



**Politecnico  
di Torino**

# **Computer Forensics Class 2024/2025**

---

**Italian Law n. 48/2008**



## **Overview and significance of Italian Law n. 48/2008 in the context of cybercrime in Italy**

## ▶ Budapest Convention on Cybercrime - Overview



- 🔍 The Budapest Convention on Cybercrime was issued by the Council of Europe on November 23, 2001.
- 🔍 Italy ratified the Convention with Law n. 48 on March 18, 2008, published in the Official Gazette on April 4, 2008.

## ▶ Italian Law n. 48/2008 - Overview



🔍 The ratification of the Budapest Convention by Italy through Law n. 48/2008 represents a critical step in the modernization of the Italian legal system to tackle cybercrime: the law's approach to harmonizing legal standards across borders underlines **the growing importance of international cooperation in addressing the rapidly evolving digital landscape**

🔍 While these legal frameworks aim to create a cohesive international strategy, challenges remain, particularly in the **areas of rapid technological change** and the need for continuous updates to legislative tools. This is reflected in the Italian legislature's cautious stance on defining technical terms within the law, allowing flexibility for future interpretations.



## The main innovations



- 🔍 International harmonization of legislations: aligning laws internationally to combat cybercrime
- 🔍 Reorganization of cybercrime offenses: amendments and integrations to the penal code, introducing new specific offenses
- 🔍 Corporate Liability: extending the liability under Legislative Decree 231/2001 to cover certain cybercrime offenses

# The Corporate Criminal Liability

## What is It?

It is the liability applicable to companies as a consequence of a criminal offense introduced by Legislative Decree 231/2001

## It applies

To all legal entities — even if foreign — if the offense is committed in Italy (and to Italian companies, under certain circumstances, even if it is committed abroad)

## When?

If the offense is committed in the interest or for the benefit of the company.

## For offences committed by:

- Persons holding a position of representation, management or direction or who exercise, even if *de facto*, management and control ("**Top Management**")
- Persons subject to the control or monitoring activity of the Top Management.

# The Corporate Criminal Liability

**CRIMES AGAINST PUBLIC  
ADMINISTRATION**

**TAX OFFENSES**

**MONEY LAUNDERING/  
RECEIVING STOLEN GOODS**

**ORGANIZED CRIME OFFENSES**

**COMPUTER CRIMES**

**"CORPORATE" OFFENSES  
(INCLUDING PRIVATE-TO-  
PRIVATE CORRUPTION)**





## The main innovations



- 🔍 Fund for combating child pornography online: establishment of a fund under the Ministry of the Interior to protect national critical IT infrastructures
- 🔍 Amendments to data retention laws: updating the rules on data retention, referencing Directive 2006/24/EC
- 🔍 International cooperation: mutual assistance between Convention member and signatory states
- 🔍 Acquisition of digital evidence: changes to the criminal procedure code to regulate the collection and use of digital and telematic evidence





# **Key provisions and their implications for digital forensics**

## ▶ Major procedural and investigative updates



- 🔍 International cooperation: The law allows the Ministry of the Interior or designated authorities to order internet and telecommunications providers to retain and protect traffic data for up to 90 days, extendable to six months for specific investigative needs, excluding the content of communications.
- 🔍 Competence for investigations and prosecutions: Investigations and prosecutions for cybercrime offenses are assigned to the Public Prosecutor's Office at the Court of Appeal's main district. This aims to improve coordination in combating cybercrime, although early issues arose due to the lack of transitional provisions for ongoing investigations, later resolved by Law n. 125 of July 2008.

## ▶ Major procedural and investigative updates



- 🔍 Service providers' role: Internet, telecommunications, and postal service providers play a key role in combating cybercrime, particularly through:
- Data retention for traffic data and communications logs
  - Seizure of correspondence, including electronic communications, when linked to criminal investigations
  - Seizure of digital data from service providers, with measures ensuring that data is copied without modification, while the original data is preserved.

## ▶ Major procedural and investigative updates



🔍 Legal recognition of computer forensics: The law marks a significant step toward integrating computer forensics into investigative practices, establishing clear protocols for handling digital evidence in line with scientific advancements. However, the evolution of these practices will require ongoing updates as technology progresses.

## ▶ Major procedural and investigative updates



🔍 The law emphasizes "best practices," advocating procedures that:

- Acquire evidence without altering the original device.
- Authenticate the evidence and its digital copy.
- Ensure the examination's repeatability.
- Maintain impartiality in technical analysis.

## ▶ Major procedural and investigative updates



### Email seizures

🔍 The law includes provisions for seizing email communications, equating traditional and electronic mail under legal protections.

## ▶ Major procedural and investigative updates



🔍 The law addresses changes to the Code of Criminal Procedure, expanding the scope of investigative measures like inspections and seizures to include digital environments. Notable amendments include:

- **Digital Inspections and Searches:** new provisions mandate technical measures to preserve the integrity of original data and prevent alterations. These measures are crucial given the volatile nature of digital evidence, which can be affected by inadvertent actions during investigations.
- **Preservation Orders (Freezing):** Introduced as a rapid measure to secure digital evidence before it is lost or tampered with.





## Law n. 48/2008: areas for improvement as both technology and cybercrime evolve



### Standardization of Digital Evidence Procedures

Law n. 48/2008 brought a unified approach to the handling of digital evidence in criminal procedures. It established clear protocols for the acquisition, preservation, and presentation of digital evidence in court, which helped overcome previous inconsistencies. Ensuring the integrity and authenticity of digital evidence became a priority to ensure its admissibility in legal proceedings.



## Law n. 48/2008: areas for improvement as both technology and cybercrime evolve



### Judicial Expertise and Training in Digital Forensics

The implementation of this law increased the responsibility of judges and legal professionals to understand the technical aspects of digital forensics. Without proper training, there is a risk that digital evidence could be misinterpreted or not fully understood. As a result, there is a growing emphasis on providing specialized training in digital forensics for those working in the judiciary and law enforcement



## Law n. 48/2008: areas for improvement as both technology and cybercrime evolve



### Legal Certainty and Data Integrity

Digital forensics is heavily dependent on the integrity and authenticity of data. Law n. 48/2008 emphasized the importance of ensuring that data is unaltered during acquisition and properly preserved. This legal requirement improved the reliability of digital evidence in court, making it more trustworthy for judicial processes. However, the need for further refinement in procedures remains, especially in light of increasingly sophisticated cyber threats.



**Case studies and practical  
applications of Italian  
Law n. 48/2008**



## Case study 1



### **Data Seizure and Service Providers**

Phishing case, where data from service providers were seized to trace illegal transactions.

While there isn't a specific named case, this application has been common in fraud and financial crime investigations



## Case study 2



### **Organized Crime and Communication Monitoring**

One significant case involved intercepting communications of mafia organizations in Italy.

This was part of larger efforts coordinated with Europol and Interpol, often using advanced digital forensics techniques to gather evidence through encrypted messaging



## Case study 3



### Cyberstalking

Several cases of cyberstalking in Italy have used digital forensics to track the origin of online threats.

Investigators were able to trace and identify offenders using data traffic analysis and IP identification. Such cases are common in modern Italian jurisprudence.





# Types of Corporate Investigations

1

## Unfair Competition

Investigating rival businesses engaging in unethical practices.

2

## Industrial Espionage

Uncovering theft of trade secrets and proprietary information.

3

## Employee Misconduct


Addressing violations of company policies and contracts.

4

## Intellectual Property Infringement

Protecting copyrights, trademarks, and patents from unauthorized use.

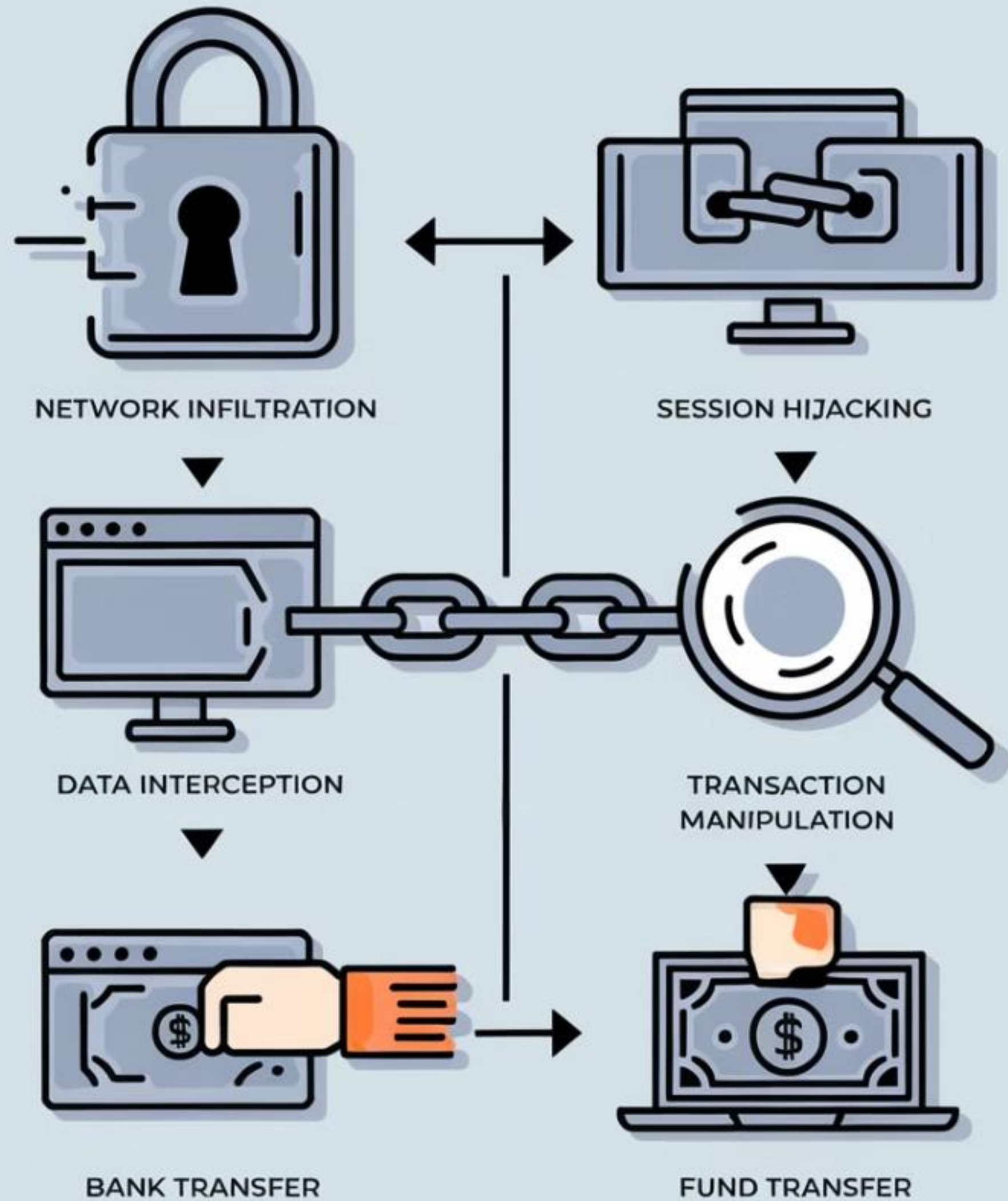




# Man-in-the-Middle (MITM) Attacks

Man-in-the-Middle (MITM) attacks are a silent and sophisticated form of cybercrime where an attacker intercepts communications between two parties. This method allows criminals to monitor, read, and modify messages without detection, often targeting businesses involved in international trade. The attack's success relies on the attacker's ability to remain undetected while gathering crucial information over an extended period.





# The Mechanics of MITM Attacks

1

## Initial Breach

Hackers compromise a company's email system using methods like phishing, brute forcing, or trojans.

2

## Monitoring Phase

Attackers observe communications for an extended period, gathering information about business practices and relationships.

3

## Interception

At the opportune moment, criminals intercept and modify payment instructions, redirecting funds to their own accounts.

4

## Execution

Victims, unaware of the deception, transfer money to the fraudulent account, often losing significant sums.





# Legal Implications of MITM Attacks

## Criminal Perspective

MITM attacks can be classified as fraud under Article 640 of the Italian Criminal Code, involving deception through false emails and documents.

## Identity Theft

These attacks may also fall under identity substitution (Article 494) and computer fraud (Article 640 ter), especially with recent legislative changes.

## Jurisdictional Challenges

Prosecution is often hindered by time constraints and jurisdictional issues, as attackers frequently operate from countries with limited judicial cooperation.

# Civil Recourse and Bank Responsibilities

## Immediate Action

Victims should request payment reversal as quickly as possible, while funds are still in the destination account. Some European banks may cooperate in freezing accounts and returning funds.

## Bank Liability

Banks often avoid liability due to European regulations like the Payment Service Regulation and Italian Legislative Decree 27 January 2010, n. 11, which justify payments even when account holder details don't match.

## Regulatory Gaps

Current regulations may be inadequate in an era of fast online payments, where financial intermediaries have the primary control over transaction verification.