International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 22-02-2026, Accepted: 25-03-2026, Published: 09-04-2026
Volume 12, Issue 2, 2026, Page No. 47-51

A critical analysis of the effectiveness of the wildlife (Protection) Act, 1972 in addressing online wildlife trafficking in India

Himadri Puri[1], Dr. Avantika Madhesiya[2]
[1] Department of Law, Amity University, Noida, Uttar Pradesh, India
[2] Assistant Professor, Amity University, Noida, Uttar Pradesh, India

Abstract
The Wildlife (Protection) Act, 1972 [1], has been the primary legislative instrument for wildlife protection in India. The main objective of the Act is to protect animals from being killed or captured by providing protection measures for endangered species, controlling poaching, and regulating hunting and trading practices. Although the law has been quite effective in dealing with the traditional forms of crimes against wildlife, its application to technologically advanced crimes like cyber-based wildlife crimes remains problematic. Therefore, this paper will explore the relevance of the Wildlife (Protection) Act, 1972, to online wildlife trafficking [2].

The paper will provide an analysis of the legislative measures outlined under the Wildlife (Protection) Act, 1972, and evaluate their effectiveness in tackling the emerging cyber-based wildlife crimes. It will also focus on the involvement of the enforcement agencies in combating the networks of online wildlife traffickers and investigate the interaction between the law enforcement officers and intermediaries in the online space. Using the cases and enforcement data from recent years, this paper will demonstrate the effectiveness of the Wildlife (Protection) Act, 1972, and explore other sources of law enforcement powers.

"The Wildlife (Protection) Act, 1972, though effective in regulating traditional wildlife crimes, lacks adequate provisions to address the emerging threat of online wildlife trafficking, necessitating urgent legal reforms and integration with cyber laws".

Keywords: Wildlife Protection Act, online wildlife trafficking, cybercrime, environmental law, legal gaps, digital wildlife trade

Introduction

Wildlife poaching remains one of the gravest threats faced by India when it comes to the issue of biodiversity. This threat poses great risks for endangered species, including tigers, elephants, pangolins, and exotic birds. The practice involves the unlawful killing, poaching, transporting, and trading of wildlife and their derivatives, including their hides, ivory, bones, and medicines. India, among some of the world's megadiverse countries, is especially vulnerable because of its diverse flora and fauna and geographic position in regard to wildlife crime. Even though the country has established strong laws against wildlife crime, these crimes remain rampant.

Historically, wildlife trafficking in India took place at physical markets and involved crossborder and secret domestic transactions. However, with the rise of modern technology, the use of the Internet for illegal wildlife trafficking has increased drastically. Wildlife traffickers utilize Social media sites like Facebook and Instagram [3], messaging applications such as WhatsApp, ecommerce websites, and the dark net to sell illegal wildlife products.

The main statute that protects wildlife in India is the Wildlife (Protection) Act, 1972. The law aims at securing the protection of wildlife in order to preserve ecological balance. The Act allows for restrictions on hunting and wildlife trade, creation of designated reserves like national parks and wildlife sanctuaries, as well as imposition of penalties. Amendments to this Act have made it an essential tool in wildlife conservation.

But the Act was passed during a period when wildlife crimes were physically committed on a very small scale. There are no specific clauses in this law dealing with cybercrimes involving wildlife trading activities. Definitions are not clearly given about wildlife crimes committed through cyberspace, there are no adequate provisions for digital surveillance, there are questions regarding territorial jurisdiction, and most importantly, no coordination has been made between the wildlife crime enforcement officials and cybercrime agencies. Other Acts, such as the Information Technology Act of 2000 [4], can be used in some instances [5].

Concept of Online Wildlife Trafficking

Meaning and scope

Online wildlife trafficking can be described as the unlawful movement of wild animals, plants, and their parts through online portals [6]. Online wildlife trafficking is an example of a growing phenomenon of the use of cyberspace in committing crimes against the environment. While traditional wildlife trafficking involves the use of physical space in carrying out trade in protected wildlife, online wildlife trafficking takes place through the virtual world, making it harder to monitor.

Online wildlife trafficking covers a wide range of practices. Posting ads about endangered animals available for sale, holding auctions, communicating with clients using encryption software, and making arrangements for shipment using courier companies are some of the practices involved in online wildlife trafficking. It involves international cooperation since the Internet gives criminals unrestricted access to buyers worldwide regardless of geographical constraints.

Platforms used

1. Social Media Networks

The rise of social media has led to increased use of online networks such as Facebook and Instagram for advertising animals available for sale. Wildlife traffickers utilize the internet's anonymity and encrypted features by using private chat rooms or using code words for the animals, such as "rare pets" instead of endangered species.

2. Encrypted Messaging Services

Encryption services in messaging applications such as WhatsApp and Telegram allow traffickers to communicate without fear of being intercepted by the police since the information is shared using an end-to-end encryption process [7].

3. Online Auction Websites and Other E-commerce Websites

Illegal trade also takes place through other websites that offer e-commerce or classified ads. This allows traffickers to advertise their items through classified listings where they may not necessarily follow the guidelines provided by the company, allowing them to get away with trading.

Kinds of Wildlife That Are Sold

Wildlife trafficking online covers a broad range of wildlife that includes the following:

Birds: Parrots, macaws, owls, and other rare and endangered birds are commonly traded for ornamental purposes and as exotic pets.

Reptiles: Turtles, snakes, and lizards are usually trafficked not only for their use as exotic pets but also for the purpose of their skins.

Exotic Pets: Rare animals and even primates like monkeys and hedgehogs are sold as exotic pets.

Animal Products and Derivatives: Examples include products such as elephant ivory, tiger bones, rhino horns, and pangolin scales.

Legal Framework in India

1. Wildlife (Protection) Act, 1972

The Wildlife (Protection) Act, 1972 [8], is the key law dealing with the conservation and protection of wildlife in India. The Act contains provisions for:

1. Restrictions on hunting of species mentioned in specific Schedules
2. Control and restrictions on trade in wildlife and their products
3. Creation of protected zones like national parks and wildlife sanctuaries
4. Penalties for wildlife offences

Under the Act, certain species are categorized into various schedules, where Schedules I and II afford the most stringent protections. The Act makes it an offence to possess, sell, or transport wildlife items without the necessary permits.

Nevertheless, the Act predates the emergence of cyberspace and does not mention wildlife trafficking on the Internet. The law does not contain any measures concerning cyber investigation, surveillance, and liability of cyber intermediaries.

2. Information Technology Act, 2000

The Information Technology Act, 2000 [9], acts as the main legislative instrument for regulating cyberspace in India. Although it does not specifically deal with wildlife crimes, it can still be applied in some ways:

1. Regulating electronic documents and communications
2. Providing penal sanctions for cybercrimes such as identity theft and hacking
3. Imposing intermediary liability as provided under Section 79 [10], which requires intermediaries to take due diligence

Where there is online trafficking of wildlife products, this Act may serve as a support to the Wildlife Protection Act since it deals with the cyber aspect of the crime. The application of this law is difficult since it lacks provisions concerning environmental crimes.

3. Functioning of Wildlife Crime Control Bureau (WCCB)

The Wildlife Crime Control Bureau [11] is a statutory authority set up under the Ministry of Environment, Forests, and Climate Change in order to fight against organized crimes in the wildlife sector. The primary responsibilities of this bureau include:

1. Gathering and sharing information concerning wildlife crime cases
2. Coordination among the concerned agencies, such as the police, customs authorities, and forest officers
3. Developing the capacity of officers for law enforcement relating to wildlife crimes
4. assisting in investigating and prosecuting wildlife offenses

In regard to cybercrimes relating to wildlife crimes, WCCB has been involved in monitoring cyber activities along with collaborating with other cybercrime cells. Yet, the capabilities of this bureau are hampered by the absence of sufficient technology and expertise in cybercrimes.

4. International Legal Mechanism: CITES

In the international arena, India is one of the signatories to the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) [12]. The convention seeks to ensure that international trade in endangered species will not lead to the endangerment of their existence through:

1. Lists of different categories of protected animals
2. System of permits and certificates in the trade of such animals.
3. International cooperation among signatory countries

Though CITES offers an international legal mechanism to control cross-border trade in wildlife, it lacks an effective enforcement strategy since it relies on national legal mechanisms. Regarding the online wildlife trade, the lack of uniform international digital enforcement standards poses a serious problem.

Legal Gaps in the Wildlife (Protection) Act, 1972

1. No Specific Provision for Online Crimes

The Wildlife (Protection) Act, 1972 [13], was formulated during an era where wildlife crimes were primarily physical, including acts of hunting, poaching, and trafficking wildlife

animals via traditional means, through local markets and border smuggling routes. Hence, the existing provisions cater to more traditional types of wildlife crime and cannot provide enough coverage in view of technological developments.

One major deficiency of the Act pertains to the lack of provisions for online wildlife crimes. The Act has not made any attempt to address any wildlife offences that may be committed on the Internet, including online advertisements or digital trading. It becomes necessary for the authorities to use their discretion to extend the scope of certain provisions in order to make them applicable to online cases. However, in doing so, the enforcement of such provisions will lack a definite approach due to the ambiguous nature of the provisions in question.

Another problem with the Act is that important terms that need to be defined with regard to cybercrime and other related offences are missing from the text. For example, no definition has been provided for 'electronic trade,' 'online intermediaries,' or 'digital platforms.'

2. Jurisdictional Issues

Among the various constraints faced in curbing the problem of online wildlife trafficking under the Wildlife (Protection) Act, 1972, the problem of jurisdiction stands out. The reason being unlike conventional wildlife crimes, online wildlife trafficking extends beyond a particular territorial boundary and hence becomes very difficult to prosecute.

This is because online wildlife trafficking usually entails the involvement of individuals operating from different territorial locations, where a seller operates from one place while a buyer operates from another, and even the web page used might be from a foreign jurisdiction [14]. At times, wildlife trade takes place using digital means across international borders, where wildlife products are sourced from one country and delivered to another. However, there are no clear provisions in the Act that cater to the handling of such crimes.

Another problem related to online wildlife trafficking is the identification of the offender. Individuals involved in these crimes often adopt anonymous names when conducting business. In addition, they use encrypted means of communication as well as virtual private networks, making it extremely difficult to pinpoint the individual responsible as well as the jurisdiction of the crime.

3. Weak Enforcement Mechanisms

Weak enforcement measures form another critical limitation when attempting to combat online wildlife trafficking under the Wildlife (Protection) Act, 1972. The problem arises owing to the rapid pace at which technology is advancing.

One of the challenges facing law enforcement agencies is a deficiency in their cyber capacity. Authorities responsible for enforcing the Wildlife (Protection) Act, 1972, are typically welltrained to handle crimes committed physically, such as poaching and illegal transport. Conversely, dealing with wildlife crime on the internet demands particular capabilities like digital surveillance, cyber forensics, analytics, and financial transaction tracking. Lack of adequate personnel with the requisite cyber skills makes it challenging to detect any dubious online actions, especially within encrypted messages, social media networks, and online marketplaces. Online traffickers usually adopt sophisticated tactics like coding language, disposable accounts, and encrypted channels, making it even harder to investigate and apprehend them. Additionally, there is an inadequacy in the necessary technological infrastructure and instruments that enable cyber monitoring of online wildlife crimes. Conventional approaches, adopted by wildlife authorities, are inadequate when dealing with cases.

This skill and resource deficit has made it challenging to detect online crimes, investigate them promptly, and secure convictions [15].

4. Lack of Platform Accountability

One major loophole in the implementation of the Wildlife (Protection) Act, 1972, is the lack of provisions providing for the accountability of digital intermediaries facilitating the sale of endangered animals or animal products online.

Facebook, Instagram, WhatsApp, and other similar social media websites have been reported to operate as intermediaries in cases where illegal online wildlife trafficking is carried out. Nevertheless, the provisions of the Act do not address the issue of regulating these digital intermediaries [16].

Therefore, the digital intermediaries are left to be regulated under the intermediary liability provisions of Section 79 of the IT Act of 2000 [17], which stipulates that an intermediary shall enjoy conditional immunity from legal liabilities if they exercise due diligence. This regulation applies only partially as it is not tailored to meet the requirements of tackling wildlife crime.

The lack of statutory regulation causes delays in the removal of illegal wildlife content, poor monitoring, and a lack of cooperation with law enforcement, among others.

Additionally, most digital intermediaries depend on users to report illegal acts, which allows for wildlife traffickers to conduct themselves without fear of being caught through the use of private accounts, coded language, etc.

The bottom line is that the lack of direct liability placed upon intermediaries in cyberspace greatly undermines the ability of wildlife law enforcement. It is imperative that there be legal changes made to ensure responsibilities are clarified, compliance is enforced, and collaboration takes place between intermediaries and wildlife law enforcement agencies.

5. Difficulty in Evidence Collection

Further challenges that have arisen due to the increasing use of cyberspace by wildlife traffickers include the challenge of collecting and preserving digital evidence for the implementation of the Wildlife (Protection) Act, 1972.

Unlike physical forms of evidence, digital evidence is very volatile and prone to alteration. Cyber traffickers can easily remove messages, photos, transactions, or even delete their profiles on platforms like WhatsApp, Telegram, and Instagram, creating a minimal digital trail for the investigators. Several platforms, such as Telegram, even come with an option of deleting messages after use and encrypted messages, thus making it even more challenging for investigators to collect evidence [18].

The other challenge is the use of techniques like setting up fake identities, temporary email IDs, and even a Virtual Private Network to hide one's identity from the authorities.

The Act itself does not lay down any guidelines or processes regarding the collection and handling of such digital evidence. While the Information Technology Act and the

Evidence laws can help in some cases, their application in the case of wildlife offences is rather unorganized.
This is because the following problems are encountered:

1. Loss of vital pieces of evidence.
2. Problems in ensuring that the evidence is authentic and can be admitted in court.
3. Time wastage owing to reliance on platform cooperation and data extraction.

Such obstacles greatly hinder prosecutions, leading to low conviction rates. The absence of efficient means of collecting and preserving digital evidence poses a great challenge in law enforcement.

Practical Challenges

Despite the presence of laws like the Wildlife (Protection) Act, 1972, and the Information Technology Act, 2000, there are numerous practical issues that stand as barriers to the regulation of online wildlife trafficking in India.

1. Use of Encrypted Platforms

The first major problem is the growing trend towards using secure messaging applications like WhatsApp and Telegram. Such messaging applications employ end-to-end encryption, which means that only the communicating individuals have access to the messages sent and received. Although the end-to-end encryption feature adds an extra layer of security, it also makes it hard for the authorities to detect any illegal activities related to wildlife trafficking.
Illegal traffickers take advantage of private chat groups, message deletion, and other similar aspects of these encrypted apps.

2. Anonymous Transactions

Anonymous means of doing business are another way in which online wildlife poaching is made easier. The offenders may use fabricated names, aliases, and untraceable means of payment, such as digital currency and e-wallets. This helps the offenders evade detection since the transactional trails are blurred.
The anonymity of the transactions means that it becomes harder to pin suspects to the illegal operations.

3. Incoordination of Different Authorities

Coordination among different authorities plays a major role in ensuring effective law enforcement. Coordination among cybercrime cells, the Forest Department, and the Wildlife Crime Control Bureau is important in dealing with online wildlife trafficking.
However, there exists inadequate coordination and cooperation among the agencies. While the cyber specialists may not be conversant with wildlife legislation, the forestry officials are not equipped with cybercrime investigative skills.

4. Limited Awareness on the Part of Enforcement Agents

A fourth challenge that is associated with combating online trafficking is limited awareness on the part of enforcement agents about online trafficking of wildlife. This is because many agents tend to be knowledgeable about traditional forms of wildlife trafficking and may be unable to detect and pursue offenses that take place online.
Limited awareness includes:

1. Detection of online activities
2. Cyber tools and knowledge
3. Accessing data from online platforms

Case Studies

1. Online sale of exotic birds and reptiles

There have been several cases reported where exotic animals like parrots, macaws, turtles, and snakes are sold online. Sellers post pictures and videos of animals in question and try to sell them under the name of 'rare pets'.
As far as the Indian star tortoise is concerned, it was reported that there were several cases where these rare species were sold using various online classifieds and social networking sites. Also, there have been many cases where exotic birds like African grey parrots and macaws are sold despite the ban on such activities.
One of the landmark judicial cases related to wildlife trafficking is "Sansar Chand v. State of Rajasthan" [19], where the Supreme Court acknowledged the existence of wildlife trafficking as an organized crime. In this case, although the court dealt with the problem of poaching and did not address the issue of wildlife trafficking via the internet, the principle can easily be extended to the modern scenario of wildlife trafficking.
Another landmark case in which the court advocated for strict interpretation and enforcement of wildlife protection laws is "State of Bihar v. Murad Ali Khan" [20].

2. Social media wildlife trade networks

Facebook and Instagram are some of the social media websites that have become primary sources for the illegal trade of wildlife products. Cases have been reported wherein there were organized systems where:

1. The sellers would keep on posting wildlife items for sale.
2. The buyers would discuss the price using direct messaging.
3. The deals would be finalized using encrypted messaging applications such as WhatsApp and Telegram.

These types of systems often span across states and countries, which makes their regulation difficult.
In the case of People for Animals v. Union of India [21], the judiciary has highlighted concerns about wildlife trade, which includes the use of modern modes for trading animals illegally.

3. Reports by TRAFFIC and WWF

Reports published by TRAFFIC [22] and the Worldwide Fund for Nature (WWF) [23] contain factual information regarding the magnitude and trends related to online wildlife trafficking. These include the following:

1. Increased wildlife trade through online platforms
2. High market demand for exotic pets such as birds and reptiles
3. Wide-scale use of social media and e-commerce websites
4. Minimal monitoring and implementation of regulations

For example, reports compiled by TRAFFIC have revealed several thousand advertisements about live animals and wildlife products offered through the internet in India and Southeast Asia.

Furthermore, judicial endorsement of wildlife conservation initiatives may be evident in the case of Centre for Environmental Law, WWF-India v. Union of India [24], wherein the apex court reiterated the significance of protecting endangered species.

Comparative Perspective

An examination of international approaches shows that many nations have been more aggressive than India in dealing with wildlife trafficking online, especially through combining wildlife legislation with cyber laws.

1. Approach in the United Kingdom

The approach used in the United Kingdom has become one that takes into consideration new technological trends and is more advanced in addressing online wildlife crime. The laws for wildlife protection, such as the COTES, are supported by adequate and strong cybercrime strategies and enforcement policies.

The authorities of the UK have been monitoring online activities that involve illegal trade in wildlife and also cooperate with the tech giants to detect illegal activities and take them down. Special enforcement groups coordinate their efforts with cybercrime specialists to trace criminals who use online services to perform their activities.

Furthermore, the UK has been participating in global campaigns like the Coalition to End Wildlife Trafficking Online, which involves cooperation between governments, NGOs, and technology companies in tackling online wildlife trade.

2. Regulating Platforms and Ensuring Accountability

Another major strength of the UK model is the regulation of the platforms and ensuring accountability of the platforms in their activities. Social media and online e-commerce platforms need to do the following:

1. Create rigorous content management systems
2. Deploy AI software for the detection of suspicious listings
3. Formulate policies that prohibit wildlife trade
4. Work in tandem with law enforcement agencies

The platforms need to act immediately to ensure the deletion of the content and block the accounts of the users who post it. The Indian model does not regulate the platforms, as its accountability laws fall under the provisions of the IT Act of 2000.

3. Stronger Cyber Laws and Law Enforcement

Additionally, the UK is fortunate enough to have stronger laws concerning cybercrime in place, such as the Computer Misuse Act 1990, which, though not specifically applicable to wildlife crime, forms a good legal framework for dealing with crimes conducted via cyberspace.

In addition, law enforcement agencies within the UK have access to sophisticated cyber forensics tools, as well as trained personnel to use them. This makes it easier for them to handle cases involving cybercrime.

Conclusion

Cybercrimes related to wildlife trafficking have become one of the significant threats to conservation efforts in the field of wildlife, making use of cyber technology to facilitate such acts. Online marketplaces have added anonymity, organization, and sophistication to the crimes and are challenging traditional law enforcement systems in detecting and preventing them.

Whereas the Wildlife (Protection) Act, 1972 [25], has proved to be a strong legislation for protecting wildlife in India, its provisions fail to meet the needs of the present era. The lack of specific provisions on online offenses, inadequate jurisdiction, ineffective law enforcement mechanisms, and other issues limit the scope of the act. However, some additional laws like the Information Technology Act, 2000 [26], can assist in tackling cyber-related crimes, but not completely in the case of wildlife offenses.

Thus, certain measures should be taken to tackle online wildlife crimes. This would include making specific provisions for such offenses, building the cyber capabilities of enforcement agencies, bringing digital platforms under scrutiny, and fostering cooperation between nations for the purpose. Reports such as those by UNODC [27] and FATF [28] highlight the increasing role of online platforms in wildlife trafficking.

In order to cope with online wildlife trafficking, the adoption of appropriate legal and technological measures is indispensable.

References

1. Wildlife (Protection) Act, 1972, No. 53 of 1972, INDIA CODE.
2. Kumar, A: Environmental Law in India (2nd edition), 2020, 112.
3. Id
4. Information Technology Act, 2000, No. 21 of 2000, INDIA CODE.
5. Singh, M: Cyber Law in India (3rd edition), 2021, 87.
6. TRAFFIC, Wildlife Trade Reports.
7. INTERPOL, Cyber-enabled Wildlife Crime Reports.
8. Id
9. Id
10. Information Technology Act, 2000, S. 79.
11. Wildlife Crime Control Bureau, Ministry of Environment, Forest and Climate Change, Government of India.
12. Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES), Mar. 3, 1973.
13. Id
14. UN Convention against Transnational Organized Crime, 2000.
15. Ministry of Environment, Forest and Climate Change, Annual Reports.
16. IT (Intermediary Guidelines) Rules, 2021.
17. IT ACT,2000 S.79
18. Indian Evidence Act, 1872, S.65B.
19. Sansar Chand v. State of Rajasthan, 10 SCC 604 (India), 2010.
20. State of Bihar v. Murad Ali Khan, 4 SCC 655 (India), 1988.
21. People for Animals v. Union of India, Delhi High Court.
22. TRAFFIC, Wildlife Trade Monitoring Reports.
23. World Wide Fund for Nature (WWF), Wildlife Trade Reports.
24. Centre for Environmental Law, WWF-India v. Union of India, 8 SCC 234 (India), 2013.
25. Id
26. Id
27. United Nations Office on Drugs and Crime (UNODC), World Wildlife Crime Report, 2020.
28. Financial Action Task Force (FATF), Wildlife Crime and Money Laundering, 2020, 18.