 2, the Presumption of Innocence Directive applies to *natural persons* who are suspects or accused persons in criminal proceedings. As explained in Recitals 13 and 14, the directive does not regard legal persons, as «the rights flowing from the presumption of innocence do not accrue to legal persons in the same way as they do to natural persons»[91]. The scope *ratione personae* of the directive is the result of a political compromise reached during the trilogue occurred between the co-legislators and the Commission, with the European Parliament calling for the inclusion of legal persons in the scope of the directive, and the Council and the Commission firmly opposing to it[92]. In addition to acknowledging that neither national laws nor national and international case law are developed enough to legislate at Union level on the presumption of innocence of legal persons[93], the EU lawmaker makes nevertheless clear that legal persons can benefit from existing safeguards and case law, namely in the ECHR as interpreted by the

casi, Turin, 2020, p. 253.

[91]Recital 13 Dir. (EU) 2016/343.

[92]As pointed out by S. Cras, A. Erbežnik, *The Directive*, cit., p. 28, the opposition of the Commission in particular is easily understandable in light of the powers it plays in competition matters, as will be seen in depth below.

[93]Although this point overlooks the fact, underlined by the European Parliament, that most domestic criminal justice systems have layed out provisions on corporate criminal liability. See S. Lamberigts, *The Directive on the Presumption of Innocence. A Missed Opportunity for Legal Persons?*, in *Eucrim*, 2016, 1, p. 37.

European Court of Human Rights and by the Court of Justice[94]. However, the reference to the jurisprudence of the Court of Strasbourg is out of keeping with the limited scope of the directive, in light of the fact that, although the European Court has never ruled on the application of the privilege against self-incrimination to legal persons, it has not excluded that companies may actually enjoy the rights enshrined in the Convention in general and in Art. 6 in particular[95].

All the more troubling is the reference to the safeguards already set out in the case law of the Court of Justice concerning the privilege of legal persons, and this is for several reasons. In the first place, only a few rulings on the interpretation of the Presumption of Innocence Directive have been delivered by the Court so far; thus, the majority of the decisions addressing the right to silence and the privilege against self-incrimination are drawn from the case law on competition proceedings between the European Commission and undertakings. Secondly, EU competition law proceedings are marked by broad investigation powers of the Commission and cooperation duties for the legal persons under investigation[96]. Yet, the Court of Justice has always been reluctant to recognize competition law as substantive criminal matter[97], despite the level of afflicting sanctions that might arise therefrom[98]. Third, the CJEU case law in antitrust matters concerns "undertakings", of which there is no clear legal definition. Therefore, although all the CJEU decisions in antritrust matters so far concern legal persons, natural persons can also qualify as undertakings, creating greater confusion as to the

[94]Recitals 14 and 15 Dir. (EU) 2016/343.

[95]ECtHR, *Menarini*, cit., ECtHR, Sec. II, 10 January 2006, *Teltronic-CATV v. Poland*, Appl. no. 48140/99, § 52 ff. Agrees to this view F. Mayer, *Duties to cooperate and their limits under the case law of the ECtHR and the ECJ*, in *European Integration Studies*, 2023, 19(2), p. 44. G. Lasagni, *Banking supervision*, cit., p. 249, notes how this would run counter to the homogeneity clause under Art. 52(3) CFREU by setting lower standards of protection for legal persons.

[96]M. Veenbrink, *The Privilege against Self-Incrimination in EU Competition Law: A Deafening Silence?*, in *Legal Issues of Economic Integration*, 2015, 42(2), p. 119.

[97]Cf. Judgment of 18 September 2003, *Volkswagen v. Commission*, C-338/00 P, ECLI:EU:C:2003:473; Judgment of 1 July 2007, *Compagnie maritime belge v. Commission*, T-276/04, ECLI:EU:T:2008:237.

[98]And despite the strikingly evident criminal nature that can be drawn from the *Engel* test developed by the Court of Strasbourg, as acknowledged in, *ex multis*, ECtHR, Sec. II, 27 September 2011, *A. Menarini Diagnostics Srl v. Italy*, Appl. No. 43509/08, § 44. See E. Amati, *Dinamiche evolutive del diritto al silenzio. Riflessi sul diritto punitivo e sugli obblighi di collaborazione con le autorità ispettive e di vigilanza*, Turin, 2022, p. 18.

rationale of having different regimes[99].

In its case law on antitrust matters, which is reflected in Regulation 1/2003[100], the Court has generally held that legal persons do not enjoy any right not to disclose the information requested by the Commission, as it would run counter to the useful effect of EU law[101]. Therefore, there is no absolute privilege against self-incrimination in competition law proceedings[102]. However, in those cases where the undertaking is obliged[103] to provide non-factual information entailing an admission of guilt or subjective assessments about the alleged fact, the privilege might be resorted to by the company under investigation, as the duty to assess the competition infringement belongs to the Commission[104]. Hence, the protec-

[99] A. DE VRIES, *Recent Developments Concerning the Right to Silence and Privilege Against Self-Incrimination Under the Charter of Fundamental Rights of the EU – A Critical Reflection on Case C-481/19 DB v Consob*, in *Review of European Administrative*, 2022, 15(1), p. 44. As explained by M. VEENBRINK, *The Privilege*, cit., p. 134, the Court adopts a functional definition, according to which an undertaking is «every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed» (Judgment of 23 April 1991, *Klaus Höfner and Fritz Elser v. Macrotron GmbH*, Case C-41/90, para. 21), including therein also the natural persons working in the company. As a consequence, they can enjoy a privilege against self-incrimination to the extent allowed by the Court.

[100] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4.1.2003.

[101] The leading case is judgment of 18 October 1989, *Orkem v. Commission*, C-374/87, ECLI:EU:C:1989:387, para. 34. It should be noted that the *Orkem* decision predated the *Funke* judgment of the European Court where Art. 6 ECHR was interpreted for the first time as to include the right to silence and the privilege against self-incrimination. However, the Luxembourg Court did not alter its case-law afterwards. See also judgment of 29 June 2006, *Commission v. SGL Carbon AG*, Case C-301/04 P, ECLI:EU:C:2006:432, para. 44-46; judgment of 20 February 2001, T-112/98, *Mannesmannröhren-Werke AG v. Commission*, ECLI:EU:T:2001:61, para. 65-66.

[102] L. GARZANITI, J. GUDOFSKY, J. MOFFAT, *Dawn of a New Era? Powers Of Investigation and Enforcement Under Regulation 1/2003*, in *Antitrust Law Journal*, 2004, 72(1), p. 175.

[103] Regulation (EC) 1/2003 under Art. 18 makes a distinction between requests for information and decisions requiring information, providing for a penalty not exceeding 1 per cent of the total turnover in the preceding business year for not supplying the required information in the latter case. It follows that an obligation to provide information only occurs in the latter case. Cf. M. VEENBRINK, *The Privilege*, cit. p. 129.

[104] Where, in other terms, the defence rights of the legal persons would be compromised. See judgment of T-112/98 *Mannesmannröhren-Werke v. Commission* [2001] ECR II-729, para. 66 and 67; judgment of 24 September 2009, *Erste Group Bank AG*, C-125/07, C-133/07 P, C-135/07 P, C-137/07 P, ECLI:EU:C:2009:576, para. 271; judgment of 25 January 2007, *Dalmine*, C-407/04 P, ECLI:EU:C:2007:53, para. 34; *SGL Carbon AG*, cit., para. 42. This case law was transposed into Recital 23 Reg. (EC) 1/2003, but does not cease to sound confusing as it seems difficult in practice to distinguish between admissible factual questions and prohibited requests

tion afforded by the privilege against self-incrimination in competition law appears particularly limited, as it only convers unsolicited admissions of autorship or participation in an infringement[105]. Against this backdrop, no matter how convincing the arguments supporting the differentiation between legal and natural persons when it comes to the enjoyment of the right to remain silent[106], the approach adopted by the Presumption of Innocence Directive is particularly restrictive and appearently flawed, since it justifies the exclusion of legal persons from its scope on the basis of a different policy field which does not require levels of protection as high as those mandated by criminal law. In sum, it is not convincing that «limitations in non-criminal fields of law [are] used as a model to define the standard of protection for defendant in criminal proceedings»[107].

As far as the material scope of application is concerned, Art. 2 Presumption of Innocence Directive states that it applies to "criminal proceedings", and Recital 11 clarifies that it does not apply to «civil proceedings or to administrative proceedings, including where the latter can lead to sanctions, such as proceedings relating to competition, trade, financial services, road traffic, tax or tax surcharges, and investigations by administrative authorities in relation to such proceedings». However, the same Recital holds, quite inconsistently, that the autonomous interpretation provided by the Court of Justice should be employed to define the scope of the Directive, «without prejudice to the case-law of the European Court of Human Right»[108]. Although the reference to the substantial approach adopted

that might entail admission of guilt, as noted by S. Lamberigts, *The Directive*, cit., p. 40; G. Lasagni, *Prendendo sul serio il diritto al silenzio: commento a Corte cost., ord. 10 maggio 2019, n. 117*, in *Dir. Pen. Cont.*, 2020, 2, p. 145. Similarly, F. Mayer, *Duties to cooperate* cit., p. 50.

[105]H. P. Nehl, *Article 48 (Administrative Law)*, in S. Peers-T. Hervey-J. Kenner-A. Ward, *The EU Charter*, cit., p. 1294, who is furthermore skeptical about a reconsideration of the jurisprudence in line with the ECtHR case law in light of the entering into force of the Charter of Fundamental Rights and the equivalence clause under Art. 52(3) therin as of December 2009. The case *DB v. Consob* that will be analyzed in detail below shows how such a change has not occurred yet.

[106]For an overview of the different rationales supporting the exclusion of legal persons from the scope of the right to silence and the privilege against-self incrimination, see extensively S. Lamberigts, *The Privilege*, cit., p. 434-437.

[107]G. Lasagni, *Banking Supervision*, cit., p. 249.

[108]Also in this case, a political compromise was reached in the negotiations, having the European Parliament asked that punitive proceedings be inserted in the scope *ratione materiae*

by the European Courts was eventually inserted in the non-binding part of the text, the limitation to criminal proceedings appears to be void[109] if not unfortunate. In fact, the Court of Justice has shown so far to have familiarized itself with a substantive approach to the notion of criminal charge and criminal proceedings under the influence of the ECtHR case law, to the point that a change of course and thus a lowering of safeguards in such a delicate field would seem implausible[110]. Of particular relevance for our purposes is the case law on insider dealing proceedings, since the Court of Justice has been in favour of recognizing the criminal nature of certain administrative sanctions applied in market abuse cases, with the consequence of broadening the application of procedural safeguards such as the *ne bis in idem* or the non retroactivity of penalties[111]. In a recent judgment concerning the right to remain silence in the context of insider dealing proceedings, the Court acknowledged and addressed the need to build a due process system that may go beyond the field of criminal law *stricu sensu*. The decision[112] originated from an Italian national proceeding whereby the supervisory national

---

or, at least, that an express reference to the Engel criteria be formulated. See S. Cras, A. Erbežnik, *The Directive*, cit., p. 29.

[109]V. Manes, M. Caianiello, *Introduzione*, cit., p. 255.

[110]The substantive approach adopted by the Court appears starting at least from Judgment of 5 June 2012, *Łukasz Marcin Bonda*, C-489/10, ECLI:EU:C:2012:319, para. 42-71 concerning administrative penalties laid down in pursuance of the objectives of the common agricultural policy. See also Judgment of 26 February 2013, *Åklagaren v. Hans Åkerberg Fransson*, C-617/10, ECLI:EU:C:2013:105 para 35. In the literature, see G. Lasagni, *Banking Supervision*, cit., p. 27 ff.

[111]See Judgment of 20 March 2018, *Enzo Di Puma v. Consob and Consob v. Antonio Zecca.*, joined cases C-596/16 and C-597/16, ECLI:EU:C:2018:192; Judgment of 20 March 2018, *Garlsson Real Estate and Others*, C-537/16, ECLI:EU:C:2018:193; Judgment of 20 March 2018, *Menci*, C-524/14, ECLI:EU:C:2018:197.

[112]Judgment of 2 February 2021, *DB v. Consob*, C-481/19, ECLI:EU:C:2021:84. In the aftermath of the ruling, several scholars have commented it. Among the others, please refer to M. Veenbrink, *The Freedom from Self-Incrimination — A Strasbourg-Proof Approach? Cases C-466/19 P Qualcomm and C-481/19 P DB v Consob*, in *Journal of European Competition Law and Practice*, 12(10), pp. 750-752; L. Lonardo, *The Veiled Irreverence of the Italian Constitutional Court and the Contours of the Right to Silence for Natural Persons in Administrative Proceedings - Judgment of the Court (Grand Chamber) 2 February 2021, Case C-481/19 DB v Consob, ECLI:EU:C:2021:84*, in *European Constitutional Law Review*, 2021, 17(4), pp. 707-723; E. Hancox, *The right to remain silent in EU Law*, in *Cambridge Law Journal*, 80(2), pp. 228-231; M. Aranci, *Diritto al silenzio e illecito amministrativo punitivo: la risposta della Corte di giustizia*, in *Sist. pen.*, 2021, 2, p. 73 ff.

authority *Commissione Nazionale per le Società e la Borsa* (hereinafter Consob), on the basis of Art. 187-*bis* D.Lgs. n. 58 of 1998, imposed on *DB* two financial penalties for insider dealing and the unlawful disclosure of inside information. In addition, it imposed a financial penalty for the administrative offence under Article 187-*quinquiesdecies* for postponing the scheduled interview requested by the authority and therefore failing to comply with Consob's requests within the time limits and delaying Consob in the performance of its functions. In challenging the constitutionality of the provision sanctioning the non-collaboration, the Court of Cassation referred the case to the Italian Constitutional Court which, noting that Art. 187-*quinquiesdecies* was introduced into the Italian legal system in performance of a specific obligation under Article 14(3) of Directive 2003/6[113], decided to stand the proceedings and refer two preliminary rulings for the interpretation and validity of the provisions. The Court of Justice, in adhering to the reasoning of the referring court[114], interpreted the EU law provision in the sense that it does not obligate Member States to penalise natural persons who refuse to provide the competent authority with answers that might be used to establish their criminal liability or their liability for an offence that is punished by administrative sanctions of a criminal nature[115].

The case *DB v. Commission* represents an interesting decision and a turning point for several reasons[116].

[113]Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation, OJ L 96, 12.4.2003, now repealed by Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse, OJ L 173, 12.06.2014.

[114]In the words of L. Lonardo, *The Veiled Irreverence*, cit., p. 709, «[t]he order did not merely set out a reasoning, it also drew the conclusion».

[115]The Court of Justice did not go on to examine the validity of the provisions as requested by the referring court, as it provided an interpretation which is consistent with Articles 47 and 48 of the Charter, in that they do not expressely require Member States to sanction natural persons for refusing to cooperate in non-punitive proceedings. *DB v. Consob*, cit., para. 49-56.

[116]For instance, from the perspective of EU market abuse scholars, it pointed at the lack of procedural safeguards in this field. See H. Andersson, *Fighting insider dealing at all costs?— due process aspects on the EU market abuse regime*, in *Capital Markets Law Journal*, 2022, 17(2), p. 209. It is also an example of a virtuous dialogue between national courts and the Court of Justice, as the preliminary request was forwarded by the Italian Constitutional Court, in line with what had already occurred in the Taricco saga (on which, extensively, A. Bernardi-C. Cupelli (eds), *Il caso Taricco e il dialogo tra Corti. L'ordinanza 24/2017 della Corte costituzionale*,

However, three points are particularly relevant for our purposes. In the first place, the Court of Justice reiterates the aforementioned case law on the substantive criminal nature of market abuse proceedings, according to which «some of the administrative sanctions imposed by Consob appear to pursue a punitive purpose and to present a high degree of severity such that they are liable to be regarded as being criminal in nature»[117], whose assessment is carried out by the Court in light of the three criteria of legal classification, nature, and severity of penalties recalling the Engel criteria[118].

Secondly, as far as the right to silence is concerned, the Court addresses the issue by meticulously following the case law of the Court of Strasbourg[119]. Blatantly departing from its rulings in competition matters, it therefore states that the privilege applies when statements or material evidence are obtained under threat of sanctions or sanctions are enforced for the refusal to testify, and that it cannot be limited to admissions of guilt but shall also cover information on questions of fact which may subsequently be used in support of the prosecution and may thus have a bearing on the conviction or the penalty imposed[120].

Third, the Court moves its reasoning a step forward, by holding that the substantial criminal nature of administrative proceedings is not the only parameter to find whether the compulsion was indeed "improper". Instead, it maintains that the right against self-incrimination shall be respected also in those non-punitive

Naples, 2017), which furthermore rightly applied the pinciple of "doppia pregiudizialità". See L. Cattelan, *Corte di Giustizia e principio del nemo tenetur se detegere: risvolti in tema di doppia pregiudizialità*, in *IUS Penale*, 15 March 2021; N. Recchia, *Il rinvio pregiudiziale alla Corte di Giustizia in materia penale ovvero della doppia pregiudizialità* in action, in *Riv. it. dir. proc. pen.*, 4, p. 1445 ff. See also C. Amalfitano, *Il dialogo tra Giudice comune, Corte di giustizia e Corte costituzionale dopo l'obiter dictum della sentenza n. 269/2017*, in *Osservatorio sulle fonti*, 2019, 2, p. 21.

[117] *DB v. Consob*, cit., para. 43.

[118] *Ibid.*, 42

[119] Since, by virtue of Art. 52(3) CFREU, «the second paragraph of Article 47 of the Charter corresponds to Article 6(1) of the ECHR and Article 48 of the Charter is 'the same' as Article 6(2) and (3) of the ECHR. When interpreting the rights guaranteed by the second paragraph of Article 47 and of Article 48 of the Charter, the Court must, therefore, take account of the corresponding rights guaranteed by Article 6 of the ECHR, as interpreted by the European Court of Human Rights, as the minimum threshold of protection». *DB v. Consob*, cit., para. 37.

[120] *Ibid.*, para. 40. Cf. A. Camon, *La disciplina costituzionale*, in A. Camon-M. Daniele-D. Negri-C. Cesari-M.L. Di Bitonto-P.P. Paulesu, *Fondamenti*, cit., p. 150.

administrative proceedings[121] insofar as the evidence collected therein «may be used in criminal proceedings against that person in order to establish that a criminal offence was committed»[122]. In so doing, the Court recalls the case-law of the Court of Strasbourg, according to which one of the three criteria to be taken into account in order to assess the nature and degree of the compulsion, and therefore the occurred violation of Art. 6 ECHR, is «the use to which evidence obtained under compulsion is put»[123].

In other words, insofar as evidence collected outside criminal proceedings is intended to be used in a subsequent criminal trial, because national legislation so allows or in accordance of the common pracitce of national authorities to exchange information[124], the *nemo tenetur* principle must be respected and procedural safeguards be put in place to prevent the violation of the privilege[125].

The article then specifies the scope *ratione temporis*, since the privilege covers «all stages of the criminal proceedings, from the moment when a person is suspected or accused of having committed a criminal offence, or an alleged criminal offence, until the decision on the final determination of whether that person has committed the criminal offence concerned has become definitive. The choice to enable the guarantees stemming from the directive at an early stage and even before the person is made aware, by official notification or otherwise, of being suspected or accused of a crime was welcomed by scholars, although the lack of a

[121]The Court does not resort to the punititve/non-punitive distinction, although it would appear more appropriate, as noted by A. DE VRIES, *Recent Developments*, cit., p. 39.

[122]*Ibid.*, para. 44.

[123]ECtHR, *Ibrahim and Others*, cit., § 269.

[124]G. CANESCHI, *La Corte di Gisutizia*, cit., p. 587, notes that the Court of Justice implies in its decision that, as suggested by the referring court, the Italian legal system allows the use in criminal proceedings of evidence collected outside of it without the necessary procedural safeguards. However, this is not allowed and Art. 220 D.lgs. 28 luglio 1989, n. 271 (*Implementing provisions of the CCP*) must be respected. What the Italian Constitutional Court referred to was rather the possibility that, in light of the double-track enforcement regime on insider trading, material gathered in non-punititve proceedings might concretely provide investigative leads to the judicial authorities. See Const. Court, order of 10 May 2019, n. 117, in *Cass. pen.*, 2019, p. 3228.

[125]Such safeguards can be proactive, *i.e.* implemented in the course of the non-punitive proceedings, or reactive, meaning that they should occur after the improper compulsion has been exerted in order to restrcit the use of that self-incriminating material. See A. DE VRIES, *Recent Developments*, cit., p. 40.

reference to the position of those who are interrogated by the police as witnesses and charged at a later stage has been critized[126].

Having outlined the scope of application and the aspects touched on by the directive, we should now address the provisions specifically concerning the right to remain silent. To start with, Recital 24 clarifies the reason why they are included in the Presumption of Innocence Directive, that is, because the right to silence «is an important aspect of the presumption of innocence»[127]. Art. 7 further elaborates on this, stating that Member States shall ensure that suspects and accused persons have the right to remain silent in relation to the criminal offence that they are suspected or accused of having committed, as well as the right not to incriminate themselves[128]. The following paragraph clarifies the material scope of the rights in comment, admittedly limiting it by excluding «evidence which may be lawfully obtained through the use of legal powers of compulsion and which has an existence independent of the will of the suspects or accused persons»[129]. This wording resonates, as it indeed follows the case law developed by the Court of Strasbourg and should therefore be interpreted accordingly[130].

However, the directive is as confusing as the decisions of the European Court, insofar as it appears to prohibit authorities from forcing suspects to «*produce evidence or documents* or to provide information which may lead to self-incrimination»[131] in Recital 25[132], while at the same time it paves the way for cooperation duties in the production of material evidence «such as material acquired pursuant to a

[126]A. Pivaty, A. Beazley, Y. M Daly, L. Beckers, D. de Vocht, P. ter Vrugt, *Opening Pandora's box:*, cit., p. 333; J. Della Torre, *Il Paradosso della Direttiva sul Rafforzamento della Presunzione di Innocenza e del Diritto di Presenziare al Processo: Un Passo Indietro Rispetto alle Garanzie Convenzionali?*, in *Riv. it. dir. proc. pen.*, 2016, 4, p. 1850.

[127]Recital 25 Dir. (EU) 2016/343 reiterates the same for the privilege against self-incrimination.

[128]Art. 7(1) and (2) Dir. (EU) 2016/343.

[129]Art. 7(3) Dir. (EU) 2016/343.

[130]Cf. Recital 27 according to which «[i]n order to determine whether the right to remain silent or the right not to incriminate oneself has been violated, the interpretation by the European Court of Human Rights of the right to a fair trial under the ECHR should be taken into account».

[131]Emphasis added.

[132]Thus adopting the "suspect-friendly approach" followed by the European Court in its early judgments ECtHR, *Funke*, cit. and *J.B.*, cit. See S. Lamberigts, *The Privilege*, cit., p. 433. See also G. Caneschi, *La Corte di Gisutizia*, cit., p. 583, ft. 60.

warrant, material in respect of which there is a legal obligation of retention and production upon request, breath, blood or urine samples and bodily tissue for the purpose of DNA testing»[133]. However, the lack of reference in the text to sanctions for those who refuse to hand over self-incriminating documents suggests that the Presumption of Innocence Directive should allow them to exercise their rights also in those circumstances[134].

From the wording of Art. 7(3), read together with the recitals, the aforementioned case law of the Court of Justice in competition metters emerges once again, showing that not only the ECtHR doctrine but also the CJEU rulings in competition law matters exerted an influence on the provisions on documentary evidence. The attention that the Court of Luxembourg paid to the effectiveness of antitrust enforcement has resulted in a narrow privilege against self-incrimination, which excludes documentary evidence from its scope of application in line with the restrictive approach adopted by the Court of Strasbourg in *Saunders*[135]. This conclusion was reached and upheld despite the fact that in the day-to-day business activity «documents constitute an important category of evidence for the enforcement of (Union) financial-economic policies»[136] and is supported by the claim that the undertaking is nonetheless free to show, «whether later during the administrative procedure or in proceedings before the European Union judicature, that the facts set out in its replies or the documents produced by it have a different meaning from that ascribed to them by the Commission»[137].

Against this backdrop, it appears that the EU lawmaker referred to the case law developed by the Court of Justice in competition matters and acritically transposed it into the Presumption of Innocence Directive dealing with criminal

[133]Recital 29 Dir. (EU) 2016/343. Whether such a list is exhaustive or not is unclear, as noted by A. Pivaty, A. Beazley, Y. M Daly, L. Beckers, D. de Vocht, P. ter Vrugt, *Opening Pandora's box*, cit., p. 339.

[134]G. Lasagni, *Prendendo sul serio*, cit., p. 153.

[135]Among the others, see judgment of 14 March 2014, *Buzzi Unicem SpA v. Commission*, Case T-297/11, ECLI:EU:T:2014:122; *Commission v. SGL Carbon AG*, cit., para. 41. More recently, judgment of 28 January of 2021, *Qualcomm v. Commission*, C-466/19 P, ECLI:EU:C:2021:76, para. 143.

[136]A. de Vries, *Recent Developments*, cit., p. 42.

[137]*Buzzi*, cit., para. 62.

matters[138] without considering that criminal proceedings require higher standards of protection. It has also been noted that the different general interests underpinning criminal proceedings on the one hand and competition proceedings on the other might have justified different approaches to the extent of the privilege[139].

Focusing on the regulation of adverse inferences from silence, that the Court of Strasbourg considers admissible to a certain extent[140], the EU Directive appearently ensures a stronger protection insofar as it provides that «[t]he exercise by suspects and accused persons of the right to remain silent or of the right not to incriminate oneself shall not be used against them and shall not be considered to be evidence that they have committed the criminal offence concerned»[141]. However, while some scholars claim that the EU lawmaker intended to render the right absolute[142], doubts arise when the provision is read together with the fourth paragraph, which does not rule out for judicial authorities to take into account the cooperative behaviors of defendants when sentencing, and with Recital 28 according to which silence should not, *in itself*, be considered to be evidence of guilt[143].

Furthermore, the recital makes it clear that the prohibition on the use of silence as evidence «should be without prejudice» to national rules on the assessment of evidence, thus potentially paving the way for lower standards of protection[144].

[138] S. Lamberigts, *The Privilege*, cit., p. 435.

[139] M. Veenbrink, *The Privilege*, cit., p. 140.

[140] *Supra* Section 2.1. See ECtHR, *John Murray*, cit.

[141] Art. 7(5) Dir. (EU) 2016/343.

[142] M. L. Villamarín López, *The Presumption of Innocence*, cit., p. 349.

[143] The words in itself seems to equate the provision to the case law of the Court of Strasbourg, which only prohibits the use of silence as the sole and main evidence of guilt. In other terms, this suggests that the Presumption of Innocence Directive allows remaining silent to be used as a corroboration of evidence. See A. Pivaty, A. Beazley, Y. M Daly, L. Beckers, D. de Vocht, P. ter Vrugt, *Opening Pandora's box*, cit., p. 336. The same doubts are expressed by S. Cras, A. Erbežnik, *The Directive on the Presumption of Innocence*, cit., p. 32; O. Mazza, *Presunzione di innocenza e diritto di difesa*, in *Dir. pen. proc.*, 2014, 12 p. 1401; J. Della Torre, *Il Paradosso*, cit., p. 1863.

[144] J. Della Torre, *Il Paradosso*, cit., p. 1863. The comparative analysis conducted by A. Pivaty, A. Beazley, Y. M Daly, D. de Vocht, P. ter Vrugt, *Strengthening the protection of the right to remain silent at the investigative stage: What role for the EU legislator?*, in *New Journal of European Criminal Law*, 2021, 12(3), p. 434 ff., shows that national courts, in different ways, do already draw negative consequences from the silence of defendants. Whether these practices are compliant or not with the directive will depend on the interpretation given

The reference to the national rules concerning the admissibility of evidence is also present in Art. 10 on remedies. Specifically, the article, after providing that Member States shall implement effective remedies in the event of a breach of the rights set out in the directive, warns that «in the assessment of statements made by suspects or accused persons or of evidence obtained in breach of the right to remain silent or the right not to incriminate oneself» according to the national rules and systems on the admissibility of evidence, the rights of the defence and the fairness of the proceedings must be respected.

Once again, the negotiations that occurred between the European Parliament and the Council with the assistance of the Commission provided proof of delivering milder steps than those advanced in the Commission proposal toward a system promoting minimum stronger procedural safeguards, which, however, does not surprise since «(full) harmonisation seems to imply the need to restructure national criminal procedure systems, which goes beyond the EU mandate»[145]. In fact, the Commission had envisaged the inadmissibility of any evidence obtained in breach of the right to remain silent and the right to self-incrimination[146], which was later enhanced by the European Parliament by ruling out any references to the "overall fairness of the proceedings"[147]. This, according to Art. 10 of the proposal, would have had the effect of «placing suspects or accused persons in the same position in which they would have found themselves had the breach not occurred»[148].

However, any reference to exclusionary rules was ultimately deleted from the

by the Court of Luxembourg of such confusing provisions.

[145]A. Pivaty, A. Beazley, Y. M Daly, L. Beckers, D. de Vocht, P. ter Vrugt, *Opening Pandora's box*, cit., p. 341.

[146]See Artt. 6 and 7 Proposal for a Directive of the European Parliament and of the Council on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceedings, COM/2013/0821 final.

[147]See S. Cras, A. Erbežnik, *The Directive*, cit., p. 34.

[148]The ECtHR had previously held in its case law that «the most appropriate form of redress for a violation of Article 6 § 1 would be to ensure that the applicant, as far as possible, is put in the position in which he would have been had this provision not been disregarded». See ECtHR [GC], 27 November 2008, *Salduz v. Turkey*, Appl. No 36391/02, § 72.

final version of the directive[149], and a reference to national systems was included in the provision on remedies, thus suggesting that «it does not clearly impose on Member States the obligation to exclude evidence obtained in violation of the right to remain silent or the right not to incriminate oneself»[150].

By ruling out the inadmissibility rule of evidence obtained in defiance of the right against self-incrimination and the right to silence, the right to an effective remedy as granted by the directive is rendered rather difficult to invoke as it is not clear what this remedy might be [151], while also leading to asymmetries in standards of protection between Member States[152].

In conclusion, the overall picture stemming from the regulation of the *nemo tenetur* principle depicted in the directive is that of a weak attempt to provide minimum standards across Member States, marked by evident omissions[153] and confusing provisions, possibly leading to lower levels of protection despite the non-regression clause under Art. 13, according to which the directive should not be interpreted as «limiting or derogating from any of the rights and procedural safeguards that are ensured under the Charter, the ECHR, or other relevant provisions of international law or the law of any Member State that provides a higher level of protection».

[149]Due to the firm opposition of the Council that deemed it incompatible with the objectives of Art. 82(2) TFEU and with the differences across ntional systems as to rules on admissibility of evidence. Ibid.

[150]A. Sakowicz, *The Right to Silence*, cit., p. 67.

[151]P. Wiliński, K. Kiejnich-Kruk, *Right to Effective Legal Remedy in Criminal Proceedings in the EU. Implementation and Need for Standards*, in *Review of European and Comparative Law*, 2023, 54(3), p. 162.

[152]A. Sakowicz, *The Right to Silence*, cit., p. 78.

[153]For instance, A. Pivaty, A. Beazley, Y. M Daly, L. Beckers, D. de Vocht, P. ter Vrugt, *Opening Pandora's box*, cit., p. 333, note that it is not clearly stated whether Art. 7 Dir. (EU) 2016/343 applies in pre-trial police investigations.

4 The privilege against self-incrimination in the context of financial investigations: an intricate playing field

Drawing from the framework depicted above on the protection of the privilege against self-incrimination and the right to silence at the international level, the question of whether and to what extent these are envisaged in the context of financial investigations analyzed in Chapter I should be addressed in the following. As was clarified in the first part of the present research, there is no clear definition of financial investigation in hard law, nor has it been tackled in the jurisprudence. In general terms, in line with their two-fold purpose, we defined financial investigations as «an enquiry into the financial affairs allegedly related to a criminal activity with a view to prevent the abuse of the financial and banking system for illicit purposes or support the prosecution of money laundering, terrorism financing, and predicate offences, for the purpose of gathering evidence or removing assets for future confiscation»[154]. It follows that the field in which financial investigations are mainly performed is that of, but not limited to, money laundering, its predicate offences, and terrorism financing. We also attempted to show, as already underlined at the academic level, how blurred the dividing lines between prevention and repression of crime are when it comes to the procedural measures dealing with acts of money laundering or terrorism financing, insofar as the criminal justice system benefits from the structures, extensive experience in financial analysis and capacity to exchange information developed by the authorities involved in the preventive system[155]. Attention was paid in particular

[154]See *supra*, Chap. I, p. 16.

[155]As observed by J. A. Vervaele, *Economic crimes and money laundering: a new paradigm for the criminal justice system?*, in B. Unger-D. van der Linde (eds), *Research Handbook on Money Laundering*, Cheltenham-Northampton, 2013, p. 392, «[i]n many countries, within the criminal procedure, alongside judicial investigation, a special track of financial investigation has been created, with measures aimed at identifying, following, freezing, seizing and confiscating the assets of the suspect and/or convicted. The monitoring and freezing of bank transactions has become common and bank secrecy has lost much of its shielding capacity in criminal matters. For financial investigations, the thresholds are flexible and most of the measures can be executed

to the Financial Intelligence Units, which constitute the «bone structure» of the AML regime [156], and to their pivotal role in playing a function of connection and filter in the regulatory financial system between private companies and judicial authorities. The duty of obliged entities to report any suspicion transaction to their national FIU, which shall be convered by «effective, proportionate and dissuasive» sanctions or measures[157], can therefore turn into a tool that investigative authorities indirectly have at their disposal to detect criminal conducts or, in a more alarming scenario, to discover symptomatic anomalies that do not equate suspicion of criminal activity according to criminal procedure rules[158][159]. In this sense, administrative procedures are drawn into the criminal justice realm, as the use of intelligence by law enforcement authorities is considered the best approach to economic crimes[160].

---

by the prosecutor and/or financial experts in the police, without any prior or *a posteriori* judicial authorization». The Author, however, refers to what he calls «the new judicial track on financial investigations», alongside classic judicial investigative activities such as search and seizure and witness interrogation, which is therefore conducted by «specialized branches of financial auditing within the Prosecutor's office, with highly specialized personnel». As much as significant this development is for criminal proceedings in terms of effectiveness and also in terms of risks for fundamental rights, what the research is focusing on is the use of the preventive system for repressive purposes.

[156]S. Allegrezza, G. Bruzzese, *Supervision and Enforcement of EU's Anti-Money-Laundering and Countering the Financing of Terrorism*, in F. Annunziata-M. Siri, (eds), *EU Banking and Capital Markets Regulation Open Issues of Vertical Interplay with National Law*, Cham, 2025, p. 492.

[157]Artt. 33, 34, 35 and 58 Dir. (EU) 2015/849. Cf. Artt. 22, 23, 24 and 53 Dir. (EU) 2024/1640 for the provisions that will be implemented by 10 July 2027.

[158]While abnormality is one of the essential factors of financial surveillance both for reporting entities and FIUs, it is not a clear-cut concept and bears a high degree of subjectivity even among different obliged entities. On this point, see A. Amicelle, V. Iafolla, *Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing*, in *The British Journal of Criminlogy*, 2018, 58(4), p. 850 ff.

[159]As it will discussed in Chapter III, Sec. 3, this effect is exacerbated in the context of Public-Private Partnerships (PPPs) for information sharing, as the informal and undisclosed environment they promote between the members would facilitate a free-flowing of information.

[160]P. de Koster, M. Penna, *The case of money laundering. Real administrative procedure used in the detection of fraudulent transactions*, in F. Galli-A. Weyembergh, *Do labels still matter? Blurring boundaries between administrative and criminal law. The influence of the EU*, Brussels, 2014, pp. 69-81. As neatly claimed by A. Amicelle, V. Iafolla, *Suspicion-in-the-making*, cit., p. 846, «the fight against money laundering and terrorist financing provides the paradigmatic example of how suspicious activity reporting can become the backbone of policing practices».

However, while intelligence and smooth procedures undoubtedly represent an asset in boosting criminal investigations against money laundering and terrorism financing allegations, it cannot be neglected that consideration of the procedural safeguards that should be in place in these cases is lacking. In fact, if we assume that customers' profiles and information are surveilled by obliged entities they engage with for personal and business activities, and eventually passed on to the FIU if deemed suspicious; if we also assume, in light of the powers granted to them by EU law provisions, that FIUs can, on their own initiative, share information with obliged entities and ask them to dig further into targeted bank accounts[161] to provide data that can be passed on to the judicial authorities, then it is only consequential that targeted individuals should be recognized with adequate procedural safeguards. As pointed out in the introduction to this research, the security or securitarian logic entailed a shift from repression to prevention of risks, with the right to security, «which does not exist in human rights, but which is invented»[162], prevailing over the due process of law. Whilst policy fields exist that are perceived as delicate and more compelling than others in terms of ensuring the safety of citizens and society as a whole, with the consequence of devaluating the protection of fundamental human rights such that they are sometimes denied[163], it cannot be tantamount to denying their absolute nature. In fact, although acknowledging that fair trial rights are not indeed absolute, insofar as they can be subject to limitations and exceptions[164], it still urges one to tackle the gray zone

[161]As already mentioned in the first chapter, FIUs can ask obliged entities to provide information regardless of the prior submission of a suspicious transaction report. Cf. Art. 33(1), lett. b) Dir. (EU) 2015/849 and Art. 69(1), lett. b) Reg. (EU) 2025/1624.

[162]J. A. Vervaele, *Economic crimes*, cit., p. 393.

[163]In this sense, a paradigmatic example is that of judgment of 26 June 2007, *Ordre des barreaux francophones et germanophone*, Case C-305/05, ECLI:EU:C:2007:383, para. 33, specifically concerning the legal privilege of lawyers-clients relationship and the alleged violation of the right to a fair trial in light of the reporting obligations imposed on lawyers, in which the Court of Justice held that «[a]s a rule, the nature of such activities is such that they take place in a context with no link to judicial proceedings and, consequently, those activities fall outside the scope of the right to a fair trial». See M. Van Den Broek, H. Addink, *Prevention of Money Laundering and Terrorist Financing from a Good Governance Perspective*, in B. Unger-D. Van Der Linde (eds), *Research Handbook on Money Laundering*, cit., p. 374, who frame the issue of the effective balance between opposing interests within the broader issue of good governance.

[164]Differently from other rights such as the prohibition of torture and degrading or inhumane

that persists in financial investigations in order to envisage proper safeguards that protect human rights, however restricted.

The reason behind the choice to conduct such an assessment against the backdrop of the privilege against self-incrimination, which, as extensively outlined above, represents the essence of fair trial, is threefold. First, the protection afforded by the privilege possibly comes into play in the context of the four types of financial investigations identified in the first chapter[165], which include access to bank accounts and banking information; access to past banking transactions; real-time monitoring of banking transactions, and postponement and freezing of bank accounts. In each of these hypotesis, obliged entities bear a duty to cooperate with Financial Intelligence Units by virtue of the AML/CTF preventive legislation pursuant to which they are either required to provide information on bank accounts and specific operations of which they already are in possession, or to collect and provide information about transactions conducted through a specific account, as in the case of real-time monitoring. This data would then be transferred to the competent judicial authorities to initiate a criminal investigation if suspicions of crime are substantiated, without prejudice to the imposition of pecuniary sanctions or the application of administrative measures either by the FIUs themselves, if these have been granted such powers within their national legal frameworks, or by the national supervisory authorities[166]. Ostensibly, the duties to cooperate set

---

treatment.

[165] As noted by M. Simonato, M. Lassalle, *A fragmented approach to asset recovery and financial investigations: a threat to effective international judicial cooperation?*, in Z. Durdevic-E. Ivicevic Karas (eds), *European Criminal Procedure Law in Service of Protection of European Union Financial Interests: State of Play and Challenges*, 2016, p. 150, all four typologies of financial investigations represent a possible infringement of other fundamental rights, such as the right to privacy under Art. 8 ECHR. This specific aspect will be dealt with in Chapter IV.

[166] While Directive (EU) 2015/849 did not provide much details on sanctioning powers, Art 53 Dir. (EU) 2024/1624 specifies that sanctions can be imposed directly by the supervisors, in cooperation with or by delegation to other authorities, or with the involvement of competent judicial authorities. In the Italian legal framework, the UIF is required under Art. 6, para. 4, lett. g) D. Lgs. n. 231/2007 to transmit any breach of reporting duties to the Bank of Italy, which is the competent authority for AML/CFT supervision of banking and financial intermediaries (*e.g.*, credit institutions, investment firms, asset management companies). According to Art. 62, para. 7 D.lgs. n. 231/ 2007, the Bank of Italy is empowered to impose pecuniary sanctions over supervised obliged entities which do not comply with their AML/CTF duties (see P. Fratangelo, *Prevention and Countering of Money Laundering and Terrorism Financing*, in

out in the AML/CTF legislation create tension with the right of obliged entities not to contribute to their own possible incrimination, which should not only be ensured in the context of *punitive* proceedings, but also insofar as «the evidence obtained in those proceedings may be used in criminal proceedings against that person in order to establish that a criminal offence was committed»[167].

In line with the ECtHR case law, especially in financial-law matters, this is even more clear when one considers the pecuniary sanctions that might stem from the refusal to collaborate with the authorities, since the threat of sanctions for non-compliance would constitute a form of improper compulsion contrary to the right against self-incrimination[168]. In this sense, the already mentioned *DB* case of the Court of Justice shows how the latter has adhered to the case law of the Court of Strasbourg, recognizing that the imposition of penalties to anyone who fails to comply with the requests of supervisory authorities in a timely manner or delays their performance, and refuse to provide those authorities with answers that are capable of establishing their liability for an offence that is punishable by administrative sanctions of a criminal nature, or their criminal liability, represents an improper coercion that runs counter to the right to remain silent and the privilege against self-incrimination of the subject under investigation[169]. In light of the penetrating powers that are attributed to national supervisors within the AML/CTF preventive legal framework, the risk of infringing the right not to contribute to one's own incrimination is higher, especially when no reference to

---

D. Siclari (ed.), *Italian Banking and Financial Law. Vol I, Supervisory Authorities and Supervision*, Houndmills, 2015, pp. 105-133, for an overview of supervisory and sanctioning powers of the Bank of Italy in the AML/CTF field, that the Bank of Italy retained even after the establishment of the Single Supervisory Mechanism with Council Regulation no. 1024/2013).

[167] *DB*, cit., para 44.

[168] See *e.g.* ECtHR, *J.B.*, cit., §§ 65 ff., where the Court found that the action of the Swiss tax authorities to attempt to compel the applicant by means of the imposition of pecuniary fines to submit all documents concerning the companies in which he had invested money, amounted to a breach of the privilege agaisnt self-incrimination under Art. 6 ECHR; similarly, ECtHR, *Chambaz*, cit., § 53. More recently, ECtHR, *De Legé*, cit., §§ 69 ff.

[169] See *DB*, cit., para. 45. Notably, the case referred to the Court by the Italian Constitutional Court involved Art. 187-*quinquiesdecies* D.lgs. n. 58/1998, which applies to the requests made by the Bank of Italy in the performance of its supervisory functions over financial intermediaries. Therefore, it follows that it also refers to cases whereby the obligation to report suspicious transaction is violated, which are detected either by the supervisory body itself or the UIF.

the application of procedural safeguards is made[170].

Secondly, the privilege against self-incrimination constitutes the first safeguard to which individuals under investigation could resort when confronted with a controlling authority exerting *de iure* or *de facto* investigative powers. As explored in the introduction to the present work, the shift toward a society built on risk, which was provoked by the rise of new forms of criminality[171] and stimulated by technological and scientific progress, has had as a consequence that preventive approaches to social control have slowly gained momentum over reactive or repressive functions. In particular, in the realm of criminal law, a growing emphasis has been placed on the shift from crime control to crime prevention[172]. It even-

[170]Art. 48 Dir. (EU) 2015/849 requiring Member States to provide supervisors with adequate powers, «including the power to compel the production of any information that is relevant to monitoring compliance and perform check». Cf. Art. 37(5), lett. f) and (6), lett. a) and b) Dir. (EU) 2024/1640, where it is stated that national supervisors, for the sake of carrying out their task to conduct all necessary off-site investigations and on-site inspections, are allowed to «compel the production of any information from obliged entities which is relevant for monitoring and verifying compliance with Regulation (EU) 2024/1624 (...)». The same concerns are expressed by S. Allegrezza, *The Proposed Anti-Money Laundering Authority, FIU Cooperation, Powers and Exchanges of Information: A Critical Assessment*, Publication for the committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2022, p. 32, with reference to the powers of the newly established AMLA. Referring to the provisions included in the proposed regulation, which were nonetheless replicated in the adopted version, the Author points out to the broad investigative powers granted to AMLA, *i.e.* to obtain written or oral explanations from obliged entities, to require the submission of documents and access to documents and information, as well as to conduct on-site inspections, which however are not counterbalanced with adequate procedural safeguards, given the general reference to the rights of defence (Art. 24 Reg. (EU) 2024/1620) and the lack of any reference to the right to remain silent. As noted by the Author, «even though AMLA is only competent to impose administrative punitive sanctions on legal entities, the cooperation with national financial supervisors and/or criminal enforcement authorities might lead to the use of those statements in administrative or criminal proceedings against the same natural person». Furthermore, the regulation interestingly provides that «[w]hen a person obstructs the conduct of the investigation», or «opposes the conduct of an on-site inspection», AMLA might request the intervention of the competent national supervisory authority to provide the necessary assistance, arguably exerting the powers conferred to it by domestic legislation.

[171]See U. Sieber, *The new architecture of security law. Crime control in the global risk society*, in U. Sieber-V. Mitsilegas-C. Mylonopoulos-E. Billis-N. Knust (eds), *Alternative Systems of Crime Control National, Transnational, and International Dimensions*, Berlin, 2018, pp. 1-34.

[172]M.F.H. Hirsch Ballin, *Anticipative Criminal Investigations*, The Hague, 2012, p. 27. The Author metaphorically refers to another «sword function» of criminal procedural law, in addition to the traditional one of gathering evidence for prosecutorial purposes. However, this

tually resulted in criminal law sharing some features and functions with different bodies of law that are typically proactive, such as administrative, police, or intelligence law, hence the blurring of the distinctions between them[173]. Therefore, it is possible that «as a consequence of the possibility to criminally investigate at an earlier phase and bearing a shared mission of 'prevention', situations where intelligence [or administrative] investigations and criminal investigations» overlap have increased[174]. This "cumulation of spheres"[175] can take place either when administrative investigations shift into criminal investigations, and administrative supervisory powers are exerted against the targeted subjects for purposes of criminal prosecution, or when parallel investigations are conducted at the same time by different authorities. In the first case, an abuse of administrative powers, aimed at circumventing the procedural safeguards stemming from criminal law, would take place, closely resambling what the Court of Strasbourg considers to be a "subterfuge" to elicit information in defiance of the will of the accused. In the second scenario, the separation between the two parallel investigations should be maintained unless the individual under administrative investigations is recognized the procedural rights granted to suspects according to criminal procedural law[176]. Among these, the right not to contribute to self-incrimination stands out as the most immediate safeguard against abuse, as opposed to the duty to cooperate with the investigating authority, which is a typical feature of administrative inquiries. In this sense, investigations into the financial affairs of targeted customers are of no exception, in light of the reporting duties that obliged entities have.

---

new function, *i.e.* the prevention of crime, shall not occur in such a way as to deminish the protective objective of criminal procedural law, that is, the protection of fundamental rights, even when considering that the security of society against criminal threats, such as terrorism, is in itself a fundamental right.

[173]See L. Bachmaier Winter, *Informacion de inteligencia y proceso penal*, in L. Bachmaier Winter (ed.), *Terrorismo, proceso penal y derechos fundamentales*, Madrid, 2012, p. 56.

[174]M.F.H. Hirsch Ballin, *Anticipative Criminal Investigations*, cit., p. 180.

[175]Referred to in M.F.H. Hirsch Ballin, *Anticipative Criminal Investigations*, cit., p. 122, citing M. Luchtman, *Grensoverschrijdende sfeercumulatie. Over de handhavingssamenwerking tussen financiële toezichthouders, fiscale autoriteiten en justitiële autoriteiten in EU-verband*, Nijmegen, 2007, p. 133.

[176]M.F.H. Hirsch Ballin, *Anticipative Criminal Investigations*, cit., p. 123

The third point to make as to the relevance of the protection offered by the privilege against self-incrimination in the context of financial investigations is related to the conceptual gap that exists between criminal procedural law on the one hand and the functioning of financial regulatory systems on the other as far as non-disclosure is concerned. Whilst the investigative stage of criminal proceedings is mostly covered by secrecy aimed at preserving the interest of the criminal justice system to effectively prosecute crime[177], a balance against the overriding rights of the defence must nonetheless be ensured. This is usually achieved *ex post* in the trial phase, when transparency on the sources of information and on the methods by which data was collected is required to enable the defendant to exert control over the investigations, challenge evidence and effectively exercise their right to confrontation. Quite to the contrary, administrative and intelligence-led investigations are characterized by strong confidentiality prerogatives, insofar as authorities and agencies involved tend not to disclose the sources of their information and the methods used to collect and analyze that data[178]. The same holds true with regard to financial investigations, as FIUs, in the performance of their operational and strategic analysis, have neither an obligation to disseminate the results of their analysis to the competent authorities, nor to provide details on how the information was collected - whether it is from a SAR or other sources[179]. The clash

[177]The principle of secrecy is not only entrenched within legal systems with an inquisitorial tradition, such as in the case of Belgium, but it is also visible in adversarial legal orders, as demonstrated by the Italian legal system. In fact, notwithstanding the adversarial approach adopted by the 1988 Italian Code of Criminal Procedure, the pretrial stage is still governed by the obligation of secrecy for public prosecutors and police authorities until preliminary investigations are terminated and the trial phase initiated. Moreover, suspects are made aware of the allegations against them and the incriminating evidence collected only insofar as specific investigative activities requiring the involvement of the suspects themselves or their defence lawyers have to be performed (Art. 369 CCP), and in any case when the Notice of Completion of pretrial investigations is sent out (Art. 415-*bis* CCP).

[178]As pointed out by F.F. Manget, *Intelligence and the Criminal Law System*, in *Stanford Law and policy Review*, 2006, 17, p. 416 «[i]ntelligence wants to protect the sources or methods that provided the information so new information can be gained, not put them on the witness stand to prove a case in a public proceeding. Intelligence looks forward and provides an estimate of what is happening and will happen». See also, M. Jimeno-Bulnes, *The use of intelligence information*, cit., p. 178.

[179]Cf. the wording of Art. 32(3) Dir. (EU) 2015/840 and Art. 19(3) and (4) Dir. (EU) 2024/1640 according to which «[t]he FIU *shall* be responsible for disseminating the results of its analyses and any additional information to relevant competent authorities», and also that

that these two frameworks «antagonistic in nature»[180] create is self-evident when it comes to the evidentiary value of financial intelligence information, inasmuch as the latter enters criminal proceedings not only with lead purposes to constitute the basis for further criminal investigations[181], but also as evidence admitted to trial in order to assess the guilt of the defendant[182]. In those circumstances, neither the defendants nor the courts themselves might be able «to establish the source of the findings and methods by which the author of a report came to a particular conclusion»[183], which deminishes the reliability of the evidence while also hampering the rights of the defence[184].

4.1 The applicability of the *nemo tenetur* principle

As shown up to this point, the performance of financial investigations requires the involvement of several actors, which could be said to include at least competent authorities - which encompass FIUs, judicial authorities and supervisory bodies -, obliged entities and their customers. In light of such complex dynamics, the issue of the applicability of the privilege against self-incrimination in the context of financial investigations should be addressed by isolating each of these relationships. The analysis of the client-obliged entity interaction will be conducted in the third chapter when the establishment of Public-Private Partnerships for information

it «shall be operationally independent and autonomous, which means that it shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and (...) disseminate specific information». See J.B. Maillart, *The Anti-Money Laundering Architecture of the European Union*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laundering Law*, cit., p. 122.

[180]B. Vogel, *Reinventing EU Anti-Money Laundering*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laundering Law*, cit., p. 945.

[181]Which is not excluded aby the FATF framework, as pointed out by J.B. Maillart, *The Anti-Money Laundering Architecture in the FATF*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laundering Law*, cit., p. 56.

[182]Or also, as pointed out by J.A.E. Vervaele, *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?*, in *Revue Internationale de Droit Pénal*, 2005, 76, p. 429, reporting a decision of a Belgian District Court, with the view of establishing wheter an individual is to be considered a suspect according to criminal procedural law standards.

[183]B. Vogel, *Balancing Procedural Fairness*, cit., p. 5.

[184]The issue concerning the evidentiary value of financial intelligence data will be extensively addressed in Section 4.2.

sharing in the context of AML/CTF policies will be introduced, as in that context an attempt to address the question as to the existence of the privilege upon clients vis-à-vis the obliged entities they enter into business with will be carried out. However, it could be mentioned here that, while individuals do not usually enjoy any procedural right that might protect them from obliged entities, since the latter do not represent a state body and customers do not have an obligation to provide them with personal information[185], it will be contended that the participation of corporations in PPPs for information sharing should not only be brought to the attention of the customers willing to engage with the companies concerned, but it should most importantly trigger the application of the procedural safeguards stemming from the criminal procedural law field, in light of the *de facto* investigative role played by the obliged entities as was drawn from the application of the doctrine of the horizontal effect of fundamental rights.

In the present chapter, attention will be payed to the customer-FIU and obliged entity-FIU dynamics, in order to assess whether private parties enjoy any form of protection against the operational analysis performed by FIUs, whose intrusiveness and close contact with other competent authorities equate these to investigations[186]. For what the situation of customers is concerned, although any reference to procedural safeguards to comply with is missing in the FATF Recommendations, the EU lawmaker has added some references to the issue, however broad and insufficient. In fact, whereas Directive (EU) 2015/849 limited itself to declaring in the recitals its respect for the fundamental rights and principles enshrined in the Charter, such as the right to an effective remedy and to a fair trial, the presumption of innocence and the rights of the defence, the new AML/CTF framework refers in the binding part of text to the need to ensure the respect of adequate national safeguards, such as the right to a legal remedy, in cases of suspension or withholding of consent to a bank transaction or to the use of a

[185]B. Vogel, *The Anti-Money Laundering Architecture of Germany*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laundering Law*, cit., p. 238, who, however, points out that the refusal on the part of customers to provide requested information to the obliged entity might result in the exclusion of customers from the services sought.

[186]G. Amato, *The Anti-Money laundering Architecture of Italy*, in B. Vogel-J.B. Maillart, *National and International Anti-Money Laundering Law*, cit., p. 368.

bank account[187]. EU provisions therefore leave certain margins of discretion to Member States as to whether or not provide defence rights to individuals whose information is being processed by FIUs. Admittedly, it should not be neglected that the applicability of defence rights vis-à-bis FIUs, and in particular the privilege against self-incrimination, strongly depends on the institutional setup of the FIU according to the national framework. As explained in the first chapter, Member States are free to determine the nature that their respective FIUs should have, namely whether they should respond to an administrative, judicial or law-enforcement model, with the consequential features deriving therefrom[188]. Although the EU lawmaker requires Member States to make their FIUs independent and autonomous, in the sense that they «shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information»[189], the units still benefit from the investigative powers and operational status attributed to the agency in which they are based[190]. This means that judicial-type and police-type FIUs, which are strongly tied to criminal justice authorities and may even be established within the Prosecutor's Office competent for preliminary investigations into ML/TF cases, operate as an additional tool in the hands of law enforcement. They are therefore entrusted with the same powers as those given to police and judicial authorities[191], and are generally granted full access to police databases and criminal intelligence[192], as well as financial and administrative information held by other public administrations[193]. In these cases, the risk for the misuse of such

[187]Art. 24 Dir. (EU) 2024/1640.

[188]See *supra*, Chapter I, Section 2.2.

[189]Art. 32 Dir. (EU) 2015/49; Art. 19 Dir. (EU) 2024/1640.

[190]G. Pavlidis, *Financial Information in the Context of Anti-Money Laundering. Broadening the Access of Law Enforcement and Facilitating Information Exchanges*, in *Journal of Money Laundering Control*, 2020, 23(2), p. 371.

[191]M. Penna, *The 'Pre-investigative' Role*, cit., p. 269 ff; IMF, *Financial Intelligence Units: An Overview*, 2004, p. 14.

[192]G. Pavlidis, *Financial Information*, cit., p. 372. At the same time, law enforcement can easily have access to the information and data collected by the FIUs through STRs or CDD information submitted to them by obliged entities, as pointed out by M. Brewczynska, *Financial Intelligence Units: Reflections on the applicable data protection legal framework*, in *Computer Law and Security Review*, 2021, 43, p. 9.

[193]For instance, the Luxemburgoise FIU (*Cellule de renseignement financier* - CFR), which

data, or rather for the use of «information for more and more purposes (...) that are unrelated to purposes for which the information was originally collected»[194], is higher. This, from a criminal procedural law perspective, raises concerns as to the safeguards - or the lack thereof - employed in collecting and processing customers data. Thus, it would appear consequential that Member States forsaw for customers whose data are analyzed and processed by FIUs, and eventually passed on to prosecuting authorities, to be equipped with adequate procedural safeguards, notwithstanding the loss of advantages that an integration of FIUs within the criminal justice system would entail in terms of swift cooperation and lower standards[195]. Be as it may, only a few to none jurisdictions envisage any defence rights for customers against the action of FIUs, and these mostly relate to the existence of remedies for the individual customer[196].

In contrast, the obliged entity-FIU relationship requires different considerations. It was already said above that obliged entities bear specific obligations pursuant to the AML/CTF legislative framework to report suspicious transac-

follows a judicial model as it was established within the office of the Public Prosecutor of Luxembourg, has almost no limits as to the information it can proactively request from obliged entities and the financial and adminsitrative information it can have access to, as a simple request is sufficient in this sense. As for the police information the CRF can have access to, the law requires it to motivate the request. For a thorough overview of the Luxemburgoise FIU, see S. Allegrezza, G. Bruzzese, *The Anti-Money Laundering Regulation and the Handling of Financial Information in Luxembourg*, in *Financial information exchange among anti-money laundering national investigative authorities: towards a stronger cooperation in a European legal framework*, Naples, 2021, pp. 75-94.

[194]N. Jentzsch, *Financial Privacy: An International Comparison of Credit Reporting Systems*, Berlin-Heidelber, 2007, p. 39. The Author refers to what he calls "purpose creep" to refer to customers data collected and used in the context of credit reporting. However, the term, elaborated from the similar "function creep", is also used to refer to data processing in surveillance and law enforcement scenarios. See T.H.A. Wisman, *Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things*, in *European Journal of Law and Technology*, 2013, 4(2); M. Brewczynska, *Financial Intelligence Units*, cit., p. 8.

[195]As noted by B. Vogel, *Reinventing EU Anti-Money Laundering*, cit., p. 939 ff, while the interlinkage between the FIU and criminal justice authorities might result in a valuable asset, it would nonetheless deprive FIUs of their informal operational setup, their high confidentiality requirements, and swift channels of cooperation and rather subject them to the stricter criminal law limitations.

[196]As the comparative analysis conducted by J.B. Maillart, *Anti-Money Laundering Architectures. Between Structural Homogeneity and Functional Diversity*, in B. Vogel-J.B. Maillart (eds) *National and International Anti-Money Laundering Law*, cit., p. 843, shows.

tions and provide FIUs with additional information upon their requests, whose violation can be sanctioned by administrative pecuniary sanctions or even by criminal penalties[197]. It seems therefore that obliged entities that are not willing to disclose certain information of their customers - whether it is in good faith or because of the knowledge of criminal conducts - are not left with much of a choice as to whether to collaborate or not, since in the latter case it would result in being sanctioned. The interest that the privilege against self-incrimination is intended to protect, *i.e.*, the moral freedom and self-determination of the "suspect", is thus inevitably compromised.

However, some clarifications must be made. For the purposes of the AML/CTF legislation, both natural and legal persons fall under the definition of obliged entities[198]. Whereas natural persons do enjoy the protection granted by the *nemo tenetur* principle pursuant to Dir. (EU) 2016/343 and in light of the case-law of the European courts, corporations have been excluded from the scope of application of said directive in line with the stand taken by the Court of Justice in competition law matters[199]. As in the case of that substantial field, where both legal and natural persons can qualify as "undertakings" under EU competition law, a conceptual confusion exists as to what procedural rights obliged entities should have vis-à-vis the powers of FIUs, regardless of their nature. Clarity should therefore be made by the Court of Justice, which has so far been reluctant to recognize any leeway for fair trial rigths to be affirmed in the context of AML/CTF preventive system[200].

[197]As in the case of the Italian system, where Art. 55 D.Lgs. n. 231/2007 provides criminal sanctions for those obliged entities that fail to comply with reporting duties or conservation obligations.

[198]Cf. Art. 2(4) Dir. (EU) 2024/1640 to be read in combination with Art. 3 Reg. (EU) 2024/1624 that provides a list of obliged entities. These are credit institutions, financial institutions, and other entities acting in the exercise of their professional activities, such as auditors, notaries, lawyers and other legal professionals, trust and company service providers, etc.

[199]See *supra*, Section 3.2.

[200]See *Ordre des barreaux francophones et germanophone*, cit., para. 33.

4.2 Evidential value of financial data: intelligence reports and their evidentiary use in criminal proceedings

So far, attention has been focused on the investigative phase of the gathering of evidence, *i.e.* the stage in which pieces of evidence are collected by the prosecuting authorities so as to assess whether a case against the suspect can be built and brought to trial. This is due to the fact that the protection afforded by the principle of *nemo tenetur* is triggered as soon as the suspected or targeted individual is confronted with the public authorities seeking to obtain her collaboration in providing useful elements to prove their case. Yet still, the respect for procedural safeguards throughout the preliminary stage where information is collected is influential for the trial phase, insofar as evidence gathered in defiance of such safeguards - whether it is of incriminating nature or not - should not be admitted to trial, and therefore relied upon to substantiate the conviction of the defendant[201]. However, before delving into the evidentiary value of the information collected by FIUs in criminal proceedings, some key points on the law of evidence should be preliminarily addressed.

Firstly, the supranational standings on the admissibility of evidence should be briefly explained. As known, neither the European Convention makes any reference to, nor the Court of Strasbourg has been prone to interfering with, the national principles regulating the admissibility and assessment of eveidence in criminal proceedings[202]. According to the judges, «[i]t is therefore not the role of the Court to determine, as a matter of principle, whether particular types of evidence – for example, evidence obtained unlawfully in terms of domestic law – may be admissible»[203], or what weight national courts should attach to particular

[201] This is reflected in the Court of Strasbourg's reasoning in its landmark decision Saunders, when it held that «what is of the essence in this context is the use to which evidence obtained under compulsion is put in the course of the criminal trial». ECtHR, *Saunders*, cit., § 71.

[202] W. Jasiński, *Admissibility of Evidence Obtained by Torture and Inhuman or Degrading Treatment. Does the European Court of Human Rights Offer a Coherent and Convincing Approach?*, in *European Journal of Crime, Criminal law and Criminal Justice*, 2021, 29, p. 130.

[203] ECtHR [GC], 26 September 2023, *Yüksel Yalçınkaya v. Türkiye*, Appl. No 15669/20; ECtHR [GC], 11 July 2017, *Moreira Ferreira v. Portugal*, Appl. No 19867/12; ECtHR, Sec. V, 9 July 2007, *Heglas v. Czech Republic*, Appl. No 5935/02.

items of evidence, as it falls within the remit of national regulation. In line with its substantive approach, the Court's assessment in cases of allegations of Art. 6 ECHR looks at whether the proceedings as a whole, including the way in which the evidence was obtained, were fair. It follows that the sole fact that evidence has been obtained illegally will not lead to the proceedings being unfair, but rather a balacing test is carried out in these circumstances. The factors that the court takes into account in the assessment are the nature of the alleged unlawfullness, whether the rights of the defence were respected, that is, whether the applicant was given the opportunity to challenge the authenticity of the evidence and to oppose its use, and whether the circumstances in which the evidence was obtained cast doubt on its reliability or accuracy[204]. However, the Court of Strasbourg has only found unlawfully obtained evidence to be *automatically* inadmissible under Art. 6 ECHR in cases of breaches of Art. 3 ECHR[205]. In other circumstances, such as those arising from alleged violations of the privilege against self-incrimination, the Court did not *per se* excluded any evidence obtained as a result of coercion, but evaluated whether other factors, *i.e.* access to legal assistance, would compensate for the coercion exerted[206]. Whilst the Court does not usually prescribe any sanction for the use of unlawfully collected evidence[207], for cases of evidence obtained through serious breaches of human rights, the Court found a violation of Art. 6 ECHR insofar as the domestic court did not exclude that piece of evi-

[204]ECtHR [GC], 10 March 2009, *Bykov v. Russia*, Appl. No 4378/02, §§88-90; ECtHR, 12 July 1988, *Schenk v. Switzerland*, Appl. No 10862/84, § 48, where it is affirmed that »consideration should be given as to whether the use of an unlawfully obtained recording as evidence deprived the applicant of a fair trial and whether the rights of the defence were respected, particularly by determining whether the applicant was able to challenge the authenticity and use of that recording [and] whether the recording at issue was the only item of evidence relied on in support of the conviction«

[205]More specifically, oral or material evidence obtained directly through torture, whereas milder stances have been taken with regard to inhumane and degrading treatments in which a balancing test is carried out. In the case law, see ECtHR [GC], 11 July 2006, *Jalloh v. Germany*, Appl. No 54810/00; ECtHR [GC], 1 June 2010, *Gäfgen v. Germany*, Appl. No 22978/05. See also W. Jasiński, *Admissibility of Evidence*, cit., pp. 130-141.

[206]See *supra* Sec. 3.1.

[207]J.A.E. Vervaele, *Lawful and Fair Use of Evidence from a European Human Rights Perspective*, in F. Giuffrida-K. Ligeti (eds), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, Luxembourg 2019, p. 72.

dence[208].

At the EU level, expressed provisions laying down admissibility or exclusionary rules are missing, thus leaving the matter up to the decisions of the Court of Justice. The latter, however, generally holds that «it is, in principle, for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of information and evidence» obtained in violation of EU law provisions[209]. Therefore, the admissibility of evidence in criminal proceedings falls within the remit of Member States, however subject to «the necessary observance of the principle of legality and the rule of law»[210], and given that those rules are «no less favourable than the rules governing similar domestic actions (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness)»[211]. In that sense, the CJEU has held for instance that national courts should *disregard* evidence which has been collected in the context of a criminal preliminary investigation through interception of communication and afterwards passed on and used in administrative proceedings, insofar as the person concerned had not been given the opportunity to challenge the evidence and exert her defence rights[212].

However, the substantive field in which the CJEU has taken bolder stances on the admissibility of evidence is that of data retention[213]. In that rich case law, relating to the retention of telecommunication data by service providers and the access to such data by law enforcement and judicial authorities for prosecuting

[208]ECtHR, Sec. II, 27 September 2009, *El Haski v. Belgium*, Appl. No 649/08, para. 99

[209]Judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, ECLI:EU:C:2020:791, para. 222; Judgment of 30 April 2024, C-670/22, *M.N.*, ECLI:EU:C:2024:372, para. 128.

[210]Judgment of 17 January 2019, C-310/16, *Dzivev and Others*, ECLI:EU:C:2019:30, para. 34.

[211]*M.N.*, cit., para. 129; Judgment of 16 December 1976, *Rewe-Zentralfinanz and Rewe-Zentral*, C-33/76, EU:C:1976:188, para. 5.

[212]Judgment of 17 December 2015, C-419/14, *WebMindLicenses Kft.*, ECLI:EU:C:2015:832, para. 89.

[213]As pointed out by G. Lasagni, *Admissibility of Evidence in Criminal Proceedings: Lessons (and Problems) from the 'Data Retention Saga'*, in L. Bachmaier Winter-F. Salimi (eds), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Oxford, 2024, p. 33.

purposes[214], the CJEU has progressively provided Member States with guidelines to be followed by national courts on *how* to use (digital) evidence which has been collected without the necessary procedural safeguards.

In the recent landmark *Ecroachat* case, the Court maintained that evidence shall be excluded under EU law if the «person is not in a position to comment effectively on that information and on that evidence and the said information and evidence are likely to have a preponderant influence on the findings of fact»[215]. However far from setting common standards on how unlawfully obtained evidence should be administered, the Court of Luxembourg attempted to shed light on the intricate relationship between the respect of fundamental rights on one hand, and effective prosecution on the other, by upholding the principles of transparency and equality of arms over indiscrimate secrecy[216].

The second point to make on the admissibility issue concerns the extent to which information sharing between administrative and criminal authorities can take place and under what circumstances the latter can use information gathered by the former as evidence. The scholarship that addresses the issue from the point of view of transnational proceedings refers to the «informational or evidential spe-

[214]The literature addressing the data retention framework and the case-law is broad. Please refer to A. Malacarne, *Lo "Statuto Europeo" della Data Retention: Luci e Ombre*, in L. Bernardini-C. De Caro (eds), *Sfide Attuali e Tendenze Future del Diritto Processuale Penale Europeo*, Turin, 2025, pp. 371-386; M.P. Granger, K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, in *European Law Review*, 2014, 39(4), pp. 835-850; M. Rojszczak, *The uncertain future of data retention laws in the EU: Is a legislative reset possible?*, in *Computer Law & Security Review*, 2021, 41; M. Brkan, T*he essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning*, in *German Law Journal*, 2019, 20(6), pp. 864-883.

[215]Thus loosing the reference to «the field of which the judge have no knowledge», that it had previously laid out (cf. judgment of 2 March 2021, *Criminal proceedings against HK*, C-746/18, ECLI:EU:C:2021:152, para. 44), which was nonetheless obscure as it made the exclusion of evidence dependant upon the possibility for the judge to counterbalance the missed challenge of the evidence on the part of the defendant, according to L. Bachmaier Winter, *The Quest for Evidentiary Rules in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, in L. Bachmaier Winter-F. Salimi (eds), *Admissibility of Evidence*, cit., p. 21.

[216]J.J. Oerlemans, D. van Toor, *Legal aspects of the Encrochat operation: a human rights perspective*, in *European journal of crime, criminal law and criminal justice*, 2022, 30(3-4), p. 309 ff.

cialty principle»[217], in order to discern it from the traditional understanding of the specialty rule in the context of extradition and surrender procedures[218]. In the former interpretation, the principle refers to the (domestic or international) flow of information and evidence for purposes that differ from those for which it was gathered in the first place, which however fulfills the same indirect protectionist function as in extradition law[219]. In fact, as also confirmed by the case law of the Court of Luxembourg in competition law, the specialty principle, also referred to as *principle of purpose limitation*, is strictly connected to the rights of defence, insofar as the information gathered in force of cooperation duties cannot be used for other purposes than those communicated to the persons concerned, and especially not as evidence outside the legal context in which the request was made[220]. However, according to the court, these data can be used to establish whether or not it is appropriate to initiate a subsequent national procedure, which means that the purpose limitation does not strictly «protect the privilege against self-incrimination (as it deals with information that can be obtained by the Commission), but rather the duty to state reasons, so that undertakings know for what purposes the information they provide may be used»[221].

Similar considerations can be drawn in the case at stake. In the field of the prevention of the misuse of financial systems for the purpose of money laundering, the specialty principle refers to the information exchange that occurs between the financial reporting units and judicial or other public authorities for the purposes

[217] G. Vermeulen, M. Kusak, *Unblurring the Fuzzy Line Between Specialty and Data Protection in EU Mutual Legal Assistance After the European Investigation Order*, in *European Journal on Criminal Policy and Research*, 2023, 29, p. 649.

[218] Which constitutes a limitation to the offences for which an extradited person can be prosecuted.

[219] G. Vermeulen, M. Kusak, *Unblurring the Fuzzy Line*, cit., p. 649. For the analysis of the specialty principle in the aftermath of the Directive on the European Investigation Order, see J. Barbosa e Silva, *The Speciality Rule in Cross-Border Evidence Gathering and in the European Investigation Order—Let's Clear the Air*, in *ERA Forum*, 2019, 19, pp. 485–504.

[220] Judgment of 16 July 1992, *Dirección General de Defensa de la Competencia / Asociación Española de Banca Privada and Others*, C-67/91, ECLI:EU:C:1992:330, para. 29-36; Judgment of 17 October 1989, *Dow Benelux v. Commission*, C-85/87, EU:C:1989:379, para 17-18.

[221] M. Luchtman, A. Karagianni and K. Bovend'Eerdt, *EU Administrative Investigations and the Use of Their Results as Evidence in National Punititve Proceeding*, in F. Giuffrida-K. Ligeti (eds), *Admissibility of OLAF Final Reports*, cit., p. 17.

of combating money laundering and terrorism financing, upon which the entire AML/CTF system is built[222]. While EU provisions enshrined in the AML/CTF Directives do seem to put forth a specialty rule, insofar as they require information to be processed only for the purposes of combating money laundering and terrorism financing[223], the question as of the use that could be made in practice of FIU-gathered information remains still open, not only because of the risk that these could be used as evidence to prove the associated predicate offence, but also because it would run counter to the requirements of due process of law. Therefore, as in competition law cases involving the investigative powers of the Commission, the rights of defence should be considered violated when data collected for preventive purposes are used directly as evidence in the subsequent criminal proceeding with the person concerned being unaware of the use to which the information is put[224]. At a closer look, providing this information to customers would operate as a warning against the potential incriminating use that the information provided could be put to, especially for the protection of customers[225]

Once these concepts are clarified, we should now look at the issue at stake, *i.e.* the (possible) use of FIU-gathered information for criminal prosecution. The self-evident differences between traditional criminal investigations on one hand, and proactive and intelligence-led investigations on the other, have already been explored, with the main focus falling on the secrecy/transparency dichotomy.

[222]Especially in those areas in which authorities rely on economic operators, «[t]he specialty principle is intended to foster and sustain a climate of mutual trust between the reporting economic operators and the reporting units», as claimed by G. Stessens, *Money Laundering: A New International Law Enforcement Model*, Cambridge, 2000, p. 198.

[223]Cf Art. 41 Dir. (EU) 2015/849; Art. 76 Reg. (EU) 2024/1624.

[224]It is contended by G. Stessens, *Money Laundering*, cit., p. 187, that judicial-type FIUs are more disadvantageous in this respect, as the purposes for which the evidence forwarded is used by public prosecution cannot be limited. This is confirmed by J. Nies, *Detecting Economic and Financial Crime: A Special Toolkit of Investigation Techniques in Luxembourg*, in K. Ligeti-V. Franssen, *Challenges in the Field of Economic and Financial Crime in Europe and the US, Oxford-Portland*, 2017, p. 87, who reports indeed that the Luxembourg FIU is not bound by any specialty rule when the information is transferred to judicial authorities, in the sense that when the public prosecutors discover an offence when acting as FIU officials, they can prosecute the case whatever the crime. However, the Author also gives account of a practice occurring in the Luxembourg FIU, according to which a *rapport de transition* is nonetheless formally compiled by the FIU official and transmitted to the public prosecutor office.

[225]Cf. the conclusions to the Chapter III.

Whereas law enforcement and judicial authorities are required to disclose their pre-trial investigative activity at some point throughout the criminal proceeding, especially for the most instrusive activities, intelligence bodies are not compelled, or in any case willing to, reveal to the defense and judicial authorities, including the courts, the methods used for information gathering and subsequent analysis[226]. However, practice shows that, in parallel with the blurring phenomenon already discussed between preventive purposes and reactive responses, intelligence agencies and secret services are increasingly involved in criminal proceedings, with law enforcement starting processing intelligence, and intelligence agencies dealing with criminal law enforcement[227]. The involvement of intelligence agencies, as well as that of private actors[228], serves the need for investigative authorities to build a solid "information position" with the vast amounts of information they collect, in order to develop targeted strategies for combating serious forms of crime, as an integral part of so-called "intelligence-led policing". The question is, therefore, what evidential value, if any, FIU-generated information has in the context of criminal proceedings.

The different organizational designs that Member States attribute to FIUs play a role also in this context. Some authors claim that «the placement of FIUs outside the criminal justice sector (...), reflects the view that suspicious transaction reports – which are transferred by the private sector to be filtered by FIUs – are not necessarily relevant to criminal proceedings», thus suggesting that these reports are not relevant for prosecuting authorities[229]. When forwarded to the criminal justice system, however, SARs alert prosecuting authorities of detected anomalous behaviors requiring attention, therefore providing them with the *notitia criminis*

[226]See B. Vogel, *Balancing Procedural Fairness and Surveillance*, cit., p. 2; M. Jimeno-Bulnes, *The use of intelligence information*, cit., p. 178; J.A.E. Vervaele, *Terrorism and information sharing*, cit., pp. 409-443; L. Bachmaier Winter, *Section III – Criminal procedure. Information society and penal law. General Report*, in *Revue Internationale de Droit Pénal*, 2014, 85(1), pp. 75-127.

[227]L. Bachmaier Winter, *Section III – Criminal procedure*, cit., p. 92.

[228]As it will be showed in Chapter III.

[229]V. Mitsilegas, N. Vavoula, *The evolving EU Anti-Money Laundeirng Regime. Challenges for Fundamental Rights and the Rule of Law*, in *Maastricht Journal of European and Comparative Law*, 2016, 23(2), p. 283.

or with an additional investigative lead for further investigations[230]. Nevertheless, «FIUs reports – more often than not – *de facto* constitute the main evidence of the ML offence, independently of the formal value of those reports according to the criminal procedural law»[231], as they often constitute the only piece of evidence against the defendant. As things stand, procedural rules should regulate the use of FIU-generated information at trial and limit to the greatest extent the possibility for this to be directly relied on to find the conviction, as it effectively constitutes a form of secret evidence[232].

Whatever the rules governing the administration of out-of-court evidence gathered in administrative or other proceedings are[233], the risk of an indiscriminate transfer into the criminal process of evidence collected without the procedural safeguards mandated by criminal procedural law is high, especially when one considers the self-incriminating material that might stem from intelligence, as well as questionnairs or other documents compiled by virtue of an enforceable duty to

[230]However, the comparative analysis conducted by J.B. Maillart, *Anti-Money Laundering Architectures*, cit., p. 848, shows that all the national legislations examined do not specify the scope of the relevant information that FIUs should transfer to the crimial justice system, thus these do not set any limit to the potentially all-encompassing mole of information that prosecuting authorities could benefit from.

[231]V. valentini, *A Short Opening Remark - The Role of FIUs in the Fight Against ML and the Intrinsic Strangeness of ML Offence*, in *Financial information exchange*, cit., p. 3. The Author posits that FIUs reports constitute in practice authentic evidence of the predicate offence, due to the fact that these generic clues of illicit derivation of money or goods are usually sufficient to inductively prove the criminal conduct and therefore the money laundering therefrom, causing a reversal of the burden of proof as the defendant will have to provide an alternative explanation as to the origin of that money.

[232]Since the reliability of the content of FIUs reports or the methods employed cannot be generally assessed, as well as the specific persons redacting them.

[233]In the Italian legal system, Art. 220 of the implementing provisions of the CCP provides that if in the course of inspection or supervisory activities, suspicions of a crime arise, the subsequent investigative activity shall be carried out in accordance with the provisions of the CCP and the safeguards therein. However, according to the jurisprudence, the material collected before the surfacing of the suspicion might nonetheless be introduced into the criminal trial in the form of documentary evidence pursuant to Art. 234 CCP. See R. Orlandi, *Atti e informazioni dell'autorità amministrativa nel processo penale*, Milan, 1992; O. Mazza, *I controversi rapporti tra processo penale e tributario*, in *Rass. trib.*, 2020, p. 233 ff, with regard to the tax proceedings, who talks about an "escamotage" to render the information usable at trial. See also G. Di Paolo, *Admissibility of E-Evidence, Transnational E-Evidence and Fair-Trial Rights in Italy*, in L. Bachmaier Winter-F. Salimi (eds), *Admissibility of Evidence*, cit., p. 79, who casts doubts on the effectivity of the rule pursuant to Art. 220, as the distinction between an administrative offence and a criminal one is far from straightforward.

cooperate[234].

However, no harmonized rules are in place that regulate the admissibility of FIU-generated information, and only a few national jurisdictions specifically address the issue[235], with the others leaving the issue to the ordinary applicable procedural provisions on evidence law[236]. This consequently adds a layer of uncertainty to the already slippery field of evidence law.

5 Preliminary conclusions: looking for legal remedies

An attempt to provide a broad overview of old and new paradigms of the privilege against self-incrimation has been carried out so far, which passed through the analysis of the relevant EU pieces of legislation, as well as the case law of supranational courts. The first conclusion that these considerations may lead us to concerns the different levels of protection of the privilege offered by the legal systems analyzed, with the Court of Justice tending to, but still not equating, the standards set by the Court of Strasbourg, especially with regards to the subjective

[234]See E. Andolina, *Dichiarazioni rese dinanzi ad autorità diverse da quella penale*, in *Riv. it. Dir. Proc. Pen.*, 2024, 1, pp. 75-76. Moreover, the Author points out that the use of out-of-court evidence which has already been assessed by the administrative autohority, according to its own legal standards, risks irremediably influencing the court's decision, hampering its impartiality.

[235]The Spanish AML law, *e.g.*, explicitly prohibits the use as evidence in trial and pre-trial judicial proceedings of intelligence reports including operational analysis conducted by the national FIU, but to the contrary attributes evidential value to the reports redacted in its supervisory functions. Cf. A. C. Carlos de Oliveira, *The Anti-Money Laundering Architecture of Spain*, in B. Vogel-J.B. Maillart (eds) *National and International Anti-Money Laundering Law*, cit., p. 498.

[236]In the Italian legal system, forn instance, FIUs reports can be introduced as documentary evidence pursuant 234 CCP, or their content can constitute the object of the FIU official's testimony. In this sense, G. Amato, *The Anti-Money laundering Architecture in Italy*, cit., p. 381. As observed by G. Lasagni, *Public-Private Cooperation*, cit., p. 269, this circumstance, however, does not raise any issue as for the respect of the rights of the defence, insofar a criminal proceeding is indeed initiated and the defendant is given the opportunity to challenge the evidence at trial. More problematic appears to be the circumstance in which criminal proceedings are not brought forward and the FIU-gathered information upon which a preventive measure has been adopted cannot be challenged.

remit of application of the privilege. We subsequently went on to assess whether and to what extent the principle of the *nemo tenetur* is applicable and protected in the context of financial investigations, as interpreted in light of the notion provided in the first chapter. In order to answer the question, several connected aspects were addressed, in particular the slippery relationship between duties to cooperate with the authorities and procedural fairness, as well as the secrecy/transparency dichotomy characterizing intelligence on one hand and criminal proceedings on the other.

It was shown how the field of the prevention/repression of the abuse of financial markets for ML/TF clashes to a great extent with the protection of the privilege against self-incrimination, due to the extensive reporting duties falling on obliged entities, as well as the non-recognition to legal persons of the right not to incriminate themselves. However, by comparison with another substantive field of law similar to a certain extent to the AML/CTF regulation, *i.e.* competition law, it was suggested that certain features of the AML/CTF preventive system might lead to an expressed recognition of the privilege against self-incrimination also in these cases[237]. We furthermore turned to considering the way in which the FIU-generated material is used, that is, whether the data so collected can be admitted to and relied on in criminal proceedings.

However, we are left with an answer. What, if any, are the legal remedies offered against the violation of the privilege against self-incrimination in the context of FIUs activities? The issue of legal remedies for procedural flaws has been extensively tackled by scholars in parallel with the analysis of the EU Procedural Directives, due to the lack of any effective guidance therein for national legislators as to the consequences of procedural violations [238]. The difficulty lies in determin-

[237]The reference goes to the system of criminal and administrative sanctions set out for non-compliance with reporting obligations falling on obliged entities, which might suggest the *coloration pénale* of the AML/CTF preventive system, as it may as well constitute a form of improper compulsion forbidden under ECtHR case law.

[238]M. Caianiello, *To Sanction (or Not to Sanction) Procedural Flaws at EU Level? A Step Forward in the Creation of an EU Criminal Process*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2014, 22(4), pp. 317-330; A. Klip, *Violations of Defence Rights' Directives*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2018, 26, pp. 271-281; S. Allegrezza-V. Covolo, *Effective Defence Rights in Criminal Proceedings. A*

ing which are the procedural measures to be implemented that would put the suspect or defendant in the position in which they would have been had the violation not occurred[239]. Also in the case of the Presumption of Innocence Directive, hints in this regard are scarce[240]. Art. 10 Presumption of Innocence Directive states in the first paragraph that «Member States shall ensure that suspects and accused persons have an effective remedy if their rights under this Directive are breached». Then it continues by establishing that «[w]ithout prejudice to national rules and systems on the admissibility of evidence, Member States shall ensure that, in the assessment of statements made by suspects or accused persons or of evidence obtained in breach of the right to remain silent or the right not to incriminate oneself, the rights of the defence and the fairness of the proceedings are respected»[241]. The reference to the admissibility issue, which does not represent a novelty as it had already been introduced in the exact same terms by Directive (EU) 2013/48 on the right of access to a lawyer[242], is however apparently inconsistent with the intentions of EU lawmakers to provide a redress aimed at placing the accused in the status *quo ante*. In fact, according to the three-fold distinction

European and Comparative Study on Judicial Remedies, Milan, 2018.

[239]In line with the case law of the Court of Strasbourg. See ECtHR, *Salduz*, cit., § 72; ECtHR, Sec. I, 30 June 2005, *Teteriny v. Russia*, Appl. No 11931/03, § 56; ECtHR, Sec. IV, 21 October 2006, *Jeličić v. Bosnia and Herzegovina*, Appl. No 41183/02, § 53; ECtHR, Sec. II, 17 July 2007, *Mehmet and Suna Yiğit v. Turkey*, Appl. No 52658/99, § 47.

[240]To borrow the questions posed by S. Cras, A. Erbežnik, *The Directive on the Presumption of Innocence*, cit., p. 34, «what could or should a judge do with evidence that has been obtained in breach of the right to remain silent or the right not to incriminate oneself? Should that evidence be automatically excluded from the file or could the judge examine and use that evidence and, if so, under which circumstances?».

[241]It should be mentioned, however, that in Recital 46 a stronger stance is taken with regard to evidence collected in breach of Art. ECHR, whose admission would render the criminal proceedings as a whole unfair.

[242]Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty. See A. Soo, *Article 12 of the Directive 2013/48/EU: A Starting Point for Discussion on a Common Understanding of the Criteria for Effective Remedies of Violation of the Right to Counsel*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2017, 25, p. 34. See also A. Pivaty, A. Beazley, Y. M Daly, L. Beckers, D. de Vocht, P. ter Vrugt, *Opening Pandora's box*, cit., p. 341.

of violations drawn in the literature[243], the gathering of information by means of improper comuplsion in violation of the privilege against self-incrimination and the right to silence constitutes a violation that affect a single piece of evidence, which should consequently be excluded[244]. It therefore appears unclear, given the non-interference with the national systems on admissibility of evience[245], «how else a Member State can achieve the objective of putting the subject of infringement in the position he or she would have been in if the infringement had not occurred, and ensure that the rights of the defense and the standard of due process are respected when evaluating evidence obtained in violation of the right not to incriminate oneself»[246].

Turning to the legal remedies envisaged against the activities conducted by FIUs, it should be mentioned that, according to some authors, the possible violations on their part do not raise any concerns when criminal proceedings are eventually initiated on the basis of FIU-generated information[247]. In those circumstances, the defendant would be put in the position to challenge that evidence at trial in accordance with the rights and prerogatives granted to her by the Criminal Procedural Code. However, while not denying this finding, we already pointed out how difficult in practice it would be for targeted persons/defendants to challenge the reliability and accuracy of the information included in the FIU reports, especially when processing methods and sources are not disclosed.
Being as it may, this does not solve the question as to the legal remedy accorded

[243]A. Klip, *Violations of Defence Rights' Directives*, cit., p. 279.

[244]See the concurring opinion of Judge Morenilla in ECtHR, *Saunders*, cit., where she holds that «the mere fact that the applicant's statements had been obtained under compulsion and were considered by the prosecution to be incriminating and thus capable of reinforcing their case are sufficient reasons per se to have excluded the statements at the trial», thus challenging the holistic approach assumed by the Court according to which not every improper comulsion is apt to infringe on the very essence of the privilege against self-incrimination, but other factors must be weighed.

[245]Promoted during the negotiations by the Council which referred to Art. 82(2) TFEU, according to which minimum rules should take into account the differences between the legal systems of the Member States.

[246]P. Wiliński, K. Kiejnich-Krukp, *Right to Effective Legal Remedy in Criminal Proceedings in the EU. Implementation and Need for Standards*, in *Review of European and Comparative Law*, 2023, 54(3), p. 162.

[247]G. Lasagni, *Public-Private Cooperation*, cit., p. 269.

to targeted suspects in the course of the pre-trial investigations, in which FIUs are most commonly involved. Targeted individuals should be given a controlling function over the way their information is used, and should therefore be given the possibility of asking an authority within the criminal proceedings to reconsider a decision or an activity already carried out. In order to achieve that, a proactive approach should be adopted in the framework of the AML/CTF system, meaning that targeted persons should be informed of the possible processing of their financial information for prosecuting purposes and their rights stemming from the principle of *nemo tenetur*, and both obliged entities and competent authorities should refrain from using subterfuges or exerting compulsion or threat of compulsion to extract information when there is the risk of self-incrimination[248]. This might also compensate for the lack of remedies in the context of FIUs activities that do not result in criminal proceedings being initiated, as neither the EU legal framework nor most of national legislations provide for a form of judicial control or remedy against them[249].

[248]This, according to A. DE VRIES, *Recent Developments*, cit., p. 40, ensures the respect of the privilege against self-incrimination also in non-punitive proceedings, and therefore the possibility that the evidence so gathered might be subsequently used in criminal proceedings.

[249]Cf. *e.g.* M. LASSALLE, *Interaction between the State and Private Actors in the Detection and Investigation of Crime in France*, in B. VOGEL-E. KOSTA-M. LASSALLE (eds), *Law of Public-Private Cooperation*, cit., p. 165; G. LASAGNI, *Public-Private Cooperation*, cit., p. 269.

Chapter III

The rise of Public-Private Partnerships for Information Sharing in AML/CTF legislation

1 Introduction

The following chapter accounts for a significant development in the EU legislation on AML and CTF introduced by the new Regulation (EU) 2024/1624 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, whose potential consequences for the rules of criminal procedure and financial investigations as we know them may be disruptive. In fact, the explicit introduction of a legal basis for the establishment of Public-Private Partnerships between obliged entities, FIUs, supervisory authorities, and prosecuting authorities opens up for a series of legal challenges that need to be addressed, most importantly the role of the private sector in *de facto* prosecuting financial crimes.

Bearing this in mind, after providing the historical and socioeconomical background in which the rise of the private sector took place, that is, the neoliberal model developed starting from the second half of the nineteenth century, Section 2 offers an overview of the existing practices aimed at drawing the private sector within the criminal justice system. Following these introductory considerations, the concept of "Public-Private Partnerships" is untangled by referring to the con-

ceptual frameworks developed in the literature on public management, as this is indeed the realm in which PPPs have been used the most. Finally, the specific role of private entities and the issue of their accountability for fundamental rights violation is addressed.

In order to appreciate the theoretical framework developed in the preceding section against our field of interest of AML legislation, the third section of the chapter is devoted to the analysis of the new provision introducing PPPs in Regulation (EU) 2024/1264. The analysis will shed light and cast doubt on the opportunity of this policy choice.

In the fourth section, the case law of the European Court of Human Rights on the violation of Art. 6 ECHR in general and the privilege against self-incrimination in particular is taken into consideration to evaluate whether the mechanisms that PPPs for (also) law enforcement purposes would be in breach of the right to a fair trial.

Finally, some preliminary conclusive remarks will be put forth.

2 New challenges and old dilemmas: the private sector enters the scene

In the introduction to this work, we referred to the phenomenon of securitization as the conceptual context in which the present research should be framed. As already mentioned, according to scholars of securitization theory, a securitarian approach to public policies aims at depicting security as «whatever significant actors may regard as such»[1]. The point to be further explored, which is strictly connected to that of securitization, relates to whom these "significant actors" exactly are or, in other terms, which entities the state avails itself of to perform its public functions according to the securitarian approach. Before addressing what this entails for the criminal law field, a preliminary point shall be made.

Although the phenomenon of securitization has mostly occurred in the public

[1] S. Guzzini, *Securitization as a causal mechanism*, in *Security Dialogue*, 42(4-5), 2011, p. 330.

security domain, it can nevertheless be framed within the broader social, economic, and political transformation that occurred in contemporary states toward a regulatory model of governance. «[U]nder the banner of a neoliberal approach»[2] beginning from the mid-nineteenth century, modern societies have been abandoning the interventionist model typical of the positive state, to adopt a new regulatory approach to governance[3].

Among the different characteristics of the new regulatory state, the one that assumes particular relevance for this research is the shift from direct to indirect governance that occurred in the way central governments regulate public affairs. More specifically, governments managed to decentralize their administrative tasks and delegate responsibility for service delivery to the private sector through contractual arrangements, which allows them to govern «at arm's lenght»[4] or, according to the term coined by others, to govern «at a distance»[5], according to a deregulation process. The latter, however, did not entail the hiving off of public powers, but rather a different level of governance in which the state delegates powers to private actors to be performed in autonomy according to abstract rules[6]. Private companies are thus empowered and turned into «agents of securitization» that operare for the protection of the public from existential threats[7], but that

[2]A. Amicelle, *Towards a 'new' political anatomy of financial surveillance*, in*Security Dialogue*, 2011, 42(2), p. 172.

[3]The topic, although interesting, is beyond the scope of the present work. However, it might be useful to refer to the work of G. Majone, *From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance*, in *Journal of Public Policy*, 1997, 17(2), pp. 139-167, in which the Author analyzes the main reasons why a new regulatory state emerged starting from 1970s and the main features of the new public policy-making approach that contributed to the decline of the positive stae, namely liberalization, privatization, and deregulation.

[4]G. Majone, *From the Positive to the Regulatory State*, cit., p. 147.

[5]N. Rose, P. Miller, *Political power beyond the state: Problematics of government*, in *The British Journal of Sociology*, 1992, 43(2), pp. 173-205.

[6]A. Amicelle, *Towards a 'new' political anatomy*, cit., p. 166. This is clear in the AML regulation in which «[t]he regulations instruct private business to report transactions that they consider suspicious of possible money laundering, *i.e.* it gives them vaguer criteria as to what transactions to report» (B. Unger, F. van Waarden, *How to Dodge Drowning in Data? Rule- and Risk-Based Anti Money Laundering Policies Compared*, in *Review of Law and Economics*, 2009, p. 954).

[7]K. Svedberg Helgesson, *The multiple positions of private actors in securitization*, in K. Svedberg Helgesson-U. Mörth (eds), *Securitization, Accountability and Risk Management:*

nonetheless are left with deciding what these threats are.

This unfolds dangerous consequences when it comes to crime control. As anticipated, the criminal law field was not exempted from these trends. If anything, translated in terms of crime control, the securitarian approach resulted in the shift from repression to prevention and pre-emption in accordance with the increasing relevance given to risk management and risk assessment activities[8]. As it has been argued, when the two concepts, that is, securitization and risk management, orverlap, the private sector gains traction[9]. Criminal law literature has already extensively addressed the link between securitization and what could be described at the same time as a side effect and a concurrent factor of this trend, *i.e.* the emerging role of the private sector in the performance of law enforcement tasks[10].

The phenomenon is not new. In the realm of crime control, the abandoning of «the myth that the sovereign state is capable of providing security, law and order, and crime control within its territorial borders»[11] has been observed in the literature for a long time now. Whereas in the mid-nineteenth century the state was believed to have a professional monopoly over the function of crime control and to govern all aspects of social life, in the last decades of the century this idea started to crumble with the emergence of the private sector delivering security and crime control functions[12].

According to the neoliberal mode of governance and the related marketiza-

Transforming the Public Security Domain, London-New York, 2012, p. 137.

[8]As a matter of fact, the risk-based approach is one of the core elements of the so-called neoliberal penality. See P. O' Malley, *Neoliberalism, Crime and Criminal Justice*, in *Sydney Law School Research Paper*, 2016, 16(10); D. Garland, *The Culture of Control: Crime and social order in contemporary society*, Oxford, 2001; P. O' Malley, *Risk, Power and Crime Prevention*, in *Economy and Society*, 1992, 21(3), pp. 252-275.

[9]M. Bergstrom, K. Svedberg Helgesson, U. Morth, *A new role for for-profit actors? The case of Anti-Money Laundering and risk management*, in *Journal of Common Market Studies*, 2017, 5, p. 1046.

[10]As it will be seen below, the link between securitization on one hand and the involvement of private individuals on the other has been observed in several fields of the crime control domain, ranging from the gathering of telecommunication for investigating purposes through service providers, to the corporate internal investigations conducted by private investigators.

[11]D. Garland, *The limits of the sovereign state. Strategies of Crime Control in Contemporary Society*, in *The British Journal of Criminlogy*, 1996, 36(4), p. 448.

[12]Ibid., p. 449.

tion of public services[13], the traditional understanding of the role of the state in the management and control of crime is watered down by the tendency of law enforcement and the judicial authority to seek the cooperation of the private sector, notoriously in possession of vast amounts of information, data, and technical knowledge, in order to compel them to assume public duties usually pertaining to the actors of the criminal justice system[14]. In so doing, private businesses such as financial and banking institutions, airline carriers, legal professionals, and online service providers are being "responsibilized"[15] by the state and turned into private informants or agents of the law enforcement system.

These practices are even more considerable when the co-option of the private sector occurs for the collection and storage of personal data to support the investigative activity of law enforcement and judicial authorities, which increasingly rely on processing personal data gathered by the private sector and subsequently passed onto the justice system. As is known, data gathering and information sharing have become the main practices in the European Union strategy for the prevention of, and the fight against crime, which in recent years has been profiting from digitalization in all areas of modern life[16].

[13]M. Djelic, *Marketization: From intellectual agenda to global policy-making*, in M. Djelic-K. Sahlin-Andersson, *Transnational Governance. Institutional Dynamics of Regulation*, Cambridge, 2006, pp. 53-73.

[14]V. Mitsilegas, *'Security Law' and Preventive Justice in the Legal Architecture of the European Union*, in U. Sieber-V. Mitsilegas-C. Mylonopoulos-E. Billis-N. Knust, *Alternative Systems of Crime Control: National, Transnational, and International Dimensions*, Berlin, 2018, p. 209.

[15]D. Garland, *The limits of the sovereign state*, cit., p. 452 uses the term "responsibilization strategy" to refer to a model according to which «the central government seeking to act upon crime not in a direct fashion through state agencies (police, courts, prisons, social work, etc.) but instead by acting indirectly, seeking to activate action on the part of non-state agencies and organizations».

[16]As noted by B. Vogel, M. Lassalle, *Developing Public–Private Information Sharing to Strengthen the Fight against Money Laundering and Terrorism Financing: Recommendations for the European Union and its Member States*, in B. Vogel-E. Kosta-M. Lassalle, *Law of Public–Private Cooperation against Financial Crime. Developing Information Sharing to Counter Money Laundering and Terrorism Financing*, Cambridge-Antwerp-Chicago, 2024, p. 623, not only are online data being increasingly produced in digital services and held by private businesses, but also the activities taking place in the physical world are organized with the help of digital devices. See also V. Mitsilegas, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law*, 2018, 3, pp. 263-265.

As a consequence, the private sector has now become the repository of relevant information - such as telecommunication data, passengers data, and financial data make no exception - from which the commission of crimes, as well as the personal features, movements, and activities of potential criminals can be deduced to better inform criminal investigations.

However, the reliance of public authorities on the private sector to support the criminal justice system is not new, although private entities have been reserved so far a different role than the one envisaged by the partnership model. In fact, private businesses, especially online service providers and communication service providers, have traditionally been the recipients of requests by public authorities to perform certain activities that usually form part of their business to meet investigative objectives. In particular, these requests can be categorized under three main headings[17]. Firstly, private businesses have undertaken a criminal justice duty in the execution of investigative measures such as the interception of communication, which should be managed by judicial authorities but are nonetheless delegated in practice to service providers that can easily have access to telecommunications networks and servers[18].

The second form of involvement of the private sector in criminal proceedings stems from the legal obligations borne by private entities to ensure the production and storage of different categories of data generated by Information and Communication Technologies (hereafter: ICTs) which can later be used as evidence in trial. The issuing of such orders (in the form of production orders or subpoenas) to provide information of which private companies already are in possession because of their business activity has increased considerably with the recourse to electronic evidence in criminal proceedings[19], and the so-called E-evidence Regu-

[17]This distinction is partly drawn from F. Gascón Inchausti, *Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial*, in J. Conde Fuentes-G. Serrano Hoyo (eds), *La justicia digital en España y la Unión Europea*, Barcelona, pp. 193-196.

[18]As a consequence, the material that the judicial authoritites is eventually provided with, is the result of what has already been filtered to a certain extent by private businesses.

[19]As a matter of fact, whether they are committed by means of electronic devices or not, criminal conducts leave behind vast amounts of digital traces which could represent both a valuable deterrent for criminals and an indispensable source of information for judicial authori-

lation adopted in 2023 attests to this trend.

Without going into the details of the Regulation[20], it is useful to mainly address the paradigmatic change it brought about in the scenario of EU mutual recognition instruments and in the relations between the public and private spheres. In fact, the E-evidence Regulation opens up to a cooperation mechanism that takes place directly between national authorities and private actors in accordance with the "responsibilisation strategy" mentioned above[21]. In particular, the regulation places an obligation on private entities operating in specific sectors - namely providers of electronic communications services and providers of information society services[22] - by envisaging criminally sanctioned orders submitted directly to them without the involvement of the public authorities of the Member State where the evidence is deemed to be stored[23]. In such a «privatized model of mu-

ties. It should be mentioned, however, that there is not agreed definition of electronic evidence, which can nonetheless be conceived as «any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated, processed, stored or transmitted using any electronic device». See S. Avveduto, S. Conti, D. Luzi, L. Pisacane, *The Conceptual Representation of the "Electronic Evidence" Domain*, in M. A. Biasiotti-J. P. Mifsud Bonnici-J. Cannataci-F. Turchi (eds), *Handling and Exchanging Electronic Evidence Across Europe*, Cham, 2018, p. 175.

[20]Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. In the broad literature on the matter see, *inter alia*, S. Tosza, *The E-evidence Package is Adopted: End of a Saga or Beginning of a New One?*, in *European Data Protection Law Review*, 2023, 2, pp. 163-172; Id., *Mutual Recognition By Private Actors In Criminal Justice? E-Evidence Regulation And Service Providers As The New Guardians Of Fundamental Rights*, in *Common Mark. Law Rev.*, 2024, 1, p. 153; C. Brière, *EU Criminal Procedural Law onto the Global Stage: The E-evidence Proposals and Their Interaction with International Developments*, in *European Papers – A Journal on Law and Integration*, 2021, 1, pp. 493-512.

[21]C. Brière, *EU Criminal Procedural Law*, cit., p. 494

[22]Cf. Recital 27) Regulation 2023/1543 pursuant to which «[t]he categories of service providers covered by this Regulation should include, for example, online marketplaces providing consumers and businesses with the ability to communicate with each other, and other hosting services, including where the service is provided via cloud computing, as well as online gaming platforms and online gambling platforms».

[23]According to Art. 7, § 1 Regulation 2023/1543, the recipients of European Production Orders or European Preservation Orders are designated establishments, or the legal representative of the service provider concerned; only under certain circumstances, *i.e.*, the type of data at stake, the issuing authority shall notify the enforcing authority which may raise a ground for refusal. See Art. 8.

tual trust»[24], private entities are entrusted with the duty not only to preserve and disclose sensitive data upon request, but also to carry out an assessment over the substantive and formal requirements of the activity ordered, which usually falls on the executing Member State[25]. Therefore, the protection of fundamental rights seems to be responsibility of business-oriented entities, more interested in complying with public authorities' requests and avoid sanctions than to respect the privacy of their customers, with no judicial control in sight[26].

The third form of reliance of the prosecuting authorities on the private sector is represented by the legal obligation of hosting services to notify Member States' competent authorities of suspicions of certain criminal offences, recently introduced by the Digital Service Act[27]. In light of the regulation, providers of information society services (for instance, online platforms) must put in place mechanisms through which individuals or entities can make the hosting-service providers aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons is taking place. In addition to that, internet service providers have an obligation to receive the orders to act against one or more specific items of illegal content issued by the relevant national judicial or administrative authorities and to execute them by removing or disabling the access to such content. As a consequence, law enforcement mechanisms to prevent, moderate, and remove illicit content online are substantially transferred to private businesses and to their Terms and Conditions where information about policies, procedures, and remedies against their action shall be included.

[24]V. Mitsilegas, *The privatisation of mutual trust*, cit., p. 265.

[25]Cf. *e.g.* Art. 9 Directive (EU) 2014/41 on the European Investigation Order. For an analysis of the differences between the two instruments, see F. Sanvitale, *Gli ordini europei di conservazione e produzione: un passo indietro per la tutela dei diritti fondamentali nelle indagini digitali?*, in L. Bernardini-C. De Caro, *Sfide attuali e tendenze future del diritto processuale penale europeo*, Turin, 2025, p. 173.

[26]As argued by M. Daniele, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Direito Processual Penal*, 2019, 3, p. 1289, it is evident that «il vaglio del rispetto dei diritti fondamentali finisca per essere privatizzato».

[27]Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.

While a general duty to cooperate falling on businesses underpins all the mechanisms depicted above[28], what they actually entail at a closer look is a form of "externalization" of strictly public functions to the private sector, which operates according to a profit-oriented logic and not with the aim of pursuing a public interest[29]. This constitutive difference occurring between the private sector and public prosecuting authorities is even more evident in those cases in which private businesses do not limit themselves to gather and provide information, but rather have a more proactive role. Corporate internal investigations on the implementation of self-regulation or voluntary compliance mechanisms are an example of this form of externalization. Internal investigations are conducted pursuant to the corporate compliance programs that companies have to implement in order to prevent organizational and operational misconducts, and whose existence and effective implementation avoid the triggering of corporate criminial liability[30]. Although corporate investigations are generally separate from criminal justice prosecutions[31], corporate investigators[32] are entrusted with some of the traditional role of the public criminal prosecution in the prevention and investigations of

[28]With particular reference to the cross-border access to personal data, the legal basis of the E-evidence Regulation is Art. 82(1) TFEU, which promotes the principle of mutual recognition as the pivot to the judicial cooperation in criminal matters in the European Union.

[29]It is precisely for this reason that the idea of reconsidering the notion of prosecuting authority has been put forth, so as to include private entities when they carry out a public function. For these insightful considerations, see F. Gascón Inchausti, *Desafíos para el proceso penal*, cit., p. 196.

[30]In the Spanish legal system in the aftermath of the amendments of the Ley Organica 1/2015, corporations that prove to have put in place an effective preventive mechanism are entirely exempted from criminal liability or have the penalty mitigated. See L.W. Bachmaier, *Public-Private Collaboration in Criminal Law Enforcement in Spain. Involvement of Private Actors in the Detection and Investigation of Crimes*, in B. Vogel-E. Kosta-M. Lassalle, *Law of Public-Private Cooperation*, cit., p. 334.

[31]As the former do not necessarily lead to the latter. There are several reasons for considering that in this field there is less a form of cooperation than there is an «*ad hoc* coexistance» between the private sector and the criminal justice system. Among the different characteristics, the diverging interests served by both, where private companies focus on the private interests of clients, whereas crimnial investigations pursue the public interest to the fight against crimes. For these considerations, see C. Meerts, *Corporate Investigations: Beyond Notions of Public-Private Relations*, in *Journal of Contemporary Criminal Justice*, 2020, 36(1), p. 91 ff.

[32]Usually, internal investigations are conducted by the legal department of the companies themeselves or by the legal entities, or dedicated departments therein, that already perform external auditing functions for the private companies under investigation.

economic crimes. In fact, especially when corporate investigations are undertaken once a criminal action has been reported or the criminal investigations initiated in parallel[33], however not straightforward the use of resulting information in court proceedings is[34], the information collected in the course of internal investigations can be used as a lead for public authorities[35] and might be even materially stored by private investigators so as to safeguard their integrity and evidentiary value when handed over to prosecuting authorities[36].

Before proceeding further, it may be useful to summarize what was said so far. In the spirit of the theories developed by the securitization scholarship, we attempted to provide the socio-cultural and historical framework in which the emergence of the private sector occurred in public governance in general and in the crime control field in particular. In this regard, we showed how the reliance of the state on private entities went alongside the paradigm shift from an *ex post* prosecution of criminal conducts to a preventive justice model, due to the invaluable contribution private businesses provide in managing risk.

The strategic importance that sound prevention systems have for crime control is particularly evident in the field of antimoney laundering and countering terrorism financing. In fact, as shown in Chapter I, the FATF, later followed by the European Union, strongly encouraged the adoption of a preventive approach, which, according to some scholars, was less driven by the urge to fight crime than it was to protect the integrity of international financial systems[37]. However, the

[33]L.W. Bachamier, *Public-Private Collaboration*, cit., pp. 336-3637 recalls that internal investigations are usually categorized into three types, *i.e.*, preventive investigations; reactive investigations to evaluate whether to forward the notitia criminis to public authorities, and defensive investigations which aim at gathering evidence so as to show the will to collaborate with prosecuting authorities.

[34]As reported by G. Lasagni, *Public–Private Cooperation in the Detection and Investigation of Criminal Offences in Italy*, in B. Vogel-E. Kosta-M- Lassalle, *Law of Public-Private Cooperation*, cit., p. 283, in the Italian legal system the material collected during internal investigations is considered as the one collected by defence lawyers and can therefore be used at trial if admitted and presented before the court according to the rules of the Code of Criminal Procedure.

[35]B. Vogel, M. Lassalle, *Developing Public–Private Information Sharing*, cit., p. 624.

[36]F. Gascón Inchausti, *Desafíos para el proceso penal*, cit., p. 197.

[37]In these terms, A. Amicelle, *Trace my money if you can: European security management*

increasing involvement of the private sector in criminal proceedings was not only due to the deregulation process that occurred in the neoliberal state, nor was it limited to financial crimes[38], as technological advancement played a key role in fostering cooperation between investigating authorities and highly skilled and sectorial private businesses, as demonstrated by the E-evidence Regulation and the Digital Service Act cases.

If, to a certain extent, these examples of interaction between the private sector and public authorities could still be labeled as forms of cooperation, although hesitantly, the potential use of public-private partnerships for information sharing in the context of ML/TF opens the way to a blatant "outsourcing" or "externalization" of traditional public functions with dangerous consequences for the criminal procedure and the protection of fundamental rights thereof. In light of this, the concept of Public-Privare Partnerships (PPPs) shall be further explored before addressing the use of such a mechanism in the AML/CTF legislation.

2.1 Untangling the concept of Public-Private Partnerhips

In the previous section, we used several terms semantically referring to forms of institutional arrangements between public authorities and private entities. We discussed the process of privatization, talked about "public-private cooperation", outsourcing, and contractual agreements. The term "public-private partnership" now enters the scene of the discussion[39], although some scholars contend that it has the same meaning as other terms such as "contracting out" and "priva-

of financial flows, in K. Svedberg Helgesson-U. Mörth (eds), *Securitization, Accountability and Risk Management*, cit., p. 110.

[38]Although, as noted by A. Amicelle, *Towards a 'new' political anatomy*, cit., p. 165, the move towards deregulation occurred in the financial market more vividly than in other fields, which however does not entail a lack of rules, but rather the implementation of prudential policies - such as the Basel principles - as a specific mode of risk-based regulation.

[39]In the words of G. Hodgea, C. Greveb, M. Biygautanec, *Do PPP's work? What and how have we been learning so far?*, in *Public management review*, 2018, 20(8), p. 1108, «we have entered an era of a globalised use of PPP policy ideas and language. The initial narrow conception of a western project delivery technique has thus now evolved into a global PPP policy agenda with a much broader meaning covering everything from economic development and infrastructure governance to multiple project delivery options».

tization" perceived as pejorative[40]. In this sense, policy makers favor the term "public-private partnerships", as it would encourage broader participation of private organizations in the public discussion and would allow them to gain a share in the delivery of public services[41]. Aside from linguistic considerations, this first point raises the following questions: Does expanding the involvement of private entities in the delivery of crime control functions serve the purposes of the criminal justice system? To whom is it beneficial in the end? Are the charachteristics of public-private partnerships suitable from a criminal procedural law perspective? In order to address these questions and to get a sense of what the EU lawmaker means by "public-private partnerships for information sharing", the research should now delve into doctrinal conceptualizations drawn from public management scholarship, as this is indeed the realm in which PPPs have been used the most. For present purposes, it will be sufficient to briefly illustrate the descriptive definitions provided in the literature, and the main features of PPPs[42].

We should start by saying that there is no core PPP concept[43], for a variety of designs and models have been empirically observed according to different classification systems. Several definitions have been offered that stress different features of PPPs and reveal the inconsistent positions of scholars on their nature. For example, they have been described in general terms as «any arrangement between government and the private sector in which partially or traditionally public activities are performed by the private sector»[44], or, more specifically, as «ongoing agreements between government and private sector organizations in which

[40]G. A. Hodge, C. Greve, *Public-Private Partnerships: An International Performance Review*, in *Public Administration Review*, 2007, 67(3), p. 547.

[41]Ibid.

[42]The historical background of PPPs and the first experiences of this kind of governance system will not be addressed in this work. However, with specific regard to PPPs attempts in the crime control sector, valuable insights can be drawn from N. Knust, *Socio legal foundations of Public-Private Partnerships in the system of crime control*, in B. Vogel-E. Kosta-M. Lassalle, *Law of Public-Private Cooperation*, cit., pp. 91-115. See also, G. Lasagni, *Public private partnerships nell'antiriciclaggio e antiterrorismo: una nuova forma di outsourcing del processo penale?*, in *Dir. Pen. cont.*, 2021, 3, pp. 153-167, and the bibliography therein.

[43]As concluded by M. Marsilio, G. Cappellaro, C. Cuccurullo, *The Intellectual Structure Of Research Into PPPs*, in *Public Management Review*, 2011, 13(6), p. 776.

[44]E.S. Savas, *Privatization and Public-Private Partnerships*, New York, 2000, p. 4.

the private organization participates in the decision-making and production of a public good or service that has traditionally been provided by the public sector and in which the private sector shares the risk of that production»[45]. Other conceptualizations stress the latter point, that is, the sharing of the risks connected with products and services ultimately delivered, with costs and resources equally to be shared among public and private participants[46], although private parties are traditionally involved in PPPs to provide management and operating services and/or to put private finance at risk[47]. All the main features that are apt to differentiate PPPs from other forms of institutional arrangements are encompassed in these definitions and will be illustrated in the following. Ultimately, the analysis aims to show that there are several reasons to contend that public-private partnership schemes are not appropriate to be implemented into the AML/CTF legal architecture.

To begin with, it can be drawn from the definitions provided above that public and private members of PPPs possess and operate according to divergent underlying premises and completely different logics. On the one hand, public authorities are required to pursue capital investments to serve public interests; on the other hand, private actors respond are driven by the aim of recovering their investments and gain profits[48]. In the criminal justice sector, this dichotomy is also evident. In fact, law enforcement agencies generally operate reactively[49] to restore the legal order once an alleged misconduct has taken place, and information sharing to that aim only takes place if an initial suspicion arises. In other terms, judicial

[45] J. Forrer, James Edwin Kee, K. E. Newcomer, E. Boyer, *Public-Private Partnerships and the Public Accountability Question*, in *Public Administration Review*, 2010, 70(3), p. 476.

[46] H. van Ham, J. Koppenjan, *Building public-private partnerships: Assessing and Managing Risks in Port Development*, in *Public Management Review*, 2001, 3(4), p. 599.

[47] M.J. Garvin, D. Bosso, *Assessing the Effectiveness of Infrastructure Public–Private Partnership Programs and Projects*, in *Public Works Management and Policy*, 2008, 13(2), p. 163.

[48] J. Forrer, James Edwin Kee, K. E. Newcomer, E. Boyer, *Public-Private Partnerships*, cit., p. 477.

[49] «Although the analysis of security law indicates that crime control measures are tending more and more towards prevention, current crime control by law enforcement agencies is still primarily retrospective in nature». N. Knust, *Socio-legal foundations*, cit., p. 112.

authorities and law enforcement authorities work on a "need to know" or "right to know" basis[50]. To the contrary, private actors in the financial sector follow a profit-oriented business model and therefore aim at preventing any potential threat to profit. Thus, intelligence sharing between them occurs proactively on a "you might need to know" basis to ensure that the regulated economic system functions well and is protected from risks[51]. These different approaches risk eroding the mutual trust that should inform the relationship between private actors and public authorities. In fact, not only are public authorities reluctant to provide feedback to private entities, hence disregarding the logic of reciprocity, but public authorities are also bound by procedural safeguards and fundamental rights' protection considerations that do not concern the private sector[52]. As a consequence, the effectiveness of PPPs involving law enforcement and financial actors may be compromised.

The second feature emerging from the varied definitions of PPPs concerns the circumstance that public and private members of partnerhisps are indeed equal partners, that is, they hold the same position when it comes to roles, rights, and duties. The relationship between public authorities and private entities in the context of a PPP is therefore shaped by «mutual influence, (...) which incorporates mutual respect, equal participation in decision-making, mutual accountability, and transparency»[53], all of which endure as long as mutuality benefits are ensured[54]. By engaging in a mechanism entailing peer relations, private and public entities

[50] J.G. Carter, *The Structure and Function of Public-Private Partnerships for Homeland Security*, in *Homeland Security Review*, 2008, 2(3), p. 243.

[51] As noted by K. Svedberg Helgesson, *The multiple positions*, cit., p. 140, «for the private actors, risk assessment and risk management are not new things, nor are they primarily associated with the public sphere. Risk and associated practices are already part and parcel of many business practices, albeit for purposes other than securitization on behalf of the state».

[52] N. Knust, *Socio-legal foundations*, cit., p. 103.

[53] J. M. Brinkerhof, *Assessing and improving partnership relationships and outcomes: a proposed framework*, in *Evaluation and Program Planning* 25(3), p. 216. According to the Author, mutuality is one of the key dimensions characterizing partnerships, which is opposed to prevalence of one member over the other. Mutuality denotes a state of interdependence, where each member has rights and responsibilities owned to the other.

[54] J.G. Carter, *The Structure and Function*, cit., p. 245, observes that this feature is typical of joint ventures partnerships for information sharing, that are «constant two-way relationship where each party stands to gain valuable information that directly influences their operations».

tend to adopt each other's behavior and priorities, with the private sector developing public interest considerations and playing a key role in decision making and public service delivery[55]. For PPPs in the criminal justice arena, this would open up to a reshuffle of roles within criminal proceedings, in which private entities have been acting so far in execution of orders from the prosecuting authority.

The third noteworthy fundamental feature of PPPs, which is strictly related to the power sharing illustrated above, is risk sharing, *i.e.* the fashion in which risk is allocated among the partners. As mentioned, parties are in a PPP on equal terms, which suggests that they both have to bear parts of the risks therefrom. However, since one of the drivers that push public authorities to involve private actors in PPPs is the assumption that the latter have the necessary know-how, financial resources, and organizational skills to address public functions[56], private actors generally assume a more significant role than the other party. Private parties are therefore more inclined to assume and manage risks involved in the partnership, which raises questions as to which party should accountability lie with. Private actors are in fact not part of the chain of delegation of powers that involves public actors, therefore their accountability is never addressed[57]. This would lead to a governance system that lacks democratic oversight[58]. Accountability is usually associated with transparency, liability, controllability, and the imposition of sanctions, and is defined as a social principal-agent relation, pursuant to which the actor (the agent) bears the obligation to explain and justify their conduct to the principal[59].

[55]S.H. Linder, *Coming to terms with the Public-Private Partnership. A grammar of Multiple Meanings*, in *American Behavioral Scientists*, 1999, 43(1), p. 37.

[56]J. Forrer, James Edwin Kee, K. E. Newcomer, E. Boyer, *Public-Private Partnerships*, cit., p. 477. Similarly, H. van Ham, J. Koppenjan, *Building public-private partnerships*, cit., p. 596., according to whom «[f]or public parties, the involvement of private parties is desirable because on the one hand they operate more efficiently than public organisations but also because they possess the market experience and innovative creativity which public parties often lack».

[57]U. Mörth, *The market turn in EU governance—the emergence of public–private collaboration*, in *Governance: An International Journal of Policy, Administration, and Institutions*, 2009, 22(1), pp. 99-120.

[58]«Indeed, the virtue of democratic accountability becomes a problem when public authority is shared with rather than delegated to private actors». *Ibid.*, p. 101.

[59]M. Bovens, *Analysing and Assessing Accountability: A Conceptual Framework*, in *Euro-*

Looking at the potential implementation of PPPs in crime control and in the AML field specifically, the risk-based approach changes the basis for accountability allocation[60] with a shift towards the private sector. Under the lenses of criminal procedure, the terms of the discussion around accountability can be translated into a responsibility issue: in other terms, if risk is shared among the partners, should not liability for the management of such risk be shared as well? Whereas democratic accountability is difficult to define as there is no straightforward view on the standards for accountable behaviour[61], the concept of accountability in criminal law is more intuitive as it does not only refer to the principle of personal liability, according to which one should take responsibility for their own actions, but also suggests that the criminal justice system as a whole should be held to specific standards of conduct[62]. It seems appropriate to argue that what ensures accountability from a criminal procedural perspective is the existence and implementation of procedural safeguards, whose encroachment by whomever *de facto* exerts public functions should be sanctioned and a remedy be offered.

Against the backdrop depicted so far, it is here challenged the policy choice to draw the tool of PPPs into the realm of crime control in general and AML/CTF legislation in particular, in light of the characteristics of the latter and the enhanced risk to overstep the boundaries of prevention into prosecution of crime. However, under these circumstances, the analysis of the traits of this kind of public-private institutional arrangements offered some insightful hints. In particular, the power sharing and the related risk sharing that members of PPPs agree to undertake, in addition to the equality of posts that public and private actors cover, suggest that they bear the same responsibilities and that the protective mechansims put in place against the action of prosecuting authorities should be extended to private entities when they take up criminal justice functions.

---

pean Law Journal, 2007, 13(4), p. 450.

[60] M. Bergström-K. Svedberg Helgesson-U. Mörth, *A New Role for For-Profit Actors?*, cit., p. 1052.

[61] M. Bovens, *Analysing and Assessing Accountability*, cit., p. 450.

[62] See for instance A. Duff, *Discretion and Accountability in a Democratic Criminal Law*, in M. Langer-D.A. Sklansky (eds), *Prosecutors and Democracy. A Cross-National Study, Cambridge*, 2017, pp. 9-39, on the role of prosecutors.

The subsequent section will analyze the role of private entities, referred to as obliged entities under AML/CTF legislation, by applying the horizontal effect theory, in an effort to provide a rationale for expanding the protection of fundamental rights.

2.2 Obliged entities within criminal proceedings: drawing lessons from the theory on horizontal effect of fundamental rights

At the heart of the political, sociological, and economic phenomena identified above, *i.e.*, securitization of criminal law, deregulation of markets and privatization of public policies, lies the private sector. Admittedly, what we are facing now is a reality in which certain private individuals or entities have been gaining such economic, social or mediatic power that closely resamble the powers detained by public authorities and that is able to nullify or seriously compromise the bare minimum of freedom of self-determination that weaker subjects have[63]. In such a scenario, the conventional approach to the public-private dicothomy, which views the two concepts as antagonistic, begins to vacillate in practice[64], and the idea that

[63] J. M. Bilbao Ubillos, *La consolidación dogmática y jurisprudencial de la Drittwirkung: una visión de conjunto*, in *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, 21, 2017, p. 50.

[64] S. Walkila, *Horizontal effect of fundamental rights in EU law*, Groningen, 2016, p. 135. This idea is rooted in the natural rights theory and the social contract theory that were developed by seventeenth and eighteenth-century political philosophers, among whom John Locke is the most representative (J. Locke, *Two Treatises of Government*, London, 1689). According to this liberal theorization, human beings are in possession of natural rights that exist independently of the state as they predate its coming to existence and that, in order to better ensure the stable, comfortable enjoyment of their lives and avoid chaos, people willingly consent to transfer some of their rights to a central government by means of a social contract. Drawing from these premises, Locke elaborated on the distinction between political and paternal, public and private sphere, in the former of which the community interacts with and is subject to the government's power which only intervene to protect and solve controversies, and in the latter of which individuals interact *inter se*. For an in-depth analysis of modern social contract and natural rights theories, see extensively A.J. Simmons, *The Lockean Theory of Rights, Princeton*, Princeton, 1992; K.A. Kelly, *Private Family, Private Individual: John Locke's Distinction Between Paternal and Political Power*, in *Social Theory and Practice*, 2002, 28(3), pp. 361-380.

the limits between them are instead blurred is widely accepted[65]. Therefore, the existence of formally private entities that nevertheless exert substantially public-alike coercive powers raises questions as to what role they do or should play in our society, and which instruments or protections do weaker parties have to uphold their rights and freedoms.

These points account for the theoretical basis upon which the legal doctrine of the "third-party effect" was built and developed. Also referred to as "horizontal effect doctrine" or *Drittwirkung* in the German constitutional order where it was formulated for the first time, this legal theory provides a method of explaining the applicability of fundamental human rights to relations between private parties[66] upholding the idea that fundamental rights should offer their protection not only in vertical, *i.e.* in such a way to defend citizens from illicit intrusions of the State into their individual sphere, but also horizontally[67]. In other words, the *Drittwirkung* doctrine was theorized in order to fulfill the gap existing in the

[65]In the words of J. M. Bilbao Ubillos, *La consolidación dogmática*, cit., p. 51, «un (...) elemento de análisis es la profunda crsis de la dicotomia publico-privado. El poder público tiende a privatizarse mientras que el privado asume cada vez más connotaciones públicas. (...) Lo que vemos realmente es una continuidad, un progresivo entrecruzamiento».

[66]K. Kamber, *Prosecuting human rights offences: Rethinking the sword function of human rights law*, Leiden-Boston, 2017, p. 35.

[67]For an overview of the scholarship on the *Drittwirkung* doctrine, extensively refer to J. Fedtke, *Drittwirkung in Germany*, in D. Oliver-J. Fedtke (eds), *Human Rights and the Private Sphere. A Comparative Study*, London, 2007, pp. 124-156; A. Clapham, *Human rights in the private sphere*, Oxford, 1993. The doctrine was formulated for the first time by the judiciary, namely by the President of the Federal Labour Court (*Bundesarbeitsgericht*, BAG), who, in a 1954 decision concerning the dismissal of a factory worker, argued that fundamental rights constitute guiding principles for social life and that certain constitutional rights might therefore *directly* influence the interpretation and validation of private agreements so as to limit private autonomy. However, not only this position was criticized by scholars, but it was also watered down by the subsequent jurisprudence following the Lüth case of 1958 in which the theory of "indirect" or "radiating" effects of fundamental rights was introduced. The applicant complained before the Federal Constitutional Court (*Bundesverfassungsgericht*, BVerfG) that his fundamental right to freedom of expression had been infringed upon by the interlocutory injunction upheld against his calls to boycott an anti-semitic film that was produced during the Nazi regime. According to the Court, which was to decide whether constitutional rights such as the right to free speech could be violated in strictly private matters, fundamental rights form an "objective order of values" whose purpose is to reinforce the individual rights. Indeed, although according to a lower level of protection than that granted against public powers, fundamental rights have a radiating effect on private relations that the judiciary and the lawmaker are compelled to take into account when performing their tasks, at the risk of violating individual rights.

German constitutional framework pursuant to which private entities were not deemed to be constrained by fundamental rights considerations, and, although different declinations of the same doctrine exist[68], the common bottom line is to hold private parties accountable for fundamental rights' violations[69].

The issue of the horizontal effect of fundamental rights is not limited to the German legal tradition, since most national constitutional laws failed to expressly bound private parties to the application of human rights, save for some exceptions[70]. The interest towards the expansion of fundamental rights discourse is the result of the reconceptualization and revitalization of human rights law occurred in the aftermath of the Second World War, when modern national constitutions were adopted and higher standards of protection of human rights were invoked in international *fora*[71].

[68]As pointed out by G. Schumann Barragán, *Derecho a la tutela judicial efectiva y autonomía de la voluntad: los contratos procesales*, Madrid, 2022, p. 105, the debate on the direct or indirect effect of the *Drittwirkung* doctrine can be considered partially solved, as the latter interpretation prevails. However, it will suffice to mention that different conceptual constructions were developed in Germany, the first one upholding the direct effect of fundamental rights (*unmittelbare* or *indirekte Drittwirkung*) able to replace inadequate lower norms, whereas the second one (*mittelbare Drittwirkung*) maintains that fundamental rights operate as complementary principles against which the judges should interprete and the lawmaker regulate lower norms. On the different theories, see M. Bilbao Ubillos, *La consolidación dogmática y jurisprudencial de la Drittwirkung*, cit., p. 52 ff.

[69]Currently, it seems that the debate within constituional scholars around the direct or indirect horizontal effect of fundamental rights has been settled and the two perspectives reconciled, in the sense that fundamental rights do operate directly as subjective rights but only limitedly, that is, in accordance with the mediation of the law which allows fundamental rights to perform their effectiveness and expand the scope of their protection. See I. Gutiérrez Gutiérrez, *Criterios de eficacia de los derechos fundamentales en las relaciones entre particulares*, in *Teoría y realidad constitucional*, 1999, 3, p. 195.

[70]M. Beladíez Rojo, *La eficacia de los derechos fundamentales entre particulares. Algunas consideraciones sobre el distinto alcance que pueden tener estos derechos cuando se ejercen en una relación jurídica de derecho privado o de derecho público*, in *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, cit. 77; J. M. Bilbao Ubillos, *La consolidación dogmática y jurisprudencial*, cit., p. 59.

[71]The reference certainly goes to the Universal Declaration of Human Rights adopted by the United Nation General Assembly in 1948 which «is unquestionably the foundational document of international human rights law. It establishes the basic parameters of the meaning of "human rights" in contemporary international relations and (...) in national discussions as well» (J. Donnelly, *Universal Human Rights in Theory and Practice*, Ithaca-London, 2013, p. 26). Moreover, as will be seen below, the entry into force of the European Convention on Human Rights in 1953 definitely fostered the notion of horizontality of the fundamental rights enshrined therein. For an account on the Italian national experience, see C. Favilli, C. Fusaro, *The pro-*

While acknowledging the application of constitutional rights to private relationships, the legal doctrine concludes that these rights have a different impact on private relationships than they do with respect to public powers - in other words, they have a radiating effect with different degrees - in light of the fact that in the latter case there are no fundamental rights to balance[72]. In fact, those fundamental rights that do not bind individuals, in the sense that they can only be infringed upon by public powers, such as the right of assembly or the right to a judicial remedy, will have a low level of horizontal effect within private relations.

At this point, in light of the considerations on the nature and physionomy of PPPs developed above[73], one could argue that every time individuals enter into a business relation with a private entity engaged with public powers by virtue of public-private partnerhips, then fundamental rights should apply horizontally as if it entailed a legal relationship in which one of the two parties - *e. g.*, the bank - is a public authority acting in a position of supremacy[74]. Therefore, if we accepted the idea that obliged entities involved in PPPs with prosecuting authorities should be treated as such when carrying out the required activities pursuant to the agreement, we would eventually conclude that the fundamental rights relating to the fair trial should apply. In fact, public authorities should not make use of public-private partnerships with private businesses to bypass the constraints and safeguards stemming from criminal procedural law[75].

However, the legal doctrine of the *Drittwirkung* is just one of the many theories that were developed to explain the effects of human rights in the private sphere.

---

tection of Constitutional Rights in the Private Sphere, in D. Oliver-J. Fedtke (eds), *Human Rights and the Private Sphere*, cit., p. 280.

[72] In view of the fact that the State exclusively holds obligations. In this sense, M. Beladíez Rojo, *La eficacia de los derechos fundamentales*, cit., p. 85; G. Schumann Barragán, *Derecho a la tutela judicial efectiva*, cit., p. 105. See I. Gutiérrez Gutiérrez, *Criterios de eficacia*, cit., on the conflicts of opposit rights.

[73] *Supra* Section 2.

[74] M. Beladíez Rojo, *La eficacia de los derechos fundamentales*, cit., p. 86.

[75] Or, how clearly put by F. Gascón Inchausti, *Desafíos para el proceso penal*, cit., p. 198 referring to private corporate investigations, «resulta aún más importante evitar que el Estato se aproveche de la externalización para dar cabida, por la puerta trasera, a una rebaja de estandares de proteccion de los derechos fundamentales, con el argumento de su diferente alcance en el ambito de las relaciones entre particulares».

Other doctrines belonging to different legal cultures attempted to hold private entities accountable for their actions by emphasizing the public element. A clear example in this sense is represented by the so-called "state action doctrine" - or, better put, by the exceptions to the rule therefrom - elaborated by the Supreme Court of the United States[76]. According to the doctrine, constitutional individual rights apply only to state action, not to private action. However, under certain conditions, private actors might be considered public actors when the infringements of individual rights they commit in their private activity are particularly serious. Pursuant to the case law of the Supreme court, fundamental rights might be invoked against private entities when a «significant state involvement» is observed in the actions of the private entity, or when the latter performs a governmental or public function[77]. In both circumstances, therefore, a public element must occur for the court to find the private party directly bound by constitutional provisions establishing individual rights[78], insofar as in the absence thereof no constitutional violation be found.

[76]The doctrine is of great importance in the US constitutional debate, as in the words of E. Chemerinsky, *Rethinking State Action*, in *Northwestern University Law Review*, 80(3), 1985, p. 504, «[t]he ability of the federal government, both through the judiciary and the legislature, to protect rights from private interference is determined, in large part, by the definition of state action». The literature on the state action doctrine dates back to the mid-nineteenth century but was particularly active in the twentieth century; among the others, see R. Hale, *Rights Under the Fourteenth and Fifteenth Amendments Against Injuries Inflicted by Private Individuals*, in *Law Guild Review*, 1946, 6, pp. 627-639; H.W. Horowitz, *The Misleading Search for "State Action" Under the Fourteenth Amendment*, in *Southern California Law Review*, 1957, 30(2), pp. 208-221; W. W. Van Alstyne, K. L. Karst, *State Action*, in *Stanford Law Review*, 1961, 14(1), pp. 3-58. More recently, *Developments in the Law — State Action and the Public/Private Distinction*, in *Harvard Law Review*, 2010, 123(5), pp. 1248-1314; M. Minow, *Alternatives to the State Action Doctrine in the Era of Privatization, Mandatory Arbitration, and the Internet: Directing Law to Serve Human Needs*, in *Harvard Civil Rights-Civil Liberties Law Review*, 2017, 52(1), pp. 145-168, M. Kumm, V. Ferreres Comella, *What Is So Special about Constitutional Rights in Private Litigation?: A Comparative Analysis of the Function of State Action Requirements and Indirect Horizontal Effect*, in A. Sajo-R. Uitz (eds), *The Constitution in Private Relations* The Hague, 2005, pp. 241-289.

[77]A complete analysis of the US Supreme Court jurisprudence in a range of fifty years is carried out by T. Perretti, *Constructing the State Action Doctrine, 1940-1990*, in *Law and Social Inquiry*, 35(2), pp. 273-310.

[78]S. Walkila, *Horizontal effect*, cit., p. 156. Indeed the Supreme Court has clarified that the overall inquiry «must be whether there is a sufficiently close nexus between the State and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the State itself». Jackson v. Metropolitan Edison Co., 419 U.S. 345 (1974).

Whereas the doctrine has been highly critized in the scholarship[79] and inconsistently applied by the court, a key point may prove relevant to our case and therefore needs consideration. The state action doctrine originally premised on a clear-cut public-private distinction drawn from the classical legal theory that dominated the US constitutional discourse, according to which the legal system is based on two separate spheres of autonomy of private and public actors. In line with that, the violation of constitutional rights of the individuals by other private actors was considered a «conceptual impossibility»[80], as they could be invoked exclusively before the government. Related to this view was the idea that natural rights of individuals were already protected from private interference under common law principles and therefore they did not need constitutional safeguards[81]. However, contemporary interpretations of the state action doctrine reject the persistence of such premises in light of the fact that the dividing lines between what is public and what is private are increasingly fading.

Whether this circumstance is to be attributed to the effects of legal definitions[82] or to the phenomenon of privatization[83], it is a fact that a formal distinction between private action and state action no longer reflects the reality of modern governance. In view of the emergence of a variety of corporate organi-

[79]The state action doctrine has been defined as a «conceptual disaster» by C. L. Black, *Foreword: "State Action", Equal Protection, and California's Proposition 14*, in *Harvard Law Review*, 1967, 81(69), p. 85. According to E. Chemerinsky, *Rethinking State Action*, cit., p. 506, the premises upon which the doctrine is based are now anachronistic.

[80]*Developments in the Law*, cit., p. 1257.

[81]E. Chemerinsky, *Rethinking State Action*, cit., p. 529, challenges the idea that the state action doctrine is indeed consistent with the natural law theory of fundamental rights, arguing that if constitutional rights are natural rights because of their inherence in pesonhood, then there is no point in denying protection when they are violated by private action.

[82]According to R. S. Kay, *The state action doctrine, the public-private distinction, and the independence of constitutional law*, in *Constitutional Commentary*, 10(2), p. 336, not only do private actions occur in a state-regulated environment, in which it is up to the law to decide whether to prohibit or permit certain conducts, but it is the law itself to define the distinction between "public" and "private", and therefore determines the content of such categories. Similarly, M. Minow, *Alternatives to the State Action Doctrine*, cit., p. 158, notes that «[t]he very notion that a private sphere is different from a public sphere varies across cultures and shifts over time».

[83]One of the first authors to acknowledge the flaws of the state action doctrine vis-à-vis the increasing involvement of private actors in the performance of government activities is G. E. Metzger, *Privatization as delegation*, in *Columbia Law Review*, 2003, 103, p. 1367, according to whom «[w]hile this kind of private involvement is longstanding, (...) it is expanding».

zations concentrating wealth and power in a quasi-public manner, and of the trend of governments to delegate traditionally public powers to these for-profit actors for the delivery of public services, especially in the field of social welfare programs[84], private entities became increasingly embadded in the public realm essentially through outsourcing and contracting mechanisms[85]. By logic, the disappearance of the premise, *i.e.* the public-private divide, should imply the failure of the doctrine.

One might claim that this argument seemingly appears not conclusive enough to debunk the doctrine, insofar as greater involvement of the state into private behaviors implies a more blatant - hence, accountable - public nexus able to trigger fundamental rights' protection. However, some scholars rebut this idea and argue that the inconsistency between the state action doctrine and the privatization of public policy lies in the fact that the state leaves private actors with broad discretionary leeways in operating control over government activities, with the public power gradually minimazing its involvement in their actions[86]. This holds all the more true when privatization is pursued by means of partnership agreements, which, as already pointed out in the previous paragraph, are distinguished by loose regulation and permanent trust and reciprocity in order to ensure the long-term existence of the cooperation mechanism[87].

Shifting away from social welfare and infrastructure public-private partner-

[84]G. E. Metzger, *Privatization as delegation*, cit., p. 1380. But the phenomenon is not limited to it. See, for instance, M. Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy*, in *Boston College Law Review*, 2005, 46(5), pp. 989-1026.

[85]For a historical analysis of the public-private dichotomy in the American society and economy, W. J. Novak, *Public-Private Governance. A Historical Introduction*, in J. Freeman-M. Minow (eds), *Government by Contract: Outsourcing and American Democracy*, Cambridge-London, 2009, pp. 23-40.

[86]See G. E. Metzger, *Privatization as delegation*, cit., p. 1395 and Id., *Private Delegations, Due Process, and the Duty to Supervise*, in J. Freeman-M. Minow (eds), *Government by Contract*, cit., p. 293, who states that «[p]ublic involvement is limited to issuing general requirements that providers must meet and conducting periodic reviews». According to the Author, this leads to an even greater default of constitutional accountability, that is, legal accountability that should work as a remedy against abuse of power. According to the state action doctrine, the government is given incentives to extensively delegate its powers to private contractors and avoid accountability.

[87]N. Knust, *Socio-legal foundations*, cit., p. 114.

ships and focusing the attention on information sharing PPPs for law enforcement purposes, it might occur that public authorities' contribution to the agreed-on activities might be of very limited extent, *e.g.*, only concerned with forwarding law enforcement information to the obliged entities that might trigger further investigations about their costumers.

At this point, we are left with questions: does the state action doctrine ensure legal accountability for private actors infringing on constitutional rights when delegated by the state to perform distinct public functions in a regime of public-private partnerships? In those cases, do private entities qualify as public actors and are therefore bound by criminal procedure safeguards?[88]. Whereas the state action doctrine seems unequipped to face «the reality of privatized government»[89], the "private delegation doctrine" advanced by some scholars might instead prove more suitable. According to this theorization, the issue of legal accountability of private actors for fundamental rights' violations should not be addressed in terms of whether a public nexus in private activity exists, but rather whether and to what extent can the state delegate public powers to private actors. In that sense, not only is the state required to oversee the delegated activity, but it should also put in place adequate "nonconstitutional accountability mechanisms" that are able to remedy or redress the infringement to the due process principle in which the private actor has incurred[90]. The constitutional crux is, in other terms, whether the state delegates public powers in private hands, and not whether the private sector performs government actions, according to constitutional requirements.

In the end, it is the state that bears the responsibility to ensure that private entities respond to the human rights violations they commit. This conclusion leads

[88]In the US constitutional system, the term used to refer to fair trial and other rights of criminal procedure is *due process of law*, as established by the Due Process Clause of the Fourteenth Amendment which prohibits the states from depriving «any person of life, liberty, or property, without due process of law».

[89]G. E. Metzger, *Privatization as delegation*, cit., p. 1456.

[90]It is interesting to note that G.E. Metzger, *Privatization as Delegation*, cit., p. 1458, draws the idea of alternative accountability mechanisms from the body of literature on the landmark case of the Supreme Court *Miranda v. Arizona* on the violation of the right against self-incrimination, in which the court formulated the so-called "Miranda warnings" that must be given to suspects of crime prior to police or custodial interrogations unless other fully effective means are provided.

us to address yet another theory developed to explain the effects of human rights in the private sphere, that is, the positive obligations doctrine developed in the case law of the European Court of Human Rights. The theorization of the positive obligations doctrine, also referred to as "duty to protect" doctrine, was indeed greatly influenced by the ideas behind the *Drittwirkung* constitutional theory, insofar as they both aim at expanding the scope of application of fundamental rights to relations between individuals[91].

As known, the Court of Strasbourg has jurisdiction *ratione personae* over the States, in the sense that it can receive individual applications complaining about a violation of the Convention rights only when committed by «one of the High Contracting Parties»[92]. This textual argument had originally been used by the court to declare the inadmissibility of complaints lodged against the behaviors of private actors. The idea that the lack of an express reference to private actors did not imply *a priori* the exclusion of private relations from the scope of application of the Convention and the fundamental rights therein took some time to sink into the jurisprudence of the Court, although some scholars had already advanced the urge to address this gap in the standards of protection[93].

[91]Besides, as noted by K. Kamber, *Prosecuting human rights offences*, cit., p. 37, the parties involved in *X. and Y. v. The Netherlands*, which is one of the first cases in which the Court elaborated on the concept of positive obligations, debated the obligation of the state to take positive action through the *Drittwirkung* doctrine. See the Report of the Commission, *X. and Y. against The Netherlands*, Appl. n. 8978/80, 5 July 1983.

[92]Art. 34 ECHR. This distinctive feature is justified by the historical origin of the Convention system, as explained by C. Loven, *Fundamental Rights Violations by Private Actors and the Procedure before the European Court of Human Rights. A Study of Verticalised Cases*, Antwerp–Gent–Cambridge, 20220, p. 4 and pp. 19-33. It here suffices to mention that the reason why the Convention was designed to mainly address vertical relations, *i.e.*, between the States and private individuals, is that it aimed at protecting individuals against arbitrary and intrusive state legislation or decisions.

[93]In the early 70s, some contended that governments should be held indirectly responsible for human rights violations by private actors. See *D. Xenos*, *The Positive Obligations of the State under the European Convention of Human Rights*, London, 2013, p. 20, where the Author, in the reconstruction of the doctrinal foundations of the positive obligations doctrine, refers to the contribution of J. de Meyer, *The right to respect for private and family life, home and communications in relation individuals, and the resulting obligations for States parties to the convention*, in A. H. Robertson (ed), *Privacy and Human Rights*, Manchester, 1973, p. 273. According to the Author, the horizontal effect of fundamental rights is indeed inherent in the Convention and could be deduced from the wording of the provisions therein pursuant to which "everyone has the right" (Artt. 1, 2, 5, 6, 8, 9, 10, 11, 13) and "no one shall" in (Artt. 3, 4).

However, the Court gradually managed to overcome that idea and increasingly offered protection of Convention rights in relations between private parties[94], in particular by leveraging on the provision stemming from Art. 1 ECHR according to which States Parties are required to secure to everyone within their jurisdiction the rights and freedoms provided for in the Convention. According to the Court, differentiating whether the treatment has been inflicted through the involvement of State agents or private individuals in order to find the Stare responsible would run counter to the obligation to secure everyone's rights. In that sense, in *Cyprus v. Turkey* the Court of Strasbourg rejected the argument of the respondent Government that it lacked jurisdiction over the acts of private parties, stating that «the acquiescence or connivance of the authorities of a Contracting State in the acts of private individuals which violate the Convention rights of other individuals within its jurisdiction may engage that State's responsibility under the Convention»[95].

Following the first cases in the late 1970s[96], the Court of Strasbourg has gradually acknowledged that Contracting States are not only holders of negative obli-

[94]See J. Gerards, *General Principles of the European Convention on Human Rights*, Cambridge, 2023, p. 213, who notes that «over time, however, it has become increasingly clear that power imbalances also exist in private law relationships. The relationship between an employer and an employee is an obvious example, especially if the employer is a large company employing hundreds or thousands of workers. Large companies also may wield significant power in other spheres, for example, by collecting and processing personal data of clients or by creating and using algorithms to selects what information users of social media receive. Over time, it has come to be acknowledged that individuals, groups, organisations and companies may pose just as great a risk to the effective enjoyment of fundamental rights as public bodies and government agents».

[95]ECtHR [GC], 10 May 2001, *Cyprus v. Turkey*, Appl. No 25781/94), § 81. In fact, as the Court notes in § 77, «in terms of Article 1 of the Convention, [the State] "jurisdiction" must be considered to extend to securing the entire range of substantive rights set out in the Convention and those additional Protocols which [it] has ratified, and that violations of those rights are imputable to [it]». More recently, see ECtHR, IV Sect., 6 November 2002, *Sovtransavto Holding v. Ukraine*, Appl. No. 48553/99, § 96, where the Court maintains that «the obligation to secure the effective exercise of the rights defined in that instrument may result in positive obligations for the State [which] cannot simply remain passive». In the literature, see D. Spielmann, *The European Convention on Human Rights: the European Court of Human Rights*, in D. Oliver-J. Fedtke (eds), *Human Rights and the Private Sphere*, cit., p. 431, according to whom the provision under Art. 1 ECHR does not allow the state «to absolve itself from responsibility *ratione personae* by delegating its obligations to private bodies or individuals».

[96]ECtHR, 23 July 1968, *Belgian Linguistic case*, Appl. No 1474/62; ECtHR, 13 June 1979, *Marckx v. Belgium*, Appl. No 6833/74; ECtHR, 9 October 1979, *Airey v. Ireland*, Appl. No 6289/73; ECtHR, 26 March 1985, *X and Y v. the Netherlands*, Appl. No 8978/80.

gations which consist in the duty to abstain from interfering with the fundamental rights of individuals[97], but they also hold positive obligations, which entail the duty of the States to actively protect and guarantee the human rights of individuals against illicit behaviors, irrespective of who commits them[98]. In this regard, the scholarship talks about "horizontal positive obligations"[99] or "indirect horizontal effect"[100] to refere to those cases in which the European Court finds the State in breach of the Convention for having tolereted or not adequatly adverted an infringement of fundamental rights by private individuals[101].

Although the Court did not engage in an accurate definition of the content of the positive obligations, it has clarified that the duty of protection of the States has a twofold nature: it implies both substantive protection, to be pursued by adequate legislative, administrative and regulatory measures providing the framework pursuant to which human rights are ensured *in abstracto*[102], and a procedural limb

[97]Which, as we have seen above, responds to the logic of the classical liberal theory of state. See Section 2.2.

[98]The boundaries between positive and negative obligations are nevertheless not always precise. However, in both cases, regard must be had in particular to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole, subject in any event to the margin of appreciation enjoyed by the State (ECtHR [GC], 12 September 2011, *Palomo Sánchez and Others v. Spain*, Appl. Nos. 28955/06, 28957/06, 28959/06 and 28964/06, § 62. On the dichotomy between positive and negative obligations, see extensively L. Lavrysen, *Human Rights in a Positive State. Rethinking the Relationship between Positive and Negative Obligations under the European Convention on Human Right*, Cambridge–Antwerp–Portland, 2016.

[99]C. Loven, *Fundamental Rights Violations*, cit., p. 77 ff.

[100]J. Gerards, *General Principles*, cit., p. 221 ff.

[101]Some scholars attempted to draw from the case law of the Court a possible categorization of the positive obligations. According to K. Starmer, *Positive Obligations under the Convention*, in J. Lowell-J. Cooper (eds), *Understanding Human Rights Principles*, Portland, 2001, pp. 146–147, these obligations consist in the duty to put in place a legal framework which provides effective protection for Convention rights; the duty to prevent breaches of Convention rights; the duty to provide information that is relevant to a breach of Convention rights; the duty to respond to breaches of Convention rights; and the duty to provide resources to individuals to prevent breaches of their Convention rights. However, cf. L. Lavrysen, *Human Rights*, cit., p. 46, who points out that the infringements committed horizontally, *i.e.* by private individuals, are not contemplated in this categorization.

[102]For instance, in ECtHR [GC], 24 March 2011, *Giuliani and Gaggio v. Italy*, Appl. No 23458/02, § 157 ff. on the alleged violation of Art. 2 ECHR and the right to life infringed upon by the State of Italy for the death of Carlo Giuliani in the poorly-managed demonstrations during the G8 summit held in Genoa in 2001, the Court of Strasbourg first verified whether the legislative, administrative and regulatory framework concerning the use of force was adequate.

of protection, that is, the duty on the State to concretely implement the necessary mechanisms to enforce the substantive content of human rights[103].

In light of the above, some conclusions may be drawn. In the first place, it was highlighted in the literature that the *Drittwirkung* doctrine and the positive obligations doctrine are two distinct, although interrelated, concepts[104]. As seen above, the third-party effect doctrine aims at directly or indirectly holding private actors accountable for human rights violations and thus making them bound by human rights constraints. Instead, the duty to protect elaborated by the case law of the European Court only binds central governments insofar as complaints against other actors but the states are inadmissible, hence «the individual invokes [positive obligations] against the State to oblige State authorities to intervene in horizontal relations»[105].

However, the state positive obligation doctrine is still valuable for the present research. Although the European Court of Human Rights lacks the jurisdiction to directly hold private actors responsible for their infringments of Convention rights, its case law may have a great impact on private relationships and the way governments regulate them. In *Bărbulescu v. Romania*[106], the state was found to be in breach of Article 8 for not having adequately protected the private life and correspondence of an employee who had been monitored by their employer through the recording of the applicant's communications in real time. The Court notes that although Contracting States have a wide margin of appreciation in designing the legal framework on the conditions of employer-employee relationships, this discretion is not unlimited. In fact, it should be assisted by adequate and

[103]When referring to cases involving criminal law mechanisms, the Strasbourg Court translates it into the procedural obligation of public authorites to effectively investigate and prosecute the violation of the human right, as in the official investigation must be prompt, expedite, thorough and carried out independently. See ECtHR, [GC], 2 February 2021, *X and Others v. Bulgaria*, Appl. 22457/16, § 178 ff. in relation to the right not to be tortured or ill-treated pursuant to Art. 4; ECtHR, Sec. I, 10 May 2010, *Rantsev v. Cyprus and Russia*, Appl. 25965/04, § 288.

[104]D. Harris, M. O'Boyle, E. Bates, C. Buckley, *Law of the European Convention on Human Rights*, Oxford, 2009, p. 20

[105]L. Lavrysen, *Human Rights in a Positive State*, cit., p. 78. This is what C. Loven, *Fundamental Rights Violations by Private Actors*, cit., refers to as "verticalisation" of human rights cases.

[106]EctHR [GC], 5 September 2017, *Bărbulescu v. Romania*, Appl. No 61496/08.

sufficient safeguards against abuse. Among the other factors taken into account, the Court mentions the need for prior warnings to the interested party that a possible interference with their fundamental rights might occur or has already taken place[107]. Whereas in the case at stake, the Court determined that the failure of the state to consider the applicable procedural safeguards was to be ascribed to the judgment of the domestic court, states are not precluded from introducing those safeguards in statutory law, be it civil, criminal or labour law, or through other operational and regulatory measures[108].

It is therefore undeniable that the decisions of the Court of Human Rights are significant for private contractual relationships and might therefore disclose an added value in assessing the degree of intrusiveness that banks or other financial institutions might have into their customers' human rights when acting by virtue of public-private agreements with public authorities. It follows that a clearer and more accurate regulation of business relationships that possibly open to serious human rights concerns in criminal proceedings might avoid failures of the governments to comply with their positive obligations pursuant to human rights law. This possibility will be explored in the last section of this chapter.

3 The new legal basis for Public-Private Partnerships for Information Sharing

Following the European Commission's proposal to adopt a legislative package including a number of amendments to the EU AML/CTF regime[109], the EU lawmaker recently adopted a new regulation on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing[110]. The provisions relating to the private sector that were previously contained in the

[107] *Bărbulescu*, cit., § 121.

[108] See J. Gerards, *General Principles*, cit., pp. 224-234 for an overview of the measures suggested by the Court to provide horizontal protection of fundamental rights.

[109] Cf. *supra* Chapter I, Section 3.1.

[110] Regulation (EU) 2024/1624 of the European Parliament and of the Council of May 31, 2024 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing.

Fourth AML Directive have been transposed to the new legislative instrument.

Of particular interest to our objective is Art. 75 Regulation (EU) 2024/1624, headed *Exchange of information in the framework of partnerships for information sharing*, which provides the legal basis for the creation of agreements between public and private parties for the exchange of information with the purpose of combating money laundering and terrorist financing. After a long period where partnerships aimed to assist law enforcement activities could only be established on a voluntary basis[111], as of the entry into force of the regulation, obliged entities and public authorities will be able to establish mechanisms for the sharing and processing of information «for the purposes of preventing and combating money laundering, its predicate offences and terrorist financing, whether at national level or on a cross-border basis, and regardless of the form of that partnership»[112].

Regulation 2024/1624 specifies which entities may participate in an information exchange agreement. Firstly, pursuant to Art. 2(1), 57) an obliged entity is an indispensable member of the PPP as it represents the private element. According to the legal definition, obliged entities are credit institutions, financial institutions, real estate agents, trading and gambling service providers, as well as a number of natural and legal persons who act in the exercise of their professional activities, including notaries, lawyers and other legal freelancers, external auditors, and tax advisors[113].
Compared to the previous provision under Art. 2 Fourth AML Directive, the regulation has broaden the scope of the definition, by including, for instance,

[111]Cf. B. Vogel, *Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing*, in *Eucrim*, 2022, 1, p. 54. As pointed out by G. Lasagni, *Public private partnerships in anti-money laundering and counterterrorism: a new form of outsourcing of the criminal process?*, in *Dir. pen. cont.*, 2021, 3, p. 158, public-private partnerships have always been characterized by voluntariness and informality, which have made them «in some jurisdictions - first and foremost the U.S. - as tools to acquire data held by financial operators, circumventing the limitations related to privileges, for example in the case of subpoena or production orders». However, the same Author warns against the motives underpinning voluntary participation of the private sector in partnerships with public authorities, as the latter always exerts a form of moral suasion on the private sector due to the need to show compliance to public authorities.
[112]Art. 2(1), 57) Reg. (EU) 2024/1624.
[113]Art. 3 Reg. (EU) 2024/1264.

crowdfunding service providers and crowdfunding intermediaries, as well as persons trading or acting as intermediaries in the trade of cultural goods.

Secondly, «where applicable», members of PPPs may be Financial Intelligence Units (FIU)[114], supervisory authorities[115], and a «public authority that has the function of investigating or prosecuting money laundering, its predicate offences or terrorist financing, or that has the function of tracing, seizing or freezing and confiscating criminal assets». As a consequence, the public competent authorities that can take part in a public-private agreement can be public prosecutor's offices, judicial police bodies or specialized branches therein dealing with tracing and recovering proceeds from crime, as well as Assets Recovery Offices (AROs), whose role within national law enfrocement systems has been recently strengthened[116].

From the wording of the recitals, one might infer that Regulation (EU) 2024/1624 in the first place aims to regulate information sharing between obliged entities for the sake of enhancing their detection and prevention abilities by engaging in more or less institutionalized structures such as groups, networks or partnerships[117]. Within these structures, obliged entities should exchange information in particular with credit institutions, financial institutions, and other entities that operate within their networks to better address the threats represented by illicit proceeds

[114]As we saw in Chapter I, FIUs already play an essential role in the AML/CTF system, as they function as a filter between the private sector and competent public authorities when serious suspicions arise that a crime related to money laundering or terrorism financing has been committed. They hold broad powers, among which, as of the entry into force of the Fifth AML Directive, the power to request information to obliged entities even if no prior report is filed.

[115]Following the approval of Reg. (EU) 2024/1620 of the European Parliament and of the Council of May 31, 2024, establishing the Anti-Money Laundering and Anti-Terrorist Financing Authority, the supervisory role over certain obligated entities will be filled centrally by the European Authority (so-called AMLA).

[116]Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation, which replaced Council Decision 2007/845/JHA of 6 December 2007 on cooperation between Asset Recovery Offices of the Member States, requires Member States to set up at least one ARO to facilitate cross-border cooperation in relation to asset-tracing investigations. In particular, AROs are tasked with tracing and identifying instrumentalities, proceeds or property deriving from one of the criminal offences enlisted in Art. 2, which are or might become the object of a freezing or confiscation order issued by a competent authority in another Member State, or to request and exchange information for the purpose thereof.

[117]Recital 45 Reg. (EU) 2024/1624.

that criminals move through chains of intermediaries in order to avoid detection[118].

From this point of view, partnerships were apparently envisaged for obliged entities to disclose information with each other, under the condition that such disclosure only takes place «with regard to the specific transaction that is carried out between or facilitated by those obliged entities, and not with regard to connected previous or subsequent transactions»[119].

However, the regulation resorts to the same organizational structure, this time defined as «public-private partnership for information sharing», when other members beside private actors might be involved, namely competent authorities as defined above. In those cases, the scenario seems to change, as the recitals suggest that the disclosure of information might also involve other relevant data related to the specific suspicious transaction, and that «information sharing should be subject to robust safeguards relating to confidentiality, data protection, use of information and criminal procedure»[120].

Therefore, a mechanism for institutional cooperation, in which risk and knowledge are traditionally shared between peer members, is transplanted into a context inherently different than that for which PPP agreements were envisaged in terms of *ratio* and rules. It is left to see how the binding part of the regulation addresses this apparent contradiction in terms. Several textual references suggest in our opinion that PPPs for information sharing in the AML crime control system were indeed envisaged - and might be dangerously employed - for prosecution purposes.

The first paragraph of Art. 75 specifies that the exchange of information may only occur if strictly necessary for the purpose of fulfilling customer due diligence, control and suspicious transaction reporting obligations, and provided that this is done «in accordance with fundamental rights and judicial procedural safeguards». The same article sets out that where a member of a partnership is a public authority with investigative and tracing, seizing or freezing and confiscating powers, it is obligated to provide, obtain and exchange the information «in accordance with national law transposing Directive (EU) 2016/680 of the European Parlia-

[118]Recital 146 Reg. (EU) 2024/1624.
[119]Ibid.
[120]Recital 147 Reg. (EU) 2024/1624.

ment and of the Council and with the applicable provisions of national criminal procedural law, including prior judicial authorisation or any other national procedural safeguard as required»[121]. Moreover, Art. 75(6) provides in an obscure wording that obliged entities should define in their internal policies differentiated or limited access to information for members of the partnership when the nature of such information or the applicable judicial safeguards so require. The provision unveils the weight attributed by EU lawmakers to the private sector in determining which personal data retrieved from their clients might be used for law enforcement reasons and how the other members of the partnerships, *i.e.* public authorities, can have access to them, thus substantially directing the prosecuting activity entrusted with the investigative authorities and *de facto* acting as their agents.

From the wording of the newly adopted rules, it seems that the *ratio legis* is to go beyond the system of controls and cooperation with obliged entities already outlined by the AML/CTF legislation and marked by a model of prevention according to a risk-based approach as depicted in the previous chapter[122]. In fact, it should be recalled that the information asymmetry shaping the AML/CTF system and the relationship between law enforcement authorities and the financial system[123], requires an assiduous exchange of information that can obviate said asymmetry, and also trust on the reporting entities' abilities to detect suspicious transactions of their clients and share their information[124].

[121]Art. 75(4), lett. *j* Reg. (EU) 2024/1624.

[122]See Chapter I, Section 3.1.

[123]I. Deleanu, *Information flows and repressive enforcement*, in B. Unger-J. Ferwerda-M. Van Der Broek-I. Deleanu (eds) *The economic and legal effectiveness of the European Union's anti-money laundering policy*, Cheltenham, 2014, p. 130. M. Bergström-K. Svedberg Helgesson-U. Mörth, *A New Role for For-Profit Actors?*, cit., p. 1050, clearly illustrate the rationale therein when they state that «[f]irms have control over databases and customer data that, for the most part and during normal circumstances, are outside the reach of public authorities. Hence, the wider the range of businesses engaged in crime prevention, within sectors at risk of being used by criminal elements, the better information authorities will get, it is presumed».

[124]However, according to M. Bergström-K. Svedberg Helgesson-U. Mörth, *A New Role for For-Profit Actors?*, cit., p. 1049, this was not always the case. The private sector acquired a prominent role in the prevention of money laundering in the aftermath of the 9/11 terrorist attacks, since this task was previously entrusted with public actors such as the FATF and the European Union.

However, the involvement of the judicial authority is only potential. In the event that the FIU, which is the recipient of suspicious transaction reports and is entitled to request the necessary information, believes that the funds involved come from criminal activity or are related to terrorism financing, it will forward the results of its analysis to judicial authorities, thus reporting the actual *notitia criminis*. In other words, there is a unilateral flow of personal data from the private sector to the FIU and, in the case of reasonable suspicion of crime, to the judicial authority.

In light of the new provision, doubts arise as to the purely preventive nature of the instrument of public-private partnerships and their appropriateness in a field where criminal prosecution and crime prevention tend to blur and at times overlap. In fact, with the establishment of partnerships for the monitoring of financial flows, a scenario opens up in which, according to a two-way flow of information, the authorities pass on data - not necessarily surging to the degree of evidence yet - gathered in the course of preliminary investigations so that on those basis the obligated entities can provide further details following the analysis of the financial activity and financial profile of the targeted clients. The possible tensions with the principles of criminal proceedings are obvious: while *nulla quaestio* about the fact that the protection of procedural rights is not harmed by the possibility for obligated entities, competent public authorities and supervisory authorities to create cooperation mechanisms aimed at enhancing the exchange of information in the context of CDD (customer due diligence) rules[125], quite different is the case in which the private sector is attributed a proactive role in the search for elements relevant to criminal proceedings on the basis of the information reported by the investigating authorities. In the latter case, the result would be the creation of a mechanism of "externalization" or "subcontracting"[126] of the powers and

[125]As noted by B. Vogel, *Potentials and Limits*, cit., p. 53, the term "public-private partnership" can take on different meanings in the context of AML/CTF legislation, referring on the one hand to agreements focused on criminal investigations, and thus aimed at the involvement of the private sector in directing the investigations, or on the other representing a tool for improving the prevention capacities and systems implemented by obliged entities in order to be up to date on new criminal trends.

[126]Scholars speak of "outsourcing". See G. Lasagni, *Public private partnerships*, cit. p. 153 ff.

prerogatives traditionally in the hand of the judiciary in favor of private parties driven by profit-oriented interests, such as the power to conduct investigations to ascertain criminal facts and to order investigative measures, including - where necessary - coercive measures[127]. The risk of a blank delegation of strictly public functions to these subjects, without the necessary counterbalance represented by the respect for fundamental rights enjoyed by those targeted, calls for an in-depth analysis of the possibility of deeming the principles of fair trial applicable even in the context of partnerships for information sharing. To that end, the principle of *nemo tenetur se detegere*, whose analysis has been conducted in the second chapter, appears paradigmatic, and the cospicuous case law of the European Court of Human Rights might provide some solutions.

4 Do the fair trial rights apply? An attempt to sort it out

The in-depth analysis of the specific features of PPPs conducted so far provided an idea of what consequences their establishment for the detection and prosecution of economic crimes might have on the respect of the fundamental rights of those targeted by financial surveillance operations.

Moreover, the public-private divide inherente to these forms of arrangements led us to address the different conceptualizations of the accountability of the private sector, that have been developed in order to extend the scope of protection of fundamental rights. While this allowed the research to account for the ongoing doctrinal debate around the role of private actors in public governance, the question as of whether natural or legal persons enjoy their right not to provide information contra se in the context of PPPs is still open.

[127]Not only is the private sector not inclined by nature to pursue a public interest, as the prosecution of crimes would be, but also the risk for conflicts of interest is greater where companies, in the expectation to benefit from their participation in the partnership, capture the political will by conditioning its choices. On that note, B. Vogel, M. Lassalle, *Developing Public-Private Information Sharing to Strengthen the Fight against Money Laundering and Terrorism Financing. Recommendations for the European Union*, Freiburg, 2024, p. 18.

In the following section, we will attempt to advance an answer by drawing from the case law of the Court of Strasbourg. Indeed, the Court has proved to endorse in its anti-formalistic case law an extensive understanding of the procedural guarantees to be recognized to individuals affected by the criminal justice system, as well as a broad scope of application thereof. The expansive potential of the protection of fundamental rights as interpreted in the case law of the Court could be upheld in all cases where obligations to cooperate appear in stark conflict with the privilege against self-incrimination and the presumption of innocence, and the case of personal data collected from bank costumers by means of public-private partnerships established between prosecuting authorities and obliged entities may fall within the scope of said cases.

Therefore, it appears necessary to look at the Strasbourg court case law to understand against which subjects and with regard to what evidentiary material the right not to provide information *contra se* can be exercised even in the context of investigative partnerships.

4.1 The subjective scope of application of the privilege against self-incrimination between *matière pénale* and de-risking practices

In order to unravel the issue concerning the subjective scope of application of the privilege against self-incrimination, *i.e.* to understand whether it can be invoked against obliged entities that are members of investigative partnerships, the case law of the ECtHR and its extensive interpretation of the procedural guarantees offered by Art. 6 ECHR might prove useful. In this regard, two points must be made that contribute to the substantive understanding of the concept of "criminal matter" as developed by the court. First, in clarifying that fair trial safeguards apply in all stages of the proceedings, namely from the moment the criminal charge is brought against the person concerned until the final judgment is issued, the ECtHR has developed an autonomous definition of criminal charge, in the sense that it is independent of the meanings attributed to it by the national legal systems of the Member States. According to the conception of the Court, a suspect is considered accused when she is officially notified by the competent

authorities of an allegation that she has committed a criminal offence, that is, when her situation is substantially affected by the authorities[128]. To determine wether the charge is indeed of a criminal nature, the Court analyses the issue in light of the criteria elaborated by the Court to assess the substantially criminal nature of the sanction and, therefore, of the illicit behaviour. We are referring to the so-called *Engel criteria* laid down by the Strasbourg court in the landmark decision *Engel and Others v. The Netherlands*[129], which laid down the test applied by the court to assess the criminal nature of the sanction regardless of the formal qualification in the national legislation.

These criteria include the legal classification of the offence under national law[130], the nature of the offence, and the degree of severity of the penalty that the person concerned risks incurring[131].

Secondly, with specific regard to the privilege against self-incrimination, the Court has developed a two-step test to evaluate whether an issue can arise from the perspective of the privilege against self-incrimination[132]. The first condition

[128]See for instance ECtHR, 27 February 1980, *Deweer v. Belgium*, Appl. No. 6903/75, § 42-46; ECtHR, Sec. III, 8 April 2014, *Blaj v. Romania*, Appl. No. 36259/04, § 74; ECtHR, Sec. I, 18 February 2010, *Aleksandr Zaichenko v. Russia*, ric. 39660/02, § 42-45.

[129]ECtHR [GC], 8 June 1976, *Engel and Others v. The Netherlands*, Appl. No. 100/71; 5101/71; 5102/71; 5354/72; 5370/72. The literature on the Engel doctrine is abundant. Refer to V. Manes, *Profili e confini dell'illecito para-penale*, in *Riv. it. dir. proc. pen.*, 2017, n. 3, p. 988 ff.; P. Caeiro, *The influence of the EU on the "blurring" between administrative and criminal law*, in F. Galli-A. Weyembergh, *Do labels still matter? Blurring boundaries between administrative and criminal law. The influence of the EU*, Brussels, 2009, p. 176 ss.; A. Andri-Jauskite, *Exploring the penumbra of punishment under the ECHR*, in *New Journal of Europe-an Criminal Law*, 2019, 4, p. 363 ff.; A. Weyembergh, N. Joncheray, *Punitive administrative sanctions and procedural safeguards. Blurred picture that needs to be addressed*, in *New Journal of European Criminal Law*, 2016, n. 2, p. 190 ff.

[130]As clearly put by the Court in *Öztürk v. Germany*, 21 February 1984, Appl. No. 8544/79, § 49, «if the Contracting States were able at their discretion, by classifying an offence as "regulatory" instead of criminal, to exclude the operation of the fundamental clauses of Articles 6 and 7 (art. 6, art. 7), the application of these provisions would be subordinated to their sovereign will. A latitude extending thus far might lead to results incompatible with the object and purpose of the Convention».

[131]Each of these criteria was further developed by the Court in its case law. See, *ex multis*, ECtHR [GC], *Öztürk*, cit.; ECtHR [GC], 24 Febbraio 1994, *Bendenoun v. France*, Appl. No. 12547/86; ECtHR [GC], 22 December 2020, *Gestur Jónsson and Ragnar Halldór Hall v. Iceland*, Appl. No. 68273/14 e 68271/14.

[132]The reasoning of the Court was systemically exposed in ECtHR, 30 January 2023, *De Legé v. The Netherlands*, Appl. no. 58342/15, § 65.

to be integrated is that the person be subjected to existing or anticipated criminal proceedings, or that incriminating information compulsorily obtained outside the context of criminal proceedings must be used in a subsequent criminal prosecution. The second condition to be met cumulatively is that there must be some form of improper coercion or compulsion exerted on the person concerned[133].

Therefore, in the Court case law two different scenarios emerge in which a violation of the privilege may arise[134]. On the one hand, the right not to incriminate oneself can be violated when information is extracted during criminal proceedings aimed at collecting evidence; in other words, when the criminal charge has already been brought[135]. In these cases, there are no doubts about the criminal nature of the proceedings and the application of fair trial rights. As a consequence, if the second prerequisite of the test, namely the coercion exercised on the person concerned, is simultaneously satisfied, any statement *contra se* will be deemed covered by the privilege against self-incrimination. Conequently, in the event that the judicial authority has already registered the *notitia criminis* and is therefore carrying out its investigative activity, even by way of an atypical instrument such as a PPP, the obliged entity would act as the *longa manus* of the public authority and therefore all due process guarantees should apply[136], with a possible violation of Art. 6

[133]The Court has identified different cases in which the improper compulsion might occur, *e.g.* where physical or psychological pressure is applied to obtain real evidence or statements, or where the public authorities use subterfuge to elicit information that they were unable to obtain during questioning

[134]ECtHR, 8 April 2004, *Weh v. Austria*, Appl. No. 38544/97, § 41 ff. For an in-depth analysis of this case law,see P. Hirvela, S. Heikkila, *Right to a fair trial. A practical guide to the article 6 case-law of the European Court of Human Rights*, Cambridge, 2021, p. 144 ff.

[135]ECtHR, Sec. IV, 4 October 2005, *Shannon v. United Kingdom*, Appl. No. 6563/03, §§ 34-39

[136]In certain circumstances, the Court has found the privilege against self-incrimination to have been violated even when a suspect or a person under investigation for a crime was not directly compelled by the public authority to provide statements or evidence, but rather indirectly by intermediaries. For instance, see ECtHR, *Allan*, cit., § 45 ff., where the Court found for the violation of the right of the applicant who, while in detention, had been elicited to make confessions of an incriminatory nature by the cellmate who had been previously instructed by the police to record the conversation. In the Court's view, this practice amounts to a subterfuge «to elicit, from the suspect, confessions or other statements of an incriminatory nature, which they were unable to obtain during such questioning», which is inconsistent with the principles enshrined in the Convention. However, the opposite outcome reached in other cases, such as ECtHR [GC], 10 March 2009, *Bykov v. Russia*, Appl. No. 4378/02, § 94 ff., and ECtHR, 9 July 2007, *Heglas v. Ctech Republic*, Appl. No. 5935/02, §§ 89-93, suggests that the indirect improper

ECHR[137].

On the other hand, the Court deemed relevant for the principle of the *nemo tenetur se detegere*, cases in which self-incriminating information has been extracted outside pending criminal proceedings, as in the context of administrative assessments, but used as evidence in subsequent proceedings[138]. According to the European Court, if a clear temporal and material connection exists between the acquisition of information and the formulation of charges[139], the guarantees under Art. 6 ECHR can be considered applicable, as does the privilege against self-incrimination[140], thus satisfying the first of the two requirements provided by the test developed by the court itself. This is the scenario that occurs most frequently in decisions originating from facts concerned with financial matters, in which the imposition of penalties by national tax authorities potentially usable in subsequent criminal proceedings as incriminating evidence has been deemed in violation of Art. 6 ECHR[141]. In light of this, it could be contended that in the event

compulsion is found only in those cases where the applicant had already expressed her will to remain silent, when she is put under physical or psychological pressure, and when the evidence so gathered lies at the core of a finding of guilt.

[137]However, it should be recalled that the Court of Strasbourg is not inclined to find the violation of Art. 6 ECHR in all the cases in which procedural failures arise, but rather only where the overall fairness of the proceeding has been substantially affected and was not compensated for by other factors. Cf. ECtHR [GC], 13 september 2016, *Ibrahim and Others v. United Kingdom*, Appl. No. 50541/08, 50571/08, 50573/08 e 40351/09, §§ 250-251. Such a substantive approach is adopted also in judgments concerning the privilege against self-incrimination, as the Court usually finds a Contracting State in breach of the right where the coercion was apt to extinguish "the very essence" of the privilege. For this purpose, the Court has regard to several factors such as the nature and degree of the compulsion used to obtain the evidence; the existence of any relevant safeguards in the procedure; the use to which any material so obtained is put; and the relevance of the public interest to prosecuting and punishing the illicit conduct at stake. On this point, see ECtHR, *Allan*, cit., § 44; ECtHR [GC], 29 June 2007, *O' Halloran and Francis v. United Kingdom*, Appl. No. 15809/02 and 25624/02, §§ 55-63. Concerning the criterion of the public interest, J. Jackson, *Re-conceptualizing the right of silence as an effective fair trial standard*, in *International and Comparative Law Quarterly*, 2009, n. 4, p. 838, observes the ambiguity in the approaches of the Court, which in *Jalloh c. Germania*, cit., § 107, apparently accepts that the public interest to prosecuting particularly serious crimes might justify the employment of self-incriminating statements to secure the applicant's conviction.

[138]Cf. ECtHR, 16 March 2010, *Elomaa v. Finland*, Appl. No. 37670/04.

[139]«L'article 6 de la Convention sera ainsi applicable lorsqu'une des procédures en cause porte sur une accusation en matière pénale et que les autres lui sont suffisamment liées». ECtHR, Sec. V, 5 April 2012, *Chambaz v. Switzerland*, Appl. No. 11663/04, § 46.

[140]P. Hirvela, S. Heikkila, *Right to a fair trial*, cit., p. 146

[141]Cf. ECtHR, *Chambaz*, cit., § 53; ECtHR, *J.B.*, cit., §§ 63-71; ECtHR, Sec. IV, 4 January

that credit or financial institutions that are members of PPPs request documents or other information from their clients, based on reports made by the judicial authority but without a criminal investigation having been officially initiated, this could fall within the case law of the Strasbourg Court described above when the material and temporal connection with the criminal prosecution is proved.

However, for a matter to be relevant under the privilege against self-incrimination, the second condition identified by the court, that is, the coercion element, must also be satisfied. In this regard, it is widely acknowledged that in commercial and financial practices, the threat of the possible opening of criminal proceedings for money laundering or terrorist financing is not the only element of psychological coercion that comes into play, since the practice of de-risking appears much more critical[142].

De-risking behaviors refer to the phenomenon whereby credit and financial institutions tend to cease or reduce contractual relationships with clients or categories of clients who present excessively high-risk profiles in order to avoid, rather than manage, the risks associated with money laundering[143]. While it is self-evident that such practices are generally adopted autonomously by obliged entities, in the exercise of their economic and business freedom, or for self-protection and convenience[144], it is indeed possible that in the context of PPPs, de-risking

2006, *Shannon v. United Kingdom*, Appl. No. 6563/03, §§ 38-40, in which the applicant had been indicted for false accounting and criminal conspiracy to defraud only a few months after being questioned by a financial investigator by virtue of an Irish security law, which provided for a pecuniary penalty for failing to attend an interview with the competent authority.

[142]L.W. Bachmaier, *Public–Private Collaboration in Criminal Law Enforcement in Spain: Involvement of Private Actors in the Detection and Investigation of Crimes*, in B. Vogel-E. Kosta-M. Lassalle (eds), *Law of Public–Private Cooperation against Financial Crime. Developing Information Sharing to Counter Money Laundering and Terrorism Financing*, Cambridge, 2024, p. 316

[143]FATF, *FATF clarifies risk-based approach: case-by-case, not wholesale de-risking*, Paris, 2023. As pointed out by B. Vogel, *Reinventing EU anti-money laundering. Towards a Holistic Legal Framework*, in B. Vogel-J.B. Maillart (eds), *National and International Anti-Money Laun-dering Law*, cit., p. 960, obliged entities are compelled pursuant to the EU AML/CTF framework to withhold the business relationship or a specific banking transaction if money laundering or terrorism financing risks emerge and to report it to the competent FIU. However, this is not sufficient for the definitive interruption of the relationship.

[144]Indeed, these operations reveal the urge for private entities to show their virtuous behaviours to the judicial and supervisory authorities, just like their participation in public-private partnerships. See G. Lasagni, *Public private partnerships*, cit., p. 164.

activities are to some extent attributable to public authorities[145], thus materializing the risk of the application of a mechanism substantially comparable to a preventive measure[146] or, in any case, a substantially criminal sanction to entire categories of individuals.

In fact, looking at the Engel criteria considered by the Court in applying its test, de-risking practices appear to be particularly afflictive in light of the second criterion, which concerns the nature and scope of the act in question. In this regard, Strasbourg judges considered decisive for assessing the substantially criminal nature of a sanction or a proceeding, factors such as whether the legal rule in question is directed solely at a specific group or is of a generally binding character; whether the proceedings are instituted by a public body with statutory powers of enforcement; and whether the legal rule has a punitive or deterrent purpose[147]. The repercussions that such a scenario entails, both in terms of discriminatory exclusion of these subjects from financial circuits[148] and in strictly procedural terms, are evident. Indeed, from this latter perspective, large-scale state-induced de-risking carried out outside the legal and protective framework offered by the rules of criminal procedure would be inconsistent with defense rights, such as the right to information, the right to silence, the right to be presumed innocent, as well as with the right to an effective judicial remedy.

4.2 The material scope of application of the privilege: PPPs as *fishing expeditions*

It is now necessary to attempt to answer the second question, namely whether, in light of the activity actually carried out by obliged entities to satisfy the re-

[145] B. Vogel, M. Lassalle, *Developing Public-Private Information Sharing*, cit., p. 15.

[146] G. Lasagni, *Public private partnerships*, cit., p. 164.

[147] Cf. ECtHR [GC], 27 November 2006, *Jussila v. Finland*, Appl. No. 73053/01, § 38; ECtHR, *Öztürk*, cit., §53.

[148] See T. Durner, L. Shetret, *Understanding bank derisking and its effects on financial inclusion. Research Report*, 2015, p. 22 ff., where the Authors note how the exclusion of an entire customer base from the formal financial sector because of common traits such as the region of origin, causes the further marginalization of vulnerable groups, such as rural communities, individuals with low financial literacy rates and subjected to criminal activities such as exploitation, slavery, and illicit trafficking.

quests of public authorities, the privilege against self-incrimination can also have its effects in the context of investigative activity carried out through public-private partnerships. The issue plays an important relevance in the case law of the European Court, since it makes a distinction between the types of evidentiary elements that can be covered by the privilege, although the doctrine often struggles to find a logic to such distinction[149]. In other words, even in cases in which the Court acknowledges that the coercion or the threat of sanction occurred in order to collect incriminatory elements, the Court considers that the *nemo tenetur* principle is not violated when these elements may be obtained from the accused through the use of compulsory powers, but the elements have «an existence independent of the will of the suspect»[150]. The so-called "*Saunders exception*", therefore, suggests that the scope of the privilege against self-incrimination would only include testimonial evidence, insofar as it is formed under coercion and in defiance of the will of the person concerned, and not real evidence[151].

[149]For example, S. Lightart, *De Legé v. the Netherlands: clarifying the privilege against self-incrimination?*, in *www.strasbourgobservers.com*, 2022; M. Redmayne, *Rethinking the Privilege Against Self-Incrimination*, in *Oxford Journal of Legal Studies*, 2007; J. Jackson, *Reconceptualizing*, cit. Moreover, the dissenting opinion of Judge Martens in the case *Saunders v. United Kingdom*, cit., is interesting in this regard, as he notices that in the decision of the majorit the two conceptually distinct privilege against self-incrimination, which is a broader safeguard, and right to silence are merged. As the first one consists in the right not to be compelled to provide evidence against themselves, and the second one in the right not to answer to the questions of the authority, it does not appear straightforward that a suspect should be free from coercion to make incriminating statements but not free from coercion to cooperate to furnish incriminating data.

[150]The formulation of this exception to the privilege against self-incrimination is found in *Saunders v. United Kingdom*, cit., § 69, although the this approach dates back to *Funke v. France*, cit., § 44. For an in-depth analysis of the case law of the Court on this matter, see F. Zacchè, *Gli effetti della giurisprudenza europea in tema di privilegio contro le autoincriminazioni e diritto al silenzio*, in A. Balsamo-R.E. Kostoris (eds), *Giurisprudenza europea e processo penale italiano*, Turin, 2008, p. 179 ff.; J.E. Veas, *De Legé v. the Netherlands: The ECHR Adopts A Line Of Reasoning Similar To That Of The United States Supreme Court On Compelled Production Of Real Or Physical Evidence*, in *Maastricht Journal of European and Comparative Law*, 2023, p. 658 ff.; M. Redmayne, *Re-thinking the Privilege Against Self-Incrimination*, cit., p. 214 ff.; C. Conti, *Il corpo dell'imputato come prova: il diritto di non collaborare tra prospettive sovraordinate, suggestioni storiche e polifunzionalità dei dati*, in *Dir. pen. proc.*, 2024, 1, p. 111 ff.

[151]As showed in the previous chapter, Directive (UE) 2016/343 on the presumption of innocence adopts the same approach as that of the Strasbourg Court, since it provides under Art. 7, para. 3 that «[t]he exercise of the right not to incriminate oneself shall not prevent the competent authorities from gathering evidence which may be lawfully obtained through the use of

However, subsequent judgments have identified cases in which real evidence may be deemed in violation of the privilege against self-incrimination and the right to silence. First, where the evidence was obtained by a measure in breach of Art. 3 and the prohibition of torture or inhumane and degrading treatment therein, which constitutes an absolute prohibition which cannot be derogated from, the right not to incriminate oneself remains applicable and fair trial is automatically violated[152]. The second exception, which was formulated in particular with respect to documentary evidence obtained under compulsion in the context of financial investigations[153], concerns the previous knowledge that public authorities have of the evidence sought. According to the Court, if the facts show that the authorities have exerted pressure on the individual to provide pre-existing documents whose existence is only presumed without having certainty of their existence, then the privilege applies. The Strasbourg judges describe this situation as «fishing expeditions», *i.e.*, investigative activities based on mere and unverified suspicions of a possible violation, which, according to the Court, can be compared to testimonal evidence gathered from a person compelled to make a self-incriminating statement on information of whose existence the authorities were not yet aware[154]. Indeed, the Court recalls that it is incumbent on the prosecution in a criminal case to prove their case without recourse to evidence obtained through compulsion in defiance of the will of the suspect or the accused.

The case law on will-dependent and will-independent evidence briefly de-

---

legal powers of compulsion and which has an existence independent of the will of the suspects or accused persons.». In addition, Recital 29) mentions the same types of material evidence that is considered to exist independent of the will of the suspect, such as material acquired pursuant to a warrant, material in respect of which there is a legal obligation of retention and production upon request, breath, blood or urine samples and bodily tissue, although it is unclear whether it is exhaustive or not. On this, see A. Pivaty, A. Beazley, Y.M. Daly, L. Beckers, D. De Vocht, P. Ter Vrugt, *Opening Pandora's box. The right to silence in police interrogations and the Directive 2016/343/EU*, in *New Journal of European Criminal Law*, 2021, 3, p. 337 ff.; S. Lamberigts, *The Directive on the presumption of innocence: a missed opportunity for legal persons*, in *Eucrim*, 2016, p. 38

[152]ECtHR, *Jalloh*, cit., § 100-108; ECtHR [GC], 1° June 2010, *Gäfgen v. Germany*, Appl. No. 22978/05, § 166-168; ECtHR, Sec. II, 25 September 2012, *El Haski v. Belgium*, Appl. No. 649/08, § 85.

[153]ECtHR, *Funke*, cit., § 44; ECtHR, *J.B.*, cit., § 69.

[154]ECtHR, *De Legé*, cit., § 76.

picted above should help understand the operability of the privilege against self-incrimination in PPPs cases. In this regard, we should look into the means that obliged entities have at their disposal to follow up on the requests of public authorities and therefore obtain further information relating to the financial profile of those targeted. There are no specific provisions or prescriptions on how private business should comply with the requests of public authorities, since obliged entities may be required not only to deliver information already in their possession by responding to requests for financial analysis or monitoring, but also to take proactive steps to produce additional information about the targeted customer, for example about the origin of funds, the purpose of a business relationship, the geolocalization of the customer.

In the latter case, private entities could autonomously perform automated checks and decrypt documents[155], or request information directly from targeted clients, either orally or in writing[156]. Following the ECtHR case law, one might consider that the gathering of customers' financial data by obliged entities does not amount to a violation of the privilege against self-incrimination, as such (potential) evidence has an existence independent of the will of the suspect or the accused and therefore was not created as a result of the very compulsion[157] for the purpose of criminal proceedings.

However, there are two exceptions. In the first place, if obliged entities make use of their powers to obtain the making of statements from their customers, orally or in writing; secondly, in the case that public authorities, being unaware of the existence of the elements they are seeking to obtain, and exactly to which obliged entity that is member of the PPP they should forward the request, might engage in a fishing expedition to collect as much financial data as possible to substantiate their investigations.

In these circumstances, it seems that the privilege against self-incrimination should find application and the customers be provided with a protection against

[155]B. Vogel, M. Lassalle, *Developing Public-Private Information Sharing*, cit., p. 103.
[156]B. Vogel, *Potentials and Limits*, cit., p. 58.
[157]As pointed out above, the psychological compulsion may be derived from the threat of discontinuation of the business relationshiop, that is, by the de-risking practice.

the improper instrusion of private businesses.

5 Preliminary conclusions: towards the contractualization of criminal procedure

The present chapter attempted to offer a comprehensive overview of a phenomenon predominantly characterized by its socioeconomic implications, yet whose ramifications are also evident within the criminal procedure realm, which consequently demands scrupulous examination. The involvement of private companies in what are intrinsically public functions and the provision of public services has become a common policy approach. This strategy is beneficial, as it enables public authorities to operate "at arm's lenght", utilize private capital, and accommodate different models of the private sector participation within the public services market, spanning from healthcare to the urban infrastructure sector.

Privatization has therefore become «endemic» in administrative practice[158], with several institutional arrangements between public and private actors being bolstered, among which the establishment of Public-Private Partnerships being favored over other forms of agreement in light of the features analyzed above[159]. The delegation of governmental powers to power- and risk-sharing partners standing on equal footing, as scholars observe, represents a threat to two main clusters of values. On the one hand, privatization has led to a lack of a clear divide between public and private and to the obsolescence of the idea that the two spheres are separate and mutually exlusive[160]. This raises questions on the actual role that private entities do or should play in our society.

On the other hand, the rationale and mechanisms behind privatization of public functions appear at odds with an overarching principle of rule-of-law-based

[158]G. E. Metzger, *Privatization as delegation*, cit., p. 1369.

[159]We saw that, although the categorization is not agreed on unanimously in the literature, PPPs differ from principal-agent agreements in short-term contracts, as well as from traditional contracting out, or privatization *strictu sensu* pursuant to which the state sells or gives in public concession former states-owned enterprises.

[160]What the legal philosopher Norberto Bobbio called la *«grande dicotomia»*, in N. Bobbio, *Stato, governo, società. Per una teoria generale della politica*, Turin, 1985.

systems, that is, constitutional accountability of formally and - as it is contended - substantially public authorities. In the absence of answerability of private actors that are being delegated traditional public powers, one is compelled to inquire about the instruments or protective mechanisms at the disposal of interested parties for the assertion of their rights and freedoms.

We have attempted to address these concerns by applying the *Drittwirkung* doctrine on the horizontal effects of fundamental rights, which is known by different names in other legal systems, such as the state action doctrine in the US constitutional scholarship or the doctrine of positive obligations in the case law of the Court of Strasbourg. What can be drawn from these different, yet interrelated, theorizations can be briefly summarized as follows.

Individuals can demand the respect of their fundamental rights in vertical relations, insofar as states and governmental authorities have the duty to refrain from encroaching upon them, but also in horizontal relationships, as states are equally recognized a duty to actively prevent private parties to violate the fundamental rights of others. Ultimately, it is the state's responsibility to oversee functions and activities delegated to private actors, which is enforced either directly through state responsibility or by ensuring private individuals' accountability.

Furthermore, the state must implement robust safeguards against abuse through statutory provisions, either civil, criminal, or labor law, or through other operational and regulatory measures.

Two main considerations can be drawn from the above. First, «government by regulation is the inevitable concomitant of government by proxy»[161], meaning that contractual arrangements appear to be the main instrument pursuant to which public authorities can perform their practice of delegating powers.

Second, although states to a certain extent hold a margin of appreciation in designing the private relationships under their jurisdiction, they cannot let fundamental rights be infringed upon in the context of said contractual arrangements, and should therefore be able to effectively regualate business relationships so as to

[161] H. Seidman, R. Gilmour, *Politics, Position and Power. From the positive to the regulatory state*, New York, 1986.

ensure legal accountability that should work as a remedy against abuse of power.

The following questions thus arise: What kind of arrangement (legally binding private or public contract? Memorandum of Understanding? Protocol?) do PPPs for information sharing in AML/CTF legislation envisage between banks or financial institutions and public prosecuting authorities? Moreover, should checking account contracts or other financial contracts provide for clauses specifically regulating rights and duties of the parties, that may have a relevance for future potential criminal investigations? In the end, are we heading towards the contractualization of criminal procedure? The topics require further analysis.

Regarding the nature of arrangement that should substantiate the rights and obligations stemming from a PPP between judicial or law enforcement authorities and obliged entities, we should acknowledge that there are no uniform approaches, as the choice of the contractual framework is usually demanded to the negotiations between the parties. Moreover, consistent evidence lacks for legally binding, and, therefore, enforceable kinds of arrangements within the criminal justice system. Although this line of research might reveal interesting profiles to be further explored, it will be set aside in this context, in order to focus on other aspects.

As for the second question, *i.e.*, whether business agreements between banking and financial market professionals and individual customers can *contractualize* features traditionally related to criminal proceedings, a twofold kind of content can be envisaged. Obliged entities might be obliged to higher transparency and disclosure standards on i) their participation in a PPP with investigating authorities and the national FIU for information sharing; ii) what such circumstance actually entails, *i.e.*, the potential indiscriminate transfer of sensitive data to the law enforcement and *viceversa*, and iii) the possible use of said financial data for evidentiary purposes in criminal proceedings and the consequences therefrom.

On this last point, it seems but appropriate that obliged entities should therefore include in their contracts the rights and remedies that the law grants to individuals when faced with (*de iure* or *de facto*) criminal investigations, among which, for instance, the right against self-incrimination and the right to silence. A contractual clause of that sort, which indeed resembles the *Miranda warnings* that the judicial police is obliged to provide in the US legal system to those suspected of crime, would empower customers to oppose to the use of incriminating infor-

mation in subsequent criminal proceedings and, therefore, to activate effective judicial remedies in courts.

Someone may object that this practice would bring about nothing but lengthy business procedures while also discouraging persons from using legal banking channels. Quite to the contrary, this would by far reduce the need for obliged entities to resort to de-risking practices against alleged high-risk profiles, insofar as other remedial mechanisms would be in place. Discriminatory practices would therefore be discouraged, and proper roles be re-established: criminals would consequently resort to, and reinforce, the shadow economy to carry out money laundering or terrorism financing activities, whose prosecution and repression is exactly what law enforcement and judicial authorities are tasked with, who are required to repress crime, while leaving the role of preventing the financial market from, and alerting the authorities of, threats of crime to for-profit actors.

The second scenario concerns the design of the rights of the customers. If we assume that, as potential persons suspected of crime, they must be granted the right against self-incrimination and all fair trial rights in general, can we also contend that they should be able to give them up pursuant to a contractual clause? This opens up to a much broader debate taking place in the human rights literature in general, that is, the waiver of fundamental rights. It refers to a situation in which an individual explicitly or implicitly relinquishes protection under a specific known right, either substantial or procedural[162], as part of their autonomy in exercising the rights and freedoms granted to them.
The debate on the possibility for individuals to waive their rights sees two opposite visions, one contending that human rights cannot be waived in any case as they are conferred on individuals in the public interest[163] which is referred to as "interest theory", and the other one invoking the freedom and autonomy of

[162]F. Shalhaei, *The anatomy of a valid waiver of human rights*, in *Human Rights Law Review*, 2025, 25(2), p. 2.

[163]According to L. G. Loucaides, *Questions of fair trial under the European Convention on Human Rights*, in *Human Rights Law Review*, 2003, 3(1), p. 49, waiver of right would actually be impossible, as they do not represent personal prerogatives that can be disposed of or negotiated. In line with that, individuals may decide not to exercise the rights granted to them but could never renounce them and give up the possibility to raise a claim for their violation.

individuals ("will theory").

From the standpoint of the European Court of Human Rights on the matter, waivers of certain convention rights might indeed exist, but in order to be valid, they must meet specific conditions. In fact, in its case law[164], the ECtHR has first of all recalled that not all fundamental rights can be derogated from, since Art. 15, § 2 ECHR makes derogation not possible for Artt. 2, 3, 4 § 1 and 7[165]. The Court also clarified that waivers must be established in an «unequivocal manner»[166], exercised «knowingly and intelligently»[167], that is, on the basis of informed consent[168], and voluntarily, *i.e.* without any form of coercion or com-

[164]For the most part, the decisions addressing the issue of the waiver of rights concern procedural rights under Art. 6 ECHR. L. Caflisch, *Waivers in International and European Human Rights Law*, in M. H. Arsanjani-J. Cogan-R. Sloane-S. Wiessner (eds), *Looking to the future: Essays on international law in honor of W. Michael Reisman*, Leiden, 2010, p. 422.

[165]«This happens, in particular, when individuals purport to waive "core" human rights, that is, those belonging to the realm of *jus cogens*, or those that cannot be suspended in times of crisis or emergency». *Ibid.*

[166]In the sense that the formulation or the intentions must be clear and unambiguous. See ECtHR, Sec. III, 1 March 2016, *Tabbane v. Switzerland*, Appl. No. 41069/12, where the Court found that a contractual clause pursuant to which the parties agreed not to seek judicial remedy but resort to arbitration represented a valid waiver.

[167]This formulation resembles the standard adopted by the US case law on the waivability of fundamental rights, according to which constitutional rights may ordinarily be waived only if it can be established by clear and convincing evidence that the waiver is voluntary, knowing, and intelligent. On the waiver doctrine in the american literature, see S. Grossi, *The Waiver of Constitutional Rights*, in *Houston Law Review*, 2023, 60(5), pp. 1021-1066; Leslie W. Abramson, *Witness Waiver of the Fifth Amendment Privilege*, in *Oklahoma Law Review*, 1988, 41(235), pp. 235-256.

[168]More specifically, it means that the right-holder must be previously informed of the fundamental right granted to him and must also foresee the consequences of waiving that right. As conveniently explained in ECtHR [GC], 1 March 2006, *Sejdovic v. Italy*, Appl. No. 56581/00, § 87 on the right to participate at trial, «where a person charged with a criminal offence had not been notified in person, it could not be inferred merely from his status as a "fugitive" (latitante), which was founded on a presumption with an insufficient factual basis, that he had waived his right to appear at the trial and defend himself (see *Colozza*, cited above, § 28). It also had the occasion to point out that, before an accused can be said to have implicitly, through his conduct, waived an important right under Article 6 of the Convention, it must be shown that he could reasonably have foreseen what the consequences of his conduct would be». See also ECtHR, Sec.enge III, 31 August 2016, *Ganking and Others v. Russia*, Appl. nos. 2430/06, 1454/08, 11670/10 and 2938/12, para. 38. The Court resorted to the special protection of the "knowing and intelligent waiver" standard especially in cases involving the right to legal assistance, which is considered a fundamental right among those that constitute the notion of a fair trial. However, it also referred to it in ECtHR, *Ibrahim and Others*, cit., para. 272 on the right against self-incrimination.

pulsion[169]. Moreover, waivers should not go against any important public interest and should be attended by minimum safeguards commesurate to the importance of the specific right.

In light of the points made in the chapter and following the judgments of the Court of Strasbourg, it can be argued what follows.

First, Public-Private Partnerships between prosecuting authorities and obliged entities for information sharing in the AML crime control system exacerbate the blurring of boundaries between prevention and repression, especially in those legal systems where a clear-cut distinction between criminal proceedings and administrative or preventive proceedings does not exist[170], with the subsequent (ab)use of such instruments for investigative purposes.

Secondly, be as it may, individuals who enter into a business relationship with an obliged entity which is member to a PPP with law enforcement should therefore be aware of the circumstance, as, differently than how the system currently works, it implies a two-way flow of information that could enable investigating authorities to entrust private actors with the task to search for evidence or, worse, for suspicions of crime, on their behalf.

In the third place, customers should therefore also be informed of the rights granted to them by law during criminal investigations, insofar as it could not be ruled out the fear of them being considered susepcts all along. This information should be provided as soon as possible, *i.e.* in the contract agreement whereby the checking account agreement or other financial contract is established.

Finally, being fair trial rights not absolute, the parties may negotiate to include a contractual clause to waive the right against self-incrimination, whereby the right-holder relinquishes the right not to contribute to her guilty plea, as long as such waiver is unequivocal, genuine, and freely agreed. In a judgment, the Court found that a pre-printed form delivered by the police to a suspect of crime in which legal assistance was ruled out was invalid, which suggests that the waiver

[169]To verify the absence of any form of constraint, the Court weighs several circumstantial factors, varying from the detention in police custody to the economic costraint. See ECtHR, 27 February 1980, *Deweer v. Belgium*, Appl. No. 6903/75, §§ 48-54.

[170]G. Lasagni, *Public private partnerships*, cit., p. 159.

of the right against self-incrimination should be discussed between the parties, personally signed by the customer, and accompanied by adequate safeguards, *e.g.* legal counsel.

Chapter IV

Drawing a conclusion: towards a comprehensive regulation of financial investigations

1 Key findings

The research conducted so far has resulted in the conceptualization of several key findings, which in part address the guiding subquestions that set the stage for the present work. Before coming to the conclusions and identifying the challenges ahead, it is now necessary for the sake of clarity to summarize the answers to such questions below.

What do we mean by (criminal) financial investigations?

Through the analysis of the relevant international legal frameworks, it was observed that there is no binding legal definition of financial investigations. These are rather to be interpreted as an umbrella concept, covering any «enquiry into the financial affairs related to a criminal activity, with a view to identifying the extent of criminal networks and/or the scale of criminality; identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and developing evidence which can be used in criminal pro-

ceedings»[1]. In light of the broadness of the concept, financial investigations can be both employed to support traditional criminal investigations into allegations of money laundering, predicate offences or terrorism financing, and to substantiate the ultimate goal of the AML/CTF preventive system aimed at preventing the abuse of the financial system for money laundering or terrorism financing purposes. However, we also observed how the "twin-track approach" adopted within the EU framework in countering the ML/CT threats does not allow for a clear-cut distinction between prevention and prosecution, with the consequential blurring of purposes, tools, and stakeholders involved. This is the key point substantiating the concerns addressed by this work, insofar as procedural safeguards stemming from criminal law might irremediably be downplayed, if not obviated, by resorting to the preventive framework to carry out law enforcement and prosecuting functions.

Can there be financial investigations without the private sector?

In light of the in-depth study of the structure and purposes of financial investigations, the question should be answered in the negative. With the shift from a rule-based approach to a risk-based one in the field of AM/CTF legislation, policy makers increasingly rely on the collaboration of the private sector by granting it broad leeways of discretion in identifying what these risks are and delegating to profit-driven actors the power to design and implement AML control mechanisms. Obliged entities, that is, firms, banks and other credit institutions and financial intermediaries, are required to comply with the obligations to put in place ongoing due diligence measures aimed at profiling their customers and their level of risk, and to report to competent authorities (that is, to FIUs) every case in which they know, suspect or have reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing. The private sector therefore plays a pivotal role in detecting potential ML/CT conducts, as it smoothly provides public completent authorities with vast amounts of information without them having to resort to cumbersome procedures and requests, as is the case for subpoenas or production orders.

[1]Interpretative Note to FATF Recommendation 30.

In this sense, the datafication of socioeconomic spheres taking place in our societies clearly contribute to enhancing the position of private actors in policy fields that do not traditionally belong to them, such as in crime control. As human relations increasingly occur in a digital context and much of what we are, we do or aim at, passes through money flows and banking transactions, inquiries into the financial affairs of individuals have risen to the status of the privileged instrument for law enforcement and judicial authorities to prevent criminals from benefiting from the proceeds of their illicit conducts. Therefore, since all actors involved in the financial system, be it banking institutions, financial intermediaries or even legal professionals, hold vast amounts of first-hand data about their customers which puts them in an "informational asymmetry" with law enforcement, their involvement in the fight against "dirty money" is in constant expansion.

How can financial investigations be consistent with the right of customers/suspects of crime and obliged entities not to provide information *contra se* stemming from the criminal procedural framework?

In the second chapter of this work, the two paradigmatic frameworks on the right not to provide self-incriminating information in the context of criminal investigations have been examined, namely the case law of the Court of Strasbourg in interpreting Art. 6 ECHR, and the Presumption of Innocence Directive together with some key decisions of the Court of Justice addressing the issue. This preliminary study helped sheding light on the standards of protection afforded to the *nemo tenetur* principle, and setting the stage for the main question to be addressed, as of whether and to what extent customers subjected to financial surveillance for law enforcement reasons, as well as obliged entities, enjoy any right not to provide information *contra se*.

As for the former issue, we tried to demonstrate how it is particularly problematic in light of the stringent cooperation duties falling on obliged entities operating in the financial system by virtue of AML/CTF legislation. However, drawing for the CJEU case law, namely the *DB v. Consob* in which the Court held that the privilege against self-incrimination shall be protected also in non-puntitive proceedings insofar as «the evidence obtained in those proceedings may be used in criminal proceedings against that person in order to establish that a criminal

offence was committed»[2], it was maintained that the limitation of fundamental rights for other compelling interests, such as national security, cannot be tantamount to depriving subjects of their minimum rights. This brought us to claim that when customers and obliged entities that are natural persons are faced with financial inquiries that might lead to them providing FIUs with self-incriminating information, they should be given notice of such circumstance and, therefore, the option not to contribute to their own incrimination, as the duty, whose non-compliance can be criminally or administratively sanctioned, would constitute improper compulsion. This would hold all the more true when confronted with judicial- or law enforcement-type FIUs, in light of the stricter conncection to the criminal justice system.

In the case of customers or obliged entities being legal persons, the issue remains open as these have not been recognized procedural safeguards by the Court of Justice, hence the urge for the Court to intervene on the matter.

What differences to the way financial investigations are conducted are brought about by the introduction of public-private partnerships for information sharing?

The third chapter mainly revolved around this research question, as it addressed the impacts that the establishment of PPPs for information sharing in the context of ML/TF prevention might have for the protection ofprocedural safeguards. To that aim, the exact meaning of PPP, as one of the forms by which privatization can be obtained, was explored by drawing from different bodies of literature, namely administrative law literature. The features of such models, in particular the loose regulation and permanent trust and reciprocity between the members in order to ensure the long-term existence of the cooperation mechanism, suggested that PPPs in the context of the AML crime control system would exacerbate the blurring of boundaries between prevention and repression, especially in those legal systems where a clear-cut distinction between criminal proceedings and administrative or preventive proceedings does not exist, with the subsequent (ab)use of such instruments for investigative purpose. Furthermore, being

[2] *DB*, cit., para 44.

clear how banks and financial intermediaries would operate as *de facto* judicial authorities to which prosecuting functions could be outsourced, it was claimed that these should be held responsible for their actions, thus envisaging a shift in accountability dynamics when information sharing PPPs are in place. Insofar as accountability works as a remedy against abuse of powers, we envisaged an accountability mechanism which passes thorugh contractual clauses that could be negotiated between banking institutions and their customers, providing the latter with the necessary information on the existence of a PPP for information sharing in which the company participates, and the rights granted to them - *e.g.*, the right not to provide information *contra se*. The establishment of PPPs for information sharing would bring about several differences in the way financial investigations are conducted, as they could lead to a form of *contractualization* of criminal procedure, according to which the parties could negotiate repsective rights, duties, and remedies.

2 What is still missing: data protection implications of financial investigations

Grounded in criminal and procedural law literture, the research conducted so far focused on the implications of financial investigations for the procedural safeguards stemming from the right to a fair trial. The polymorphus and composite nauture of financial investigations, however, compels one to take into account the data protection concerns arasing therefrom.

In fact, it should not be neglected that financial investigations, in all forms they may take, entail access to confidential information «which allows an intimate insight into the person's daily life and habits [and which] has a connection to a person's health, sex life, and political opinions or religious persuasion»[3]. In this sense, these may potentially infringe upon the fundamental rights to private life

[3]J. Milaj, C. Kaiser, *Retention of Data in the New Anti-Money Laundering Directive - 'Need to Know' versus 'Nice to Know'*, in *International Data Privacy Law*, 2017, 7(2), p.119.

and data protection enshrined in Art. 8 ECHR and Artt. 7 and 8 CFREU[4]. The right to data protection is particularly relevant for this research, as the focus so far has been centered on *who* collects financial information that might have an

[4]The scope of the foregoing does not allow us to delve into the scholarly debate around the different scope of protection stemming from the right to privacy and the right to data protection. However, some remarks appears to be necessary in this regard. Whereas some authors deem these rights to be interchangeable, others claim that they do intersect to some extent but eventually protect different interests. Following the conceptualization of P. De Hert, S. Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in E. Claes-A. Duff-S. Gutwirth (eds), *Privacy and the Criminal Law*, Antwerp-Oxford, 2006, pp. 61-104, the right to privacy shall be interpreted as the "right to opacity" (hence, the definition as an «opacity tool») or the "right to be left alone", insofar as it protects individuals and their private life and home from state interference and interferences from private actors, which is clearly enshrined in Art. 7 CFREU and Art. 8 ECHR. See also S. Gutwirth, P. De Hert, *Regulating profiling in a democratic constitutional state*, in M. Hildebrandt-S. Gutwirth (eds), *Profiling the European Citizen*, Cham, 2008, pp. 271–293. To the contrary, the right to data protection goes beyond the protection of intimacy and actually operates at a different level, as it aims to set out the procedural requirements that need to be complied with in order for the processing of personal data to be in accordance with law, such as the access to data, the right to control or oversight over the processing of data, the right to rectify them, etc. In this sense, the right to data protection operates as a transparency tool «to increase the transparency of information flows and to limit them in order to prevent disproportionate informational power relationships to be developed or perpetuated between public and private data controllers and citizens» (A. Rouvroy, Y. Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, S. Gutwirth-Y. Poullet-P. De Hert-C. de Terwangne-S. Nouwt (eds), *Reinventing Data Protection?*, Cham, 2009, p. 70). In this sense, Art. 8 CFREU is clear in acknowledging the protection of personal data as a fundamental right (S. Rodotà, *Data Protection as a Fundamental Right*, in S. Gutwirth-Y. Poullet-P. De Hert-C. de Terwangne-S. Nouwt (eds), *Reinventing Data Protection?*, cit., pp. 77-82) insofar as it establishes that «[e]veryone has the right to the protection of personal data concerning him or her». Other classifications are based on the substantive nature of the right to private life and the right to privacy on one hand, and the procedural nature of the right to data protection (N.N. Gomes de Andrade, *Oblivion: The Right to be Different ... from Oneself: Re-Proposing the Right to be Forgotten*, in A. Ghezzi-A. Guimaraes Pereira-L. Vesnic-Alujevic (eds), *The Ethics of Memory in a Digital Age. Interrogating the Right to be Forgotten*, London, 2014.). For an exhaustive overview of the different positions in the literature, see P. Vogiatzoglou, P. Valcke, *Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data protection in EU law*, in E. Kosta-R. Leenes-I. Kamara (eds), *Research Handbook on EU Data Protection Law*, Chelthenam, 2022, pp. 22-29; M. Tzanou, *Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures*, in *Journal of Internet Law*, 2013, 17, p. 26 ff; O. Lynskey, *Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order*, in *International and Comparative Law Quarterly*, 2014, 63, p. 569-597; J. Kokott, C. Sobotta, *The distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 2013, 3(4), pp. 222-228.

incriminating nature, *how* such data is gathered - namely what, if any, procedural safeguard is granted to targeted individuals - and *for what* purpose. In this sense, notwithstanding the different conceptualizations that were offered in the literature, data protection is conceived as a catch-all term referring to the rights of data subjects to have their data processed fairly, according to their consent, and for specified purposes.

The recognition of the right to data protection as a fundamental, and (quasi) constitutionalized right by the Charter[5] is to be attributed to national experiences and EU secondary legislation, according to an «unconventional expansive bottom-up approach»[6]. As for the former, the most remarkable initiative towards the construction of a data protection right is uncontestedly traced back to the landmark decision of the German Constitutional Court (*Bundesverfassungsgericht*) in 1983, in which the Court debunked the narrow concept of the right to privacy, and referred to the fundamental values of dignity, autonomy and self-developement in order to put forth the idea of a right to informational self-determination to be understood as «the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others»[7].

Informational self-determination, therefore, is conceived as the right of control over personal data, which data subjects should be able to exert throughout all the stages data processing, with the consequence that «every step of processing

[5]R. Gellert, S. Gutwirth, *The Legal Construction of Privacy and Data Protection*, in *Computer Law and Security Review*, 2013, 29, p. 522; L. Dalla Corte, *A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection*, in D. Hallina-R. Leenes-S. Gutwirth-P.De Hert (eds), *Data Protection and Privacy, Volume 12: Data Protection and Democracy*, Oxford, 2020, p. 37.

[6]M. Brkan, *The Unstoppable Expansion of the EU Fundamental Right to Data Protection: Little Shop of Horrors*, in *Maastricht Journal of European and Comparative Law*, 2016, 23(5), p. 815.

[7]BVerfGE 65, 1 – Volkszahlung, 15 December 1983, as reported in A. Rouvroy, Y. Poullet, *The Right to Informational Self-Determination*, cit., p. 45. The Authors argue that the concept of informational self-determination entails that «an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said 'self-determined'». For a reflection over the right to informational self-determination in the German legal culture, where it was conceived and elaborated, see M. Albers, *Realizing the Complexity of Data Protection*, in S. Gutwirth-R. Leenes-P. De Hert, (eds), *Reloading Data Protection*, Cham, 2014, pp. 213-235.

must be based either on consent or on a costitutional legal basis»[8]. Conceived as a right with a strong societal component rather than an individualistic right[9], informational self-determination is one of the interests underpinning the right to protection of personal data, as also acknowledged by European Courts[10]. A brief overview of ECtHR and CJEU case law appears then necessary.

In the case law of the Court of Strasbourg, an extensive interpretation of the concept of "private life" has been elaborated, which shall not be limited to the inner circle of intimacy, but rather comprises the right to establish and develop relationships with other human beings, and therefore includes activities of professional or business nature[11]. This broad interpretation is also attested by the fact that, according to the Court, «information retrieved from banking documents undoubtedly amounts to personal data concerning an individual, irrespective of it being sensitive information or not» and therefore falls under the notion of both "private life" and "correspondence", whose breaches amount to an illegal interfer-

[8]Ibid., p. 219.

[9]Cf. S. Rodotà, Data Protection, cit., p. 79, who confers an individualistic nature to the right to privacy, as it ensures that others do not interfere with one's personal sphere, while arguing that the right to data protection entails a redistribution of social and legal powers insofar as data subjects are no longer the only ones responsible for data processing, but independent authorities are envisaged. See P. M. Schwartz, *Beyond Code for Internet Privacy: Cyberspace Filters, Privacy control, and Fair Information Practice*, in *Wisconsin Law Review*, 2000, p. 787, where the idea of "information privacy" is conceived as a «constitutive value that safeguards participation and association in a free society».

[10]P. De Hert, S. Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in S. Gutwirth-Y. Poullet-P. De Hert-C. de Terwangne-S. Nouwt (eds), *Reinventing Data Protection?*, cit., p. 19.

[11]ECtHR, 16 December 1992, *Niemietz v. Germany*, Appl. No 13710/88, § 29; ECtHR, 25 June 1997, *Halford v. The United Kingdom*, Appl. No 20605/92, § 42; ECtHR, Sec II, 27 October 2004, *Sidabras and Džiautas v. Lithuania*, Appl. Nos 55480/00 and 59330/00, § 45. The Court has drawn this broad interpretation from the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2). See ECtHR [GC], 16 February 2000, *Amann v. Switzerland*, Appl. No 27798/95, § 65. On the case law of the European Court, see R. Sicurella, V. Scalia, *Data Mining and Profiling in the Area of Freedom, Security and Justice: State of Play and New Challenges in the Balance between Security and Fundamental Rights Protection*, in *New Journal of European Criminal Law*, 2013, 4(4), pp. 409-460.

ence for the purposes of Art. 8 ECHR[12].

However, financial and other personal data are not only protected by the Convention in their privacy dimension, but also in view of data protection implications. In including personal data in the notion of private life[13], the Court of Strasbourg has even gone further in embracing a broad and dynamic interpretation of the rights enshrined in Art. 8 ECHR[14] by considering that the mere storing of data related to the private life of an individual amounts to an interference pursuant to Art. 8. In order to assess that, «the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained»[15].

Building on that finding, and on the positive obligations that fall on States Parties bound by the Convention[16], the Court envisaged specific rights that precisely relate to data protection, whose infringement on the part of the State or private actors might lead to the violation of Art. 8 ECHR. In so doing, the Court has included in the material scope of Art. 8 ECHR issues strictly related to the right to data protection, ranging from ensuring access to information stored systematically about the interested party within a reasonable time and through an effective and accessible procedure[17], to the right to oversight by an independent

[12]See ECtHR, 7 July 2017, *M. N. v. San Marino*, Appl. No 28005/12, § 51; ECtHR, Sec. III, 22 December 2015, *G. S. B. v. Switzerland*, Appl. No. 28601/11, § 51; ECtHR, Sec. V, 27 July 2017, *Sommer v. Germany*, Appl. No. 73607/13, § 59; ECtHR, 1 March 2016, *Brito Ferrinho Bexiga Villa-Nova c. Portugal*, Appl. No 69436/10, § 44. The idea is shared by G. Lasagni, *Banking supervision and Criminal Investigation: Comparing the EU and US Experiences*, Cham, 2019, p. 334.

[13]L. Tomasi, *sub. Art. 8*, in S. Bartole-P. De Sena-V. Zagrebelsky (eds), *Commentario Breve alla Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali*, Padua, 2012, p. 299.

[14]In order to face the new challenges posed to human dignity and privacy especially by technological advancement. Cf. A. Rouvroy, Y. Poullet, *The Right to Informational Self-Determination*, cit., p. 61.

[15]ECtHR [GC], 4 December 2008, *S. and Marper v. the United Kingdom*, Appl. No 30562/04 and 30566/04, § 67.

[16]P. De Hert, S. Gutwirth, *Data Protection in the Case Law*, cit., p. 17. Cf. *supra*, Chapter III, Section 2.2, where the positive obligations doctrine was analyzed.

[17]*Haralambie v. Romania*, 2009, § 79; *Jarnea v. Romania*, 2011, § 50; *Joanna Szulc v. Poland*, 2012, § 87; *Gaskin v. the United Kingdom*, 1989, § 49

authority in surveillance case law[18].

As for the EU framework, a parallel can be drawn between financial data and digital traffic and content data, which has been in the spotlight of the Court of Justice for the high relevance it has gained vis-à-vis IT developments[19]. This case law revealed that «the retention of and the access to data which make it possible to depict essential aspects of the private life of individuals bring to a serious interference with their right to private life and the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter»[20]. However reluctant the CJEU has been so far to draw a clear-cut distinction between data protection and privacy[21], it has acknowledged in its case law that a series of requirements must be complied with by public authorities willing to process personal data.

For instance, the Court held that the processing of electronic communication

[18]ECtHR, 24 April 1990, Huvig v. france, Appl. No 11105/84; ECtHR, Sec. III, 29 June 2006, *Weber and Saravia v. Germany*, Appl. No 54934/00; ECtHR [GC], 25 May 2021, *Big Brother Watch and Others v. The United Kingdom*, Appl. No 58170/13, 62322/14 and 24960/15; ECtHR, 4 May 2000, *Rotaru v. Romania*, Appl. No 28341/95. For an in-depth analysis of the European Court's surveillance case law and its implications for the right to protection of personal data, see P. De Hert, G. Malgieri, *One European legal Framework for Surveillance: the ECtHR's expanded legality Test Copied by the CJEU*, in V. Mitsilegas-N. Vavoula (eds), *Surveillance and Privacy in the Digital Age*, Oxford, 2021, pp. 256-284.

[19]The reference is to the so-called Data Retention Saga, namely a series of rulings of the CJEU delivered on the EU legal framework concerning the access to and retention of electronic communication data by public authorities for the purposes of criminal prosecution and by digital service providers. The first ruling is judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, where the Court found in para. 27 that data, «taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them». Among others, judgment of 21 December 2016, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970; judgment of 2 March 2021, *H. K. v. Prokuratuur*, C-546/16, ECLI:EU:C:2021:152.

[20]L. Bernardini, F. Sanvitale, *Searches and seizures of electronic devices in European criminal proceedings: a new pattern for independent review?*, in *Revista Ítalo-Española de Derecho Procesal*, 1, p. 109. Cf. CJEU, judgment of 6 October 2020, *La Quadrature du Net*, Joined Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, para. 117.

[21]M. Albers, *Realizing the Complexity*, cit., p. 224; H. Kranenborg, *Article 8*, in S. Peers-T. Hervey-J. Kenner-A. Ward (eds), *The EU Charter of Fundamental Rights. A Commentary*, London, 2021, p. 242, who observes how the CJEU adopts a «classical fundamental rights approach» in always referring to the right to privacy rather than to the right to data protection.

data does not infringe on the essence of the right to data protection[22] insofar as «appropriate technical and organisational measures against accidental or unlawful destruction, accidental loss or alteration of the data» are envisaged[23]; if access to personal data by public authorities is proportionate to the seriousness of the criminal offence investigated and prosecuted[24] and subjected to prior review by a judge or an independent administrative body[25]; if the possibility for data subjects to pursue effective legal remedies is envisaged in national legislation[26].

In the following, specific fundamental principles of data protection law will be briefly outlined before presenting the pieces of EU secondary legislation and addressing the issue as to which legal framework applies in financial investigations.

2.1 Core principles: fairness of processing and purpose limitation

The principle of fairness processing has been conceived as the cornerstone of data protection law, insofar as it gives origin to the other fundamental principles[27]. According to Art. 8(2) CFREU, data must be processed *fairly*. The fairness of data processing is one of the most fundamental principles in data protection law, inasmuch as it enables data subjects to gain awareness of the way their data is processed, *i.e.*, to understand «how their personal data are handled, as regards the identity of the controller, the purpose of the processing, as well as the risks, rules, safeguards and rights in relation to the processing activities and how they

[22] This case law of the Court of Luxembourg especially pivotes around the notion of "essence" of the fundamental right to data protection, insofar as according to Art. 52(1) CFREU it must always be respected in cases of limitations (that is, instrusions) on the exercise of fundamental rights. See P. Vogiatzoglou, P. Valcke, *Two decades of Article 8 CFR*, cit. p. 33 ff.

[23] *Digital Rights Ireland*, cit., para 40.

[24] Judgment of 2 October 2018, *Ministerio Fiscal*, Case C-207/16, ECLI:EU:C:2018:788, para 51.

[25] Judgment of 4 October 2024, *CG v Bezirkshauptmannschaft Landeck*, Case C-548/21, ECLI:EU:C:2024:830, para 110.

[26] Judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650, para 95.

[27] L. A Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague, 2002, p. 58.

can exercise those rights»[28]. The principle therefore refers to the relationship between the data subject and the data controller[29], which should be informed by the respect for the necessity and proportionality of the interference[30].

However, the fairness principle is not limited to the re-balancing of said relationship, but it also ensures that procedural fairness requirements are adopted[31] to empower data subjects[32]. In this sense, the fair processing of data warrants the implementation of procedures and measures that envisage procedural safeguards for data subjects and the respect for their rights, such as informational duties of the data controller, the right to notification and the right to object data processing[33].

When it comes to financial surveillance pursuant to the AML/CTF preventive framework, the principle of fair processing of data meets several limitations. In the first place, as will be seen in the following section, the level of transparency, which is entrenched with the fairness principles, greatly differs depending on the applicable data protection regime, in that Directive (EU) 2016/680 on the processing for law enforcement purposes does not envisage any transparency requirement in light of its specific objective. It follows that, when the data controller processing financial data is subjected to such directive, instead of the general data protection framework stemming from Regulation (EU) 2016/679, it is not bound by the obligation to process data «in a transparent manner», to make the information related to data processing and the specific purposes thereof clear and easily accessible.

[28]M. Catanzariti, *Data protection: Handbook on Techniques of Judicial Interaction in the Application of the EU Charter*, Florence, 2021, p. 16.

[29]Fundamental Rights Agency, *Handbook on European Data Protection Law*, Luxembourg, 2018, p. 118.

[30]M. Brewczyńska, E. Kosta, *The EU Data Protection Framework*, in B. Vogel-E. Kosta-M. Lassalle (eds), *Law of Public-Private Cooperation against Financial Crime*, Cambridge-Antwerp-Chicago, 2024, p. 444.

[31]D. Clifford, J. Ausloos, *Data Protection and the Role of Fairness*, in *Yearbook of European Law*, 2018, 37, p. 132.

[32]On the vulnerability of data subjects and how data protection principles address such vulnerability, see G. Malgieri, *Vulnerability and Data Protection Law*, Oxford, 2023.

[33]It should be pointed out that the principle of fairness, although often interlinked to, goes beyond the principle of transparency, which for instance does not apply in cases of data processing for law enforcement purposes. For the analysis of Dir. (EU) 2016/680 see below, Section 2.2.

Furthermore, as already observed[34], the AML/CTF system is marked to a great extent by confidentiality duties falling on obliged entities and FIUs, preventing them from disclosing to customers/suspects that they are being targeted by data processing for whatever reason, as well as by the erosion of bank secrecy, with the consequent indiscrimante sharing of information with public authorities.

Therefore, AML/CTF legislation allows for the restriction, in whole or in part, of the right of the persons concerned to access their personal data, to ensure that investigation into money laundering is not jeopardized, or to enable competent authorities and obliged entities to carry out their functions, «to the extent that such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned»[35]. In light of these prohibitions of disclosure[36], AML/CTF legislation does not envisage any right of data subjects to be notified of their data being processed for AML/CTF purposes, notewithstanding the high importance that the Court of Luxembourg has recognized to notifications insofar as it enables «the persons affected to exercise, inter alia, the right to a legal remedy»[37].

With regard to other procedural fairness requirements, the AML/CTF legislation does not envisage any mechanism for customers to object to the surveillance of their bank accounts, nor to be exempted from it[38]. Moreover, the retention period envisaged by the provisions raises concerns vis-à-vis the proportionality requirement, since it is prescribed that financial documents and information should be retained for a period of 5 years commencing on the date of the termination of the business relationship[39], with a possible extension of 5 years if the need for the prevention, detection, investigation or prosecution of money laundering or terrorist financing is proven by Member States. As highlighted by the EDPS when the proposal for the Fourth AML Directive was put forth by the Commission, the «chosen data retention period should correspond to a demonstrated necessity of

[34] See *supra*, Chapter II, Section 2.
[35] Art. 41(4) Dir. (EU) 2015/849.
[36] See Art. 39 Dir. (EU) 2015/849 and Art. 73 Reg. (EU) 2024/1624.
[37] *Tele2*, cit., para 121.
[38] J. Milaj, C. Kaiser, *Retention of Data*, cit., p. 122.
[39] Art. 40(1) Dir. (EU) 2015/849; Art. 77(3) Reg. (EU) 2024/1624.

keeping the data for a certain amount of time» on a case-by-case basis[40].

Connected to the principle of transparency is the principle of purpose limitation, also considered as a cornerstone of data protection[41]. As stated in the previous section, the right to data protection centers on the control of data subjects over who processes their personal data and for what purposes. The purpose limitation principle establishes that personal data must be collected for specified, explicit and legitimate purposes and that their further processing for purposes other than the original ones shall be allowed only if compatible with those purposes[42]. Influenced by social, as well as political norms[43], the purpose specification principle has been enshrined in Art. 8 CFREU, whose second paragraph states that «data must be processed fairly for specified purposes»[44], and in secondary law provisions[45]. In this sense, the principle constitutes a limitation to the powers of the data controller[46] and a safeguard against its abuse, insofar as it is obligated to specify the purpose of processing, to make it explicit, and to process data in accordance with the law[47]. The features outlined above suggest the similarities

[40]EDPS, Opinion on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds, 2013, para 27.

[41]Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, April 2013, p. 4; T.H.A. Wisman, R.J.L. Tijm, *The Radical Reframing of the Purpose Limitation Principle – Why the Dutch Delegation Uprooted Data Protection*, in E. Kosta-R. Leenes-I. Kamara (eds), *Research Handbook on EU Data Protection Law*, cit., p. 355.

[42]Cf. M. Catanzariti, *Data protection*, cit., p. 18.

[43]H. Beate Bentzen, *Context as key: The protection of personal integrity by means of the purpose limitation principle*, in E. Kosta-R. Leenes-I. Kamara (eds), *Research Handbook on EU Data Protection Law*, cit., p. 384-385.

[44]See P. Vogiatzoglou, P. Valcke, *Two decades of Article 8 CFR*, cit., p. 20, on the controversy as to whether Art. 8 CFREU attributes greater values to the data protection principles and rights referred to therein.

[45]See the following section.

[46]According to the European Data Protection Supervisor (EDPS) Glossary, the data controller is «the party that, alone or jointly with others, determines the purposes and means of the processing of personal data (...) responsible for the lawfulness of the processing, for the protection of the data, and respecting the rights of the data subject». Data controller must be differentiated by the data processor, who is the natural or legal person who processes the data on behalf of the controller, following strict instructions. However, in both cases they bear a legal responsibility for complying with the respective obligations pursuant to data protection rules. Cf. Fundamental Rights Agency, *Handbook on European Data Protection Law*, cit., p. 101.

[47]As recalled by H. Beate Bentzen, *Context as key*, cit., p. 386, the purpose limitation

that the purpose specification principle shares with the informational or evidential specialty rule that was analyzed in the second chapter[48], as they both constitute a use limitation for information (and evidence) gathered for one original specific purpose[49].

Within the AML/CTF legislative framework, Art. 41(2) Fourth AML Directive establishes a purpose limitation insofar as it states that «[p]ersonal data shall be processed by obliged entities on the basis of this Directive only for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 and shall not be further processed in a way that is incompatible with those purposes»[50]. As suggested by the following sentence, the rationale of such provision is that of prohibiting the processing of financial data for commercial purposes. However, the purpose limitation principle in the context of AML/CTF investigations seems to be destined to be undermined, insofar as the original anti-money laundering objective increasingly becomes less determinate[51] and other purposes for data processing emerge, such as prosecuting predicate offences, analytical purposes, countering tax evasion, supervision of financial markets, etc. In addition, a multitude of data controllers with different structures, resources, and constitutive purposes is by the AML/CTF provisions, which increases the uncertainity as to the purposes for which data are processed.[52].

Furthermore, with regard to the establishment of PPPs for information sharing, the EDPS pointed out that data processed in the context of partnerships might lead to the risk of discriminatory financial exclusions of targeted customers, that is de-risking practices, insofar as obliged entities might employ law enforce-

principle also finds its roots in Art. 8 ECHR, where the need for a legal basis for an interference to be lawful is underlined.

[48] *Supra*, Chapter II, Section 4.2.

[49] On the need to keep them separated, see G. Vermeulen, M. Kusak, *Unblurring the Fuzzy Line Between Specialty and Data Protection in EU Mutual Legal Assistance After the European Investigation Order*, in *European Journal on Criminal Policy and Research*, 2023, 29, pp. 647–667.

[50] Cf. Art. 79 Reg. (EU) 2024/1624.

[51] EDPS, Opinion 1/2017 on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC with regards to the Commission Proposal for the Fifth AML Directive, 2 February 2017, p. 9.

[52] Ibid., p. 8

ment data for business operations[53].

All of the above raises concerns about the compatibility of the AML/CTF legislative framework with data protection principles, as also interpreted by the case law. However, we should now move onto addressing EU secondary legislation on data protection to assess whether data subjects rights, with specific regard to their right not to provide personal data against their will, or their knowledge thereof, are respected.

2.2 EU data protection frameworks and the never-ending discourse around the applicable regime

The EU data protection framework preceding the entry into force of the Lisbon Treaty was composed of a first-pillar instrument providing the general regulation for the processing of personal data[54], and a third-pillar instrument specifically addressing data processing in the context of law enforcement and police cooperation in criminal matters[55]. In the aftermath of the Lisbon Treaty and the abolishment of the three-pillars structure, a comprehensive legal basis for data protection in all EU sectors pursuant to Art. 16 TFEU[56], which indeed constituted the legal basis for the two instruments proposed in 2012 by the Commission[57] and eventually enacted in 2015[58].

[53]EDPS, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, 23 July 2020, para. 46. See also M. Brewczyńska, E. Kosta, *The EU Data Protection Framework*, cit., p. 450.

[54]Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/3.

[55]Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350.

[56]E. Kosta, *A divided European data protection framework: A critical reflection on the choices of the European legislator post-Lisbon*, in E. Kosta-R. Leenes-I. Kamara (eds), *Research Handbook on EU Data Protection Law*, cit., p. 69.

[57]See Commission proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final.

[58]see E. Kosta, *A divided European data protection framework*, cit., pp. 68-89 who carries out an assessment of the soundness of the EU lawmaker's choice to follow a "package approach" in adopting two different instruments at the same time, rather than extending the scope of application of the GDPR to data processing for law enforcement purposes.

Regulation (EU) 2016/679[59] (hereafter: GDPR) generally covers any processing of data of natural persons by wholly or partly automated means, and explicitly excludes from its scope of application the processing of personal data the purposes of the prevention, investigation, detection or prosecution of criminal offences[60]. Accordingly, Directive (EU) 2016/680 (hereafter: LED)[61] applies to the processing of personal data by competent authorities «for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security»[62]. However, the demarcation of the material scope of these instruments is not clear-cut *in abstracto*, and it is practically demanded to national legislators, insofar as the applicability of the LED depends on the definition of "competent authority" and "criminal offences" in domestic legislation[63].

Although the two instruments share similar features when referring to some data protection principles, such as purpose limitation, fairness, and data minimization[64], the ways they regulate data processing are remarkably different. To illustrate that, some examples will be given.

[59]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119.

[60]Cf. Art. 2(2) GDPR.

[61]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119. For the historical background of the LED, see M.R. Leiser, B.H.M. Custers, *The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680*, in *European Data Protection Law Review*, 2019, 5(3), pp. 367-378.

[62]Cf. Artt. 1(1) and 2(1) LED.

[63]H. Kranenborg, *Article 2 - Material Scope*, in C. Kuner-L.A. Bygrave-C. Docksey (eds), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, 2020, p. 70. The issue of the material scope of application of the data protection regimes at stake, whereby the GDPR constitutes the *lex generalis* and the LED is a piece of *lex specialis*, has been widely addressed in the literature due to the different levels of safeguards these frameworks entail. While a thorough analysis of the material scope of the instruments falls outside of the scope of the research, the main points will be addressed in the analysis of the applicable regime to FIUs

[64]See M. Brewczyńska, E. Kosta, *The EU Data Protection Framework*, cit., p. 433; M.R. Leiser, B.H.M. Custers, *The Law Enforcement Directive*, cit., p. 372 ff.

To begin with, the principle of lawfulness is dealt with in a different manner. The principle provides that data processing is legitimate only insofar as it is justified or permitted by law[65]. In this sense, the legal grounds for data processing, *i.e.* the basis upon which it is legitimate for the data controller to process data, differ. While the GDPR provides for six different legal grounds of processing, including consent of the data subjects[66], the LED provides that processing is lawful only if and to the extent that «[it] is necessary for the performance of a task carried out by a competent authority» for law enforcement purposes[67]. Furthermore, no reference to the duty of transparency is made in the LED, in light of the specific objectives of the processing conducted thereon, in light of the idea that transparency in criminal pre-trial investigation phase might hamper the effectiveness of the investigation itself.

Another striking difference concerns the reach of the rights and safeguards envisaged for data subjects by the two frameworks. The GDPR provides in Chapter III a set of rights, including the right to receive transparent information about the data processing[68], the right to access to information about data processing and the personal data processed[69], the right to rectification, erasure, and restriction of processing[70], the right to data portability[71], the right to object[72], and the right not to be subject to automated decision-making[73]. Furthermore, the regulation allows for a restriction of any of these rights pursuant to Art. 23, to the extent that such exception is provided by law, is aimed at pursuing one of the objectives exhaustively listed in the GDPR, and «respects the essence of the fundamental

[65]As enshrined in Art. 8 CFREU, according to which «data must be processed (...) on the basis of the consent of the person concerned or some other legitimate basis laid down by law».

[66]See Art. 6 GDPR.

[67]Art. 8 LED. While consent does not constitute one possible legal ground for data processing, M.R. Leiser, B.H.M. Custers, *The Law Enforcement Directive*, cit., p. 375, claim that the LED does not entirely exclude consent from its scope, insofar as it forms the basis for the data subjects rights, however restricted, envisaged by the directive.

[68]Artt. 12, 13 and 14 GDPR.

[69]Art. 15 GDPR.

[70]Artt. 16, 17 and 18 GDPR.

[71]Art. 20 GDPR.

[72]Art. 21 GDPR.

[73]Art. 22 GDPR.

rights and freedoms and is a necessary and proportionate measure in a democratic society»[74].

Although the LED follows the structure of the GDPR in acknowledging certain data subjects rights, such as the right to information, the right to access data and the right to rectification, erasure, and restriction of processing, it sets out «a basic filter under which all individual rights to information, access and rectification will be exercised», *i.e.* the obstruction of official or legal inquiries, investigations or procedures[75]. This means that the transparency and informational rights set out in the LED are not absolute but are subject to several limitations to protect the confidentiality of criminal proceedings[76].

All of the above suggests that the LED sets out a more flexible regime of personal data processing by data controllers, insofar as it establishes lower thresholds of protection for data subjects rights, broader margins for data controllers in re-

[74]Art. 23(1) GDPR. Among the explicit conditions laid out by the provision, Art. 23(1), lett. d) envisages the purposes of the «the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security». However, as suggested by Recital 19, since this restriction applies to data processing that falls within the scope of GDPR, it concerns processing activities for law enforcement purposes but that are not carried out by competent authorities as defined by the LED.

[75]P. De Hert, V. Papakonstantinou, *The New Police and Criminal Justice Data Protection Directive. A First Analysis*, in *New Journal of European Criminal Law*, 2016, 7(1), p. 13.

[76]T. Marquenie, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, in *Computer Law and Security Review*, 2017, 33, p. 332, who nevertheless concludes that the LED provides for satisfactory safeguards for data subjects insofar as it requires restrictions to be established by law and necessary and proportionate in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned. Moreover, Art. 17 LED provides that in cases of restrictive measures, data subjects may exercise their rights through the supervisory authoritity. On the same note, T. Quintel, *Follow the Money, if you can – Possible solutions for enhanced FIU cooperation under improved data protection rules*, University of Luxembourg Law Working Paper No 2019-001, p. 10, who deems the LED adequately formulated to strike a fair balance between fundamental rights and law enforcement activities, notwithsanding the margins of flexibility granted to competent authorities. In this sense, the provision under Art. 25 LED according to which competent authorities are required to keep logs of at least six processing activities - collection, alteration, consultation, disclosure including transfers, combination and erasure - grants additional transparency and controllability safeguards to data subjects. On the logging provision, see further J. Sajfert, T. Quintel, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, in M. Cole-F. Boehm (eds), *Commentary on the General Data Protection Regulation*, Cheltenham, 2018.

stricting data subjects rights without the duty to provide a justification thereof and less stringent transparency obligations. This appears to be at odds with the general trend registered among the measures adopted with the aim of realizing an Area of Freedom, Security and Justice, as these generally strengthen the protection of fundamental rights[77] and are, therefore, extensively interpreted. On the contrary, the LED regime entails harsher rules for the fundamental right to data protection compared to those stemming from the GDPR, and should therefore be limited «to the areas where specific rules are really necessary»[78]. This leads us to address the issue of the applicable data protection regime in financial investigations into money laundering and terrorism financing, more specifically when FIUs and private entities, that is, obliged entities, are involved.

Within the landscape of EU data protection regimes[79], the GDPR and the LED set out the regulatory frameworks potentially applicable to the AML/CTF field, which is admittedly one of the clearest examples of the blurring lines be-

[77]As is the case for the instruments adopted pursuant to Art. 82(2) TFEU, as noted by M. Brewczyńska, *A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation*, in E. Kosta-R. Leenes-I. Kamara (eds), *Research Handbook on EU Data Protection Law*, cit., p. 105.

[78]EDPS, Opinion 6/2015 on A Further Step towards a Comprehensive EU Data Protection. EDPS Recommendations on the Directive for Data Protection in the Police and Justice Sectors, 28 October 2015, p. 6.

[79]In addition to those stemming from the GDPR and the LED identified above, other specific regulations on data processing exist. *E.g.*, these include Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC OJ L 295 21.11.2018; Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016; Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA OJ L 135 24.5.2016; Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, OJ L 312.

tween their scopes of applicability[80], especially in light of the different nature of the actors involved therein. Focusing on data processing activities that involve FIUs, it should be noted in the first place that a straightforward disposition on the matter is missing[81], and that the main interpretative crux lies in the variety of institutional models — administrative, law enforcement or judicial — adopted by Member States for their respective units, which have consequences over the structure of FIUs and their relationship with judicial and law enforcement authorities[82]. For FIUs to fall within the material scope of application of the LED, two conditions should be cumulatively satisfied, *i.e.*, the processing of personal data must be carried out by a "competent authority" and for law enforcement purposes[83]. As for the personal scope, the definition of "competent authority" is provided for by the directive, and it shall mean «any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security», or any other body or entity entrusted to exercise public authority and public powers for the same purposes[84]. Albeit no doubts arise as to the publicness of FIUs, there is no agreement on their similarity with traditional law enforcement authorities such as police or criminal justice authorities, which fall under the first category[85] and this is regardless of the formal institutional status of FIUs[86]. Admittedly, FIUs, at least law enforcement ones,

[80]M. Brewczyńska, E. Kosta, *The EU Data Protection Framework*, cit., p. 413.

[81]According to Art. 43 Dir. (EU) 2015/849, the applicable data protection regime for AML/CTF purposes is the GDPR, although it also states under Recital 42) that it is without prejudice to the legislative framework on data processing in the law enforcement context. Moreover, Dir. (EU) 2019/1153 on facilitating access to financial information for law enforcement purposes provides that both the GDPR and the LED are relevant to it «in their respective scope of application».

[82]For the features of the different models, see *supra* Chapter I, Section 2.2.

[83]Cf. Artt. 1 and 2 LED.

[84]Art. 3(7) LED.

[85]M.M. Caruana, *The Reform of EU Data Protection framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement*, in *International Review of Law, Computers and Technology*, 2019, 33(3), p. 253.

[86]M. Brewczyńska, *Financial Intelligence Units: Reflections on the applicable data protection legal framework*, in *Computer Law and Security Review*, 2021, 43, p. 11, according to whom three main differences occur between traditional law enforcement authorities and FIUs, namely the lack of independence, the lack of judicial oversight over FIUs activities and decisions, and

might fall under the second type of "competent authority" under the LED, insofar as they are entrusted with public authority and public, that is (some) coercive, powers[87], including the power to freeze suspicious transactions and seize assets[88]. However, the already mentioned lack of harmonization across Member States on the powers that FIUs have at their disposal entails higher levels of uncertainty. For this reason, it was contended that the applicable data protection framework shoul not be determined upon the nature of the data controller, *i.e.*, FIUs, but rather upon the purpose of the data processing according to a function-oriented approach[89]. This leads to the second condition for the application of the LED, notably the material scope of application, which covers the purposes of preventing, investigating, detecting or prosecuting criminal offences, and executing criminal penalties. The text of the directive neither provides a definition of these law enforcement tasks, nor defines what a criminal offence is for the purpose of the LED, rather referring to the «autonomous concept of Union law as interpreted by the Court of Justice of the European Union»[90].

Being as it may, although not univocally agreed upon[91], FIUs' rationale appear suitable to serve law enforcement purposes, insofar as these bodies collect and

---

lastly the limited scope of accountability for FIUs.

[87]P. De Hert, J. Sajfert, *Variety, velocity and volume of personal data in criminal investigations and proceedings: the limits drawn by the purpose limitation and data minimization principles in Directive (EU) 2016/680*, in V. Mitsilegas-M. Bergström-T. Quintel, (eds), *Research Handbook on EU Criminal Law*, Chelthenam, 2024, p. 223.

[88]T. Quintel, *Follow the Money*, cit., p. 7

[89]F. Mouzakiti, *Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive*, in *New Journal of European Criminal Law*, 2020, 11(3), p. 369.

[90]Recital 13 LED. See M. Brewczyńska, *A critical reflection*, cit., p. 108 ff.

[91]See F. Mouzakiti, *Cooperation between Financial Intelligence Units*, cit., p. 367, who upholds the idea that FIUs activities do satisfy the material scope of application of the LED, however acknowledging the different stance on the issue undertaken by the European Commission. In fact, according to the Commission, FIUs are to be regarded as "publi administration". Cf. EU FIUs Platform, *Minutes of the 35th Meeting of the EU FIUs Platform*, 8 June 2018. See also Commission, *Report from the Commission to the European Parliament and the Council – Assessing the Framework for Cooperation between Financial Intelligence Units*, COM (2019) 371 final. On slightly different notes, M. Brewczyńska, *Financial Intelligence Units*, cit., p. 13, who maintains that the data protection regime applicable to FIUs is the GDPR, as these do not carry out law enforcement tasks, but rather act in support of them. However, the Author does not radically rule out the application of the LED to instances where FIUs take up an actual law enforcement role.

analyze information received «with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing»[92], and also in view of their powers to obtain information from obliged entities regardless of the previous submission of SARs. Furthermore, a decisive factor to be considered in assessing whether FIUs might be said to carry out law enforcement tasks concerns the powers granted to them to access law enforcement data «where the information is necessary for the prevention, detection and combating of money laundering, associate predicate offences and terrorist financing»[93], and to exchange financial infomration and financial analysis with competent authorities requesting them for the prevention, detection, investigation or prosecution of serious criminal offences[94]. Directive (EU) 2019/1153 furthermore addresses the transnational exchange of financial information between FIUs of different member States, which can occur in urgent cases «for the processing or analysis of information related to terrorism or organised crime associated with terrorism»[95]. According to the scholarship, this rule attests to the criminal law purpose of FIU data exchange and, therefore, to their law enforcement nature of the tasks performed[96].

In view of the above, and also considering that across the EU landscape most FIUs apply the LED to their data processing activity, it seems that the longstanding debate should be solved for the application of the LED regime, regardless of the institutional nature of the FIUs in question and only in view of the purpose of data processing. This practically means that FIUs, whether of an administrative, police or judicial type, should be required to process data pursuant to the

[92]Recital 37 Dir. (EU) 2015/849 and Recital 64 Dir. (EU) 2024/1640.

[93]Art. 8 Dir. (EU) 2019/1153.

[94]Art. 7(1) Dir. 2019/1153. The Directive also provides under Art. 10 that competent authorities that have obtained financial data from their national FIUs can exchange such data with their counterparts abroad when it is necessary to combat money laundering and terrorism financing.

[95]Art. 9(1) Dir. (EU) 2019/1153

[96]V. Mitsilegas, *EU Criminal Law*, Oxford, 2022, p. 557. In addition to that, it shall be pointed out that Dir. (EU) 2019/1153 was adopted under the legal basis provided for by Art. 87(2) TFEU which is a criminal law provision, notably on police cooperation. See, F. Mouzakiti, *Cooperation between Financial Intelligence Units*, cit., p. 357.

LED regime when they do so for law enforcement tasks[97], and on the contrary they should apply the GDPR when processing data for purposes not related to law enforcement.

More critical, and less debated in the literature, is the question concerning what data protection regime applies to obliged entities when they collect, analyze, and eventually transfer to competent authorities financial data gathered from their customers for law enforcement purposes. In this sense, Recital 11 LED seemingly provides a straightforward answer, insofar as it states that «Regulation (EU) 2016/679 (...) applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject» and, to illustrate this circumstance, refers to financial institutions retaining personal data and providing them to competent authorities in accordance with the law. However, the recital continues by affirming that the LED regime indeed applies to bodies or entities which process personal data on behalf of such competent authorities by virtue of a contract or other legal act, in that in those cases the provisions on data processors stemming from the LED apply. The reference to the fulfillment of a legal obligation binding the private party might be interpreted as suggesting that the establishment of a PPP for information sharing could entail the application of the LED data protection regime also to obliged entities that are members of a partnership together with competent authorities, and this would be in line with the conclusions drawn in the third chapter. In that circumstance, after an in-depth analysis of the rationales and features of PPPs, against which the various doctrines on the horizontal effects of fundamental rights were applied[98], we contended that private actors that take part in PPPs act as *de facto* agents of law enforcement authorities and should be held accountable accordingly. Thus, it would seem consequential that the data protection regime applicable to them in the context of PPPs is the LED, but this is admittedly still controversial.

While some authors contend that in no circumstance can private actors be

[97]As argued by T. Quintel, *Follow the money if you can*, cit., p. 11, «FIUs, by preventing criminal activity, would fall within the scope of the LED».

[98]Chapter III, Section 2.2.

considered data controllers under the LED[99], others claim that the privatization wave taking place in the law enfrocement field, evidenced by the establishment of PPPs, might open up to a scenario in which private actors are considered as competent authorities pursuant to Art. 3(7), lett. b, LED, *i.e.* as a «body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences»[100]. However, other scenarios arise which depend upon the specific configuration of the PPP, and, therefore, the structure of the partnership, as well as the allocation of decision-making and risk-sharing[101]. The more controllership over data processing is entrusted with the private members of the PPP, and are therefore recognized with public powers and public authority, the more likely it is that they act as joint controllers under the LED together with public authorities.

The provision establishing the legal basis for information sharing PPPs in the AML/CTF context does not offer details on what specific configuration these PPPs should have. However, it stems for Art. 75 Regulation (EU) 2024/1624 that information exchanges in the framework of a partnership should mostly concern categories of data collected by obliged entities, including information on customers, on the purpose and intended nature of the business relationships or occasional transactions, information on risk factors, etc. Moreover, it is prescribed that the obliged entities are entrusted with an assessment as to the necessity of the information exchange for the purposes of the established partnership[102]. These provisions seem to signal the intention of the EU legislator to include obliged entities within the criminal justice system, or to externalize traditional law enforcement functions to them. Accordingly, the LED data protection regime should

[99] M. Brewczyńska, E. Kosta, *The EU Data Protection Framework*, cit., p. 429.

[100] The idea is put forth by N. Purtova, *Between the GDPR and the police directive: Navigating through the maze of information sharing in public-private partnerships*, in *International Data Privacy Law*, 2018, 8(1), p. 62, according to whom this latter provision «looks into the future and anticipates changes in the national approaches to law enforcement along the lines of the current trend of privatization and PPPs, in particular, privatization of policing (...)».

[101] N. Purtova, *Between the GDPR and the Police Directive*, cit., p. , identifies six different parameters to assess the configuration of information sharing within PPPs, including ground of information sharing, degree of structure, degree of centralization, party releasing information, jurisdictional and sector boundaries.

[102] Art. 75(3) Reg. (EU) 2024/1624.

apply.

The potential application of the LED data protection regime to obliged entities taking part in PPPs for information sharing, however, should not in any case enable private parties to circumvent the data protection restrictions stemming from the GDPR generally covering private data processing[103]. This means that the safeguards and data subjects' rights enshrined in the LED should be strenghtened and effectively enforced to the possible extent. In the next section, where the takeways of the research will be consolidated, the specific right to object data processing will be accounted for, in light of the undeniable connection it shared with the *nemo tenetur se detegere* principle.

3 Contributions and recommendations for a prospective framework on financial investigations

The overarching rationale of the research was to explore whether and to what extent customers of financial and banking services enjoy any leeways of self-determination in deciding not to provide personal information that might jeopardize their position before law enforcement and judicial authorities. Through the lenses of criminal procedure law, this pertains to the right that suspects and defendants have not to provide information *contra se*, commonly referred to as the "privilege against self-incrimination". The privilege is embodied in the broader principle *nemo tenetur se detegere*, according to which no one shall be compelled to harm herself, also encompassing the right to silence. While the latter more precisely is attached to defendants and covers any kind of contribution, whether incriminating or not, whereas the privilege only concerns incriminating information, these two safeguards equally orbit the concept of silence as a form of control over data and information coming from individuals. This led to address the data protection implications that any form of interference into one's personal sphere has, and the enquiries into the financial affairs of customers are no exception. In this sense, through the lenses of data protection law, data subjects must be

[103]N. Purtova, *Between the GDPR and the Police Directive*, cit., p. 60.

enabled to exert control over who, what, where, and why their personal data are processed, and potentially to object to the use of that information. The idea of silence as a form of control over personal data, which would therefore be relinquished in cases of compulsory self-incrimination, is in line with the majoritarian take in the literature according to which privacy «is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves»[104].

The analysis of the AML/CTF preventive system showed how the control of individuals over their personal information, and consequently the rights stemming therefrom, are subordinated in the hierarchy of values to the public interest to an effective criminal justice system and sound financial markets. The original administrative nature of the whole preventive architecture, whereby obliged entities are called on to monitor their own customers' profiles and financial transactions, and FIUs' mandate is to receive and analyze reports, should not mislead one to think that it does not have any sort of implications for fundamental rights and that it is unnecessary to set out safeguards for those involved. To the contrary, the measures that have been set out in the EU preventive legislation to tackle the phenomena of money laundering and terrorism financing reveal that a new EU security governance has been on the rise for quite some time, which is inextricably interwoven with the emerging phenomenon of datafication of socio-economic spheres, according to which every human action passes through massive amounts of data which are collected, processed and exploited for numerous purposes. Information so gathered and stored by an uncontrollable number of entities, both public and private, is «channeled through various investigation mechanisms, aiming at rendering it a useful policing tool in the fight against money laundering»[105], meaning that it is eventually used to support criminal prosecutions and conviction.

The EU legislation in the AML/CTF field is just one of the several instances[106]

[104]C. Fried, *Privacy*, in *Yale Law Journal*, 1968, 77, p. 475. See also L. Menges, *A Defense of Privacy as Control*, in *The Journal of Ethics*, 2021, 25, pp. 385-402.

[105]V. Mitsilegas, *Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance versus Fundamental Legal Principles*, The Hague, 2003, p. 232.

[106]Another case of an administrative tool is used to serve also a crimnial law purpose is

of the 'preventive justice' paradigm dominating the EU Security Union[107], which blurs the boundaries between prevention and prosecution, administrative and criminal, legislative and political[108] by, *inter alia*, enabling the gathering, storage and exchange of vast amounts of data that easily flow among public and private entities in what has turned into a generalized surveillance system[109].

In light of the above, also in the context of financial investigations aimed at, but going beyond, the prevention of the abuse of financial markets, tensions with fundamental rights *within* the criminal justice system - that is, fair trial rights - and protected *from* the threats it represents, namely the right to privacy and data protection, need to be addressed.

The foregoing research does not claim to answer in a decisive and exhaustive manner to the issues addressed by the research questions presented in the Introduction. Nor does it intend to formulate any legislative or regulatory proposal to be adopted to address and solve the issues raised therein. However, the research advocates a renovated focus on the part of stakeholders on the challenges posed by the "follow the money approach" to economic offences that has been widely praised. In view of that, we will attempt to lay the groundwork for future discussions around the topic, by building on the main findings of the research and providing some recommendations to adhere to. The reflection will be informed by

---

the European Travel Information and Authorisation System (ETIAS) for the collection and management of third countries nationals traveling data. In the literature, see F. Michéa, L. Rousvoal, *The Criminal Procedure Out of Itself: A Case Study of the Relationship Between EU Law and Criminal Procedure Using the ETIAS System*, in *European Papers*, 2021, 6(1), pp. 473-492.

[107]D. Curtin, M. de Goede, *Bits, Bytes, Searches, and Hits: Logging-in Accountability for EU Data-led Security*, in D. Curtin- M. Catanzariti (eds), *Data at the Boundaries of European Law*, Oxford, 2023, p. 175.

[108]V. Mitsilegas, *The Preventive Turn in European Security Policy. Towards a Rule of Law Crisis?*, in F. Bignami (ed), *EU Law in Populist Times. Crises and Prospects*, Cambridge, 2020, pp. 301-318.

[109]V. Mitsilegas, *The Preventive Turn*, cit., p. 303, who argues that «[i]n the EU context, the preventive justice trend is apparent in the development of new databases, the broad access given to security authorities to consult these databases (including on immigration) and the introduction of systems of generalised surveillance through data retention (requiring telecommunication companies to retain and transfer customer data to state authorities) and passenger name records (PNR systems requiring airlines to collect and transfer passenger data to state authorities)».

an overall view approach, whereby the different points touched upon in the course of the research will be held together.

3.1 Striving for silence: the protection of informational self-determination and control over self-incriminating data

The main node to be untangled concerns how to ensure that silence, *i.e.* control over personal data, is guaranteed in financial investigations.

The first recommendation in this sense would be to expressly regulate who enjoys margins of control in the course of financial investigations. As extensively seen, financial investigations involve numerous stakeholders, including FIUs, obliged entities belonging to the private sector and operating in the market, competent authorities, and customers, that is, natural or legal persons engaging with banks and other credit and financial intermediaries in order to have access to their services and participate in the banking system. Both obliged entities and their customers have their own interest in preventing their personal data not to be disclosed, processed, and exchanged in an unlawful or indiscriminate manner and should be able to control their (potentially self-incriminating) data.

An obstacle is immediately detected: the lack of recognition to legal persons of any right not to provide self-incriminating information in the context of administrative proceedings *à coloration penale*, which potentially has serious consequences in the field at stake given that obliged entities are to a great extent legal persons. Indeed, this would entail that neither corporations falling within the remit of the AML/CTF preventive reporting and CDD duties, nor legal persons engaging with the banking and financial system would be able to avoid the (ab)use of their data for law enforcement purposes. Legal persons are expressly excluded from the scope of the Presumption of Innocence Directive, so that the procedural safeguard stemming from criminal law does not apply to them. Moreover, the LED explicitly regulates the processing of personal data of natural persons by competent authorities for law enforcement purposes, thus leaving out legal entities. By drawing a parallel between our field and competition law, it can be observed that undertakings, whether individuals or societies, do enjoy a margin

of control, however restricted, insofar as they cannot be compelled to «provide [the Commission] with answers which might involve an admission on its part of the existence of an infringement which it is incumbent upon the Commission to prove»[110]. By resorting to the argument of the burden of proof, which in administrative competition proceedings falls on the Commission, the Court of Justice acknowledged some margins in which the privilege against self-incrimination can apply[111]. Awaiting an intervention of the Court of Justice to clarify the position of obliged entities that are legal persons, this argument should be upheld when referring to the position of legal persons within the AML/CTF system, either serving as obliged entities or customers/suspects.

The second recommendation would be to take into account the dilemma that individuals concerned by financial investigations are confronted with when having to choose between compliance with rules and obligations on one hand, and non-disclosure of personal data on the other. This can be subsumed in the cooperation duties/self-determination dichotomy. As illustrated in the research, both obliged entitied and customers are destined to face harmful consequences in case of noncompliance, insofar as the former would be sanctioned with pecuniary or even criminal penalties, whereas the letter would be excluded from the access to specific transactions or to the banking system entirely (de-risking). Since the circumstance itself of being subject to the threat of penalties constitutes a form of improper compulsion according to the Court of Strasbourg case law[112], the issue needs to be taken into account and a balance must be sought. Notewithstanding the reference in Regulation (EU) 2024/1624 to the limitation of de-risking behaviours on the part of obliged entities receiving data from their PPP "colleauges"[113], no balance has ever been struck between fundamental rights and cooperation duties stemming from AML/CTF preventive legislation. The discussion around the reg-

[110]Judgment of 18 October 1989, *Orkem v Commission*, C-374/87, ECLI:EU:C:1989:387, para 35.

[111]Which should not be called into question by the judgment of 2 February 2021, *DB v. Consob*, C-481/19, ECLI:EU:C:2021:84. as it concerned natural persons.

[112]*Ex multis*, ECtHR [GC], 13 September 2016, *Ibrahim and Others v. The United Kingdom*, Appl. nos 50541/08, 50571/08, 50573/08 and 40351/09, § 267.

[113]Whose enforceability is however difficult to imagine.

ulation on financial investigations, and their interplay with the privilege against self-incrimination, cannot neglect that the priorities of the public interests to be achieved need to be reconsidered, and that the achievement of a cooperation system at the expenses of the elimination of any form of control of subjects over their informational self-determination leads to a state of surveillance.

This leads to the third recommendation, which concerns the data protection implications of financial investigations. Inquiries into the financial affairs of natural and legal persons allow banks and other financial service providers to access and retain vast amounts of personal data, which seriously interfere with their private life and data protection. For this reason, data protection provisions must be accounted for, and the research showed that the most appropriate regime to be applied in the instance at stake is that stemming from the LED. It was also posited that the LED should not only regulate data processing by public competent authorities tasked with the investigations and prosecution of criminal offences, but also to FIUs and private actors when they participate in PPPs thus serving as an arm of law enforcement authorities. The analysis of the two relevant EU data protection frameworks showed that the LED, as it applies to law enforcement activities, allows minor control of data subjects over the processing of their personal data, in line with the general restrictive approach to data subject rights followed therein, and that it does not mention certain rights enshrined in the GDPR. One of these is the right to object to the processing of personal data, according to which data subjects in particular situations can at any time oppose the processing of their personal data collected for the performance of a task carried out in the public interest, or for the purposes of the legitimate interests pursued by the controller[114]. When the objection is well-founded, the processing instigated by the controller may no longer involve those data[115]. According to relevant scholarship, the right to object constitutes an important manifestation of the fairness principle, insofar as it empowers data subjects to exert a form of *ex post* control over

[114]Artt. 21 and 6(1) GDPR.

[115]Judgment of 13 May 2014, *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317, para 76.

processing activities performed by data controllers[116] and it contributes to the fair balancing of powers between the data controller and the data subject. By reducing the aymmetries between the parties, the right to object to data processing enables data subjects to challenge the way their data are being used when there is a risk that data subjects may suffer from prejudicial effects[117]. Interestingly, the provision entails the reversal of the burden of proof, as it is on the controller to demonstrate that the legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject claimed in the objection[118].

The reference to the right to object is not intended to call into question the applicability of the regime stemming from the LED in the cases at stake, as we are aware that many facets of this are incompatible «with the nature of processing personal data by public entities in the law enforcement sector for the purposes related to their core activity»[119]. However, a similar «control-centric» effect is played by the right of erasure, pursuant to Art. 16(2) LED, which grants data subjects to obtain the erasure of personal data when unlawfully processed by data controllers. In any case, the reflection over the implications of financial investigations for data protection and the rights and safeguards than can be enjoyed by customers/data subjects, cannot look away from the central issue of informational self-determination of the persons concerned, which therefore requires to strenghten the measures enabling control over personal data.

The right to object and the right to erasure are not the only empowering tools in connection with the fairness principle, insofar as *ex ante* safeguards also exist in data protection law as well as in criminal law, as will be shown in the following section.

[116] D. Clifford, J. Ausloos, *Data Protection*, cit., p. 172.

[117] G. Malgieri, *Vulnerability*, cit., p. 138.

[118] Recital 69 GDPR.

[119] G. Zanfir-Fortuna, *Article 21. Right to object*, in C. Kuner-L.A. Bygrave-C. Docksey (eds), *The EU General Data Protection Regulation (GDPR). A Commentary*, cit., p. 511.

3.2 Striving for remedies: the right to notification to ensure informed consent

For control over personal information to be effective and the right not to contribute to their own incrimination to be exercised, customers need to be aware that their data are being collected, stored, and used for specified purposes. Just as suspects of crime are put in the position to properly defend themselves when they are informed of such rights and the consequences of the exercise thereof, so too data subjects are expected to be informed by the controller that their personal data have been collected, stored and retained. However, in the context of criminal prosecution, notification is the right of data subjects that is «probably most prominently and commonly at odds with the goals of combating money laundering and terrorism financing»[120], since the secrecy of the investigations is essential to their efficacy. Therefore, it is not surprising that neither the LED nor the AML/CTF legislation provide for notification obligations falling on data controllers and competent authorities. As for the former, it requires data controllers to provide specific information on processing activities to data subjects[121], thus acknowledging the importance to ensure transparency about how personal data are used in the law enforcement area. Nevertheless, a set of important information enabling data subjects to exercise their rights can be restricted by national laws "in specific cases" and should never «prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance»[122].

As for the latter, persons concerned by FIUs processing activities, or whose transactions have been subjected to to suspicious activities reports, do not enjoy notification rights, and obliged entities may even be sanctioned for disclosing information to their customers insofar as it might jeopardize the performance of analyses and investigations.

However, mainstream constitutional scholarship agrees that the right of individuals to be afforded a minimum of information constitutes an essential element

[120] M. Brewczyńska, E. Kosta, *The EU Data Protection Framework*, cit., p. 462.
[121] Art. 13 LED.
[122] Recital 26 LED.

of the right to an effective judicial remedy enshrined in Art. 47 CFREU, inasmuch as it enables them «to be in a position to defend themselves which, too, may be considered to form part of the essence of that right»[123], and this holds true even when there are compelling concerns for confidentiality or national security[124]. This view has been developed in the jurisprudence of European courts. In its case law on secrete surveillance and access to personal data in the law enforcement field, the ECtHR clarified how relevant notification is to the effectiveness of remedies before the courts, insofar as «there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively»[125]. Tthe Strasbourg court has furthermore struck a balance between the competing interests at stake, by establishing that persons concerned should be notified as soon as it can be made without jeopardizing the purposes of the investigative measures[126], which has been also applied by the European Court of Justice in her decisions on data retention for law enforcement purposes[127]. According to the Court, competent authorities are required to notify data subjects when their electronic communication data or PNR (Passenger Name Record) data are accessed for law enforcement purposes as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities[128],

[123]K. Gutman, *The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?*, in *German Law Journal*, 2019, 20, p. 902;

[124]S. Prechal, *The Court of Justice and Effective Judicial Protection: What Has the Charter Changed?*, in C. Paulussen-T. Takacs-V. Lazić-B. Van Rompuy (eds), *Fundamental Rights in International and European Law. Public and Private Law Perspectives*, The Hague, 2016, p. 153.

[125]ECtHR, 29 June 2006, *Weber and Saravia v. Germany*, Appl. No 4934/00, § 135.

[126]See ECtHR [GC], 4 December 2015, *Roman Zakharov v. Russia*, Appl. No 47143/06, § 287; ECtHR [GC], 6 Septemebr 1978, *Klass and Others v. Germany*, Appl. No 5029/71, § 58.

[127]The CJEU has derived from Art. 47 CFREU several procedural obligations that need to be complied with, of which notification obligations are one of the manifestations, such as the duty of public bodies to reason their acts. See judgment of 4 June 2013, *ZZ*, C-300/11, ECLI:EU:C:2013:363, para 53; judgment of 3 September 2008, *Kadi I*, joined Cases C-402/05 P and C-415/05 P, ECLI:EU:C:2008:461, para 337. See H. Hofmann, *Article 47*, in S. Peers-T. Hervey-J. Kenner-A. Ward (eds), *The EU Charter of Fundamental Rights. A Commentary*, cit., p. 1261 ff.

[128]*Digital Rights Ireland*, cit., para.; *Tele2*, cit. para 121; Opinion 1/15 of 26 July 2017, *EU-Canada PNR Agreement*, ECLI:EU:C:2017:592, para 220.

so that minimum safeguards against the risk of abuse are granted to persons concerned by interferences with their personal data[129].

Information is key to protecting fundamental rights in the field of crime control and criminal prosecution, and it is instrumental in exerting control over the way personal data are used. The case of the privilege against self-incrimination and the right to silence is self-evident in this regard, given that suspects need to be informed in advance that their information might be used against them, of the existence of these rights and the consequences of exercising them. Only then may the person concerned «consciously make a decision to provide explanations and may freely shape the content of his or her explanations»[130].

The regulation of financial investigations in the AML/CTF preventive legislation cannot look away from this important component without risking to be in violation of the well-established case law envisaging minimum safeguards against interferences into one's personal sphere. Therefore, the fourth recommendation is that the AML/CTF legislation should therefore account for a form of notice to be given to customers. Of course, this should strike a fair balance between the main objectives of investigations and of the AML/CTF system itself and the protection of fundamental rights, in accordance with European case law.

In this sense, specific warnings should be laid down, either to be given prior to the financial analysis, when it concerns past financial transactions, or as soon as it is not able to compromise the outcome of the inquiry, in those cases entailing real-time monitoring of specific transactions or bank accounts by competent authorities. A mechanism of this kind, similar to that in place in the US legal system[131], would ensure awareness, *i.e.* control, to customers/data subjects, while also responsibilizing those performing the financial investigations. In other terms, it would ensure accountability, especially as far as the private sector is concerned.

[129] Judgment of 6 October 2015, *Maximillian Schrems*, C-362/14, ECLI:EU:C:2015:650, para 91.

[130] A. Sakowicz, *The Right to Silence in the EU Directive 2016/343 on the Strengthening of Certain Aspects of the Presumption of Innocence from the Perspective of Polish Criminal Proceedings*, in *Review of European and Comparative Law*, 2020, 41, p. 76, with a view to the Polish criminal procedural system.

[131] U.S. Supreme Court, *Miranda v. Arizona,* 384 U.S. 436 (1966).

3.3 Striving for accountability: the need to address the role of private actors

The fifth recommendation for the regulation of financial investigations would be to address more clearly the role played by private actors in monitoring customers' transactions occurring within the financial system, and their potential involvement in criminal investigations, which is the central challenge of privatization[132]. The research showed in this regard that concerns arise when private actors *de facto* operate as agents of securitization, by performing functions and powers traditionally pertaining to the public domain. In this sense, the question of accountability arises.

Accountability, which can be defined as «the obligation to explain and justify conducts»[133], entails a two-tier social relationship, whereby the principle, which can also be a forum, delegates the authority to the agent, which is required to give account of its actions[134]. Answerability is ensured by the implementation of legislative or regulatory mechanisms that provide substantial protection against abuse of powers by those who would otherwise elude accountability for their substantially public actions in view of their private nature. Therefore, only a widened notion of accountability - which is fostered by the securitization of public policies - can ensure the inclusion of private actors within the chain of responsabilities for decision and actions.

Looking at the AML/CTF regulatory system, a vertical accountability structure can be observed[135], insofar as bank customers voluntarily delegate powers

[132]See G. A. Hodge, K. Coghill, *Accountability in the Privatized State*, in *Governance*, 2007, 20(4), pp. 675-702.

[133]M. Bovens, *Analysing and Assessing Accountability: A Conceptual Framework*, in *European Law Journal*, 2007, 13(14), p. 450. The Author conceptualizes accountability as «a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgement, and the actor may face consequences». See also M. Bovens, *Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism*, in *West European Politics*, 2010, 33(5), 946–967.

[134]Another intuitive definition, provided by B. S. Romzek, M. J. Dubnick, *Accountability*, in J. Shafritz (ed), *Defining Public Administration*, 2000, pp. 382-395, views accountability as a mechanism whereby an agent is «held to answer for performance that involves some delegation of authority to act».

[135]M. Bovens, *Analysing and Assessing Accountability*, cit., p. 460.

to the agents, *i.e.* the obliged entities operating in the financial system providing services to them. However, banks and other credit and financial institutions hold a twofold position, insofar as they are both agents of private principles, *i.e.* their customers, and agents of securitization, as they serve the purposes of law enforcement authorities[136]. In view of that, it is here contended that private businesses cannot always be held accountable for their actions as *de facto* agents of public competent authorities when fundamental rights of their clients are infringed upon, but only when an explicit collaboration between competent authorities and obliged entities exists. That is the case of PPPs, where a clear public-private divide is lacking by virtue of the specific features of such arrangements.

Therefore, it can be concluded that the recognition of an increasingly wider and systemic involvement of the private sector in the crime control and law enforcement field, especially according to a PPP form of governance, calls for the introduction of accountability mechanisms that should work as a remedy against abuse of power. One of the research outputs in this regard, has suggested that the "contractualization" of rights and obligations of the parties to a business relationship, *e.g.* banks and their clients, might represent an appropriate alternative accountability mechanism[137], insofar as breaches of the contractual clause would lead to legal remedies being afforded to the clients if so provided by the contract. In this regard, a salient contribution would be to ensure that the checking account contracts make reference to the circumstance of a PPP being established with competent authorities; the possibility of financial data being processed for law enforcement purposes; and the remedies available to customers, such as, *inter alia*, the inadmissibility of incriminating data as evidence in a potential subsequent criminal proceeding, or other measures penalizing the agent and compensating the principle[138].

[136]K. Svedberg Helgesson, *The multiple positions of private actors in securitization*, in K. Svedberg Helgesson-U. Mörth (eds), *Securitization, Accountability and Risk Management: Transforming the Public Security Domain*, London-New York, 2012, p. 137.

[137]G. E. Metzger, *Privatization as delegation*, in *Columbia Law Review*, 2003, 103, p. 1458.

[138]This latter aspect, according to some authors, is key in the contruction of the notion of accountability, which would be «incomplete without effective rectification», and should therefore include «an element of redistributive justice in making the guilty pay for their wrongdoing. The principal must be able to have remedies or sanctions imposed on the agent as part of the right

of authoritative direction that lies at the heart of accountability relationship». See R. MULGAN, *Holding Power to Account. Accountability in Modern Democracies*, Houndmills, 2003, p. 9.

Bibliography

Abramson LW, "Witness Waiver of the Fifth Amendment Privilege" (1988) 41(235) Oklahoma Law Review.

Albers M, "Realizing the complexity of data protection" in *Reloading data protection: Multidisciplinary insights and contemporary challenges* (Springer 2013).

Allegrezza S, "Collecting criminal evidence across the European Union: the European investigation order between flexibility and proportionality" in S Ruggeri (ed), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases* (Springer 2013).

— *The Proposed Anti-Money Laundering Authority, FIU Cooperation, Powers and Exchanges of Information A Critical Assessment* (techspace rep, 2025-04, Publication for the committee on Economic, Monetary Affairs, Policy Department for Economic, Scientific, and Quality of Life Policies, European Parliament, Luxembourg 2022).

Allegrezza S and Bruzzese G, "The Anti-Money Laundering Regulation and the Handling of Financial Information in Luxembourg" in *F.I.N.A.N.C.E.* (JOVENE Editore 2023) ⟨https://financeresearchproject.com/#results-and-publications⟩.

— "Supervision and Enforcement of EU's Anti-Money-Laundering and Countering the Financing of Terrorism", in F Annunziata and M Siri (eds), *EU Banking and Capital Markets Regulation: Open Issues of Vertical Interplay with National Law* (Springer 2025).

S Allegrezza and V Covolo (eds), *Effective Defence Rights in Criminal Proceedings. A European and Comparative Study on Judicial Remedies* (Wolters Kluwer 2018).

Amalfitano C, "Unione europea e principio del reciproco riconoscimento delle decisioni penali" in H Belluta and M Ceresa-Gastaldo (eds), *L'ordine europeo di protezione. La tutela delle vittime di reato come motore della cooperazione giudiziaria* (Giappichelli 2016).

— "Il dialogo tra giudice comune, Corte di giustizia e Corte costituzionale dopo l'obiter dictum della sentenza n. 269/2017" (2019) 12(2) Osservatorio sulle fonti.

Amati E, *Dinamiche evolutive del diritto al silenzio. Riflessi sul diritto punitivo e sugli obblighi di collaborazione con le autorità ispettive e di vigilanza* (G Giappichelli Editore 2022).

Amato G, "The Anti-Money Laundering Architecture of Italy" in B Vogel and J.-B Maillart (eds), *National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection* (Intersentia 2020).

Amicelle A, "Towards a 'new'political anatomy of financial surveillance" (2011) 42(2) Security dialogue 161.

— "Trace my money if you can: European security management of financial flows", in KS Helgesson and U Mörth (eds), *Securitization, Accountability and Risk Management* (Routledge 2012).

Amicelle A and Chaudieu K, "In search of transnational financial intelligence: questioning cooperation between financial intelligence units" in C King, C Walker, and J Gurulé (eds), *The Palgrave handbook of criminal and terrorism financing law* (Springer 2018).

Amicelle A and Iafolla V, "Suspicion-in-the-making: Surveillance and Denunciation in Financial Policing" (2018) 58(4) The British Journal of Criminology 845.

Amodio E, "Diritto al silenzio o dovere di collaborazione" [1974] Rivista di diritto processuale 408.

Andersson H, "Fighting insider dealing at all costs?—due process aspects on the EU market abuse regime" (2022) 17(2) Capital Markets Law Journal 196.

Andolina E, "Dichiarazioni rese dinanzi ad autorità diverse da quelle penale" [2024] (1) Rivista italiana di diritto e procedura penale 71.

Andrade NNG de, "Oblivion: the right to be different... from oneself: re-proposing the right to be forgotten" in *The ethics of memory in a digital age: Interrogating the right to be forgotten* (Springer 2014).

Andrijauskaitė A, "Exploring the penumbra of punishment under the ECHR" (2019) 10(4) New Journal of European Criminal Law 363.

Aprile E, *Diritto processuale penale europeo e internazionale* (Cedam 2007).

Aranci M, "Diritto al silenzio e illecito amministrativo punitivo: la risposta della Corte di giustizia. Nota a Corte giust., sent. 2.2. 2021, causa C-481/19, Consob" (2021) 2021(2) Sistema penale 73.

Ashworth A, "Self-incrimination in European human rights law-a pregnant pragmatism" (2008) 30 Cardozo L. Rev. 751.

Avveduto S and others, "The Conceptual Representation of the "Electronic Evidence" Domain" in MA Biasiotti and others (eds), *Handling and Exchanging Electronic Evidence Across Europe* (Springer 2018).

Bachmaier Winter L, "Información de inteligenciay proceso penal" in L Bachmaier Winter (ed), *Terrorismo, proceso penal y derechos fundamentales* (Marcial Pons Ediciones Jurídicas y Sociales 2012).

— "Section III-criminal procedure information society and penal law general report" (2014) 85(1-2) Revue Internationale de Droit Pénal 75.

— "Public-Private Collaboration in Criminal Law Enforcement in Spain. Involvement of Private Actors in the Detection and Investigation of Crimes", in *Law of Public-Private Cooperation against Financial Crime: Developing Information-Sharing on Money Laundering and Terrorism Financing* (Intersentia 2024).

— "The Quest for Evidentiary Rules in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights", in L Bachmaier Winter and F Salimi (eds), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights* (Bloomsbury Publishing Plc 2024).

Bachmaier Winter L, "Il principio del mutuo riconoscimento" in R Kostoris (ed), *Manuale di Procedura Penale Europea* (Giuffrè 2025).

Ballin MFH, *Anticipative criminal investigation: Theory and counterterrorism practice in the Netherlands and the United States* (Springer Science & Business Media 2012).

Balsamo A, “Il contrasto internazionale alla dimensione economica della criminalità organizzata: dall’impegno di Gaetano Costa alla “Risoluzione Falcone” delle Nazioni Unite” [2020] Sistema Penale 16.

Balzacq T, “Securitization theory: Past, present, and future” (2019) 51(2) Polity 331.

Barbosa e Silva J, “The speciality rule in cross-border evidence gathering and in the European Investigation Order—let’s clear the air” (3, 2019) vol 19.

Barents R, “Some observations on the Treaty of Amsterdam” (1997) 4(4) Maastricht Journal of European and Comparative Law 332.

Beck U, *Risk society: Towards a new modernity* (Sage Publications 1992).

Beladiez Rojo M, “La eficacia de los derechos fundamentales entre particulares. Algunas consideraciones sobre el distinto alcance que pueden tener estos derechos cuando se ejercen en una relación jurídica de derecho privado o de derecho público” [2017] Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid 75.

Bentzen HB, “Context as key: the protection of personal integrity by means of the purpose limitation principle” in *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022).

Berger M, “Europeanizing self-incrimination: the right to remain silent in the European court of human rights” (2006) 12(2) Columbia Journal of European Law 339.

Bergström M, “Legal Perspectives on Money Laundering” in V Mitsilegas, S Hufnagel, and A Moiseienko (eds), *Research Handbook on Transnational Crime* (Edward Elgar Publishing 2019).

Bergström M, Svedberg Helgesson K, and Mörth U, “A new role for for-profit actors? The case of anti-money laundering and risk management” (2011) 49(5) JCMS: Journal of Common Market Studies 1043.

Bergstršm, Maria, “Money laundering” in V Mitsilegas, M Bergstršm, and T Quintel (eds), *Research Handbook on EU Criminal Law* (Edward Elgar Publishing 2024).

A Bernardi and C Cupelli (eds), *Il caso Taricco e il dialogo tra le corti: l’ordinanza 24/2017 della Corte costituzionale* (Jovene editore 2017).

Bernardini L and Sanvitale F, "Searches and seizures of electronic devices in european criminal proceedings: a new pattern for independent review?" [2023] (1) Revista Ítalo-española de Derecho procesal.

Bilbao Ubillos JM, "La consolidación dogmática y jurisprudencial de la Drittwirkung: una visión de conjunto" [2017] Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid 41.

Billing FM, *The right to silence in transnational criminal proceedings: Comparative law perspectives* (Springer 2016).

Black Jr CL, "Foreword: State Action, Equal Protection, and California's Proposition 14" (1967) 81 Harvard Law Review 69.

Bobbio N, *Stato governo società: per una teoria generale della politica* (Einaudi 1985).

Boer M den, "An Area of Freedom, Security and Justice: Bogged Down by Compromise" in D O'Keeffe and P Twomey (eds), *Legal Issues of the Amsterdam Treaty* (Hart Publishing 1999).

Borgers MJ, "Confiscation of the proceeds of crime: the European Union framework" in C King and C Walker (eds), *Dirty Assets. Emerging Issues in the Regulation of Criminal and Terrorist Assets* (Ashgate 2014).

Borlini L and Montanaro F, "The evolution of the EU law against criminal finance: the hardening of FATF standard within the EU" (2016) 48 Georgetown Journal of International Law 1009.

Borrello I, "Financial Intelligence Unit (FIU)" in D Siclari (ed), *Italian Banking and Financial Law: Vol I, Supervisory Authorities and Supervision* (Springer 2015).

Bovens M, "Analysing and assessing accountability: A conceptual framework 1" (2007) 13(4) European law journal 447.

— "Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism" (2010) 33(5) West European Politics 946.

Brandão N, "The right of defence under Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and confiscation orders" (2022) 13(1) New Journal of European Criminal Law 28.

Brewczyńska M, "Financial Intelligence Units: Reflections on the applicable data protection legal framework" (2021) 43 Computer Law & Security Review 105612.

— "A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation", in *Research handbook on EU data protection law* (Edward Elgar Publishing 2022).

Brewczyńska M and Kosta E, "The EU Data Protection Framework" in *Law of public-private cooperation against financial crime: Developing information sharing to counter money laundering and terrorism financing* (Larcier-Intersentia 2024).

Brière C, "EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments" (2021) 2021(1) European Papers-A Journal on Law and Integration 493.

Brinkerhoff JM, "Assessing and improving partnership relationships and outcomes: a proposed framework" (2002) 25(3) Evaluation and program planning 215.

Brkan M, "The unstoppable expansion of the EU fundamental right to data protection: Little shop of horrors?" (2016) 23(5) Maastricht Journal of European and Comparative Law 812.

— "The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning" (2019) 20(6) German Law Journal 864.

Broek M, *Preventing money laundering: A legal study on the effectiveness of supervision in the European Union* (eleven international publishing 2015).

Busillo S, "Mutual Recognition in EU Judicial Criminal Cooperation and Its 'Conditional Application'to the European Investigation Order (EIO) Under ECJ Case Law" in T Russo, A Oriolo, and G Dalia (eds), *Solidarity and Rule of Law: The New Dimension of EU Security* (Springer 2023).

Buzan B and Waever O, *Regions and powers: The structure of international security* (vol 91, Cambridge University Press 2003).

Bygrave L, *Data protection law: approaching its rationale, logic and limits,(Vol. 10)* (Kluwer Law International 2002).

Caeiro P, “The Influence of the EU on the “Blurring” between Administrative and Criminal Law” [2014] (Galli F and Weyembergh A eds 171.

Caflisch L, “Waivers in international and European human rights law” in MH Arsanjani and others (eds), *Looking to the Future* (Brill Nijhoff 2011).

Cahn O and Juliette T, “Procedural aspects of freezing in Europe. A comparative analysis (Belgium, France, Germany, Italy, Netherlands, Romania)” in A Bernardi (ed), *Improving confiscation procedures in the European Union* (Jovene Editore).

Caianiello M, “To Sanction (or not to Sanction) Procedural Flaws at eu Level?: A Step forward in the Creation of an eu Criminal Process” (2014) 22(4) European Journal of Crime, Criminal Law and Criminal Justice 317.

Calderoni F, *Organized crime legislation in the European Union: harmonization and approximation of criminal law, national legislations and the EU framework decision on the fight against organized crime* (Springer Science & Business Media 2010).

Camaldo L, “Presunzione di innocenza e diritto di partecipare al giudizio: due garanzie fondamentali del giusto processo in un’unica Direttiva dell’Unione europea” [2016] Diritto penale contemporaneo 1.

Camon A, “La disciplina costituzionale” in A Camon and others (eds), *Fondamenti di procedura penale* (Wolters Kluwer-Cedam 2025).

Caneschi G, “La Corte di Giustizia sul diritto al silenzio: un primo passo verso il" giusto procedimento" amministrativo punitivo” (2021) 2021(2) Rivista italiana di diritto e procedura penale 561.

Canestrini N, “La direttiva sul rafforzamento di Alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali: Una introduzione” (2016) 56(5) Cassazione penale 2224.

Carlos de Oliveira JC, “The Anti-money laundering architecture in Spain” in B Vogel and J.-B Maillart (eds), *National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection* (Intersentia 2020).

Carter JG, “The structure and function of public-private partnerships for homeland security” (2008) 2 Homeland Security Rev. 235.

Caruana MM, "The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement" (2019) 33(3) International Review of Law, Computers & Technology 249.

Cassani U, "L'internationalisation du droit pénal économique et la politique criminelle de la Suisse: la lutte contre le blanchiment d'argent" (2008) 127 Revue de droit suisse 227.

Catanzariti M, Data protection: handbook on techniques of judicial interaction in the application of the EU charter (European University Institute 2021).

Cattelan L, "Corte di Giustizia e principio del nemo tenetur se detegere: risvolti in tema di doppia pregiudizialità" [2021] IUS Penale.

Chemerinsky E, "Rethinking state action" (1985) 80 Northwestern University Law Review 503.

Clapham A, *Human rights in the private sphere* (Oxford University Press 1993).

Clifford D and Ausloos J, "Data protection and the role of fairness" (2018) 37 Yearbook of European Law 130.

Conti C, "Il corpo dell'imputato come prova: il diritto di non collaborare tra prospettive sovraordinate, suggestioni storiche e polifunzionalità dei dati" [2024] Diritto penale e processo 109.

Cordero F, *Procedura penale* (Giuffrè Editore 1979).

— *Procedura penale* (Giuffrè Editore 2012).

Costanzo P, "The risk-based approach to anti-money laundering and counter-terrorist financing in international and EU standards: what it is, what it entails" in B Unger and D van der Linde (eds), *Research Handbook on Money Laundering* (Edward Elgar Publishing 2013).

Cras S and Erbeznik A, "The directive on the presumption of innocence and the right to be present at trial: genesis and description of the new EU-measure" [2016] (1) Eucrim: the European Criminal Law Associations' forum 25.

Curtin D, "The Constitutional Structure of the Union: A Europe of Bits and Pieces'(1993) 30" 1 CML Rev 17.

Curtin D and De Goede M, "Bits, Bytes, Searches, and Hits: Logging-in Accountability for EU Data-led Security" in (Oxford University Press 2023).

Dalla Corte L, "A right to a rule: On the substance and essence of the fundamental right to personal data protection" in *Data protection and privacy: Data protection and democracy* (Hart Publishing 2020).

Dalla Pellegrina L and Masciandaro D, "The risk-based approach in the new European anti-money laundering legislation: a law and economics view" (2009) 5 Review of Law & Economics 931.

Damaska MR, *The faces of justice and state authority: a comparative approach to the legal process* (Yale University Press 1986).

Daniele M, "L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale" (2019) 5(3) Revista Brasileira de Direito Processual Penal 1277.

Daniele M and others, "Evidence gathering" in R Kostoris (ed), *Handbook of European Criminal Procedure* (Springer 2018).

De Hert P and Gutwirth S, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" [2006] Privacy and the criminal law 61.

— "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action", in *Reinventing data protection?* (Springer 2009).

De Hert P and Papakonstantinou V, "The new police and criminal justice data protection directive: a first analysis" (2016) 7(1) New journal of European criminal law 7.

De Hert P and Sajfert J, "Variety, velocity and volume of personal data in criminal investigations and proceedings: the limits drawn by the purpose limitation and data minimization principles in Directive (EU) 2016/680" in V Mitsilegas, M Bergstršm, and T Quintel (eds), *Research Handbook on EU Criminal Law* (Edward Elgar Publishing 2024).

De Mayer J, "The right to respect for private and family life, home and communications in relation individuals, and the resulting obligations for States parties to the Convention" (Robertson AH ed, Manchester University Press 1973).

De Oliveira IS, "The governance of the financial action task force: an analysis of power and influence throughout the years" (2018) 69(2) Crime, Law and Social Change 153.

De Vries A, "Recent Developments Concerning the Right to Silence and Privilege Against Self-Incrimination Under the Charter of Fundamental Rights of the EU–A Critical Reflection on Case C-481/19 DB v Consob" (2022) 15(1) Review of European Administrative Law 31.

De Wit J, "A risk-based approach to AML: A controversy between financial institutions and regulators" (2007) 15(2) Journal of Financial Regulation and Compliance 156.

Del Coco R, "Registrazioni audio-video effettuate da un privato su impulso dell'investigatore" in A Scalfati (ed), *Le indagini atipiche* (Giappichelli 2019).

Deleanu I, "FIUs in the European Union - facts and figures, functions and facilities" in B Unger and others (eds), *The economic and legal effectiveness of the European Union's Anti-Money Laundering policy* (Edward Elgar Publishing 2014).

— "Information flows and repressive enforcement", in B Unger and others (eds), *The economic and legal effectiveness of the European Union's Anti-Money Laundering policy* (Edward Elgar Publishing 2014).

Della Torre J, "Il paradosso della direttiva sul rafforzamento della presunzione di innocenza e del diritto di presenziare al processo: un passo indietro rispetto alle garanzie convenzionali?" [2016].

Demetriades P and Vassileva R, "Money laundering and central bank governance in the European Union" (2020) 23(2) Journal of International Economic Law 509.

Den Boer M, "The fight against organised crime in Europe: a comparative perspective" (2001) 9(3) European journal on criminal policy and research 259.

Developments in the Law-State Action and the Public/Private Distinction, "Harvard Law Review" (2010).

Dezza E, *Accusa e inquisizione: dal diritto comune ai codici moderni* (Giuffrè Editore 1989).

Di Paolo G, "Admissibility of E-Evidence, Transnational E-Evidence and Fair Trial Rights in Italy" in L Bachmaier Winter and F Salimi (eds), *Admissibility of evidence in EU cross-border criminal proceedings: Electronic evidence, efficiency and fair trial rights* (Blomsburry Publishing Plc 2024).

Di Stasi A and Festa A, "Breaches of the Rule of Law in the EU: What Implications for the Principle of Mutual Trust in the Area of Freedom, Security and Justice?" in T Russo, A Oriolo, and G Dalia (eds), *Solidarity and Rule of Law: The New Dimension of EU Security* (Springer 2023).

Djelic M.-L, "Marketization: From intellectual agenda to global policy making" in M.-L Djelic and K Sahlin-Andersson (eds), *Transnational governance. nstitutional Dynamics of Regulation* (Cambridge University Press 2006).

Donnelly J, *Universal Human Rights in Theory and Practice* (Cornell University Press 2013).

DPWP A2, *Opinion 03/2013 on purpose limitation* (techspace rep, April 2013).

Duff R, "Discretion and accountability in a democratic criminal law" [2017] Prosecutors and Democracy. A Cross-National Study 9.

Durner T and Shetret L, *Understanding bank de-risking and its effects on financial inclusion: An exploratory study* (techspace rep, Global Center on Cooperative Security 2015).

EDPS, *Opinion 1/2017 on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC with regards to the Commission Proposal for the Fifth AML Directive* (2 February 2017).

— *Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing* (23 July 2020).

— *Opinion 6/2015 on A Further Step towards a Comprehensive EU Data Protection. EDPS Recommendations on the Directive for Data Protection in the Police and Justice Sectors* (28 October 2015).

— *Opinion on a proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, and a proposal for a Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds* (4 July 2013).

Escobar Veas J, "De Legé v. the Netherlands: The ECtHR adopts a line of reasoning similar to that of the United States Supreme Court on compelled production of real or physical evidence" (2023) 30(5) Maastricht Journal of European and Comparative Law 653.

Fedtke J, "Drittwirkung in Germany" in D Oliver and J Fedtke (eds), *Human rights and the private sphere–A comparative analysis* (Routledge 2007).

Ferrajoli L, *Diritto e Ragione. Teoria del garantismo penale* (Laterza 1989).

Fiandaca G and Di Chiara G, *Una introduzione al sistema penale: per una lettura costituzionalmente orientata* (Jovene 2003).

Fichera M, "Organised crime: Developments and challenges for an enlarged European Union" in C Eckes and T Konstadinides (eds), *Crime within the Area of Freedom, Security and Justice: A European Public Order* (Cambridge University Press 2011).

Fijnaut C, *A peaceful revolution: The development of police and judicial cooperation in the European Union* (Intersentia Cambridge 2019).

Forrer J and others, "Public–private partnerships and the public accountability question" (2010) 70(3) Public administration review 475.

Fratangelo P, "The CDD obligations following a risk-based approach" in D Siclari (ed), *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive* (Palgrave 2015).

Fried C, "Privacy" (1968) 77(3) The Yale Law Journal 475.

Fundamental Rights EUA for, *Handbook on European Data Protection Law* (Council of Europe 2018).

Fusaro C and Favilli C, "The protection of constituional rights in the private sphere" in D Oliver and J Fedtke (eds), *Human Rights and the Private Sphere. A comparative Study* (Routledge 2007).

Gaja G, "How flexible is flexibility under the Amsterdam Treaty?" (1998) 35(4) Common Market Law Review.

Garland D, "The limits of the sovereign state: Strategies of crime control in contemporary society" (1996) 36(4) The British journal of criminology 445.

— *The culture of control: Crime and social order in contemporary society* (Oxford university press 2001).

Garvin MJ and Bosso D, "Assessing the effectiveness of infrastructure public—private partnership programs and projects" (2008) 13(2) Public Works Management & Policy 162.

Gascón Inchausti F, "Desafíos para el proceso penal en la era digital: externalización, sumisión pericial e inteligencia artificial." (Conde Fuentes J and Serrano Hoyo G eds, 2019).

Gellert R and Gutwirth S, "The legal construction of privacy and data protection" (2013) 29(5) Computer Law & Security Review 522.

Gerards J, *General Principles of the European Convention on Human Rights* (Cambridge University Press 2023).

Gilmour PM, "Lifting the veil on beneficial ownership: Challenges of implementing the UK's registers of beneficial owners" (2020) 23(4) Journal of Money Laundering Control 717.

Golobinek R, "Financial investigations and confiscation of proceeds from crime" (2002) 2003 Training Manual for Law Enforcement and Judiciairy, Cards Regional Programme.

Granger M.-P and Irion K, "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection" (2014) 39(6) European Law Review 835.

Grasso G, "La «competenza penale» dell'Unione europea nel quadro del Trattato di Lisbona" in G Grasso, L Picotti, and R Sicurella (eds), *'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona* (Giuffrè Editore 2011).

Grevi V, *«Nemo tenetur se detegere». Iinterrogatorio dell'imputato e diritto al silenzio nel processo penale italiano* (Giuffrè Editore 1972).

Grossi S, "The Waiver of Constitutional Rights" (2022) 60 Houston Law Review 1021.

Gutiérrez IG, "Criterios de eficacia de los derechos fundamentales en las relaciones entre particulares" [1999] (3) Teoría y realidad constitucional 193.

Gutman K, "The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?" (2019) 20(6) German Law Journal 884.

Gutwirth S and De Hert P, "Regulating profiling in a democratic constitutional state" in *Profiling the European citizen: Cross-disciplinary perspectives* (Springer 2008).

Guzzini S, "Securitization as a causal mechanism" (2011) 42(4-5) Security dialogue 329.

Hale RL, "Rights Under the Fourteenth and Fifteenth Amendments Against Injuries Inflicted by Private Individuals" (1946) 6 Law Guild Review 627.

Harris DJ and others, *Law of the European convention on human rights* (Oxford University Press 2023).

Helgesson KS, "The multiple positions of private actors in securitization" in KS Helgesson and U Mörth (eds), *Securitization, Accountability and Risk Management* (Routledge 2012).

Helmholz R, "The Privilege and the Ius Commune: the Middle Ages to the Seventeenth century" in RH Helmholz and others (eds), *The Privilege Against Self-Incrimination: Its Origins and Development* (University of Chicago Press 1997).

Herlin-Karnell E, "The EU's Anti Money Laundering Agenda-Built on Risks. A European public order" in T Konstadinides and C Eckes (eds), *Crime within the Area of Freedom, Security and Justice* (2008).

— "EU criminal law and its complicated relationship to the internal market", in V Mitsilegas, M Bergstršm, and T Quintel (eds), *Research Handbook on EU Criminal Law* (Edward Elgar Publishing 2024).

Hernández Weiss A, "Effective protection of rights as a precondition to mutual recognition: Some thoughts on the CJEU's Gavanozov II decisión" (2022) 13(2) New Journal of European Criminal Law 180.

Hirvelä P and Heikkilä S, *Right to a fair trial: a practical guide to the Article 6 case-law of the European Court of Human Rights* (Intersentia 2021).

Hodge G, Greve C, and Biygautane M, "Do PPP's work? What and how have we been learning so far?" (2018) 20(8) Public Management Review 1105.

Hodge GA and Coghill K, "Accountability in the privatized state" (2007) 20(4) Governance 675.

Hodge GA and Greve C, "Public–private partnerships: an international performance review" (2007) 67(3) Public administration review 545.

Hofmann H, "Article 47" in S Peers and others (eds), *The EU Charter of fundamental rights: a commentary* (Bloomsbury Publishing 2021).

Horowitz HW, "The Misleading Search for State Action Under the Fourteenth Amendment" (1956) 30 Southern California Law Review 208.

Illuminati G, *La presunzione d'innocenza dell'imputato* (Zanichelli 1979).

Inchausti FG, "Mutual Recognition and Transnational Confiscation Orders" in S Ruggeri (ed), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings: A Study in Memory of Vittorio Grevi and Giovanni Tranchina* (Springer 2012).

Ioannides E, *Fundamental principles of EU law against money laundering* (Routledge 2016).

Jackson J, "Re-conceptualizing the right of silence as an effective fair trial standard" (2009) 58(4) International & Comparative Law Quarterly 835.

Jackson JD, "The effect of human rights on criminal evidentiary processes: Towards Convergence, Divergence or Realignment?" (2005) 68(5) The Modern Law Review 737.

Jackson JD and Summers SJ, *The internationalisation of criminal evidence: beyond the common law and civil law traditions* (Cambridge University Press 2012).

Jasiński W, "Admissibility of Evidence Obtained by Torture and Inhuman or Degrading Treatment. Does the European Court of Human Rights Offer a Coherent and Convincing Approach?" (2021) 29(2) European Journal of Crime, Criminal Law and Criminal Justice 127.

Jentzsch N, *Financial privacy: An International Comparison of Credit Reporting Systems* (Springer 2007).

Jimeno-Bulnes M, "The use of intelligence information in criminal procedure: A challenge to defence rights in the European and the Spanish panorama" (2017) 8(2) New Journal of European Criminal Law 171.

Kamber K, *Prosecuting human rights offences: rethinking the sword function of human rights law* (vol 11, Brill 2017).

Kay RS, "The State Action Doctrine, the Public-Private Distinction, and the Independence of Constitutional Law" (1993) 10 Constitutional Commentary 329.

Kelly KA, "Private family, private individual: John Locke's distinction between paternal and political power" (2002) 28(3) Social Theory and Practice 361.

Kilchling M, "Tracing, seizing and confiscating proceeds from corruption (and other illegal conduct) within or outside the criminal justice system" (2001) 9 European Journal of Crime, Criminal Law and Criminal Justice 264.

Klip A, "European criminal law: an integrative approach" [2016].

Klip A, "Violations of Defence Rights' Directives" (2018) 26(4) European Journal of Crime, Criminal Law and Criminal Justice 271.

Knust N, "Socio legal foundations of Public-Private Partnerships in the system of crime control" in *Law of Public-Private Cooperation against Financial Crime: Developing Information-Sharing on Money Laundering and Terrorism Financing* (Intersentia 2024).

Kokott J and Sobotta C, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR" (2013) 3 International Data Privacy Law 222.

Kosta E, "A divided European data protection framework: A critical reflection on the choices of the European legislator post-Lisbon" in *Research handbook on EU data protection law* (Edward Elgar Publishing 2022).

Koster P de and Penna M, "The case of money laundering. Real administrative procedure used in the detection of fraudulent transactions" in F Galli and A Weyembergh (eds), *Do labels still matter? Blurring boundaries between administrative and criminal law. The influence of the EU* (Editions de l'Université de Bruxelles 2014).

Kumm M and Comella VF, "What is so special about constitutional rights in private litigation? A comparative analysis of the function of state action requirements and indirect horizontal effect" in A Sajó and R Uitz (eds), *The Constitution in Private Relations: Expanding Constitutionalism* (Eleven International Publishing Utrecht 2005) vol 241.

La Spina A, "The role of organized crime in illicit trades: drug trafficking, migrant smuggling, arms trafficking and cigarette smuggling" in V Militello and others (eds) (Giappichelli 2019).

Lamberigts S, "The directive on the presumption of innocence. A missed opportunity for legal persons?" [2016] Eucrim.

— "The privilege against self-incrimination: A chameleon of criminal procedure" (2016) 7(4) New Journal of European Criminal Law 418.

Langbein JH, *Torture and the law of proof: Europe and England in the Ancien Régime* (University of Chicago Press 1977).

Lasagni G, "The new Frontiers of Financial Investigation: Banking supervision and real-time monitoring of Financial Records. A comparative analysis between the EU and the US" (PhD thesis, Università di Bologna 2016).

— *Banking Supervision and Criminal Investigation. Comparing the EU and US Experience* (Springer 2019).

— "Prendendo sul serio il diritto al silenzio. Commento a Corte cost. ord. n. 117 del 10 maggio 2019" (2020) 2 Diritto Penale Contemporaneo 135.

— "Public Private Partnerships nell'antiriciclaggio e antiterrorismo: una nuova forma di outsourcing del processo penale?" (2021) 3 Diritto Penale Contemporaneo 153.

— "Admissibility of Evidence in Criminal Proceedings: Lessons (and Problems) from the 'Data Retention Saga'", in L Bachmaier Winter and F Salimi (eds), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights* (Bloomsbury Publishing Plc 2024).

— "Public-Private Cooperation in the Detection and Investigation of Criminal Offences in Italy", in B Vogel, E Kosta, and M Lassalle (eds), *Law of Public-Private Cooperation against Financial Crime. Developing Information Sharing to Counter Money Laundering and Terrorism Financing* (Intersentia 2024).

Lassalle M, "Interaction between the state and private actors in the detection and investigation of crime in France" in *Law of Public-Private Cooperation against Financial Crime: Developing Information-Sharing on Money Laundering and Terrorism Financing* (Intersentia 2024).

Lavrysen L, *Human rights in a Positive State. Rethinking the Relationship between Positive and Negative Obligations under the European Convention on Human Right* (Intersentia 2016).

Leiser M and Custers B, "The law enforcement directive: Conceptual challenges of EU directive 2016/680" (2019) 5 Eur. Data Prot. L. Rev. 367.

Levi M, "Regulating money laundering: the death of bank secrecy in the UK" (1991) 31(2) The British Journal of Criminology 109.

Levi M and Gilmore W, "Terrorist finance, money laundering and the rise and rise of mutual evaluation: a new paradigm for crime control?" in M Pieth (ed), *Financing terrorism* (Springer 2002).

Ligeti K and Franssen V, "Current Challenges in Economic and Financial Criminal Law in Europe and the US" in V Franssen and K Ligeti (eds), *Challenges in the Field of Economic and Financial Crime in Europe and the US* (Hart Publishing 2017).

Ligeti K and Simonato M, "Asset Recovery in the EU: Towards a Comprehensive Enforcement Model beyond Confiscation? An Introduction" in K Ligeti and M Simonato (eds), *Chasing Criminal Money: Challenges and Perspectives on Asset Recovery in the EU* (Bloomsbury Publishing 2017).

Linder SH, "Coming to terms with the public-private partnership: A grammar of multiple meanings" (1999) 43(1) American behavioral scientist 35.

Locke J, *Two Treatises of Government* (JM Dent & Sons Ltd 1689).

Lonardo L, "The Veiled Irreverence of the Italian Constitutional Court and the Contours of the Right to Silence for Natural Persons in Administrative Proceedings: Judgment of the Court (Grand Chamber) 2 February 2021, Case C-481/19, DB v Consob, ECLI: EU: C: 2021: 84" (2021) 17(4) European Constitutional Law Review 707.

Loucaides LG, "Questions of fair trial under the European Convention on Human Rights" (2003) 3 Human Rights Law Review 27.

Loven C, *Fundamental rights violations by private actors and the procedure before the European Court of Human Rights: A study of verticalised cases* (Intersentia 2022).

Luchtman M, Karagianni A, and Bovend'Eerdt K, "EU Administrative Investigations and the Use of Their Results as Evidence in National Punititve Proceeding" in F Giuffrida and K Ligeti (eds), *Admissibility of OLAF final reports as evidence in criminal proceedings* (2019).

Luchtman M and Vervaele JAE, "Comparison of the Legal Frameworks" in M Luchtman and JAE Vervaele (eds), *Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with other EU law enforcement authorities (ECN/ESMA/ECB)* (Utrecht University 2017).

Luchtman MJJP, "Grensoverschrijdende sfeercumulatie-Over de handhavingssamenwerking tussen financiële toezichthouders, fiscale autoriteiten en justitiële autoriteiten in EU-verband" (PhD thesis, Wolf Legal Publishers 2007).

Lynskey O, "Deconstructing data protection: the 'added-value'of a right to data protection in the EU legal order" (2014) 63(3) International & Comparative Law Quarterly 569.

Maillart J.-B, "Anti-money Laundering Architectures. Between Structural Homogeneity and Functional Diversity" in B Vogel and J.-B Maillart (eds), *National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection* (Intersentia 2020).

— "The Anti-Money Laundering Architecture of the European Union", in B Vogel and J.-B Maillart (eds), *National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection* (Intersentia 2020).

— "The Anti-Money Laundering Architecture of the FATF", in B Vogel and J.-B Maillart (eds), *National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection* (Intersentia 2020).

Majone G, "From the positive to the regulatory state: Causes and consequences of changes in the mode of governance" (1997) 17(2) Journal of public policy 139.

Malacarne A, "Lo "Statuto Europeo" della Data Retention: Luci e Ombre" (Bernardini L and De Caro C eds, 2025).

Malgieri G, *Vulnerability and data protection law* (Oxford University Press 2023).

Malgieri G and De Hert P, "One European legal framework for surveillance: The ECtHR's expanded legality testing copied by the CJEU" in *Surveillance and privacy in the digital age: European, transatlantic and global perspectives* (Bloomsbury Publishing 2021).

Manes V, "Profili e confini dell'illecito para-penale" (2017) 60(3) Rivista italiana di diritto e procedura penale 988.

Manes V and Caianiello M, *Introduzione al diritto penale europeo. Fonti, metodi, istituti, casi* (Giappichelli Editore 2020).

Manget FF, "Intelligence and the criminal law system" (2006) 17 Stan. L. & Pol'y Rev. 415.

Mangiaracina A, "A new and controversial scenario in the gathering of evidence at the European level: the proposal for a directive on the European investigation order" (2014) 10(1) Utrecht Law Review.

— "Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici... e non solo" [2021] (4) Processo penale e giustizia 729.

Marafioti L, *Scelte autodifensive dell'indagato e alternative al silenzio* (Giappichelli 2000).

Marchesi D and Panzavolta M, "Keep silence for yourself: The protection of the right to silence in the Italian criminal justice system" (2021) 12(3) New Journal of European Criminal Law 365.

Marcus AJ, *Financial intelligence units (FIUs): Effective institutional design, mandate and powers* (Transparency International 2019).

Marquenie T, "The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework" (2017) 33(3) Computer Law & Security Review 324.

Marsilio M, Cappellaro G, and Cuccurullo C, "The intellectual structure of research into PPPS: A bibliometric analysis" (2011) 13(6) Public Management Review 763.

Maugeri AM, "Il regolamento (UE) 2018/1805 per il reciproco riconoscimento dei provvedimenti di congelamento e di confisca" [2019] (1) Diritto Penale Contemporaneo 42.

Mazza O, "L'interrogatorio e l'esame dell'imputato nel suo procedimento" [2004].

— *Presunzione d'innocenza e diritto di difesa*, Diritto penale e processo (2014).

— "I controversi rapporti tra processo penale e tributario" (1) Rassegna tributaria.

Meerts C, "Corporate investigations: Beyond notions of public–private relations" (2020) 36(1) Journal of Contemporary Criminal Justice 86.

Menges L, "A defense of privacy as control" (2021) 25(3) The Journal of Ethics 385.

Metzger GE, "Privatization as delegation" (2003) 103 Colum. L. Rev. 1367.

— "Private Delegations, Due Process, and the Duty to Supervise", in J Freeman and M Minow (eds), *Government by contract: Outsourcing and American democracy* (Harvard University Press Cambridge, MA 2009).

Meyer F, "Recognizing the unknown–the new confiscation regulation" (2020) 10(2) European Criminal Law Review 140.

— "Duties to cooperate and their limits under the case law of the ECtHR and the ECJ" (2023) 19(2) European Integration Studies.

Michéa F and Rousvoal L, "The Criminal Procedure Out of Itself: A Case Study of the Relationship Between EU Law and Criminal Procedure Using the ETIAS System" (2021) 2021(1) European Papers-A Journal on Law and Integration 473.

Miettinen S, *Criminal law and policy in the European Union* (Routledge 2013).

Milaj J and Kaiser C, "Retention of data in the new Anti-money Laundering Directive—'need to know'versus 'nice to know'" (2017) 7(2) International Data Privacy Law 115.

Minow M, "Outsourcing power: How privatizing military efforts challenges accountability, professionalism, democracy" (2004) 46 Boston College Law Review 989.

— "Alternatives to the State Action Doctrine in the Era of Privatization, Mandatory Arbitration, and the Internet: Directing Law to Service Human Needs" (2017) 52 Harvard Civil Rights-Civil Liberties Law Review 145.

Mirandola S, "Borderless enforcement of freezing and confiscation orders in the EU: the first regulation on mutual recognition in criminal matters" (3, 2020) vol 20.

Mireille D.-M, "Les forces imaginantes du droit I. Le relatif et l'universel" [2004] Éditions du Seuil.

Mitsilegas V, "New forms of transnational policing: The emergence of financial intelligence units in the European Union and the challenges for human rights: Part 1" (1999) 3(2) Journal of Money Laundering Control 147.

— "Money laundering counter-measures in the European Union" [2003].

— "Countering the chameleon threat of dirty money:'Hard'and 'soft'law in the emergence of a global regime against money laundering and terrorist finance",

in A Edwards and P Gill (eds), *Transnational Organised Crime* (Routledge 2004).

Mitsilegas V, "The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU" (2006) 43 Common Market Law Review 1277.

— "European criminal law and resistance to communautarisation after Lisbon" (2010) 1(4) New Journal of European Criminal Law 458.

— *EU criminal law after Lisbon: rights, trust and the transformation of justice in Europe* (vol 1, Bloomsbury Publishing 2016).

— "'Security Law'and Preventive Justice in the Legal Architecture of the European Union", in U Sieber and others (eds), *Alternative systems of crime control: national, transnational, and international dimensions* (Duncker & Humblot 2018).

— "The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence" (2018) 25(3) Maastricht Journal of European and Comparative Law 263.

— "The preventive turn in European security policy: Towards a rule of law crisis?", in (Cambridge University Press 2020).

— *EU criminal law* (Hart Publishing 2022).

Mitsilegas V, Bergstršm M, and Konstantidines T, *Money laundering* (Edward Elgar Publishing 2016).

Mitsilegas V and Gilmore B, "The EU legislative framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards" (2007) 56(1) International & Comparative Law Quarterly 119.

Mitsilegas V, Monar J, and Rees W, *The European Union and internal security: guardian of the people?* (Springer 2003).

Mitsilegas V and Vavoula N, "The evolving EU anti-money laundering regime: challenges for fundamental rights and the rule of law" (2016) 23(2) Maastricht journal of European and comparative law 261.

Monar J, "Justice and Home Affairs: The Treaty of Maastricht as a decisive intergovernmental gate opener" in (Routledge 2012).

Monar J, "Justice and home affairs" (2012) 50 Journal of Common Market Studies 124.

Moneyval, *The postponement of financial transactions and the monitoring of bank accounts* (techspace rep, Council of Europe 2013).

Morgan R, "The Third Pillar: an introduction" in J Monar and R Morgan (eds), *The Third Pillar of the European Union: Cooperation in the fields of justice and home affairs* (European Interuniversity Press Brussels 1994).

Mörth U, "The market turn in EU governance—the emergence of public–private collaboration" (2009) 22(1) Governance: An International Journal of Policy, Administration, and Institutions 99.

Mouzakiti F, "Cooperation between financial intelligence units in the European Union: stuck in the middle between the general data protection regulation and the police data protection directive" (2020) 11(3) New Journal of European Criminal Law 351.

Murphy C, "Proposal to amend Directive (EU) 2019/1153: Single access point to bank account registries" [2024].

Nance MT, "The regime that FATF built: an introduction to the Financial Action Task Force" (2018) 69(2) Crime, Law and Social Change 109.

Negri D, "La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)" [2016] Archivio penale 44.

— "Modelli e concezioni", in A Camon and others (eds), *Fondamenti di procedura penale* (Wolters Kluwer-Cedam 2025).

Nehl HP, "Article 48 (Administrative Law)" in S Peers and others (eds), *The EU Charter of fundamental rights: a commentary* (Bloomsbury Publishing 2021).

Neo D, "A Conceptual Overview of Bank Secrecy" in S Booyse and D Neo (eds) (Cambridge University Press May 2017).

Nies J, "Detecting Economic and Financial Crime: A Special Toolkit of Investigation Techniques in Luxembourg" in V Franssen and K Ligeti (eds), *Challenges in the Field of Economic and Financial Crime in Europe and the US* (Hart Publishing 2017).

Novak WJ, "Public-private governance: A historical introduction" in J Freeman and M Minow (eds), *Government by contract: Outsourcing and American democracy* (Harvard University Press Cambridge, MA 2009).

O'Keeffe D, "The Tampere summit: The ties that bind or The Policeman's Ball" [1999] Common Market Law Review 1119.

O'Malley P, "Neoliberalism, crime and criminal justice" (2016) 16(10) Sydney Law School Research Paper.

O'malley P, "Risk, power and crime prevention" (1992) 21(3) Economy and society 252.

Oerlemans J.-J and Van Toor D, "Legal aspects of the EncroChat operation: a human rights perspective" (2022) 30(3-4) European Journal of Crime, Criminal Law and Criminal Justice 309.

Orlandi R, *Atti e informazioni della autorità amministrativa nel processo penale: contributo allo studio delle prove extracostituite* (Giuffrè Editore 1992).

Panzavolta M, "Ordine di indagine europeo e indagini bancarie: spunti di riflessione sul concetto di caso interno analogo e atto di indagine alternativo" in M caianiello and A Di Pietro (eds), *Indagini penali e amministrative in materia di frodi IVA e doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale* (Cacucci 2016).

Patanè V, *Il diritto al silenzio dell'imputato* (vol 21, G Giappichelli Editore 2006).

— "Nemo tenetur se detegere: coordinate europee e parametri costituzionali del diritto a non collaborare dell'imputato" (2024) 64(6) Cassazione penale 1999.

Pavlidis G, "Financial information in the context of anti-money laundering: Broadening the access of law enforcement and facilitating information exchanges" (2020) 23(2) Journal of Money Laundering Control 369.

Pavlidis G, "Financial action task force and the fight against money laundering and the financing of terrorism: Quo vadimus?" (2021) 28(3) Journal of Financial Crime 765.

Peers S, "Mutual recognition and criminal law in the European Union: Has the Council got it wrong" (2004) 41 Common Market Law Review 5.

— *EU Justice and Home Affairs Law: Volume II: EU Criminal Law, Policing, and Civil Law* (Oxford University Press 2024).

Penna M, "The 'pre-investigative'role of financial intelligence units in recovering assets" in K Ligeti and M Simonato (eds), *Chasing Criminal Money: Challenges and Perspectives on Asset Recovery in the EU* (Bloomsbury Publishing 2017).

Peretti T, "Constructing the state action doctrine, 1940–1990" (2010) 35(2) Law & Social Inquiry 273.

Pivaty A and others, “Opening Pandora’s box: The right to silence in police interrogations and the Directive 2016/343/EU” (2021) 12(3) New Journal of European Criminal Law 328.

Pivaty A and others, “Strengthening the protection of the right to remain silent at the investigative stage: What role for the EU legislator?” (2021) 12(3) New Journal of European Criminal Law 427.

Prechal S, “The Court of Justice and Effective Judicial Protection: What Has the Charter Changed?” in C Paulussen and others (eds), *Fundamental Rights in International and European Law: public and private law perspectives* (Springer 2015).

Pulitanò D, “Sicurezza e diritto penale” (2009) 2 Rivista italiana di diritto e procedura penale 547.

Purtova N, “Between the GDPR and the police directive: Navigating through the maze of information sharing in public–private partnerships” (2018) 8(1) International Data Privacy Law 52.

Quintel T, “Follow the Money, If You Can-Possible Solutions for Enhanced FIU Cooperation Under Improved Data Protection Rules” [2019] University of Luxembourg Law Working Paper No 2019-001.

Quintel T and Sajfert J, “Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities” in *Commentary on the General Data Protection Regulation* (Edward Elgar Publishing Ltd 2017).

Rafaraci T, “General Considerations on the European Investigation Order” in S Ruggeri (ed), *Transnational Evidence and Multicultural Inquiries in Europe: Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-border Cases* (Springer 2013).

Recchia N, “Il rinvio pregiudiziale alla corte di giustizia in materia penale ovvero della doppia pregiudizialità in action” [2023] (4) Rivista italiana di diritto e procedura penale 1437.

Redmayne M, “Rethinking the privilege against self-incrimination” (2007) 27(2) Oxford Journal of Legal Studies 209.

Rizcallah C, “Le principe de confiance mutuelle dans l’Union européenne: un principe en péril” (2022) 3(3) Les Cahiers de la justice 447.

Roberts A, "Pre-trial defence rights and the fair use of eyewitness identification procedures" (2008) 71(3) The Modern Law Review 331.

Rodotà S, "Data protection as a fundamental right" in *Reinventing data protection?* (Springer 2009).

Rojszczak M, "The uncertain future of data retention laws in the EU: Is a legislative reset possible?" (2021) 41 Computer Law & Security Review 105572.

Romzek BS and Dubnick MJ, "Accountability" in JM Shafritz (ed), *Defining public administration* (Routledge 2018).

Rose N and Miller P, "Political power beyond the State: problematics of government" (2010) 61 The British journal of sociology 271.

Rossi Dal Pozzo F and Gialuz M, "Articolo 6 - Diritto alla libertà e alla sicurezza" in P Oreste and others (eds), *Carta dei diritti fondamentali dell'Unione europea* (Giuffrè Editore).

Rouvroy A and Poullet Y, "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy" in *Reinventing data protection?* (Springer 2009).

Sakowicz A, "The right to silence in the EU directive 2016/343 on the strengthening of certain aspects of the presumption of innocence from the perspective of polish criminal proceedings" (2020) 41 Rev. Eur. & Comp. L. 55.

Salazar L, "La lotta alla criminalità nell'Unione: passi in avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il programma dell'Aia" (2004) 11 Cass. pen 3533.

— "La costruzione di uno spazio penale comune europeo", in G Grasso and R Sicurella (eds), *Lezioni di diritto penale europeo* (Giuffrè Editore 2007).

Sanvitale F, "Gli ordini europei di conservazione e produzione: un passo indietro per la tutela dei diritti fondamentali nelle indagini digitali?" (Bernardini L and De Caro C eds, 2025).

Savas ES, *Privatization and public-private partnerships* (Chatham House New York 2000).

Sayers D, "Article 48 (Criminal Law)" in S Peers and others (eds), *The EU Charter of fundamental rights: a commentary* (Bloomsbury Publishing 2021).

Schumann Barragán GJ, *Derecho a la tutela judicial efectiva y autonomía de la voluntad: los contratos procesales* (Marcial Pons 2022).

Schwartz PM, "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices" [2000] Wis. L. Rev. 743.

Seidman H and Gilmour R, *Politics, position, and power: From the positive to the regulatory state* (Oxford University Press 1986).

Shahlaei F, "The anatomy of a valid waiver of human rights" (2024) 25(2) Human Rights Law Review.

Sicurella R, "Il Corpus Juris come modello per la definizione di un sistema penale europeo" in G Grasso and R Sicurella (eds), *Lezioni di diritto penale europeo* (Giuffrè Editore 2007).

Sicurella R and Scalia V, "Data mining and profiling in the Area of Freedom, Security and Justice: state of play and new challenges in the balance between security and fundamental rights protection" (2013) 4(4) New Journal of European Criminal Law 409.

Sieber U, "The New Architecture of Security Law-Crime Control in the Global Risk Society" in U Sieber and others (eds), *Alternative systems of crime control: national, transnational, and international dimensions* (Duncker & Humblot 2018).

Siena FA, "The European anti-money laundering framework–At a turning point? The role of financial intelligence units" (2022) 13(2) New Journal of European Criminal Law 216.

Silva PG, "Recent developments in EU legislation on anti-money laundering and terrorist financing" (2019) 10(1) New Journal of European Criminal Law 57.

Silva SO, "Regulation (EU) 2018/1805 on the mutual recognition of freezing and confiscation orders: A headlong rush into Europe-wide harmonisation?" (2022) 13(2) New Journal of European Criminal Law 198.

Simmons AJ, "The Lockean theory of rights" [2020].

Simmons B, "International efforts against money laundering" [2000].

Simonato M and Lassalle M, "A fragmented approach on asset recovery and financial investigations: a threat to effective international judicial cooperation?" (Durdevic Z and Ivicevic Karas E eds, Croatian Association of European Criminal law 2015).

Soo A, "Article 12 of the Directive 2013/48/EU: A starting point for discussion on a common understanding of the criteria for effective remedies of violation of

the right to counsel" (2017) 25(1) European Journal of Crime, Criminal Law and Criminal Justice 31.

Spielmann D, "The European Convention on Human Rights: the European Court of Human Rights" in D Oliver and J Fedtke (eds), *Human rights and the private sphere–A comparative analysis* (Routledge 2007).

Starmer K, "Positive Obligations under the Convention" in J Jowell and J Cooper (eds), *Understanding Human Rights Principles* (Hart Publishing 2001) vol 4.

Stessens G, *Money laundering: a new international law enforcement model* (Cambridge University Press 2000).

Taruffo M, *La semplice verità: il giudice e la costruzione dei fatti* (Laterza 2009).

Thony J.-F, "Processing financial information in money laundering matters: the financial intelligence units" (1996) 4 European Journal of Crime, Criminal Law & Criminal Justice 257.

Tonini P and Conti C, *Il diritto delle prove penali nel sistema accusatorio contemporaneo* (Giuffrè Editore 2025).

— *Manuale di procedura penale* (Giuffrè Editore 2025).

Tonnara P, "Risk assessment" in D Siclari (ed), *The New Anti-Money Laundering Law: First Perspectives on the 4th European Union Directive* (Palgrave 2015).

Tosza S, "The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?" (2023) 9(2) European Data Protection Law Review.

Tosza S, "Mutual Recognition By Private Actors In Criminal Justice? E-Evidence Regulation And Service Providers As The New Guardians Of Fundamental Rights" (2024) 61(1) Common Market Law Review.

Trechsel S and Summers S, *Human rights in criminal proceedings* (Oxford university press 2006).

Tzanou M, "Is data protection the same as privacy? An analysis of telecommunications' metadata retention measures" (2013) 17(3) Journal of Internet Law 20.

Ubertis G, *Principi di procedura penale europea. Le regole del giusto processo* (Cortina 2009).

— *Profili di epistemologia giudiziaria* (Giuffrè Francis Lefebvre 2015).

— "Prova, verità e processo" [2020] Archivio penale 547.

Unger B and Van Waarden F, "How to dodge drowning in data? Rule-and risk-based anti money laundering policies compared" (2009) 5 Review of Law and Economics 953.

Van Alstyne WW and Karst KL, "State Action" [1961] Stanford Law Review 3.

Van den Broek M and Addink H, "Prevention of money laundering and terrorist financing from a good governance perspective" in B Unger and D van der Linde (eds), *Research Handbook on Money Laundering* (Edward Elgar Publishing 2013).

Van Ham H and Koppenjan J, "Building public-private partnerships: Assessing and managing risks in port development" (2001) 3(4) Public management review 593.

Vavoula N, *Immigration and privacy in the law of the European Union: the case of information systems* (Brill 2022).

Veenbrink M, "The privilege against self-incrimination in EU competition law: a deafening silence?" (2015) 42(2) Legal Issues of Economic Integration.

— "The Freedom from Self-Incrimination—A Strasbourg-Proof Approach? Cases C-466/19 P Qualcomm and C-481/19 P DB v Consob" (2021) 12(10) Journal of European Competition Law & Practice 750.

Vermeulen G and Kusak M, "Unblurring the Fuzzy Line Between Specialty and Data Protection in EU Mutual Legal Assistance After the European Investigation Order" (2023) 29(4) European Journal on Criminal Policy and Research 647.

Vervaele JAE, "Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?" [2005] Revue internationale de droit pénal 409.

— "Economic crimes and money laundering: a new paradigm for the criminal justice system?", in B Unger and D van der Linde (eds), *Research Handbook on Money Laundering* (Edward Elgar Publishing 2013).

— "Surveillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system?", in S Gutwirth, R Leenes, and P De Hert (eds), *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges* (Springer 2013).

Vervaele JAE, "Lawful and fair use of evidence from a European Human Rights Perspective" in F Giuffrida and K Ligeti (eds), *Admissibility of OLAF final reports as evidence in criminal proceedings* (2019).

Villamarín López ML, "The presumption of innocence in Directive 2016/343/EU of 9 March 2016" (3, 2017) vol 18.

Virzo R, *La confisca nell'azione internazionale di contrasto ad attività criminali* (Edizioni scientifiche italiane 2020).

Vogel B, "Reinventing EU Anti-Money Laundering. Towards a Holistic Legal Framework" in B Vogel and J.-B Maillart (eds), *National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection* (Intersentia 2020).

— "The Anti-Money Laundering Architecture of Germany", in B Vogel and J.-B Maillart (eds), *National and international anti-money laundering law: developing the architecture of criminal justice, regulation and data protection* (Intersentia 2020).

— "Balancing procedural fairness and surveillance in criminal procedure law: between the adversarial principle and a resurgence of the inquisitorial process", in *Secret evidence in criminal proceedings: balancing procedural fairness and covert surveillance* (Duncker & Humblot 2021).

— "Potentials and limits of public-private partnerships against money laundering and terrorism financing" (01, 2022).

Vogel B and Lassalle M, "Developing Public–Private Information Sharing to Strengthen the Fight against Money Laundering and Terrorism Financing: Recommendations for the European Union and its Member States" in *Law of Public-Private Cooperation against Financial Crime: Developing Information-Sharing on Money Laundering and Terrorism Financing* (Intersentia 2024).

Vogiatzoglou P and Valcke P, "Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law" in *Research handbook on EU data protection law* (Edward Elgar Publishing 2022).

Vogler R, *A world view of criminal justice* (Routledge 2005).

Wæver O, "Politics, security, theory" (2011) 42(4-5) Security dialogue 465.

Wahl T, "The EU's New AML Single Rulebook Regulation" [2024] Eucrim.

Walkila S.-HI, *Horizontal effect of fundamental rights in EU law* (Europa Law Publishing 2016).

Weyembergh A and Joncheray N, "Punitive administrative sanctions and procedural safeguards: a blurred picture that needs to be addressed" (2016) 7(2) New Journal of European Criminal Law 190.

Wilinski P and Kiejnich-Kruk K, "Right to Effective Legal Remedy in Criminal Proceedings in the EU. Implementation and Need for Standards" (2023) 54 Review of European & Comparative Law 147.

Wisman T, "Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things" (2013) 4(2) European Journal of Law and Technology.

Wisman TH and Tijm RJ, "The radical reframing of the purpose limitation principle-why the Dutch delegation uprooted data protection" in *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022).

Xenos D, *The positive obligations of the state under the European Convention of Human Rights* (Routledge 2012).

Zacchè F, "Gli effetti della giurisprudenza europea in tema di privilegio contro le autoincriminazioni e diritto al silenzio" in *Giurisprudenza europea e processo penale italiano* (Giappichelli 2008).

Zanfir-Fortuna G, "Article 21 - Right to object" in C Kuner, LA Bygrave, and C Docksey (eds), *The EU General Data Protection Regulation (GDPR)* (Oxford University Press 2020).