

IntechOpen

IntechOpen Series
Social Sciences, Volume 17

Criminology

Understanding Crime, Criminality,
and Justice in a Changing World

Edited by Kamil Hakan Dogan



Criminology - Understanding Crime, Criminality, and Justice in a Changing World

Edited by Kamil Hakan Dogan

Published in London, United Kingdom

Criminology - Understanding Crime, Criminality, and Justice in a Changing World
<http://dx.doi.org/10.5772/intechopen.1010543>
Edited by Kamil Hakan Dogan

Contributors

Barbara Szabó, Csongor Herke, Damian Hutchinson, Fadila Ait Boughima, Gabriela Mesquita Borges, Jennifer Garcia Ospina, Laura Neiva, Melike Erbaş, Thomas Joyce

© The Editor(s) and the Author(s) 2026

The rights of the editor(s) and the author(s) have been asserted in accordance with the Copyright, Designs and Patents Act 1988. All rights to the book as a whole are reserved by INTECHOPEN LIMITED. The book as a whole (compilation) cannot be reproduced, distributed or used for commercial or non-commercial purposes without INTECHOPEN LIMITED's written permission. Enquiries concerning the use of the book should be directed to INTECHOPEN LIMITED rights and permissions department (permissions@intechopen.com).

Violations are liable to prosecution under the governing Copyright Law.



Individual chapters of this publication are distributed under the terms of the Creative Commons Attribution 4.0 License which permits commercial use, distribution and reproduction of the individual chapters, provided the original author(s) and source publication are appropriately acknowledged. If so indicated, certain images may not be included under the Creative Commons license. In such cases users will need to obtain permission from the license holder to reproduce the material. More details and guidelines concerning content reuse and adaptation can be found at <http://www.intechopen.com/copyright-policy.html>.

Notice

Statements and opinions expressed in the chapters are those of the individual contributors and not necessarily those of the editors or publisher. No responsibility is accepted for the accuracy of information contained in the published chapters. The publisher assumes no responsibility for any damage or injury to persons or property arising out of the use of any materials, instructions, methods or ideas contained in the book.

First published in London, United Kingdom, 2026 by IntechOpen

IntechOpen is the global imprint of INTECHOPEN LIMITED, registered in England and Wales, registration number: 11086078, 167-169 Great Portland Street, London, W1W 5PF, United Kingdom

For EU product safety concerns: IN TECH d.o.o., Prolaz Marije Krucifikse Kozulić 3, 51000 Rijeka, Croatia, info@intechopen.com or visit our website at intechopen.com.

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

Criminology - Understanding Crime, Criminality, and Justice in a Changing World

Edited by Kamil Hakan Dogan

p. cm.

This title is part of the Social Sciences Book Series, Volume 17

Series Editor: Sandro Serpa

Print ISBN 978-1-80631-562-8

Online ISBN 978-1-80631-561-1

eBook (PDF) ISBN 978-1-80631-563-5

ISSN 2977-6473

If disposing of this product, please recycle the paper responsibly.

IntechOpen Book Series

Social Sciences

Volume 17

Aims and Scope of the Series

The social sciences, as a form of scientific knowledge anchored on epistemological foundations, theories, and specific methodologies, both in their fundamental and applied dimensions, are paramount for understanding and, consequently, developing instruments that contribute to improving social and environmental living conditions. This Social Sciences book series, based on the concept of the social sciences as key elements in the promotion of scientific knowledge and its inherent consequences, has as its primary goal to be a space for the dissemination of relevant information on various objects of study, aimed at specialists, students, policymakers, and others interested in the challenges facing humanity. Thus, the aim is to promote scientific progress through the sound and rigorous dissemination of studies that, from the perspective of the social sciences, either through a specialised disciplinary approach or through interdisciplinary perspectives, foster a deeper understanding of the objects under analysis, clarifying the issues addressed and their implications.

Meet the Series Editor



Sandro Nuno Ferreira de Serpa (PhD, FRSA, FRSS, FRGS, FR-SPH, FRAI, FISDS, GLO Fellow), is an Associate Professor with tenure in the Department of Sociology at the University of the Azores and a Senior Integrated Researcher at the Interdisciplinary Centre of Social Sciences (CICS.NOVA.UAc). With over 25 years of experience in higher education, in 2025 Dr. Serpa is ranked by ScholarGPS as the 8th scholar worldwide in Sociology (Prior 5-Year category) and 1st in Portugal. His career is distinguished by encompassing over 400 scientific publications published in Brazil, Canada, China, Germany, India, Kazakhstan, the Netherlands, Pakistan, Poland, Portugal, Romania, Spain, Switzerland, Turkey, the United Arab Emirates, the United Kingdom, and the United States of America with a high research impact, as evidenced by a Google Scholar h-index of 29 and a Scopus h-index of 14 (with 79 documents indexed). His international prestige is underscored by his status as a Fellow of five distinguished British Royal Societies: the Royal Society of Arts (FRSA), the Royal Statistical Society (FRSS), the Royal Geographical Society (FRGS), the Royal Society for Public Health (FRSPH), and the Royal Anthropological Institute (FRAI), alongside being a Fellow of the International Society for Development and Sustainability (FISDS) and Fellow of the Global Labor Organization (GLO). Registered Vetted Expert for the European Commission and the United Nations. Dr. Serpa's research focuses on the sociotechnological co-evolution of Society 5.0, Artificial Intelligence in Education, and Algocratic Governance. An expert in strategic editorial leadership, he currently serves as the Series Editor for Social Sciences Series at IntechOpen, Editor for SAGE Open, and is a member of the Editorial Board for International Studies in Sociology of Education (Taylor & Francis) and Societies (MDPI). His extensive administrative background includes roles as Department Head, Degree Director, and Deputy Director of CICS.UAc, reflecting a profile that harmonizes scientific excellence with high-level academic management.

Meet the Volume Editor



Kamil Hakan Dogan, MD, Ph.D., is a Full Professor and Chair in the Department of Forensic Medicine at Selcuk University, Faculty of Medicine in Türkiye. Dr. Dogan received his MD from the Faculty of Medicine at Gazi University in 2000. After extensive research in forensic medicine, he earned his Ph.D. in Biochemistry in 2012. He gives lectures on Forensic Medicine and Medical Ethics to medical students as well as students of the dentistry and law faculties. He is the editor of 10 books, a reviewer for several international journals, and has published over 200 articles in refereed journals, textbook chapters, and abstracts at scientific meetings. His publications have been cited more than 1400 times.

Contents

Preface	XIII
Chapter 1 Adaptive Violence: Community Embeddedness and the Limits of Suppression Across Caribbean and North American Contexts <i>by Damian Hutchinson</i>	1
Chapter 2 The Use of Big Data to Address Refugee Victimization: A Scoping Review <i>by Gabriela Mesquita Borges and Laura Neiva</i>	17
Chapter 3 Artificial Intelligence and Crime on Social Media Platforms <i>by Csongor Herke and Barbara Szabó</i>	35
Chapter 4 Cybercrime and Organised Crime: Distinct Criminal Forms in the Digital Era <i>by Thomas Joyce</i>	63
Chapter 5 Crime and Science Forensic <i>by Fadila Ait Boughima</i>	77
Chapter 6 Review of Medical Crimes from Unauthorized Applications to Malpractices <i>by Melike Erbaş</i>	87
Chapter 7 Forensic Characterization of Bagged Bodies: A Four-Year Review from Medellín, Colombia <i>by Jennifer Garcia Ospina</i>	99

Preface

Current criminological studies are being fundamentally altered by technological innovation, global migration, and intricate methods of underground oversight. *Criminology - Understanding Crime, Criminality, and Justice in a Changing World* brings together researchers from diverse fields to examine evolving criminal landscapes and the interface between sociological studies of crime and forensic science. This work is organized to transition readers from large-scale social systems to the digital and infinitesimal front lines of modern-day enforcement. The book starts by exploring the assimilation of group violence as a type of non-traditional authority in neglected urban zones. Shifting its focus to the digital sphere, the book evaluates how big data, AI, and the attention-based economy serve as dual-purpose assets that modify the foundations for criminal activity and surveillance. As criminal activities migrate across platforms, this book offers a precise theoretical framework to distinguish digital offenses from conventional organized crime.

Furthermore, the focus shifts to the application of justice, examining the evolution of electronic evidence and the complex legal nuances of medical negligence in clinical forensic science. The book concludes with sophisticated forensic field techniques, showing how global standards apply diverse investigative approaches to interpret symbolic meanings in intricate body-hiding scenarios. Ultimately, this work highlights that addressing the evolving nature of contemporary criminal activity demands a unified and situational blend of criminological concepts, digital proficiency, and principled forensic practices.

Kamil Hakan Dogan

Department of Forensic Medicine,
Selcuk University Faculty of Medicine,
Konya, Türkiye

Chapter 1

Adaptive Violence: Community Embeddedness and the Limits of Suppression Across Caribbean and North American Contexts

Damian Hutchinson

Abstract

This chapter advances the concept of adaptive violence to explain why suppression-based strategies often fail to produce durable reductions in community violence. Drawing on comparative analysis across Caribbean and North American urban contexts, it conceptualizes violence as socially embedded and territorially organized, capable of reconfiguring in response to enforcement pressure. Using Jamaica and Trinidad and Tobago as primary Caribbean cases, alongside selected North American cities including Chicago, the chapter demonstrates how community embeddedness shapes both the resilience of violent systems and the limits of enforcement-led interventions. While intensified policing and emergency powers may reduce visible manifestations of violence, such approaches frequently generate fragmentation, displacement, and tactical adaptation rather than long-term transformation. The analysis argues that sustainable reductions are more likely when enforcement strategies are accompanied by shifts in community legitimacy, informal governance, and local authority structures. By foregrounding the adaptive nature of violence, the chapter challenges conventional suppression models and calls for integrated public safety approaches that extend beyond enforcement to engage community-centered mechanisms capable of reshaping the social conditions that sustain violence.

Keywords: adaptive violence, community embeddedness, suppression strategies, informal governance, Caribbean violence, urban criminology, public safety policy

1. Introduction

Contemporary patterns of violence increasingly challenge conventional criminological assumptions that frame violent behavior as episodic, irrational, or primarily responsive to coercive control. Across diverse social contexts, violence has demonstrated a capacity to persist, reorganize, and adapt in response to intensified suppression, suggesting that enforcement-centric approaches alone are insufficient for achieving durable reductions in harm [1]. This chapter advances the concept of adaptive violence to describe forms of collective violence that are socially

embedded, territorially grounded, and capable of evolving in response to state intervention rather than being eliminated by it.

Central to this analysis is the role of community embeddedness in shaping both the durability of violent systems and the limits of suppression-based responses. In certain contexts, violence is not merely tolerated by surrounding communities but is interwoven with political history, social identity, and informal systems of governance. Where violence becomes embedded within community structures and legitimacy frameworks, state efforts to suppress it through policing or militarized intervention may disrupt visible manifestations of violence without dismantling the underlying social logic that sustains it [2]. Instead, such efforts often provoke adaptive responses, including spatial displacement, organizational fragmentation, and tactical innovation.

The Caribbean, and Jamaica in particular, offers a critical yet underutilized lens through which to examine these dynamics. Historical patterns of political mobilization and territorial control in Jamaica during the latter half of the twentieth century produced violence-producing spaces in which collective violence was closely aligned with partisan identity, community loyalty, and access to material and symbolic resources. Unlike many North American urban contexts – where violence is frequently driven by illicit markets and fragmented gang structures – Caribbean political violence has historically involved broader forms of community participation and social normalization. This distinction makes the Caribbean context analytically valuable for understanding how violence acquires legitimacy, how communities regulate it, and why suppression alone often fails to produce lasting change.

Using a comparative framework, this chapter examines adaptive violence across Caribbean and North American contexts to illuminate both points of convergence and divergence in how violent systems respond to suppression. While identity, territoriality, and symbolic control emerge as common features across settings, the degree of community embeddedness fundamentally shapes the effectiveness of state interventions. By contrasting these contexts, the chapter argues that suppression-oriented strategies are inherently limited when they fail to account for the historical, social, and spatial conditions that enable violence to function as a form of informal governance.

By situating violence within its broader social ecology, this chapter contributes to criminological debates on crime control, legitimacy, and justice in a changing world. It challenges universalized models of violence prevention and calls for context-sensitive approaches that recognize violence not only as a criminal act but as a social phenomenon shaped by history, community alignment, and adaptive capacity. In doing so, the chapter seeks to extend criminological theory beyond narrow enforcement paradigms and toward more sustainable, community-informed responses to violence.

2. Conceptual framework: Adaptive violence, space, and community embeddedness

Conventional criminological approaches often conceptualize violence as a discrete behavioral outcome driven by individual pathology, criminal opportunity, or rational choice. Within this framing, suppression-oriented responses – arrest, incarceration, and militarized policing – are assumed to function as primary

mechanisms of control. While such approaches may produce short-term reductions in visible violence, they struggle to explain the persistence, recurrence, and transformation of violence across time and space. This chapter advances an alternative conceptual framework that treats violence as an adaptive social system, shaped by community embeddedness, historical legitimacy, and spatial governance rather than solely by deterrence.

2.1 Violence as an adaptive social system

Adaptive violence refers to forms of collective violence that reorganize in response to social, political, and institutional pressures. Rather than diminishing linearly under enforcement pressure, violence frequently changes its structure, visibility, and modes of operation. Suppression may disrupt existing hierarchies, displace violent actors, or temporarily reduce overt incidents, but it also generates incentives for fragmentation, decentralization, and tactical innovation [3]. In this sense, violence behaves less like an isolated criminal act and more like a resilient social system capable of adjustment and survival [4].

Understanding violence as adaptive challenges the assumption that enforcement intensity correlates directly with long-term reductions in harm [4]. Instead, adaptive violence highlights how coercive interventions can unintentionally accelerate volatility by dismantling centralized control structures, increasing uncertainty, and pushing violence into less predictable forms. This perspective aligns with public health and systems-based approaches that emphasize feedback loops, latency, and unintended consequences over linear causality.

2.2 Violence-producing spaces and the social ecology of harm

Violence does not emerge randomly across urban environments. It is concentrated within specific violence-producing spaces – geographic and social contexts shaped by historical marginalization, political exclusion, and weakened formal governance [5]. These spaces are not defined solely by poverty or density but by the interaction between territory, identity, and authority. Within such environments, violence often performs regulatory functions, including territorial defense, dispute resolution, and the enforcement of informal norms.

Violence-producing spaces are sustained through social relationships and shared histories that extend beyond individual perpetrators. Community members may not actively participate in violence, yet their daily interactions, silences, and survival strategies can inadvertently reinforce violent systems. This embeddedness complicates suppression-based responses, as enforcement actions targeting individuals or groups fail to address the broader social ecology that enables violence to regenerate.

2.3 Community embeddedness and legitimacy

Community embeddedness refers to the degree to which violent actors and practices are integrated into local social structures and legitimacy frameworks. Where violence is embedded, it derives authority not only from coercion but also from perceived utility, protection, or representation within the community. Legitimacy in this context is relational rather than legal, rooted in historical alignments, political identity, and the absence or unreliability of state institutions [6].

The degree of embeddedness fundamentally shapes the effectiveness of suppression. In contexts where violence lacks community legitimacy, enforcement may rapidly incapacitate actors and disrupt networks. Conversely, where violence functions as a form of informal governance, suppression tends to produce displacement and adaptation rather than resolution. Durable reductions in violence occur not when force overwhelms violent actors but when legitimacy shifts – when communities withdraw consent, redefine norms, and reassert non-violent forms of regulation.

2.4 Suppression as a limited and context-dependent tool

Within this framework, suppression is not dismissed outright but is reclassified as a context-dependent and limited intervention. Suppression can provide short-term stabilization, reduce immediate harm, and create windows for intervention. However, when treated as a primary strategy rather than a supporting measure, it fails to address the social foundations of violence and may entrench adaptive cycles.

Empirical evidence from the Caribbean demonstrates that suppression-oriented strategies function most effectively as temporary relief mechanisms rather than as drivers of long-term transformation. In the absence of parallel efforts to rebuild community governance, address social norms, and create legitimate pathways for identity and economic participation, suppression alters the form of violence without dismantling its underlying logic.

2.5 Implications for comparative analysis

This conceptual framework provides the basis for comparative analysis across contexts. While adaptive violence, spatial concentration, and legitimacy dynamics are present in both Caribbean and North American urban settings, their relative configurations differ significantly. The degree of community embeddedness, historical political alignment, and informal governance shape how violence responds to suppression and why similar enforcement strategies yield divergent outcomes.

By foregrounding adaptation, space, and legitimacy, this framework moves beyond universalized models of violence control and toward a context-sensitive criminology. It allows violence to be understood not only as a problem of crime but as a social process embedded within communities and shaped by history, governance, and collective action. This perspective is essential for explaining the limits of suppression and for designing interventions capable of producing sustainable reductions in harm.

3. Methods and analytical approach

This chapter employs a qualitative, comparative analytical approach to examine the adaptive nature of community violence and the limits of suppression-based interventions across different socio-political contexts. The analysis is grounded in comparative historical interpretation, supported by secondary empirical sources, policy analyses, and long-term programmatic documentation related to community violence intervention and prevention efforts.

The comparative framework focuses primarily on the Caribbean – particularly Jamaica – as an analytically productive case through which to interrogate dominant criminological assumptions about violence, legitimacy, and control. The Caribbean context is not treated as an exceptional or peripheral case but rather as a setting in which the dynamics of community embeddedness, political history, and violence adaptation are especially visible. These dynamics are then contrasted with patterns more commonly observed in North American urban contexts, where violence is often more fragmented, market-driven, and less overtly embedded in collective community identity.

Empirically, the chapter draws on three categories of material. First, it engages established criminological, sociological, and public health literature on violence, suppression, and social ecology to situate the analysis within broader theoretical debates. Second, it utilizes secondary data sources, including crime trends, policy evaluations, and historical accounts, to contextualize shifts in violence patterns over time. Third, the analysis is informed by longitudinal programmatic documentation, including internal evaluations, implementation reports, and policy analyses, produced through sustained community-based violence intervention initiatives in Jamaica. This approach provides insight into the evolution of violence-producing spaces, community responses, and state intervention outcomes over extended periods.

These programmatic materials are treated as secondary empirical sources rather than as narrative or autobiographical accounts. Their analytical value lies in their capacity to illuminate patterns of violence, adaptation, displacement, fragmentation, and legitimacy formation that are difficult to capture through short-term studies or enforcement-centered datasets alone. In particular, they provide evidence of how violence reorganizes in response to suppression, how community participation shapes the durability of violent systems, and how peace-building efforts succeed or fail depending on the extent of broader community engagement.

The analytical strategy is interpretive rather than causal. The chapter does not seek to establish linear cause-and-effect relationships between specific interventions and crime outcomes. Instead, it examines how violence operates as a socially embedded and adaptive system, shaped by historical legacies, spatial organization, and relationships between communities and the state. Attention is given to shifts in the organization of violence – from centralized forms of control to fragmented and decentralized structures – and to the implications of these shifts for suppression-oriented policy responses.

Several limitations of this approach should be acknowledged. The chapter relies on secondary and programmatic sources rather than original quantitative data collection, and its comparative scope necessarily abstracts from local variation within both Caribbean and North American contexts. However, this approach allows for a level of historical and contextual depth that is often absent from narrowly focused empirical studies. By foregrounding adaptation, legitimacy, and community embeddedness, the chapter seeks to contribute analytically to criminological debates on violence and justice in a changing world, rather than offer prescriptive or universally generalizable policy solutions.

Caribbean context: Political violence, community embeddedness, and adaptation patterns of violence in the Caribbean, and Jamaica in particular, cannot be adequately understood without reference to their historical roots in political mobilization, spatial control, and community alignment. From the 1970s through the

1990s, violence in many urban communities in Kingston and other population centers was closely linked to partisan competition, territorial demarcation, and access to state resources. During this period, violence-producing spaces emerged not as isolated criminal enclaves but as politically embedded communities in which coercion, loyalty, and identity were mutually reinforcing.

Political affiliation functioned as a primary organizing principle of violence. Community boundaries were marked symbolically through party colors, murals, and public displays of allegiance, transforming geographic space into politicized territory. Violence served both defensive and regulatory purposes, enforcing territorial boundaries and deterring rival incursions while simultaneously mediating relationships between communities and political elites. In this context, violent actors often derived legitimacy not solely from their capacity for coercion but from their perceived role as protectors, brokers, and enforcers within a broader system of political patronage.

As formal political violence declined toward the late 1990s, these violence-producing spaces did not disappear. Rather, they underwent a process of adaptation. The weakening of overt partisan control coincided with the rise of illicit economies, shifts in leadership structures, and changing relationships between communities and the state. Centralized systems of control – often associated with dominant community figures – fragmented into smaller, decentralized groups operating at the level of streets, corners, and micro-territories. This transition marked a shift from ideologically framed political violence toward more localized, turf-based forms of armed control.

Crucially, this transformation did not sever the relationship between violence and community embeddedness. Instead, it reconfigured it. Violence remained socially regulated, even as its organizational form changed. Armed actors continued to draw protection, information, and legitimacy from segments of the community, while communities retained informal mechanisms for constraining excesses, negotiating truces, and mediating disputes. Violence thus persisted not as an external imposition upon communities but as a system partially sustained through social relationships, shared histories, and collective memory.

State responses during this period were overwhelmingly suppression-oriented, relying on intensified policing, militarized interventions, and targeted enforcement operations. While such interventions frequently produced short-term reductions in visible violence, they also generated predictable adaptive responses. Armed actors displaced geographically, reorganized internally, or temporarily withdrew from overt activity, only to re-emerge under altered conditions. Suppression disrupted established hierarchies, often accelerating fragmentation and increasing volatility rather than dismantling the underlying social foundations of violence.

Evidence from sustained community violence intervention initiatives in Jamaica illustrates these dynamics with particular clarity. Periods of aggressive enforcement were frequently followed by apparent lulls in violence, which masked the accumulation of latent conflict. Weapons were hidden rather than surrendered, grievances remained unresolved, and informal authority structures persisted beneath the surface. When violence resurfaced, it often did so in less predictable and more diffuse forms, complicating subsequent intervention efforts and undermining public trust in state institutions.

At the same time, these initiatives demonstrated that violence was most effectively reduced when legitimacy shifted at the community level, rather than

when coercion intensified. Interventions that engaged entire communities – rather than focusing exclusively on armed actors – were more likely to produce durable reductions in violence. This was particularly evident in contexts where community members actively participated in redefining norms, delegitimizing violent authority, and reasserting non-violent forms of regulation. Where such shifts occurred, violence lost its social anchoring, rendering it less resilient to suppression.

The Jamaican case thus illustrates a central argument of this chapter: the effectiveness of suppression is fundamentally conditioned by the degree of community embeddedness of violence. Where violence functions as a form of informal governance – regulating space, identity, and access to resources – state efforts to eliminate it through force alone are inherently limited. Suppression may alter the outward expression of violence, but without corresponding changes in legitimacy and community alignment, it is unlikely to produce lasting transformation.

This Caribbean experience provides a critical comparative baseline for understanding violence in other contexts. It highlights how historical trajectories of political mobilization shape contemporary violence-producing spaces and how adaptive responses emerge when suppression fails to engage the social systems within which violence is embedded. These dynamics stand in contrast to, but also intersect with, patterns observed in North American urban settings, where the relationship between violence, community legitimacy, and state authority often takes different forms.

4. Contemporary Caribbean responses: Suppression, emergency powers, and regional signals

In recent years, the Caribbean has witnessed a renewed emphasis on suppression-oriented responses to escalating violence, particularly through the expanded use of emergency powers and intensified security operations. In Jamaica, public discourse surrounding the 2025 general election highlighted a reported decline in national homicide levels, with political leadership receiving regional and international attention for adopting a firm security posture. These developments have been closely observed across the Caribbean as governments confront similarly complex violence dynamics.

Comparative regional analysis, however, suggests a more nuanced picture. Independent assessments of states of emergency in both Jamaica and Trinidad and Tobago indicate that, while such measures may coincide with short-term reductions in visible violence, they are not consistently associated with sustained long-term declines [7]. Moreover, these approaches have been accompanied by heightened concerns regarding lethal force, accountability, and the durability of suppression-led gains. This tension underscores the limits of emergency governance when underlying social and community dynamics remain unchanged.

Trinidad and Tobago offers an important regional comparator that further illustrates these dynamics. Positioned within major narcotics and firearms trafficking routes, Trinidad's violence profile has been shaped by gang fragmentation, access to high-powered weapons, and competition over illicit markets. Repeated states of emergency have been deployed to counter rising homicide levels, reflecting a regional convergence in enforcement strategy. At the

same time, Trinidad stands out for having implemented and evaluated community-based violence interruption initiatives. A formal evaluation of a cure violence adaptation reported significant reductions in violent incidents and gunshot injuries within intervention areas, demonstrating that people-centered approaches can yield measurable impact even in environments marked by organized criminality and firearm proliferation [8]. Together, these experiences reinforce a central argument of this chapter: suppression may disrupt violence temporarily, but durable reductions are more likely when interventions engage community legitimacy and social regulation alongside enforcement.

5. North American urban contexts: Fragmentation, markets, and suppression

Violence in North American urban contexts shares certain surface similarities with Caribbean violence-producing spaces, including territoriality, identity formation, and the concentration of harm within marginalized neighborhoods. However, the social organization and legitimacy dynamics of violence in these settings differ in critical ways. These differences shape both how violence manifests and how it responds to suppression-oriented interventions.

In much of North America, urban violence has evolved primarily through the expansion and entrenchment of illicit markets – particularly drug distribution – within economically marginalized communities. While historical political exclusion and racialized inequality remain central to understanding these environments, violence is less frequently embedded in overt community-wide political identity or collective governance structures. Instead, it tends to be organized through fragmented networks of gangs or crews, whose authority is narrower, more transactional, and more directly tied to market control than to broad-based community legitimacy.

This fragmentation has important implications. Violent actors in North American cities often operate with limited community consent and face ambivalent or hostile relationships with residents, who experience violence primarily as victimization rather than protection. While fear and silence may still characterize community responses, violence is less likely to be viewed as a legitimate form of regulation or representation. As a result, violent systems are comparatively more vulnerable to disruption through targeted enforcement, especially when suppression coincides with incarceration, probation regimes, and surveillance infrastructures that extend state control deep into community life.

Suppression thus occupies a more central position in North American violence reduction strategies. Policing, incarceration, and deterrence-based models are frequently treated as primary tools rather than as temporary stabilizing measures. These approaches can generate measurable reductions in violence, particularly when enforcement is strategically focused on high-risk individuals or groups. However, even in these contexts, suppression has demonstrated diminishing returns over time. Arrest-driven strategies often accelerate organizational fragmentation, leading to the proliferation of smaller, less predictable groups and contributing to cycles of retaliation that complicate long-term prevention efforts.

Unlike in Caribbean contexts shaped by political mobilization, suppression in North America is more likely to be absorbed into an already expansive carceral

system. This system functions as an alternative mechanism of social regulation, partially substituting for the informal governance roles that violence plays elsewhere. In this sense, the state's capacity to incapacitate violent actors through incarceration reduces the degree to which violence must be socially regulated within communities themselves. Yet, this substitution comes at a substantial social cost, including family disruption, economic exclusion, and the normalization of surveillance and punishment as features of everyday life.

Despite these differences, adaptive dynamics remain evident. Violence in North American cities responds to enforcement pressure through displacement across neighborhoods, shifts in weapon use, changes in recruitment patterns, and the diffusion of conflict into less visible forms. Suppression may reduce homicide rates while leaving underlying drivers – economic marginalization, identity formation, and contested legitimacy – largely intact. As enforcement intensity fluctuates, violence often re-emerges in altered configurations, reinforcing the limits of suppression as a stand-alone strategy.

The North American experience thus illustrates a different configuration of adaptive violence – one in which fragmentation and market logic constrain community-wide legitimacy but do not eliminate the capacity of violence to reorganize in response to state intervention. These dynamics underscore the importance of context in shaping both the form of violence and the outcomes of suppression. While enforcement may achieve greater immediate traction in North American settings than in Caribbean contexts, its long-term effectiveness remains contingent on complementary strategies that address legitimacy, identity, and social integration.

In mid-sized North American cities such as Trenton, these dynamics are increasingly visible. Such cities often experience concentrated disadvantage, fragmented governance, and sustained exposure to illicit markets, creating environments in which organized criminality can adapt and embed. While demographic change has been a feature of many urban areas, research consistently shows that immigration itself does not drive violent crime [9]. Rather, organized violence capitalizes on opportunity structures created by economic strain, social fragmentation, and enforcement pressure.

Within this context, the growing visibility of highly organized gangs such as Mara Salvatrucha (MS-13) illustrates how criminality shifts across jurisdictions and asserts its presence through symbolic and territorial means. State-level investigative reporting identifies MS-13 as a persistent threat operating across jurisdictions and asserting territorial presence through symbolic and coercive practices in extortion, drug distribution, and violent enforcement. In cities like Trenton, increased graffiti, tagging, and symbolic territorial marking reflect mechanisms through which organized violence claims space, reinforces identity, and signals dominance. These practices mirror patterns observed in other violence-producing spaces, underscoring that the issue is not population change but the adaptability and mobility of organized violence as it responds to local vulnerabilities and enforcement regimes.

6. Comparative analysis: Adaptive violence and the limits of suppression

The comparative analysis across Caribbean and North American urban contexts reinforces a central argument of this chapter: community violence operates as an

adaptive social system whose form, organization, and legitimacy evolve in response to pressure. While the historical motivations and trajectories of violence in these regions differ, contemporary patterns reveal a steady convergence driven by shared mechanisms of fear, identity formation, territorial control, and economic exploitation. Suppression-oriented strategies, when decoupled from community empowerment, alter the expression of violence without dismantling its underlying logic.

6.1 Fear as a tool of social control

Across both geographic contexts, fear functions as a primary mechanism of governance within violence-producing spaces. Fear enforces silence, deters resistance, and normalizes compliance where formal authority is weak, contested, or mistrusted. In Caribbean settings historically shaped by political mobilization, fear operated alongside partisan loyalty and collective identity to regulate territory and behavior. In North American urban contexts, fear has been more directly instrumentalized to protect illicit markets, discipline internal members, and deter retaliation or cooperation with authorities.

Despite these contextual differences, fear performs a similar regulatory role. It substitutes for formal rule-making and sustains violent systems by discouraging collective challenges. Suppression may temporarily intensify fear through visible force, but it rarely dislodges fear as a governing mechanism unless communities are empowered to redefine norms and legitimacy. Where fear remains central to social order, violence adapts rather than recedes.

6.2 Identity, territoriality, and the claiming of space

Identity formation is a critical mechanism through which violence becomes durable across both contexts. Symbols, names, colors, rituals, and spatial markings serve to claim territory, reinforce internal norms, and facilitate recruitment. In Caribbean communities, political murals, party colors, and historical allegiances transform physical space into symbols of collective identity and control. In North American cities, gang tagging, sets, and visual markers perform analogous functions, signaling dominance and embedding violent identity into the urban landscape.

These practices are not merely expressive but strategic. Identity converts violence from episodic behavior into a collective project anchored in space and memory. As violence adapts, identity evolves alongside it, absorbing new cultural influences, migration patterns, and transnational affiliations. The persistence of identity-based territorial claims across both contexts highlights a shared mechanism through which violence reproduces itself, even as its economic or political motivations shift.

6.3 Economic control and the convergence of violence ecosystems

Historically, the economic foundations of violence diverged across regions. In North America, organized violence emerged primarily from illicit markets – alcohol during Prohibition, followed by drugs, firearms, and extortion – with community control developing as a means of protecting profit. In contrast, Caribbean violence was initially rooted in socio-cultural, political, and labor struggles, with economic activity playing a secondary or instrumental role.

By 2025, these distinctions have increasingly eroded. Global research on organized crime documents the expansion of multi-crime ecosystems in which gangs combine drug trafficking, extortion, and financial fraud, reflecting broader trends of diversification and transnational linkage in criminal activity [10]. At the same time, highly organized gangs in North America have expanded beyond market protection to exert deeper forms of social regulation. Contemporary research on transnational street gangs, such as Mara Salvatrucha (MS-13), highlights how decentralized organizational structures, territorial control, and coercive governance enable such groups to remain resilient and adaptive in the face of sustained law enforcement pressure, complicating suppression-based strategies that rely primarily on incapacitation [11].

This convergence suggests that the critical distinction between contexts is no longer origin, but stage of evolution. Violence in both regions increasingly blends economic rationality with community embeddedness, amplifying its adaptive capacity and complicating suppression-based responses.

6.4 Technology, built environment, and the precision of suppression

The effectiveness of suppression strategies is further conditioned by the built environment and the availability of technological surveillance. In many North American urban contexts, violence occurs within highly structured physical spaces characterized by formal street grids, stable infrastructure, and the widespread use of surveillance technologies such as closed-circuit television systems. Empirical research indicates that such technologies can support modest but meaningful reductions in certain categories of crime, particularly where dense infrastructure enables attribution and targeted enforcement [12].

In contrast, violence in many Caribbean settings is concentrated in underdeveloped or informally constructed communities, including squatter settlements and densely packed urban enclaves with limited infrastructure, poor lighting, and restricted accessibility. In these environments, technological surveillance is structurally constrained, making it more difficult to individualize responsibility for violent acts. Similar dynamics have been observed in informal settlements globally, where terrain, spatial density, and infrastructural deficits limit precision policing and increase reliance on blunt enforcement tactics.

These spatial conditions do not render suppression ineffective, but they significantly shape its outcomes. Where technology enables individualized targeting, suppression may fragment violence more efficiently. Where infrastructure limits surveillance, suppression is more likely to produce collective disruption, displacement, and adaptation rather than resolution.

6.5 Community empowerment as the decisive variable

Across both contexts, the comparative evidence points to a decisive variable: community empowerment. Violence proves most resilient where communities remain disempowered, fearful, and excluded from governance. Suppression in such environments may temporarily reduce visible harm, but it leaves intact the social conditions that enable violence to reorganize.

In North American cities, the failure to center communities has coincided with the entrenchment of organized and coercive gang structures within increasingly

impoverished neighborhoods shaped by migration, identity fusion, and economic exclusion. In the Caribbean, the absence of sustained community empowerment has allowed violence to gain renewed legitimacy through economic opportunity, criminal organization, and transnational connectivity. In both regions, violence adapts faster than institutions can respond.

7. Philadelphia as a contemporary hybrid model: Enforcement with community centrality

Philadelphia's recent experience illustrates the limits of suppression when detached from community legitimacy, as well as the potential of hybrid approaches that combine enforcement with sustained community investment. Under new police leadership, the city adopted a more assertive law enforcement posture in high-violence and high-disorder areas, most visibly in Kensington, where open-air drug markets and chronic violence prompted intensified patrols, targeted arrests, and coordinated inter-agency action. These efforts reflected a clear shift toward visible order maintenance and the disruption of violent and narcotics-related activity.

At the same time, city leadership explicitly framed enforcement as insufficient on its own. Large-scale public funding was directed toward community-based violence prevention, street outreach, hospital-based intervention, and trauma-informed services, positioning community actors as essential partners rather than ancillary supports. Philadelphia's homicide decline has occurred alongside – not in place of – these investments, reinforcing evidence that enforcement can suppress violence in the short term but cannot sustain reductions without community engagement, service provision, and legitimacy. The Philadelphia case thus underscores a central argument of this chapter: strong law enforcement may be necessary to stabilize violence-producing spaces, but without people-centered strategies that address social regulation, trust, and opportunity, suppression alone risks displacement, adaptation, and eventual resurgence rather than durable change.

8. Conclusion

This chapter has examined community violence across Caribbean and North American urban contexts through a comparative lens that treats violence as an adaptive social system rather than a static criminal phenomenon. Across settings, violence demonstrates a capacity to reorganize in response to pressure – altering its form, visibility, and organization while preserving core functions related to territorial control, identity, and informal governance. Suppression-oriented strategies, including states of emergency, intensified policing, and militarized rhetoric, may produce short-term disruption, but they rarely dismantle the social conditions that allow violence to persist and evolve.

The comparative analysis highlights a growing convergence in contemporary violence dynamics, despite differing historical origins. In the Caribbean, particularly Jamaica and Trinidad and Tobago, governments have increasingly relied on emergency powers and intensified enforcement in response to escalating homicide rates. These measures have coincided with periods of reduced visible violence and have attracted regional attention as potential models. At the same time, independent

analysis underscores that such gains are uneven and difficult to sustain, especially where legitimacy, accountability, and community agency remain weak. Trinidad's experience further demonstrates that people-centered interventions – such as evaluated violence interruption programs – can produce measurable reductions in violence, even in environments shaped by organized criminality and firearms proliferation.

Similar patterns are evident in North American cities. Philadelphia's recent experience illustrates the limits of enforcement when detached from community legitimacy, as well as the potential of hybrid approaches. Under new police leadership, the city adopted a more assertive law enforcement posture in high-violence areas such as Kensington, targeting open-air drug markets and chronic disorder. Crucially, these efforts were accompanied by substantial investment in community-led violence prevention, hospital-based intervention, and trauma-informed services. The city's marked decline in homicides and shootings has occurred alongside – not in place of – these community-centered strategies, reinforcing the conclusion that enforcement may stabilize violence-producing spaces but cannot sustain reductions without people-centered engagement.

This tension between suppression rhetoric and lived outcomes is especially visible in Chicago's contemporary public safety debate. In 2025, federal proposals to deploy National Guard troops to Chicago were advanced despite official data showing significant declines in homicides and shootings [13]. State and local leaders pushed back against militarized intervention, citing evidence that violence was already trending downward and emphasizing the role of community violence intervention and public health-oriented strategies in driving that progress. The juxtaposition is instructive: even as violence declines through community-engaged approaches, suppression-first responses continue to dominate political discourse, revealing a persistent disconnect between evidence and enforcement reflexes.

Taken together, these cases reinforce a central conceptual insight: violence behaves like an evolving social pathogen. Like a virus, it mutates in response to suppression – shifting geography, reorganizing networks, and exploiting new vulnerabilities. Yet the pathogen does not exist independently of its environment. Communities are the host. Where social trust, opportunity, and legitimacy are weakened, violence finds conditions conducive to transmission and persistence. Public health-oriented approaches recognize that durable change cannot be achieved by targeting symptoms alone [14]. Just as disease control requires strengthening the host's capacity to resist infection, effective violence prevention depends on empowering communities to interrupt transmission, reduce exposure to risk, and reinforce positive, non-violent norms. Without treating the host – by investing in people, relationships, and collective efficacy – suppression may reduce visible harm temporarily, but it cannot produce lasting immunity against the re-emergence of violence.

This understanding challenges prevailing assumptions about public safety across regions. It suggests that the question is not whether enforcement is necessary, but whether it is sufficient. The evidence presented here indicates that it is not. Sustainable reductions in violence are more likely when communities are positioned not as passive recipients of security but as active agents in redefining legitimacy, governance, and social order. Recognizing violence as adaptive – and communities as central to resistance – offers a more credible path toward lasting public safety in both Caribbean and North American urban contexts.

Acknowledgments

The author acknowledges the Peace Management Initiative and the Ministry of National Security in Jamaica for providing the platform to engage with more than fifty volatile communities over an eighteen-year period. These experiences provided invaluable insight into the dynamics of violence, community resilience, and grass-roots conflict mediation.

The author also wishes to recognize the influence of Dr. Elizabeth Ward and Mr. Horace Levy of the Violence Prevention Alliance in Jamaica, who encouraged the documentation and research of field experiences, as well as the development of innovative approaches to public safety across the Caribbean.

Appreciation is also extended to Anchor House Inc. in Trenton, New Jersey, for providing opportunities to engage with grassroots organizations and community leaders in Trenton. The author further acknowledges the dedication and creativity of violence prevention organizations in Philadelphia, as well as the supportive environment fostered by a progressive and community-focused municipal government and police force.

This work reflects years of professional engagement and research across multiple locations, including Jamaica, Trinidad and Tobago, the Bahamas, St. Lucia, St. Kitts and Nevis, Chicago, Trenton, Philadelphia, and Canada, where valuable lessons were learned about community-based approaches to violence prevention.

During the preparation of this chapter, the author used AI-assisted tools, including ChatGPT and Perplexity, to support language editing, structural organization, and clarity of expression. All conceptual arguments, analyses, and interpretations presented in this chapter remain the sole responsibility of the author.

Finally, the author extends gratitude to peace builders and community leaders around the world who continue to believe in the power of humanity and the capacity of individuals and communities to create meaningful change.

Author details

Damian Hutchinson

Independent Researcher, Philadelphia, United States

*Address all correspondence to: anefthutchie@gmail.com

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] National Academies of Sciences, Engineering, and Medicine. Proactive Policing: Effects on Crime and Communities. Washington, DC: National Academies Press; 2018
- [2] Sampson RJ. Great American City: Chicago and the Enduring Neighborhood Effect. Chicago: University of Chicago Press; 2012
- [3] Braga AA, Weisburd DL. The effects of focused deterrence strategies on crime: A systematic review and meta-analysis. *Journal of Research in Crime and Delinquency*. 2012;**49**(3):323–358
- [4] Papachristos AV, Braga AA, Hureau DM. Network exposure and homicide victimization in an African American community. *American Journal of Public Health*. 2013;**103**(1):103–109
- [5] Weisburd D. The law of crime concentration and the criminology of place. *Criminology*. 2015;**53**(2):133–157
- [6] Tyler TR. Why People Obey the Law. Princeton, NJ: Princeton University Press; 2006
- [7] Harriott A. Controlling violent crime in Jamaica: Policy and practice challenges. *Journal of Criminal Justice*. 2003;**31**(3):231–243
- [8] Butts JA, Roman CG, Bostwick L, Porter JR. Cure Violence: A public health model to reduce gun violence. *Annual Review of Public Health*. 2015;**36**:39–53
- [9] Ousey GC, Kubrin CE. Immigration and crime: Assessing a contentious issue. *Annual Review of Criminology*. 2018;**1**:63–84
- [10] United Nations Office on Drugs and Crime. Transnational Organized Crime in Central America and the Caribbean: A Threat Assessment. Vienna: United Nations Office on Drugs and Crime; 2012
- [11] Dura WSM. The Politics of Gang Control in El Salvador. Austin: University of Texas Press; 2017
- [12] Welsh BC, Farrington DP. Effects of closed-circuit television surveillance on crime. *Campbell Systematic Reviews*. 2009;**5**(1):1–62
- [13] Federal Bureau of Investigation. Crime in the United States 2023. Washington, DC: U.S. Department of Justice; 2024
- [14] Krug EG, Dahlberg LL, Mercy JA, Zwi AB, Lozano R, editors. World Report on Violence and Health. Geneva: World Health Organization; 2002

Chapter 2

The Use of Big Data to Address Refugee Victimization: A Scoping Review

Gabriela Mesquita Borges and Laura Neiva

Abstract

This scoping review maps the empirical landscape of how Big Data has been used in the context of refugee victimization. Drawing on six empirical studies published between 2021 and 2022, identified through a systematic search across four electronic databases, the review examines the ways Big Data has been used to detect, represent, and respond to violence, exclusion, and neglect affecting refugees. The findings reveal that, while Big Data offers significant potential to enhance visibility, inform protective measures, and guide institutional responses, it also raises critical ethical challenges related to privacy, representativeness, algorithmic bias, and digital exclusion. Through a descriptive-analytical approach, the review underscores the dual role of Big Data: as both a means of addressing vulnerability and a mechanism that can inadvertently generate new forms of harm or reinforce existing inequalities. By offering a critical synthesis of the empirical literature, this review contributes to ongoing debates in refugee studies, highlighting the urgent need for context-sensitive, participatory, and ethically robust approaches to the use of Big Data in this context.

Keywords: Big Data, refugee victimization, digital exclusion, algorithmic bias, hate speech, surveillance

1. Introduction

In recent years, the global refugee crisis has intensified, with millions of individuals forcibly displaced due to armed conflict, political persecution, environmental degradation, and systemic instability. This escalation reflects not only the growing number of global crises but also the compounded vulnerabilities faced by displaced populations [1–12].

According to the 1951 Refugee Convention, refugees are outside their country of nationality or habitual residence and are unable or unwilling to return due to a well-founded fear of persecution based on race, religion, nationality, membership in a particular social group, or political opinion. This legal definition, while foundational, does not fully capture the range of hardships and risks refugees face throughout their displacement [13]. As refugees navigate complex and often

prolonged journeys – from initial displacement through transit, asylum-seeking, and resettlement – they encounter overlapping forms of victimization [13]. These include not only physical and psychological violence but also symbolic and structural harms such as discrimination, exclusion, exploitation, and institutional neglect [3].

This form of victimization is not limited to moments of crisis; it is frequently embedded within the very systems intended to provide protection. Inadequate access to healthcare, education, and legal support exacerbates this precarity [4, 7, 14, 15]. Scholars have drawn attention to how both structural and symbolic violence permeate migration systems, often concealed within humanitarian frameworks and institutional policies [4, 13, 16]. Media narratives also contribute to this marginalization by reinforcing racialized images of refugees as threats or outsiders [17, 18].

Institutional actors – governments, humanitarian agencies, and international organizations – play a pivotal role in shaping the refugee experience [5]. Yet, their responses remain fragmented, reactive, and often limited by data deficits, bureaucratic inefficiencies, and policy inertia [1]. While frameworks such as the Global Compact on Refugees promote responsibility-sharing and rights-based protection, systemic gaps persist [19]. A growing focus on border securitization further erodes institutional commitments to equitable, consistent, and sustainable support [7, 20].

Concurrently, the digital transformation of social life has created new arenas – both threatening and empowering – for refugees. Among the most prominent developments within this transformation is the growing use of Big Data to capture, process, and interpret refugee-related information across multiple digital environments.

As used in this paper, Big Data refers to the techniques, practices, and systems employed to collect, cross-reference, analyze, and process large volumes of structured and unstructured data from sources such as social media platforms, institutional records, electronic health data, and participatory digital environments [21]. These methods – including sentiment analysis, machine learning, topic modeling, and geospatial mapping – are increasingly utilized to identify patterns and correlations related to refugee victimization. Under this definition, a wide range of digital systems and practices, from social media monitoring to institutional data processing and participatory platforms, constitute forms or sources of Big Data. While these tools offer powerful means to make refugee experiences more visible, assess risks, and inform interventions, they also carry the potential to reproduce violence, exclusion, or neglect when applied uncritically or without participatory and ethical safeguards.

This dual capacity of Big Data is perhaps most visible in the role digital platforms play in shaping refugee representation, discourse, and exposure to violence. Digital platforms enable xenophobic discourse, surveillance, and systemic exclusion; on the other hand, they provide tools for visibility, advocacy, and community building. Studies show that far-right actors have weaponized digital platforms to spread antirefugee disinformation across Europe, particularly during high-profile crises such as the Evros border standoff and the Moria camp fire [22]. These hostile narratives often extend to NGOs and activists, undermining humanitarian advocacy through coordinated online harassment and discrediting campaigns [23].

At the same time, digital technologies can act as catalysts for cultural preservation and political participation [24]. Refugees and other marginalized groups are

increasingly using digital platforms to document their experiences, share narratives, and build transnational communities [23, 25–28]. These “cybercultures” offer spaces for identity negotiation and belonging. However, digital participation is also stratified. Access to digital infrastructure and literacy remains uneven, particularly for women and young people, who face layered vulnerabilities in displacement contexts [29–31]. Online spaces are also shaped by corporate and hegemonic cultural logics that often marginalize refugee voices or commodify their experiences.

This marginalization extends into migration governance. Digital technologies such as biometric registration, facial recognition, and mobile phone data extraction are now central to refugee management systems [24]. As Amnesty International [32] notes, these tools often operate without transparency or accountability and risk reinforcing racialized surveillance regimes. While such technologies may offer efficiencies and enhanced monitoring capabilities, they also pose significant threats to refugee privacy, due process, and protection [26].

Participatory platforms and social media channels hold promise for real-time feedback and localized response [33], but they also generate risks. Without strong data governance and community control, these systems may amplify inequality and exclusion, undermining the very rights they purport to protect [28]. Ethical concerns around consent, data representativeness, and algorithmic bias remain under-addressed [33].

While refugee studies have acknowledged the increasing role of digital systems, no scoping review to date has systematically examined how Big Data has been used in the context of refugee victimization. Although individual studies have examined specific applications or ethical concerns, there remains a need for a broader synthesis of how Big Data contributes to identifying vulnerability – or, conversely, how it may shape new forms of harm and reinforce existing challenges. Considering this, this review, by focusing specifically on Big Data and refugee victimization, and drawing on six empirical studies published between 2021 and 2022 – identified through a systematic search across four electronic databases – offers an original contribution to the fields of refugee and migration research, as well as Big Data.

Adopting a descriptive-analytical approach [34, 35], it highlights the dual role of Big Data: while it holds significant potential to enhance refugee visibility, inform protective measures, and support institutional responses, it simultaneously raises critical ethical concerns related to privacy, representativeness, algorithmic bias, and digital exclusion. It moves beyond a merely technical or celebratory view of innovation and instead offers a critical, interdisciplinary synthesis that foregrounds ethical, political, and methodological concerns. The findings call for more reflexive, context-sensitive, and inclusive approaches to Big Data – ensuring that these tools serve not only to detect harm but also to advance protection, inclusion, and justice for displaced populations.

2. Methods

To develop this scoping review, we followed the guidance for descriptive reviews by Levac and colleagues (2010) and adopted the methodological framework for scoping studies proposed by Arksey [34].

2.1 Stage 1: Identifying the research question

The research question of this scoping review is: *How has Big Data been used in the context of refugee victimization?*

2.2 Stage 2: Identifying relevant studies

A search of the publications on three electronic databases (Web of Science, Scopus, and Annual Reviews) and via Google Scholar was undertaken in April 2025, with no restriction set for the time of publication. We used the following search expressions to identify relevant studies on the topic: “Refugees” AND “Big Data” AND “Victimization.” In addition, this search was followed by backward reference tracking, examining the references in the selected publications based on full-text assessment.

2.3 Stage 3: Study selection

The inclusion criteria allowed only original empirical studies written in English, reporting data on refugees, victimization, and Big Data. Nonoriginal full-length studies (commentaries, editorials, notes, newspaper articles, conference proceedings, and reports) were excluded. The titles of 330 records were retrieved. After removing duplicates, 219 articles were screened and assessed for eligibility. The first two authors independently screened all the papers based on the title and abstract, and subsequently based on the full text. This was cross-checked and discussed in both phases, and perfect agreement was achieved. The screening process is shown in **Figure 1**. Based on the title and abstract assessments, 214 records were excluded because they were not related to the research question ($n = 208$) or were not empirical studies ($n = 6$). Of the 5 fully read articles, 5 met the inclusion criteria. One article was included following backward reference tracking, and the final scoping review was composed of 6 articles. The search and screening process is shown in **Figure 1**.

2.4 Stage 4: Charting the data from the primary research

We developed a structured data charting form to systematically organize and synthesize relevant information from each study included in this scoping review. This form was designed to capture key descriptive characteristics of the empirical literature, including author(s), year of publication, country of study origin, study aims, data collection methods, participants, sample size, and the specific technologies or analytical tools used. This comprehensive mapping provided a clear overview of the landscape of Big Data applications in refugee research and allowed for consistency in comparative analysis.

Following the “descriptive–analytical” framework proposed by Arksey [34] and further refined by Levac [35], we approached the data extraction not simply as a technical inventory but also as a step toward critically assessing the results. Particular attention was paid to how each study conceptualized and operationalized **Big Data** – including its sources (e.g., social media platforms, institutional datasets, participatory platforms), analytical methods (e.g., machine learning, sentiment analysis, geospatial mapping), and stated or implied objectives related to refugee victimization.

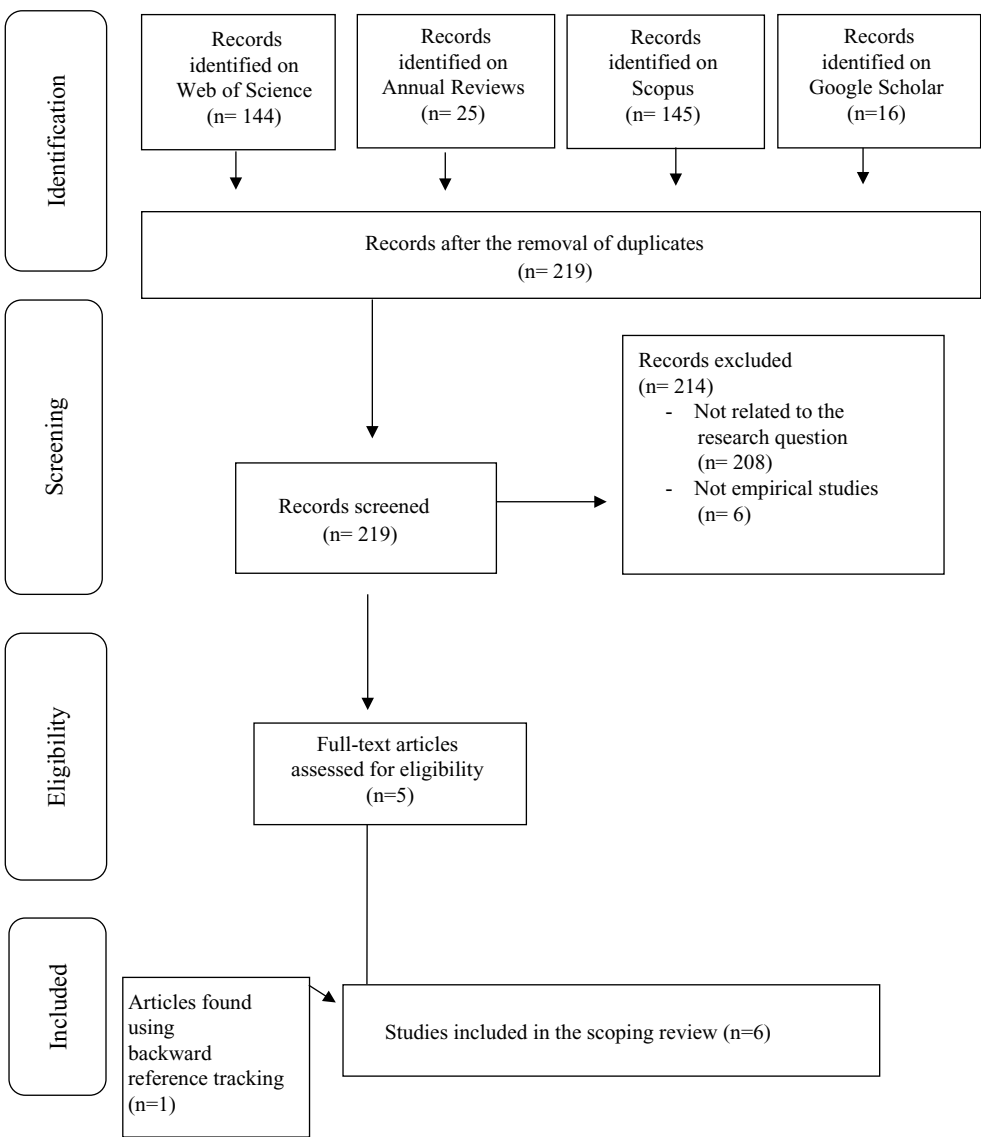


Figure 1.
Flowchart detailing the search and screening process of the scoping review.

Rather than organizing findings by methodological type or chronology, we opted for a conceptual structure that highlights the dual role of Big Data: (1) its capacity to respond to refugee victimization, and (2) its potential to reproduce or intensify vulnerability through bias, fragmentation, or exclusion.

2.5 Stage 5: Collating, summarizing, and reporting the results

Table 1 presents information about the main characteristics of the six included studies, ordered by year of publication. The main empirical achievements of the studies are discussed in the second part of the Results section.

Author(s)	Year	Country of origin	Study aim	Data collection methods	Participants	Sample size
Arcila-Calderón, C.; Blanco-Herrero, D.; Frías-Vázquez, M.; Seoane-Pérez, F.	2021	Spain	To analyze expressions of hate speech and sentiments on Twitter in Spain during the reception of the boat Aquarius.	Manual coding and computational analysis of tweets using sentiment analysis and topic modeling	Twitter users posting in Spanish using #Aquarius.	24,254 tweets
Huang, L. S.	2021	Canada	To identify and analyze the language-learning needs of adult Syrian refugees in Canada and realign language instruction accordingly.	Mixed methods: needs assessment surveys, semi-structured interviews, and analysis of learners' oral production using IELTS and NVivo.	17 LINC instructors and 14 adult Syrian refugee learners.	31 participants (survey), 17 interviews (instructors and learners), oral data from 14 learners.
Koukoulis, K. & Koukopoulos, D.	2021	Greece	To propose and evaluate crowdsourced collective memory management services using interactive refugee route maps to support cultural identity and integration in smart cities.	System development, user interaction testing, scenario-based evaluation.	Volunteers (refugees and descendants), specialists, and general users of the platform.	Not specified quantitatively; the system was tested via a case study and comparative evaluation.
Nyanchoga, M. M.; Lee, P.; Barbery, G.	2021	Australia	To explore electronic health records to estimate the extent of catch-up immunization and assess factors associated with under-immunization among refugees and asylum seekers in South-East Queensland.	Secondary analysis of electronic health records using statistical software (SPSS).	Refugees and asylum seekers referred to a specialized clinic in South East Queensland (aged 2 + years).	397 individuals

Author(s)	Year	Country of origin	Study aim	Data collection methods	Participants	Sample size
Sánchez-Holgado, P.; Amores, J. J.; Blanco-Herrero, D.	2022	Spain	To explore whether online hate speech on Twitter can be used as a predictor of social acceptance toward immigrants at the provincial level in Spain.	Analysis of 97,710 geolocated tweets using machine learning for hate speech detection; secondary data analysis from INE and CIS for immigration statistics and attitudes.	Geolocated tweets about migrants and refugees (2015–2020); Spanish citizens surveyed in the CIS 2017 study.	97,710 tweets; secondary survey data from CIS (exact number not specified).
Vrysis, L., Vryzas, N., Kotsakis, R., Saridou, T., Matsiola, M., Veglis, A., Arcila-Calderón, C., and Dimoulas, C.	2021	Greece (primary affiliation – first part of the study developed), with international collaboration (Spain, based on Arcila-Calderón – second part of the study developed).	To develop and present a web-based platform (PHARM) for the detection and analysis of hate speech against refugees and migrants across social media and online content.	Web scraping from multiple platforms (Twitter, Facebook, YouTube, news websites); sentiment and topic analysis; machine learning classification; geolocation tools.	Not applicable (no human subjects interviewed; data collected from publicly available digital content).	Multiple corpora are used; precise numeric sample is not given, but data is sourced continuously from multiple social platforms and web sources in real time.

Table 1.
 Overview of the five empirical studies included in the article.

3. Results

The studies span diverse geographic and thematic contexts, including the real-time monitoring of antirefugee sentiment through social media mining and automated analysis in Spain, the deployment of a web interface for multiplatform hate speech detection and analysis across Southern Europe, the use of participatory digital platforms to reconstruct disrupted narratives and document resilience in Greece, the exposure of immunization access disparities via institutional Big Data analysis in Australia, and the role of learner-generated data in shaping inclusive language programs for Syrian refugees in Canada.

4. Study characteristics

The included studies were published between 2021 [36–39] and 2022 [40]. All studies were conducted in single countries: three in Spain [39, 40], one in Canada [36], one in Greece [37], and one in Australia [38].

The methodological approaches varied: four studies employed computational or statistical methods using large datasets, particularly social media analysis and machine learning [39, 40] and electronic health records (EHRs) [38]; one study used a mixed-methods design, incorporating surveys, interviews, and language production analysis [36], while another focused on system development and scenario-based user evaluations [37].

Participants ranged from Twitter users [39, 40], social media users, and digital content creators across multiple platforms [39], to adult Syrian refugees and Language Instruction for Newcomers to Canada (LINC) instructors in Canada [36], and from healthcare clients and professionals involved in immunization programs [38] to volunteers and specialists engaged in digital heritage and identity-building platforms [37]. Sample sizes also varied, with studies analyzing 50,000–60,000 tweets and online posts [39]: 24,254 tweets [40]; 97,710 tweets [39]; multiplatform corpus (precise figures not reported), health records of nearly 400 individuals [38], and qualitative input from over 30 participants [36].

5. The use of big data to address refugee victimization

The review highlights the diverse applications of Big Data in addressing refugee victimization, revealing both its transformative potential and the critical challenges that accompany its use. Spanning applications in digital discourse analysis, hate speech detection, narrative preservation, healthcare data integration, and structured educational assessments, the six studies reviewed illustrate the multifaceted roles Big Data can play in making refugee victimization more visible – while also exposing critical gaps in coverage, interpretation, and inclusivity.

The study by Vrysis [39] provides empirical evidence on the application of Big Data to examine refugee victimization through public digital discourse. Analyzing 24,254 Twitter posts related to the reception of the Aquarius rescue ship in Spain, the authors employed sentiment analysis and topic modeling to detect patterns of online hostility. Their findings show that 27% of the tweets expressed hate or rejection toward refugees, while 9.9% were explicitly categorized as hate speech. These tools

enabled large-scale detection and emotional analysis of discourse, highlighting the capacity of Big Data to identify targeted hostility and track shifts in public sentiment. A temporal analysis revealed a paradox: while hate speech increased following the Spanish Prime Minister's decision to accept the Aquarius, overall sentiment became slightly more positive. This underscores the ability of Big Data to reveal layered and sometimes contradictory emotional trends in refugee-related discourse.

Vrysis [39] extends this potential through the development of the PHARM platform, a multiplatform web interface designed to detect hate speech against refugees and migrants across Twitter, Facebook, YouTube, and digital news outlets. By integrating machine learning, sentiment lexicons, and geospatial mapping, the platform enables real-time monitoring of xenophobic discourse. The study illustrates the role of Big Data infrastructures in consolidating fragmented digital sources and supporting the early detection of refugee-directed hostility. However, it also exemplifies the limitations of such tools. The reliance on automated classifiers and lexicon-based analysis presents challenges in interpreting nuanced content, such as sarcasm, coded language, or multilingual posts. These limitations are compounded by reliance on public data, which introduces sampling biases and excludes offline or less visible forms of victimization.

Sanchez-Holgado [40] offers a further example of Big Data use in monitoring refugee-targeted hostility. Using a dataset of 97,710 geolocated tweets from 2015 to 2020, the authors applied a machine learning classifier to identify hate speech directed at refugees in Spain. They correlated these findings with demographic data and public opinion surveys to assess whether digital hate discourse could predict local attitudes toward forced displacement. Although no significant statistical relationship was found, the study underscores both the promise and the interpretive risks of using digital trace data. The authors caution that online discourse is shaped by complex sociopolitical dynamics and that algorithmic tools are vulnerable to misclassification, particularly in relation to irony and culturally contingent expressions. This highlights the need for contextual and qualitative triangulation when using Big Data to assess exclusionary sentiment.

Koukoulis [37] presents Crowdpower, a participatory platform that applies principles associated with Big Data – such as metadata tagging, modular system design, and scalable content aggregation – to preserve refugee migration narratives. Although the platform does not employ predictive analytics or real-time data mining, it enables refugees and their descendants to contribute personal stories, images, videos, and geotagged content assembled into interactive maps. Migration routes are conceptualized as dynamic data containers, linking narrative fragments that reconstruct the emotional and cultural dimensions of displacement. The system affirms refugee agency and digital storytelling as tools for empowerment and cultural preservation. However, the lack of real-time monitoring and limited predictive capacity pose challenges for broader institutional adoption. Questions of data validation, long-term scalability, and systemic impact remain open.

Nyanhoga [38] demonstrates how Big Data is applied in healthcare settings to reveal refugee victimization through institutional neglect. Analyzing the EHRs of 397 refugee clients in South East Queensland, the study identified significant gaps in vaccine coverage. This use of Big Data exposes structural neglect that might otherwise be obscured in aggregated statistics. It also underscores the potential for digital integration across sectors – such as health, immigration, and settlement – to improve service delivery. However, the study also notes that fragmentation between

systems can limit the effectiveness of data infrastructures, leading to delayed or inadequate care. Even where Big Data exists, its underutilization or lack of coordination can reinforce vulnerability.

Huang [36], a mixed-methods study of adult Syrian refugees in Canada's LINC program, does not deploy Big Data technologies directly, but it draws on structured datasets analyzed with NVivo software and IELTS descriptors. The study highlights how institutional barriers – such as rigid curriculum standards, language assessments, and digital literacy gaps – mediate refugee vulnerability in education. Although based on qualitative tools, the structured nature of the data collection and analysis parallels certain aspects of Big Data methodology. However, the study also reveals how such structured systems can marginalize already vulnerable learners when they fail to reflect diverse socio-cultural realities.

Together, these studies present a nuanced picture. Big Data offers powerful capabilities for enhancing refugee visibility, detecting targeted hostility, and informing more inclusive policies. Yet, these same systems face critical limitations: algorithmic misclassification, data representativeness issues, lack of contextual sensitivity, and structural fragmentation can all reduce their effectiveness or even reinforce the exclusions they aim to redress. Moreover, the adoption of Big Data tools without participatory design or ethical safeguards risks depoliticizing refugee experiences and overlooking localized forms of victimization. For Big Data to contribute meaningfully to refugee protection, its use must be context-aware, ethically grounded, and integrated with broader institutional reforms that center refugee voices and address systemic forms of neglect.

6. Discussion

This scoping review highlights the diverse applications of Big Data in addressing refugee victimization, examining its potential to reveal patterns of violence, exclusion, and neglect, as well as its role in generating new forms of harm and reinforcing existing challenges. However, it is crucial to underscore that these insights are drawn from only six empirical studies meeting the strict inclusion criteria. This small corpus reflects the nascent and exploratory stage of research at this intersection. Consequently, the findings discussed here should be interpreted as indicative of emerging trends rather than as a comprehensive or generalizable account of the field.

The selected studies reflect a growing methodological shift in refugee research toward the adoption of large-scale, algorithmic, and automated approaches aimed at detecting patterns of exclusion, hostility, and neglect. While these technologies offer the potential to enhance visibility and responsiveness, they also raise critical ethical, methodological, and epistemological challenges.

Across the reviewed literature, a dual pattern emerges: on one hand, Big Data is shown to reveal hidden dimensions of refugee victimization that traditional methods may overlook – such as digital hate speech, service disparities, and emotional undercurrents in public sentiment. On the other hand, the same tools can introduce new risks, including algorithmic misclassification, contextual oversimplification, and the reproduction of institutional blind spots. The studies analyzed illustrate this ambivalence clearly.

Vrysis [39] and Sanchez-Holgado [40] demonstrate how sentiment analysis, topic modeling, and machine learning can detect hate speech against refugees on

social media platforms, revealing correlations between hostility and negative emotional tone, especially during politically sensitive moments. Vrysis [39] goes further by developing PHARM, a real-time platform that consolidates data from multiple digital sources to monitor xenophobic discourse. Their use of geospatial mapping and automated classifiers exemplifies how Big Data can support large-scale tracking and visualization of refugee-directed hostility. Meanwhile, Nyanhoga [38] analyzes EHRs to expose vaccination gaps among refugee populations, showing how institutional datasets – when mobilized effectively – can identify forms of structural neglect otherwise invisible in aggregated national statistics. Huang [36]'s study, while based on structured qualitative data rather than Big Data per se, reinforces the value of systematic data use in revealing institutional barriers in refugee education and integration processes.

However, these technological applications are accompanied by clear limitations. Vrysis [39] and Sanchez-Holgado [40] warn against the interpretive risks of relying on sentiment metrics alone, noting that irony, coded language, or cultural nuance often elude algorithmic detection. These limitations highlight a broader concern: that Big Data, despite its capacity for scale, may lack the cultural calibration and contextual sensitivity necessary to fully grasp the complexity of refugee victimization. This echoes broader critiques of how algorithmic systems – especially in migration governance – may reflect and reproduce symbolic and structural violence embedded in state and humanitarian practices [13, 16, 4].

Vrysis [39] raises similar concerns, pointing to classifier bias and content ambiguity that undermine the generalizability and ethical use of automated detection tools. These risks are intensified in securitized digital environments, where technologies such as biometric registration, facial recognition, and mobile phone surveillance often operate without transparency or accountability, reinforcing racialized forms of monitoring and social control [24, 26, 32].

Nyanhoga [38] shows that even institutional Big Data – such as health records – can be underutilized or poorly integrated across systems. Fragmented data governance and lack of cross-sector coordination reduce the proactive potential of these tools, allowing structural neglect to persist. Huang [36]'s study deepens this critique by demonstrating how educational institutions, despite having access to detailed learner data, may reinforce exclusion through rigid assessment frameworks, limited inclusivity, and inadequate attention to digital literacy.

Koukoulis [37] offers a contrasting vision of Big Data use through Crowdpower, a participatory platform that centers refugee agency in the co-production of migration narratives. While not predictive or real-time, the platform embodies key principles of Big Data – such as metadata tagging and scalable aggregation – while subverting its extractive tendencies. By prioritizing ethical storytelling, cultural preservation, and collaborative knowledge-making, this approach challenges dominant digital paradigms that often erase refugee perspectives. This addresses the problem of epistemic exclusion, as noted by Berg [29, 30], where refugee voices are marginalized by design in dominant digital systems – either through lack of access, algorithmic bias, or platform governance structures [28, 31].

These findings underscore the importance of combining the scale of Big Data with the depth of qualitative insight. While Big Data offers valuable tools for detecting emerging threats – such as hate speech, misinformation, or systemic service gaps – its effectiveness depends on ethical reflexivity, contextual interpretation, and methodological pluralism. Yet, given the very limited empirical base, caution is

warranted in extrapolating these results to broader contexts. The evidence available provides a useful snapshot of methodological and ethical tendencies, but the absence of longitudinal, comparative, and cross-regional analyses limits the robustness of general claims. Technological optimism must, therefore, be tempered by critical awareness of power asymmetries embedded in data design, access, and application – especially when dealing with displaced and vulnerable populations.

This review also raises questions about the institutional responsibilities shaping data governance in refugee contexts. As noted by McAdam [19] and [20], policy approaches often prioritize border control and bureaucratic efficiency over long-term protection. These tendencies are mirrored in digital contexts, where securitized logics, fragmented systems, and limited accountability continue to undermine refugee rights and dignity [1, 4].

Furthermore, the reviewed literature remains geographically imbalanced. Most studies are based in high-income Western countries, with limited empirical research emerging from the Global South, where the majority of the world's refugee populations reside. Countries such as Lebanon, Turkey, Kenya, and Bangladesh are underrepresented despite their critical relevance. This contributes to global knowledge hierarchies that prioritize Western data regimes and overlook the socio-political dynamics of refugee-hosting states [4].

In addition, the small number of studies ($n = 6$) reviewed here highlights both the novelty and the fragility of the empirical evidence base. The scarcity of studies constrains the ability to draw general conclusions but underscores the value of this synthesis as a first step toward systematizing a still-emerging research domain. Future research should build on this foundation by expanding the scope to include underrepresented regions, diverse data sources, and interdisciplinary methodologies that better capture local and cultural specificities.

Finally, a notable gap persists in the inclusion of refugee voices in the development, implementation, and evaluation of Big Data tools. Few studies engage refugees as active participants or cocreators of knowledge. This reinforces epistemic inequalities and raises concerns about who defines victimization, who controls data narratives, and how those narratives are operationalized in policy [3, 4, 13].

In sum, this review affirms the analytical potential of Big Data in refugee research but cautions that the current empirical base remains too limited to support broad generalizations. Its application must, therefore, be ethically grounded, context-sensitive, and participatory. Without these safeguards, data-driven innovation risks reproducing the very exclusions it seeks to redress.

7. Limitations

This scoping review has several important limitations that should be acknowledged to appropriately contextualize its findings.

First, the empirical base is extremely limited: only six studies met the strict inclusion criteria. This reflects the novelty of research at the intersection of Big Data and refugee victimization, but it also constrains the generalizability of the conclusions. The review should, therefore, be read as a preliminary mapping of an emerging field rather than as a comprehensive synthesis.

Second, all included studies were published between 2021 and 2022 and primarily originated from high-income, Western contexts. This temporal and geographic

concentration limits the diversity of perspectives represented, particularly from the Global South, where the majority of the world's refugees reside. As such, the insights generated here may disproportionately reflect Western data infrastructures, institutional frameworks, and socio-political contexts.

Third, the methodological heterogeneity of the included studies – ranging from machine learning applications and institutional data analyses to participatory and mixed-method designs – complicates direct comparison across findings. This variability, while enriching the descriptive scope, precludes systematic assessment of efficacy, validity, or replicability.

Finally, although the scoping review followed recognized methodological guidelines [34, 35], publication bias and language restrictions (English-only inclusion) may have led to the exclusion of relevant nonindexed or regional studies.

Future research should broaden both the linguistic and geographic scope of systematic searches and encourage empirical studies that integrate ethical, participatory, and cross-sectoral dimensions of Big Data use in refugee contexts.

8. Conclusion

As Big Data technologies become increasingly embedded in the study and governance of refugee populations, this scoping review provides an initial descriptive and analytical mapping of their diverse applications in addressing refugee victimization – highlighting both their potential to uncover patterns of violence, exclusion, and neglect, and their capacity to generate new forms of harm and reinforce existing challenges. Based on only six empirical studies, the evidence base remains limited and uneven, warranting cautious interpretation of the patterns identified. The findings presented here should, therefore, be read as indicative of emerging directions rather than conclusive trends.

The six studies reviewed reveal a fundamental tension between the promise of enhanced visibility, responsiveness, and institutional insight on one hand, and the risks of exclusion, misrepresentation, and neglect on the other. Big Data has enabled researchers and institutions to detect hate speech, identify health disparities, visualize large-scale hostility, and coconstruct refugee narratives with unprecedented scale and detail. These capacities offer the potential to surface marginalization that may go unnoticed through conventional methods. When used critically and responsibly, Big Data can contribute to a more proactive and informed response to the complex realities of forced displacement – particularly when deployed across platforms and sectors with integrative, real-time functionalities.

However, the relatively small number of studies included in this review underscores both the novelty and the fragility of the empirical field. This limitation does not diminish the contribution of the review; rather, it highlights its role as a foundational effort to consolidate a scattered and emerging area of inquiry. Future research must expand this evidence base through longitudinal, comparative, and cross-regional analyses, particularly in the Global South, to ensure that insights are contextually grounded and globally representative.

Nonetheless, the limitations of current Big Data practices remain significant. Algorithmic classifiers continue to struggle with nuance, irony, and culturally embedded expressions, while fragmented or siloed data systems restrict the ability to act on insights in a coordinated and effective way. Moreover, refugee voices are often

excluded from the design, validation, and interpretation of digital tools, reinforcing epistemic inequalities and undermining participatory justice. The depoliticizing effect of abstraction – where complex experiences of displacement are reduced to patterns or data points – also raises concerns about the ethical desirability of such approaches when used uncritically.

Importantly, the studies reviewed reflect a growing awareness of these risks and a willingness among scholars to move beyond simplistic views of technological progress. Participatory platforms like Crowdpower (as shown by Koukoulis [37]), critical analyses of algorithmic bias, and efforts to combine computational tools with qualitative insight suggest a promising path forward for recalibrating Big Data use in refugee research. These examples point to the value of hybrid, ethically grounded methods that center refugee agency, cultural specificity, and the need for institutional accountability.

Rather than positioning Big Data as inherently progressive or inherently problematic, this review advocates for interdisciplinary and reflexive frameworks that combine computational capacity with grounded, context-sensitive analysis. Such models are essential to ensure that technological innovation in refugee studies aligns with the core values of protection, inclusion, and social equity.

The implications of these findings extend to both research and policy. By identifying the capabilities and constraints of existing Big Data applications, this review can inform the development of ethical standards in refugee data governance, promote cross-sectoral integration, and support the creation of rights-based digital tools that respond to the actual needs and experiences of displaced populations. Policymakers, humanitarian actors, and technologists must work collaboratively to ensure that Big Data infrastructures not only expose vulnerabilities but actively contribute to meaningful protection and social transformation.

Ultimately, while Big Data continues to reshape humanitarian knowledge and decision-making, sustained attention to ethical governance, power asymmetries, and the lived realities of refugees remains essential. Given the limited and geographically narrow empirical foundation, these conclusions should be viewed as a starting point for deeper, more inclusive, and empirically grounded inquiry – one capable of preventing the reinforcement of the very exclusions these tools aim to address.

Conflict of Interest

The authors declare no competing interests.

Acknowledgments

The authors acknowledge the use of ChatGPT for language polishing of the manuscript.

Author details

Gabriela Mesquita Borges^{*1} and Laura Neiva²

1 Center for Legal, Economic, and Environmental Studies (CEJEIA),
Communication and Society Research Center (CESC), Lusíada University of Porto,
Porto, Portugal

2 Department of Sociology, Center for Legal, Economic, and Environmental Studies
(CEJEIA), Communication and Society Research Center (CESC), Lusíada University
of Porto, Institute for Social Sciences, University of Minho, Braga, Portugal

*Address all correspondence to: gabrielamborges@por.ulusiada.pt

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Aas KF. *The Crimmigrant Other: Migration and Penal Power*. London: Routledge; 2019
- [2] Ataç I, Rygiel K, Stierl M. The contentious politics of refugee and migrant protest and solidarity movements: Remaking citizenship from the margins. *Citizenship Studies*. 2016;**20**(5):527–544. DOI: 10.1080/13621025.2016.1182681
- [3] Borges GM. Journey of violence: Refugee women's experiences across three stages and places. *Journal of International Migration and Integration*. 2024a;**25**:673–693. DOI: 10.1007/s12134-023-01102-z
- [4] Borges GM. Refugee women's intersecting social locations: A contemporary perspective on the process of becoming a refugee woman. *International Criminology*. 2024b;**4**:279–292. DOI: 10.1007/s43576-024-00138-0
- [5] Canning V. *Gendered Harm and Structural Violence in the British Asylum System*. London: Routledge; 2017. DOI: 10.4324/9781315720975
- [6] Canning V. Corrosive control: State-corporate and gendered harm in bordered Britain. *Critical Criminology*. 2020;**28**:259–275. DOI: 10.1007/s10612-020-09509-1
- [7] Freedman J. Sexual and gender-based violence against refugee women: A hidden aspect of the refugee "crisis." *Reproductive Health Matters*. 2016;**4**(47):18–26. DOI: 10.1016/j.rhm.2016.05.003
- [8] Freedman J. Grand challenges: Refugees and conflict. *Frontiers in Human Dynamics*. 2019;**3**:1–3. DOI: 10.3389/fhumd.2019.00001
- [9] Ilcan S. The borderization of waiting: Negotiating borders and migration in the 2011 Syrian civil conflict. *Environment and Planning C: Politics and Space*. 2020;**40**(5):1012–1031
- [10] Ilcan S. The border harms of human displacement: Harsh landscapes and human rights violations. *Social Sciences*. 2021;**10**(123):1–16. DOI: 10.3390/socsci10040123
- [11] Reilly N, Sahraoui N, McGarry O. Exclusion, minimization, inaction: A critical review of Ireland's policy response to gender-based violence as it affects migrant women. *Frontiers in Human Dynamics*. 2021;**3**:1–17. DOI: 10.3389/fhumd.2021.642445:contentReference[oaicite:0]{index=0}
- [12] Tastsoglou E, Petrinioti X, Karagiannopoulou C. The gender-based violence and precarity nexus: Asylum-seeking women in the Eastern Mediterranean. *Frontiers in Human Dynamics*. 2021;**3**:1–17. DOI: 10.3389/fhumd.2021.660682:contentReference[oaicite:1]{index=1}
- [13] Borges GM, Faria R. Breathing under water: Gendering the violence against refugee women. In: Bošković M, Globalization and Its Impact on Violence against Vulnerable Groups. USA: IGI Global; 2020. p. 1–25. DOI: 10.4018/978-1-5225-9627-1.ch001
- [14] Farmer P. *Pathologies of Power: Health, Human Rights, and the New*

War on the Poor. California: University of California Press; 2005

[15] Horn R, Wachter K, Friis-Healy EA, Ngugi SW, Creighton J, Puffer ES. Mapping complex systems: Responses to intimate partner violence against women in three refugee camps. *Frontiers in Human Dynamics*. 2021;**3**:1–15. DOI: 10.3389/fhumd.2021.613792

[16] Chamberlain-Salaun J, Mills J, Usher K. Linking symbolic interactionism and grounded theory methods in a research design: From Corbin and Strauss' assumptions to action. *SAGE Open*. 2013;**3**(3). DOI: 10.1177/2158244013505757

[17] Bailey OG, Harindranath R. Racialised 'othering': The representation of asylum seekers in news media. In: Stuart A, editor. *Journalism: Critical Issues*. Maidenhead: Open University Press; 2005. p. 274–286

[18] Himmel R, Baptista MM. Migrants, refugees and othering: Constructing Europeaness. An exploration of Portuguese and German media. *Comunicação E Sociedade*. 2020;**38**:179–200

[19] McAdam J. The global compacts on refugees and migration: A new era for international protection? *International Journal of Refugee Law*. 2018;**30**(4):571–574. DOI: 10.1093/ijrl/eez004

[20] Mayblin L, Wake M, Kazemi M. Necropolitics and the slow violence of the everyday: Asylum seeker welfare in the postcolonial present. *Sociology*. 2019;**54**(1):107–123. DOI: 10.1177/0038038519862124

[21] Cukier KN, Mayer-Schoenberger V. The rise of Big Data. *Foreign Affairs*. 2011; **33**(3):28–40

[22] Institute for Strategic Dialogue. The Networks and Narratives of Anti-refugee Disinformation in Europe. 2021. Available from: <https://www.isdglobal.org/wp-content/uploads/2021/07/The-networks-and-narratives-of-anti-migrant-discourse-in-Europe.pdf> [Accessed: 2025-April-12]

[23] Alencar A, Kondova K, Ribbens W. The smartphone as a lifeline: An exploration of refugees' use of mobile communication technologies during their flight. *Media, Culture & Society*. 2019;**41**:828–844

[24] Berg M. Refugee integration in Germany: The interplay of othering, digital exclusion, and identity negotiation. *Journal of International Migration and Integration*. 2025;**26**:235–254. DOI: 10.1007/s12134-025-01238-0

[25] AbuJarour SA, Krasnova H, Diaz Andrade A, Olbrich S, Tan CW, Urquhart C, Wiesche M. Empowering refugees with technology: Best practices and research agenda. In: *Proceedings of the European Conference on Information Systems*. 2017

[26] Alsaleh A. The impact of technological advancement on culture and society. *Scientific Reports*. 2024;**14**:32140. DOI: 10.1038/s41598-024-83995-z

[27] Andrade AD, Doolin B. Information and communication technology and the social inclusion of refugees. *MIS Quarterly*. 2016;**40**:405–416

[28] Gillespie M, Osseiran S, Cheesman M. Syrian refugees and the digital passage to Europe: Smartphone infrastructures and affordances. *Social Media + Society*. 2018;**4**(1):2056305118764440

[29] Berg M. Women refugees' media usage: Overcoming information precarity

in Germany. *Journal of Immigrant & Refugee Studies*. 2021;**20**(1):125–139. DOI: 10.1080/15562948.2021.1907642

[30] Berg M. Information-precarity for refugee women in Hamburg, Germany, during the COVID-19 pandemic. *Information, Communication & Society*. 2022;1–17. DOI: 10.1080/1369118X.2022.2129271

[31] Kutscher N, Hüttmann J, Fujii MS, Engfer NP, Friedrichs-Liesenkötter H. Educational participation of young refugees in the context of digitized settings. *Information, Communication & Society*. 2022;**25**(4):570–586

[32] Amnesty International. Defending the Rights of Refugees and Migrants in the Digital Age. 2024. Available from: <https://www.amnesty.org/en/documents/pol40/7654/2024/en/> [Accessed: 2025-March-21]

[33] UNHCR. Using Social Media in Community-based Protection: A Guide. 2021. Available from: <https://www.unhcr.org/innovation/wp-content/uploads/2021/01/Using-Social-Media-in-CBP.pdf> [Accessed: 2025-May-13]

[34] Arksey H, O'Malley L. Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*. 2005;**8**(1):19–32. DOI: 10.1080/1364557032000119616

[35] Levac D, Colquhoun H, O'Brien KK. Scoping studies: Advancing the methodology. *Implementation Science*. 2010;**5**(1):69. DOI: 10.1186/1748-5908-5-69

[36] Huang LS. “I have big, big, big dream!”: Realigning instruction with the language-learning needs of adult Syrians with refugee experience in

Canada. *Refuge: Canada's Journal on Refugees*. 2021;**37**(2):141–163

[37] Koukoulis K, Koukopoulos D. Rediscovering refugee routes: On the creation of collective memory map services. *Procedia Computer Science*. 2021;**191**:41–48

[38] Nyanchoga MM, Lee P, Barbery G. Exploring electronic health records to estimate the extent of catch-up immunisation and factors associated with under-immunisation among refugees and asylum seekers in South East Queensland. *Vaccine*. 2021;**39**(42):6238–6244

[39] Vrysis L, Vryzas N, Kotsakis R, Saridou T, Matsiola M, Veglis A, Arcila-Calderón C, Dimoulas C. A web interface for analyzing hate speech. *Future Internet*. 2021;**13**(3):80. DOI: 10.3390/fi13030080

[40] Sanchez-Holgado P, Amores JJ, Blanco-Herrero D. Online hate speech and immigration acceptance: A study of Spanish provinces. *Social Sciences-Basel*. 2022;**11**(11):1–20

Chapter 3

Artificial Intelligence and Crime on Social Media Platforms

Csongor Herke and Barbara Szabó

Abstract

In contemporary digital environments, social media platforms operate through artificial intelligence (AI)-driven systems, including algorithmic ranking, recommender infrastructures, targeted advertising architectures, and automated moderation processes. These systems do not merely organize content distribution; they also shape user attention, patterns of interaction, and exposure to digital risks. This study examines how AI-based platform ecosystems reconfigure opportunity structures for criminal conduct while simultaneously functioning as algorithmic gatekeeping mechanisms capable of mitigating harm. Drawing on routine activity theory, rational choice theory, and situational crime prevention, the article conceptualizes platforms as dynamic criminogenic environments that influence offending costs, the likelihood of detection, and victim vulnerability. The analysis identifies major forms of crime and harmful conduct associated with social media, particularly fraud, scams, harassment, cyberstalking, online abuse against children, deepfakes, and other forms of synthetic deception. It also explores central dilemmas of platform governance, including procedural safeguards, transparency, accountability, and the management of algorithmic bias, while reviewing key developments in European and international regulatory and liability frameworks. Special attention is given to the tension between platform efficiency and due process, especially where automated detection tools affect content visibility, user reporting, and account restrictions without adequate meaningful explanation or accessible avenues for review and redress. By linking investigative and evidentiary challenges to prevention-oriented governance mechanisms, the study formulates analytically grounded recommendations concerning safety by design, evidentiary readiness, and stronger child protection safeguards. It argues that effective responses to crime in AI-mediated platform environments require an integrated approach that combines criminological insight, technological governance, and rights-based regulation.

Keywords: artificial intelligence, social media, attention economy, platform governance, online fraud, cyberstalking, child protection, deepfake, digital evidence

1. Introduction

Social media platforms have become core infrastructures for everyday communication, information-seeking, and commercial exchange. A central

determinant of platform success lies in the acquisition and retention of user attention; competitive advantage accrues to actors capable of maximizing limited attentional resources and converting them into monetizable engagement. The monetization of attention extends beyond commercial strategy, as engagement-optimization logics may generate socially harmful externalities by prioritizing metrics such as view duration and audience reach. Within this environment, artificial intelligence (AI) constitutes a core infrastructural layer of platform governance, structuring feed ranking, personalization processes, advertising delivery, and rule enforcement through automated and semi-automated mechanisms.

From the perspective of crime, the AI-driven platform ecosystem exhibits dual characteristics. On the one hand, it reconfigures opportunity structures for offenders by reducing the transaction costs of initiating contact and deception, facilitating the identification of vulnerable target groups, and enabling the scalable industrialization of fraud or harassment campaigns. On the other hand, the same technological layer also expands the repertoire of algorithmic control mechanisms: Pattern recognition can support spam and bot detection, fraud prevention, the identification of content that endangers children, and the rapid sanctioning of rule-breaking behavior. Accordingly, risk management is structurally embedded in platform decision architectures, particularly in the configuration of visibility, accessibility, friction, and verification mechanisms.

The study proceeds from the recognition that crime-related risks on platforms cannot be explained solely by individual offender motivations. In the digital environment, offenses often emerge in situations shaped by platform design choices and optimization goals. Accordingly, the analysis interprets AI within a criminological framework, both as an opportunity structure and as a control tool. Routine activity theory (RAT) helps to explain how victim exposure increases through everyday platform use, while rational choice and situational crime prevention provide a basis for examining offending costs, the probability of detection, and the expected “benefit” from the perspective of platform features and rules.

Accordingly, the objectives of the study are organized around four interrelated research questions:

- (1) It explains how platforms’ AI ecosystems operate within the attention economy and through the mechanisms by which they can amplify risky content or connections.
- (2) It provides a criminological typology of the roles played by AI and interprets major crime types from a crime script perspective, especially in relation to fraud, harassment, the endangerment of children, and deepfake-based deception.
- (3) It reviews the dilemmas of platform governance, including the role of procedural safeguards and remedies, as well as the risks of bias and erroneous decisions.
- (4) Through an analysis of investigative and evidentiary challenges, it highlights why attribution, the integrity of digital evidence, and cross-border access to data are critical. It also proposes prevention and policy recommendations, with particular attention to safety-by-design, capacity building, and child protection.

The structure of the chapter is organized according to a coherent analytical logic: The study first clarifies the technological and economic operating modes of platforms and then interprets risks within a criminological framework; next, it discusses platform governance and regulatory dilemmas, and finally, it links evidentiary and prevention issues to concrete intervention points that are relevant both for platforms and public authorities.

2. The AI ecosystem of platforms and the attention economy

At the center of the business model of social media and content-sharing platforms is the acquisition, retention, and monetization of user attention. In the logic of the “attention economy,” platforms compete not merely through their content catalogs but through their ability to claim as large a share as possible of users’ limited daily attentional capacity. Tim Wu’s [1] analysis of the commodification of attention demonstrates how user attention has become a primary resource within the value chains of media markets and digital platforms. In the case of digital platforms, the mass collection of behavioral data and predictive analytics makes this extraordinarily efficient. As noted by Zuboff [2], this mode of operation is no longer simply advertising sales but “surveillance capitalism” built on predicting and shaping behavior.

This attention- and data-driven logic is operationalized through platforms’ AI ecosystems: Data-driven models rank the feed, recommend what to watch next, optimize ad delivery, and moderate user activity in automated (or semi-automated) ways. A distinctive feature of this system is continuous feedback; user interactions (clicks, view duration time, comments, shares) are also training signals that reappear in subsequent decisions. A ranking- and recommendation-driven environment is, therefore, not static. The platform calibrates the distribution of attention in real time, often along engagement-optimized objective functions [3].

However, maximizing attention can produce social and criminogenic externalities. Audits and experimental research suggest that engagement-based ranking, at least in certain topics and settings, may disproportionately amplify emotionally charged, divisive, or intergroup-hostile content, while user “satisfaction” and social welfare do not necessarily align with engagement metrics [3]. The dynamics of misleading content spreading on platforms are also connected to this. Large-scale analyses indicate that false news can spread faster and more widely in social networks than true news, partly because it appears more novel and elicits stronger reactions [4]. Overviews of the mechanisms of “fake news” emphasize that the incentive system of the attention economy (the logic of visibility and revenue) can favor polarizing and manipulated information [5]. This picture is nuanced by the fact that filter bubbles and ideological selection are partly the result of users’ networks and choices and partly a consequence of ranking and recommendation. Disentangling the two empirically is difficult but important [6].

In what follows, we review five core elements of the AI ecosystem (as shown in **Table 1**): Section 2.1 addresses algorithmic amplification/ranking followed by Section 2.2 on recommender systems, Section 2.3 on targeted advertising and micro-targeting, Section 2.4 on automatic/semi-automatic moderation, and Section 2.5 on generative AI and synthetic media (deepfakes). Particular attention is paid to how these technical solutions shape criminogenic risk channels (e.g., fraud, manipulation, harassment, disinformation) and to what governance and compliance tools may mitigate harms.

AI component	Primary objective/metric	Typical techniques	Criminogenic risks	Governance instruments
<i>Ranking (feed/search)</i>	Engagement, view time, “satisfaction” proxies	Learning-to-rank, multi-task models, A/B testing	Increasing the visibility of harmful/scam content; sensationalism and outrage spirals	Transparency; auditing; risk assessment
<i>Recommender system</i>	Retention, session length, relevance	Collaborative filtering; embeddings; DNNs; RL	“Rabbit hole” dynamics: the growth of extremist/prohibited content	Audits; mitigation; researcher access; parameter controls
<i>Targeted advertising/RTB</i>	CTR, conversion, revenue	Auction mechanisms; profiling; lookalike audiences	Targeting vulnerable groups; scams; discrimination; political manipulation	Data protection compliance; consent; advertising transparency
<i>Automatic/semi-automatic moderation</i>	Detecting rule violations; harm reduction	Classification; hashing; NLP; human-in-the-loop	False negatives/positives; bias; inconsistent enforcement	Procedural safeguards; appeals; quality assurance
<i>Generative AI/synthetic media</i>	Content production speed; scaling	LLMs; diffusion models; voice cloning	Deepfakes; identity theft; AI-Assisted phishing/scams	Labeling; provenance; risk management; regulatory requirements

Table 1.
Core components of platforms’ AI ecosystems, their objective functions, and typical risk channels.

2.1 Algorithmic amplification and ranking

Algorithmic ranking is the platform’s “visibility engine”; it determines which of the available posts, videos, comments, or search results are demonstrated to the user, in what order, and with what frequency. Ranking is not merely a form of filtering; it is also an amplification mechanism:

- The higher an item is placed, the more people see it.
- The more it is seen, the more interactions it generates.
- Those interactions are then fed back into the system as additional signals.

As a consequence of this feedback dynamic, ranking systems may disproportionately amplify specific categories of content, including material that is socially harmful or unlawful.

The social consequences of ranking are closely linked to the risks of disinformation and online crime. The rapid spread of false news is partly related to user psychology (e.g., novelty, confirmation bias) and partly to platforms’ visibility and engagement incentives [4]. For ranking systems, content that is “exciting,” “surprising,” or “outrage-inducing” often performs better on the metrics, meaning that the logic of the attention economy can easily converge on increasing the visibility of misleading content. This mechanism is also relevant to crime: Scammers, propagandists, and manipulators intentionally try to infer and exploit the “rules of

the ranking game” (e.g., through bot networks, coordinated sharing, clickbait headlines, or emotional triggers).

When interpreting the effects of ranking, it is important to distinguish user choice (whom I follow, what I click) from algorithmic mediation (what the system offers and what it makes visible). In criminological terms, this matters because the platform is not merely a mirror; it actively shapes the structure of publicity. Therefore, the visibility of risky, unlawful, or victim-harming content is partly the result of design and optimization decisions [6].

From a crime prevention perspective, ranking is ambivalent. It can reduce certain harms (e.g., by suppressing spam or obvious scams), but for more subtle “borderline” harms (manipulative ads, disinformation, harassing content), metric optimization can increase visibility. In practice, this is why solutions that add objectives beyond engagement (e.g., “quality,” “reliability,” “harm risk”) are gaining importance and why platforms increasingly test how changes in ranking parameters affect the “information health” of the platform [5].

2.2 Recommender systems

Recommender systems operationalize personalization in a manner that extends beyond mere ranking functions. They not only prioritize and order content originating from sources already followed by the user, but also proactively generate recommendations of new content, channels, accounts, or products, thereby shaping exposure patterns and influencing the expansion of user networks and consumption trajectories. A substantial share of platform experience is now “push”-based: Users do not necessarily search; they move along recommendation pathways assembled by the system. This is especially true for short-video formats, where user decisions (scrolling on, rewatching, liking) provide very rapid feedback to the models.

From a criminological perspective, the importance of recommender systems lies in the fact that they organize user attention into “paths.” Public discourse frequently invokes the “rabbit hole” metaphor to describe progressive exposure to increasingly extreme or conspiratorial content; however, empirical findings indicate that such trajectories are context-dependent and heterogeneous. The empirical evidence is mixed, so the issue requires nuance. Large-scale audits suggest that YouTube’s recommendations tend to suggest ideologically congenial content to partisan users and that, as viewing paths deepen, the share of ideologically problematic channels can increase for certain groups, while any increase in extremity is not necessarily linear [7]. Other work audits radicalization pathways and finds that the risk is not, in all cases, as strong as suggested by public discourse, but in certain communities and topic areas, recommendations can meaningfully contribute to exposure to problematic content [8].

For opportunity structures, it is especially important that recommender systems make visible parts of the network that were previously inaccessible to the user. This can be beneficial (e.g., discovering relevant educational content), but it can also facilitate crime:

- Gateways to illegal products or services (e.g., fraudulent “investment advice,” fake giveaways).
- Access to recruitment and radicalization content.

- Finding harassing or hate-promoting communities.
- Identifying vulnerable target groups (e.g., children, older users).

This is particularly the case when the recommender system can build a profile quickly, even from short interactions.

2.3 Targeted advertising and micro-targeting

Targeted advertising is the monetization core of the attention economy: Platforms build profiles from users' behavior and demographic characteristics and then sell the "right" attention moment to advertisers. Micro-targeting is the extreme form of this, where targeting moves beyond broad segments (e.g., "urban men aged 25–34") to fine-grained micro-groups defined by behavior and inferred interests. Analyses of political micro-targeting highlight that personalized messaging can simultaneously promise more effective mobilization and participation while carrying democratic risks (e.g., opaque campaign messages, presenting different "faces" to different voters, and intensive use of personal data) [9].

Micro-targeting is not only politically sensitive; it is also problematic from a criminological perspective. The targeted advertising infrastructure allows scammers and manipulators to reach vulnerable groups cost-efficiently and with high precision (e.g., in investment scams, users under financial stress; in health-related fraud, users searching for particular conditions). To interpret such "persuasive" techniques in legal terms, Calo [10] offers the concept of digital market manipulation: Firms (and by analogy, malicious actors) can tailor influence to individuals on the basis of behavioral data and cognitive biases, thereby challenging traditional consumer protection categories.

Micro-targeting constitutes a central revenue-generating mechanism within platform business models; from a criminological perspective, however, it simultaneously operates as infrastructural support for scalable deception, targeted victim selection, and manipulative practices. Risk management, therefore, cannot be limited to removing individual fraudulent ads; it also requires making the advertising ecosystem (adtech) more transparent, ensuring meaningful legal bases and consent, and clarifying platforms' responsibilities [11].

2.4 Automatic and semi-automatic moderation

A key question of platform governance is how platforms define and enforce the boundaries of permissible content, behavior, and account use. Moderation has traditionally been a human activity, but due to economies of scale and time pressure, automation is now indispensable. The term "algorithmic moderation" refers to technical and organizational solutions in which machine-learning systems and rule-based filters identify potentially rule-violating content, prioritize reviews, impose restrictions automatically, or support moderators' decisions in a human-in-the-loop configuration [12].

The technical repertoire of moderation is broad:

- Content classifiers (e.g., hate speech, harassment, fraud patterns, signals of self-harm).

- Hashing and “fingerprint”-based matching (especially for known unlawful images/videos).
- Spam and bot detection.
- Analysis of network behavior (coordinated inauthentic behavior).
- Language-technology models that attempt to capture context and intent.

From a criminological perspective, moderation is critical because platforms increasingly become both the “scene” and the “tool” of crime: Fraud, extortion, child abuse, harassment, hate campaigns, and disinformation operations can all occur on these surfaces. The effectiveness of automated moderation depends on multiple factors. False negatives (harmful content remains) cause direct victim harm, while false positives (legitimate speech is restricted) can reduce trust and push communities toward “shadow platforms.”

2.5 Generative AI and synthetic media (deepfakes)

The emergence of generative AI represents a qualitative shift in platforms’ content ecosystems. Whereas producing manipulated content typically required expertise and resources in earlier decades, widely accessible tools can now generate highly realistic text, images, voices, and videos. “Synthetic media” is thus both a creative innovation and a security risk, as the cost of producing forgeries drops dramatically and scaling becomes automatable.

Legal and security policy scholarship identified deepfakes early as a strategic risk. Chesney and Citron [13] argue that deepfake technology enables new types of abuse (e.g., extortion, reputational sabotage, fraud) and can undermine public trust, not least through the “liar’s dividend.” This is a challenge for democratic publics and for evidentiary processes alike. From a media-forensics perspective, Verdoliva [14] highlights that forgery and detection are locked in an arms race: As generative techniques improve, detection must continually adapt, especially in the compressed, metadata-poor environment of platform uploads.

From a criminological standpoint, one of the most important consequences of generative AI is the industrialization of deception. In online fraud, perceived “authenticity” is key; the more personalized and credible a message, the higher the probability of victimization. Europol assessments emphasize that deepfakes and voice cloning can expand the toolkit of classic “CEO fraud” (executive impersonation), document and identity forgery, and extortion [15]. Large language models (LLMs) can scale social engineering attacks by enabling criminals to generate high-quality, grammatically correct messages that fit the target’s context across languages and channels [16].

A key risk channel of generative AI is targeted phishing and organizational deception. Experimental research suggests that LLM-generated lateral phishing emails can be comparably effective to emails written by communication professionals, which is particularly risky for large organizations [17]. This connects closely to platforms because social media profile patterns, posts, and networks provide rich reconnaissance data for personalizing such attacks.

Generative AI and synthetic media open new scalable criminal capacities within platforms' AI ecosystems (deepfakes, voice cloning, AI-assisted fraud, automated disinformation). An effective response rests on multiple pillars [17]:

- Technical defenses (detection, provenance).
- Platform governance interventions (de-amplification, rapid removal, monitoring).
- Regulatory compliance and transparency.
- User and organizational resilience (awareness, verification protocols).

3. Criminological framework: AI as opportunity structure and control tool

In the context of social media platforms, AI constitutes not merely a technical infrastructure but a layer of socio-technical organization that simultaneously structures opportunity conditions for offending and mechanisms of control. A criminological interpretation is informed by theoretical frameworks that conceptualize crime not as an inherent offender attribute but as the outcome of situational configurations, decision-making processes, and contingent structural conditions. One such approach is RAT, which treats the spatio-temporal convergence of a motivated offender, a suitable target, and the absence of capable guardianship as central [18].

Rational choice and situational crime prevention extend this logic: They interpret offenders' decisions in terms of expected gain, effort, risk, and moral/psychological "costs," and they locate prevention primarily in changing the situation [19]. On digital platforms, situational conditions are algorithmically structured: Visibility, accessibility, communicative contact, diffusion dynamics, and sanction probabilities are mediated through automated decision-making systems. As a result, platform AI can be understood as a form of "criminogenic architecture" that can create new opportunity structures but also narrow opportunities.

Several authors in the digital crime literature note that classic theories can be applied online only with adaptations: For example, "space" and "proximity" are interpreted differently; guardianship is partly technical (e.g., identification, access control) and partly organizational (moderation), and it is often not local at all [20]. At the same time, platform logic is precisely what enables certain elements of offending and victim exposure to be industrially scalable (automated messaging, mass profiling, micro-targeting), making the online environment a productive field for situational approaches.

3.1 Theoretical starting points: Routine activity, rational choice, situational prevention

Routine activity theory suggests that crime levels are often driven not by the "mass" of offenders but by changes in everyday activities and the encounter patterns they produce [18]. On platforms, routine activities are linked to digital

presence (posting, commenting, messaging, consuming content, shopping, joining communities). Artificial intelligence does not “serve” these routines neutrally; it actively shapes them (what the user sees, whom they connect with, how quickly a message or ad reaches them). In doing so, it changes the visibility and accessibility of suitable targets, which is directly linked to victimization risk [21].

Rational choice models treat crime as a decision situation in which offenders weigh options under limited information and rely on heuristics [22]. Platform AI systems partly provide information (e.g., micro-targeting parameters, trends, publicly available profile data) and partly conceal risks (pseudonymity, rapid account cycling, cross-border operations). Decision situations are therefore often asymmetric: For offenders, risk is diffuse; for victims, loss is immediate and personal.

Situational crime prevention seeks to reduce the likelihood of offending by “hardening” the environment: It increases effort, increases detection risk, reduces rewards, reduces provocation, and removes excuses [19]. In platform environments, equivalents include contact limits (rate limiting), authentication steps, user reporting with rapid response, dampening the spread of risky content, and predictable enforcement of the consequences of rule-breaking. Artificial intelligence may, therefore, operate both as an instrument of algorithmic guardianship that mitigates risk and as a scaling mechanism that expands criminogenic exposure.

3.2 AI as opportunity structure: Access, visibility, scaling, and friction

A central component of AI-mediated opportunity structures concerns the distribution and amplification of visibility. Through algorithmic ranking and recommendation, certain content and profiles receive disproportionate attention, which can function as a “free marketing channel” for fraud and deception. Risky ads, fake promotions, or manipulated videos can reach mass audiences quickly without offenders having to maintain conventional infrastructure [23].

A second element is the radical reduction in the costs of access and contact. Direct messaging, commenting, or joining groups enables “target attempts” at speeds and volumes unimaginable in physical space. This is especially important for social engineering offenses, where industrial-scale volume compensates for low individual success probabilities [24].

A third element is scaling and automation. Generative AI and LLMs enable offenders to produce persuasive, linguistically and culturally adapted messages, create chatbots that imitate customer support, or even conduct voice- and likeness-based impersonations. The expertise requirements for crime decrease, while campaigns become more professional [16].

A fourth element concerns friction (resistance). Platforms often aim to maximize user experience by minimizing friction: fast sign-up, easy sharing, quick payments, and minimal identification. From a criminological perspective, reducing friction can also reduce the “transaction costs” of crime. Conversely, deliberately increasing friction (e.g., an extra step before opening a suspicious link or warnings for risky messages) can be understood as a digital equivalent of situational prevention [19].

3.3 AI as a control tool and gatekeeper: Moderation, fraud detection, and limits

Platform AI systems create not only opportunities but also checkpoints. Content moderation, spam and bot detection, fraud prevention, and risk-based ranking are domains where the volume would be unmanageable without automated models. “Capable guardianship” in digital space is often algorithmic [21]:

- Pattern recognition.
- Network analysis.
- Anomaly detection.
- Prioritization of user reports.

The effectiveness of algorithmic control mechanisms remains structurally constrained for several interrelated reasons. First, the relationship between platforms and offenders is adversarial: Rule breakers adapt to detection thresholds, develop new coded language and visual symbol systems, or use multistep steering across platforms. Second, AI models can make errors (false positives/negatives), undermining the legitimacy of enforcement and victims’ trust. Third, excessive automation can generate an “avalanche” of reports that is not proportional to the number of relevant cases authorities can process.

Child online protection is a particularly sensitive area. Mandatory reporting systems and platform detection tools (hash-based matching, behavioral analysis) are indispensable, but the quality of reports and missing context can reduce investigative effectiveness. International reports and data consistently indicate that online enticement and sextortion are increasing in volume and that expanding platforms’ reporting duties can drive further increases [25].

3.4 Typology

For the criminological analysis of platform AI, it is useful to employ a typology that categorizes not by crime types, but by the role of the technology:

- First, AI-enabled offending: when offenders directly use AI tools to carry out the act (e.g., generating persuasive text/voice or producing a deepfake) [13].
- Second, AI-amplified dissemination: when the platform’s recommender and ranking systems increase the reach of harmful content or help offenders “find” suitable victims.
- Third, AI-driven control: when automated platform systems detect, sanction, or reduce reach.

The analytical advantage of this typology lies in its capacity to demonstrate that a single offense category may manifest across multiple AI-mediated functional roles. For example, in fraud, generative AI can be the tool for producing deceptive messages, the recommender system can be the channel of diffusion, and platform

Role of AI	Criminological mechanism	Typical examples	Possible controls
<i>AI-enabled offending</i>	Lowers expertise requirements, increases persuasiveness, and automates communication	LLM-based phishing and romance scams; voice cloning; deepfake video	Authentication steps; detection models; increasing friction
<i>AI-amplified dissemination</i>	Increases visibility, accelerates network diffusion, and enables targeted reach	Harmful content going viral; targeting victims by interests	Ranking rules; risk-based demotion; transparency and auditing
<i>AI-driven control</i>	Algorithmic guardianship: pattern recognition, risk scores, rapid sanctions	Spam/bot detection; fraud prevention; CSAM matching	Human-in-the-loop; feedback channels; high-quality reports
<i>Adversarial dynamics</i>	Cat-and-mouse game: adaptation, threshold optimization, cross-platform steering	Coded language; account rotation; “link-in-bio” steering	Cross-platform cooperation, reporting standards, threat sharing.

Table 2.
The roles of artificial intelligence in platform-enabled crime: criminological mechanisms and intervention points.

fraud detection can be the control mechanism. In deepfake cases, AI is typically an offending tool, but detection also requires AI, meaning that control and offending are both AI-dependent [26].

As shown in **Table 2**, AI plays multiple roles in criminogenic processes – ranging from enabling offending and amplifying dissemination to AI-driven control and adversarial dynamics – with typical examples and possible controls summarized as follows.

4. Main crime types and patterns

Crime on social media platforms is highly heterogeneous: It ranges from economically motivated fraud to digital forms of interpersonal violence and sexual abuse committed against children. In the following section, we highlight four areas in which AI-based platform functions particularly strongly shape offending patterns:

- F and scams.
- Harassment and cyberstalking.
- Children’s online exposure and endangerment.
- Deepfakes and identity-based deception.

The objective is not to provide a comprehensive typology but to identify AI-mediated crime scripts and corresponding situational intervention points.

4.1 Fraud and scams: Social engineering, marketplace fraud, and trust-building

A common structural feature of platform-based fraud schemes is accelerated trust formation combined with the manipulation of decision-making contexts. Classic social engineering techniques (phishing, pretexting, impersonation) can be

particularly effective on social media because users see cues that resemble “real” relationships and brands (profile pictures, follower counts, comments), which function as heuristics of credibility.

Fraud scripts are often multistage:

- Capturing attention: an ad, a comment, a private message, or viral content.
- Building trust: a longer conversation, a “support” narrative emphasizing shared interests.
- Steering: moving the victim to an off-platform channel (encrypted messenger, email, or fake website) where platform control is weaker.
- Transaction: financial data, a crypto wallet, gift cards, and bank transfer.
- Account disappearance: deleting the profile, re-registering.

Within this structure, the role of AI appears in both mass reach and personalized persuasion [27].

Generative AI brings a new quality to deception: Instead of poorly written, easily recognizable scam messages, attackers can produce coherent communication adapted to local language use and emotionally “tuned” to the target and can even maintain automated dialogs that respond to victims’ messages. Europol assessments explicitly note that LLMs can lower entry barriers and improve the effectiveness of social engineering campaigns [16].

From a criminological viewpoint, prevention hinges on increasing friction and risk: warnings before suspicious links, additional identity checks tied to payments, limits on mass messaging, and rapid removal of brand impersonation. In situational terms, reducing “payoff” and increasing offender effort can have a direct impact [19].

4.2 Harassment and cyberstalking: Persistent surveillance, doxxing, and coordinated attacks

Harassment and cyberstalking may be conceptualized as digital extensions of interpersonal violence: Offenders repeatedly violate victims’ physical or symbolic private spheres, causing threats, fear, and loss of control. Classic accounts of cyberstalking emphasize that the online environment makes surveillance and contact cheap, and uncertainty constant [28].

Platform features (following, stories, location sharing, commenting) can provide offenders with an information-gathering infrastructure. The AI-based tools can further accelerate OSINT-style collection (mass search, sorting faces, language summarization) and can assist in producing communication “packages” aimed at shaming and dehumanization. Harassment is often not purely individual but group-based (brigading), where algorithmic diffusion amplifies visibility and increases victims’ isolation.

Harassment patterns often escalate: After initial online “attempts” (comments, messages), doxxing (publishing personal data), creating fake profiles, or the non-consensual distribution of intimate images may follow. Legal and criminological

discourse stresses that online harassment is not a “minor” abuse but can have serious psychological, social, and economic consequences [29].

Control here is twofold: the speed of platform moderation and reporting systems on the one hand and evidentiary viability (logging, screenshots, metadata) on the other. Excessive automation can easily result in under- or over-moderation; therefore, human-in-the-loop review and transparent complaint procedures are crucial for legitimacy.

4.3 Risks of online abuse against children

Children’s endangerment online encompasses several interlinked phenomena:

- Grooming and enticement.
- Sexual extortion (sextortion).
- The production and distribution of child sexual abuse material (CSAM).
- Exploitation linked to live streaming.

International threat assessments stress that the scale and complexity of the problem are increasing and that the capacity of the global response system often lags behind the risks [25].

Available data indicate that reports related to online enticement have risen significantly in recent years and that sextortion is increasingly financially motivated.

From a criminological perspective, grooming often connects to routine activities: Children’s “accessibility” (public profiles, open message reception), the absence of capable guardianship (parental oversight, platform constraints), and offender motivation jointly create risky convergence [21]. Platform AI is two-faced in this space: Recommendations, groups, and content pathways can create new meeting surfaces, while detection systems (behavioral signals, hash matching) are essential for any scalable discovery.

Generative AI also introduces new threats: Synthetic or manipulated images/videos can facilitate extortion and victim-blaming, and deepfake-like materials may be produced using real children’s faces. The risk is not only legal but also psychological and social: The threat of “irreversible publicity” is particularly severe for children [15].

4.4 Deepfakes, identity theft, and synthetic deception: A crisis of trust and evidentiary challenges

Deepfakes and related forms of synthetic media denote AI-based techniques capable of generating or manipulating audio-visual content in ways that simulate authenticity. Legal and security policy analyses suggest that deepfakes are simultaneously privacy-violating tools (harassment, extortion), economic risks (CEO fraud, impersonation), and social risks (disinformation) [13].

In criminal contexts, deepfakes often produce a “trust short-circuit”: Victims rely on familiar authentication cues (voice, face, brand visuals), while those cues become forgeable. Europol explicitly warns that deepfake technology is relevant across

Crime type	Typical platform pattern	AI-linked risk point	Prevention focus
Fraud/scams	Ad/DM → trust-building → steering to an external channel	Generative, personalized messages; voice/face impersonation	Friction + authentication; fraud detection
Harassment/cyberstalking	Repeated contact, surveillance, doxxing, coordinated swarming	OSINT automation; content and network amplification	Rapid moderation, evidence preservation, complaint procedure
Endangerment of children	Grooming via DMs; sextortion; CSAM distribution	High volume of detection signals; generative/synthetic content	Safety-by-design; age assurance; high-quality reports
Deepfake/identity theft	Fake profiles; deepfake calls/videos; imitating authenticity cues	Arms race between deepfake production and detection	Multistep authentication, detection, and user training

Table 3.
Selected crime types, platform patterns, and AI-related links.

several serious offense categories (e.g., fraud, extortion, evidence manipulation) and that law enforcement must adapt [15].

Identity theft and synthetic identity construction (fake profiles, “synthetic identity”) often begin with data that can be collected on platforms: photos, networks, workplace information, and life events. Offenders build coherent narratives that fit victims’ expectations. Generative AI accelerates this process (image generation, assembling personal stories, multilingual communication), making classic fraud types (romance scams, investment scams) increasingly difficult to detect [27].

On the control side, detection itself is AI-dependent: Deepfake detection methods are developing rapidly, but the literature suggests there is no “final” solution [26]. Prevention, therefore, requires both technical tools (detection, authentication) and situational measures (friction, enforcement, user awareness).

As shown in **Table 3**, different online crime types tend to follow recurring platform patterns, each with specific AI-linked risk points, and therefore require tailored prevention priorities, as summarized as follows:

5. Criminological framework: AI as opportunity structure and control tool

Crime risks on social media platforms (e.g., Facebook, Instagram, TikTok) do not arise merely because “many people are present” in the same digital space. Platforms’ AI-based systems (profiling, ranking, recommendation, targeting, and moderation) create a dynamic opportunity structure that both increases scalability (more victims, faster iteration, lower costs) and shapes the conditions of control (detection, evidentiary traceability, deterrence). The purpose of the following combined chapter is twofold:

- To provide a criminological set of concepts that interpret AI among the “environmental conditions” of offending.

- On this basis, to typologize the most common platform-adjacent crime types and characteristic offending patterns.

5.1 Opportunity structure from the perspectives of routine activity and rational choice

Routine activity theory suggests that most predatory crime requires, in space and time, the convergence of a “likely offender,” a “suitable target,” and the absence of capable guardianship [18]. In online environments, this triad does not disappear; rather, it transforms: Target “suitability” is increased by personal data, behavioral traces, vulnerability profiles, and accessibility (contactability), while capable guardianship is embodied by platform rules, moderation capacity, and users’ protective routines (e.g., two-factor authentication, privacy settings) [23].

Artificial intelligence directly affects all three elements:

- On the offender side, automated content production and targeted outreach (LLM-based messages, bots, “fraud-as-a-service”) reduce entry barriers and costs, thereby increasing the number and capacity of motivated offenders [30].
- On the target side, data collected and inferred by platforms’ advertising and recommendation systems enable high-precision identification of vulnerable groups (e.g., lonely users, users in crisis, users under financial pressure), which is critical, especially for fraud and sexual extortion [31].
- On the guardianship side, automated moderation, fraud detection, and the “trust and safety” toolkit can strengthen protective capacity; however, due to scale and adaptive counter-strategies (adversarial behavior), an arms race often develops between attackers and platforms [26].

5.2 Environmental criminology

Environmental criminology and crime pattern theory emphasize that crime is not randomly distributed in space; it is linked to nodes, paths, and edges [32]. On digital platforms, “place” can be captured functionally: groups, comment threads, live streams, private message channels, and micro-audiences “brought together” by recommendation systems. These digital places organize visibility and accessibility algorithmically; thus, platform “hot spots” relevant to crime are also AI-mediated: A given content type or community may reach large audiences temporarily, increasing opportunities for recruitment, grooming, or mass deception [30].

Situational prevention and crime script analysis break offending down into steps and identify intervention points (e.g., entry, reconnaissance, approach, communication, transaction, concealment). Artificial intelligence plays a dual role here as well: On the offender side, it accelerates steps of the script (e.g., mass generation of personalized outreach), while on the control side, platforms try to recognize those same steps as patterns (anomaly detection, spam filtering, risk scoring) [26].

Platforms’ AI toolkits typically target three functions:

- Detection (e.g., known CSAM hash matching, fraud patterns).

- Intervention (content removal, account suspension, warnings).
- Supporting evidentiary traceability (logging, auditable decision traces).

However, excessive automation carries the risk that false-positive signals and missing context may distort decisions and overwhelm reporting and investigative channels, especially in child protection, where report quality and the presence of metadata are key [33].

5.3 AI-mediated risks and main offense types

The following typology treats platforms’ AI systems not as “causes” but as catalysts: AI scales up already known offending logics (deception, coercion, exploitation) and creates new variants (synthetic identities, deepfake-based extortion). The chapter highlights four main groups:

- Online fraud and scams.
- Harassment and cyberstalking.
- Online abuse committed against children.
- Deepfakes, identity theft, and synthetic deception.

In practice, these categories overlap: For example, deepfakes can be instruments of fraud, harassment, and child abuse alike (as shown in **Table 4**).

Social media is a natural “distribution channel” for online fraud: Offenders can reach targets directly, and trust-building (rapport) often begins within the platform. Generative AI makes classic social-engineering techniques cheaper and more effective: It enables high-volume, personalized outreach; coherent, culturally adapted messaging; and rapid iteration and script fine-tuning. Artificial intelligence and LLM tools reduce expertise requirements while professionalizing fraud campaigns.

Type	Typical pattern	Role of AI (offense/control)	Key evidentiary risk
<i>Fraud/scams</i>	Social engineering; romance/investment scams	Mass, personalized outreach; fraud detection	Attribution: linking financial flows and platform data
<i>Harassment/cyberstalking</i>	Persistent contact, doxxing, threats, intimate deepfakes	Bots and generative content; moderation prioritization	Context interpretation, chain of custody, proving repetition
<i>Abuse against children</i>	Grooming, sextortion, CSAM distribution	Relationship-building and recommendation: hash matching and reporting	Missing metadata; encrypted channels; international cooperation
<i>Deepfake/synthetic deception</i>	Impersonation, extortion, fabricated evidence	Synthetic audio/video; deepfake detection	Authenticity; provenance verification; forensic assessment

Table 4.
Main platform-adjacent crime types and typical roles of AI (overview).

The magnitude of harm is reflected in the FBI Internet Crime Complaint Center (IC3) 2024 annual report, which documents nearly 860,000 complaints and reported losses exceeding USD 16.6 billion [34]. Although the report does not focus exclusively on social media, the relevant categories (phishing, investment fraud, identity misuse) are strongly platform-dependent because outreach, trust-building, and transaction preparation often occur in social spaces. INTERPOL's global assessment of financial fraud similarly emphasizes that combining AI/LLM tools with crypto-assets supports more sophisticated and rapidly scalable fraud operations [31].

Particular attention should be paid to long-horizon, trust-based scams such as the so-called “pig butchering” investment fraud, where offenders “fatten” trust over time and then steer the victim to a fake investment platform. Generative AI can add further “authenticity layers” to this: Voice cloning, visual manipulation, and automated tools for making identity and circumstances appear plausible. Consumer protection authorities have issued specific warnings about the risks of voice cloning [35].

Harassment and cyberstalking in the online environment often represent two points on a continuum: from recurring, unwanted contact to sustained pursuit involving threats, surveillance, reputational harm, and coercion [28]. A central point in criminological interpretations is that platforms provide low-cost, constant access to the target (messages, comments, tagging), while social networks and algorithmic visibility provide information about routines, relationships, and, in many cases, location patterns [20].

Applying situational crime prevention to cyberstalking emphasizes that narrowing opportunities (privacy settings, blocking, access control) and online “place manager” tools are both relevant. Artificial intelligence plays a dual role here as well: Offenders can automate harassing communication (bots) or use generated images/videos to increase shaming; at the same time, platform AI can prioritize intervention by recognizing content patterns. The challenge is that harassing messages are context-dependent (irony, coded threats, relationship history), so purely automated decisions can easily under- or over-moderate, resulting in uneven protection for vulnerable groups [36].

The policy salience of stalking and online pursuit is indicated by the Istanbul Convention, which treats stalking as a distinct form of violence and expects criminal-law responses. This is especially important in digital space because some harassing behaviors appear as a series of “small” events that may not seem severe individually but together form a high-risk pattern. Preserving platform logs and the chain of custody, as well as assessing repetition and the level of threat, are therefore key issues for investigation and courtroom proof.

Taken together, AI within social media ecosystems simultaneously expands criminogenic opportunity structures while redefining and partially strengthening mechanisms of algorithmic control. Criminological frameworks (routine activities, environmental criminology, crime scripts) help us understand the phenomenon not only as a technical innovation but as a reorganization of the situations that lead to criminal acts. For this reason, the following chapters justify a more detailed discussion of platform governance and responsibility, as well as evidentiary and investigative challenges, especially attribution and cross-border data access.

6. Investigative and evidentiary challenges: Attribution, digital evidence, and cross-border data access

Investigating crime that occurs on online platforms takes place in a distinctive evidentiary environment: Relevant data are dispersed across multiple actors (users, platforms, infrastructure providers, advertising and payment intermediaries, cloud providers), often exist only briefly, and fall under different jurisdictions. Digital traces are massive in volume, yet proof often depends on a single “link”: connecting an account to a natural person, authenticating a transaction, or establishing the origin of content (authenticity/provenance). Based on law enforcement threat assessments, the greatest challenges are as follows:

- Attribution and identification.
- Maintaining evidence integrity.
- The time burden and legal fragmentation of cross-border data access.

6.1 Attribution and the fragmentation of online identities

Attribution refers to the inferential process by which an investigation links an online act (post, message, ad, login, payment) to a particular account, device, and ultimately, a person. In the ecosystem of social media and related services, attribution is complicated by several factors [31].

- The separation of account and device layers (e.g., multiple devices per account; multiple accounts on one device).
- Account takeover and bot networks.
- Anonymization techniques (VPN, proxy, Tor).
- Platforms’ differing logging and data-retention practices.

For evidentiary purposes, it is critical to understand that “account = person” is typically not a direct factual identity but rather a probabilistic inference based on the convergence of multiple data sources. These may include login patterns, device and browser identifiers, Internet Protocol (IP) and Autonomous System Number (ASN) information, Subscriber Identity Module (SIM) and payment data, messaging time series, social graphs, location data, and open-source intelligence (OSINT). AI-based analysis can meaningfully support the development of investigative hypotheses through pattern recognition, clustering, and anomaly detection, but it does not replace attribution: Model outputs become probative only if data acquisition is lawful, processing is documented, and results are reproducible (audit trail). Excessive automation (especially given the risk of misattribution) directly affects the presumption of innocence and fair-trial guarantees.

6.2 Digital evidence as lifecycle, integrity, and chain of custody

A distinctive feature of digital evidence is that it can be copied easily and altered without visible traces; therefore, proving integrity can be at least as important in court as the content itself. International good practice approaches digital evidence from a lifecycle perspective [37]:

- Identification.
- Collection.
- Acquisition (imaging/extraction).
- Preservation.
- Analysis.
- Presentation.

At every point in the process, it must be documented who had access, when, with what tools, under what procedure, and how the evidence was kept unchanged (hashing, write-blocking, versioning, secure storage).

The importance of the chain of custody is particularly high for platform-related crime because evidence typically passes through multiple systems: platform exports, agency systems, forensic workstations, and analytical and visualization tools. A single undocumented transformation, time-zone issue, loss of metadata, or uncertain-provenance screenshot can provide a point of attack for the defense. Standards and guidelines for digital evidence (e.g., ISO/IEC 27037, NIST SP 800-86) therefore emphasize controlled, repeatable procedures and detailed logging [38].

As shown in **Table 5**, each phase of digital evidence handling involves characteristic risks and, therefore, requires minimum controls and clear documentation elements, as summarized as follows.

Phase	Typical risk	Minimum control	Documentation element
<i>Identification/seizure</i>	Omitting relevant data; unauthorized access	Immediate isolation; access control	On-scene record; timestamp
<i>Acquisition (imaging/extraction)</i>	Data loss; metadata damage; modification	Forensic acquisition; write-blocking; hashing	Hash values; device; and software versions
<i>Preservation</i>	Storage corruption; access incident	Encrypted, redundant storage; access logging	Chain-of-custody log; access log
<i>Analysis</i>	Non-reproducible steps; tool failures	SOPs; peer review; validated tools	Analysis log; audit trail
<i>Presentation</i>	Loss of context; ambiguous visualization	Proving provenance; methodological transparency	Expert report; appendices

Table 5.
Typical risks and controls across the digital evidence lifecycle.

6.3 Platform data, encryption, and the “time factor”

Types of data available from platforms (subscriber/account data, access logs and traffic data, content data, advertising and payment metadata) differ in sensitivity and are subject to different legal tests. In practice, temporal constraints constitute a critical limitation: Content may be deleted, logs may rotate, accounts may be terminated, and devices may be replaced. This is why the first critical step is often not the formal “request” but rapid preservation, freezing relevant data so that it can later be obtained lawfully.

The spread of end-to-end encryption (E2EE) further narrows the pool of direct content evidence: Service providers often cannot access message content, so proof relies more heavily on metadata, device-side forensics, and financial/communication correlations. The European e-evidence package, especially European Preservation and European Production Orders, is designed to reduce time loss. The regulation is due to apply from 18 August 2026 and aims to make service providers faster and more consistently reachable [39].

6.4 Cross-border data access: Instruments and conflicts

The traditional route for cross-border data access is mutual legal assistance (MLA/MLAT), and within the EU, the European Investigation Order (EIO) [40]. These channels, however, are often slow relative to platforms’ data-retention cycles. The Second Additional Protocol to the Budapest Convention (CETS No. 224) and the EU e-evidence package introduce new instruments intended to balance speed with rule-of-law safeguards, such as more direct cooperation with service providers, emergency cooperation, standardized forms, and frameworks for remedies [41].

Toward third countries, the US CLOUD Act is especially important because many global platforms operate under US jurisdiction. It provides a framework for compelling disclosure of data stored across borders and, through bilateral agreements, may enable faster access [42]. In parallel, jurisdictional conflicts such as data protection constraints, encryption, and local freedom-of-expression guarantees can create compliance dilemmas for providers. Investigative strategy, therefore, needs multiple tracks:

- Rapid preservation.
- Requests/orders based on an appropriate legal basis.
- Alternative evidentiary routes (device forensics, open-source data, financial traces).
- Early international coordination.

As shown in **Table 6**, key cross-border cooperation instruments differ in scope and in what they accelerate, and they therefore rely on distinct safeguards while also creating practical implementation risks, as summarized as follows.

Instrument	Scope/territory	What it speeds up	Key safeguard	Practical risk
<i>EIO (2014/41/EU)</i>	EU Member States	Standardization of investigative measures	Judicial control; remedies	Time-consuming; divergent practices
<i>EU e-evidence (2023/1543)</i>	EU; platform providers operating in the EU	More direct production/preservation of data	Fundamental-rights exceptions; executing authority	IT implementation; compliance burdens
<i>Legal representative (2023/1544)</i>	EU	Reachability and enforceability	Central authorities; sanctions	Incomplete global coverage
<i>Budapest 2nd Protocol (CETS 224)</i>	Parties to the Protocol	More direct cooperation; emergency channels	Rule-of-law and data protection safeguards	Uneven ratification/implementation
<i>CLOUD Act</i>	US + bilateral agreements	Faster access with US providers	Remedies and treaty conditions	Conflict with other data protection regimes

Table 6.
Comparison of cross-border electronic evidence-gathering instruments.

6.5 Proof in the age of AI: Prevention and policy recommendations

As generative tools and synthetic media become increasingly accessible, evidentiary assessment must place heightened emphasis on authenticity verification and provenance analysis: An image, audio, or video is no longer persuasive on its own if the source file, creation context, or the possibility of manipulation cannot be examined. Technical detection (e.g., deepfake classification) is not sufficient in itself; courtroom usability requires validated methods, known error rates, and verifiable procedures. Artificial intelligence systems, therefore, strengthen proof only if organizations operate them within a risk management and quality assurance framework, similar to the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (NIST AI RMF) approach (context, impact, measurement, monitoring), and if methodological control can also be ensured for the defense (expert contestability, documented parameterization, audit traces).

The mitigation of platform-enabled crime cannot rely exclusively on ex-post investigative responses. An effective strategy integrates prevention (design, business incentives, user protection), enforcement (rapid response, evidence preservation), and accountability (transparency, auditing, remedies).

The essence of safety-by-design is that providers assess abuse risks early in product and feature development and apply built-in protective elements that reduce harms. This can include safe default settings, limiting risky viral mechanisms, adding abuse-signaling “frictions,” strengthening authentication, and making advertising and content-distribution processes more transparent [43]. In the European context, this aligns with the Digital Services Act (DSA)’s risk assessment and risk mitigation expectations, as well as the General Data Protection Regulation (GDPR)’s requirement of data protection by design and by default.

From an investigation and proof perspective, an “evidence-ready” approach is also recommended: Platforms should design logging and incident-response processes

so that, upon a lawful request, they can provide data quickly, in standard formats, and with verifiable integrity. This includes automating the handling of preservation requests, implementing strict internal controls over log access, and publishing transparent statistics on data requests [43].

Capacity building for law enforcement and justice systems is needed on three levels:

- Human competencies: digital forensics, OSINT, basics of crypto-assets, platform regulation knowledge, and critical interpretation of AI outputs.
- Organizational processes: standard operating procedures (SOPs), quality assurance for forensic labs, and consistent documentation of the chain of custody (especially for first responders).
- Technological infrastructure: scalable data storage, secure evidence repositories, and validated analytical tools.

International threat assessments suggest that increasing data volumes and legal uncertainty (e.g., data-retention frameworks) are major drivers of overload, which directly worsen response times and the chances of successful proof [37].

In preventing online abuse against children, risk-based platform governance is not sufficient on its own: Age- and development-sensitive solutions are needed that reduce exposure and increase the chance of accessing help. International policy materials emphasize age-appropriate defaults, limiting personalized recommendations for minors, child-friendly reporting channels, and strengthening parents' and schools' digital competencies [44].

An important element of a victim-centered approach is balancing rapid removal with evidence preservation: Removing harmful content matters, but processes must ensure that evidence can be preserved lawfully and used later. This is especially sensitive, requiring coordination among providers, authorities, and child protection actors, and involving simultaneous requirements for remedies, encryption, and data minimization [44].

The effectiveness of policy and platform regulation can improve only if interventions are measurable and feedback-driven. Possible instruments include the following:

- Standardized transparency reports (content removals, account actions, data requests).
- Independent audits of risk management and the abuse exposure of recommender and advertising mechanisms.
- Incident data sharing and exchange of good practices through Eurojust, Europol, and other international networks.

This approach corresponds to a model of adaptive or “learning” regulation, in which regulatory frameworks evolve in response to empirical feedback and technological change; alongside norms, implementation and measurement should also evolve, especially given the fast innovation cycles of AI systems [45].

7. Summary

The central conclusion of this study is that AI systems within social media platforms simultaneously expand criminogenic opportunity structures while functioning as algorithmic gatekeeping mechanisms. Because the incentive system of the attention economy pushes platforms to optimize visibility and reach, it can create situations that favor deception, harassing behavior, or the exploitation of vulnerable groups. In parallel, without AI-based moderation and risk management tools, protection proportional to the volume of activity would be practically impossible. The central challenge does not concern the existence of automation but rather the institutionalization of safeguards, transparency obligations, and effective remedial mechanisms within platform decision architectures, as well as how bias and erroneous decisions can be managed, since these can cause both victim harm and fundamental-rights infringements.

With respect to the main offense types, the study highlights that:

- The industrialization of fraud and scams is enabled by scalable outreach and personalized deception.
- In harassment and cyberstalking, persistent access and network amplification create risk.
- In the endangerment of children, new forms of relationship-building and steering emerge.
- Deepfakes and synthetic deception raise a crisis of authenticity and new evidentiary questions.

In light of these dynamics, effective prevention points toward embedding safety in design, improving evidentiary readiness, expanding organizational and technological capacity, and enhancing child protection safeguards. In investigation and proof, attribution, preservation of data, consistent documentation of the chain of custody, and faster international cooperation are the key determinants of practical effectiveness.

AI-use disclosure statement (translation)

This chapter was originally written in Hungarian. During the preparation of the English version, an artificial intelligence tool (ChatGPT, OpenAI) was used solely to assist with translation and language editing. The authors reviewed, verified, and edited the AI-assisted output. The authors take full responsibility for the content of the chapter.

Author details

Csongor Herke* and Barbara Szabó
University of Pécs, Pécs, Hungary

*Address all correspondence to: herke.csongor@ajk.pte.hu

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Wu T. *The Attention Merchants: The Epic Scramble to Get inside Our Heads*. New York: Alfred A. Knopf; 2016
- [2] Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs; 2019
- [3] Milli S, Carroll M, Wang Y, Pandey S, Zhao S, Dragan AD. Engagement, user satisfaction, and the amplification of divisive content on social media. *PNAS Nexus*. 2025;**4**(3):pgaf062. DOI: 10.1093/pnasnexus/pgaf062
- [4] Vosoughi S, Roy D, Aral S. The spread of true and false news online. *Science*. 2018;**359**(6380):1146–1151. DOI: 10.1126/science.aap9559
- [5] Lazer DMJ, Baum MA, Benkler Y, Berinsky AJ, Greenhill KM, Menczer F, et al. The science of fake news. *Science*. 2018;**359**(6380):1094–1096. DOI: 10.1126/science.aao2998
- [6] Bakshy E, Messing S, Adamic LA. Exposure to ideologically diverse news and opinion on Facebook. *Science*. 2015;**348**(6239):1130–1132. DOI: 10.1126/science.aaa1160
- [7] Haroon M, Wojcieszak M, Chhabra A, Liu X, Mohapatra P, Shafiq Z. Auditing YouTube's recommendation system for ideologically congenial, extreme, and problematic recommendations. *Proceedings of the National Academy of Sciences*. 2023;**120**(50):e2213020120. DOI: 10.1073/pnas.2213020120
- [8] Ribeiro MH, Ottoni R, West R, Almeida VAF, Meira Jr W. Auditing radicalization pathways on YouTube. In: *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAccT '20)*; 27-30 January 2020; Barcelona, Spain. New York: ACM; 2020. p. 131–141. DOI: 10.1145/3351095.3372879
- [9] Zuiderveen Borgesius FJ, Möller J, Kruikemeier S, Fathaigh R Ó, Irion K, Dobber T, et al. Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review*. 2018;**14**(1):82–96. DOI: 10.18352/ulr.420
- [10] Calo R. Digital Market Manipulation. *The George Washington Law Review*. 2014;**82**:995–1051. DOI: 10.2139/ssrn.2309703
- [11] Veale M, Zuiderveen Borgesius F. Adtech and real-time bidding under European data protection law. *German Law Journal*. 2022;**23**(2):226–256. DOI: 10.1017/glj.2022.18
- [12] Gorwa R, Binns R, Katzenbach C. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*. 2020;**7**(1):1–15. DOI: 10.1177/2053951719897945
- [13] Chesney R, Citron DK. Deep Fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*. 2019;**107**:1753–1819. DOI: 10.2139/ssrn.3213954
- [14] Verdoliva L. Media Forensics and DeepFakes: An Overview. *IEEE Journal of Selected Topics in Signal Processing*. 2020;**14**(5):910–932. DOI: 10.1109/JSTSP.2020.3002101
- [15] Europol. Facing reality? Law enforcement and the challenge of

- deepfakes [Internet]. Luxembourg: Publications Office of the European Union; January–2024. Available from: <https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes> [Accessed: 2026-March-03]
- [16] Europol. ChatGPT – The impact of Large Language Models on Law Enforcement [Internet]. Luxembourg: Publications Office of the European Union; 2023. Available from: <https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement> [Accessed: 2026-March-03]
- [17] Bethany M, Galiopoulos A, Bethany E, Bahrami Karkevandi M, Beebe N, Vishwamitra N, Najafirad P. Lateral Phishing with large language models: A Large organization comparative study. *IEEE Access*. 2025;13:60684–60701. DOI: 10.1109/ACCESS.2025.3555500
- [18] Cohen LE, Felson M. Social change and crime rate trends: A routine activity approach. *American Sociological Review*. 1979;44(4):588–608
- [19] Clarke RV, editor. *Situational Crime Prevention: Successful Case Studies*. 2nd ed. Monsey, NY: Criminal Justice Press; 1997
- [20] Yar M. The novelty of ‘cybercrime’: An assessment in light of routine activity theory. *European Journal of Criminology*. 2005;2(4):407–427. DOI: 10.1177/147737080556056
- [21] Leukfeldt ER, Yar M. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*. 2016;37(3):263–280. DOI: 10.1080/01639625.2015.1012409
- [22] Cornish DB, Clarke RV, editors. *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York: Springer-Verlag; 1986
- [23] Wall DS. *Cybercrime: The Transformation of Crime in the Information Age*. 2nd ed. Cambridge: Polity; 2024
- [24] Verizon. 2024 Data Breach Investigations Report (DBIR). 2024. Available from: <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf> [Accessed: 2026-March-03]
- [25] WeProtect Global Alliance. *Global Threat Assessment 2021*. 2021. Available from: <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf> [Accessed: 2026-March-03]
- [26] Mirsky Y, Lee W. The creation and detection of Deepfakes: A Survey. *ACM Computing Surveys*. 2021;54(1):1–41. DOI: 10.1145/3425780
- [27] Button M, Cross C. *Cyber Frauds, Scams and their victims*. London: Routledge; 2017
- [28] Spitzberg BH, Hoobler G. Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society*. 2002;4(1):71–92. DOI: 10.1177/14614440222226271
- [29] Citron DK. *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press; 2014
- [30] Europol. *The changing DNA of serious and organised crime: EU-SOCTA 2025* [Internet]. Luxembourg: Publications Office of the European Union; 2025. Available from: <https://www.europol.europa.eu/cms/sites/>

default/files/documents/EU-SOCTA-2025.pdf [Accessed:: 2026-March-03]

[31] Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024 [Internet]. Luxembourg: Publications Office of the European Union; 2024. Available from: <https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> [Accessed: 2026-March-03]

[32] Brantingham PL, Brantingham PJ. Nodes, paths and edges: Considerations on the complexity of crime and the physical environment. *Journal of Environmental Psychology*. 1993;**13**(1):3–28. DOI: 10.1016/S0272-4944(05)80212-9

[33] National Center for Missing & Exploited Children (NCMEC). CyberTipline Report [Internet]. 2024. Available from: <https://www.missingkids.org/cybertiplinedata> [Accessed:: 2026-March-03]

[34] Federal Bureau of Investigation (FBI). Internet Crime Complaint Center (IC3) 2024 Annual Report: Internet Crime Trends and Statistics [Internet]. 2024. Available from: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf [Accessed:: 2026-March-03]

[35] Puig A Fighting back against harmful voice cloning [Internet]. 2024. Available from: <https://consumer.ftc.gov/consumer-alerts/2024/04/fighting-back-against-harmful-voice-cloning> [Accessed:: 2026-March-03]

[36] Gillespie T. Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media. New Haven: Yale University Press; 2018. DOI: 10.12987/9780300235029

[37] Kent K, Chevalier S, Grance T, Dang H Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. Gaithersburg (MD): National Institute of Standards and Technology; August 2006. DOI: 10.6028/NIST.SP.800-86

[38] Nath S, Summers K, Baek J, Ahn G-J Digital Evidence Chain of Custody: Navigating New Realities of Digital Forensics. In: *Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA 2024)*. Washington, DC, USA: IEEE; 2024. p. 11–20. DOI: 10.1109/TPS-ISA62245.2024.00012

[39] European Parliament and Council. Regulation (EU) 2023/1543 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. (E-evidence Regulation). *Official Journal of the European Union*. 2023;**191**:118–180. <http://data.europa.eu/eli/reg/2023/1543/oj>

[40] European Parliament and Council. Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters. *Official Journal of the European Union*. 2014;**130**:1–36. <https://eur-lex.europa.eu/legal-content/en/NIM/?uri=celex:32014L0041>

[41] Eurojust. Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence The Hague: Eurojust; 27 July 2022 Available from: <https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access> [Accessed: 2026-March-03]

[42] United States Department of Justice (US DOJ), Criminal Division, Office of International Affairs. CLOUD Act Resources: Guidance and Overview of the Clarifying Lawful Overseas Use of Data Act [Internet]. Washington (DC): US Department of Justice; 2019. Available from: https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf [Accessed: 2026-March-03]

[43] Australian eSafety Commissioner. Safety by Design [Internet]. Canberra (ACT): eSafety Commissioner; 8 January 2026. Available from: <https://www.esafety.gov.au/industry/safety-by-design> [Accessed: 2026-March-03]

[44] United Nations Children's Fund (UNICEF). Keeping children safe online: Trends in online platform regulation and emerging lessons. [Internet] Policy brief. New York: UNICEF; Dec 2025 Available from: <https://www.unicef.org/documents/keeping-children-safe-online> [Accessed: 2026-March-03]

[45] Tabassi E. (ed.). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1 [Internet]. Gaithersburg (MD): National Institute of Standards and Technology; January 2023. DOI: 10.6028/NIST.AI.100-1 [Accessed: 2026-March-03]

Chapter 4

Cybercrime and Organised Crime: Distinct Criminal Forms in the Digital Era

Thomas Joyce

Abstract

The digital era has changed the face of organised crime. Not only has physical world organised crime become increasingly suffused with cybernetic elements – encrypted communication technologies and crypto-currency based money laundering – but digital-world cybercrime has become progressively more organised, mirroring the criminal motivations and opportunity structures traditionally associated with organised crime. Nevertheless, the effect of digitalisation on organised crime should not be overstated; the conflation of these two distinct criminal forms can have unfortunate theoretical and political consequences. This book chapter explores this dual dynamic with specific reference to the cybercrime and organised crime literature. The proposed argument undercuts simplistic conceptions of cyber and organised crime in favour of a more complex, flexible approach that seeks to better delineate collaborative profit-driven crime in the offline and online domains.

Keywords: cybercrime, organised crime, digitalisation, criminal profile, modus operandi, organisational structure

1. Introduction

Crime does not exist in a vacuum. Much like everything else in our world, crime evolves. The advent of new technologies has allowed criminals to conduct their real-world operations with greater efficiency and has facilitated the development of innovative, online iterations of classic crimes. Drug trafficking finds its counterpart in darknet drug vending, prostitution in online sex work, and theft in hacking [1–3]. While we once had organised crime, we now have an organised crime enhanced through technology, along with a new category of crime, cybercrime [4].

For years, the debate as to whether cybernetic offences qualified as an entirely distinct form of crime or were simply a digitalised version of older forms, raged on [5–9]. Without a clear resolution to the deadlock, a grand softening appeared to take place, whereby scholars seemed to come to the apparently measured conclusion that the truth lies somewhere in between. We now accept, on the one hand, that there exist crimes that cannot be committed without a computer, while, on the other hand,

we emphasise that the offender motivations and opportunity dynamics across the digital and physical spheres remain broadly the same [10]. This compromise satisfies not merely cyber-criminologists striving to gain recognition for cybercrime as a concept, but also those of us who work within the vaguely defined schools of dispositional and situational criminology. What this apparent balance ignores, however, are the significant changes in other theoretical components that occur when criminality shifts from the physical to the digital [11]. In some cases, these changes are so dramatic that associations between the digital and physical iterations of a given crime start to break down – the physical crime ceases to be clearly recognisable in its digital equivalent [2, 11].

Organised crime, as a concept, is in particular danger. Long has it stood on uneven theoretical ground [10–14]. Scholars have been arguing since the better part of the 21st century as to what does, and what does not, qualify as organised crime [10, 14]. Is organised crime simply crime that is organised? Is organised crime better understood as crime that is organised, and serious? Are there other, deeper, more complex dynamics at play that designate criminal activity as organised? Though the literature seems to reveal a now generally agreed-upon understanding of organised crime as defined by *governance*, policy makers, states, and the media have insisted on preserving the concept in its broadest interpretation: as any crime that is organised [14]. By this logic, cybercrime has been both implicitly and expressly included – in everything from legal directives to newspaper coverage – under the firmament of organised crime [15].

This chapter presents the argument that organised crime and cybercrime should not be conflated, and that continuing to do so could have unfortunate consequences for law enforcement, academics, and justice. The argument is structured as follows: first, an understanding of cybercrime, drawn from the literature, is presented; second, an understanding of organised crime, drawn from the literature, is presented; third, the two are empirically compared; fourth, analysis is made on the basis of the same; fifth, conclusions are drawn on the basis of this analysis. The chapter seeks to acknowledge the impact of digitalisation in the creation of cybercrime, challenge it in relation to the evolution of organised crime, and ultimately emphasise the theoretical and practical importance of keeping these two forms of criminality separate.

2. Cybercrime

When the cybercriminal organisation Scattered Spider broke into virtual infrastructure, they did so through a clear process [16]. Initially, the group sent a phishing message to employees of a target company, purporting to be a supplier of said company. They would, for example, present themselves as a VPN provider, warning that the VPN had been deactivated, and, in order to prevent data risks, the employee should access their website immediately. Scattered Spider cleverly designed the website to appear legitimate so as to lure an employee into providing their confidential login details. Once they gained access to these details, they then used them to access the computer systems of the target company, in order to retrieve confidential data sets or transfer the cryptocurrency discovered therein into their own private accounts. In this way, the two-step mistake of an employee from a major streaming service – initially being duped by the fraudulent email and then foolishly

inserting their details into the unregistered website – could allow these criminals to access subscription data, which they could then copy and sell on the darknet. According to the U.S. case files pertaining to their arrest and prosecution, the group earned millions of dollars through this process [16].

The advent of cybercrime has yielded heated debate as to its nature. Many argued that cybercrime solely refers to crimes that can be perpetrated over the internet; others argued that cybercrime rather refers to crimes that are facilitated by the internet [5–9]. Though scholars seem to have agreed that both statements are descriptive of cybercrime, both of these arguments are, in fact, wholly problematic. By focusing solely on computer-exclusivity, you eliminate almost all crimes being committed online, and by focusing solely on facilitation, you broaden the scope of online crime to include almost all crimes committed in the modern era [10]. Hackers still operate in a physical space, and many even collaborate in person; using Telegram to organise a drug deal does not make it cybercrime [17–20]. Most worryingly, both of these approaches undermine attempts to gain a better grasp of what cybercrime actually is, as they imply that physical-world crime only differs substantially from its digital analogue when it has a new name. Hacking is hacking, not theft; a drug deal remains a drug deal. But this is far too presumptuous. A criminal act (drug dealing), and the motivation behind it (money), might be the same in either the offline or online domains, but that does not imply the actor profiles, modus operandi, and business structure are not sufficiently different to be worthy of distinction [1, 2, 11].

We are all familiar with the stereotype: a lone hacker, young, wearing a dark hoodie, busily hacking the personal information of individuals, from any potential location in our world. This is the image consistently presented to the public by television entertainment, social media, and the news. Yet, it is largely inaccurate [10, 17, 20]. Rather than simply engaging in hacking, the truth is that for-profit cybercrime is a far-reaching category of crime, with countless variations – from online fraud scams to the exchange of child pornographic material – of which hacking is simply one [3]. Nor does cybercrime necessarily involve significant technological expertise: it very much depends on the given form of cybercrime being perpetrated and the specific role of the actor involved [10]. The success of Scattered Spider was as much about social engineering – the ability to confidently charm employees of victim companies into believing their legitimacy – as technological fluency. Despite the well-established connection between both youth and criminal activity, and youth and the use of internet technologies, young people are by no means synonymous with cybercrime [1, 10]. Though the Scattered Spider group were indeed all young, evidence from recent data from diverse studies hints at an enormous age range amongst cybercriminals. Not merely age: all profile indicators, from gender, to ethnicity, to socio-economic background, present a diversity rarely evidenced in other forms of serious crime [1, 10]. Anonymity, distance from collaborators and victims, the absence of violence, and porous barriers to entry facilitate the possibility that almost anyone could, hypothetically, become involved in cybercrime. Conversely, victims of same tend to be quite specific. Of course, the victim of a given cybercrime wholly depends on the cybercriminal act; but when speaking of for-profit cybercrime, in opposition to other forms of crime, the victims tend to be institutions [10]. Either private enterprises are targeted for their monetary wealth and access to personal data, or the state is targeted, indirectly, through the cybercriminal capacity to flaunt laws and regulations governing online and offline practises alike.

Cybercriminal activity can be quite complex. Though modus operandi vary across forms of cybercrime, studies have shown that for-profit cybercrime often demands significant collaboration and expertise from its participants [1, 10, 11, 17, 20]. Scattered Spider worked as a unit to develop phishing strategies, create convincing fraudulent interfaces, and launder their illicit proceeds. This required a variety of different capacities, in terms of problem-solving (manipulation techniques), technological expertise (developing fraudulent websites), and ingenuity (capitalising on company access). Of course, the real-world incarnation of the same crime – the robbery of a major multinational by a group of burglars – might also present complexity, the finesse of which would depend on the given group. Yet it would be temporally and spatially quite different, requiring the criminals to actually be on-site at the company, likely involving forceful methods to break in, avoid, intimidate, or threaten present employees, and being centred around physically escaping with large quantities of on-site money. For phishing scams, time is stretched: it may take a long time to hook a duped employee, and once their credentials are secured, it may be a long time before they are used. When exploited, those credentials may simply be used to explore the interior space of the company before anything of value is actually taken. Space is similarly altered. Scattered Spider executed crimes against companies across the world, all from the comfort of their respective homes [16]. Our hypothetical burglars would need to be on-site to commit the crime, implying a degree of mental fortitude and bodily immediacy. Distance allows for psychological detachment – which has a variety of implications, from techniques of neutralisation to a flattening of physical requirements demanded by theft. Thus, the nexus of tension is not necessarily between simplistic (real-world) and complex (digital domain) but rather between distinct kinds of complexity; the point of emphasis being that cybercrime is complex in a radically different way.

Cybercriminal groups tend to have the structure of a firm [10, 11, 21, 22]. Just as Scattered Spider operated like a small company, working together in unison towards a financial goal, so too do most cybercriminal groups collaborate for the sake of gain [1, 17, 20]. Theoretically speaking, this means that, as opposed to disorganised entrepreneurs, or highly organised complex networks, cybercriminal activity likely lies somewhere in between [10]. This is not necessarily ubiquitous – there remain freelance actors, and there may be cases of larger organisations at work – but the evidence shows that cybercriminals – from ransomware attacks to darknet trafficking offences – seem to operate in small, close-knit groups either in online or offline spaces [10, 11, 21, 22]. People, even scholars up until quite recently, tended to discount this offline dimension. Yet it is critical for understanding cybercrime. This is because of a certain contradiction of our expectations: despite being radically international hypothetically, studies show that cybercrime tends to be quite localised, with particular countries being vulnerable to particular expressions of cybercrime [10, 17]. Hackers based in Russia are the prototypical example. During the Soviet period, American technologies were banned, and even if sourced, often unusable. This led to a unique hacking cultural development, whereby the pathway into the use of technologies was often through decryption and alteration – deviance being somewhat of a constituent of their cybernetic landscape. Relatedly, the economy of Russia remains highly centred on the provision of energy; in comparison with the West, education for, work in, and income derived from, the tech sector is limited. Combined with democratic integrity effects – cybercriminals that focus solely on Western companies may hold little punitive intrigue for the State – and

corruption – cybercriminals that are of interest may be able to purchase immunity – the result is a context relatively ideal for hacking. Going further, recent studies have revealed that cybercrime may even be entirely localised, with criminals working together in-person over an extended period of time [1, 10, 11]. We can thus imagine that cybercriminal firms may actually operate in a manner similar to online businesses. There is a hierarchical structure, an entrepreneurial boss develops the business model, and employees fill out particular roles within it; with the firm itself being born out of a specific context, with criminal conduct being committed in both, and along the intersection of, the online and the offline domain [11, 22].

3. Organised crime

To ensure control over their cocaine trafficking route through Ecuador, Los Choneros exploited a vast network of direct employees, and indirect freelance connections [22]. In collaboration with a number of other cartels, they formed a critical part of the chain that ultimately started with the production of cocaine deep in South American forests, and ended in small bags of white powder in the pockets of consumers on North American city streets. People were murdered, businesses exploited, and politicians corrupted on a vast scale to fulfill this role; the results of which were significant growth across the horizons of membership, notoriety, and wealth. Despite the arrest and prosecution of their leadership, Los Choneros continue to operate, albeit while wrestling with a power vacuum and in a somewhat weakened state.

Our understanding of organised crime has evolved over time. From initial associations with particular ethnic groups in the past to the current focus on modus operandi in the present, our understanding of the phenomenon has gradually deepened through the dedicated work of a small band of scholars [13, 14]. We now recognise organised crime proper as a function of governance: what truly makes an organised crime group is the attempt to manage and regulate a given market, service, or territory [13, 14]. The Mafia controls the supply of protection; cartels control a given trafficking route. In this sense, organised crime should be understood as implicit to a will-to-monopolise. A number of high-profile scholars have delved deeply into this idea, exploring the theoretical margins of governance and quietly arguing for a narrow definition of organised crime centred around this concept [13, 14, 23–25]. Unfortunately, this narrow, and more nuanced approach, marks a clear distinction from policy, where organised crime is frequently insisted upon as synonymous with ‘crime that is organised’. The issue with this approach is that it essentially encompasses all forms of collaborative, profit-driven crime, including cybercrime – risking a dramatic conflation.

Organised crime profiles have been largely untouched by digitalisation. However, the relationship between organised crime, and those who commit it, remains complicated. Take ethnicity, for example. Though scholarship has advanced far beyond considering ethnicity a key motivating factor in participation in organised crime, the concept has nonetheless lingered as an apparent dynamic underlying criminal group formation – with the majority of groups being ethnically homogenous. This does not necessarily imply the imposition of hard-coded, exclusionary rules but rather relates to how all groups – criminal or non-criminal – develop and grow based on similarity and common interests [14, 23, 25]. This also makes ethnicity across groups highly variable: we can have the Kinahan Drug Cartel

emerge from the Irish context, and the 'Ndrangheta come forth from the Italian. Members of organised crime groups tend to be male [26–28]; but show a broader age-curve variability than for standard crime, with older leaders, and sometimes older new recruits [25]. It is apparent that Los Choneros, for example, is comprised largely of Ecuadorian men, of varied ages, with effort and organisation split across the various tasks mandated by a drug trafficking operation of that scale. Relatedly, today, as in the past, formal education amongst organised crime group members tends to be low [29, 30] as does legitimate employment experience [31]. The overall connection between reduced legitimate economic opportunity and participation in organised crime thus appears well established [29–33]. To our knowledge, digitalisation has not resulted in significant changes these profile dynamics.

Organised crime has certainly been made more efficient by technology. While hard evidence of organised crime proper – trafficking cartels and mafia-type organisations – being involved in cybercriminal activity remains scarce, it is widely apparent, especially in the wake of major international-level enforcement operations – such as the Sky and EncroChat takedowns – that members of traditional organised crime groups are using computer technologies to communicate, launder their illicit proceeds, and manage their operations [29]. Los Choneros, like any large business operation, would have most certainly availed themselves of the internet, as a facilitator of their activities. Nonetheless, we should not overstate the influence of contemporary technology on organised crime; as in the digital era, organised crime role requirements remain fundamentally unchanged. The capacity for violence, intimidation, and other criminal expertise still plays a direct, crucial role [26, 30, 31]. Financial talents, particularly as they relate to money laundering, are also advantageous [32]. Competency, however, appears to be the critical factor. For freelance or network members, roles may be specifically delineated – such as lawyers or dock workers – but for direct participants, their roles may be best understood in terms of rank – whether soldiers or generals – with tasks being variable across time and space [23, 32, 33]. Organised crime group participation thus distinguishes itself as following the logic of careers, with members reporting prolific crime-for-profit histories [27, 34, 35]. This longevity breeds group culture. When combined with the various rituals that often come with membership in these organisations, a strong sense of loyalty can develop, with many organised crime group members drawing their identity markers from their participation in the given group [13, 23, 33, 36, 37].

Organised crime structure varies [38]. Size can depend greatly on where one draws the lines of participation. In the case of Los Choneros, for instance, if one were to consider the entirety of their criminal network as a single group, membership could readily clear the thousands; but if one were to only consider the top-brass leadership as true members, we would be looking at a much smaller firm. It is perhaps for this reason that organised crime scholarship has shifted from once considering organised crime the sole province of large groups to favouring the idea that, in contrast, organised crime tends towards firms of varying sizes [13, 38, 39]. The manner in which these firms are organised is also variable: some appear to embody clearly hierarchical forms, while some have structures complicated by family ties, and others are decidedly more ad-hoc and informally collaborative [26, 28, 38–40]. Structure is ultimately highly dependent on the criminal context – how the landscape of criminal opportunity shifts and evolves across time – and the wider needs, capabilities, and dynamics of the given group – ethnic, cultural, economic, and social effects [13, 14, 39, 41]. Mounting police pressure, in any criminal environment, forces increased secrecy, and reduced risk-taking,

inhibiting the expansion of the given enterprise [41]. Yakuza tend to be larger, more hierarchical, and more complex in their structure than other mafia-style organisations, due to their semi-legal status, which has allowed them to flourish over time [42]. Thus, real-world control and enforcement practises directly serve to influence the structure of organised crime groups.

4. Comparison

On the surface, we can observe that there are a lot of similarities between cybercrime and organised crime. Both are criminal enterprises, and both involve, to a certain extent, new technologies. They are collaborative and may involve high profits. Different organisational models abound, but within firms, we can observe hierarchical management, amongst individuals, market dynamics, and within a broader field of collaboration, network effects. Cybercrime can thus be deemed organised crime; organised crime, if not cybercrime, then at least becoming rapidly more digitalised, bleeding slowly into the digital sphere. Yet, looking deeper, it quickly becomes clear that this comparison is complicated by substantive differences in the definition, profiles, *modus operandi*, and structure of organised crime and cybercrime groups.

Quite simply: cybercrime takes place online, organised crime, most often, in the real world. Though state and institution-published documents are replete with references to organised crime involvement in ransomware attacks, the provision of online sexual services, and participation in darknet markets, there is no robust academic support for such claims [15]. Of course, these institutions are not basing these claims on imagination, they are drawing such conclusions directly from their own data analysis, and communication with law enforcement [4]. This is why the questions of defining cybercrime and organised crime are so important. If national and international policing organisations consider groups participating in cybercrime to be organised crime groups, then such claims about their involvement in cybercrime become instantly well-supported and evidentially true; if, however, one begins from the definitional standpoint that organised crime proper can only be understood through the lens of governance, then such claims suddenly become inaccurate, even bizarre. There is no known evidence that Mafia-type organisations or trafficking-type organised crime groups are participating in cybercriminal activity; nor would there be any reason to assume they would be.

As we have seen, cybercrime requires a different profile than that of organised crime. With significant variation across age, gender, ethnicity, and sociodemographic details, cybercriminals collaborate to commit crimes in an online sphere [1, 10]. This stands in contrast to the homogeneous nature of organised crime groups, which tend towards disadvantaged men from a single ethnic background, collaborating to commit crimes in the physical world [14, 23, 25]. This does not mean that some dynamics are not paralleled. Actors in both cybercrime and organised crime require trust-through-reputation to succeed [10, 13]. Yet this manifests in very different ways across respective criminal spheres. Cybercriminals operate anonymously, and as such must develop the reputation of their online identities, rather than themselves – such as through reviews, forum discussions, and criminality proofs [1, 10, 11]. Organised crime often involves a kind of corporate-style ascent, based on proven capacity to complete tasks and dedication to the organisation [43]. The latter, being in person, is far more high-stakes, where mistakes, divided

loyalties, or arrest could prove life-threatening. It is also more emotional – family ties, cultural connections, status, and group politics all play a role in the ascent to power [26, 28, 30]. Perhaps for this reason, cybercriminal profiles have managed to include husband-and-wife teams, people with high-level qualifications, and the elderly – the assessment of the given enterprises' reputation being based solely upon the quality of their criminal performance, rather than any apparent demographic kinship [1, 11]. Profiles of victims also differ. The victims of cybercrime are typically companies or the state, there is no violence involved, high levels of education or expertise are often required, and profiteering, while significant, is not necessarily dramatic [10, 11]. While in organised crime, victims range from companies, and the state, to individuals – violence, exploitation, and corruption being direct influences of organised crime within a given area. We feel the presence of organised crime, their influence is corrosive for those proximate to it. Cybercrime, in sharp contrast, is largely invisible. Ecuador has been ravaged by Los Choneros; few people likely know or care about Scattered Spider's existence.

Different profiles follow from different *modus operandi*. While there is complexity in both forms, it is a different kind of complexity. To sell drugs on the darknet, vendors must gather resources (computers, drugs, shipping materials, etc.), set-up software (encryption software, cryptocurrency, etc.), conduct sales (advertising, branding, etc.), ship products (packing, dropping off, etc.), launder proceeds (tumbling and converting cryptocurrency), and manage their operation (working with employees; ensuring a high level of operational security across various horizons) [44, 45]. The investment of time and resources to become a darknet drug vendor is significant, and it generally requires a broad set of operative roles and expertise – the firm that sells the drugs is a one-stop-shop, often even producing the drugs themselves [44]. For organised crime, however, drug trafficking is far from a closed loop, it involves multiple organisations of different sizes, and with different roles, participating in the production, manufacture, processing, shipping, and wholesaling of narcotics [46]. Rather than performing each role in the chain, organisations will often simply perform one major role (e.g., shipping), with members of that organisation taking on relevant tasks (e.g., bribing customs officials) to achieve that aim. In this sense, organised crime groups may be less variable in terms of their overall function, but they may nonetheless end up covering a broad array of fluctuating tasks, as they become subject to political considerations, law enforcement pressure, internal disputes, theft, betrayal, and violence, factors that – due to anonymity and distance effects – are rarely as relevant for darknet drug vendors. Even aside from scale (the millions made by some darknet drug vending operations do not compare to the vast profiteering of international drug cartels), the digital and physical domains are truly distinct, made so by virtue of the particularity of those domains.

Cybercriminals do not manage a route, control a market, or govern a territory. Borrowing from the logic of Reuter (1983), cybercriminals are instead more like individual entrepreneurs or the managers of small criminal firms [42]. Take prostitution, for instance. Though the degree, manner, and expression of organised crime influence in the market for the provision of sexual services has long been a matter of debate, some scholars are of the opinion that, at the very least, organised crime is responsible for the trafficking of young women for the purposes of sexual exploitation [47]. In this case, the organised crime group in question would qualify their governance through the management of the route in which women are trafficked. Arguments could also be made for the involvement of organised crime

groups in the management of the in-person sex market, through the mediation of brothel disputes and the arrangement of protection rackets [48]. And indeed, disputes arise, protection is required: it is well established that, in its present incarnation, in-person sex work subjects the women who practise it to potential harm [49, 50]. Now compare this with online sex work. While sexual services are still exchanged, and money is paid in kind, digital sex work does not present any apparent or necessary exposure to harm [2]. There is no evidence to-date that suggests a causal link between human trafficking and digital sex work, or organised crime and digital sex work. Unsurprisingly so. Unlike in in-person sex work, where organised crime has a plausible role in the provision of sex workers, the exploitation of the same, and the mediation of related markets; it is difficult to see what role organised crime groups could play in an environment where participants appear to engage in the given activities through their own volition. Substantially reduced danger means a lack of opportunity for protection and therefore control, and the markets in question are already mediated by legal companies, with participants being non-criminal and readily capable of availing themselves of standard civilian rights. There just isn't a place for organised crime in the same way; while the broadest strokes of the physical and the digital worlds align, the details of the finer strokes vary so greatly as to radically change enforcement, policy, and academic approaches to the same.

5. Analysis

At first glance, it may appear useful to broaden organised crime as a concept to encompass cybercrime. Organised crime denotes serious crime, crime that is organised, crime-for-profit, and, as such, cybercrime fits comfortably within its remit. But there are two critical issues here. The first is that organised crime is not a broad category of crime, but a narrow one. It is best defined by governance, not organisation [13, 14]. And, as such, fraud, theft, and other forms of criminality, simply because they are planned and executed by a group of two or more people for financial gain, do not qualify as organised crime. The second is that even if such a broad category were applied to organised crime, it would still be important to distinguish cybercrime as a distinct form of crime, as the necessary use of technologies to commit a given crime radically changes the what, how, and who of the crime carried out. Burglars and hackers require different skillsets, and approach the crime of theft in unique ways; the balance of risks and benefits for in-person drug traffickers and darknet drug vendors is very different [1, 11, 44, 45]. Arguments that seek to diminish the need for definition, or for flexibility in our understanding of these concepts, fail, perhaps, to recognise the issues posed by the unfortunate conflation of organised crime and cybercrime.

The term 'organised crime' holds a lot of weight [13, 15, 46]. It is drenched in history. Through the presentation of news cycles, political movements, music, films, television shows, historical popular records, and academic criminology, organised crime, as a concept, has been pressed deep into the public consciousness. In normative terms, when someone says, 'organised crime' everyone understands what they are talking about, everyone immediately conjures up images of *The Godfather*, Pablo Escobar, and the Yakuza. When policy makers use the term, they draw upon this telescopic series of associations; by referring to cybercrime as organised crime, they present cybercrime as an extension of this history, which it is not. This is the

logic of political correctness in reverse. We recognise that a particular term is loaded with decades of negative connotations, but rather than trying, as such, to replace it with a neutral term, we instead extend the use of this term even further, applying it to that which is not actually captured by its original meaning.

The reasons policy makers adopt this approach are obvious. By calling cybercrime organised crime, you immediately make the public understand it as serious and worthwhile. Arresting the creator of a given piece of ransomware technology sounds like a win, but it has nowhere near the sense of gravitas as arresting the head of an international organised cybercrime syndicate. Victim empathy is a related factor. Cybercriminals tend to target companies, or, by flaunting trade and taxation laws, the state. Short of particular cybercrimes, like those related to paedophilia, and individual-level scams, most of the focus tends to be on exploiting (often foreign) companies. Of course, the public can be affected, their private information might be violated, or their financial assets stolen as part of this company-level targeting. But this does not evoke the same reaction as the violence and exploitation carried out by real-life organised crime groups, where innocent people routinely suffer extreme physical or emotional harm as a direct or indirect result of their criminal actions. Framing cybercrime as organised extends those sympathies to better justify the focus on tackling cyber criminality.

This conflation only produces short-term gains. While treating cybercrime as organised crime might make it more politically relevant, over time it risks eroding our understanding of these two major categories of crime. We all fall prey to our own games. By constantly framing individual entrepreneurs as the heads of organised crime syndicates, the individuals behind such framing start to believe it themselves, it becomes their reality. This could lead to ineffective investigative practises, as investigators expect that human-factor leads, given their framing of cybercriminal groups as a collective, may more readily lead to arrests than is actually the case. Not to mention the question of justice. By over-associating cybercrime with organised crime, we open individual cybercriminals up to increased avenues of prosecution, and harsher punishments. This does not show appropriate respect for the rights of accused persons: if cybercriminals are to be punished, then their punishments should be devised, designed, and applied with reference to cybercrime, not organised crime.

The solution? Go in the opposite direction. We, as academics, should be seeking to further compartmentalise organised crime, rather than expanding it. This does not refer to compartmentalisation along the lines of crime type, as is typically approved, but rather along particular theoretical lines. As we have seen, crime type and motivation are not reliable means of defining crime categories. Instead, we need to take a deeper, more complex approach, taking account of the various profiles, modus operandi, and structural dynamics that percolate around different forms of crime, and use them to formulate new theories around what is and what is not organised crime.

6. Conclusion

The primary difference between cybercrime and organised crime relies on a single, fundamental truth: that the change in criminal activity between the digital and physical spheres changes more than simply how the crime is conducted in the online sphere [11]. And while cybercrime might be organised, and organised crime might now avail of internet technologies, this does not make them organised crime

and cybercrime, respectively. Cybercrime, as a unique form of criminality, must be designated as such. Organised crime in the digital era is, in short, still simply, organised crime.

The resolution to the cybercrime definitional debate is not sufficient. Agreeing that cybercrime is not ‘old crimes in new bottles’ or ‘new crimes in old bottles’ but somewhere in between calls to an abrupt stop our otherwise vital explorations into better understanding this concept. Veering away from these Schrodinger’s cybercrime explanations, we should strive to embrace the more complex truth that cybercrime largely features iterations of well-established crimes, and that there are broad similarities with same, but that the finer details are often so radically different that we cannot respond, theoretically, empirically, or legally to these crimes as we would their physical-world correlates. As such, it is imperative that, broad similarities aside, they stand alone.

Organised crime, as a concept, should not be misused. When a theoretical construct is stretched over too wide a surface, it thins, becoming permeable, conveying nothing. To say that organised crime is all crime that is organised robs us of the opportunity to understand organised crime as a function of governance. It blurs the lines that we, as academics, strive to use to delineate trafficking cartels and mafia-type organisations. The term becomes meaningless. Efficiency of communication and organisation; money laundering. This appears to be the broad empirical limit of the impact of the digital world on organised crime operations. Though states, the media, and international bodies might make claims for organised crime’s involvement in the production of malware and ransomware attacks, it simply is not helpful, in the long term, to barter truth for political relevance.

Crime is as crime does. A darknet drug vendor who purchases wholesale cocaine from an organised crime group is part of their wider network; a mafioso who engages in a denial-of-service attack is a cybercriminal. We need to focus on the conduct of a given actor within a given organisational structure when determining the given crime type classification, not simply their motivation and opportunity context. Doing so should maintain our fidelity to academic crime classification – ensuring a better understanding of high-level, for-profit crime in both online and offline domains.

Author details

Thomas Joyce
Tilburg University, Tilburg, The Netherlands

*Address all correspondence to: t.p.joyce@tilburguniveristy.nl

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Joyce T. Situating high-level darknet drug vending: An emancipation from open and closed market dealing? *Trends in Organized Crime*. 2025. DOI: 10.1007/s12117-025-09560-w
- [2] Joyce T. Sweden, sex work, screens: The criminalisation of online sex work and article 8 of the ECHR. *Verfassungsblog*
- [3] Wall D. *Crime and the internet*. Routledge. 2001;3–7. DOI: 10.4324/9780203299180
- [4] Europol. *Serious and Organised Crime Threat Assessment Report*. Luxembourg: Publications Office of the European Union; 2025. DOI: 10.2813/0758057
- [5] Wall D. What are Cybercrimes? *Criminal Justice Matters*. 2004;**58**: 20–21
- [6] Capeller W. Not such a neat net: Some comments on virtual criminality. *Social and Legal Studies*. 2001; **10**(2):229–242
- [7] Grabosky P. Virtual criminality: Old wine in new bottles? *Social and Legal Studies*. 2001;**10**(2):243–249
- [8] Yar M. The novelty of cybercrime”: An assessment in light of routine activity theory. *European Journal of Criminology*. 2005;**2**(4):407–427
- [9] Wall D. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity; 2007
- [10] Lusthaus J. *Industry of Anonymity*. USA: Harvard University Press; 2021
- [11] Joyce T. Disorganized crime? Applying Reuter’s classic theory to darknet drug vending. *European Journal on Criminal Policy and Research*. 2025. DOI: 10.1007/s10610-025-09635-y
- [12] Reuter P. *Disorganized Crime: The Economics of the Visible Hand*. USA: MIT Press; 1983
- [13] Paoli L. The paradoxes of organized crime. *Crime, Law and Social Change*. 2002;**37**:51–97. DOI: 10.1023/A:1013355122531
- [14] Varese F. What Is Organised Crime? In: Carnevale S, Forlati S, Giolo O, editors. *Redefining Organised Crime: A Challenge for the European Union?* London: Hart Studies in European Criminal Law; 2017
- [15] Lavorgna A. Cyber-organised crime. A case of moral panic? *Trends in Organized Crime*. 2019;**22**:357–374. DOI: 10.1007/s12117-018-9342-y
- [16] United States Department of Justice. CR. NO. 2:24-CR-00595-JWH (2024)
- [17] Lusthaus J, Varese F. Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice*. 2021;**15**(1):4–14. DOI: 10.1093/police/pax042
- [18] Korshøj NT, Søgaard TF. Hybrid drug dealing: Merging on- and offline spheres when dealing drugs via social media. *International Journal of Drug Policy*. 2024;**130**:104509. DOI: 10.1016/j.drugpo.2024.104509
- [19] Moyle L, Childs A, Coomber R, Barratt MJ. #Drugsforsale: An exploration of the use of social media

- and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy*. 2019;**63**:101–110. DOI: 10.1016/j.drugpo.2018.08.005
- [20] Lusthaus J. Honour among (cyber) thieves? *European Journal of Sociology*. 2018;**59**(2):191–223. DOI: 10.1017/S0003975618000115
- [21] Lusthaus J, van Oss J, Amann P. The gozi group: A criminal firm in cyberspace? *European Journal of Criminology*. 2023;**20**(5):1701–1718
- [22] Caulkins JP, Schicker PC, Milward HB, Reuter P. A detailed study of a prominent dark web fentanyl trafficking organization. *Global Crime*. 2024;**25**(1):50–71. DOI: 10.1080/17440572.2023.2291352
- [23] Gambetta D. *The Sicilian Mafia*. USA: Harvard University Press; 1993
- [24] Finckenauer JO. Problems of definition: What is organized crime? *Trends in Organized Crime*. 2005;**8**:63–83. DOI: 10.1007/s12117-005-1038-4
- [25] Campana P, Varese F. Cooperation in criminal organizations: Kinship and violence as credible commitments. *Rationality and Society*. 2013;**25**(3):263–289. DOI: 10.1177/1043463113481202
- [26] Calderoni F, Campedelli GM, Comunale T, Marchesi ME, Savona EU. Recruitment into organised criminal groups: A systematic review. *Trends and Issues in Criminal Justice*. 2020. DOI: 10.52922/ti04183
- [27] Kirby S, Francis B, Humphreys L, Soothill K. Using the UK general offender database as a means to measure and analyse organized crime. *Policing: An International Journal of Police Strategies and Management*. 2016;**39**(1):78–94. DOI: 10.1108/PIJPSM-03-2015-0024
- [28] Spapens T, Moors H. Intergenerational transmission and organised crime: A study of seven families in the south of the Netherlands. *Trends in Organized Crime*. 2019. DOI: 10.1007/s12117-019-09363-w
- [29] Carvalho LS, Soares RR. Living on the edge: Youth entry, career and exit in drug-selling gangs. *Journal of Economic Behavior and Organization*. 2016;**121**:77–98. DOI: 10.1016/j.jebo.2015.10.018
- [30] Savona EU, Calderoni F, Campedelli GM, Comunale T, Ferrarini M, Meneghini C 2017. Recruitment into mafias: Criminal careers of mafia members and mafia bosses. D.1.1 Report on factors relating to OC. Milan: Università Cattolica del Sacro Cuore – Transcrime. https://www.researchgate.net/profile/France-sco-Calderoni/publication/333632781_Recruitment_into_Mafias_Criminal_Careers_of_Mafia_Members_and_Mafia_Bosses/links/5cf7e4eaa6fdc84750888b0/Recruitment-into-Mafias-Criminal-Careers-of-Mafia-Members-and-Mafia-Bosses.pdf
- [31] Jhi KY, Gerber J. Texan gangs in “Da Hood: The impact of actual and perceptual neighborhood qualities on gang membership. *Justice Policy Journal*. 2015;**12**. <https://www.cjcj.org/mobile/news/9924>
- [32] Decker SH, Chapman MT. *Drug Smugglers on Drug Smuggling: Lessons from the inside*. Philadelphia: Temple University Press; 2008
- [33] Sergi A. A qualitative reading of the ecological (dis)organisation of criminal associations: The case of the ‘Famiglia

- Basilischi' in Italy. Trends in Organized Crime. 2016;**19**(2):149–174. DOI: 10.1007/s12117-015-9254-z
- [34] Blokland A, van Hout L, van der Leest W, Soudijn M. Not your average biker: Criminal careers of members of Dutch outlaw motorcycle gangs. Trends in Organized Crime. 2019;**22**(1):10–33. DOI: 10.1007/s12117-017-9303-x
- [35] Campedelli GM, Calderoni F, Comunale T, Meneghini C. Life-course criminal trajectories of mafia members. Crime and Delinquency. 2019. DOI: 10.1177/0011128719860834
- [36] Densley JA. Street gang recruitment: Signaling, screening, and selection. Social Problems. 2012;**59**(3):301–321. DOI: 10.1525/sp.2012.59.3.301
- [37] Zhang S, Chin K-L. Enter the dragon: Inside Chinese human smuggling organizations. Criminology. 2002;**40**(4):737–768. DOI: 10.1111/j.1745-9125.2002.tb00972.x
- [38] Natarajan M, Zanella M, Yu C. Classifying the variety of drug trafficking organizations. Journal of Drug Issues. 2015;**45**(4):409–430
- [39] Morselli C. Inside Criminal Networks. New York: Springer; 2009
- [40] Eck JE, Gersh JH. Drug trafficking as a cottage industry. In: Natarajan M, Hough M, editors. Illegal Drug Markets: From Research to Prevention Policy. Monsey, NY: Criminal Justice Press; 2000. p. 241–272
- [41] Reuter P. Disorganized Crime: The Economics of the Visible Hand. USA: MIT Press; 1983
- [42] Varese F Mafia life: Love, death, and money at the heart of organized crime. 2017
- [43] Joyce T, Jofre M. The offline side of darknet drug vending. European Journal of Criminology. 2025. DOI: 10.1177/14773708251365077
- [44] Joyce T. Following the (DNM) bible? A crime script analysis of darknet drug vending. Crime, Law and Social Change. 2023;**80**:419–439
- [45] von Lampe K. Organized crime: Analysing illegal activities, criminal structures, and extra-legal governance. USA: Sage; 2016
- [46] Raymond JG. Not a Choice, Not a Job: Exposing the Myths about Prostitution and the Global Sex Trade. USA: Potomac Books; 2013
- [47] Weitzer R. Legalizing Prostitution: From Illicit Vice to Lawful Business. USA: NYU Press; 2011
- [48] Sanders T, O'Neill M, Pitcher J. Prostitution: Sex Work, Policy and Politics. London: SAGE; 2009
- [49] Joyce T. Criminalised Sex Work and the Violation of the Ultima Ratio Principle of Criminal Law. Tilburg: Tilburg University Press; 2025
- [50] United States Department of Justice. CR. NO. 25-CR-00114 (2025)

Chapter 5

Crime and Science Forensic

Fadila Ait Boughima

Abstract

This article explores the role of forensic investigations in the field of crime. Having a crucial impact on the conduct of trials and the administration of justice, forensic science has evolved from an auxiliary discipline into a central pillar of the modern criminal justice system. Forensic sciences have developed over the years, bringing a multidisciplinary approach that allows for the precise reconstruction of the chronology of events. They rely on the contributions of medical sciences and several laboratory techniques integrating new technologies, which optimize the collection of biological evidence while minimizing the risk of contamination. Furthermore, digital forensics has become indispensable today for processing hybrid evidence (physical and virtual). Finally, the article highlights the challenges and regulatory standards imposed by these advances, calling for an international standardization of protocols to guarantee the impartiality of judicial decisions in the face of the increasing complexity of criminal operating methods.

Keywords: criminology, forensic science, forensic medicine, forensics, expertise, scientific evidence

1. Introduction

Crime, a social phenomenon, is a highly variable concept whose definition depends on the values of each community. Classically, it encompasses a set of offenses commonly divided into crimes, misdemeanors, and contraventions covered by the penal code. While abortion is decriminalized in many Western countries, it remains a crime in the Kingdom of Morocco.

At the same time, ever since primitive society, man has always been concerned with rendering justice whenever a crime is committed, particularly against the human person in the form of cruelty to existence, which would break the link between the individual and the human race [1].

When it comes to scientific investigation, forensic science is playing an increasingly important role. There are a number of reasons for this: the increasingly limited role of confessions as evidence, the fragility of witness testimony, the development of adversarial principles, the resources offered by scientific progress, the media coverage of criminal cases, and the influence exerted on the public and legal practitioners by film and television productions devoted to criminal cases [2].

Criminologists work to identify the underlying causes of crime and propose prevention solutions based on social theory and empirical research. Forensic studies, on the other hand, are based on natural and applied sciences, and they provide empirical methods for detecting, analyzing, and interpreting physical and digital evidence [3].

Today, the joint collaboration between forensic science and criminal investigation is no longer in doubt, as scientific evidence is increasingly used in criminal cases. Forensic science not only establishes facts such as the cause and forensic form of death but is also increasingly involved in identifying the chronology and sequence of events. These operations are governed by legal texts, in particular the Code of Criminal Procedure, which codifies the procedures for administering evidence.

The aim of this article is to highlight the importance and contribution of forensic investigations in criminal investigations.

2. Criminology and forensic science: Main concepts

Criminology is a field of sociology that studies the nature, causes, and consequences of criminal behavior in a broader social context. It analyzes aberrant behavior from a variety of perspectives, including sociological, psychological, economic, and political, examining factors such as poverty, inequality, social disorganization, and peer influence. Its ultimate aim is to identify the causes of criminal acts or behavior and to propose effective measures to prevent them. The importance of criminology also lies in its relevance to the development of adaptive and responsive legal policies, which can serve as a basis for crime prevention, law enforcement, and the improvement of the criminal justice system. By integrating multidisciplinary contributions from law, sociology, psychology, anthropology, and cultural studies, criminology offers a more comprehensive perspective for understanding the dynamics of crime while proposing evidence-based strategies for creating sustainable social justice and community safety [3]. Criminology was developed primarily through the work of Cesare Lombroso (1835–1909), an Italian professor of forensic medicine at the University of Turin. Lombroso's research into the physical and psychological types of criminals led many to consider him the “father” of criminology. Shortly after the publication of Lombroso's work, the Austrian jurist and professor of criminology Hans Gross, the “grandfather” of forensic criminology, published his treatises on criminal investigation (1906) and criminal psychology (1911). Émile Durkheim added a sociological approach, stressing the importance of anomie and social integration in understanding deviance. Durkheim saw crime as a natural and necessary component of society, contributing to social progress by challenging norms. The twentieth century saw an evolution in criminological thinking. The Chicago School of the 1920s and 1930s pioneered ecological and sociological approaches to crime, emphasizing how urban context, poverty, and social disorganization influenced criminal behavior. In the mid-to-late twentieth century, psychological, feminist, critical, and postmodern theories entered the criminological discourse, expanding its disciplinary boundaries and fostering interdisciplinary collaboration [4, 5]. Approaches in criminology play an important role in formulating more effective

policies and practices to reduce crime rates and strengthen legal and social response mechanisms for perpetrators and victims. Through a variety of theories, criminology not only helps explain the causes and dynamics of crime from different perspectives, including structural, psychological, and cultural, but also provides a conceptual basis for designing more targeted prevention, law enforcement, and rehabilitation strategies [3].

Forensic science is the application of science to law. Used in criminal cases, it consists of searching for and examining material traces that can be used to establish a suspect's guilt at the scene of the crime or on the victim. These include traces of blood or bodily fluids, clothing and textiles, hair, footwear, and any tools used, etc. Forensic science also encompasses everything that contributes to the collection, preservation, and analysis of evidence, such as DNA identification [6].

Forensic science remains a very broad term (often abbreviated to criminalistics) in its broadest definition. On the other hand, forensic science and forensic medicine are terms commonly and differently used in different states to designate the branch of medicine that deals with the application of medical principles and knowledge to the purposes of law, both civil and criminal. Forensic medicine deals with the legal aspect of medical practice, focusing on the application of medical knowledge to the administration of justice. The human history of written forensic science goes back 6,000 years. Sumer, Babylon, and Egypt all contributed to the development of forensic medicine. Imhotep was probably the first true forensic expert. Hippocrates, the Greek physician, and Galen, the Roman physician, made considerable contributions. Little progress was made during the Middle Ages. Forensic science has come a long way since its documented beginnings in the eighth century. The combination of forensic approaches in the study of crime originated in England in the twelfth century. Among the earliest forensic procedures were the application of toxicology by Mathieu Orfila in the early nineteenth century and the Bertillon anthropometric system, created by Alphonse Bertillon at the end of the nineteenth century. Sir Francis Galton's work on fingerprint categorization and Karl Landsteiner's discovery of blood groups paved the way for identification-based forensic analysis. The twentieth century saw significant advances in ballistics, forensic pathology, and serology. However, the greatest leap forward came in the 1980s, when Sir Alec Jeffreys introduced DNA fingerprint analysis, transforming forensic science into an indispensable tool for criminal justice [3, 4].

The forensic sciences encompass several subdisciplines, such as forensic pathology, whose role is to determine the cause of death and its forensic form, or forensic biology, which analyzes DNA and establishes identities. Thanks to these specializations, the forensic sciences are able to integrate a variety of scientific techniques to provide forensic evidence that can be used in criminal investigations to prove that a crime has been committed or establish the key elements of an offense; establish the link between the suspect, the victim, and the crime scene; establish the identity of people linked to an offense; exonerate the innocent; corroborate a victim's testimony; and help establish the facts [5].

The rise of forensic science, or the scientific study of crime scene evidence, has bridged the gap between sociological inquiry and empirical research. The move toward a multidisciplinary approach based on the use of technology in the criminal justice system offers tremendous opportunities to improve the efficiency of the treatment of even the most innovative forms of crime. Indeed, the rise of digital forensics in the twenty-first century, tackling cybercrime, data breaches, and online

fraud, has enhanced the potential for cooperation between these disciplines. By recognizing the central position of the digital trace as an object of scientific interest, the development of research into its identification, exploitation, and interpretation offers the possibility of multiplying the sources of information that can testify to previous activities and contribute significantly to the development of knowledge in criminology, particularly in terms of a better understanding of offenders' schemes, evolutionary mechanisms, and intentions. What's more, it is increasingly common for courts to grant digital traces sufficient probative value to support their decisions. At the same time, these developments call for heightened vigilance in the face of a number of concomitant challenges, notably those relating to ethics, procedures, and the principle of equality. It remains imperative that the application of technology in criminal justice should always be accompanied by mechanisms for control, transparency, and critical evaluation, so that the innovations proposed are genuinely capable of creating meaningful advancements [7].

Finally, it should be remembered that the field of forensic science is not yet fully integrated worldwide. The multidisciplinary and interdisciplinary nature of forensic science requires an interprofessional approach, which is often lacking. There are many reasons for this restrictive or reluctant use of forensic science, including lack of technological development, misuse of physical evidence, failure to respect the chain of custody, late submission of physical evidence to the court, and sometimes failure to provide details of the evidence [5].

The intersection between criminology and forensic science is a key element in analyzing and solving criminal cases more effectively. By integrating these two fields, a more comprehensive and holistic approach is created, in which theoretical perspectives on human behavior can be combined with empirical evidence, resulting in an investigation process that is not only more accurate but also more scientifically and socially accountable [3].

3. The impact of forensics on criminal investigations

Expertise is a technical mission in which a competent authority calls on the advice of an expert to examine and resolve a highly specialized technical problem. The purpose of expertise is to clarify certain factual circumstances, revealing a particular skill (scientific, technical, or artistic). Forensic expertise has proven its importance and place in criminal investigations over the decades, as in the case of genetic expertise providing DNA evidence that led to the indictment of a sex offender, or an autopsy that determined the cause and circumstances of death in a homicide case. This work has highlighted the place and probative value of scientific evidence, defined by Locard as "a mode of administration of proof in criminal proceedings, consisting in the systematic analysis of traces left by the perpetrator or carried away by him on his body and clothing" [2, 8].

While the importance of forensic expertise is growing with new scientific and technical advances applied to the judicial system, it remains important to understand its limits in each case. Ultimately, forensic expertise considerably improves the investigative process by reconstructing the sequence of events that preceded, accompanied, and followed a crime, identifying the suspect through DNA profiling and fingerprint analysis, and contributing to the exoneration of wrongfully convicted offenders. Forensic expertise provides objective evidence that can

corroborate or refute testimonies and alibis, thus narrowing down the list of potential perpetrators. To be admissible in court, forensic evidence must withstand rigorous judicial scrutiny. This requires forensic experts to follow strict protocols and maintain high standards of accuracy and reliability in their analyses. The standard set by the US Supreme Court defines the criteria for the admissibility of expert testimony, ensuring the validity and scientific relevance of forensic evidence [8].

4. The main fields of forensic science

Forensic science encompasses a wide range of subdisciplines, each playing a unique role in the investigative process [5, 9]:

- **Forensic pathology:** a cross-disciplinary field and a veritable bridge between medicine and law. Forensic medicine has been instrumental in delivering justice in both criminal and civil cases, for both living and deceased victims. It is a ferment of evolution with certain related disciplines, notably forensic anatomic pathology, whose joint collaboration contributes to a more precise determination of the cause of death; the same applies to radiology and molecular biology.
- **Forensic anthropology:** is the application of physical examination to forensic cases, usually focusing on the human skeleton. Investigations usually begin with a corpse search team at the scene, using a variety of means. Anthropological expertise includes not only search and recovery but also determination of the nature of the evidence (bones or teeth), species identification, estimation of the time elapsed since death, sex, ancestry, age at death, stature of the living, taphonomic history, and recognition of any other characteristics that may contribute to the identification and detection of criminal acts. The scope of forensic anthropology has been extended to include questions relating to living persons, particularly in the field of identification and age determination.
- **Forensic odontology:** a branch of dentistry that examines dental elements for forensic purposes. It plays a key role in the identification of victims of mass disasters, crimes, and child abuse, among others. This examination is often based on dental elements such as restorations, missing teeth, and prostheses. Dental prosthetics, and in particular, denture identification systems, play an essential role in the postmortem identification of individuals.
- **Forensic entomology:** the study of insects and other arthropods in relation to legal issues, particularly in court, is particularly useful for estimating the post-mortem period and remains a fairly reliable method.
- **Toxicology:** the application of toxicology to the forensic investigation of death and poisoning. It encompasses the determination of alcohol, drugs, and other harmful substances in biological samples, and the interpretation of these results in a forensic context. The choice of appropriate samples depends on the application but always requires adequate documentation, transport, and storage to ensure the integrity of the substances to be analyzed. Knowledge of the effects

of drugs and their pharmacokinetics, as well as consideration of the possible limits to the interpretation of results, guarantees credible and not exaggerated evidence. It is based on the analysis of biological fluids, as well as certain tissues and phanera, such as hair. Indeed, human and animal hair has been used in forensic investigations for over a century and is one of the most common types of evidence. The identification and comparison of human and animal hair can prove useful in demonstrating physical contact with a suspect, victim, or crime scene.

- **DNA analysis:** one of the most important achievements in forensic science is DNA profiling. DNA analysis enables individuals to be identified on the basis of their unique genetic make-up. This technique is essential for linking suspects to crime scenes, identifying victims, and exonerating the innocent. The introduction of the Combined DNA Index System (CODIS) in the USA has further enhanced law enforcement's ability to match DNA samples from different cases.
- **Forensic psychiatry/psychology:** this is a medical discipline that studies the behavior and mental processes of criminals. It plays an important role in determining whether a person is criminally irresponsible and helps to understand the perpetrator of the crime, as well as the victim. Forensic psychology has grown considerably over the last 20 years. It is a vast applied field offering a wide range of opportunities for practitioners. Forensic psychologists work in many different legal environments, writing reports, giving evidence, providing direct care, or working with therapeutic communities.
- **Forensic engineering:** the application of engineering principles and techniques to the analysis of materials, products, structures, or components that are defective or not functioning as intended. Forensic engineering can include the analysis of the physical causes of accidents or other sources of claims and litigation.
- **Forgery analysis:** this includes the use of new technologies to analyze inks and papers, as well as the use of chemometrics to evaluate analytical data. Forensic graphology involves the comparison of handwriting samples by forensic document experts to determine whether they have been written by the same person. The comparison should ideally include original, freely and naturally written documents; comparable to the contested document in terms of format, style, characters, and character combinations; and provided in sufficient quantity and quality to be representative of the individual's handwriting range.
- **Fingerprints:** fingerprint analysis remains a cornerstone of forensic science, as each individual has unique fingerprints. Integrated automated fingerprint identification systems have streamlined the process of comparing fingerprints taken at the scene of a crime with those contained in a database, speeding up investigations considerably.
- **Ballistics:** examines firearms, ammunition, and their effects. This subdiscipline is crucial in cases of gun violence. Close collaboration between the forensic pathologist and the ballistics expert is imperative, as it enables the type of

weapon used to be determined, as well as the distance and impact of the shot, in order to rule on the forensic form of death. The search for gunshot residue, which generally comes out of the barrel in the form of a cone and may be deposited on the target, enables the firearms expert to assess how close the shooter was to the target at the time of firing, or, in other words, to determine the distance of the shot. This research can be carried out using sample kits taken from hands, clothing, etc.

- Digital forensics: with the rise of cybercrime, digital forensics has become increasingly important. This field involves the recovery and examination of data from electronic devices, such as computers, smartphones, and storage media. Computer forensics can reveal crucial evidence, including communications, financial transactions, and deleted files. Indeed, it is increasingly common for courts to grant digital traces sufficient probative value to support their decisions. Other branches of forensic science include forensic linguistics, forensic geology, forensic botany, forensic archeology and forensic podology. Forensic sciences also encompass more specialized fields, such as forensic accounting. Clearly, then, the application of forensic science varies from one country to another and depends essentially on the resources granted to develop it. In the end, forensic science is indispensable in the realm of crime investigation. Its scientific rigor and methodical approach not only aid in solving crimes but also uphold the principles of justice by ensuring that evidence presented in court is credible and scientifically valid. As technology advances, the role of forensic science will continue to expand, offering new tools and techniques to combat crime and support the judicial system. It is that piece without which the puzzle of a criminal investigation is incomplete. Without the application of forensic science, criminals can never be convicted unless an eyewitness is present. While detectives and law enforcement agencies are involved in the collection of evidence, be it physical or digital, it is forensic science that deals with the analysis of that evidence in order to establish facts admissible in the court of law.

5. Future prospects

Recent advances in digital forensics, AI-assisted surveillance, and forensic linguistics are profoundly reshaping traditional investigative paradigms. Digital forensics is no longer limited to hard disk analysis but now encompasses cloud storage, blockchain data, and encrypted communications, enabling investigators to trace digital footprints within complex cybercrime networks. AI and machine learning support facial recognition, behavior prediction, and pattern detection, dramatically improving the speed and scope of surveillance operations. Forensic linguistics, meanwhile, enables investigators to analyze written or spoken communications to determine authorship, intent, and threat level. Alongside these advances, criminologists are increasingly relying on Big Data, predictive analysis, and geographic mapping to anticipate criminal trends and develop targeted strategies. These tools, frequently used in conjunction with forensic databases, facilitate real-time policing and informed policy-making. The convergence of criminological knowledge and forensic precision improves law enforcement's ability to anticipate and respond to criminal behavior with greater efficiency and

accountability. Furthermore, the changing nature of crime necessitates a fresh focus on multidisciplinary education and training. Future practitioners must possess not only technical knowledge of forensic instruments and scientific techniques but also a critical grasp of legal frameworks, ethical norms, and socio-cultural contexts. Universities and criminal justice institutions must continue to create courses that reflect this convergence, producing professionals who are equally effective in the courtroom as they are in the laboratory or on the field. Moreover, the emphasis on multidisciplinary criminal justice training reflects this integrated mentality. Universities and law enforcement training schools now focus on cross-disciplinary training of students in both theoretical frameworks and scientific skills. This comprehensive training strategy ensures that practitioners are not only technically proficient but also ethically and legally competent. The fusion of criminology and forensic studies has become increasingly important in the fight against modern, technologically sophisticated crimes such as cybercrime, human trafficking, terrorist financing, and financial fraud. These crimes frequently cross jurisdictional boundaries and require a combination of sociological understanding, technological expertise, and legal clarity. As a result, the demand for collaborative training, ethical oversight, and legal reform is growing. These reforms must protect civil liberties while strengthening the rigor of investigations, ensuring that judicial procedures do not jeopardize human rights in the name of efficiency or national security [3, 7].

6. Conclusion

Forensic science is indispensable to criminal investigation. Its scientific rigor and methodical approach contribute not only to solving crimes but also to upholding the principles of justice by guaranteeing the credibility and scientific validity of evidence presented in court.

As technology advances, the role of forensic science will continue to expand, offering new tools and techniques to combat crime and support the justice system.

Challenges in forensic science include the need for constant technological advances, rigorous staff training, and strict ethical standards. The reliability of forensic evidence relies on the meticulous collection and processing of samples according to well-established, codified protocols, and on the expertise of forensic science technicians.

Acknowledgments

For my family, and for the editor who allowed me to participate in this work, I am very honored to be part of it.

Declaration to editor

I used the DeepL platform for the translation; no other tool was used for writing.

Author details

Fadila Ait Boughima

Faculty of Medicine and Pharmacy, Rabat, Morocco

*Address all correspondence to: ouaidef@gmail.com

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Jurovics Y. Crimes against humanity: Definition and context. *Les Cahiers de la Justice*. 2011;1(1):45–64. Éditions Dalloz. Available from: <https://droit.cairn.info/revue-les-cahiers-de-la-justice-2011-1-page-45?lang=fr>
- [2] Schuliar Y. Scientific investigations in criminal inquiries: The benefits of appointing a scientific coordinator. *Medicine/sciences*. 2011;27:214–219. Available from: https://ipubli.inserm.fr/bitstream/handle/10608/7521/MS_2011_02_214.html?sequence=7&isAllowed=y
- [3] Thakur M, Gupta CM. Criminology and forensic studies: An interdisciplinary nexus. *Law and Judicial Review*. 2025;01(2):79–89
- [4] Petherick WA, Turvey BE, Claire E. F. *Forensic Criminology*. Elsevier. 2010. Available from: https://booksite.elsevier.com/samplechapters/9780123750716/Sample_Chapters/01~Front_Matter.pdf
- [5] Manikantan B. Forensic criminology. *International Journal of Advance Research, Ideas and Innovations in Technology*. 2019;5(2):582. Available from: https://www.academia.edu/39029680/Forensic_Criminology
- [6] Krishnan S, Suyash KJ. Use and importance of forensic science in criminal justice administration. *Journal of Forensic Sciences and Criminal Investigations*. 2025;19(1):556004. DOI: 10.19080/JFSCI.2025.19.556004
- [7] Mousseau V, et al. Forensic science and criminology: Towards a diverse co-construction of knowledge on the phenomenon of crime and its regulation. *International Journal of Criminology and Forensic Science*. 2022;3(22):334–346. Available from: researchgate.net/publication/374165821_Science_forensique_et_criminologie_Vers_une_co-construction_diversifiee_des_savoirs_sur_le_phenomene_criminel_et_sa_regulation
- [8] Gheorghe B. Expertise in the criminal judicial process. *Technium Social Sciences Journal* February. 2024;54:216–233
- [9] Koul R, et al. Role of forensics in crime investigation-A review article. *International Journal of Research and Review* 2024;11:492–497

Chapter 6

Review of Medical Crimes from Unauthorized Applications to Malpractices

Melike Erbaş

Abstract

Malpractice is harm resulting from an illegal or wrongful act committed during the practice of a profession. When this harm occurs in a way that compromises a person's physical integrity, it is considered within the scope of clinical forensic medicine. When such harm occurs during medical procedures, it is called medical malpractice, which is also considered within the scope of clinical forensic medicine. Furthermore, illegal practices, often perceived as affordable and readily available but frequently carried out by unauthorized individuals, can also cause physical or psychological harm to individuals worldwide. In this chapter, it is aimed to review crimes in the medical field, from unauthorized practices to malpractice.

Keywords: malpractice, unauthorized application, crime, medicine, harm, botox injections

1. Introduction

1.1 Definition of the crime

When defining “crime” from the perspective of criminology, a scientific discipline, it is noted that there are some inconsistencies in practice and literature and that defining the word “crime” is quite difficult [1]. At this point, it is worth recalling McCabe's famous quote:

“In the whole lexicon of legal and criminological terms, there is no word more difficult to define than ‘crime!’” [2]

The difficulty in defining “crime” lies in the fact that what an individual considers or does not consider a “crime” is strongly influenced by factors such as their worldview, social environment, and religious beliefs [1, 3, 4].

When considered within the framework of universal legal literature in terms of protecting the common fundamental values of societies, “crime” can be defined as actions prohibited and punishable by laws established as written rules by public authorities [3]. For an act to be considered a crime, it must be clearly defined as such

by pre-existing written laws and regulations; it must also violate the general principles of justice and human rights, and the perpetrator must have committed the act intentionally and of their own free will [5–7].

1.2 Intent

According to the universal literature, making the outcome of an act (which is considered a crime) the primary goal is called “purposive intent” or “*dolus directus*” [8, 9]. In some cases, the act deemed a crime is not the direct target but rather a situation of “*dolus eventualis*,” where the possibility of the act occurring is known but neglected [5, 10].

1.3 Negligence

In universal legal literature, “negligence” is defined as a breach of the duty of care and diligence [10–12].

“Ordinary negligence” is defined as negligence committed without a standard level of care, despite the possibility of a harmful outcome, and without foreseeing the consequences. “Advertent negligence,” on the other hand, involves a situation where the person acts with the confidence that nothing will happen, even though they foresee the consequences. The difference between advertent negligence and inadvertent intent is that the person thinks, “It won’t happen anyway,” while with inadvertent negligence, the prevailing thought is, “Let it happen” [11, 12].

The purpose of defining these situations is to ensure that the penalties for each type of crime – whether committed intentionally or resulting in negligent harm – are determined separately within the legal system [10].

1.4 A simple example to help distinguish all definitions

To better illustrate this point, I would like to share an anecdote told by a respected elder of mine to make it more concrete:

Someone is waiting on a street corner. He has decided that, at two o’clock in the morning, he will confront another man passing by, empty all the bullets from his gun, and kill him. There is intent here.

Another man was cleaning his gun in the garden, but somehow the gun slipped from his hand. There was only one bullet in the chamber. The trigger got stuck, the gun fired, and it hit someone passing by on the road. The person died. Now, this man, as can be clearly seen from the perspective of thought, did not plan to kill the person he hit. His thoughts were on the gun at that moment; he was busy cleaning it. There was no intent. This man’s only share in the death of that person was carelessness and negligence. Ultimately, he caused the end of another life, but there was no intent – just negligence.

Someone’s foot gets caught in the railway tracks, and someone else saves the person by breaking their leg. Was the rescuer’s intention to deliberately break the leg to save the person? Could they have saved the person without breaking their leg?

The basis of the crime is intent. Although the first two examples given within the legal system resulted in death, the punishments will not be the same, depending on the presence or absence of intent, or the degree of intent in cases of gross negligence. In fact, while the person in the first example is clearly considered to have committed a crime, what the person in the second example did is not a direct crime. So, how

should the third example be evaluated? Should this person be rewarded or punished? Is it always possible to assess the degree of intent based on the available evidence?

However, while acts deemed to be crimes based on available evidence and demonstrable intent are considered criminal cases, civil law matters are handled as civil cases. Ninety-five percent of medical malpractice cases are actually “civil law matters”; they are not “crimes.” So, what are the crimes in the medical field?

2. Medical crimes

If we look at the field of medical practice from the framework we described earlier, what are the points that must be considered in order for something in the field of medicine to be considered a crime?

2.1 What is medical intervention?

Medical intervention is the application of any procedure accepted as standard current medical practice for the purpose of treatment, preservation of physical, physiological, and psychological integrity, or for other medical purposes [13–15].

Medical interventions must be performed by authorized persons in order to avoid endangering the bodily integrity of the person.

2.2 Who can perform medical procedures?

While physicians are primarily responsible for medical interventions, other healthcare professionals may also perform medical interventions under the supervision of a physician or within the limits of their authority [16, 17].

2.3 What is a medical crime?

For a medical intervention to be legally acceptable, it must be performed by physicians, dentists, midwives, healthcare professionals, nurses, circumcisers, dental prosthetic technicians, and emergency medical technicians within the scope of the authority granted by their diplomas and licenses [18, 19].

Malpractice is damage resulting from an illegal or wrongful act committed during the performance of a profession. When such damage occurs during medical procedures, it is called medical malpractice. Most cases of medical malpractice are considered within the framework of the concept of negligence described earlier [20].

Under the law, unauthorized medical procedures are considered a direct crime. In addition to unauthorized procedures, acts committed intentionally or through gross negligence, such as performing surgery under the influence of drugs, deliberately injecting high doses of medication, engaging in organ trafficking, using medical science for torture, and committing malicious data breaches in violation of confidentiality obligations, are considered medical crimes [5, 21–23].

2.3.1 Unauthorized applications

It is known that, in many parts of the world, including our country, individuals without valid medical training sometimes perform practices that can be defined as

medical interventions, and this is considered a crime under the law and is defined as unauthorized procedures [5, 23].

These individuals are seen prescribing medications and making treatment recommendations. These practices are referred to in the literature as unauthorized medicine, informal health services, unqualified medicine, and allopathic medicine. Recently, they have become quite widespread due to their relatively low cost and easy accessibility, resulting in many physical and psychological harms [24–26].

Procedures that cause serious physical and psychological harm as a result of medical interventions performed by unauthorized individuals include laser hair removal, tattoo removal, Botox, Dermapen, cryolipolysis, bone correction procedures, tooth extraction/prosthetics, intramuscular injections, and cupping therapy. A study showed that 87.1% of these procedures are performed in beauty salons, but they can also be performed in places such as hairdressers, homes, medical supply stores, pharmacies, and dental clinics [27].

3. Medical malpractice

Malpractice is harm resulting from an illegal or wrongful act committed during the performance of a profession. When such harm occurs during medical procedures, it is called medical malpractice. Most cases of medical malpractice are handled within the legal framework described earlier; however, although rare, there may also be cases of medical malpractice that fall under the category of crime [20, 21].

To understand the concept of malpractice, it is first necessary to clarify the concept of complication.

3.1 The concept of complication and its legal nature

A complication is an undesirable adverse event that may occur during or after a medical procedure, despite adherence to all rules and standards of medical science (the highest duty of care), due to the patient's individual characteristics or the nature of the procedure [17].

Medical interventions, by their very nature, involve various risks. The legal system, considering the societal benefit of medical science, grants physicians the authority to take these risks within certain limits; this is explained in legal literature as the concept of “permitted risk” [16]. Complications arising within this framework differ fundamentally from medical malpractice. The most prominent characteristics of a complication are that it is “predictable” because the situation is defined in medical literature and that the outcome is “unavoidable” despite the physician exercising all the necessary care and attention required by medical science [21]. Current studies emphasize that these boundaries become blurred, especially in interventions performed by unauthorized individuals, and that harmful outcomes, from a forensic medicine perspective, cannot be considered complications [27].

3.2 Liability in medical intervention: Distinction between complication and malpractice

Medical interventions are protected by the legal system within the framework of the concept of “permitted risk” due to the risks they inherently contain; however, for

an outcome to be considered a “complication not requiring compensation,” certain conditions must be met cumulatively [16]. First, it is essential that the physician has obtained “informed consent” from the patient by explaining the possible risks before the intervention, because if a foreseeable risk is not communicated to the patient in the medical literature, this directly gives rise to legal liability [21]. Second, there should be no technical defects in the process of performing the intervention, and the application should fully comply with current medical standards (*lege artis*). Finally, after the risk occurs, the physician must quickly recognize the situation and demonstrate “complication management” in accordance with the standards. Delayed risk detection or inadequate crisis management transforms the situation into medical malpractice. Therefore, it is not sufficient for the outcome to be foreseeable; deficiencies in the management of the process form the basis of criminal and legal responsibility [15].

4. An example to evaluate the issue from a forensic medical perspective: Botox injections

Botox injections are medical procedures that should only be performed by authorized personnel. However, since they are performed with just a syringe and botulinum toxin (BoNT), they are also performed outside of hospitals. This medical procedure can be performed by authorized individuals in out-of-hospital settings. However, this situation is often misused by unauthorized individuals [27].

We have chosen to examine the example of Botox injections to help us understand whether it constitutes a “complication,” a “medical malpractice” case that warrants legal considerations, or a “crime.”

Similar situations may arise with other aesthetic or medical procedures. Unauthorized individuals posing as doctors may perform these procedures, and even if the person performing them is a doctor, the unwanted outcome must be evaluated in terms of complications or medical malpractice.

Botulinum toxin was first approved by the Food and Drug Administration (FDA) in 1989 for the treatment of neurological disorders such as blepharospasm and hemifacial spasm [28]. Over time, its medical use has expanded to include various indications such as migraines, hyperhidrosis, bladder dysfunction, and muscle spasms; its widespread use in aesthetic applications has also led to an increase in off-label applications. Due to its ease of application, accessibility, and reversible effects, BoNT has become a very common treatment in aesthetics [29].

These injections are the most commonly performed cosmetic procedure worldwide, with approximately 3 million injections per year, and they are effective for many clinical disorders involving involuntary muscle activity or increased muscle tone [30, 31]. However, this widespread use has also brought with it claims of medical negligence or unauthorized application and resulting harm, particularly due to factors such as off-label use (using the drug outside of its stated indications) and insufficient practitioner experience [32, 33].

At this point, it is necessary to clarify the issue of off-label practices. In medical law, “off-label” use refers to the use of a drug or medical device outside the information in its approved package insert – for a different disease (indication), a different dosage/age group, or through a different application method. Although this is common in medical practice, it is a factor that increases the legal responsibility

of the physician. This is because the physician's obligation to obtain "informed consent" is much broader in off-label use; the patient must be clearly informed that this use is nonstandard and of its potential risks [21].

In medical law, off-label use is not prohibited, but it does increase the physician's responsibility. A physician may resort to this method when standard treatment is insufficient, based on current scientific data and prioritizing the patient's best interests.

From a legal perspective, these practices are considered an area where the physician pushes the boundaries of "permitted risk"; therefore, in the event of harm, the medical necessity and scientific basis of the intervention are subject to much stricter scrutiny [16]. The fact that some BoNT applications, especially those used in the cosmetic field, are off-label, necessitates a meticulous examination of potential side effects and complication management within the framework of "standard practice" in forensic medicine reports.

The use of BoNT for various aesthetic indications remains the most frequently performed nonsurgical aesthetic procedure worldwide. As more and more people from diverse specialties and varying levels of experience begin injecting the toxin, an increase in complications associated with toxin use is inevitable [34].

In addition to expected but undesirable side effects, such as complications, anatomical variations, incorrect injection techniques, and the spread of toxin to adjacent muscles, can contribute to the development of adverse events. This unpredictability complicates forensic medical assessment, as it can make it difficult to prove the practitioner's negligence or fault in causing the complication. However, these situations are easier to prevent from the outset. Careful administration of BoNT-A and adherence to established injection guidelines are necessary. Any deviation from these practices may potentially lead to malpractice claims [35].

In recent years, there has been an increase in the number of applications to the field of forensic medicine due to reasons such as systemic side effects developing after application, permanent neurological findings, or procedures performed without sufficient information being given to the patient [32, 33].

However, it is reported that there are also shortcomings in the legal approach to this issue, as well as problems such as the lack of adequate injection administration guidelines together with off – label usage. Besides the question of whether it constitutes malpractice, the presence of unauthorized procedures further complicates the matter. It should be noted that if adverse outcomes are caused by medical malpractice or by unauthorized persons, a forensic medical expert should prepare a report on the harm suffered [27, 35].

For a medico-legal report to be prepared, it must be clearly established whether the situation constitutes a crime (unauthorized action) or malpractice. It would not be appropriate to prepare a medico-legal report for a situation considered a complication; therefore, medico-legal experts must also possess a basic level of knowledge in these matters in the context of clinical forensic medicine.

In this context, multidisciplinary evaluation is of great importance to better understand the complications that may arise during BoNT applications and their legal consequences [36, 37].

When faced with such a case, before preparing a medico-legal report, it is necessary to investigate the answers to certain questions regarding the harm caused. If a report is prepared on the harm caused without such investigation, it means that the procedure has been unfairly and directly considered a "crime" or "medical

malpractice.” Therefore, when faced with such a case, the following questions should be asked before preparing a forensic report on the harm:

- Did the person performing the procedure identify themselves as a doctor?
- Was the person performing the procedure actually a doctor?
- Was the identity of the person performing the procedure clearly stated?
- If the person performing the procedure is authorized, is there an informed consent form that details the potential side effects and adverse events and states that the person understands and accepts them?
- Was the medication used sourced from a reliable source?

Although aesthetic procedures are gaining popularity worldwide, the fact that these interventions are fundamentally medical procedures should not be overlooked. When determining the legal nature of any undesirable outcomes, it is crucial to meticulously distinguish whether the situation constitutes an unavoidable complication or medical malpractice.

This process should involve a comprehensive review not only of the procedural technique but also of the appropriateness of the procedure, the content of the toxin used, and the legality of the toxin within the supply chain (use of approved/licensed products).

All these factors should be evaluated by multidisciplinary, high-level boards encompassing clinical branches and forensic medicine specialists. Only through such an approach can both patient safety be protected and the limits of the physician’s legal responsibility be fairly determined.

4.1 Checklist for clinical forensic medicine practices before preparing a medical report for such cases

- Is medical malpractice involved?
- Is there an unauthorized action?
- Is it an unwanted side effect?
- Is there an off-label application?
- Is there an inappropriate procedure or the use of an inappropriate toxin?
- Is there a problem with the supply and distribution of the toxin? (Was an unapproved, illegal toxin used?)

Therefore, before preparing a forensic medical report regarding the resulting harm, it is crucial to determine, through a multidisciplinary approach, whether the issue is due to malpractice, complications, or drug-related damage, and whether this has been clarified by the competent authorities. All these factors

should be evaluated by multidisciplinary, high-level committees, preferably including forensic medical assessments. Only if the matter has been fully clarified through sufficient investigations conducted by the relevant prosecutor's office and court, and it constitutes a crime, will the preparation of the report be appropriate.

It should be considered that this procedure, which is becoming increasingly popular for aesthetic purposes, is inherently a medical procedure.

4.2 Recommendations for current practices

- As with all other medical procedures, records must be kept, especially for out-of-hospital applications.
- Undesirable events and side effects must be reported.
- Due to the rapid increase in the popularity of these procedures in recent years, a mandatory reporting system is also recommended in the literature.
- Another important point is that the distribution and supply of the toxin used must be meticulously controlled, and the necessary legal regulations must be brought to the agenda worldwide.
- It should be considered that, even if the person performing the procedure is authorized, undesirable effects may occur due to a toxin that has been illegally introduced to the market, regardless of professional care and experience.

5. Conclusion

The basis of the crime is intent. The punishments will not be the same, depending on the presence or absence of intent, or the degree of intent in cases of gross negligence. When considering this assessment in terms of preparing a forensic medical report regarding harm occurring during medical procedures, preparing a report on the harm implies that we directly consider the existing practice causing the harm as a crime. Therefore, a forensic medical expert must have a basic knowledge of complications, malpractice, and crimes in the medical field and be able to assist the judiciary by providing sufficient information when necessary.

Thanks

I am grateful to my elders, who guided me and instilled the concepts of justice and righteousness, causing them to hold an important place in my life. I also extend my heartfelt thanks to my dear daughter, son, and close friends for their great help in fulfilling my responsibilities at home and at work during the writing of this chapter and all my studies.

Author details

Melike Erbaş
Bakırköy Directorate of Forensic Medicine Institute, Istanbul, Türkiye

*Address all correspondence to: dr.melikeerbasm@gmail.com

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Morrison W. What is crime? Contrasting definitions and perspectives. In: Hale C, Hayward K, Wahidin A, Wincup E, editors. *Criminology*. 3rd ed. Oxford: Oxford University Press; 2013. p. 3–23. DOI: 10.1093/he/9780199691296.001.0001
- [2] McCabe S. Crime. In: Walsh D, Poole A, editors. *A Dictionary of Criminology*. London: Routledge and Kegan Paul; 1983. p. 49–52
- [3] Beccaria C. On Crimes and Punishments and Other Writings. Toronto: University of Toronto Press; 2009
- [4] Lamond G. What is a Crime? *Oxford Journal of Legal Studies*. 2007;27(4):609–632. DOI: 10.1093/ojls/gqm018
- [5] International Criminal Court. Rome Statute of the International Criminal Court [Internet]. 1998. Available from: [https://legal.un.org/icc/statute/english/rome_statute\(e\).pdf](https://legal.un.org/icc/statute/english/rome_statute(e).pdf) [Accessed: 2026-January-31]
- [6] Dönmezer S, Erman S. *Nazari Ve Tatbiki Ceza Hukuku Genel Kısım Cilt II*. 12 ed. İstanbul: Beta Yayınları; 1999
- [7] Göktürk N. Suçun Yasal Tanımında Yer Alan “Hukuka Aykırılık” İfadesinin İcra Ettiği Fonksiyon. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*. 2016;7(1):407–450
- [8] Artuk ME, Gökçen A. *Ceza Hukuku Genel Hükümler*. 17 ed. Ankara: Adalet Yayınevi; 2024
- [9] Fletcher GP. *Rethinking Criminal Law*. Oxford: Oxford University Press; 1996
- [10] Türk Ceza Kanunu [Internet]. 2004. Available from: <https://www.resmigazete.gov.tr> [Accessed: 2026-February-01]
- [11] Blyth v Birmingham Waterworks Co [Internet]. 1856. Available from: <https://www.casemine.com/judgement/uk/5a8ff8ca60d03e7f57ec1060> [Accessed: 2026-February-01]
- [12] Koca M, Üzülmüş İ. *Türk Ceza Hukuku Genel Hükümler*. 16 ed. Ankara: Seçkin Yayıncılık; 2023
- [13] Dizdar E. Yetkisiz hekimlik suçu (1219 Sayılı Kanun m. 25). *Türkiye Adalet Akademisi Dergisi*. 2019; 38:295–314
- [14] Hızal A. Hatalı tıbbi müdahalelerden kaynaklanan tam yargı davaları [thesis]. İzmir: İzmir Üniversitesi Sosyal Bilimler Enstitüsü; 2015
- [15] Çakmut ÖY. Tıbbî müdahaleye rızanın ceza hukuku açısından değerlendirilmesi. *Legal Hukuk Dergisi*. 2002;1:26–41
- [16] Gökcan HT. *Tıbbi Müdahaleden Doğan Hukuki Ve Cezai Sorumluluk*. 2 ed. Ankara: Seçkin Yayıncılık; 2014
- [17] Caymaz M. Sağlık personelinin tıbbi uygulama hataları üzerine bir araştırma. *Uluslararası Yönetim Ve Sosyal Araştırmalar Dergisi*. 2015;2:1–14
- [18] 1219 sayılı Tababet ve Şuabatı San’atlarının Tarz-ı İcrasına Dair Kanun [Internet]. 1928. Available from: <https://www.mevzuat.gov.tr/mevzuatmetin/1.3.1219.pdf> [Accessed: 2026-February-01]

- [19] Ambulans ve Acil Bakım Teknikerleri ile Acil Tıp Teknisyenlerinin Çalışma Usul ve Esaslarına Dair Tebliğ [Internet]. 2009. Available from: <https://www.resmigazete.gov.tr/eskiler/2009/03/20090326-4.htm> [Accessed: 2026-February-01]
- [20] Kennedy I, Grubb A. Principles of Medical Law. 2nd ed. Oxford, United Kingdom: Oxford University Press; 2000. DOI: 10.1017/S0008197300083306
- [21] Hakeri H. Tıp Hukuku. 11 ed. Ankara: Seçkin Yayıncılık; 2016. p. 171
- [22] World Medical Association. WMA Declaration of Geneva: The physician's pledge. Journal of the American Medical Association. 2017;**318**(20):1971–1972. DOI: 10.1001/jama.2017.16230
- [23] European Court of Human Rights. European Convention on Human Rights [Internet]. 1950. Available from: https://www.echr.coe.int/documents/d/echr/convention_ENG [Accessed: 2026-February-01]
- [24] Das J, Chowdhury A, Hussam R, Banerjee AV. The impact of training informal health care providers in India: A randomized controlled trial. Science. 2016;**354**(6308):aaf7384. DOI: 10.1126/science.aaf7384
- [25] Gautham M, Spicer N, Chatterjee S, Goodman C. What are the challenges for antibiotic stewardship at the community level? An analysis of the drivers of antibiotic provision by informal healthcare providers in rural India. Social Science and Medicine. 2021;**275**:113813. DOI: 10.1016/j.socscimed.2021.113813
- [26] Chandra S, Bhattacharya S. Their illegal but indispensable role in primary healthcare unqualified medical practitioners. Economic and Political Weekly. 2019;**54**:36–44
- [27] Vural T, Erbaş M, Balcı Y, Baysal İ. Evaluation of forensic medical aspects of medical interventions and damages caused by unauthorized persons. Legal Medicine (Tokyo). 2024;**69**:102450. DOI: 10.1016/j.legalmed.2024.102450
- [28] Jabbari B. Botulinum Toxin Treatment in Neurology. Seminars in Neurology. 2016;**36**(1):3–4. DOI: 10.1055/s-0036-1571849
- [29] Naumann M, Jankovic J. Safety of botulinum toxin type A: A systematic review and meta-analysis. Current Medical Research and Opinion. 2004;**20**(7):981–990
- [30] Yiannakopoulou E. Serious and long-term adverse events associated with the therapeutic and cosmetic use of botulinum toxin. Pharmacology. 2015;**95**:65–69. DOI: 10.1159/000370245
- [31] International Society of Aesthetic Plastic Surgery (ISAPS) [Internet]. 2021. Available from: <https://www.isaps.org/discover/about-isaps/global-statistics/reports-and-press-releases/global-survey-2021-full-report-and-press-releases/> [Accessed: 2026-February-01]
- [32] Di Santis EP, Hirata SH, Di Santis GM, Yarak S. Adverse effects of the aesthetic use of botulinum toxin and dermal fillers on the face: a narrative review. Anais Brasileiros de Dermatologia. 2025;**100**(1):87–103. DOI: 10.1016/j.abd.2024.04.007
- [33] Viana FFR, Frezarin PA, Neves AVO, Pereira RF, Tessarin GWL. Botulinum Toxin In Aesthetic Medicine: Current Overview And Safety Challenges. IOSR Journal of Dental and

Medical Sciences (IOSR-JDMS).
2025;24(4 Ser. 5):22–26. DOI: 10.9790/
0853-2404052226

[34] Sethi N, Singh S, DeBoulle K, Rahman E. A review of complications due to the use of botulinum toxin A for cosmetic indications. *Aesthetic Plastic Surgery*. 2021;45(3):1210–1220. DOI: 10.1007/s00266-020-01983-w. (Erratum in: *Aesthetic Plastic Surgery*. 2022;46(1):595)

[35] Nittari G, Savva D, Gibelli F, Vulcanescu D, De Leo D, Ricci G. Anatomy, etiology, management, and medico-legal implications of botulinum-induced blepharoptosis. *Current Reviews in Clinical and Experimental Pharmacology*. 2025; 20(1):32–37. DOI: 10.2174/0127724328310459240809073519

[36] Petition for Writ of Certiorari. *Allergan, Inc. v. Sharla Helton*, No. 108,538 (Okla. Sup. Ct. Jan. 30, 2014). Available from: <https://www.uschamber.com/assets/documents/Petition20for20Cert.-20Helton20v.20Allegran2028Oklahoma20Supreme20Court29.pdf> [Accessed: 2026-March-18]

[37] Health Care Complaints Commission (HCCC). Prohibition Order: Ms Norsafiza Binti Zakaria-Cosmetic Injectables [Internet]. Available from: <https://www.hccc.nsw.gov.au/decisions-orders/prohibition-orders/ms-norsafiza-binti-zakaria-cosmetic-injectables> [Accessed: 2026-February-01]

Forensic Characterization of Bagged Bodies: A Four-Year Review from Medellín, Colombia

Jennifer Garcia Ospina

Abstract

This chapter presents a detailed forensic and criminological analysis of homicides involving body concealment in plastic bags (bagged bodies) in Medellín, Colombia. The primary scope is transition from raw forensic data to an integrated understanding of this specific, evolving pattern of urban violence between 2020 and 2023. The forensic scope encompasses analyzing the frequency, victim demographics (predominantly young adults), and the specific mechanisms of death and trauma. We examine common injury patterns, such as mixed asphyxia, torture (overkill), and sharp-force trauma, alongside the evidentiary value of wrapping materials, focusing on successful latent fingerprint recovery. The criminological scope goes beyond the autopsy table, interpreting these findings within the context of organized crime groups (GDOs) operating in the city. We analyze the use of concealment and dismemberment not merely to hide the victim but as a form of symbolic communication and territorial control. This method serves as a brutal warning and a display of extrajudicial social control. The chapter concludes by outlining critical recommendations for the criminal justice system, advocating for standardized protocols and multidisciplinary training to enhance investigations, victim identification, and ultimately, to strengthen the justice response to this complex form of targeted violence.

Keywords: bagged bodies, forensic investigation, homicide, organized crime, social control, Medellín

1. Introduction

Homicides involving body concealment in plastic bags represent a growing forensic challenge in Latin America. These cases often reflect organized crime dynamics, intimidation strategies, and attempts to hinder identification and evidence recovery [1, 2].

In recent years, the recovery of “bagged bodies” has emerged as a persistent and unsettling trend across various Colombian cities [1]. Far from being mere statistics, these findings expose complex patterns of violence, concealment, and torture that necessitate a comprehensive, multidisciplinary forensic approach.

The forensic examination of these cases varies significantly in terms of trauma type, decomposition status, and overall complexity. Scenarios range from straightforward cases involving a single sharp force or firearm injury – where bagging serves primarily for disposal and concealment – to highly complex presentations involving decomposed, charred, or dismembered remains. These latter cases often exhibit combined trauma mechanisms (asphyxia, sharp force, blunt force, gunshot wounds), where the bagging acts to conceal evidence, facilitate transport, or serve as an instrument of torture, presenting a significant challenge for forensic analysis.

This chapter will present a detailed forensic and criminological analysis of homicides involving body concealment in plastic bags (bagged bodies) in Medellín, Colombia. The primary scope is transition from raw forensic data to an integrated understanding of this specific, evolving pattern of urban violence between 2020 and 2023.

2. Materials and methods

A retrospective descriptive study was conducted on 67 cases of bagged bodies examined at the Basic Unit of Medellín (UBM) between January 2020 and December 2023. Data were extracted from official autopsy reports and photographic documentation. Variables analyzed included annual frequency, demographic profile (age, sex), associated elements (plastic bags, adhesive tape, ropes, blankets), injury patterns (defensive wounds, sharp-force trauma, asphyxia signs), and trace evidence (latent fingerprints on wrapping materials). Ethical compliance was ensured in accordance with Colombian legal standards and international forensic guidelines.

3. Results

During the years 2022–2023, 67 autopsies of bagged bodies were registered at the Medellín Basic Unit. Annual distribution: 2022 recorded the highest number of cases ($n = 27$; 40%), followed by 2020 ($n = 17$; 25%), 2023 ($n = 13$; 19%), and 2021 ($n = 10$; 15%) – see **Figure 1**. Age profile: Victims were predominantly young adults, with 41.7% aged 15–25 years and 34.3% aged 26–35 years (see **Figure 2**: age distribution of victims).

Males accounted for the majority of the sample ($n = 62$; 92.5%) versus females ($n = 5$; 7.5%). Asphyxia (strangulation, suffocation, or mixed) was the leading cause of death ($n = 38$; 56.7%). Other causes included firearm injuries ($n = 14$; 20.89%), sharp force trauma ($n = 13$; 19.4%), and craniocerebral trauma ($n = 2$; 2.98%). The manner of death was homicide in 100% of cases. Regarding preservation, 70.15% ($n = 47$) of the bodies were fresh, compared to 29.85% ($n = 20$) that were decomposed (**Table 1**).

The massive concentration of cases among males (92.5%) and within the 15–35 age range (76%) is not a statistical coincidence, but rather an indicator of the urban conflict's demographics in Medellín. This profile suggests that victims are primarily “operational links” or high-risk individuals within Organized Crime Group (GDO) structures. The victims' youth represents a significant loss of potential years of life and reflects a violent dynamic in which the young body is used as a canvas for power-driven messaging.

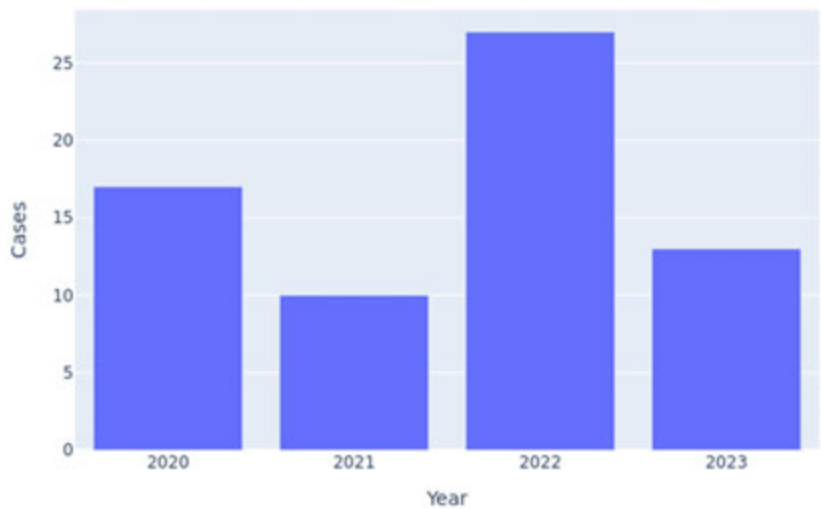


Figure 1.
Annual distribution of bagged body cases (2020–2023).

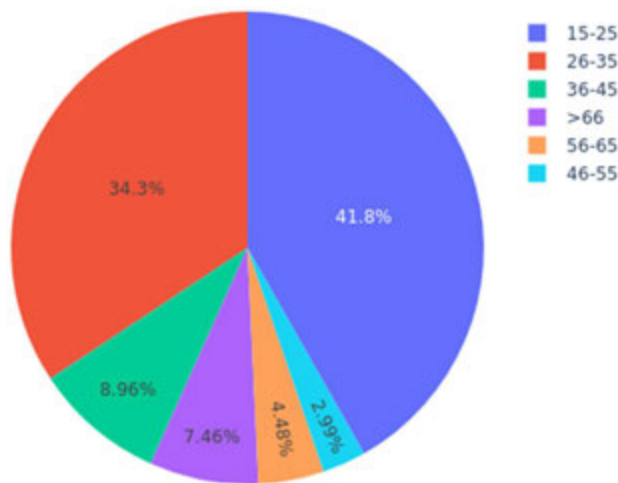


Figure 2.
Age distribution of victims.

From a pathological perspective, the fact that 100% of cases are homicides confirms that “bagging” is an exclusively criminal technique.

The predominance of fresh bodies (70.15%) compared to decomposed ones indicates that, despite the intent to conceal, discovery is typically rapid; this suggests bodies are abandoned in transit zones or “invisible borders” specifically to be found, serving a purpose of public terror rather than permanent disappearance.

In 29 cases (43.28%), other related traumas different from the cause of death were found. Blunt force polytrauma was the most frequent (21; 74.41%), followed by sharp force trauma (8; 27.5%) and the two previous combined (5; 17.24%) (**Table 2**).

Variable		n	%
Sex	Men	62	92.5
	Women	5	7.5
Cause of death	Asphyxia	38	56.7
	Firearm injuries	14	20.89
	Sharp force trauma	13	19.4
	Craniocerebral trauma	2	2.98
Manner of death	Homicide	67	100
Body preservation	Fresh body	20	29.85
	Decomposed body	47	70.15

Table 1.
Sociodemographic and forensic characteristics of bagged bodies autopsied in Medellín (2022–2023).

Variable		n	%
Other related traumas		29	43.28
	Blunt force polytrauma	21	72.41
	Sharp force trauma	8	27.5
	Blunt force polytrauma and sharp force trauma	5	17.24

Table 2.
Other related traumas.

The discovery of additional trauma in 43.28% of cases, predominantly blunt force polytrauma (72.41%), constitutes physical evidence of “overkill” or extreme cruelty. These traumas, which are often not the direct cause of death, suggest a phase of prior subjugation. In the context of Medellín, this frequently translates into interrogations under torture in so-called “casas de pique” (chop shops) or territorial control sites.

The combination of blunt and sharp force trauma reveals a progression of violence. While the cause of death may be asphyxia or a gunshot wound, perimortem injuries indicate the perpetrator’s desire to inflict suffering or to “mark” the body. For the pathologist, this requires meticulous dissection to differentiate vital from post-mortem injuries, allowing for the establishment of the *iter criminis*, or the sequence of the attack.

In 53 cases (79%), additional materials used for wrapping, binding, or gagging the body were identified (see **Table 3**).

The ubiquity of plastic bags, combined with adhesive tape (45.28%) and ropes (22.6%), outlines a logistical “packaging” pattern. The use of domestic items such as blankets, sheets, and mattresses suggests that the homicide and initial body manipulation occur in private or residential settings before being transported to public spaces. This indicates a criminal infrastructure that allows for body handling without immediate detection.

The presence of binding elements (ropes, cables, tapes) not only facilitates transportation by compacting the body to fit into small containers but also serves as

Variable	n	%
Other associated materials	53	79
Adhesive tape	24	45.28
Fiber sacks	17	32
Ropes	12	22.6
Blanket	10	18.8
Plastic wrap	9	16.9
Shoelaces	8	15
Bed sheets	8	15
Wires	3	5.66
Curtains	2	3.7
Elastic bandage	1	1.8
Mattresses	1	1.8
Plastic strapping	1	1.8
Belts	1	1.8
Cables	1	1.8
Clothing	1	1.8
Latex gloves	1	1.8
Suitcases	1	1.8

Table 3.
Other associated materials.

evidence of physical restraint. The analysis of knots and the arrangement of ligatures can provide valuable information regarding the criminal group's "signature" or the perpetrators' level of expertise in load handling and concealment logistics.

Regarding psychoactive substances, rapid urine screening was conducted in 34 cases (50.74%). Positive results for cocaine and marijuana were identified in 32.35% of the tested cases. It is important to note that testing was contingent upon sample availability; in the remaining cases, screening was precluded by the state of decomposition or the absence of urine (see **Table 4**).

The positivity for psychoactive substances in nearly one-third of the evaluated cases (specifically the combination of cocaine and cannabis at 32.35%) opens two interpretative avenues. First, it may indicate a vulnerability of the victim associated with consumption in high-risk environments. Second, in some contexts, substance use is forced or facilitated by the perpetrators to overcome the victim's resistance prior to execution.

The finding of ketamine and MDMA in specific cases suggests a link to nightlife contexts or expanding synthetic drug markets in Medellín. For criminal investigation, these data are crucial: a body with high levels of cocaine and signs of torture points to a settling of scores related to trafficking, whereas the absence of substances in a dismembered body could suggest a different victim profile, perhaps linked to social control or internal discipline.

Scene findings: Plastic bags were universally present, often combined with adhesive tape, ropes, and blankets.

Urine screening*	n	%
Negative	10	29.4
Amphetamines	1	2.94
Cocaine	1	2.94
Cannabis	5	14.7
Cocaine and Cannabis	11	32.35
Cannabis and ketamine	1	2.94
Cocaine and opioids	1	2.94
Cocaine, ketamine, and Cannabis	2	5.88
Cocaine and ketamine	1	2.94
Cocaine, ketamine, opiates, and MDMA	1	2.94
Total	34	50.74

**Applied urine test.*

Table 4.
Associated psychoactive substances.

Injury patterns: Common findings included defensive wounds, overkill lesions, mixed asphyxia, and signs of dismemberment.

Trace evidence: A total of 15 cases (22.38%) yielded positive latent fingerprint impressions on wrapping materials, underscoring their evidentiary value. **Table 5** details the number of fingerprints obtained per case.

Case	Evidence	Result
Case 1	Black plastic bag	15 Fingerprints
Case 2	Black plastic bag	2 Fingerprints
Case 3	Black plastic bag	1 Fingerprints
Case 4	Black plastic bag	2 Fingerprints
Case 5	Red plastic bag	1 Fingerprints
Case 6	Black plastic bag	1 Fingerprints
Case 7	Black plastic bag	13 Fingerprints
Case 8	Black plastic bag	3 Fingerprints
Case 9	Black plastic bag	3 Fingerprints
Case 10	Black plastic bag	1 Fingerprints
Case 11	Black plastic bag	9 Fingerprints
Case 12	Black plastic bag	6 Fingerprints
Case 13	Black plastic bag	3 Fingerprints
Case 14	Black plastic bag	2 Fingerprints
Case 15	Black plastic bag	9 Fingerprints

Table 5.
Positive latent fingerprint.

Evidence	N° EMP analyzed	N° EMP with negative findings	N° EMP with positive findings
Year 2020			
Plastic bag	11	7	4
Adhesive tape	4	4	0
Plastic wrap	1	1	0
Year 2021			
Plastic bag	5	3	2
Adhesive tape	2	2	0
Plastic wrap	4	4	0
Year 2022			
Plastic bag	21	15	9
Adhesive tape	4	4	0
Plastic wrap	5	5	0
Year 2023			
Plastic bag	8	5	3
Adhesive tape	6	6	0
Plastic wrap	1	1	0

Table 6.
Latent impressions.

Regarding the examination of evidence for latent lophoscopic impressions, positive results were obtained from plastic bag materials. However, stretch film and adhesive tapes failed to yield any latent impressions (**Table 6**).

The results obtained in latent fingerprint recovery are highly significant for field forensics. The success found with plastic bags, contrasted with the absolute failure on adhesive tapes and stretch film, reveals both technical and material limitations. The porous texture or surface irregularity of the stretch film, combined with the use of gloves (frequent in these crimes), hinders the transfer of papillary ridges. However, obtaining up to 15 prints from a single black polyethylene bag demonstrates that the container itself is the most valuable piece of evidence. The analysis suggests that the perpetrator, under the stress or urgency of abandoning the body, tends to handle large bags without full protection, leaving latent traces that constitute the only direct physical link between the killer and the scene of the discovery.

4. Discussion

Literature reports regarding autopsies of bodies found in bags are scarce. An article published in 2021 by Maria De Matteis et al., covering a series of 13 cases over the last 20 years and a literature review on homicides involving concealment maneuvers, identified freezing, dismemberment, burial in concrete, submersion, bagging, incineration, and earth burial as the most frequent methods of concealment [3].

In another study published by K. Janben et al., a retrospective analysis of forensic autopsies performed at the University of Cologne Medical School, Germany, from 2009 to 2016 revealed that, out of 5,539 autopsies conducted at the Institute of Forensic Medicine in Cologne, 12 cases of packaged or bagged bodies were recorded (0.2%). Of these 12 cases, 7 were homicides (58%), 3 were suicides (25%), one was a case of autoerotic asphyxia, and one was a natural death. The sex distribution was even: 6 men and 6 women. The cohort of homicide victims was aged between 22 and 37 years [4].

In Medellín, Colombia, over a four-year period, a total sample of 67 cases was obtained—a figure significantly higher than what has been reported in the literature to date. In all cases, the manner of death was homicide, and the most frequent age range was between 15 and 25 years.

In this study, beyond identifying body bagging as a method for concealment or final disposal, cases were also identified where the purpose of the bag was to cause death or to serve as a specific method of torture. The finding of other types of trauma (43.28% of cases) that did not directly cause death necessitates the consideration of torture within the contextual investigation of the case. In more than half of the cases (79%), other materials used for packaging the bodies or restraining the victims (tapes, ropes, straps, among others) were found; the nature and evidentiary potential of these materials must be considered, ensuring proper handling and processing according to the specific circumstances of each case.

The recovery of latent fingerprints from the wrappings in this study demonstrated that materials such as plastic bags have a high probability of yielding latent lophoscopic impressions, which are of vital importance for linking potential perpetrators or suspects to the crime during the investigation. In these cases, the adequate preservation and care of the evidentiary items (EMP) are fundamental to guarantee their probative value within the judicial investigation process.

On the other hand, the most frequent causes of death were asphyxia (56.7%), followed by gunshot wounds and sharp force trauma. This study identified suffocation with a bag and strangulation (manual or ligature) as methods of asphyxia. In cases of sharp force trauma, instances of dismemberment or the presence of other injury patterns, such as overkill and defense wounds, were not uncommon.

Regarding asphyxia by suffocation with a bag specifically, the available literature is very limited, as most reported cases occur in suicidal contexts. In a study published by Jorge Ivan Pareja, characterizing homicides by suffocation among 38,772 autopsies performed between 2008 and 2021 at the National Institute of Legal Medicine and Forensic Sciences in Medellín, 96 cases (14.1%) related to suffocation with plastic bags were found. Eighty individuals (83.3%) presented additional signs of blunt force trauma that did not explain the death and could be related to torture maneuvers [5].

Regarding cases associated with dismemberment, although most cases registered in the literature describe defensive dismemberment as the most common, in Colombia, offensive dismemberment – or dismemberment as a specific method to cause death – is not uncommon. A systematic review by N. Wilke-Schlhorst et al. of 51 cases of dismemberment (30 defensive, 21 offensive) occurring over a 57-year period and autopsied at the Department of Legal Medicine in Hamburg, Germany, concluded that the majority of dismemberment cases are defensive; perpetrators belong to the victim's close social circle, are middle-aged men with no primary

psychiatric illnesses, and lack experience in the medical sector or professional butchery [6]. In the case of Medellín, Colombia, a study published by Catalina Vasquez et al. characterizing dismembered bodies handled at the Medellín Basic Unit of the National Institute of Legal Medicine and Forensic Sciences between 2013 and 2017 found a total of 54 cases – a figure exceeding the German caseload of 57 years. Of these, 9 cases (16.7%) involved disarticulation where anatomical knowledge and expertise by the aggressor were evident, while 41 cases (75.9%) were rough dismemberments (hacking/chopping) [7]. In the current study, sharp force trauma was found in 8 cases (27.5%), associated with the presence of rough dismemberment in 2 cases.

Unlike the cases reported in Germany and Italy, where “bagging” is typically a method of domestic or individual concealment (often linked to passionate or psychiatric motivations), in Latin America, “bagging” serves as a fundamental tool for criminal governance.

- Mexico: The encobijados (bodies wrapped in blankets) share structural similarities with the “bagged bodies” of Medellín. However, Mexico shows a higher prevalence of using blankets decorated with narcomensajes (narco-messages). While the message in Medellín is typically implicit and territorial, in Mexico, it is explicit and directed toward the state or rival cartels[8–9].
- Brazil: In favelas controlled by groups such as Comando Vermelho or the PCC, the “microwave” (micro-ondas) – burning bodies inside stacks of tires – is frequently used to eliminate evidence. Bagging in Brazil, similar to the Medellín context, is primarily reserved for bodies that must be “dumped” in neutral zones to avoid triggering police intervention within the favela[10–11].
- El Salvador: Historically, gangs (MS-13 and Barrio 18) have utilized clandestine graves for the total disappearance of victims. Nevertheless, the abandonment of bodies in bags on public roads has emerged as a tactical defiance against intensive security policies, mirroring the patterns observed in Medellín between 2020 and 2023[12–13].

The investigation of these cases in Medellín is governed by the Minnesota Protocol (2016), as these findings often suggest crimes committed within contexts of territorial control by armed groups.

5. Conclusions

The forensic approach to a “bagged body” can vary significantly depending on the type of trauma, the state of decomposition, and the complexity of the case. Scenarios range from situations involving a single sharp force or gunshot injury – where the bagging serves primarily for disposal and concealment – to highly complex cases involving decomposed, charred, or dismembered bodies. These latter cases may present multiple traumatic mechanisms (asphyxia, sharp force, blunt force, firearm), where the bagging is used for concealment, facilitation of final disposal, or as a method of torture, representing a case of extremely high complexity.

Furthermore, contextual information is frequently deficient, which hinders the ideal and optimal approach to the specific case. Therefore, whenever one is presented with a bagged body, it is crucial to question the objective behind this method of disposal. In this regard, during the autopsy procedure, four key questions must be answered:

- What is the purpose of bagging?
- Is there an associated injury pattern?
- Are there other associated elements or items?
- What should be done with the containers and other recovered items?

In light of the above, the following flowchart is proposed (see **Figure 3**). In all cases involving bodies found in bags, the Minnesota Protocol must be applied, ensuring compliance with all autopsy and sampling standards. Ideally, post-mortem imaging (X-ray or CT) should be conducted before opening the container to document the body’s position, locate ballistic elements, and assess trauma.

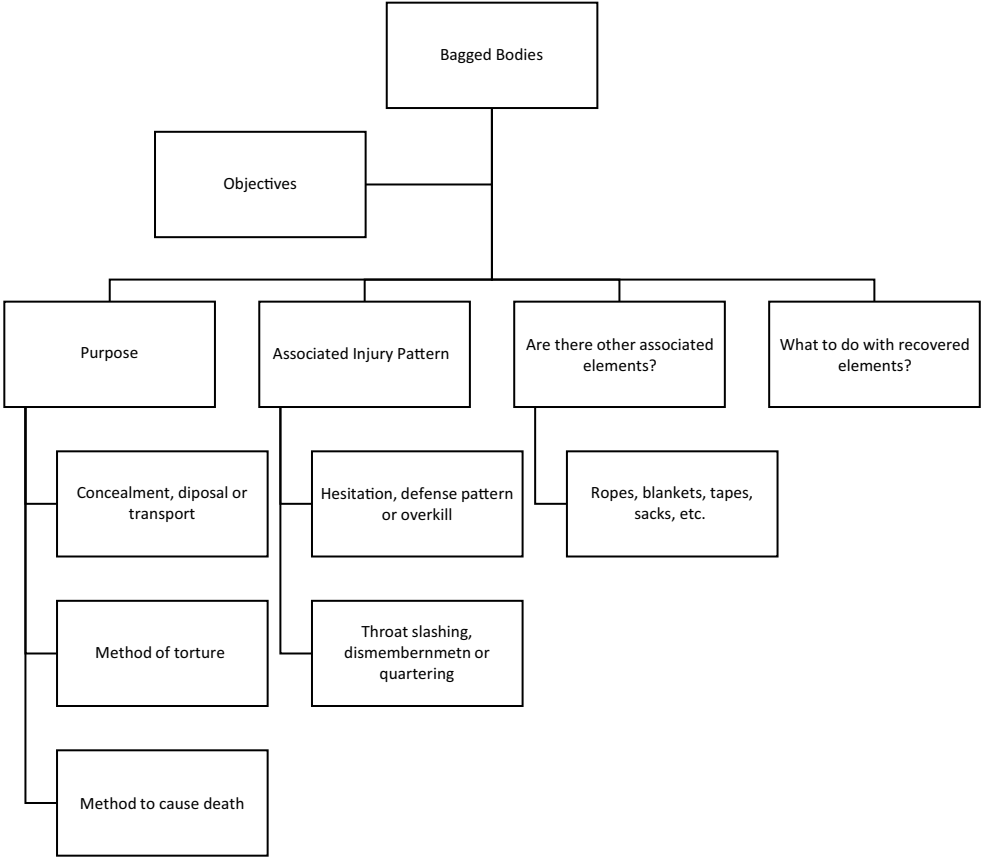


Figure 3.
Key objectives and factors in bagged body investigations.

The leading causes of death in these scenarios are asphyxia, gunshot wounds, sharp force trauma, and blunt force trauma. Each mechanism requires a specific investigative approach. For asphyxia, it is necessary to differentiate between torture maneuvers and the lethal mechanism itself.

Regarding sharp force trauma, findings of dismemberment or quartering are common. The investigation must establish whether the pattern is defensive, offensive, aggressive, or necromaniacal. Note that in Colombia, aggressive dismemberment is a frequent method used for both torture and homicide.

Forensic anthropology consultation is recommended to evaluate tool marks and establish the common origin of anatomical segments. While genetics is useful, re-association can often be achieved through analysis of traumatic continuity and anatomical/taphonomic features in fresh remains. Additionally, histopathology and immunohistochemistry are fundamental for determining the vitality of wounds, distinguishing between aggressive dismemberment (torture) and post-mortem mutilation.

Careful examination of the containers (bags, wrappings) is essential to recover trace, biological, or fingerprint evidence. A fingerprint specialist should assist during the autopsy to ensure proper handling of items like stretch film and adhesive tapes, maximizing the recovery of latent prints.

Respect to other associated evidence (ropes, wires, mattresses, etc.), coordination with other forensic labs (biology, chemistry, trace evidence) is necessary to determine the appropriate analysis and packaging for these evidentiary items. An interdisciplinary approach is strongly advised. See the flowchart in **Figure 4**.

Finally, the phenomenon of “bagged bodies” has drastically reconfigured the perception of security in Medellín. Despite the general reduction in homicide rates observed over the last decade, the recurrence of these findings generates a profound sense of qualitative perceived insecurity. This phenomenon does not represent mere isolated events of human waste disposal; rather, it exposes dynamics of social and territorial control within organized crime groups.

- **Invisible Borders and Territorial Delimitation:** The abandonment of bodies is often localized at the geographic boundaries between districts (comunas). This practice responds to the strategic need to demarcate territories and broadcast symbolic messages of dominance aimed at the citizenry, rival criminal structures, and state institutions. This “violent messaging” tactic forces the municipal administration to re-evaluate the effectiveness of video surveillance systems and strengthen institutional presence in peripheral road corridors identified as critical disposal points.
- **Instrumentalization of Public Space as a Stage of Terror:** The discovery of a bagged body transmutes a place of everyday transit into a scene of terror and extrajudicial control. This phenomenon negatively impacts social cohesion, community mental health, and the real estate value of the affected sectors. Therefore, security policies must transcend the traditional model of capturing ringleaders to focus on neutralizing the “logistics of disposal” and strengthening the judicial response to these complex forms of targeted violence.

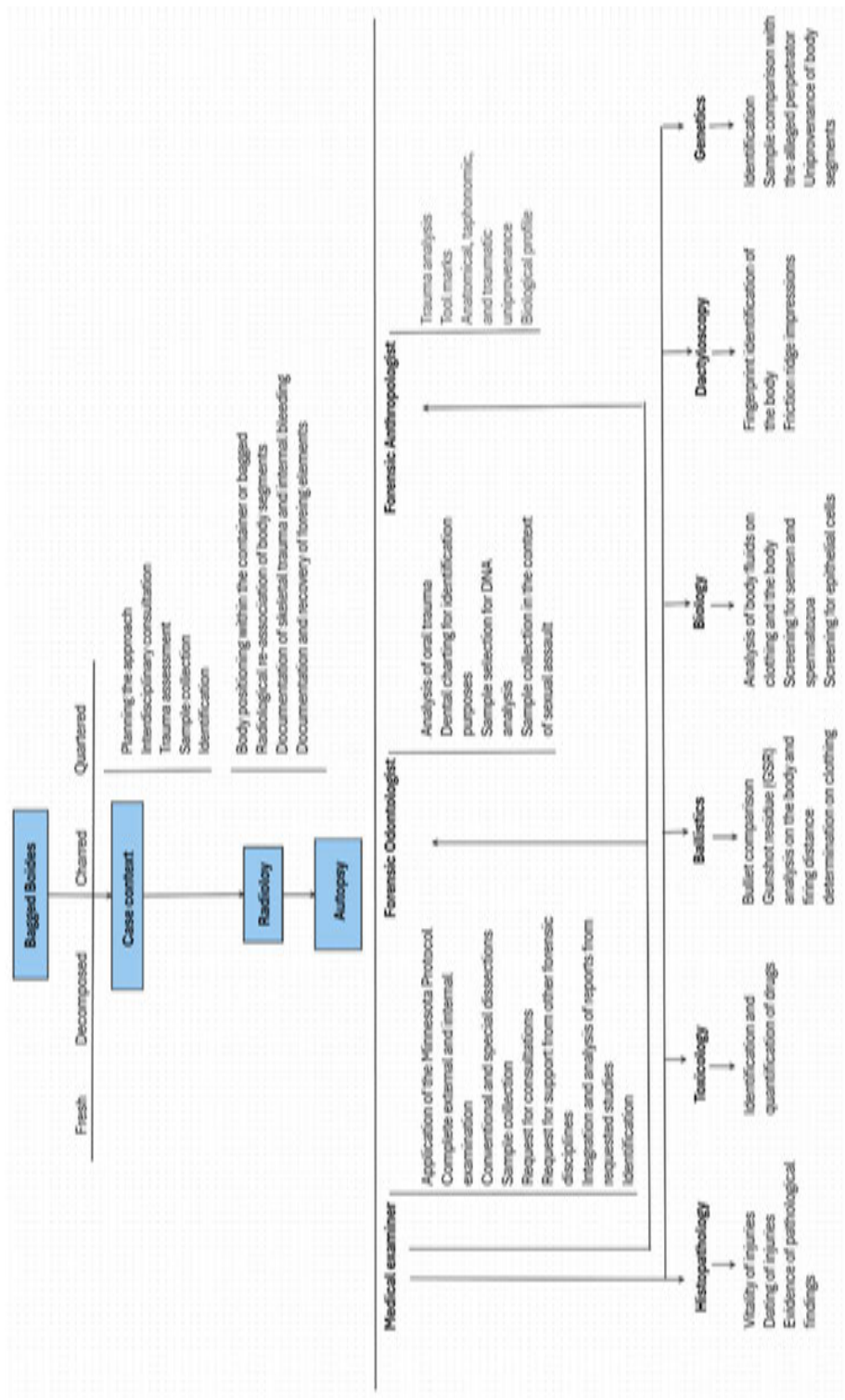


Figure 4.
Analytical schema for the forensic investigation of bagged bodies.

Acknowledgments

I would like to express my gratitude to Cristian Yorley Otálvaro for sharing his expertise and valuable insights regarding the handling and processing of latent lophoscopic impressions.

This document has been prepared by the author, Jennifer Garcia Ospina, who holds full copyright ownership of the original research, the data collected, and the scientific conclusions. The use of Artificial Intelligence (AI) tools is acknowledged as editorial support for textual expansion, narrative structuring, and linguistic optimization of the content. Technical supervision, validation of forensic data, and the final interpretation of the findings have been carried out entirely by the author, ensuring the accuracy and ethical responsibility of the scientific work.

Author details

Jennifer Garcia Ospina*
National Institute of Legal Medicine, Medellín, Colombia

*Address all correspondence to: jennifer.garcia@medicinalegal.gov.co

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] National Institute of Legal Medicine and Forensic Sciences. Forensis 2022: Data for Life. Bogotá: National Reference Center on Violence; 2023. Available from: <https://www.medicinalegal.gov.co/cifras-estadisticas/forensis>
- [2] United Nations Office on Drugs and Crime. Global study on homicide 2023: Homicide and organized crime in Latin America and the Caribbean. Vienna: UNODC; 2023. Available from: https://www.unodc.org/documents/data-and-analysis/gsh/2023/GSH_2023_LAC_web.pdf
- [3] De Matteis M, et al Homicide and concealment of the Corpse. Autopsy case series and review of the literature. *International Journal of Legal Medicine*. 2021;**135**:193–205
- [4] Janßen K, Rothschild MA, Kamphausen T. Die verpackte Leiche: Auswertung des Sektionsgutes von 2009–2016 hinsichtlich unterschiedlicher Fallumstände und Motivationen. *Rechtsmedizin*. 2018;**28**:1–9. DOI: 10.1007/s00194-017-0206-6
- [5] Pareja JI. Epidemiological characterization and findings in homicides by suffocation with plastic bags in the city of Medellín, Colombia 2008-2021. *Revista Española de Medicina Legal*. 2023;**49**(4): 151–156. DOI: 10.1016/j.reml.2023.08.001
- [6] Wilke-Schalhorst N, Schröder AS, Püschel K, Edler C. Criminal corpse dismemberment in Hamburg, Germany from 1959 to 2016. *Forensic Science International*. 2019; **300**:145–150. DOI: 10.1016/j.forsciint.2019.04.038
- [7] Guarín CV, Ospina JG, Molina CF. Factors associated with the identification of dismembered bodies in Medellín, Colombia. *Revista Española de Medicina Legal*. 2021;**47**:9–15. DOI: 10.1016/j.remle.2019.12.001
- [8] Fuentes Díaz A. Necropolitics and the Spectacular Nature of Violence in Mexico. Benemérita Universidad Autónoma de Puebla; 2019. Available from: https://www.researchgate.net/publication/368330260_Violence_in_Mexico_Necropolitics_and_Extraction
- [9] Ovalle L. Between indifference and spectacularization: Visual representations of violence in Mexico. *Estudios Culturales*. 2010;**6**(12): 150–168. <https://www.redalyc.org/articulo.oa?id=69410203>
- [10] Manso BP, Dias CN. The war: The rise of the PCC and the world of crime in Brazil. *Todavía*; 2018. Available from: <https://dialnet.unirioja.es/servlet/articulo?codigo=7416183>
- [11] Sant’Anna G, et al. Forensic patterns of lethal violence in Brazil: A review of the literature. *Journal of Forensic and Legal Medicine*. 2017;**49**:12–20. https://www.researchgate.net/publication/354251591_Lethal_Violence_in_Brazil_A_Systematic_Review_of_Portuguese-Language_Literature_From_2000_to_2020
- [12] International Crisis Group. (2022). The Miracle or Mirage of El Salvador’s Security Policy? Crisis Group Latin America Report.

Available from: <https://www.crisisgroup.org/latin-america-caribbean/el-salvador/081-miracle-or-mirage-gangs-and-plunging-violence-el-salvador>

[13] Cruz JM. Central American maras: From youth street gangs to transnational protection rackets. *Global Crime*. 2010;**11**(4):379–398. <https://ideas.repec.org/a/taf/fglcxx/v11y2010i4p379-398.html>

Edited by Kamil Hakan Dogan

Traditional justice systems are struggling to keep pace with contemporary criminal activities that span both the real world and the online domain. This work integrates sociological criminology and forensic evidence to analyze new forms of societal harm. The book shifts its focus from physical social structures to virtual spaces, exploring how adaptive violence and technological advancements, such as big data and AI, redefine criminal opportunities. From a multidisciplinary perspective, international researchers assess the lifecycle of electronic evidence, the legal framework of medical forensics, and advanced field protocols for untangling the complexities of organized crime. Functioning as a necessary tool, this collection aids educators, law enforcement officers, and legal experts in understanding the elaborate framework of justice in an ever-altering world.

Sandro Serpa, Social Sciences Series Editor

Published in London, UK

© 2026 IntechOpen
© 9parusnikov / iStock

IntechOpen

ISSN 2977-6473

ISBN 978-1-80631-563-5



9 781806 315635