



Breaking the vicious cycle: Confiscation, whistleblowing and technological innovations in the battle against criminal networks

Victoria Koutsoupia

<https://doi.org/10.3013/f22wmd70>

Abstract

High-risk criminal networks operate across all EU Member States, with significant disruptive consequences for both the economy and society. The landscape of organised crime is characterised by a networked environment where collaboration among criminals is seamless, systematic and profit-oriented. The most effective approach to severely weaken these networks is by targeting their illicit gains. The most significant – and perhaps the only effective – way to disrupt the criminal chain is through the confiscation of their profits. Additionally, whistleblowing and recent developments of similar practices are explored as effective methods for dismantling criminal networks. Confiscation targets the economic lifeblood of organised crime; whistleblowing improves detection and evidentiary leads; and technology (e.g. blockchain analytics, interoperable EU systems) scales both detection and recovery. The development of new technological tools offers more opportunities than ever to detect illegal profits and, consequently, seize them. Emerging technologies, such as artificial intelligence, blockchain and big data analytics, can play an important role in combating organised crime and enhancing law enforcement efforts. This paper explores confiscation as a strategy to combat organised crime and dismantle criminal networks, utilising new technologies to efficiently and effectively extract criminal profits. Furthermore, it delves into the efficiency of whistleblowing in disbanding and punishing criminal networks and ensuring justice. The paper examines these aspects not only by scrutinising recent legal developments but also by analysing case-law and providing examples of best practices from Member States. The analysis is structured accordingly: the second section defines the phenomenon; the third section examines confiscation; the fourth section analyses whistleblowing; the fifth section discusses technology-enabled crime and enforcement responses; and the last section concludes with policy priorities and future research.

Keywords: criminal networks, confiscation, whistleblowing, emerging technologies.

Methodology

This study employs a qualitative, multi-method design combining: (1) doctrinal legal analysis of EU and Member State instruments on asset recovery and whistleblower protection; (2) structured desk research of authoritative policy sources (e.g. serious and organised threat assessment reports by the European Union Agency for Law Enforcement Cooperation (Europol), European Commission communications and the new Directive (EU) 2024/1260 on asset recovery and confiscation); and (3) illustrative case studies to examine how confiscation, whistleblowing and technology interact in practice. Case studies were purposively selected based on three criteria: relevance to high-risk criminal networks; availability of triangulable public documentation (judgments, official reports, peer-reviewed literature); and variation in the underlying mechanism (confiscation-led disruption, whistleblower-led detection and technology-enabled investigation). Data was coded thematically across three pillars – confiscation, whistleblowing and technology – using an analytical framework that maps each pillar to its intended objective, mechanism of action, enabling legal tools and observable outputs. This framework supports within-case and cross-case comparisons and links findings back to the research problem. Limitations include reliance on secondary sources for some cases, uneven data granularity across Member States and absence of original interviews. Ethical considerations focus on the use of public sources and the protection of any named individuals through reliance on official documents and anonymised case descriptions, where appropriate.

1. Introduction

High-risk criminal networks generate revenues exceeding EUR 139 billion annually (European Commission, 2021), equivalent to approximately 1 % of the EU's gross domestic product (European Commission, 2020). These networks operate internationally, leveraging innovations in technology to enhance their activities. Such revenues could otherwise be utilised to improve public education and healthcare. High-risk criminal networks pose a significant threat to EU security, their operations spreading across the globe.

The enormity of the damage induced by such organised crime has been emphasised by the European Parliament and the Council (European Parliament, 2016, 2020). But what does 'high-risk criminal network' mean, and what strategies are employed to combat these malicious activities? This paper aims to dissect the role of confiscation in destabilising these networks, exposing their vulnerabilities and sabotaging their foundations.

To monitor these unlawful activities involving high-value targets, whistleblowing remains a critical tool. Our reliance on technology cannot be disregarded as these criminal networks also utilise it in their operations. The focus here is on the effective implementation of confiscation and whistleblowing to dismantle high-risk criminal networks in the digital age.

2. Defining serious and organised criminal activities in the EU

Organised crime refers to a consistent alliance of individuals engaged in illegal activities, adhering to an intricate system (Rider, 2023). Interestingly, the code of conduct and demeanour can hint at unity or shared mutual objectives within these groups (Gambetta, 2011). Crime is their regular occupation, usually involving affiliations with other criminal networks (Sergi, 2021). Organised crime is a sophisticated international operation (European Commission, 2021), involving members of multiple nationalities (Europol, 2021).

These networks thrive on cooperation, with operations orchestrated around profitability. Violence is unfortunately becoming more frequent and extreme (Europol, 2021). Some networks are mono-criminal, focusing on specific activities like drug trafficking or organised property crime, while others are poly-criminal, engaging in multiple types of criminal activity. The ominous potential of these high-risk criminal networks arises from their invasion of legitimate businesses, use of money-laundering tactics, resilience and adaptability, countermeasures to evade law enforcers, recruitment of minors and frequent reliance on corruption or violence. Therefore, understanding such high-risk networks paves the way to shattering their foundations, with the ultimate aim of bringing about trusted societal reform (European Commission: Directorate-General for Migration and Home Affairs and Kantar, 2020).

3. Confiscation of criminal assets

To impair the operations of high-risk criminal collectives, it is essential to target their financial underpinning, as illicit earnings are the lifeblood of their ventures (Hryniewicz-Lach, 2023). Enforced asset confiscation aims to be a powerful tool against these crime syndicates. Through judicial or authorised authority decisions, properties procured through unlawful pursuits are permanently confiscated. Thus, networks' prosperity and power are dramatically impeded. International collaboration is of paramount importance for the dynamic enforcement of asset seizures (Laghidze, 2023). Building close legal relations facilitates the forfeiture of properties derived from transnational criminal enterprises. Despite efforts to seize unlawfully acquired assets, which would have otherwise been laundered into the legitimate economy, the effectiveness of asset confiscation in the EU has been limited, with criminals retaining control over 98 % of their ill-gotten gains (Europol, 2016).

Asset recovery operates in five phases: identification, freezing, management, confiscation and disposal. Effective execution of these phases necessitates the collaborative efforts of diverse agencies – law enforcement, judiciary and asset management offices, to name a few. Within the EU, asset recovery offices, responsible for asset forfeiture and international cooperation, play a central role in this multi-agency network (Europol, 2021, p. 30).

The recently enforced Directive (EU) 2024/1260 on combating intensified criminal networks, with a focus on asset recovery and confiscation (European Parliament and Council of the European Union, 2024), exemplifies this crucial collective effort. Resolving discrepancies among national laws following the implementation of the previous asset recovery directive is essential to fostering effective inter-EU cooperation that adheres to the new confiscation rules. A strategic step towards disrupting high-risk criminal networks is the incorporation of unequivocal provisions on non-conviction-based confiscation (European Parliament and Council of the European Union, 2024a) and the introduction of an unexplained wealth confiscation regime (European Parliament and Council of the European Union, 2024b) as part of Directive (EU) 2024/1260. This innovative model targets organised crime by enabling the confiscation of assets without the requirement of a criminal conviction (Boeri et al., 2024). The United Kingdom's civil confiscation measures have proven to be particularly effective against organised crime (Hendry and King, 2016).

However, such revolutionary harmonisation of laws compels the provision of extensive security for fundamental rights at the EU level (Hryniewicz-Lach, 2023, pp. 243–267). Chapter V of Directive (EU) 2024/1260 outlines the mandatory protection at the national level for the right to a fair trial, effective remedy and defence for impacted individuals (European Union Agency for Fundamental Rights, 2012). This progress illuminates the potential for developing increasingly potent tools to streamline every stage of asset recovery (Sakellarakis, 2022). Demands to create a secure environment that substantially mitigates risks posed by high-risk criminal networks (European

Commission, 2020) are murmurings of a society impatient for change. The primary goal of the legislation is to pre-empt and combat organised crime and high-risk criminal networks.

Investing in efforts to prevent and combat these high-risk criminal networks addresses one of the most significant threats to the EU's security (European Union, 2024). Directive (EU) 2024/1260 targets crimes committed within criminal organisations. Profits from these illicit operations often pave the way for more serious cross-border crimes, as noted in recital 10 (Sakellarakis, 2022). Reallocating and investing confiscated assets into local communities can play a pivotal role in curbing the activities of high-risk criminal networks (Maugeri, 2024). While confiscation strikes at illicit gains, whistleblowing accelerates detection and case-building by providing insider information that is otherwise costly or impossible to obtain.

4. The power of whistleblowing

Unveiling criminal activities is like solving a complex puzzle, and the integral pieces that lead to its resolution are often supplied by whistleblowers. These individuals form the backbone of the investigative process, triggering 95 % of police investigations through their diligent reporting (Miethe and Rothschild, 1994). In the heart of flourishing organisations and societies lies the ability to recognise and address deviant behaviour (Bergemann, 2024). Here, the whistleblower plays the role of an internal watchdog, catching and reporting instances of misconduct or criminality as they occur (Gottschalk and Asting, 2022). As the world advances, so does the art of whistleblowing, evolving into an essential tool for detection, investigation and prosecution of economic crimes (European Parliament and Council of the European Union, 2019a). European Union policymakers are harnessing the power of whistleblowing, aiming to uncover illicit activities on a broader scale (Karpacheva and Hock, 2024). The role of technology in whistleblowing is also becoming increasingly prominent. It can ensure stronger protections for the whistleblowers, increasing the volume of leaked information and facilitating its analysis and global distribution (Munro and Kenny, 2023).

In essence, whistleblowing serves as an efficient means to penetrate formidable criminal networks. Leaders who have so far managed to elude justice can now be targeted with accuracy. Acquiring specific information disrupts the foundations of these networks and leads to effective arrests. Although pivotal in unveiling high-risk criminal networks, whistleblowers inevitably expose themselves to potential dangers. They may face job loss, legal suits, threats or even physical harm. Therefore, creating a safe ecosystem for these individuals is indispensable, as it encourages reporting and aids in crime prevention, detection and penalisation (Terracol, 2023).

Countries worldwide are recognising this need and establishing robust whistleblower protection legislation (Vandekerckhove, 2010). Key among these is Directive (EU) 2019/1937 (Kačiku Baljija and Min, 2023), which aims to harmonise whistleblower legislation among Member States, ensure confidentiality and protect against retaliation (Council of Europe, 2019). By contrast, the United States looks to monetary rewards as an incentive for whistleblowing, raising ethical dilemmas as this approach may be perceived as commercialising a public service. Nevertheless, the power of incentives in encouraging whistleblowing cannot be overlooked (European Commission, 2018).

Thus, a modified model that provides whistleblowers of high-risk criminal networks with protections, possible amnesty and leniency for their role in the network is proposed. Furthermore, significant rewards sourced from seized

criminal assets could be offered. Involving legal intermediaries in these processes can heighten efficiency and inspire confidence. They could serve as private attorney generals, earnestly joining the fight against high-risk criminal networks (Nyrreröd and Andreadakis, 2023). Whistleblowing is not just a tool; it is a revolution that empowers societies to cleanse themselves of corruption. With the right environment, legislation and motivation, more individuals could be encouraged to come forward, holding a mirror to wrongdoing and ensuring that justice prevails. Both confiscation and whistleblowing now unfold in a technology-saturated environment, which criminals exploit – and which authorities can leverage. The following section considers these dual effects.

5. The rising challenge of tech-savvy criminal networks

Currently, criminal networks are adapting to contemporary advancements, employing technology-facilitated means such as encrypted interactions, social media and instant messaging services for illicit transactions and criminal endeavours. A considerable portion of their activities now occurs online, exploiting the secretive and pervasive nature of the Dark Web and various digital platforms (European Commission: Directorate-General for Migration and Home Affairs et al., 2021) that offer encrypted communication and transaction systems. These outlets give such criminal syndicates vast operational latitude – subterranean yet ubiquitous. Moreover, they exploit less regulated financial channels like virtual currencies, which exacerbates the problem's magnitude. The crypto-asset ecosystem exemplifies this, having grown rapidly to over 22 476 assets in circulation by early 2023 (Kapsis, 2023). Encryption's promise of anonymity serves as a veil, shielding criminals from law enforcement agencies' detection of unlawful profits, posing a complex regulatory challenge. A notable instance is the Silk Road (Adler, 2018), an online drug bazaar that used Bitcoin for transactions until halted by the US Federal Bureau of Investigation in 2013 ⁽¹⁰⁾. This example illustrates the dual nature of technology: it empowers criminal networks but also creates opportunities for law enforcement to innovate. These sophisticated technologies embolden high-risk criminal networks to undertake complex criminal activities (Demetis, 2023). For instance, a human trafficking ring used unique radio frequency identification microchips to catalogue its victims digitally (Barton and Laffan, 2016), intertwining exploitative practices with cutting-edge technology (Voas and Kshetri, 2017). Consequently, bridging technological risks with actionable strategies becomes essential for effective disruption. Thus, the pressing question becomes how law enforcement agencies can harness blockchain technology to detect, prevent and dismantle these organised criminal networks, and how blockchain can facilitate international collaboration in curbing high-risk criminal activities.

On a brighter note, digital tools have proven vital in enhancing whistleblower safety and protecting their identities, especially when using encrypted platforms like GlobaLeaks (Di Salvo, 2020). These tools highlight the practical implications of technology – not only as a threat vector but also as a safeguard for whistleblowers – underscoring the need for integrated policy responses. Still, a nuanced approach to digital tools is a requisite for better comprehending their impact on whistleblowing in the persistent fight against corruption (Fubini and Lo Piccolo, 2024).

⁽¹⁰⁾ Ross Ulbricht, the founder of the Silk Road, was convicted and sentenced to a double life sentence plus 40 years.

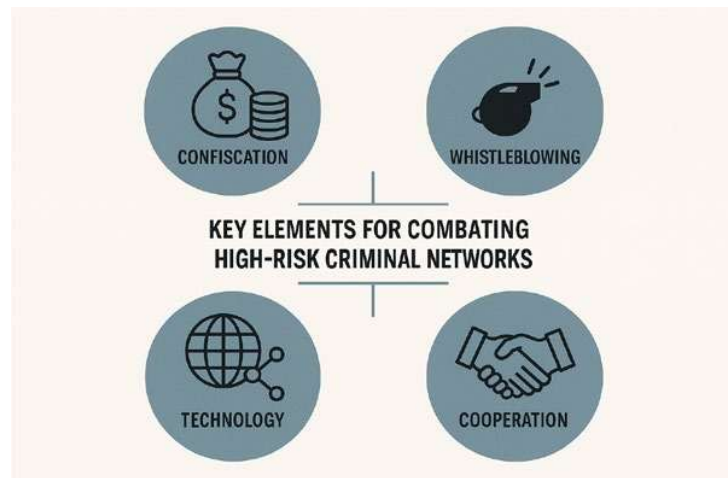


Figure 5.1. Key elements for combating high-risk criminal networks

Source: Conceptual diagram created by the author with AI support (Microsoft Copilot).

6. Conclusions

The European Union is actively grappling with the challenge of curbing the activities of high-risk criminal networks. Despite considerable steps having been made, a continuous and amplified effort remains essential to disbanding these complex criminal infrastructures. In enhancing these efforts, the EU has relied heavily on the Schengen information system (SIS) (European Commission, 2021, p. 3) and the European multidisciplinary platform against criminal threats (Empact). SIS is a consolidated database that empowers competent authorities in identifying offenders and their illicit wealth derived from organised crime (European Union, 2019ba, 2019b). Empact, on the other hand, functions as a multidimensional collaboration platform ⁽¹¹⁾ among diverse authorities (European Commission, 2021). This includes law enforcement, taxation departments, magistrates, European institutions and agencies, non-EU countries, international organisations and the private sector ⁽¹²⁾.

The prospect of these platforms is set to be enhanced by a forthcoming framework for the interaction of EU information systems, the purpose of which is an integrated data check across these systems. The primary objective of this framework is to address identity fraud efficiently (Council of Europe, n.d.). Furthermore, a marked improvement in the disruption of criminal networks can be brought about by enhancing cooperation among law enforcement authorities. This involves an exchange of information and collaborative investigations with non-EU country authorities. Intelligence-driven strategies are of crucial importance for combating the multifaceted structure of these networks. In order to ensure the efficacy of such investigations, it is essential to strengthen the jurisdiction of the competent authorities, while cognisant of the transborder aspect of these criminal activities. Member States need to establish clear objectives, dedicate resources, facilitate investigators' work through training and creatively employ the existing legal apparatus in a holistic, coherent and committed manner (Council of Europe, 2022).

⁽¹¹⁾ Between 2018 and 2021, EU crime priorities included cybercrime, drugs trafficking, facilitation of illegal immigration, organised property crime, trafficking in human beings (for all forms of exploitation), excise and missing trader intra-community fraud, illicit firearms trafficking, environmental crime, criminal finances and money laundering and document fraud.

⁽¹²⁾ The EU policy cycle for organised and serious international crime is utilised to define the cooperation framework for setting common priorities. Empact serves as the operational platform that facilitates cooperation between practitioners. It is the only programme that utilises intelligence-led policing and a multidisciplinary and integrated approach to combating organised crime.

Innovative solutions like developing an open-source platform could greatly augment criminal investigations and furnish crucial leads about assets held by criminals, their associates and instated businesses (Europol, 2021). A sound understanding of burgeoning technologies can also aid law enforcement authorities. Furthermore, technologies such as regtech (regulatory technology), can foster regulatory compliance and enable oversight of financial markets (Anagnostopoulos, 2018), including the crypto-asset ecosystem.

In essence, high-risk criminal networks pose a direct threat to the EU's security fabric by generating illicit profits and leveraging advanced technologies for evasion. Despite illicit assets being seized as a deterrent, only a fraction of the criminal proceeds is successfully recovered, due to a lack of seamless transborder cooperation and enforcement. Given such predicaments, proactive measures like whistleblower protections, leniency agreements or rewards might encourage insiders to report illicit activities. Additionally, criminal activities involving digital platforms, cryptocurrencies and encrypted technologies complicate investigations. This necessitates a coordinated EU effort, with advanced data sharing and specialised tools being critical for dismantling criminal networks and safeguarding society against such threats. Equally important is the role of whistleblowing, which provides early intelligence and actionable leads that complement technological and legal measures. Priority actions may include: (1) harmonising confiscation frameworks across Member States; (2) strengthening whistleblower protection and incentives; (3) using advanced analytics and blockchain tools for asset tracing; and (4) enhancing cross-border intelligence sharing. Future research should focus on the effectiveness of integrated strategies combining confiscation, whistleblowing and technology, and explore the ethical implications of AI-driven enforcement tools.

References

Adler, D. (2018), 'Silk Road: The dark side of cryptocurrency', *Fordham Journal of Corporate and Financial Law*, 21 February.

Anagnostopoulos, I. (2018), 'Fintech and regtech: Impact on regulators and banks', *Journal of Economics and Business*, Vol. 100, pp. 7–25, <https://doi.org/10.1016/j.jeconbus.2018.07.003>.

Barton, H. and Laffan, D. A. (2016), 'The dark side of the internet', in: Connolly, I., Palmer, M., Barton, H. and Kirwan, G. (eds), *An Introduction to Cyberpsychology*, Taylor and Francis, London, pp. 58–70, <https://doi.org/10.4324/9781003092513>.

Bergemann, P. (2024), 'How social influence affects reporting: Toward an integration of crime reporting, whistleblowing, and denunciation', *Annual Review of Sociology*, Vol. 50, pp. 209–228, <https://doi.org/10.1146/annurev-soc-030222-013736>.

Boeri, F., Di Cataldo, M. and Pietrostefani, E. (2024), 'Localized effects of confiscated and re-allocated real estate mafia assets', *Journal of Economic Geography*, Vol. 24, Issue 2, pp. 219–240, <https://doi.org/10.1093/jeg/lbad035>.

Chin, K. (1996), *Chinatown Gangs: Extortion, enterprise and ethnicity*, Oxford University Press, New York, https://archive.org/details/chinatowngangsex0000chin_e0o5/mode/2up.

Council of Europe (2019), 'The protection of whistleblowers: Challenges and opportunities for local and regional government', CG36(2019)14 final of 3 April, <https://rm.coe.int/the-protection-of-whistleblowers-challenges-and-opportunities-for-loca/16809312bd>.

Council of Europe (2022), 'Regional study on legislation with focus on search, seizure and confiscation of cybercrime proceeds and prevention of money laundering on the Internet – Eastern Partnership region – CyberEast project report', <https://rm.coe.int/regional-study-on-legislation-with-focus-on-search-seizure-and-confisc/1680a956e2>.

Council of Europe (n.d.), 'Financial investigations', Council of Europe website, <https://www.coe.int/en/web/moneyval/implementation/financial-investigations>.

Demetis, D. (2023), 'Organised crime – The cyber dimension', in: Rider, B. (ed.), *A Research Agenda for Organized Crime*, Edward Elgar Publishing, Cheltenham, pp. 177–194, https://econpapers.repec.org/RePEc:elg:eechap:20952_8.

Di Salvo, R. P. (2020), *Digital Whistleblowing Platforms in Journalism – Encrypting leaks*, Palgrave Macmillan, Cham, <https://doi.org/10.1007/978-3-030-38505-7>.

European Commission (2018), Commission staff working document – Impact assessment – Accompanying the document 'Proposal for a directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law', SWD(2018) 116 final of 23 April, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52018SC0116>.

European Commission (2020), Communication on the EU security union strategy, COM(2020) 605 final of 24 July, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0605>.

European Commission (2021), Communication from the Commission to the European Parliament, the Council, 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 of 14 April, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0170>.

European Commission: Directorate-General for Migration and Home Affairs and Kantar (2020), *Special Eurobarometer 502 – Report – Corruption*, Publications Office of the European Union, Luxembourg, <https://data.europa.eu/doi/10.2837/91891>.

European Commission: Directorate-General for Migration and Home Affairs, Ernst & Young, Government Transparency Institute, Optimity Advisors, RAND Europe and Centre for the Study of Democracy (2021), *Mapping the risk of serious and organised crime infiltration in legitimate businesses – Final report*, Publications Office of the European Union, Luxembourg, <https://data.europa.eu/doi/10.2837/64101>.

European Parliament (2016), 'Report on the fight against corruption', A8-0284/2016, https://www.europarl.europa.eu/doceo/document/A-8-2016-0284_EN.pdf.

European Parliament (2020), 'European Parliament resolution of 17 December 2020 on the EU security union strategy', P9_TA(2020)0378, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0378_EN.pdf.

European Parliament and Council of the European Union (2019a), Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17, ELI: <http://data.europa.eu/eli/dir/2019/1937/oj>), Recital 2.

European Parliament and Council of the European Union (2019b), Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27, ELI: <http://data.europa.eu/eli/reg/2019/817/oj>).

European Parliament and Council of the European Union (2019c), Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85, ELI: <http://data.europa.eu/eli/reg/2019/818/oj>).

European Parliament and Council of the European Union (2024a), Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation (OJ L, 2024/1260, 2.5.2024, ELI: <http://data.europa.eu/eli/dir/2024/1260/oj>), Recital 2.

European Parliament and Council of the European Union (2024b), Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation (OJ L, 2024/1260, 2.5.2024, ELI: <http://data.europa.eu/eli/dir/2024/1260/oj>), Article 15.

European Parliament and Council of the European Union (2024c), Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation (OJ L, 2024/1260, 2.5.2024, ELI: <http://data.europa.eu/eli/dir/2024/1260/oj>), Article 16.

European Union Agency for Fundamental Rights (2012), 'Opinion of the European Union Agency for Fundamental Rights on the confiscation of proceeds of crime', 3/2012, 4 December, p. 6, paragraph 6, https://fra.europa.eu/sites/default/files/fra-opinion-3-2012_confiscation-of-proceeds-of-crime.pdf.

Europol (2016), *Does Crime Still Pay? Criminal asset recovery in the EU – Survey of statistical information 2010–2014*, European Police Office (Europol), The Hague, <https://www.europol.europa.eu/publications-documents/does-crime-still-pay>.

Europol (2021), *European Union Serious and Organised Crime Threat Assessment – A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime*, Publications Office of the European Union, Luxembourg, <https://data.europa.eu/doi/10.2813/346806>.

Fubini, A. and Lo Piccolo, A. (2024), 'Anti-corruption initiatives and the digital challenge: The role of civil society organizations and whistleblowing infrastructures in the Italian context', *American Behavioral Scientist*, I. 70, Issue 8, <https://doi.org/10.1177/00027642241268590>.

Gambetta, D. (2011), *Codes of the Underworld – How criminals communicate*, Princeton University Press, <https://jpub.ub.uni-giessen.de/server/api/core/bitstreams/fcba5645-1e22-4eaf-8c46-d7a94e2c36ca/content>.

Gottschalk, P. and Asting, C. (2022), 'Crime signal detection theory: Two case studies of the five-stage model from observer to whistleblower', *Deviant Behavior*, Vol. 43, Issue 4, pp. 461–471, <https://doi.org/10.1080/01639625.2020.1816147>.

Hendry, J. and King, C. (2016), 'Expediency, legitimacy, and the rule of law: A systems perspective on civil/criminal procedural hybrids', *Criminal Law and Philosophy*, Vol. 11, pp. 733–757, <https://doi.org/10.1007/s11572-016-9405-6>.

Hryniewicz-Lach, E. (2023), 'Expanding confiscation and its dimensions in EU criminal law', *European Journal of Crime, Criminal Law and Criminal Justice*, Vol. 31, Issue 3–4, pp. 243–267, <https://doi.org/10.1163/15718174-bja10046>.

Kapsis, I. (2023), 'Crypto-assets and criminality: A critical review focusing on money laundering and terrorism financing', in: Jasinski, D., Phillips, A. and Johnston, E. (eds), *Organised Crime, Financial Crime, and Criminal Justice – Theoretical concepts and challenges*, 1st edition, Routledge, London, pp. 122–141, <https://doi.org/10.4324/9781003020813-8>.

Karpacheva, E. and Hock, B. (2024), 'Foreign whistleblowing: The impact of US extraterritorial enforcement on anti-corruption laws in Europe', *Journal of Financial Crime*, Vol. 31, Issue 1, pp. 1–13, <https://doi.org/10.1108/JFC-11-2022-0283>.

Kaçıku Baljija, S. and Min, K. (2023), 'Evaluating the effectiveness of whistleblower protection: A new index', *Data and Policy*, Vol. 5, e28, <https://doi.org/10.1017/dap.2023.20>.

Laghidze, E. (2023), 'Seizure and confiscation as an effective means of combating transnational organized crime', *Law and World*, Vol. 9, No 25, pp. 146–155, <https://doi.org/10.36475/9.1.15>.

Maugeri, A. M. (2024), 'Regulation (EU) 2018/1805: Mutual recognition of freezing and confiscation orders between efficiency and safeguards – "Proceedings in criminal matters" and non-conviction based confiscation', *New Journal of European Criminal Law*, Vol. 15, Issue 2, pp. 164–208, <https://doi.org/10.1177/20322844241239781>.

Miethe, T. D. and Rothschild, J. (1994), 'Whistleblowing and the control of organizational misconduct', *Sociological Inquiry*, Vol. 64, Issue 3, pp. 322–347, <https://doi.org/10.1111/j.1475-682X.1994.tb00395.x>.

Munro, I. and Kenny, K. (2023), 'Networked whistleblowing, counter-hegemony and the challenge to systemic corruption', in: Gabbioneta, C., Clemente, M. and Greenwood, R. (eds), *Organizational Wrongdoing as the 'Foundational' Grand Challenge – Consequences and impact*, Vol. 85, Emerald Publishing, <https://doi.org/10.1108/S0733-558X20230000085007>.

Nyreröd, T., Andreadakis, S. and Spagnolo, G. (2023), 'Money laundering and sanctions enforcement: Large rewards, leniency and witness protection for whistleblowers', *Journal of Money Laundering Control*, Vol. 26, No 5, pp. 912–925, <https://doi.org/10.1108/JMLC-05-2022-0068>.

Rider, B. (ed.) (2023), *A Research Agenda for Organized Crime*, Edward Elgar Publishing, Cheltenham, <https://econpapers.repec.org/RePEc:elg:eebook:20952>.

Sakellaraki, A. (2022), 'EU asset recovery and confiscation regime – *Quo vadis?* A first assessment of the Commission's proposal to further harmonise the EU asset recovery and confiscation laws – A step in the right direction?', *New Journal of European Criminal Law*, Vol. 13, Issue 4, pp. 478–501, <https://doi.org/10.1177/20322844221139577>.

Terracol, M. (2023), *How Well Do EU Countries Protect Whistleblowers? Assessing the transposition of the EU whistleblower Protection Directive*, Transparency International, https://images.transparencycdn.org/images/2023_How-well-do-EU-countries-protect-whistleblowers_EN.pdf.

Vandekerckhove, W. (2010), 'European whistleblower protection: Tiers or tears?', in: Lewis, D. (ed.), *A Global Approach to Public Interest Disclosure*, Edward Elgar Publishing, Cheltenham, pp. 15–35, <https://gala.gre.ac.uk/id/eprint/4360>.

Voas, J. and Kshetri, N. (2017), 'Human tagging', *Computer*, Vol. 50, Issue 10, pp. 78–85, <https://doi.org/10.1109/MC.2017.3641646>.