Science, Education and Innovations in the Context of Modern Problems
Issue 11, Vol. 8, 2025

Title of research article

The Role of Nanotechnology in Criminal Evidence: Practical Applications and Legal Challenges

Meliani Fayçal	Maitre de Conférences A Mohamed Boudiaf-msilaUniversiy Algeria E-mail: melianifaycal55@gmail.com
Hakim Belil	Maitre de Conférences A Mohamed Boudiaf-msilaUniversiy Algeria E-mail: belil.hakim@univ-msila.dz

Issue web link	https://imcra-az.org/archive/385-science-education-and-innovations-in-the-context-of-modern-problems-issue-11-vol-8-2025.html
Keywords	Criminal evidence, judicial reasoning, evidentiary fallacies, presumption of innocence, public opinion, impartiality, legal certainty, fair trial.

Abstract

Criminal justice is fundamentally grounded in certainty, with the judge's conviction forming the cornerstone of public trust in judicial rulings. Evidence serves as the primary means to reach that certainty, making the theory of proof the foundation upon which fair criminal adjudication is built. Justice is only realized when judges adhere strictly to legally established rules of evidence, and when the prosecution substantiates its claims with valid, objective proof. Avoiding evidentiary fallacies is therefore essential; as such errors can compromise the fairness of criminal judgments. Among these are: the overly broad interpretation of criminal statutes, biased selection or evaluation of evidence, reliance on personal knowledge, public opinion, or rumor. Other fallacies include the reversal of the presumption of innocence, undue emphasis on appearances, unexamined confessions, or the weight given to a single testimony. A fair trial demands that judges maintain impartiality, resisting influence from extraneous or unlawful factors. Ultimately, rulings must rest solely on admissible, well-examined evidence, thus safeguarding the integrity of the justice system and upholding both fairness and legal certainty in criminal proceedings.

Citation. Meliani F., Hakim B. (2025). The Role of Nanotechnology in Criminal Evidence: Practical Applications and Legal Challenges. *Science, Education and Innovations in the Context of Modern Problems*, 8(11), 520–528. https://doi.org/10.56352/sei/8.11.40

Received: 10.01.2025	Accepted: 01.04.2025	Published: 04.09.2025 (available online)

Introduction

Technological advancement is one of the most pressing topics that has attracted the attention of many researchers in the legal field. This is due to its profound negative impact on societies, particularly with the recent emergence of artificial intelligence. While this advancement has brought about significant positive changes, it has also become a potential threat to societal security. Among the most notable AI technologies is **nanotechnology**, which focuses on studying, understanding, and manipulating matter at the nanoscale. This technology finds applications in several scientific fields such as physics, chemistry, engineering, and beyond.

Although nanotechnology has existed for quite some time, it did not begin to flourish and evolve significantly until around 1981. Since then, it has witnessed remarkable development.

It is undeniable that nanotechnology offers considerable practical benefits. It plays a vital role in enhancing various sectors including information technology, medicine, energy, security, environment, food safety, and more. In fact, it has even been integrated into products used directly by consumers. However, the use of such technology also poses serious risks, as it has been linked to the emergence of various forms of crime. On this basis, we raise the following research question:

What are the forms of crimes arising from the use of nanotechnology?

To address this issue, we have divided the study into the following sections:

Section One: Nanotechnology-related crimes affecting state security

Section Two: Nanotechnology-related crimes affecting property and individuals

Section One: Nanotechnology-Related Crimes Affecting State Security

Nanotechnology-related crimes that target state security are among the most dangerous to society. Threats to the state and its stability have profound implications not only domestically but also internationally. These crimes can be categorized as follows:

Subsection One: Crimes Affecting High-Level State Institutions

The world has witnessed various crimes targeting senior state institutions, posing direct threats to national safety and stability. Among these are:

1. Cybercrimes

The Algerian legislator has used two main terminologies to refer to cybercrime. The first is "crimes against automated data processing systems," introduced by Law No. 04-15 amending the Penal Code. Later, another term was adopted: "crimes related to information and communication technologies," which appears in Law No. 09-04 concerning the specific rules for preventing and combating crimes related to ICT.
[1]

Nanotechnology can be employed in acts of espionage and surveillance, such as planting highly miniaturized sensors in sensitive locations to collect information without detection. It can also be used in

[1] *Habet Amal, "The Role of the National Body for the Prevention and Combat of ICT-Related Crimes," International Journal of Legal and Political Research, Vol. 5, No. 3, Algeria, 2021, p. 466*

forgery, such as producing counterfeit documents or currency that is nearly impossible to detect due to advanced protective applications.

These crimes represent serious obstacles to state development due to their significant impact on essential state functions.

Information technologies have permeated nearly all aspects of life in both developed and developing countries. Today, IT systems organize transportation, communication, economic transactions, industrial and agricultural inputs, education, healthcare, and even military operations. As a result, crime has evolved: modern criminals now utilize advanced technologies to commit crimes far beyond the traditional scope.

The subject of this research is cybercrimes and their evidentiary challenges—i.e., crimes committed via computers and the Internet.[2]

Perpetrators of cybercrimes may infect computer systems with malicious software to damage or disable them, delete or steal data, or disrupt services. They might also prevent users from accessing websites or networks, or block a software provider from reaching its clients—a tactic known as **Denial-of-Service (DoS) attack**.

Moreover, criminals may use computers to distribute malware, illicit information, or illegal images. Often, they simultaneously use infected devices to propagate viruses across networks. Some jurisdictions also recognize crimes where computers are merely tools used in the offense, such as storing stolen data.

2. Terrorism-Related Crimes

Nanotechnology-related terrorism is perhaps the most alarming due to its multifaceted and highly destructive nature. Examples include:

a. Infrastructure-Based Extortion

Nanotechnology can be used to develop materials capable of causing physical damage to critical infrastructure—such as corroding bridges or destroying industrial pipelines—through methods that are difficult to detect. Criminals may leverage such technologies to extort governments or inflict economic harm.

b. Nano-Weapons

Miniaturized and highly precise weapons developed through nanotechnology can be extremely difficult to detect. Toxic nanoparticles could be used in assassinations or acts of terrorism.

c. Cyber-Terrorism and Advanced Viruses

Nano-enabled computer viruses can become increasingly complex and difficult to detect or eliminate. These may be used to extort corporations or individuals by threatening to compromise or disable their systems.

d. Advanced Concealment and Camouflage

Materials that change color or properties at the nanoscale may be used to disguise individuals or objects, enabling the execution of crimes without detection of the perpetrator or tools involved.

E- Causing Disruptions in Electrical Networks

Nanodevices can be developed to emit electromagnetic signals that affect electrical networks or control systems, leading to power outages or unexpected disturbances. Such disruptions may be exploited by terrorist cells around the world to cause chaos or exert pressure on critical infrastructure.

Subsection Three: Causing Severe Environmental Damage

[2] *Abdul Jabbar Awad and Talib Abbas, "Cybercrimes and Their Proof," Journal of Rafidain for Legal and Political Sciences, Vol. 4, No. 6, Jordan, 2021, p. 421*

The environmental risks of nanotechnology remain poorly understood, primarily due to the extremely limited funding allocated to this area of research. For example, in 2006, the U.S. government spent 33% of the National Nanotechnology Initiative's $1.3 billion budget on military applications, while only $11 million (approximately 0.0085%) was dedicated to research on the health and environmental risks of nanotechnology.

Despite the scarcity of such studies, the few that do exist often yield conflicting and sometimes alarming results. Some preliminary research has shown that certain nanomaterials already widely used in commercial products may pose toxic risks to the environment and human health.

For instance, studies have revealed that fullerene particles (buckyballs) may cause brain damage in fish species commonly used as models for environmental toxicity. Additionally, by-products of the manufacturing of single-walled carbon nanotubes have been found to be lethal to certain types of crustaceans.

The antimicrobial properties of some nanomaterials have raised concerns that nanotechnology might disrupt microbial activities essential to environmental balance, such as nitrogen-fixing bacteria and other beneficial microorganisms. This scenario holds serious ecological implications and significant economic consequences. Further, early studies suggest that plants may be capable of absorbing, modifying, and accumulating nanoparticles, which could then propagate through the food chain.[3]

Subsection Four: Causing Severe Health Hazards

In the early 2000s, scientific studies began to reveal the toxic potential of nanomaterials. Due to their unique properties, nanoparticles may pose significant health risks to humans. As noted by Marc Audétat, a researcher at the Science and Society Department of the University of Lausanne, nanotechnology has been promoted over the past two decades as a scientific revolution with the capacity to enhance production processes and advance electronics, medicine, renewable energy, and agriculture.

However, the risks and uncertainties surrounding this new and tangible technology have prompted the Swiss Consumer Protection Association, in collaboration with the University of Lausanne, to launch awareness campaigns aimed at promoting public discourse on the benefits and drawbacks of nanotechnology. This is particularly important given that the majority of consumers remain unaware of the technology's potential dangers.

Biologist Houma Khamis, an expert in nanotechnology at the Swiss Consumer Protection Association, explained:

"Some materials, when reduced to nanoscale dimensions, exhibit altered properties. For example, titanium dioxide, which is normally used as a white pigment, becomes transparent and acts as a UV filter when reduced to nanoparticles."

While the results of this technology are remarkable and often unpredictable due to the sensitivity of nanoparticles—where even a single additional or missing atom can fundamentally alter their properties—they interact easily with their environment due to their large surface area. Therefore, despite widespread use, research on the health effects of nanotechnology on consumers remains limited. This scarcity of data, combined with growing concerns, was highlighted in a 2004 study by the British Institute, which warned about the dangers of nanotech and called on governments and NGOs to address its potential negative impacts.

As such, before integrating this technology into all sectors—especially those related to consumer health and safety or the surrounding environment—there must be regulatory oversight. Presently, there are no clear or

[3] Brar, S., Verma, M., Tyagi, R., & Surampalli, R. (2009). Nanoparticles. Contaminants of Emerging Environmental Concern, pp. 416–445.

specific regulations addressing the risks associated with nanotechnology. As a result, general principles concerning[4]

In this context, the World Health Organization, civil society organizations, and interested governments have held and continue to hold conferences to examine the latent dangers of nanotechnology. In some respects, this technology may be like "poison in honey." For example, in 2008, the first global conference addressing the health risks of nanotechnology was held in Brussels. The conference concluded that nanotechnology is a double-edged sword. Despite its many advantages, it poses significant and, as of yet, poorly defined threats to human health.

One of the most alarming risks is that nanoparticles with diameters of 300 nanometers or less can easily penetrate the human body and reach cells. Even more concerning is that particles of 70 nanometers or smaller can enter the cell nucleus, potentially causing toxicity or altering cellular function. Due to their tiny size, conventional protective gear—such as masks and respirators—are ineffective in filtering them out.[5]

Subsection Two: Nanotechnology-Related Crimes Affecting Society

Nanotechnology also negatively impacts society through various forms of crime. In this section, we explore several of these criminal implications:

1. Impact on Human Activities

Nanotechnology affects different aspects of human activity in multiple ways:

[See: Abdul Jabbar Awad and Talib Abbas, op. cit., p. 456]

a. Agricultural Disruption:

Nanotech can be used to compromise agricultural productivity, either by reducing crop yields or introducing targeted nanodiseases, which in turn can jeopardize food security.

b. Infiltration of Biological Systems:

Through nanoscale engineering, the biological systems of microorganisms or insects can be targeted—for example, altering insect behavior to become more aggressive or more effective disease vectors.

c. Disease Transmission via Nano-Injection:

Undetectable nanoinjection devices can deliver toxins or viruses to specific individuals, making the crime both hard to detect and nearly impossible to trace back to a perpetrator.

d. Production of Carcinogenic Nanomaterials:

Nanotechnology can be employed to create materials that interfere with biological systems in a way that increases cancer risk among exposed populations.

e. Environmental Nano-Chemical Attacks:

Releasing nanochemicals into the natural environment may lead to excessive pollution or harmful changes, such as groundwater contamination or air toxicity.

f. Memory and Cognitive Manipulation:

Specific nanomaterials may be designed to affect neural cells or neurotransmitters in the brain, enabling illegal manipulation of memory or behavior.

2. Impact on Other Societal Activities

Additional forms of nanotechnology-related crimes affecting society and the state include:

[4] Bouhouia Amal & Omran Aisha, "The Impact of Nanotechnology on Consumer Health and Safety under Algerian Consumer Law," Al-Ustadh Al-Bahith Journal for Legal and Political Studies, Vol. 4, No. 2, Algeria, 2019, pp. 1298–1299.
[5] Mohamed Magdy Wasel, Introduction to Nanoscience, For University Publishing House, Egypt, 2008, p. 45

a. Nano Attacks on Sensory Devices:

Using nanomaterials that interfere with vision or hearing devices, it is possible to disrupt or degrade their performance, impairing individuals' ability to perceive the environment.

b. Manipulation of Artificial Intelligence via Nanodust:

Nanoparticles can be used to infiltrate AI systems or corrupt training data, leading to incorrect outputs or biased decisions in automated systems.

c. Development of Nano-Hacking Tools:

Nano-sized hacking devices can be employed to gain unauthorized access to user data or critical network infrastructure without leaving a detectable trace.

d. Economic Sabotage through Nanotechnology:

Nanotech can alter the physical properties of commercial goods—such as reducing durability or affecting quality—which results in substantial losses for businesses and harms consumer trust. This, in turn, poses a serious threat to economic stability, society, and the individual alike.

Section Two: The Role of Nanotechnology in Criminal Evidence

Nanotechnology is a field that intersects with nearly all branches of science and engineering. With rapid advancements in areas such as molecular electronics, biomolecular motors, and DNA-based self-assembly, the applications of nanotechnology are broad and ever-expanding. The term was first coined in 1974 by Japanese scientist **Norio Taniguchi**, a professor at the Tokyo University of Science, to refer to the precise fabrication of materials at the nanometer scale.

In truth, nanotechnology has many valuable uses in the field of **criminal evidence**, and this section will explore those in detail.

Section I: Forms of Nanotechnology Use in Crime Detection

As nanotechnology evolves and expands into various fields—including materials science, atomic energy, biology, pharmaceuticals, cosmetics, biotechnology, tissue engineering, informatics, IT, environmental protection, agriculture, food safety, and health risks—it has also begun to influence forensic science significantly. Applications of modified nanomaterials in forensic investigation include techniques such as:

- High-Performance Liquid Chromatography (HPLC)
- Scanning Probe Microscopy (SPM)
- Infrared Spectroscopy
- X-ray Photoelectron Spectroscopy (XPS)
- Time-of-Flight Mass Spectrometry (ToF-MS)
- Atomic Force Microscopy (AFM)

These tools have revolutionized forensic science by enabling detection and analysis of evidence at the nanoscale. For instance, nanomaterials such as **gold nanoparticles (Au-NPs)** are used in forensic investigations to reveal fingerprints, footprints, DNA traces, explosive residues (via nanosensors), or even "brainprints" that may store crime-related memories.

These novel properties of nanomaterials significantly aid in the **collection, discovery, and establishment of criminal evidence** through nanotechnology.[6]

[6] *Andan Prasada, Sally Lokusib, Lalit Prasada, "Emerging Forensic Applications in Nanotechnology," International Journal of Engineering and Applied Sciences (IJEAS), Vol. 2, Feb 2016, School of Basic and Applied Sciences, Galgotias University, Greater Noida, Uttar*

Subsection I: Nanotechnology and Forensic Medicine

Forensic medicine is a field dedicated to elucidating medical issues presented before the judiciary. With nanotechnology, the study of forensic materials has shifted to the nanoscale using advanced instruments that can manipulate molecules with extreme precision.[7]

Nanotechnology can be employed in:

- **Estimating time of death**
- **DNA analysis**
- **Fingerprint comparison**
- **Bloodstain pattern analysis**

Technological advancements have expanded the boundaries of what is possible in **detecting and proving criminal acts**, especially in modern, complex crimes. The future promises even greater reliance on nanotechnology, particularly in **reconstructing crime scenes**, **rebuilding atoms and molecules**, and **establishing the identity of suspects** based on the smallest traces of evidence.[8]

Subsection II: Lie Detection Technology in Criminal Evidence

The **polygraph** (lie detector) is a modern scientific tool used in criminal investigations to identify deception. It works on the premise that lying causes unique psychological and physiological responses—such as changes in heart rate, perspiration, and blood pressure—that can be measured via involuntary bodily functions.

While some countries like **Algeria, Poland, Russia, and Norway** prohibit its use, others such as **Sweden** permit it, though only in criminal matters and under specific conditions.

Legal scholars have long debated the **legitimacy of polygraph results** in criminal cases, with opinions ranging from strong opposition to cautious acceptance. Algerian jurisprudence largely rejects the use of polygraphs, citing concerns over **violations of the defendant's rights**, including the **right to remain silent** and **freedom of defense**.

Compelling a defendant to undergo polygraph testing without consent renders the process invalid. Courts in **France and the UK**, along with international treaties and conferences—such as the **European Scientific Section in Brussels, 1951**—have emphasized the **inadmissibility of coercion and the importance of protecting human rights**.

According to Interpol's Mr. Roeck, member states are warned against the use of lie detectors, especially if they involve psychological pressure or physical coercion. However, he notes that polygraphs may be used **under two conditions**:

1- The defendant's voluntary consent

2- The results are not used as direct evidence of guilt[9]

Section II: Evidentiary Value of Nano-Based Evidence

The admissibility of nanotechnology-derived evidence has sparked **significant debate** among legal scholars and across legal systems. Jurisdictions that do recognize such evidence typically do so within the framework of **judicial discretion**.

Pradesh, India, p. 7

[7] *Jadoui Sidi Mohamed Amin, "Nanotechnology and Its Role in Criminal Evidence," Eliza Journal for Legal and Political Research, Vol. 8, No. 1, Algeria, 2023, p. 172*

[8] *Omar Abdel-Majid Musbah, "The Role of Bloodstains in Crime Detection Using Nanotechnology," Arab Journal of Security Studies, Vol. 30, No. 61, Saudi Arabia, 2014, p. 35*

[9] *Jadoui Sidi Mohamed Amin, op.cit pp. 174-175*

Subsection I: Judicial Discretion in Evidence Evaluation

In criminal proceedings, the **principle of the judge's personal conviction** governs the evaluation of evidence. This principle results in two key outcomes:

1- The judge is free to accept any form of evidence, unless otherwise restricted by law

2- The judge has absolute authority to weigh the credibility and sufficiency of the evidence presented

However, such conviction must be based on **certainty and logical coherence**—the evidence must be consistent, complete, and free of contradiction. The judge must examine all elements thoroughly.

Algerian legislation affirms this principle in **Article 212(1) of the Code of Criminal Procedure**, which states:

"Crimes may be proven by any means of evidence, except in cases where the law provides otherwise. The judge may issue a ruling based on his personal conviction."

Thus, Algerian law, in line with other legal systems, subjects all evidence—including that derived from nanotechnology—to the judge's discretionary evaluation.[10]

Subsection II: Limitations of Judicial Discretion

Despite the general rule, there are several important exceptions where judicial discretion is restricted:

1- **Adultery Offenses:**

Under Algerian law, adultery can only be proven by (a) a flagrante delicto report by judicial police, (b) the accused's confession, or (c) judicial admission. Therefore, nanotechnology-based evidence is **inadmissible** in such cases.

2- **Non-Criminal Matters:**

When a criminal ruling depends on determining a **civil issue** (e.g., establishing a contractual relationship), the judge must follow **civil evidentiary rules**, not the general rules of criminal procedure.

3- **Exclusion of Certain Evidence:**

Some forms of evidence are **inadmissible** in criminal cases if they violate the defendant's right to a fair trial. For example, a letter sent by the accused to their lawyer admitting guilt **cannot** be used as evidence, as it breaches attorney-client confidentiality.

4- **Evidentiary Weight of Official Reports:**

According to **Article 218 of the Code of Criminal Procedure**, some official reports have **probative value unless falsified**, such as **customs reports** or those by **commercial inspectors**, which are regulated by special laws

Conclusion

Nanotechnology is a **double-edged sword**—it offers immense benefits to society and the world at large, especially in **solving complex issues**. At the same time, it poses serious risks and has the potential to enable crimes on a global scale.

Among its most notable contributions is in the field of **criminal evidence**, where it has revolutionized the **detection and proof of crimes**, particularly in areas that were previously difficult or impossible to investigate—such as **environmental crimes**. Thus, nanotechnology holds a pivotal place in modern criminal justice, demanding careful regulation and ethical oversight.

[10] *adoui Sidi Mohamed Amin, op.cit pp.176*

Bibliography:

1- Bouhouia, Amal, and Aicha Omrane. *The Impact of Nanotechnology Use on Consumer Health and Safety in Algerian Consumer Law*. Journal of the Research Professor for Legal and Political Studies 4, no. 2 (2019). Algeria.

2- Brar, Satinder, Manish Verma, R. D. Tyagi, and R. Y. Surampalli. "Nanoparticles." In *Contaminants of Emerging Environmental Concern*, 2009

3- Habet, Amal. *The Role of the National Authority for the Prevention and Combat of ICT-Related Crimes in Facing Cybercrimes*. International Journal of Legal and Political Research 5, no. 3 (2021). Algeria.

4- Jadoui, Sidi Mohamed Amin. *Nanotechnology and Its Role in Criminal Evidence*. Eliza Journal for Research and Studies 8, no. 1 (2023). Algeria.

5- Masbah, Omar Abdelmajid. *The Role of Bloodstains in the Detection and Proof of Crimes through Nanotechnology*. Arab Journal of Security Studies 30, no. 61 (2014). Saudi Arabia.

6- Owad, Abdul Jabbar, and Taleb Abbas. *Cybercrimes and Their Proof*. Rafidain Journal of Legal and Political Sciences 4, no. 6 (2021). Jordan.

7- Prasada, Andan, Sally Lukoseeb, and Lalit Prasada. *Emerging Forensic Applications in Nanotechnology*. International Journal of Engineering and Applied Sciences (IJEAS) 2 (February 2016). Galgotias University, Greater Noida, Uttar Pradesh, India.

8- Wasel, Mohamed Magdy. *Introduction to Nanoscience*. Cairo: Four University Publishing, 2008. Egypt.