Chapter 17
Legal and Ethical Considerations in Cyber Forensics

Omowunmi F. Makinde
https://orcid.org/0009-0004-9372-7539
Amazon, USA

ABSTRACT

This chapter examines the complex legal and ethical landscape surrounding human threat intelligence analysis in cyber forensic investigations, addressing challenges created by integrating artificial intelligence, behavioral analysis, and user-centric techniques. The analysis explores constitutional protections in behavioral profiling, digital evidence admissibility standards for AI-enhanced investigations, and cross-border legal challenges in dark web intelligence. Privacy rights under frameworks like GDPR require balancing security needs with individual privacy through data minimization and consent mechanisms. Ethical considerations encompass algorithmic bias, transparency requirements, and professional conduct standards. The chapter addresses regulatory compliance across industry sectors and emerging challenges from quantum computing threats and social engineering analysis, demonstrating that successful navigation requires collaboration between practitioners, legal professionals, and policymakers.

1. INTRODUCTION

The interactions between human threat intelligence and cyber forensic practices have altered the digital investigations definition to center on the intentional and malicious intrusions, ceasing to be just about technical breaches but focused on

DOI: 10.4018/979-8-3373-4898-8.ch017

human-made intrusions like the social engineering technique, insider abuse, and targeted attacks on a long-term basis. It is due to this change that new legal and ethical issues have arisen, which should be approached with utmost care (Saeed et al., 2023). The increased application of machine learning and artificial intelligence to forensic practice is only making the area more complicated where courts must deal with the automated results, how to curb the application of bias, and how to comprehend human accountability when machines aid in the investigative process. Such advances demand a better idea of the applicability of old legal principles to new forensic technology (Solanke and Biasiotti, 2022).

The law of human threat intelligence lies at a cross-road of the constitutional protection, laws of privacy, the standard of evidence, and international collaboration. The Fourth Amendment rights in the U.S. and similar protections of privacy in other parts of the world also impose significant restrictions on surveillance of activities and electronic surveillance (Rai et al. 2016; Rai, 2019; Nain, 2024). These safeguards have to balance with the requirement to identify and mitigate severe risks (Zhang, 2025). There is also a problem with the court assessing artificial intelligence evidence, as machine-learning algorithms and machine analysis are not easily categorized under the traditional evidentiary rules. The extra levels of complexity include cross-border investigations, in particular, those that involve intelligence of dark-webs, as the various jurisdictions might possess incongruent rules or protocols (Durán et al., 2024).

The other vital component of this landscape is privacy and data protection laws. Several aspects of human threat intelligence, such as behavioral profiling, require the intensive use of personal information, thus the need to ensure high protection and ethical control (Marikyan et al., 2023). There are rules and laws like the GDPR that are in place to ensure that a number of requirements are met especially in situations where the data moves across the borders. Insider-threat programs should also weigh between organizational security and employee rights and thus should be clearly consented, proportional and limited to its scope of monitoring (Javed & Sajid, 2024).

Ethical issues comprise algorithmic discrimination, openness, and consideration of personal dignity. AI systems may generate injustice when monitored without care, and they may make legal procedures complex and interfere with individual rights due to their inability to be explained (Quang Huy & Kien Phuc, 2025).

1.1 Constitutional Protections in Behavioral Analysis

The fundamental boundaries to the application of human threat intelligence work in behavioral analysis are constitutional protections, particularly the Fourth Amendment prohibition of unreasonable searches and seizures. The Fourth Amendment stipulates that government searches must be reasonable, which should be typically

Broad Perspective of Smart Home Technology in 2024
Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186

Broad Perspective of Smart Home Technology in 2024
Joseph M. Schulzand Jack S. Scilla (2024). *International Journal of Smart Technologies (pp. 1-27).*
www.irma-international.org/article/broad-perspective-of-smart-home-technology-in-2024/350186