Cybercrime Legislation and the Role of Digital Forensics in Ireland

Michael Hegarty

Abstract: This document provides an analysis of the evolving legal landscape in Ireland concerning cybercrime, with a particular focus on the implications for digital forensics. The Internet's increasing use for both legitimate and illicit purposes has driven the need for robust legislation to combat crimes such as hacking, identity theft, and fraud. The paper reviews key Irish laws, including the **Criminal Justice (Offences Relating to Information Systems) Act 2017**, **Data Protection Acts (1988-2018)**, and the recently introduced **NIS2 Directive**, highlighting their relevance to digital forensics. By outlining how these laws support the investigation and prosecution of cybercriminals, the document demonstrates the pivotal role of digital forensics in preserving digital evidence, complying with data protection standards, and enhancing cross-border cooperation. Additionally, the analysis addresses older but still relevant laws, such as the **Criminal Damage Act 1991** and the **Criminal Justice (Theft and Fraud Offences) Act 2001**, which continue to provide a framework for prosecuting cybercrime in conjunction with newer regulations. The review underscores the importance of integrating legal and technical expertise in responding to the growing complexity of digital threats.

Keywords: Computer Forensics, Cybercrime legislation, Data Protection Acts, Cybersecurity laws, Cross-border cybercrime

---

Introduction

The Internet, a global communications system, has become integral to businesses, allowing them to increase their customer base and improve service delivery. However, its vast, anonymous nature has also made it an attractive target for criminals, who exploit it for fraud, identity theft, and other cybercrimes. While businesses and individuals use the Internet for legitimate purposes, cybercriminals exploit its open protocols and technological vulnerabilities to gain unauthorized access to sensitive information such as personal, financial, and authentication details. Classic examples include phishing scams and malware attacks designed to steal data or cause harm.

The rise of cybercrime has led to the development of **digital forensics**, a specialized field within computer science, designed to extract and analyse data from digital devices for legal investigations. Initially developed by law enforcement agencies, digital forensics has now grown to encompass contributions from academia, professional cybersecurity companies, and

open-source communities. This document explores Ireland's legal framework for prosecuting computer-related crimes, focusing on the most recent and relevant legislation affecting digital forensics and cybersecurity.

Irish Legislation and Digital Forensics

Ireland's legal framework for addressing computer-related crime has evolved significantly, reflecting the rapid advancements in technology and the increasing threat posed by cybercriminals. Key legislation includes:

1. Criminal Justice (Offences Relating to Information Systems) Act 2017

This Act is central to combating cybercrime in Ireland, covering offences such as hacking, denial-of-service attacks, and unauthorized access to computer systems. The Act also criminalizes the possession or use of tools designed to facilitate cybercrime. Notably, it addresses cross-border cybercrimes by including provisions for prosecuting crimes committed outside Ireland if they affect Irish systems or interests. Penalties under this Act range from fines to imprisonment, with up to 10 years for severe cases, such as attacks on critical infrastructure (Irish Statute Book, 2017).

For digital forensics professionals, this legislation provides a clear legal framework for investigating unauthorized access or damage to information systems. Their role is crucial in gathering admissible evidence, such as identifying how and when an attacker accessed a system, what tools they used, and whether data was stolen or manipulated.

2. Data Protection Acts (1988 to 2018) and the General Data Protection Regulation (GDPR)

The **GDPR**, enforced alongside the Data Protection Acts, regulates the processing of personal data. It is especially relevant in cases where digital forensics investigations involve personal information, such as in data breaches or identity theft cases. Under GDPR, any entity handling personal data must ensure strict compliance with privacy and security standards (Data Protection Commission, 2018). Fines for non-compliance can reach €20 million or 4% of global turnover, whichever is higher.

For digital forensics, this legislation emphasizes the importance of data integrity and security. When investigating a breach, forensic experts must ensure that the collection and analysis of

personal data comply with GDPR requirements, minimizing intrusion into individuals' privacy while collecting necessary evidence.

3. NIS Directive (2016/1148) and NIS2 Directive

The **Network and Information Security (NIS) Directive**, introduced in 2016, aimed to improve the cybersecurity of essential services such as energy, health, and finance. Ireland adopted this directive to increase the resilience of its critical infrastructure to cyber-attacks. In 2024, **NIS2 Directive** will strengthen these rules further, bringing more sectors under regulation and increasing penalties for cybersecurity failures. This directive mandates that digital forensics professionals engage in more rigorous investigation processes to detect and mitigate cyber incidents, especially those affecting critical systems (European Union, 2022).

The introduction of the NIS2 directive represents a significant development for digital forensics. It expands the scope of mandatory reporting for cyber incidents, requiring organizations to notify authorities within 24 hours of detecting a significant breach. This creates new challenges and opportunities for digital forensics professionals, who are tasked with swiftly identifying the source and scope of cyber-attacks and preserving crucial evidence.

Relevant Older Laws Still in Force

1. Criminal Damage Act 1991

Section 5 of the Criminal Damage Act criminalizes unauthorized access to computer systems, even if no actual damage occurs. It focuses on intent rather than results, making it a powerful tool for prosecuting attempted cyber-attacks. Digital forensics is critical here, as investigators can trace an attacker’s actions to establish intent, even if the attack was unsuccessful (Criminal Damage Act, 1991).

Section 2 of the same Act deals with damage to property, including digital property. For example, introducing a virus or malware that damages a system, or data could lead to prosecution under this section, with penalties ranging from fines to 10 years in prison (Criminal Damage Act, 1991).

2. Criminal Justice (Theft and Fraud Offences) Act 2001

Section 9 of this Act addresses the unlawful use of a computer for dishonest gain or causing loss to another. This section is particularly relevant to cases of electronic fraud, where criminals use digital tools to manipulate financial data or engage in phishing schemes. Digital forensics plays a crucial role in investigating these crimes by examining digital evidence such as logs, emails, and transaction data to establish a timeline of fraudulent activity (Irish Statute Book, 2001).

International Framework: The European Convention on Cybercrime

Ireland is a signatory to the **European Convention on Cybercrime** (2001), which aims to harmonize laws across Europe to combat cybercrime. The Convention sets guidelines for criminalizing activities such as unauthorized access, data interference, and system interference, and promotes cooperation between member states for investigations. This framework is vital for digital forensics, as it facilitates cross-border cooperation in cybercrime cases, allowing for faster evidence-sharing and coordinated legal action (Council of Europe, 2001).

Conclusion

Ireland's legislative framework for addressing cybercrime and digital forensics has evolved to meet the growing complexity of modern digital threats. Laws such as the **Criminal Justice (Offences Relating to Information Systems) Act 2017**, **Data Protection Acts**, and the **NIS2 Directive** provide the necessary legal tools for investigating and prosecuting cybercriminals. These laws highlight the pivotal role of digital forensics in collecting, preserving, and analysing evidence to ensure that cybercrimes are effectively prosecuted.

References

- **Criminal Justice (Offences Relating to Information Systems) Act 2017**. Available at: http://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/html (Accessed: 15 October 2024).
- **Data Protection Commission (2018)**. General Data Protection Regulation (GDPR). Available at: https://www.dataprotection.ie/en/organisations/know-your-

obligations/data-protection-law-general-data-protection-regulation (Accessed: 15 October 2024).

- **European Union (2022)**. NIS2 Directive. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 (Accessed: 15 October 2024).
- **Criminal Damage Act 1991**. Available at: http://www.irishstatutebook.ie/eli/1991/act/31/enacted/en/html (Accessed: 15 October 2024).
- **Irish Statute Book (2001)**. Criminal Justice (Theft and Fraud Offences) Act 2001. Available at: http://www.irishstatutebook.ie/eli/2001/act/50/enacted/en/html (Accessed: 15 October 2024).
- **Council of Europe (2001)**. European Convention on Cybercrime. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 15 October 2024).