Environmental Deception in Cyber-Enabled Wildlife Trafficking: A Comparative Legal Analysis

Charu Bhatt[1], Dr. Tanvi Yadav[2]
[1] PhD Scholar National Forensic Sciences University; charu.phdlaw2386@nfsu.ac.in; 8800939196
[1] Assistant Professor, National Forensic Sciences University Delhi Campus;
tanvi.yadav_dc@nfsu.ac.in

Abstract
Wildlife trafficking has also 'gone digital' and today, online markets, social media platforms, encrypted communications and electronic payments are used to trade wildlife and wildlife products across borders, often without the buyer's knowledge. Although cyber wildlife trafficking has been a focus of existing scholarship, and the use of digital technologies in wildlife trafficking has been discussed, fewer researchers have focused on the legal and regulatory difficulties created by environmental deception in cyber wildlife trafficking networks.
The article reviews the phenomenon of 'environmental deception' in wildlife trafficking in the context of Wildlife Trafficking and compares the legal frameworks in India, the United States and the United Kingdom. By using a doctrinal and comparative legal approach, the study examines the ability of current wildlife protection and cybercrime laws to create tools to tackle digitally mediated wildlife trafficking. It discusses the typology of environmental deception in relation to species misrepresentation, origin laundering, documentation fraud, digital concealment and legitimacy laundering, and how these deceptions leverage regulatory fragmentation between jurisdictions.
The analysis reveals that the three jurisdictions have laws that criminalise wildlife trafficking, but the current laws are largely focused on the traditional trafficking model and are poorly designed for the digital wildlife market environment. These differences in regulatory effectiveness are more due to the differences in the institutional coordination, digital investigative capacity and enforcement mechanisms, than to the legislative prohibition itself. The article contends that it is a big problem for today's environmental governance and that the environmental protection law needs to be more integrated with the regulation of cybercrime and transnational cooperation for its enforcement in this area.
Keywords: **Cyber-enabled wildlife trafficking; Environmental deception; Wildlife crime; Environmental governance; Digital wildlife markets**

Introduction
Trafficking in wildlife is a well established form of transnational environmental crime, which has substantial ecological, economic and governance impacts, both within and beyond borders.[3] Trafficking in protected species and wildlife products aggravates biodiversity loss, species depletion, ecosystem disruption and loss of international conservation efforts. Wildlife trafficking has traditionally been linked to physical wildlife trafficking lines, black markets and organised criminal networks that function along the lines of geographically identifiable routes.[4] Over the past few years, however, the infiltration of digital technologies into the field of illegal wildlife traffickers has reshaped the nature of wildlife trafficking, allowing it to be carried out via online platforms, encrypted communications, digital currency and transnational networks much further afield of traditional territorial limits.[5]

[3] UNODC, World Wildlife Crime Report 2024
[4] Sollund, The Crimes of Wildlife Trafficking (2019); Wyatt, Wildlife Trafficking (2013)
[5] Lavorgna, 'Wildlife Trafficking in the Internet Age' (2014) 3 Crime Science 5

Wildlife trafficking has taken to the internet, changing the way and the manner in which this illegal trade takes place.[6] Social media, online marketplaces, encrypted messaging applications, and cryptocurrency, payment systems enable the promotion, negotiation, and sale of wildlife products with limited visibility to regulatory bodies.[7] These technologies allow traffickers to link suppliers and consumers between jurisdictions and to evade many of the logistical and surveillance barriers that are inherent in traditional trafficking networks.[8] As a result, the trafficking of wildlife has become part of technologically driven commercial networks, breaking with traditional environmental governance and enforcement methods.

This digital revolution has also given birth to a related phenomenon that is the focus of this article: environmental deception. Environmental deception - the use of deceptive practices and digital technologies that conceal, misrepresent or legitimate unlawful source, status, ownership or trade of wildlife and wildlife products.[9] This can involve falsified permits, fake captive-breeding status claims, forged provenance documentation, misleading online listings, digital manipulation of images and more.[10] These practices have hindered species identification, made transactions with the species unclear and weakening the effectiveness of frameworks for protecting wildlife.[11]Traditionally, wildlife laws have been geared towards the actual possession, transportation, and trade of wildlife specimens, but they may be less well suited to the technologically mediated modes of deception that take place in digital environments.[12]

The rise of wildlife trafficking using cyber technology presents the broader challenge of regulatory nexus between environmental and cyber regulations. While the existing wildlife protection laws have addressed poaching, trafficking, illegal trade in physical form, the cybercrime laws will generally be in respect of offences of unauthorised access, fraud, identity theft, computer misuse etc.[13] This means that digitally mediated wildlife trafficking often crosses regulatory jurisdictions, and there is a lack of specific attention given to it in either the wildlife or cybercrime law.[14] Gaps in governance are evident, and enforcement is increasingly hampered by issues of intermediary liability, digital evidence, encrypted communications and cryptocurrency transactions, platform accountability and cross-border jurisdiction.[15]

While the study of wildlife trafficking, online wildlife trade, cybercrime and digital governance have been explored, the topics have largely been explored separately.[16] Research has established that digital platforms have been increasingly utilized in wildlife trafficking and that technologies are being used in the detection and monitoring of wildlife trafficking.[17] There has been, however, comparatively little research that focuses on the interplay between wildlife protection law and cybercrime regulation, the regulation of environmental deception in digital wildlife markets, and the extent to which current law is effective at meeting the challenges of technologically enabled wildlife crime.[18] Furthermore, comparative legal studies on the different approaches to the legal regulation of cyber-enabled wildlife trafficking are still largely undeveloped.

This article aims to fill these gaps by a comparative legal analysis of the regulatory measures in response to the wildlife trafficking via cyber in India, the United States and the United Kingdom. It explores how digital technologies are changing the nature of wildlife trafficking, reviews the ways in which wildlife is

[6] Lavorgna (2014); UNODC World Wildlife Crime Report 2024
[7] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); IFAW, 'Digital Markets: Wildlife Trafficking Hidden in Plain Sight' (2021)
[8] Lavorgna (2014); Wingard and Pascual, 'Catch Me If You Can' (2018)
[9] As defined and developed in this article
[10] Wingard and Pascual, 'Catch Me If You Can' (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[11] UNODC, World Wildlife Crime Report 2024; IFAW, 'Digital Markets' (2021)
[12] Wingard and Pascual (2018); Singh Tomar, 'A Legal Analysis of Cyber-Enabled Wildlife Offences in India' (2024)
[13] Wingard and Pascual (2018); for India specifically: Singh Tomar (2024); for UK: Crown Prosecution Service, 'Wildlife Offences' (2022)
[14] Wingard and Pascual (2018); UNODC World Wildlife Crime Report 2024
[15] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); Eurojust/SIRIUS, 'Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence' (2024)
[16] Lavorgna (2014)
[17] TRAFFIC, 'Wildlife Cybercrime in Asia'; IFAW, 'Digital Markets' (2021); UNODC World Wildlife Crime Report 2024
[18] Wingard and Pascual (2018)

deceived by technology, and discusses the capabilities of current laws and policies to address technology-facilitated wildlife crime. Special focus is given to intermediary liability, digital evidence, platform governance, cross-border enforcement and regulatory coordination.

There are three main findings from the analysis. First, while all three jurisdictions have laws against the illegal trade in wildlife, neither jurisdiction has a specific law targeting wildlife trafficking via the internet. Second, it is easier to achieve regulatory effectiveness with coordination of the institutions than with legislation.Second, regulatory effectiveness is less dependent on legislation than on institutional coordination, ICT and investigative capabilities, and enforcement mechanisms. Third, Internet platforms, encrypted communications, transnational digital networks continue to reveal some weaknesses of the law, which was mostly conceived for traditional wildlife trafficking.

It is argued that cyber-enabled wildlife trafficking creates a huge challenge for current environmental governance, as it allows environmental damage to be organised, hidden, and facilitated via digital environments which operate across the borders of conventional regulatory frameworks. A more integrated approach is needed to address these issues across the three legal frameworks (wildlife protection law, digital governance, cybercrime regulation and transnational enforcement cooperation).

The rest of the paper is organized as follows. Part II lays the groundwork by developing the conceptual framework of cyber-enabled wildlife trafficking and environmental deception. The digital architecture of wildlife trafficking networks is explored in Part III. The comparative analysis of the regulatory frameworks in India, U.S. and U.K. is covered in Part IV. Digital evidence and enforcement challenges are assessed in Part V. Regulatory and policy responses are proposed in Part VI, with a conclusion in Part VII.

2. Conceptualizing Cyber-Enabled Wildlife Trafficking and Environmental Deception

2.1 Cyber-Enabled Wildlife Trafficking: Expanding the Dimensions of Environmental Crime

Trafficking in wildlife has long been recognised as a common form of transnational environmental crime which involves the illegal trade in protected wildlife species, including their hunting, transportation, possession and trade.[19] The major trafficking trends of History were mostly along geographical lines, physical markets and masked trafficking corridors.[20] With the introduction of digital technologies, however, the nature of wildlife trafficking has also changed dramatically, with criminals now utilising online communication platforms, digital markets, encrypted platforms and anonymous financial technologies.[21] This has made wildlife trafficking more technologically-driven and border-crossing, beyond the scope of conventional border controls.[22]

Cyber-enabled wildlife trafficking refers to any form of wildlife trafficking that utilizes digital technologies and online platforms and infrastructures as part of the wildlife trafficking chain, such as for advertising, communicating, paying, coordinating transportation and hiding identities. Digital wildlife trafficking is different from traditional wildlife crime in that traffickers are using decentralized and fast-evolving technological ecosystems, allowing them to extend the size and anonymity of their businesses by leveraging social media, e-commerce websites, encrypted messaging apps, darknet markets, cryptocurrency payment platforms and more.[23] The use of digital means in the context of wildlife trafficking has revolutionized environmental crime, making it a hybrid crime of the cyber and environmental worlds, which is transnational in nature, invisible and flexible in its means of implementing.[24]

[19] UNODC, World Wildlife Crime Report 2024; CITES (Preamble)
[20] Sollund, The Crimes of Wildlife Trafficking (2019); Wyatt, Wildlife Trafficking (2013)
[21] Lavorgna, 'Wildlife Trafficking in the Internet Age' (2014) 3 Crime Science 5
[22] Wingard and Pascual, 'Catch Me If You Can' (2018)
[23] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); IFAW, 'Digital Markets: Wildlife Trafficking Hidden in Plain Sight' (2021)
[24] Lavorgna (2014); UNODC, World Wildlife Crime Report 2024

Social media and encrypted communication systems are important tools in today's wildlife trafficking.[25] This technology facilitates the linking up of suppliers, intermediaries, and consumers in different jurisdictions and lowers the visibility of the transactions to enforcement authorities.[26]Private communications, coded language, and limited online communities pose serious challenges to digital investigations, evidence collection, and regulatory oversight.[27]

The anonymously operated darknet marketplaces also make the enforcement of wildlife trafficking more complex and challenging, as they offer highly anonymous platforms for wildlife products to be advertised and traded.[28] Anonymisation technologies and cryptocurrency payments make it harder to be transparent, harder to be sure of the jurisdiction and harder to be effective with traditional investigative tools.[29] Wildlife trafficking is therefore becoming a growing source of regulatory issues akin to those faced in other types of transnational digital crimes.

Wildlife trafficking is therefore a technologically mediated environmental harm, and must be considered alongside the conservation dimension of environmental crime, as well as requiring coordinated legal and governance responses.

2.2 Environmental Deception in Digital Wildlife Markets

In the era of digitalization, wildlife trafficking has created new kinds of environmental deception, which go beyond the classic deceptive modes in the past that were linked to the illegal wildlife trade.[30] Environmental deception in digital wildlife markets are technologically-based practices that involve misrepresenting legal status, origin, sustainability, ownership, or authenticity of wildlife products, to avoid regulatory inspection and enable illegal commerce. This can be done not only by falsification of documents, but also by algorithmic manipulation, by misrepresentations on the Internet, by not using commercial systems on the Internet properly.[31]

The most frequently used form of environmental deception is the falsification of the origin and legal status of the wildlife by falsifying the electronic permit, ownership records and captive-breeding certificates.[32] Illegal wildlife trade is frequently accompanied by false documentation that the wildlife species were legally raised or that they were sustainably harvested, to circumvent national and international laws and regulations. [33]Documentation processes were digitized to improve the efficiency of the regulatory environment, but at the same time it has opened the door to technologically advanced falsification and manipulation of documentation for the trade in wildlife products across the world.[34] In many countries, the regulatory systems are also very vulnerable to fraudulent digital documentation, due to weak verification systems and fragmented digital databases.[35]

Digital platforms are also being used for deceptive advertising practices, through coded words and termed images and descriptions, to disguise the protection of wildlife products.[36] One of the standard tricks in the trade of wildlife is to use euphemisms or to alter the species' designation or to evade automated moderation systems and platform detection algorithms. Photographs or illustrations of protected animals or birds can be modified with the use of a computer, to make them less recognizable, or be created as part of a

[25] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); IFAW, 'Digital Markets' (2021)
[26] Lavorgna (2014); Wingard and Pascual (2018)
[27] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[28] INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017)
[29] INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017); Wingard and Pascual (2018)
[30] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[31] Wingard and Pascual (2018); IFAW, 'Digital Markets' (2021)
[32] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[33] UNODC, World Wildlife Crime Report 2024; IFAW, 'Digital Markets' (2021)
[34] Singh Tomar, 'A Legal Analysis of Cyber-Enabled Wildlife Offences in India' (2024)
[35] UNODC, World Wildlife Crime Report 2024; Wingard and Pascual (2018)
[36] IFAW, 'Digital Markets' (2021); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)

"legitimate" commercial communication.[37]Wildlife species protected under the Wildlife Act may portray on the computer in photographs or illustrations to produce a less recognizable species, or may be incorporated into seemingly legal commercial advertisements. These practices mirror the growing use of technology as a means to not only camouflage illegal behavior, but to deliberately shape digital regulatory landscapes as well.

New and evolving technologies such as Artificial Intelligence could also make the tracking of wildlife trafficking more difficult as it would allow evidence to be manipulated, synthetic content to be produced, and more advanced forms of digital misrepresentation. While use of these technologies in the context of wildlife trafficking is still a developing field, their capacity for causing environmental deception serves as an example of the need for regulatory measures to be able to adapt to the rapidly changing technological context.

Environmental deception has other ecological and governance consequences besides being commercially illegal. Misaligned sustainability statements and illegality statements are causes of misguided conservation action, misrepresentations in government information and a loss of consumer awareness and loss of institutional trust in environmental governance.[38] When trafficked products of wildlife appear legal and sustainable, it's very difficult for regulatory bodies to accurately track the trends of trafficking, vulnerability of species and enforcement effectiveness. Thus, environmental deception not only enables the spread of illegal trade but also the lack of systemic governance on biodiversity protection.

2.3 Typology of Environmental Deception

Wildlife trafficking involves environmental deceptions that can be done in any manner. Instead, it has a number of techniques to cover the source, the protection or trafficking history of samples of wildlife in digital space. These are usually comparable in their application, but can be split up into individual forms based on the type of deception used. A typology aids in the comprehension of a changing approach by wildlife traffickers, and exposes gaps in regulation of today's online environment.

The typology conceptualised in the present study is an analytical typology based on the recurring typologies found in the literature on wildlife trafficking, the enforcement experiences and regulatory activities on digital wildlife markets.[39] Some have delved into specific aspects of deception in various contexts, but there is no current scholarship that has systemically approached environmental deception as a regulatory phenomenon in cyber-enabled wildlife trafficking. The typology suggested here aims to bridge this, by tracing and categorizing the major ways in which digital technologies enable the hiding and legitimization of illegal wildlife trade.

2.3.1 Species Misrepresentation

Misrepresentation is when the following occurs: Protected wildlife specimens are advertised or sold under a false or misleading description, in an attempt to conceal the protected status of the specimen. Traffickers can use a different species name, abbreviated names, 'coded' names, or mis-label the species in online advertisements to avoid platforms' moderation and enforcement systems.[40] There are also a number of practices that might make it difficult to monitor, because the transaction would be illegal, but this would not be apparent, even from the content of the digital communication or commercial listing.

2.3.2 Origin Laundering

Origin laundering is a type of falsified-origin of wildlife samples. Wild caught animals may be marketed as captives and illegally caught wildlife products may be marketed as products of legal and/or sustainable sources. This type of deception is particularly significant since some regulatory regimes permit the trade of

[37] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[38] UNODC, World Wildlife Crime Report 2024; IFAW, 'Digital Markets' (2021)
[39] Lavorgna (2014); Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[40] IFAW, 'Digital Markets' (2021); Lavorgna (2014)

some captive bred animals and not wild bears. To exploit the shortcomings of verification and certification, traffickers disguise the origin of wildlife products.

2.3.3 Documentation Fraud

Documentation Fraud: Obtaining or falsifying permits, certificates, licenses or ownership papers to import or export wildlife. In these digital settings, documents may be modified and after that, sent digitally and reproduced rapidly from one setting to the next.[41] The electronic version of regulatory documents has led to greater efficiency in the administration of the process, and to an increase in opportunities for changes in the documents and the possibility for falsification.

2.3.4 Digital Concealment

Digital concealment refers to using technology and online communication practices that cover up trafficking activity. These methods include encrypted messaging apps, disappearing messages, private online groups, anonymous accounts, doctored images, and coded speech.[42] These practices may not impact the wildlife product itself, but may make it less visible in digital spaces, thus hindering detection and investigation.

2.3.5 Legitimacy Laundering

Legitimacy laundering is when traffickers try to portray sustainability, ethical sourcing, legal ownership, or legal compliance to make it look like the product was lawfully obtained. Wildlife products can be sold as legally obtained wildlife products, responsibly sourced products or free from trade restrictions even if no legal justification exists.[43] These practices are especially worrisome because they question consumer understanding and erode trust in conservation and certification systems.

The above typology shows that environmental deceptive trafficking is not limited to the usual methods used for hiding wildlife trafficking, and is now increasingly using digital technologies, communication systems on the internet and manipulation of information. It is important to recognise these forms of deception and understand the nature of these types of crime in order to design regulatory responses that can adapt to the changing nature of the relationship between wildlife crime and digital environments.

2.4 Theoretical framework: Green Criminology and Environmental Governance

Green criminology offers a useful lens with which to see wildlife trafficking not just as a crime under the law, but also as an environmental crime that inflicts harm on biodiversity, species, and the environment.[44] From this perspective, wildlife trafficking is not only a legal offense, it's also a means of environmental damage.[45]

Cybercriminology is a factor in comprehending the impact of digital technologies on criminal activity. The use of online platforms, encrypted communications, cryptocurrencies and other digital infrastructures provide opportunities for anonymity, transnational connectivity and organisational flexibility, allowing for wildlife trafficking networks to be more difficult for enforcement authorities to trace across jurisdictions.[46]

The main analytical lens for this study is environmental governance theory which focuses on issues of environmental governance in a fragmented and transnational regulatory regime. Wildlife trafficking reaches across jurisdictions, multiple digital platforms and a multitude of private actors, and is therefore not easily dealt with in a traditional state-centred way through enforcement.[47] These views help address

[41] Wingard and Pascual (2018); Singh Tomar (2024)
[42] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017)
[43] IFAW, 'Digital Markets' (2021); Wingard and Pascual (2018)
[44] Lynch and Stretesky, Exploring Green Criminology (2014); Sollund, The Crimes of Wildlife Trafficking (2019)
[45] Lynch and Stretesky (2014); South, 'Green Criminology: Reflections, Connections, Horizons' (2014) 3 International Journal for Crime, Justice and Social Democracy 5
[46] Lavorgna (2014); Wingard and Pascual (2018)
[47] UNODC, World Wildlife Crime Report 2024; Wingard and Pascual (2018)

the issue of wildlife trafficking via the internet as a 'technological' phenomenon of environmental harm, and help create a framework and strategy for coordinated legal and governance action.

3. Methodology

The methodology used in this study is either doctrinal or comparative legal method. It analyses Indian, US and UK laws and policies on wildlife protection, cybercrime, digital evidence and intermediary liability, and explores the challenges associated with such laws. The study also relies on reports produced by international organizations such as the Convention on International Trade in Endangered Species (CITES), INTERPOL, and the United Nations Office on Drugs and Crime (UNODC), as well as the literature on wildlife trafficking, cybercrime and environmental governance. The comparative analysis aims to detect regulatory gaps, institutional enforcement constraints and governance strategies which are relevant for cyber-enabled wildlife trafficking and environmental deception.

4. Digital Architecture of Wildlife Trafficking Networks

4.1 Transformation of Wildlife Trafficking in the Digital Environment

Networks have evolved over time as the use of online platforms has grown.[48] Previously market-based, goods and services exchanges and transactions can now be supported via digital communication technologies, online marketplaces, and multi-national business networks.[49] This is broadening the opportunities for contacts between suppliers and consumers between jurisdictions, but also bringing fresh difficulties to monitoring, investigating and regulating.[50] Enforcement, governance and legal accountability are therefore more the point of interest when digitalisation is discussed than the technologies themselves.

4.2 Social Media Platforms and Online Wildlife Markets

Social media platforms and online marketplaces are important infrastructures in wildlife trafficking networks as they deliver wide markets, quick communication and possibilities for jurisdictions to reach consumers.[51] Social media including Facebook, Instagram, TikTok, Telegram and a range of e-commerce websites are increasingly being employed to promote protected species, exotic pets, wildlife products, ivory, reptile skins and other banned wildlife products.[52] While more traditional wildlife markets enable the transaction of wildlife between buyer and seller, digital platforms do so without the need for them to be physically present, thus contributing to the wider and more accessible nature of the illegal wildlife trade.[53]

To evade platform moderation and law enforcement detection, traffickers often use coded language, abbreviations or hashtags, false descriptions, and private communication channels. The visual aspect of social media also helps in trafficking operations by allowing the trafficking perpetrators to present live animals and wildlife products for sale without revealing the species, origin or legal status of the product.[54] In addition, online marketplaces can be used for wildlife trafficking in either the disguise of wildlife products in other commercial listings or by mislabeling them as legally traded items.[55] These practices illustrate how environmental manipulation is used to obfuscate the illegal nature of wildlife trade, and makes the job of regulators more difficult. As such, social media platforms, online marketplaces have emerged as sites of regulatory concern, where issues of intermediary responsibility, content moderation, and cooperation in enforcing laws have arisen in relation to digital wildlife markets.[56]

4.3 Encrypted Communications and Regulatory Visibility

[48] UNODC, World Wildlife Crime Report 2024; Lavorgna, 'Wildlife Trafficking in the Internet Age' (2014)
[49] Lavorgna (2014); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[50] Wingard and Pascual, 'Catch Me If You Can' (2018)
[51] IFAW, 'Digital Markets: Wildlife Trafficking Hidden in Plain Sight' (2021); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[52] IFAW, 'Digital Markets' (2021); UNODC, World Wildlife Crime Report 2024
[53] Lavorgna (2014); IFAW, 'Digital Markets' (2021)
[54] IFAW, 'Digital Markets' (2021); Lavorgna (2014)
[55] Wingard and Pascual (2018); IFAW, 'Digital Markets' (2021)
[56] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)

The growing use of encrypted communication systems and anonymised online platforms presents further challenges for wildlife law enforcement, making it harder to detect wildlife trafficking and to gather evidence. Digital communications can cross jurisdictions and service providers may not be within the reach of the enforcers.[57] This makes it harder for regulators to have timely access to information they need to investigate wildlife crime, and more difficult to obtain information, all the time.

These are important not because they lead to new types of wildlife trafficking, but because they reveal shortcomings in the existing laws, which are primarily drafted to address the physical trade.[58] The issues that emerge are not technical, but relate to access to evidence, jurisdiction, platform cooperation, and international regulatory coordination.[59]

4.4 Implications for Environmental Governance and Law Enforcement

The fact that wildlife trafficking networks are digital exposes some structural flaws in today's environmental governance and law enforcement. Traditional approaches to wildlife trafficking have concentrated on trafficking of wildlife through physical means and on the border operations and crime inside the countries.[60] The transnational nature of these ecosystems and fluid flows in the digital realm, however, make cyber-enabled wildlife trafficking challenging to regulate in a jurisdictionally fragmented and weak regulatory framework.

One of the most significant issues to effective enforcement is a lack of uniformity of jurisdiction. Wildlife trafficking on digital platforms can include actors and servers in various jurisdictions, financial systems, and consumers, all of which may have varying laws and enforcement capabilities. This means a "transnational" approach to investigations, with the sharing of evidence across borders and coordinated regulatory action between public and private digital intermediaries.

The increased digitalization also raises related issues of intermediary liability and platform responsibilities.[61] New actors, such as social media platforms, online trading platforms, encrypted messaging services, and online payment services are now integrated in the various stages of wildlife trafficking, but current laws and regulations regarding monitoring, reporting and removal of content are not harmonised between jurisdictions. Lack of harmonised regulations, which traffickers still exploit, results in significant regulatory shortcomings.

As a result, the technologic revolution of the wildlife trafficking industry underscores the need to shift from a traditional conservation, towards an approach for wildlife crime. The nexus of cyber technology, criminal gangs, and environmental damage requires more holistic regulatory responses, that combine elements of cybercrime enforcement, the governance of digital platforms, the protection of wildlife and the cooperation of legal responses across countries.

5. Regulatory Fragmentation and the Limits of Existing Legal Frameworks

5.1 India: Fragmented Regulation and Limited Cyber Integration

The laws of the land for protection of wildlife in India are largely covered under the Wild Life (Protection) Act, 1972 which will punish hunting, possession, transportation and trade of protected wildlife and their derivatives.[62] It is the primary law in India for biodiversity conservation and control of wildlife trade, and also provides for protection area regulations, wildlife trade restrictions, powers of seizure, and penal

[57] Eurojust/SIRIUS, 'Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence' (2024); Wingard and Pascual (2018)
[58] Singh Tomar, 'A Legal Analysis of Cyber-Enabled Wildlife Offences in India' (2024); Wingard and Pascual (2018)
[59] Eurojust/SIRIUS (2024); Wingard and Pascual (2018)
[60] Sollund, The Crimes of Wildlife Trafficking (2019); UNODC, World Wildlife Crime Report 2024
[61] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[62] Wild Life (Protection) Act 1972 (Act No 53 of 1972), ss 9, 39, 44, 49B, 51

powers.[63] The legislative framework was however formed in a pre-digital environment that is predominantly focused on the traditional methods of trading in wildlife, such as possession and movement, and not on technologically-enabled wildlife trafficking via digital ecosystems.

The Wild Life (Protection) Act, 1972 doesn't suffice to cover online markets for wildlife, intermediary liability, encryption of communication systems, and the governance of digital platforms entirely. The exploitation of social media, encrypted messaging apps and online platforms for trafficking in wildlife is therefore increasingly facilitated by gaps in legislation and a lack of transparency of the nature of existing wildlife laws with respect to online enforcement. Enforcement agencies generally have access to traditional seizure and investigation tactics which may be ineffective in the fight against technologically adaptive trafficking networks in decentralized online environments, but they can also implement novel tactics.While traditional seizure and investigation techniques might be ineffective in a technologically adaptive trafficking network in a decentralised online world, it does not prevent innovative techniques from being adopted.[64]

The primary law on cyber crimes, electronic records and intermediary liability in India is the Information Technology Act, 2000. Some of the rules on electronic evidence, intermediary due diligence and online content that is unlawful, may indirectly apply to online wildlife trafficking.[65] But cyber enabled wildlife trafficking is not listed as a specific concern for regulation in the law. Consequently, the institutional connection between wildlife protection legislation and cybercrime legislation is weak and wildlife protection authorities lack any formal connection with cybercrime authorities.

Similarly, the Bharatiya Nyaya Sanhita, 2023 updates parts of the criminal law related to electronic communications and organised crime, but does not mention the cyber-enabled wildlife trafficking or digital wildlife markets.[66] Currently, there are no specific provisions in the Convention that deal with the markets for wildlife products on the Internet, online sales of wildlife using cryptocurrencies or the transnational trafficking of wildlife via the Internet.

The legal landscape in India brings a new set of challenges with digital evidence. Electronic records can be introduced and are subject to the statutory requirements for evidence, but the practicalities of chain of custody, authenticating records, encrypted communications and trans-border access to data continue to hamper prosecutions of wildlife crimes committed via electronic platforms. In many situations, there are jurisdictional issues due to the international servers, the encrypted international financial transfers and communications.

Institutionally, wildlife laws in India are being largely enforced in the fight against physical poaching gangs, illegal trafficking of wildlife and traditional trafficking. While the specialized integration of the wildlife enforcement agencies and the cybercrime authorities is still limited, there is an increase in cybercrime cells and digital investigation mechanisms in recent years. These show that a lot needs to be done to counter wildlife trafficking across digital and transnational networks.

5.2 United States: Expanding Digital Enforcement Mechanisms

The U.S. has become more pragmatic in its approach to wildlife trafficking and cyber crime. The main federal laws regulating wildlife protection are the Lacey Act and the Endangered Species Act, which

[63] Wild Life (Protection) Act 1972, ss 18, 40, 50, 51
[64] UNODC, World Wildlife Crime Report 2024; TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[65] Information Technology Act 2000, ss 67, 67A, 67B; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
[66] Bharatiya Nyaya Sanhita 2023

prohibit the illegal trade in protected wildlife species and give broad investigative and enforcement authority.[67] The U.S. structure is particularly applicable because there is a higher level of digital investigative mechanisms use in the digital world, and high levels of collaboration between wildlife and cybercrime agencies.[68]

The use of digital surveillance technology, undercover online investigations, financial tracking and cyber-forensic tools has been increasingly relied upon by federal enforcement agencies like the United States Fish and Wildlife Service and cybercrime investigation units to trace illegal wildlife trade on the internet and darknets.[69] The U.S. has a wildlife enforcement system that is more receptive to the fact that there is a technological revolution in organized crime and that new investigative methods are necessary to catch criminals.[70]

Enforcement capabilities on digital platforms and digital intermediaries are also increasing in the United States, which can help facilitate greater efforts to tackle cyber-enabled wildlife crime. While the doctrine of intermediary liability is still important in the U.S. legal system, digital platforms can still be subject to regulatory requirements around illegal online content, participation in investigations, and adherence to law enforcement requests.[71] Federal governments have also been more likely to apply cybercrime laws, anti-money laundering laws and financial investigation tools to tackle the transnational nature of OWWC activities via digital platforms.[72]

The U.S. also boasts more advanced investigative capabilities for cryptocurrency investigations and the tracing of electronic financial transactions. The financial surveillance tools and cyber-forensic capabilities are crucial elements in the identification of illegally trafficked wildlife using anonymous transactional infrastructures in the darknet. The capacity of enforcement authorities to be able to respond to technologically sophisticated and increasingly complex operations of wildlife trafficking can take place outside of the commonly conceived ‘trafficking routes'.

There are, however, many important regulatory challenges to be addressed. Enforcement issues continue to be jurisdictional issues between the federal and state governments, new digital technology, encrypted communication and cross-border trade in wildlife. In addition, the battle between privacy protection and intermediary immunity and digital surveillance powers introduces legal and constitutional challenges about the nature of investigative powers on the Internet.[73] The overall U.S. system, however, is a fairly flexible, responsive system for cyber-enablement of environmental offenses.

5.3 United Kingdom: Platform Governance and Coordinated Enforcement

In the United Kingdom, the Wildlife and Countryside Act 1981 is the primary legislation on wildlife trafficking, and the United Kingdom is party to CITES and other international and environmental laws.[74] The UK approach is also important because of increased attention to the importance of co-ordinated wildlife crime policing and ‘intermediate governance' in the digital arena.[75]

[67] Lacey Act 1900 (16 USC ss 3371–3378); Endangered Species Act 1973 (16 USC ss1531–1544)
[68] ICE Homeland Security Investigations, 'Wildlife Trafficking Program'; US Fish and Wildlife Service, 'Laws and Regulations'
[69] ICE HSI, 'Wildlife Trafficking Program'; INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017)
[70] ICE HSI, 'Wildlife Trafficking Program'; Congressional Research Service, 'Criminal Lacey Act Offenses' (2025)
[71] Communications Decency Act 1996, s 230 (47 USC s.s 230)
[72] ICE HSI, 'Wildlife Trafficking Program'; Congressional Research Service, 'Criminal Lacey Act Offenses' (2025)
[73] Communications Decency Act 1996, s 230; Eurojust/SIRIUS (2024)
[74] Wildlife and Countryside Act 1981 (c 69); CITES 1973
[75] Crown Prosecution Service, 'Wildlife Offences' (2022)

A crucial institutional feature of the UK system is the establishment of the National Wildlife Crime Unit (NWCU) that allows for the sharing of intelligence, inter-agency co-ordination and specialised investigation of wildlife crime. There are dedicated institutional arrangements in place, which enables comparatively higher level of integration of wildlife with the overall effective organized crime investigation including that of the online trafficking network and the communication system.[76]

Recent news regarding regulation of online platforms and digital safety platforms also relates to the regulation of CTWT in the UK.[77] The increasing need for intermediary accountability and the new regulatory expectations on harmful online content and responsibility of digital platforms have resulted in a broader variety of regulatory expectations regarding monitoring and removal of illegal commercial operations established through Internet systems.[78] In that regard, the regulation of digital platforms in the United Kingdom may be better scrutinised in relation to the content on these platforms that relates to the trafficking of wildlife.

The United Kingdom is also a country that has increasingly been turning to intelligence-led enforcement and international cooperation models for dealing with transnational wildlife crime. Working with international organizations, police and customs authorities, cybercrime units and financial investigation organizations helps to create a more streamlined enforcement framework to address transnational trafficking networks that leverage digital networks.[79]

However, there are questions about technologies employed for encrypted communications, darknets and cross-border digital evidence, affecting enforcement. As in other jurisdictions, the UK was initially not subject to its wildlife laws in technologically mediated environments of wildlife trafficking involving algorithmic communication systems, cryptocurrency transactions and decentralized online markets.[80] Therefore, legal adaptation is an ongoing process and is adapting itself to the evolving technological situation.

5.4 Comparative Regulatory Gaps and Emerging Governance Challenges

A comparison of the three jurisdictions shows how wildlife trafficking using digital technologies is becoming a source of structural gaps in traditional wildlife protection mechanisms. While all three jurisdictions have laws against the illegal wildlife trade, there are significant variations in institutional coordination, cybercrime integration, intermediary governance, and digital investigative capacities.

Table 1. Comparative Assessment of Regulatory Responses to Cyber-Enabled Wildlife Trafficking

Regulatory Dimension	**India**	**United States**	**United Kingdom**
Wildlife protection legislation	Strong conventional wildlife protection framework	Strong wildlife protection framework	Strong wildlife protection framework
Recognition of online wildlife trafficking	Limited and largely indirect	Increasingly recognized through enforcement practice	Increasingly recognized through enforcement and policy initiatives

[76] Crown Prosecution Service, 'Wildlife Offences' (2022); INTERPOL and WCO, 'Operation Thunder 2023'
[77] Online Safety Act 2023 (c 50)
[78] Online Safety Act 2023 (c 50); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[79] INTERPOL and WCO, 'Operation Thunder 2023'; Eurojust/SIRIUS (2024)
[80] Wildlife and Countryside Act 1981 (c 69) — cite to show absence of digital provisions; Singh Tomar (2024) for comparative context

Regulatory Dimension	India	United States	United Kingdom
Integration of wildlife and cybercrime enforcement	Limited institutional integration	Moderate integration through federal enforcement mechanisms	Moderate integration through coordinated enforcement structures
Digital investigation capabilities	Developing	Relatively advanced	Relatively advanced
Regulation of online platforms	Fragmented and evolving	Mixed approach with limited intermediary liability	Expanding emphasis on platform responsibility
Cryptocurrency and financial tracing capacity	Limited	Comparatively stronger	Developing
Cross-border enforcement cooperation	Dependent upon existing international mechanisms	Extensive participation in international enforcement initiatives	Extensive participation in international enforcement initiatives
Capacity to address cyber-enabled wildlife trafficking	Emerging	Moderate to strong	Moderate

The comparative assessment highlights that none of the three jurisdictions has created a framework dedicated to the regulation of cyber-enabled wildlife trafficking, although each jurisdiction has legal mechanisms that can be used to deal with parts of wildlife trafficking and cybercrime.[81] Whereas most of the distinctions do not stem from the presence of wildlife protection legislation, but from differences in investigative capacity through digital means, institutional coordination of the platforms, platform governance, and enforcement practice.[82] In other countries, such as the United States and the United Kingdom, there is greater adaptation to technology-enhanced wildlife crime by the creation of specific enforcement entities and digital investigative tools, but regulatory fragmentation is a constant challenge in all jurisdictions.[83] In India, there is still a huge gap between wildlife law enforcement and cybercrime regulation, and provisions need to be strengthened and adapted to achieve full integration of the two.[84]

While there are institutional differences and varying practices of enforcement, all three jurisdictions are confronted with challenges related to encrypted communications, cryptocurrency transactions, cross-border evidence gathering, intermediary accountability, and jurisdictional fragmentation.[85] Current wildlife protection systems are still largely focused on traditional trafficking and have not sufficiently responded to digitised trafficking methods of wildlife.[86] A comparative analysis is therefore useful, as it reveals the necessity to strengthen integration between wildlife protection law, digital governance and transnational enforcement mechanisms.

There are common problems within the three jurisdictions in relation to encrypted communications, cryptocurrency transactions, gathering evidence across jurisdictions, accountability of intermediaries and

[81] Wingard and Pascual, 'Catch Me If You Can' (2018); UNODC, World Wildlife Crime Report 2024
[82] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); ICE HSI, 'Wildlife Trafficking Program'
[83] ICE HSI, 'Wildlife Trafficking Program'; Crown Prosecution Service, 'Wildlife Offences' (2022); Wingard and Pascual (2018)
[84] Singh Tomar, 'A Legal Analysis of Cyber-Enabled Wildlife Offences in India' (2024); Wild Life (Protection) Act 1972; Information Technology Act 2000
[85] Eurojust/SIRIUS, 'Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence' (2024); Wingard and Pascual (2018); UNODC, World Wildlife Crime Report 2024
[86] Wingard and Pascual (2018); Singh Tomar (2024); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)

the fragmentation of jurisdictions. Existing laws on wildlife continue to be fundamentally based on traditional enforcement models that do not adequately capture the nature of the operations in digitally mediated environmental crime.[87] The comparative analysis therefore highlights the importance of a holistic legal and institutional response in order to address the convergence of cyber-crime and environmental damage and trans-national digital governance more effectively.

6. Digital Evidence and Enforcement Challenges

The success of any regulatory regime to control wildlife trafficking is ultimately based on the capacity of law enforcement to identify the perpetrators of the illegal trade, secure admissible facts, assert jurisdiction and secure convictions. Digital technologies have also opened new avenues for the wildlife traders and have posed new challenges for wildlife investigators and regulatory bodies.[88] Online wildlife trafficking is transnational, decentralised, technologically sophisticated, and with an incalculable number of transactions taking place, it can often be difficult to keep up.[89] As a result, legal and practical challenges with digital evidence, encrypted data, anonymous financial transfers and multi-jurisdictional investigations are increasingly facing enforcement agencies.[90]

6.1 Digital Evidence in Wildlife Trafficking Investigations

The importance of electronic evidence in wildlife trafficking investigations has increased as trafficking has become increasingly online and through communication networks.[91] Social media posts, online ads, e-communications, transaction records, geolocation, digital photos, and cryptocurrency transactions and metadata generated from activity online can be evidence of wildlife trafficking.[92] This type of material may hold important information on the identities of those who are involved in trafficking, what products of wildlife are being trafficked, and the trafficking networks.[93]

Digital evidence is of evidentiary value, but has unique legal and procedural problems. In contrast to physical evidence, e-records can be changed, erased, encrypted or located in several jurisdictions.[94] Investigations are often a source of issues of authenticity, reliability, preservation and chain of custody; such issues can also be raised in court.[95] Evolving nature of digital information creates even more difficult evidence processes as information can so easily disappear from the Internet because of account deletion, moderation by the platform, or automated data removal policies.[96]

As a result of this, the use of digital evidence is growing and the legal system needs to be equipped with specific technical skills and investigative means. When primary evidence is largely digital, for example as found in traditional wildlife crime investigations based on wildlife seizures, real-world examinations and forensics analyses, investigating wildlife crimes may not be sufficient.[97] With the rise of electronic evidence, there is an even greater need for wildlife enforcement agencies to be integrated with cyber-forensic experts.[98]

6.2 Encrypted Communications and Anonymity

[87] Wingard and Pascual (2018); Singh Tomar (2024); UNODC, World Wildlife Crime Report 2024
[88] Wingard and Pascual, 'Catch Me If You Can' (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[89] UNODC, World Wildlife Crime Report 2024; Lavorgna, 'Wildlife Trafficking in the Internet Age' (2014)
[90] Eurojust/SIRIUS, 'Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence' (2024); Wingard and Pascual (2018)
[91] Singh Tomar, 'A Legal Analysis of Cyber-Enabled Wildlife Offences in India' (2024); IFAW, 'Digital Markets: Wildlife Trafficking Hidden in Plain Sight' (2021)
[92] IFAW, 'Digital Markets' (2021); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[93] UNODC, World Wildlife Crime Report 2024; INTERPOL and WCO, 'Operation Thunder 2023'
[94] Eurojust/SIRIUS (2024); Wingard and Pascual (2018)
[95] Singh Tomar (2024); Eurojust/SIRIUS (2024)
[96] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); Wingard and Pascual (2018)
[97] Singh Tomar (2024); UNODC, World Wildlife Crime Report 2024
[98] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); Wingard and Pascual (2018)

One of the biggest obstacles in investigating wildlife trafficking over the Internet is the shared features of the technologies that are used to encrypt the communication.[99] End-to-end encrypted messaging services provide traffickers with a secure way to communicate, but also help to restrict the ability of law enforcement agencies to monitor or intercept communication.[100] These technologies can have benefits for organised crime groups, including reducing the risk of detection and ease of command and control of trafficking operations between various countries.[101]

Similar issues exist for anonymity technologies. To avoid identification, wildlife traffickers are often using anonymity-enhancing technologies and pseudonymous identities that make it difficult to identify the traffickers and link online activities to specific persons.[102] These practices limit the efficiencies of traditional investigative methods and enhance digital forensic methods. Consequently, it can be one of the most challenging parts of investigating a digital wildlife crime is being able to identify the criminals.

However, privacy rights and interests, and regulatory responses, are complicated by enforcement interests. Valid cybersecurity and privacy protections can be offered via encryption technologies, but so can illegal operations.[103] The challenge set for the policymaker is to strike the balance between individual rights and effective investigation of serious environmental offences.

6.3 Cryptocurrency and Financial Concealment

Cryptocurrencies have been increasingly being used on online wildlife markets, which adds to the difficulties of enforcement.[104] Cryptocurrencies offer new alternatives to payment systems that could lessen the need to use traditional banking systems and hinder the ability to carry out conventional financial investigations.[105] Digital currencies are often used by wildlife traffickers through darknet marketplaces to conduct transactions anonymously or pseudonymously of illegal wildlife products.[106]

Blockchain technologies can provide proof of transactions, but it is difficult to trace the owners of the particular cryptocurrency wallets without substantial technical abilities and international cooperation.[107] Moreover, privacy-enhancing cryptocurrencies and decentralized financial systems can be a further challenge in the relationship of transactions. It is more challenging to trace the finances, identify criminal networks and seize funds raised from wildlife trafficking.[108]

Financial investigations have long been an integral part of the efforts against organized crime. The rise of digital financial systems however, necessitates new investigatory capabilities for enforcement agencies to deal with technologically advanced ways of hiding financial transactions.[109] If these are not available, the economic underpinnings of wildlife trafficking could continue to be largely outside the reach of effective regulation.

6.4 Cross-Border Investigations and Jurisdictional Challenges

Wildlife trafficking often happens in a multi-jurisdictional manner, with the use of cyber technology.[110] It may be one transaction where the seller is in one country, the buyer is in another country, the platform is

[99] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[100] Eurojust/SIRIUS (2024); Wingard and Pascual (2018)
[101] UNODC, World Wildlife Crime Report 2024; INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017)
[102] INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017); Lavorgna (2014)
[103] Eurojust/SIRIUS (2024) — which discusses this tension explicitly in the context of the Budapest Convention Second Protocol
[104] INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017); UNODC, World Wildlife Crime Report 2024
[105] ibid
[106] INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017)
[107] ibid
[108] UNODC, World Wildlife Crime Report 2024; ICE HSI, 'Wildlife Trafficking Program'
[109] INTERPOL, 'Illegal Wildlife Trade in the Darknet' (2017); Wingard and Pascual (2018)
[110] UNODC, World Wildlife Crime Report 2024; Wingard and Pascual (2018)

located in a third, and the payment system is based on a decentralized digital network. This complexity also results in a lot of jurisdictional issues as the legal authority is primarily territorial and activities in the virtual world are now increasingly global.

Information on foreign servers or information controlled by multinational technology companies may be a challenge for investigators. The processes of mutual legal assistance can be time consuming and may not be able to keep pace with the pace of change and deletion of digital evidence. Another issue that complicates international cooperation is the variation in national laws on privacy, surveillance, data retention and measures to protect wildlife.

This cross-border nature of online wildlife trafficking is therefore an obstacle to the effectiveness of the existing 'one-stop-shop' approach. Mechanisms of international cooperation enabling the sharing of information, coordinated investigations and timely access to digital evidence are gaining in significance for effective regulation. If there were no cooperation, traffickers may exploit the regulations and various jurisdictions.

6.5 International Enforcement Operations and Emerging Investigative Practices

The interregional and international dimensions of wildlife trafficking have made it increasingly important to have coordinated enforcement action across jurisdictions and international institutions.[111] Large-scale enforcement operations in recent years highlight the extent of today's wildlife crime and the need for increased intelligence-led investigation, digital monitoring and international cooperation to bring trafficking networks to a standstill.[112]

A key development in this respect has been the string of multinational enforcement operations organized via international law enforcement networks.[113] These operations have included cooperation between wildlife, customs, police, border, and international agencies in order to locate trafficking routes, break up wildlife trafficking networks, and to disrupt illegal wildlife markets. This has led to significant protected wildlife seizures and exposed the transnational and well-structured nature of today's wildlife trade.[114]

Importantly, enforcement reports are beginning to take place in the context of trafficking operations, and they show that digital technology is increasingly used in these operations. Advertisements, social media messaging, encrypted apps, electronic payment systems, and digital record-keeping systems have often been a component of investigations.[115] Investigators have thus had to draw on a range of conventional wildlife crime enforcement practices, digital investigation, cyber-forensic techniques and collaborative information sharing, including with other countries.[116]

These enforcement experiences also raise ongoing issues of jurisdiction, access to electronic evidence and international cooperation.[117] Relevant information for a specific investigation could be spread out in several countries and available in digital systems out of the reach of investigating authorities.[118] The ability of investigations to be effective is often limited by delays in obtaining electronic evidence, the different legal systems in the home country, and challenges with encrypted communications.[119]

The realities of multi-national wildlife crime operations illustrate that this modern problem of wildlife trafficking cannot be solved with traditional conservation law enforcement.[120] Instead, investigations are

[111] UNODC, World Wildlife Crime Report 2024; INTERPOL and WCO, 'Operation Thunder 2023'
[112] INTERPOL and WCO, 'Operation Thunder 2023'; INTERPOL and WCO, 'WCO-INTERPOL Operation Thunder 2021'
[113] ibid
[114] ibid
[115] IFAW, 'Digital Markets: Wildlife Trafficking Hidden in Plain Sight' (2021); INTERPOL and WCO, 'Operation Thunder 2023'
[116] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); INTERPOL and WCO, 'Operation Thunder 2023'
[117] Eurojust/SIRIUS, 'Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence' (2024); Wingard and Pascual (2018)
[118] Davies and Kennedy-Mayo, 'The Promise and Pitfalls of the Second Protocol to the Budapest Convention' (2026)
[119] Eurojust/SIRIUS (2024); Wingard and Pascual (2018)
[120] UNODC, World Wildlife Crime Report 2024; INTERPOL and WCO, 'Operation Thunder 2023'

increasingly being conducted in a coordinated fashion that combines wildlife protection and cyber investigation methods, financial intelligence, and transnational law enforcement cooperation. This reinforces the notion that wildlife trafficking has an additional regulatory challenge in the form of cyber-enabled wildlife trafficking, which goes beyond the traditional wildlife trafficking control mechanisms.

6.6 Emerging Enforcement Imperatives

Cyber-enabled wildlife trafficking poses challenges not only with regard to digital evidence, encrypted communications and anonymous financial systems, but also transnational investigations, which require a combination of investigation and enforcement tools, many of which are not available.[121] The landscape of investigations has changed, as have the methods used by wildlife traffickers, as a result of technological shifts.[122] This means that the enforcement institutions have to adjust to new and more complex types of environmental offences that occur in digital environments.

They must be addressed in the context of strengthening institutional cooperation among wildlife and animal authorities, cybercrime agencies, financial intelligence agencies and international enforcement agencies.[123] It requires also the specialization of the skills in cyber-forensics, on-line investigations and on-line intelligence gathering.[124] It also underscores the importance of adopting regulatory approaches and mechanisms that can identify cyber-enabled wildlife trafficking as a specific enforcement challenge, at the nexus of environmental criminality, organized criminality and digital governance.

This recognition is used as a starting point for discussions of policy and regulatory changes in the next section.

7. Towards an Integrated Regulatory Framework for Cyber-Enabled Wildlife Trafficking

The above analysis indicates that existing laws and institutions are poorly designed to address the cyber-trafficking issues. Laws have a role in regulating unlawful activities, which include wildlife protection, cybercrime and digital governance, but are not necessarily connected. This division is creating regulatory gaps which are being increasingly taken advantage of by traffickers via digital platforms, encrypted communication networks and transnational online market places. In order to tackle these challenges, a more coordinated and integrated regulatory framework is needed which will consider the convergence of environmental crimes and digital crimes.

7.1 Integrating Wildlife Protection and Cybercrime Regulation

The current dichotomy between wildlife law enforcement and cybercrime regulation is one of the major challenges in the current regulatory regime.[125] In many jurisdictions, the issue of wildlife trafficking is considered to be a conservation problem and cybercrime laws target activities such as unauthorised access, financial fraud, identity theft and crimes involving the misuse of data.[126] Wildlife offences facilitated by digital technology can be found therefore in the space between regulatory and institutional frameworks.[127]

Future regulatory changes should thus be more conducive to closer collaboration between wildlife protection authorities and cybercrime authorities. This would help to share knowledge, intelligence and investigation resources which are important to the challenges of technologically facilitated wildlife crime.[128] There should also be specific provisions in the regulatory framework for the importance of the digital

[121] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); Eurojust/SIRIUS (2024)
[122] UNODC, World Wildlife Crime Report 2024; Lavorgna, 'Wildlife Trafficking in the Internet Age' (2014)
[123] INTERPOL and WCO, 'Operation Thunder 2023'; Eurojust/SIRIUS (2024
[124] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); ICE HSI, 'Wildlife Trafficking Program'
[125] Wingard and Pascual (2018); Singh Tomar, 'A Legal Analysis of Cyber-Enabled Wildlife Offences in India' (2024)
[126] Wingard and Pascual (2018); Information Technology Act 2000 (India); Computer Misuse Act 1990 (UK)
[127] Wingard and Pascual (2018); Singh Tomar (2024)
[128] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); INTERPOL and WCO, 'Operation Thunder 2023'

technologies in current-day trafficking in wildlife and clear procedures for investigating offenses through online platforms or communication systems.

7.2 Strengthening Digital Investigative Capacity

With the increase of electronic evidence in the field of wildlife trafficking investigations, the skills of investigators need to be developed accordingly.[129] Wildlife enforcement agencies tend to be more interested in species identification, Wildlife field investigations and regular trafficking investigations and are not necessarily interested in Digital investigations or Cyber-forensics.[130]

There is a need to invest in technical training, digital evidence management, online intelligence gathering and cyber-forensic analysis for strengthening investigative capacity. It is welcome to note that the current resource and skills limitations can be overcome by better institutional cooperation between the Wildlife authorities and computer/cybercrime experts.[131] Establishing dedicated investigative protocols on online wildlife trade would also further develop the enforcement agencies' capacity to effectively gather, preserve and present digital evidence.[132]

An increase in investigative capabilities is particularly important, since the digital information generated by wildlife markets online could be extensive and provide the opportunity for the identification of trafficking patterns, criminal networks and commercial links.[133] The ability of investigators to identify and prove digital evidence and analyze it within legal boundaries is key to the effective use of this information.[134]

7.3 Platform Responsibility and Digital Governance

Digital platforms are a key element in today's wildlife trafficking networks.[135] Wildlife trafficking often occurs via social media services, online marketplaces, messaging applications and digital payment systems.[136] As a result, and in the context of the discussion of regulating digital wildlife crime, questions regarding the responsibility of platforms have come to the fore.[137]

Platforms can't be looked at just in terms of content moderation. Rather, questions around platform governance are indicative of a broader spectrum of issues concerning monitoring systems, reporting, working with legal authorities and implementing systems that are able to identify and disrupt wildlife trafficking.[138] There is no requirement to remove all illegal content from platforms, but greater cooperation between platforms and other institutions and increased clarity in the requirements of the regulations may help reduce the opportunities for misuse of digital infrastructures.

At the same time, regulatory measures need to be careful as well about privacy, freedom of expression and technological innovation issues.[139] Therefore, a balanced approach for controlling the illegal wildlife trade will be crucial for good governance, without unduly curtailing legal use of digital technologies.

7.4 Enhancing International Cooperation

Wildlife trafficking is by definition transnational and what is needed is a facilitated by cyber. Trafficking networks are often trans-border and digital evidence, communications, and monetary transactions are

[129] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); Eurojust/SIRIUS (2024)
[130] Singh Tomar (2024); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[131] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); INTERPOL and WCO, 'Operation Thunder 2023'
[132] Eurojust/SIRIUS (2024); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[133] UNODC, World Wildlife Crime Report 2024; IFAW, 'Digital Markets' (2021)
[134] Eurojust/SIRIUS (2024); Singh Tomar (2024)
[135] IFAW, 'Digital Markets' (2021); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[136] IFAW, 'Digital Markets' (2021); UNODC, World Wildlife Crime Report 2024
[137] Wingard and Pascual (2018); TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020)
[138] TRAFFIC, 'Tackling Wildlife Cybercrime in the EU' (2020); Online Safety Act 2023 (c 50)
[139] Eurojust/SIRIUS (2024)

frequently trans-border.[140] Therefore, the effective enforcement is possible only in combination with other measures, domestic regulatory capabilities.[141]

Cooperation on a global level continues to be necessary to strengthen cooperation and tackle jurisdictional fragmentation in order to implement coordinated actions to combat digital wildlife crimes. Information sharing, mutual legal assistance and transnational criminal investigations should be enhanced to meet the challenges of technologically-enabled crimes.[142] Greater cooperation and coordination between and within wildlife enforcement agencies, cybercrime agencies, customs agencies, financial intelligence agencies and international agencies is needed to enhance the capacity of states to investigate and prosecute cross-border wildlife trafficking.

An area that is particularly suitable for international cooperation is the field of digital evidence, which is increasingly being used as a tool in investigations and information must be retrieved in a timely and efficient manner in jurisdictions across the border.[143] Not obtaining this information can be a major impediment to investigations. Therefore, future governance strategies should aim to have tools that allow for more efficient and coordinated access to digital evidence in wildlife trafficking cases.

7.5 Recognising the Digital Dimensions of Wildlife Trafficking

Current laws and policies still view wildlife trafficking largely as a traditional conservation and/or enforcement issue.[144] The growing dependence on digital platforms, encrypted communications, electronic payment systems and transnational online markets, however, shows that contemporary wildlife trafficking is increasingly digitalised and happening through digital infrastructures.[145]

Regulatory measures should therefore reflect the increasing importance of digital technologies in the facilitation of wildlife trafficking flows. No new category of offence need to be created for this recognition. Instead, it draws the attention of the community to the importance of modifying current wildlife protection laws to address the challenges of e-commerce, electronic evidence, platform control, and multi-jurisdictional enforcement.

A more coordinated and comprehensive regulatory framework would allow for coordinated action by wildlife protection authorities, cybercrime investigators, digital platforms and international enforcers in addressing technology-related wildlife trafficking without losing focus on the overall wildlife conservation goals.

7.6 Concluding Observations

The foregoing analysis shows the shortcomings of the existing legal frameworks in combating wildlife trafficking as a typical criminal activity, when addressing cyber-enabled wildlife trafficking. Current law already provides protection for wildlife, but in today's reality the efficacy of this protection is increasingly reliant on the ability of regulatory institutions to deal with online markets, electronic evidence, intermediaries, and international law enforcement issues.[146]

Hence, strengthening the substantive protection of wildlife should be complemented with the improvement of institutional coordination, investigative capacity, platform governance and international cooperation in the future regulatory approach. These would help towards making wildlife protection systems work in a more digitalised world and continue to improve overall biodiversity protection and environmental governance.

8. Conclusion

Wildlife trafficking is a modern problem facing criminal and regulatory frameworks today. The proliferation of social media platforms, encrypted communications, online marketplaces, and online

[140] Eurojust/SIRIUS (2024); INTERPOL and WCO, 'Operation Thunder 2023'
[141] UNODC, World Wildlife Crime Report 2024; Wingard and Pascual (2018)
[142] Eurojust/SIRIUS (2024); Davies and Kennedy-Mayo (2026)
[143] ibid
[144] Wingard and Pascual (2018); Singh Tomar (2024)
[145] UNODC, World Wildlife Crime Report 2024; IFAW, 'Digital Markets' (2021)
[146] Wingard and Pascual (2018); UNODC, World Wildlife Crime Report 2024

payment systems has increased the scope of wildlife trafficking networks and made it more difficult to implement measures against traditional wildlife crimes. Wildlife trafficking is more and more moving online and through international borders, and current legislation is becoming more and more challenged to respond to technologically enabled or transnational offences.

This study has shown that cyber-enabled wildlife trafficking is not just the consequence of the technological evolution of wildlife trafficking but an overall shift in the organization, concealment and modalities of the illegal wildlife trade. The use of the tools of species misrepresentation, origin laundering, documentation fraud, digital concealment and claims of lawfulness are all vehicles traffickers use to hide the illegal nature of wildlife transactions.[147] These practices take advantage of technological infrastructures, as well as regulatory gaps, posing new challenges to investigators, regulators and policymakers.

This comparative analysis of India, United States and the United Kingdom shows that the three jurisdictions all criminalise illegal trade in wildlife but have not created a detailed and comprehensive legislation dedicated to tackling cyber trafficking in wildlife.[148] The key difference is less about legal bans and more about the extent of institutional coordination, digital investigative ability, and regulation concerning online spaces.[149] Current laws and policies remain largely focused on physical trafficking scenarios and have not been able to effectively address wildlife crimes in decentralized and transnational digital domains.

The study also shows that cyber-enabled wildlife trafficking is increasingly at the nexus of environmental crime and digital regulation. Therefore, there is a need for increased synergy between wildlife protection law, regulation of cybercrime, governance of digital platforms and international law enforcement co-operation in order to respond to the challenges effectively. To combat new generation wildlife trafficking in the digital era, strengthening digital investigative capacity, facilitating access to electronic evidence, institutional cooperation, and more coherent approaches to regulation will be crucial.

Finally, it shows how environmental damage now works through networks and through digital technologies, which are beyond the scope of regulation. In this context, a greater degree of convergence is needed between wildlife protection, digital government, and transnational environmental cooperation. As the effects of environmental damage spread through technology, the capacity of legal systems to respond to techno-environmental harms is likely to become a major influence on the effectiveness of wildlife conservation and environmental governance going forward.

[147] Wingard and Pascual (2018); IFAW, 'Digital Markets' (2021)
[148] Wild Life (Protection) Act 1972; Lacey Act 1900; Wildlife and Countryside Act 1981
[149] Singh Tomar (2024); ICE HSI, 'Wildlife Trafficking Program'; Crown Prosecution Service, 'Wildlife Offences' (2022)