The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail. See Treaty of Lisbon (2007), art. 2, available at www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-european-union-and-comments/title-1-common-provisions/2/article-2.html.

Daily News Hungary, cit.


Daily News Hungary, cit.


Ibid.


ANTI-CORRUPTION AND ANTI-MONEY LAUNDERING: CRIMINAL NETWORKS AND PREVENTION MODELS COMPARED
Marco Naddeo*

*University of Salerno, Department of Legal Sciences (School of Law)
(mnaddeo@unisa.it)

Abstract
This paper aims to examine the phenomena of corruption and money laundering, outlining the relationship of “continuity” running between them. The analysis presented here focuses on the evolution of modern criminal networks and their methods in recent years. The results highlight the points of convergence between the prevention models compared here (anti-corruption and anti-recycling) and the importance of redressing the information imbalance underlying the asymmetry between the State and organised crime. From this point of view, judicial support and internal control systems are indispensable tools in the fight against transnational crime.

Keywords: Anti-Corruption, Anti-Money Laundering, Criminal Networks, Prevention Models.
LUFTA KUNDËR KORRUPSIONIT DHE PASTRIMIT TË PARAVE: RRJETET KRIMINALE DHE KRAHASIM I MODEVELE TË PARANDALIMIT

Marco Naddeo*

*Universiteti i Salernos, Departamenti i Shkencave Ligjore (Shkolla e së Drejtës) (mnaddeo@unisa.it)

Abstrakt
Ky punim ka për qëllim të shqyrtojë fenomenin e korrupsionit dhe pastrimit të parave, duke përcaktojë marrëdhënien “e vazhdimitisë” me tyre. Analiza e paraqit ur këtu fokusueset në evolimin e rrjetevës modern shqiptar kriminale dhe metodat e tyre në vitet e fundit. Rezultatet nxjerrin në pah pikat e konvergjencës midis modevele të parandalimit të krahasuara këtu (anti-korrupsioni dhe anti-riciklimi) dhe rëndësinë e korrigjimit të mosbalancës së informacionit që qëndron në themel të asimetrisë midis shtetit dhe krimit të organizuar. Nga ky këndvështrim, mbështetja gjyqësore dhe sistemet e kontrollit të brendshëm janë mjete të domosdoshmë në luftën kundër krimit transnacional.

Fjalë kyçë: anti-korrupsioni, lufta kundër pastrimit të parave, rrjetet kriminale, modele parandalimi.

1. Corruption and Money Laundering from the Criminological Perspective

Empirically speaking, it is clear that corruption and money laundering are functionally interconnected and are, from a meta-legal point of view, linked along a continuum. We therefore witness the laundering of proceeds from acts of corruption that can be considered predicate offences under article 648-bis of the Italian Criminal Code. After all, bribery is an offence committed with criminal intent to obtain money, goods, or other benefits potentially carried out in such a way as to conceal their criminal origin. Recalling the words of Hassemer, one could say that there is a perfect correspondence between the “elements of the offence and the type”.

From the phenomenological point of view, these two forms of white-collar crime frequently go hand in hand, now constituting a means for organised crime to take control of entire revenue cycles over larger territorial areas. It is no coincidence that those who have recently attempted to represent the position assumed by criminal networks in geometric form place them at the peak of a triangle with public administrations and the economy (1) at opposite corners of the base. Thus, corruption is a method of infiltration, and money laundering is a link between the market and crime. Naturally, organised crime exploits the damage arising from (different levels of) corruption to influence decisions taken by the public administration, resorting to bribes (level I), the buying and selling of civil functions (level II), and even the regular infiltration of members of criminal organisations in public service (level III). Corruption can affect the management of public affairs, diverting considerable resources for criminal...
gain. These then enter the market and contaminate the economy, damaging healthy operators and others. This then is the lowest common denominator of two circumstances that can cause severe disruption to the public administration and the economy, as well as the power to act across borders typical of the so-called crimes of opportunity. These can constitute critical financial assets and even influence the weightiest decisions concerning the economy and the administration of public affairs (2)

On the other hand, white-collar and organised crime follow at least partially identical channels with overlapping results; indeed, it may be more correct to say that they intensify each other, being able to count on “a multiplier of polluting income conveyed by enterprises with mafia stakeholders or through illegal practices, which bring together and conceal the criminal links and illicit conduct of normal enterprises. Distortions of the market and competition, at national and international levels, affected by ‘non-competitive’ actors in terms of production, together with their profit- and financial management logic, constitute the indirect, but not remote, consequence of those synergies” (3). The driving force behind this dangerous upward spiral is the considerable (Return on Investment) ROI of the criminal economy, which – as will be explained below – makes the rules of the market even less attractive and often lacks the indispensable basis of consent required for them to be effective.

As a further complication, globalisation, paired with the technological innovation of the Fintech era, is providing new opportunities for economic crime, creating fresh and unexpected challenges for prevention and countering it. In addition, this illegality increasingly takes the form of a complex organisation, enticed by interests converging with those of enterprises and becoming so intricately intertwined as to reduce any probability of discovery. Similarly, “liquid corruption” eludes the typical pattern of criminal corruption and allows misconduct to reach the highest levels of local government, infiltrating public administrations and the economy using non-violent methods, also in the form of commercial activities (4). The goal is always the same: to increase profits and exceed the limit of optimisation in defiance of the rules of the game, forcing the instruments at their disposal (public office and economic resources) through increasingly complex and sophisticated manoeuvres that are difficult to intercept (5).

It should not be forgotten that such crimes can be compared to the dynamic games with incomplete information to which J. Nash reduced mixed strategies or probability distributions over pure strategies, namely games where pay-offs become multilinear forms regarding the probabilities the various actors play out their pure strategies by (6).

In this segment, the offender is very often a refined calculator adopting a strategy that takes the instruments of prevention and combat into consideration to find the best possible result (both in terms of gain and minimising inherent risk). This result will also depend on the decision that the other players in the field decide to adopt, providing the State with their invaluable support rather than shirking the requirement to take positive action or even deciding to collude with the criminals.

These, briefly, are the reasons compelling the legislator to draw up a cohesive criminal policy with prevention at the core of anti-corruption and anti-recycling strategies without the system relinquishing the necessary controls by falling back on a criminal policy that risks lagging behind the criminal “infiltration” examined here.
2. Models of Prevention vs. Criminal Networks

Effectiveness – in terms of the general observance of the law by those to whom it is addressed and those in charge of applying it – feeds on empirics (7). Hence, investigating the phenomenon and the current configuration of the criminal offence that it brings before the jurist must underpin the new models of prevention (and repression). Two principle factors deserve particular consideration in this regard: i) the asymmetry of information that places enforcement at a disadvantage with respect to criminal organisations, which are allowed to make their choice over again in sequence – also after observing the State-player’s move, and ii) the existence of several solutions which, to return to the aforementioned Game Theory, allow more balance and make the optimal strategy more complex, also considering the non-cooperative nature of the game (precluding preliminary negotiations between the opposing forces).

Regarding the first aspect, both corruption and money laundering can count on the predominance of rational choices adopted by professionals with access to sophisticated techniques and able to exploit the opportunities offered by technological developments aiming at the rarefaction of criminal conduct (the so-called de-individualisation of economic crime). In this area, a central role is played by the precious asset of information, which the white-collar workers aim to preserve, containing the risk of discovery despite State attempts to eliminate or, at least, reduce the information gap thanks to which it is at a disadvantage.

From this perspective, strategies to counter money laundering (Legislative Decree No. 231 of 21 November 2007) and corruption (Law No. 190 of 6 November 2012) are moving in the same direction, setting up structures to create essential information flows in terms of both prevention and repression. The obligation to co-operate actively and the figure of the Anti-Money Laundering Officer have counterparts in the anti-corruption plans and the Anti-Corruption and Transparency Officer, merged – according to the corporate compliance process – into the organisation and management models envisaged by Legislative Decree No. 231 of 8 June 2001 to protect the authority from liability arising from offences. In short, the system focuses on safeguarding the integrity of the economy and markets through the active collaboration of the public authorities (PTCT) and public employees (whistleblowing reports), as well as the support of numerous categories of qualified operators holding “privileged” financial/asset-related information (the so-called obliged parties: numerous categories including lawyers, notaries, accountants, etc.). These are “antibodies” inoculated into complex organisations to neutralise the “crime virus”, preventing it from corrupting the healthy subject and undermining its immune system, thus preventing it from being penetrated and exploited as a useful screen to reduce the probability of discovery of the crime. On the other hand, the best results depend precisely on the culture of legality and the resulting extent of social consensus that the law obtains (8). Thus, the second factor postulates that the decision to collaborate becomes dominant, namely maximising possible utility in terms of reconciling the commitment-incentive binomial (9) in such a way as to reach and oblige the involvement of the greatest number of actors.

The prevention of recycling and corruption models comply – at least in part – with this political-criminal ratio, seeking to internalise integrity and thus reclaim the humus in which economic crime can take root. By inducing the public administration and the private sector to set up internal supervisory bodies and equip themselves with information
flows, these disciplines allow a reduction of the asymmetry mentioned above and guarantee constant monitoring of the areas exposed to the risk of criminal activity through organisational protocols calibrated to the specific level of gravity to be addressed (the so-called risk-based approach) during the risk-assessment and risk management phases. The Italian legislator has understood that organised crime cannot exist without corruption, nor can it assume or maintain control of businesses without laundering large amounts of illicit wealth before injecting it into the market. This is why money laundering operates on a continuum with corruption, transforming unlawfully created gains from potential to actual wealth (10). The complex relationship between the two crimes is indicated by the supposition of stronger (anti-recycling) obligations to verify the identity of politically exposed persons and is formally legitimated by the leading international anti-recycling body operating within the OCSE framework: the Financial Action Task Force (FATF). In its 40 Recommendations, the FATF prioritised strengthening controls of politically exposed persons (PEPs). The Task Force analysed the connections between anti-recycling measures and the goal of fighting corruption, drawing up specific guidelines for the best use of anti-recycling safeguards to combat corruption (11), highlighting the vulnerability of corruption to anti-recycling safeguards. The same is true of the collaboration between the FATF and the G20 Anti-Corruption Working Group experts, which directs national policies to institutionalise collaboration between anti-money laundering and anti-corruption authorities, favouring information exchange. This kind of action can prevent corruption and help reduce the risk of money laundering, and anti-money laundering strategies can hinder the reuse of proceeds from corruption, increasing costs and making it less profitable. Furthermore, it is widely known that laundering proceeds from corruption often involves companies, non-profit organisations, and intermediaries/specialised professionals (gatekeepers) who facilitate operations to prevent unlawfully accumulated income being traced back to the bribe-taker (at the same time, the bribe-taker tends to conceal the resources set aside for corruption so as to prevent them being traced). For this reason, pursuing its goal to assist in the detection of suspicious transactions, the Financial Intelligence Unit for Italy (FIU) has drawn up patterns and models of anomalous conduct that (under Article 6(7)(b) of Legislative Decree 231/2007) supplement the indicators of anomalies that identify instances of corruption. Operational anomalies linked to officials or persons in charge of a public service in an environment prone to corruption are likely to be reported. Cases range from receiving bribes via front companies to cases of extortion and bribery. Other cases include the appropriation of public funds through one of the many forms of fraud, abuse of power, or conflict of interest (12). This figure reveals the transverse nature of corruption in relation to other offences (committed as a way of creating funds as a means of bribery), which is why corruption investigations often stem from inquiries into a variety of offences through which the relevant funds are obtained (invoices for non-existent transactions through shell companies, misleading accounting, etc.). It is thus possible to overcome the obstacles linked to the unjustifiable exercise of institutional prerogatives exploited by PEPs to influence their interlocutors or to use public office in their own interests. From this point of view, we can already read in the communiqué of the Unità di Informazione Finanziaria per l’Italia (FIU) of 8 July 2010, that “in terms of recycling prevention, abuse in the disbursement and management of public funding to undertakings is becoming increasingly significant”. It is interesting to note that – even then – the issue
was considered “significant, on the one hand, because of disruption to market mechanisms damaging honest businesses, and, on the other, due to the obvious connections between the criminal activity in question and corruption, with a high risk of influencing and interfering with public decision-making choices”. It is no coincidence that the anomaly indicator linked to the identity of the person involved in the transaction relates to PEPs, i.e. natural persons who hold a key public office (or ceased to hold one less than a year previously), as well as their family members and those who are known to have close links with them as listed in Article 1(2)(dd) of Legislative Decree 231/2007.

3. Transnationality and Economic Activities in the Fintech Era

Upon closer inspection, the prevention system mentioned just now is based on collaboration between the private and public sectors but also on co-operation between authorities at both national and international levels. This holds true for both anti-money laundering and anti-corruption strategies, both of which involve economic activity and therefore tend to occur across national borders, exploiting the lack of regulatory uniformity and opacity within national legal systems.

The economic imprint and profitability are highly characteristic of foreign bribery, which distorts the economy and impedes growth. The profile of the new form of organised crime overturns the cliché of the old mafias and has become a new reality, taking the threat it poses to society to a higher level than anything conveyed through violence and intimidation. In the new criminal mindset, weapons take a backseat to economic power, fostering elastic corruption capable of eluding rigid national control (both in geographical and normative terms).

The sophisticated methods of today’s criminals demand new methods of investigation, especially judicial co-operation or powerful organisations such as the Joint Investigation Teams (JITs), fostering co-ordination and greater mutual trust between law enforcement bodies and judicial authorities. In this sphere too, we find synergies such as the agreement established in the memorandum of understanding between the National Anti-Mafia Directorate (NAD) and the Financial Intelligence Unit for Italy signed on 15 March 2021 seeking to “enable the judiciary to make more immediate use of the information contained in reports of suspicious operations and the data from foreign FIUs, thus allowing the Units to carry out comprehensive financial analysis”. It is significant that: i) the forms of collaboration between the NAD and the FIU are further strengthened to allow in-depth analysis of cases that emerge when cross-checking their data, and ii) that the information-sharing envisages communication with foreign FIUs.

The legislative response reveals the new features of an ontologically trans-national and invisible form of crime, one requiring strategic choices based on suspicion with workable rules that can reduce the offence to a level of mere danger, designing forms of prevention that engage the collaboration of persons informed of the facts who can assist in ascertaining possible criminal offences. Obligatory active co-operation involves creating indispensable databases (e.g., the Archivio Unico Informatico concerning money laundering) containing information collected during due diligence. It also gives rise to investigations by means of reports of suspicious transactions. These provide investigators with possible grounds for investigations or material for an investigation to corroborate crime reports.
The range of persons obliged to co-operate is also emblematic of the objectives pursued by the European and, consequently, national legislators: to prevent the financial system becoming a vehicle for laundering the proceeds of criminal activities or financing terrorism. Collaboration requires the contribution of various categories (from banking and financial intermediaries working with professionals to statutory auditors and other non-financial operators), and others are continually being added. It is significant, for example, that, among its main innovations, Directive 2018/843/EU, known as the Fifth European Anti-Money Laundering Directive, extends the list of those required to collaborate to include virtual currency service providers. The update incorporates the requirements of the FATF standards, stating that “a virtual currency service provider is considered to be any natural or legal person who provides third parties, on a professional basis, including online, with services relating to the use, exchange, and/or storage of virtual currency and its conversion from or into legal tender or digital representations of value, including those convertible into other virtual currencies, as well as the services of issuing, offering, transferring and clearing, and any other service relating to acquisition, negotiation, or intermediation in the exchange of such currencies”. Such is the mark left on anti-money laundering by the new Fintech era.

This evolution in legislative terms reminds us that “the more complex the structures of society become, the more complex the crime that reflects its disorders” (13). This process involves a form of currency skeuomorphism, initially represented by electronic money and then by the Altcoin, an instrument equivalent to the banknote in terms of anonymity as it “requires neither the identity of the counterparties nor the reason for payment to be made known. However, being digital, a pure number divisible and multipliable at will, it allows transfers of any amount, from micro-payments of a few cents to the settlement of international business transactions” (14). In short, financial technology complicates the “game”, making it even more challenging to identify the actual holder of the financial transaction, shielded by the ubiquitous nature of virtual currencies. In this context, criminals can engage mixing services (also known as cryptocurrency tumblers) to exploit the complex virtual currency transfer techniques. Using bounce accounts or pool/pot accounts combined with Blockchain technology, these practices make the reconstruction of the intermediate steps between the entry (gateway) and exit (withdrawing) phases almost impossible, thus guaranteeing anonymity (15). It is no coincidence that the latest Europol (16) Internet Cybercrime Centre (EC3) report reveals the directly proportional relationship between the capitalisation of the cryptocurrency market and the development of cybercrime, with consequences for integral digital recycling.

The possibility of new perspectives involving the professional “exchangers” converting virtual currency into legal tender (and vice versa) explains why exchangers feature among the figures required to provide input in terms of active collaboration in a bid to stabilise the enforcement of anti-money laundering policies. The logic remains the same, namely to exploit collaborators’ knowledge and their proximity to the actions, operations, or organisations that may constitute a risk of criminal behaviour. Once alerted, the authorities can take preventive measures to combat the crime in question.
4. The Contribution of AI (Artificial Intelligence)

The last aspect to discuss here is Artificial Intelligence (AI), which opens up whole new vistas, and, combined with the modern payment methods, shifts the game to the sphere of virtual reality, where traditional methods of combat have become anachronistic and, often, ineffective (17).

In addition to automation software, computer systems equipped with more than merely instrumental decision-making capabilities are increasingly becoming widespread. Robots come between humans and crime with significant implications for the criminal charges system (18) and the probability of the crime being successful. Setting aside any considerations regarding dogma, we can focus on the empirical aspect, confirming that thanks to Artificial Intelligence, the process of de-individualisation of financial crime appears to have been completed. Using what some researchers have called “rational entities” puts a further distance between humans and crime, also making it more difficult to detect a crime and trace it back to the perpetrator. The latest generation of algorithms metabolise an inconceivable amount of data they receive thanks to their advanced computational power by cloud-based computing technologies. In this way, the machine elaborates increasingly complex behaviour patterns that can result in highly opaque and unpredictable operations, even elaborating, with, for example, the so-called black-box algorithms, inextricable chains suitable for laundering vast flows of money of illicit origin.

This is the epitome of the crime of opportunities, where the increase of means is directly proportional to the realisation of opportunities for crime, which, on the other hand, hinders collective growth.

5. The Limits of a Criminal Law Based on Risk

The criminal abuse of Fintech tools is reflected in criminal policy, which shifts its main focus towards the frontiers of market access (for example, the criminalisation and repression of banking and financial abuse arising from malpractice in the management of savings-investment services, which echoes the administrative offence of service providers using virtual currency unlawfully under article 17-bis, paragraph 5 of legislative decree 141/2010) and contributes to risk situations or whistleblowing based on suspicion and often reflects a precautionary approach in criminal law.

Breaches of anti-money laundering obligations sanctioned according to the variegated Article 55 of Legislative Decree 231/2007 and the mechanisms of anti-corruption are risk-based in conjunction with the reduction of the scope of punishability that plays a predominant role in the related need to reduce the risk of criminal conduct through the stigma attached to crime (19).

On the other hand, the complexity of the crimes under discussion and the kind of interests involved justify the functional projection of rules merely designed to avert the exposure of the protected asset to risk before the illicit conduct translates into intrusion in the economy and commerce, causing further and, perhaps, even more severe consequences. It is precisely this preventive aspect that could lead to abandoning the protection of specific legal interests and favour a more indulgent perspective based on the ratio of protection, where the “punishment” verges on the “neutralisation of danger” (20) and offers the indubitable advantages of a criminal law based on crime-fighting. Nevertheless,
although the law of justice and the struggle for law still coexist in today’s world, revealing still admissible room for a law based on fighting crime, there is no question of allowing an unlawful “criminal law of the enemy” (21).

If not suitably contained, the advancement of criminal law grounded in a culture of suspicion risks overturning the rules and principles that guide it in the direction of justice. In this sense, an indispensable safeguard is that of “reasonableness”, which permits acceptance of the broader range of action typical of prevention and, therefore, an anticipated focus on the primary protection of the interests/function (procedures, orders, monitoring, etc.), assuring legal certainty and the exhaustiveness of the criminal precept with respect to the degradation typical of the flexibilization of the type.

This trend is well represented by those who hold that “economic crimes fall within the paradigm of the criminal law of globalisation. And this implies, by its very nature, less ‘protection at all costs’, springing from the flexibilization of the categories and the relativisation of the fundamental principles of legality, guilt, and proportionality, thus favouring the tendency of criminal law to expand” (22).

It is not only the problem of the ethical and deontological nature of the criminal proceeding that is worrying but the devaluing of the legal interest, the core of values that justifies the intervention of criminal law as a form of protection from the attacks typical of this kind of offence. To free the offence of the descriptive elements and modes of aggression that may constitute precise co-ordinates for those called upon to interpret the law means to bias criminal law towards a focus on efficiency, losing sight of the offence-legal interest binomial which can, instead, ensure that epistemological verification of the abstractly positivised type, especially when the legal interest requires protection of a preventive nature and is as volatile as the economic-financial one (23).

The themes of anti-corruption and anti-money laundering in the context of the “new finance” therefore mark the field and the problems to be addressed in economic criminal law. Superindividual legal interests deserve preventive protection (24), but starting from the interest rather than the rationes of protection is fundamental to ensure critical control over criminalisation also when criminal protection takes on the appearance of the protection of functions (25).

The probability of success of such a system, i.e., the prevention and repression of crimes by monitoring and managing risk, which can also use reports from private insiders, will shift – as mentioned previously – away from the participation or otherwise of the associates in the collaborative obligations able to become a “dominant” option from the point of view of enforcement. The underlying strategy is based on the asymmetrical power relationship with the antagonist-addressee. It must, therefore, consider a triple limitation that subordinates its effectiveness to i) the clarity of the rules, ii) the investments necessary to implement them (e.g., drafting organisational models and prevention plans) and, above all, iii) the advantages gained by their correct application. In this regard, legal scholarship clearly underlines how “the precise fulfilment of the regulations (...) must be accompanied and managed according to an ascending scale by mechanisms to qualify ratings and standing, by forms of privileged access to procedures of negotiation with the authorities, even admitting specific extenuating circumstances and reasons for non-punishability” (26). These are the basic premises of the chosen strategy. When they are not observed, they translate into the limits of the criminal law of risk when the traditional canons of the criminal law based on the act are already compromised. Implementing a culture of prevention puts fundamental principles of criminal law at risk.
leading to the full normalisation of offences that lose the characteristics of illegality of their positive and natural construct with an uncontrolled expansion of the criminal domain.

The consequence is confusing prevention, i.e., the containment of the risk of crime, with the extension of (theoretical and not even real) criminal risk producing particularly significant collateral effects, since “if this type of legislation has meaning, it is because it neutralises danger”. If it does not neutralise it, we are left with a mere attack on the right to confidentiality, professional loyalty with the advancement of a culture of suspicion, and the broadening of the obligation to denounce and disclose” (27).

References

(14) M. AMATO, L. FANTACCI, Per un pugno di Bitcoin, Milan, 2016, p. 3.
(18) L. PICOTTI, Diritto penale e tecnologie informatiche: una visione d’insieme, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), Trattato di diritto penale. Cybercrime, Milan, Utet, 2019, pp. 35 ff.; P. SEVERINO, Intelligenza artificiale e diritto penale, U. RUFFOLO (a cura di), Intelligenza artificiale. Il diritto, i diritti, l’etica, Milan, Giuffrè Francis Lefebvre, 2020; R. BORSARI,
(21) M. DONINI, op. cit., p. XXVIII; see also, Id., Diritto penale di lotta. Ciò che il dibattito sul diritto penale del nemico non deve limitarsi a esorcizzare, in Studi sulla questione criminale, n. 2/2007, pp. 55 ff.
(22) M. GAMBARDELLA, Condotte economiche e responsabilità penale, Turin, 2020, p. 7.
(23) M. NADDEO, Il diritto penale dell’economia nell’era del Fintech, BLP, forthcoming.
(26) A.R. CASTALDO, op.cit., p. 22.
(27) M. DONINI, op. cit., p. XXVIII.