Navigating Legal Challenges in Digital Evidence: A Case Study of Cybercrime Prosecutions

Jordan Miller
PhD
Humboldt University of Berlin
Unter den Linden 6, 10099 Berlin, Germany

Kai Rodriguez
Associate Professor
Harvard Law School
Cambridge, MA 02138, USA

Casey Hill
Professor
University of Paris 1 Pantheon-Sorbonne
12 Place du Panthéon, 75005 Paris, France

Abstract. This study explores the complexities and challenges of prosecuting cybercrime cases through the lens of digital evidence. Given the exponential growth in internet usage and technological advancements, the legal system faces unprecedented hurdles in adapting traditional legal frameworks to address digital evidence effectively. Employing a case study methodology, this analysis examines notable legal precedents and prosecutorial strategies utilized in landmark cybercrime cases. The findings highlight significant gaps in existing legal standards and the pressing need for updated regulations that account for the nuances of digital evidence. Ultimately, this paper offers recommendations for legal practitioners and policymakers to enhance the efficacy of cybercrime prosecutions while ensuring justice and due process are upheld.

Keywords: cybercrime, digital evidence, legal challenges, prosecution strategies, jurisdictional issues, cybersecurity law, technological advancements, evidence law, criminal justice

Introduction

The rapid proliferation of digital technology has transformed various aspects of daily life, including communication, commerce, and social interactions. However, this digital revolution has concurrently given rise to a myriad of legal challenges, particularly in the realm of cybercrime. Cybercrime, defined as criminal activities conducted via the internet, presents unique challenges to the legal system. These challenges stem from the fleeting nature of digital evidence, the layered anonymity provided by the internet, and the variability of legal interpretations across jurisdictions. The relevance of this issue continues to escalate as cybercriminals employ increasingly sophisticated techniques that outpace existing legal frameworks. As we move further into 2024 and beyond, addressing the complexities surrounding digital evidence in cybercrime prosecutions is paramount. This paper delves into these complexities through a focused examination of specific cases that illustrate the legal quagmires faced by prosecutors. By analyzing these important cases, we aim to shed light on the implications for legal practitioners and the judicial system as a whole. In doing so, we will provide a structured approach to understanding the evolving landscape of cybercrime legislation and its enforcement. This paper is organized as follows: we first define the scope of cybercrime and its implications for legal proceedings. Next, we analyze selected case studies that exemplify the hurdles in prosecuting cybercriminals effectively. Finally, we conclude with strategic recommendations for law enforcement and legal professionals to enhance the management and prosecution of cybercrime cases.

This is a preliminary version. To read the full version of the article, please purchase a subscription.

References

1. Kullolli, B. (2018). Confidentiality-A Two-Appeal Principle. European Journal of Social Sciences, 1(3), 53-60.