International Insurance Law Review
ISSN: 0968-2090
Vol 34 S1 (2026): Special Issue
https://lumarpub.com/iilr

Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress

Anik

Author Biography: *Advocate Anik M. Iktear Uddin, LL.M. (Business Law), Second Rank Holder from Bangalore University, lifetime alumnus of University Law college, Bangalore, well-known criminal lawyer since 2010 and member of the Karnataka Bar Association, special public prosecutor for the government of Karnataka, managing partner at Prime Legal, Author of various books, national awardee advocate, and recipient of various appreciation from different state law enforcement agencies and best-known cybercrime lawyer.*

INTRODUCTION: WHEN TRUST BECOMES A TRAP

Trust is an extremely important resource and a potentially dangerous threat in the modern business environment, personal relationships and online communication. Trust is an asset of ours and a greatest weakness in a period where people can reach out to each other on an emotional level easily. The 21st century has revolutionized the concept of intimacy. Discussion now occurs on a screen, romance has become virtual, and dating is usually a mouse-click. However, behind this otherwise refined manner of individuals becoming acquainted with one another is a frightening reality, the trust has turned into a weapon. What starts with a feeling of warmth, friendship and emotional involvement, usually turns out to be lying, manipulation and financial exploitation. The issue of a so-called honeytrap where emotional or sexual contact is feigned with the view of exploiting, blackmailing, or extorting has become a big social and legal concern. These scandals are no longer limited to spies and scandals with celebrities. This is making them grow more significant to professionals, businesspeople, students and ordinary people. Their working styles are too often gruntingly alike. A person is contacted via dating application, social media, or even a work-related talk. It painstakingly develops emotional rapport, pushes comfort zones and after trust has readily developed the lying begins. It may begin as a solicitation of funds but it may soon degenerate into coercion, blackmail or even threats of exposure through personal communications or photographs. Under the guise of emotional trust, personal information or private business or data are stolen in more complicated situations. This compounds emotional and financial fraud that is not only very complex but damaging as well.

This type of exploitation is the most dangerous due to the psychological factor of this matter. Victims may struggle to know when they crossed over into being manipulated by love. They remain silent due to their shame and self-blame and are scared of the opinion others will hold about them. They fear that they will be mocked at by going to the police, that their personal life will be exposed to the eyes of everyone, and that the law will fail to realize the emotional infidelity. However, under the emotional facade, there is an evident legal offense that fits the descriptions of cheating, extortion, criminal intimidation and invasion of privacy. In legal terms, honeytraps and relationship-based lies expose the differences between morality, consent and criminality. The Bharatiya Nyaya Sanhita (BNS), and the Information Technology Act, 2000 are solutions; however, they are fragmented, reactive and often ineffective to deal with the compound harm that emotional and online lies can bring. The action of emotional exploitation is more nuanced, immaterial than thievery or force. As an example, one can find some evidence in personal messaging, deleted chats, or non-physical promises of love. Since there is no self-governing body of laws that addresses fraud

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

in intimate relationships, victims are usually required to apply sections of a few statutes, which solely apply to sections of their woes. It is not only a matter of an individual. It is more of a social problem with technology becoming both a means and a weapon, intimacy being commodified and emotional borders being broken. Voice cloning using AI, deepfake films, and high-tech internet impersonation have rendered lying on a scale and with an accuracy never witnessed before. One altered photograph or chat log digitally can now accomplish what previously required a lot of effort on the part of individuals.

We are also witnessing increasing instances of instances of private trust becoming public humiliation in terms of advocates. Clients enter the chambers not only with a broken wallet but also a broken heart, having their dignity on the line, with the legality uncertain. This is not just a case of a few incidences but a larger trend of emotional and cyber exploitations that transcend the boundaries of classes, gender and geographic locations.

The law must therefore not merely ensure that people are not injured physically. It is bound to recognize emotional and psychological deception as crimes that should be not only guarded but also corrected as well. The Supreme Court recognized privacy as a key right in *K.S. Puttaswamy v. Union of India, 2017*[1]. The legal system has already been made more humane. but the way before must have more than that. It requires specific legislations, digital literacy and practices that are responsive of victims and safeguard them rather than causing them to feel embarrassed with reporting.

The matter is not only on the part of the law but it is also on the vulnerability of people in the digital era. The emotional abuse flourishes where the individuals lack knowledge of it. It can be stopped by first knowing that the law can punish. The early warning signs of manipulation, cautiousness over the Internet, and familiarity with the law are the first steps you can take to ensure that you are not tricked. This somewhat complicated topic is the purpose of this essay as it will examine the Indian law, as is, dealing with the deception and monetary exploitation in intimate relationship, and see the weaknesses of the law and what individuals can do to protect themselves both legally and practically. When filters can make people fall in love and computers can demonstrate that relationships do exist, it is even harder to distinguish between emotional truth and legal fraud. The modern dilemma of the law is not only the one which tries to punish after the damage is done but to predict, prevent and enable. Trust is something that is very difficult to regain once lost. However, when you know the law and have it yourself, then you may have the opportunity to defend it.[2]

I. UNDERSTANDING TRICKS AND HONEYTRAPS

Honeytraps rarely begin with pressure- they begin with comfort

Honeytraps are much more than spying or spy movies in the contemporary personal and business relationships. The Honeytraps is a strategized manner of controlling the feelings, affection, existence or thoughts of a person so as to get something out of them that they do not know about. This may be money, reputation or otherwise. The honeytrap of the modern world has transformed into an instrument of intelligence activity to a versatile danger that could occur on social media, dating applications, in business, and even in marriage or individual relationships.

[1] *K.S. Puttaswamy v. Union of India, 10 SCC 1 and AIR 2017 SC 4161.*

[2] Ms. Aswathy Nair, Dr. Devashree Awasthy, Ms. Aarzoo Bishnoi *"Honey Traps in India: A Legal Analysis, Case Studies, and the Imperative for Legislative Reform"*. Volume 3 | Issue 5 | May 2025 Available at: https://theacademic.in/wp-content/uploads/2025/06/30.pd

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

The issue with this type of exploitation is that it is so unobtrusive and complicated. Money or physical items are also stolen in plain sight, unlike when money or other items are stolen in honeytraps, which most of the time exploit emotional reliance or professional trust and close personal relationships to deceive individuals. This makes them the more difficult to find and to prove. Even a mere conversation, some useful advice, or a confession can gradually become a form of manipulation of a person, placing him/her in a situation that costs him/her money, damages his/her reputation, or leaves him/her extremely angry.[3]

Honeytraps can be of many different forms and each of them has its own qualities, purposes and consequences, including:

1. Manipulation of money

"Financial Harm in close relationship usually begins with emotional reliance"

Typically, the most notable and damaging aspect of honeytraps right off is financial manipulation. Financial exploitation, conversely, has actual losses, which harm personal and professional life. The distinction between honeytraps perpetrated financial fraud and non-honeytrap perpetrated fraud is that the former depends on trust and proximity and the strength of relationships. The offenders rely on emotional attachment or professional reputation to make victims hand over money, property or other personal financial data.

A. Normal Situations

Romantic or intimate relationships: Abusers tend to seek money through emotional attachment, dependency or love in romantic or sexual relationships. The manipulation typically begins with the gradual building of trust and affection, often by communicating with one another often, they should be given emotional validation and appear to be loving, or to be interested in their future dreams. After getting the victim emotionally dependent on the offender, the offender then takes his/her time to raise a financial tale, mostly in the form of a pressing need or an investment.

Others popular tricks include luring the victim into investing in a non-existent or malicious enterprises, requesting them to give them temporary financial assistance on false grounds (such as medical, financial situations, traveling or family issues, demanding luxury gifts or loans that do not get repaid, etc. In more complex scenarios, the offenders will exploit victims by pretending to assist them in preparing their finances in partnership or make life easier in the event of a crisis by gaining access to their bank accounts, digital wallets, or credit cards.

As an illustration, a person who is posing as a love partner can fabricate a medical crisis or claim that their bank account has been frozen and they need money immediately. Emotionally affected victim forwards the money without verifying the claim since they care about the individual and do not want to lose his trust. This means short-term and often irreversible financial loss.

Work or business relationships: Honeytraps does not only occur in personal cases but they usually occur in work and business too. In the given instance, emotional or psychological manipulation is associated with commercial dishonesty. Attackers can use the trust between colleagues, shared business objectives, or professional respect to access confidential information, obtain resources that they are not entitled to access, and make decisions that damage their finances.

This can be used to gain access to sensitive trade secrets, corporate data or intellectual property by imprisoning someone to work together; compelling or inducing some executives to sign forged contracts or approve payments; or fooling victims into joining joint ventures that are only on paper.

[3] Honey Trapping in Cybersecurity Available at: https://community.nasscom.in

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

As an example, a criminal who is an investor or business associate can gradually establish a relationship with a company executive to a point that he/she is willing to accept payment or transfer company funds to a non-existent project. Such acts do not only cost the company some money, but also expose it to litigations, tarnished image and internal punishment.

Forcing into contract: The victims can be duped or even coerced to sign legally binding contracts without necessarily knowing what they entail. The victim signs document relinquishing property rights, running a business, or imposing financial burdens on him or her because the person who asked them to sign them is in an authority position.

Some common signs are:

● Joint ownership transfers that are aimed at passing the ownership of property to the offender;

● Investment agreements or joint deeds limiting the victim in terms of his/her financial or decision-making autonomy;

● Loan contracts that represent professional partnerships.

These types of contracts are also employed to ensure that people are under control and exploit them after signing. It is not uncommon to have to wage a lengthy battle against them in a court of law claiming to have been defrauded, misrepresented, or under duress as stipulated in the Indian Contract Act, 1872 (Sections 14-19).

B. Digital Facilitation and Cyber Exploitation

"Online connection form quickly, but they deserve careful boundaries"

Online sources such as social media, dating applications, and career networking websites have turned honeytrap trickery into a lot more global and covert. The digital channels enable criminals to operate across borders and they conceal their identities too making it difficult to probe and reclaim.

Some common strategies are:

● Fraud in Online Banking and Fintech: deception in the form of a trusted individual or an official in the bank to lure individuals to remit money to him through the internet.

● Cryptocurrency and Digital Wallet Schemes: stealing money that cannot be recovered or investigated by the blockchain through the anonymity and irreversibility of transactions.

● Phishing and Social Engineering Phishing and Social Engineering involves the sending of counterfeit messages or links that appear to be sent by trusted organisations to make people provide personal data, such as OTPs, passwords, or bank details.

The cross-border and pseudonymous attributes of these digital schemes give challenges with the existing legal regimes. Information Technology Act, 2000 (Sections 66C and 66D) provides solutions to identity theft and impersonation but in many cases implementation of these laws requires cyber-forensic research, international co-operation, and assistance with lawyers who have specialized training.

C. Psychology of Financial Honeytraps

"Trust is valuable, but it should grow with understanding, not urgency"

The manipulation of the mind that is involved in honeytrap works is as significant as the money or technology that is involved in honeytraps. By exploiting such fundamental human feelings as trust, empathy, attachment, and terror, criminals make other people be dependent on them.

Trust and Emotional Attachment: the victims are trained to believe the offender to be caring or

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

trustworthy, which defeats their ability to judge and resist.
Fear of Loss or Abandonment: This could be emotional withdrawal, social humiliation, or exposure by the perpetrator to demand compliance. This system of control by fear is a successful replacement of the rational choice with emotional obedience.
Cognitive Bias and Optimism: Victims are biased because they are part of the event, hence perceiving that the intentions of the offender are real in ignoring any evidence that the offender is lying or being inconsistent.
The mixture of cognitive distortion and emotional exploitation makes individuals less independent, more difficult to notice fraud, and less likely to report abuse due to the feeling of shame or denial.
For Instance: A young man from Bengaluru was honey trapped by a woman he met through a dating app: the woman named Kavipriya created an account on the Happn dating app and became acquainted with the victim. They later met at a restaurant, where both of them consumed alcohol. As the victim became heavily intoxicated and was unable to return to his PG accommodation, Kavipriya took him to a lodge. After giving him food, he lost consciousness, and she allegedly took his gold chain, gold bracelet, and a headset, collectively valued at ₹6.89 lakhs[4].

D. Long-term Effects
The effects of finances abuse are far reaching and extend beyond financial loss in the short run.
● Personal Impact: Victims might need to cope with long-term debt, poor credit, and a psychological issue. Breach of emotional trust may lead one to be less sure of themselves and reluctant to form new relations.
● Professional Impact: Employees or leaders who are in business or other leadership roles may lose their credibility due to the loss of their reputation, investor trust and investigation in-house.
Issues with the law and processes: cross-border electronic transactions, counterfeit cryptocurrency firms, and lawbreakers operating in multiple countries complicate the recovery of money via the law. The victims usually need the assistance of individuals in various disciplines as including cyber-forensics, lawyers and therapists.
A full-scale plan that should involve taking legal action, learning to use technology, and therapy are required to get back to the state of financial and emotional stability.

2. Capitalizing on Heaven and Hell:
A. The Knowledge of Emotional Exploitation
Emotional exploitation is a coordinated and strategic attempt to manipulate the emotions, thoughts and decisions of a victim to benefit or dominate him/her by the culprit. Emotional exploitation is less apparent than physical or financial abuse. It occurs in terms of emotional dependence, cognitive distortion, and psychological manipulation.
The primary objective might be to receive money, receive information or receive control, but the tool is psychological coercion. It is gradually trained to make victims doubt what they see and hear and this encourages them to go with the flow and unlikely to resist or report to another person about the abuse.

[4] https://www.indiatoday.in/cities/bengaluru/story/bengaluru-couple-arrested-for-drugging-robbing-youth-in-dating-app-honeytrap-2821236-2025-11-17

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

B. General Psychological Foresight

"Emotional Manipulation often hides behind concern and reasonable"

Gaslighting: Gaslighting is a style of influencing the mind of a person by distorting facts, refuting a historical event, or going against the reality to make the victim question their own recollection, perception or sanity. This leads to confusion, self-uncertainty and emotional addiction in the long run.

● At the work place: An employee/person that has wronged someone might cast blame on the victim to an unsuccessful project or poor money management that leave him/her questioning his/her abilities.

● With personal relationships: A controlling spouse might not keep commitments, or may not even speak to the victim, so that he or she will question what he/she recalls of what transpired.

This type of conduct may result in claims of emotional distress under the tort law. More crucially, in more severe instances, may also be applied in accordance with Section 498A IPC (cruelty in relationships) wherein emotional abuse is mentally painful (or coercive).

Emotional Blackmail and Coercion: Other forms that people who hurt others use to dominate them are through emotional manipulation where they can threaten others, make them feel guilty or they can only show love when they do what they want. Some examples are:

● Risking to ruin a relationship in case of demands to be met financially or personally;

● Trying to expose personal or humiliating material;

● Embarrassing someone publicly to achieve something.

In the event of this type of conduct being threatening, it might be deemed criminal intimidation as per Section 351 BNS or extortion as per Section 308 BNS in case it involves illegal requirements.

"When affection is conditional freedom quietly disappears"

When people depend on emotions: They tend to want to make their own decisions in personal or professional life, which are created, Dependency and Too Much Control. They influence or manipulate decisions regarding money, employment and personal life and often impersonate that they are interested or making plans on their future.

As an example, a romantic partner may force them to handle all the finances or even decide on the job of the victim by claiming it is out of love or protection. This slowly undermines the independence and autonomy of the victim making him or her legally and psychologically vulnerable.

C. Psychological Effects

The psychological impact of emotional exploitation in the long term is great and diverse. The victims often experience enhanced anxiety and stress caused by the continuous manipulation, as well as by their depressions caused by the feelings of powerlessness, self-reproach, and betrayal. They can be severely harmed in their belief in relationships, colleagues, and even in their personal judgment. The mental deficits may cause them to find it difficult to make decisions as they increasingly look at the manipulator to assist them. In severe cases, long-term abuse or threats to one's social or professional position can lead to post-traumatic stress with long-term emotional and psychological trauma.

D. In a Business Setting

Emotional exploitation is not a personal relationship phenomenon; it has become a serious

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

problem and even in the business and company environments. The offenders could attack CEOs, supervisors, or co-workers and employ deceit to alter strategic move, embezzle funds or gain access to confidential operational or financial data. Emotional pressure can also be employed to acquire such things as contract approvals, access to valuable resources, or decisions that favor the manipulator over the organization in a corporate partnership. Continuous emotional manipulation may in the long run disintegrate trust in teams, establish a culture of fear and mistrust, and significantly reduce productivity and morale at work. Such cultures are harmful, not only to the performance of the economy, but also place organizations in danger of legal and reputational issues as the actions taken under the imbalance of influence may be identified later or become a subject of the regulatory inspection.

In case of: *Mukesh Kumar V. State of Haryana (2025)*: Faridabad court rejected the bail plea of Mukesh Kumar, alleged mastermind of a honey-trap gang accused of extortion of Rs.33 Lakh by falsely implicating a businessman in a rape case, the court said that granting bail at this stage would shake public confidence in justice system.[5]

3. Sexual and Reputational Abuse

"Damage to reputation often lasts longer than the relationship that caused it"

Sexual and reputational exploitation is one of the most detrimental and invasive forms of honeytraps. It occurs when criminals manipulate sexual, personal, or reputational vulnerabilities of a victim to acquire power, generate money, or alter his or her mind. The effects of sexual and reputational exploitation, in turn, may extend beyond personal, social and professional areas. This cannot be more difficult to the victims seeking support or legal action.

For instance, "A senior physician employed as the head of department at a reputable hospital falls prey to a honey trap. He was filmed in the nude and extorted large sum of money by threatening to let the video go public and even file a false rape case." [6]

A. Coercion of the revealment of personal information

One of the most common applications of sexual and reputational honeytraps is to threat to disclose personal and sensitive data. Individuals who commit evil acts can obtain photographs, videos, or conversations apparently by appearing credible, affectionate, or business-like and leverage them. These types of threats may be financial coercion, in which victims are made to pay money or relinquish property to keep their secrets confidential, or behavioral control, in which victims are made to do against their best interests, such as doing favors or making specific choices. The emotional impact is also enormous; the fear of being discovered usually causes people to become nervous, humiliated, and submissive which makes them easier to do what the abuser desires. In the case of an online dating ordeal, the recordings can be made privately and the partner can demand money in which case they might release the records or just withhold the pictures and records and ask the partner to pay.

[5] https://lawbeat.in/top-stories/faridabad-court-denies-bail-to-honey-trap-mastermind-33-lakh-extortion-of-businessman-exposed-1517724

[6] https://timesofindia.indiatimes.com/city/nagpur/top-hospital-hod-falls-in-honeytrap-seven-arrested-in-daring-trap-operation/articleshow/126083934.cms

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

B. Defamation and Damage to Reputation

"What begins as professional cooperation can turn into exploitation, When trust is assumed rather than verified"

Honeytrap usually exploits vices in the reputations of the people, particularly in the workplace and social arena. Bad people are also likely to disclose personal information to damage the reputation of another individual or their relationships, spread rumors to damage the reputation of another person, or intentionally betray colleagues, clients, or social media. This defamation may result in missed economic opportunities, ruptured business relationships and a social stigmatization that may continue over a long period. As an example, one of the corporate associates may leak confidential messages or tell falsities about the way in which a victim would behave in the office which will create troubles at the workplace and render a victim less credible in the organisations.

C. Coercion at the Workplace or in Marital Relationships

A weapon can be a personal or professional information which is sensitive in nature to gain control or influence the choice of decisions. In a marriage, the threat of revealing secrets, cheating, or subjecting other personal flaws may alter the way the people behave at home. The business world is a business where business decisions are influenced by confidential company information or communications, or financial records in order to get a business contract passed, or to control the use of resources. Victims often do what they are instructed to maintain their status in society, preserve their personal relationships or safeguard their career growth. Moral, emotional, and professional pressures may easily confuse the victims and hence they find it difficult to oppose or report the manipulation.

D. Psychological and Social Effects

Reputational and sexual exploitation have profound and long-term effects on both mental and social health. Emotions are usually traumatized in victims, and may encompass anxiety, despair, humiliation and low self-esteem. Professional setbacks are also numerous and might complicate the process of climbing up the career ladder, damage your reputation and also complicate interpersonal relationships at work. The isolation of victims also leads to their social isolation since they disconnect themselves to networks in order to be noticed or judged. Besides, most victims do not want to go to the court as they fear to have their shame in front of the crowd, being sidelined by their colleagues, and even be fired. This allows the criminal gangs to continue exploiting them.

E. The Significance of Digital Technology

The sexual and reputational exploitation has become more widespread and sophisticated due to the development of digital communication. Pictures, videos, and texts can be easily distributed through a number of platforms, and it only exacerbates the situation. There are new technologies, deepfakes and AI-generated media, which produce fake content that can cause people to appear bad in risky situations. There are also several apps, devices, and territories that contain digital footprints, which complicates the processes of evidence collection and prosecution. An example is when a manipulator can threaten a professional to harm his/her reputation with a deepfake video unless the required actions are performed. This is an amalgamation of hi-tech technology with psychological strategies which are intended to frighten individuals.[7]

[7] Ahona Rudra, *"Honey Trap Scam: Meaning, Examples & How to Avoid"* Available at:

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

II. LEGAL CHARACTERISATION UNDER INDIAN LAW

"Law recognizes harm even when it is emotional or digital"

The idea of honeytraps, the art of manipulation by deception itself, the use of trust, closeness, or emotional weakness to gain illicit gain, has a more delicate presence in the context of Indian law. The law has yet to come up with a single statutory definition of relationship fraud. Nevertheless, its core business of deception, coercion, extortion, and electronic privacy is explicitly defined in the Bharatiya Nyaya Sanhita, 2023 (BNS), the Information technology Act, 2000, as well as under the family, contract, and even tort law. These rules offer a multi-layered approach to restitution by the Indian court system because honeytrap cases often involve overlapping grievances, emotional abuse, financial abuse, reputational injury, and digital abuse. This paper looks into how this activity can be classified legally by the updated criminal code and other related laws and also the case laws and how the doctrine on privacy and consent evolved.

1. The Bharatiya Nyaya Sanhita, 2023 (BNS)

The Bharatiya Nyaya Sanhita (2023) that has replaced the Indian Penal Code (IPC) put the criminal code in the present day and retained the fundamental concepts of not telling the truth, compelling a person to commit something, and exploiting another person. It is also significant to mention that it has the laws that are more adaptable to the current reality, including online coercion, online fraud, and relationship-based manipulation. Honeytrap crimes based on trust, proximity, or emotional vulnerability sometimes implicate more than one BNS provision, particularly the ones on cheating and dishonest inducement.

- Under the Section 318, there are two categories of cheating and Dishonest Inducement (a) and (b).
- Sections 318 of the BNS resemble the previous IPC Section 420, but are more systematic and more current. They also explicitly discuss fraudulent inducement both online and offline. According to these laws, it is a crime when one deceives or lies to another individual to make him do something, surrender property, money, or any other valuable thing,
- Do things that hurt them, or
- Loss which is unjust or give an undue edge to an offender.

In order to prove a person liable in these sections, the following must be the case:

- Deception or Misrepresentation of Fact: The offender has to appropriate the material facts that matter, create false impressions or conceal the truth in order to manipulate the victim.
- Dishonest Inducement: It has to be purposely undertaken to modify the mind of the victim, which in most cases is conducted through trust, emotional attachment or business relations.
- Resulting Wrongful Gain or Loss: The falsehood must be real in a sense that it harms the falsehood victim or provides an unfair advantage to the criminal.

With honeytraps, lies tend to appear as below:

- Fake emotional investment: The offender of this kind of investment fakes romantic interest or love to obtain financial or other means.
- Faking an identity: Fabricating false social media identities or business names or personas

https://powerdmarc.com/what-is-a-honeytrap-scam/

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

to appear credible or influential.

- Bogus business or financial relationship: Making an offer to accept money, investment, or other partnership under a fake or deceptive pretense.

As an illustration, in *Honeytrap Case in Mangalore (The Hindu, 2021)*[8], the alleged assailant tempted the victim into an alleged personal relationship, obtained compromising videos and demanded 30 lakh rupees to ensure that the videos were not leaked. The offense satisfied the demands of Subsections 318 BNS because any disinformation was provided intentionally and the victim was forced to act contrary to her interests. The court has observed that the deception was there since the start of the conversation, and this is what distinguishes criminal cheating with the usual differences that occur between individuals.

Hridaya Ranjan Prasad Verma V. State of Bihar[9], the Supreme Court clarified that a person can only be liable of cheating in case he/she had the intention of cheating at the time when the inducement was made. This notion ensures that acts of honeytrap-based exploitation, where the initiator would like to lie initially, would be explicitly addressed under Sections 318, 320 BNS. But everyday misunderstandings or post fact conflicts do not count.

2. Information Technology Act of 2000.

The Information Technology Act, 2000 (IT Act) plays a very significant role in addressing honeytraps cases, particularly because an increasing number of individuals are exploiting digital platforms, social media, and online communication in order to deceive and exploit others. The BNS primarily concerns the primary components of deceit, coercion, and exploitation, however, the IT Act has been added to the criminal law system to address cyber-supported offenses, which are the core of the existing honeytrap scams (sextortion, online impersonation, and digital harassment).

A. Fraud by impersonation

Stealing the identity of a person and deceiving him or her (Sections 66C and 66D). Perpetrator of fraud using another person's electronic signature, password or unique identifier is a crime as stipulated in Section 66C. Other section 66D also does not permit cheating through impersonation online by claiming to be another person, which is lying about your online identity in a bid to deceive or steal another person. In honeytrap scenarios, the perpetrators of the crime will normally use fake social media accounts, online dating profiles, or professional identities to mislead the victim. Once this has been done, such accounts are used to retrieve money, private details or personal objects. The significance of such rules is that these ensure that online fraud is perceived as an independent offense, which is significant since the manipulation of virtual identities implies special dangers. They also create an apparent fact that having the knowledge of and a desire to lie is a valuable aspect of committing a crime.

B. Obscene or sexually explicit contents (Section 67 and 67A)

Section 67 renders the obscene materials published, transmitted, or disseminated electronically inappropriate. Section 67A instead, specifically punishes sexually explicit acts involving nudity or pornography and imposes stiffer punishments in sensitive cases or where the minor is involved.

[8] https://www.thehindu.com/news/cities/Mangalore/woman-arrested-in-honey-trap-case/article35138145.ece

[9] *Hridaya Ranjan Prasad Verma v. State of Bihar (AIR 2000 SC 2341)*

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

The honeytrap activities may also involve threats to release personalized sexual content, which is also referred to as sextortion or revenge porn. The passages present a tangible legal solution to the problem of distributing such content and allow the government to punish the violators who exploit personal photos to exert coercive power. The court established a precedent of prosecuting internet harassment and sextortion by stating that fictitious digital identities and pornography are potentially important crimes in case of *Suhas Katti v. State of Tamil Nadu,* 2004. Courts are beginning to understand that there can be physical implication of what one does on the internet. In India, it is illegal to use electronic communication in lying, blackmailing, and damaging someone. The examples of modern honeytraps prove that it is essential to be cautious of your digital privacy, of your online behavior and to make use of the law to your advantage. This is an indication of the significance of the IT Act in the modern world.[10]

C. Invasion of privacy or confidentiality of the person (Section 72)

Section 72 penalizes the individuals who disclose information they acquired in confidence, through technological means without authorization. This is specifically significant in situations where honeytrap offenders enter private messages, images, or letters and intimidate them in order to receive money or other goods. Section 72 discusses the importance of violating trust, which occurs in the context of digital interactions. It further adds that the information, which was acquired illegally privately or on an individual basis, cannot be used in blackmailing or obtaining something. Section 72 is also available to criminal justice to victims of honeytraps whereby the victim is manipulated with access to personal content acting as leverage, alongside civil actions such as injunctions or damages.

D. Its effectiveness with BNS and others.

The IT Act is not a standalone legislation. Honeytrap crimes are associated with a great number of crimes that occur simultaneously. To give one example, digital compulsion would assist in financial fraud, defamation, or criminal intimidation. BNS Sec 308 and Sec 351 (Extortion and Criminal Intimidation) can be utilized, in the case when one threatens to reveal something on the internet. Posting of personal materials might result in BNS Sec 77 and Sec 78 (Voyeurism and Stalking) and IT Act Sec 67A. Frauding/Impersonation Fraud Lying or falsifying identity: This is Sec 66C-66D of the IT Act and is combined with BNS Sec 318 (Cheating and Dishonest Inducement) and is to ensure that victims have claimed damages on criminal and civil cases against any individual who lies and defrauds them using a sweet butter trap or a honeytrap online.

3. Family and Contract Law Framework of Honeytrap Cases

Lying intentionally to gain a personal, financial, or marital advantage could also be involved in honeytrap tactics. Criminal law deals with not only are crimes themselves, but civil remedies under family and contract law can be useful means of safeguarding yourself, repayment of money, and attorneys' services. These are the legal instruments that enable the victims to terminate fraudulent marriages, strike invalid contracts and receive compensation in their emotional, social, and economic injuries.

[10] *Suhas Katti v. State of Tamil Nadu (C No. 4680 of 2004)*

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

A. Section 12 of the Hindu marriage act, 1955,

Provides any marriage through fraud or concealment of important information to be invalid under the family law. Section 12 of the Hindu marriage act provides the jurisdiction of courts to abrogate a marriage obtained through fraud or concealment of important information. The law states that the fraud should have to relate to something of immense significance to the marriage such as:

- The information about the age, marital status, and other details of the person.
- Covering up some significant health issues or infections that are communicable.
- Fibbing about in regard to financial status, home ownership or debt.
- Lies regarding fidelity, dedication or readiness to fulfill marital duties.

Within a honeytrap situation, one belligerent party can deliberately lie about his or her identity, marital status, financial position, or even intentions with the view of pressuring the other party into getting married or acquiring property, money, or social power. It nullifies the consent, which is a basic constituent of a valid marriage, thus rendering the marriage voidable at the will of the cheated partner.

In *Saroj Rani v. Sudarshan Kumar Chadha*[11] passed a decision by Supreme Court, according to which concealing or misrepresenting significant information, which passes to the root of consent, renders the marriage unlawful. The Court has emphasized that the consent must be truthful and transparent and any intentional concealment or falsification that contradicts the consent can be brought to court in accordance with the provisions of Section 12. This will assist them in recovering their legal rights, gaining possession of their property and cease to be exploited due to the false marriage. This structure ensures that individuals cannot be coerced into getting into relationship that was established through lies, hence the significance of consent in marriage legislation.

B. Fraud and Misrepresentation in Contract Law (Sections 17-18, Indian Contract Act,1872)

Financial and professional exploitations can also be experienced courtesy of honeytraps, in which an individual deceives another to give him or her money, enter into agreements or divulge personal details. This may be lying that you are in love, giving false promises of a professional partnership, or lying regarding your identity, what you can or cannot do, or what you desire.

The law places a clear structure on this under sections 17 and 18 of the Indian Contract Act:

Fraud is considered to be any act aimed at deceiving another party into contract including false representation, obscuring facts among other activities performed having the motive of deceiving. Misrepresentation is a kind of statement that it is false and a person does not know that the statement is false but still it influences the consent of the victim.

In such cases, contracts entered into may be canceled at the discretion of the aggrieved party who has the option to:

- Repudiate the contract and leave it never to be.
- Recover any fund, property or possession that was transferred on false claim.
- Request money in order to cover up lies.

The courts consider the motive, significance and the outcome of the false statement. When the misrepresentation is of significant impact on the decision of the victim to sign the contract, the decision is null and void and the victim can seek assistance. Notably, the digital or online agreements that were concluded on false grounds are addressed in Sections 17-18 as well. This

[11] *Smt. Saroj Rani v. Sudarshan Kumar Chadha (AIR 1984 SC 1562)*

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

implies that victims will be able to challenge electronically made or online contract.
"Justice becomes accessible when victims understand their remedies"

4. Difficulties and drawback in dealing with honeytraps Cases: Despite the good rules that exist in the Bharatiya Nyaya Sanhita (BNS), the Information Technology Act, and the civil law frameworks, the difficulties associated with securing justice in hacking and relationship fraud cases are numerous. You should be familiar with these limits in order to prevent and enforce better:

A. Lack of coherent Act: Currently, Indian law does not have a definite clause that addresses honeytraps or faking relationships. Rather, victims are forced to depend on a combination of criminal, cyber, family, and contract law. This ruptured legal framework may complicate the identification of what remedies are applicable, decelerate the process and it may not be easy to categorize new or hybrid forms of exploitation, particularly when both digital and personal spheres are involved in cases of deception.

B. Evidentiary Problems: You usually have to examine online conversations, personal photos, or computer payment records in order to find evidence of the honeytraps crimes. There should be strict compliance with rules relating to evidence by the courts including Section 65B of the Evidence Act which states that evidence must be authenticated. The intent, fraud, and causality are more difficult to prove in the case of digital content that can be destroyed, altered, or manipulated. Moreover, private messages can be encrypted or inaccessible and, thus, it becomes extremely difficult to obtain evidence that can be presented in the court.

C. Issues of Online and Cross-Jurisdictional Enforcement: Many honeytraps are conducted across more than one state or nation and most of these occur on social media or dating websites. This raises issues of who is supposed to prosecute, the effectiveness of law enforcement agencies in co-operation and whether Indian law applies to the citizens of other nations. The process of cross-border investigations is time-consuming due to diplomatic or procedural issues. This implies that the victims will take more time to receive assistance and in some cases the individuals who committed the offense can get away with it.

D. Underreporting Due to Social Stigma: In general, individuals who become victims of honeytrap schemes rarely report the experience, particularly when there was sexual or confidential material. Victims usually do not report to police because they fear being exposed in the society, they are ashamed and they feel they will be judged by others and they will also lose their jobs. This underreporting does not only complicate the ability of individual victims to get justice, but it also complicates the ability to recognize new trends of exploitations, which complicates the ability to intervene and prevent it and institute new policies in the public.

E. Lack of awareness regarding civil remedies: Criminal prosecution is the matter of punishment, whereas the victims are usually not aware of the civil remedies in family and contract law. Most individuals are not aware that they have the right to cancel contracts, terminate unreal marriages, and receive compensation due to emotional and financial losses. This is ignorance and increases the chances of victims being exploited and the ineffectiveness of civil legal system.

F. Need of Strengthening Procedures and Institutions: Based on the above-mentioned issues, both the investigative and the judicial system require reforms, are equipped with specialized digital forensic expertise, and are more sensitive to victims. It would be easier to locate, prosecute and save individuals with more education of the police, judges and lawyers on the digital evidence, online fraud trends and psychological impact of victims. In addition, there can be a campaign to

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

educate the people on the civil and criminal remedies that can be offered in case the victim is a victim to some evil.

III. HOW TO PROTECT YOURSELF FROM EMOTIONAL, FINANCIAL, AND DIGITAL EXPLOITATION

Digital spaces shorten the distance but not removes risk

In the modern globalized society, personal, professional and digital communication is increasingly becoming intertwined such that individuals are becoming simple victims of honeytraps and exploitation based on relationships. In order to counteract such a deception, we must take a proactive step and be multi-layered in that we should be aware of it, be safe on the internet, managing our emotions, knowing the law, and acting swiftly.

1. Digital Security Steps

Modern honeytraps have a substantial portion of digital platforms, and digital security is a necessity. Individuals exploiting others react to the invitation to meet and connect through social media, messaging apps, dating platforms, and LinkedIn to establish trust and dominate their victims. With the increase in the number of contacts occurring over the internet, individuals must be aware that any digital footprint, such as messages, photographs or financial data, may be used to their detriment.

Strong Passwords protects more than accounts, they protect identities

Good Passwords and 2 Factor Authentication: One of the easiest and the most effective ways to defend yourself is to use a strong and unique password in all of your online accounts. Hackers can easily access your emails, social media accounts, or bank accounts in case you use weak or overused passwords. Two-factor authentication (2FA) introduces an additional security measure by ensuring that a password is not enough to log in. This renders it very difficult to intrude on such a person.

Secrecy of personal information: This is something that people need to be very sensitive about when they are making disclosures on the net. This consists of personal data such as the bank account numbers, OTP, and prisoners content. Criminals can also use even the information which appears innocent to commit a fraud, blackmail or steal the identity of a person. Social networking and messaging apps: update your privacy settings to ensure the safety of your information, only share this type of information with trusted and known people on social networking and messaging apps. Individuals reduce their exposure to the possibility of their contents being manipulated or abused by restricting access to their personal profiles, posts, photos, or status updates. In addition, the verification of the apps and platforms authorization on a regular basis ensures that your personal data are not disclosed to strangers accidentally.

Watch out when contacted by an unknown person: Sometimes exploiters begin contacting individuals by sending them unsolicited messages on dating apps, professional networks, or social media. Before attending to them in case of a real discussion or sharing information, people ought to be cautious and ensure that they know who they are talking to. Too pleasant or too pressing messages, solicitation of funds, insisting on a special communication channel is all indications of trouble.

For Instance: In thane district Maharashtra, one senior citizen duped of Rs. 23.5 Lakhs on threat of Digital Arrest, “Digital arrest” is a growing form of cybercrime in which fraudster pose as a law

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

enforcement officials or personnel of govt. agencies & intimidate victims through audio/ video calls, they hold the victim hostage and put pressure on them to pay money[12].

Being able to identify Phishing and Impersonation; There are several times when cybercriminals may impersonate a person or a company that you trust in to obtain confidential information. Users are required to authenticate the identity of the person sending the request to them regarding the need of money, private details or other kinds of favors before they can respond. However, it is possible to prevent phishing attacks and online fraud by being cautious about links, emails, or attachments that appear suspicious.

Documentation and Backup: It is important to have records of all the digital transactions that are made to prevent any safety and other legal claims. Individuals are advised to regularly store their emails, chat logs, screenshots or transaction receipts somewhere secure. In case one makes a legal complaint, such recordings are highly significant since they demonstrate intention, the way people speak to one another, and when someone was exploited or coerced to act.

These measures will predispose people to a significantly smaller likelihood of becoming victims of digital manipulation, identity theft, and online coercion. This makes them safer, both personally and professionally in the digital world of our age.

2. Legal Actions and Legal Protections

The Indian law can address the issues of emotional, financial and digital abuse in a variety of ways. It is highly essential to take legal action immediately since it prevents the occurrence of harm and maximizes the chances of recovering your money and obtaining a verdict. Preservation of evidence is the first and most crucial step that an individual may take in case he is a victim. The citizens ought to maintain a historical record of all their contacts, interactions, and transactions. This must contain some screenshots of conversations, emails, and online receipts, and any other significant financial records. This information becomes critical in establishing the date, motive and actions of the criminal and is the foundation of the criminal and civil processes.[13]

Criminal remedies pursuant to the Bharatiya Nayaya Sanhitha (BNS): Sometimes two or more areas of the criminal law are involved in causing someone to perpetrate honey trapping, in particular, criminal law airing with lying and compelling someone to do something. The section 318 (cheating and dishonest inducement), 308 (extortion) and 351 (criminal induction) can all be applied in case a person acts on the basis of trust to obtain money or personal benefits. As an example, when a person has been compelled to surrender money or property through unscrupulous emotional influence, such clauses will enable bringing of charges with ease. BNS is aware that it is crime when premeditated exploitation occurs where the criminal decides the deception in advance. Trust and vulnerability of the victim are perceived to be aggravating factors by the courts in general.

Information Technology Act of 2000: Cyber Laws: Cyber Laws are a recent addition to the criminal framework as digital mediums have become so significant in contemporary exploitation. Section 66C is concerned with identity theft and criminalizes anybody who wrongfully applies electronic signatures, passwords, and unique identifiers. The punishment may take up to three years of imprisonment and/or fine of up to 100,000/-. Section 66D targets individuals that defraud through

[12] https://www.newindianexpress.com/nation/2025/Dec/22/senior-citizen-duped-of-rs-235-lakh-on-threat-of-digital-arrest-in-thane

[13] http://us.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

deceiving others online like using fake social media or dating platforms. The whole of section 67 and section 67A criminalize the transmission and publication of sexually explicit material, even sextortion or revenge porn. Punishment may take place a maximum of three years imprisonment and/or a fine of up to 5,00,000 rupees. The section 72 also protects privacy of electronic communications and penalizes anybody who discloses sensitive information he received in confidence without authorization. The penalty may take up to two years in jail and/or 100000 rupees fine. These regulations ensure that the processes of digital control and manipulation, as well as coercion, are illegal and can be penalized.

Civil Remedies: In addition to criminal proceedings, the civil law provides the victim with 2 beneficial options of protecting themselves as well as recovering their money. The Indian Contract Act (Sections 17-18) also states that fraudulent or misrepresenting contracts may be cancelled by the defrauded part and thus they will be refunded their money and cancel the agreements. In Hindu marriage, section 12 of the Hindu marriage act gives the courts the power to declare marriages invalidated due to reason of either fraud of material facts. This guards the victims against the exploitation of both the law and the society. The victims may also request injunctions and damages to either end the abuse or dissemination of personal information, and to receive money to cover emotional, financial, or reputational harm by the offender.

"Awareness transforms victims into informed protectors of their own rights"

Cybercrime reporting: In case you have encountered online bullying, identity theft, or any form of online bullying, you may submit a report at the National Cyber Crime Reporting Portal (https://cybercrime.gov.in/). The portal helps easily file complaints and collaborate with the law enforcement to investigate the digital crimes.

Seeking Legal Assistance: Legal advice is very crucial as criminal, cyber, and civil laws are not always clear-cut. A lawyer can ensure that the complaints are written properly, evidence preserved and it is followed up in the most appropriate manner using the right legal channels. Having early legal advice assists victims to navigate through complex processes, prevent further abuse and provide them with the best opportunity of receiving preventive relief and compensation as well. Honeytrap victims and relational exploitation may safeguard their rights, interests and reclaim their personal, financial, and emotional well-being through criminal prosecution, civil actions, reporting cybercrime, and effective legal assistance.

3. Money Safety

People are financially exploited in personal, professional or online settings through honeytraps to their advantage. To prevent such a mishandling, you must be a go-getter and take care of your money. Before providing access to another person to their bank accounts, digital wallets, or other financial tools, people must be very careful. It should never be by trust that one shares authority in money or property. To grant access, one must verify the identity, intentions and credentials of the person seeking access particularly in new and untested connections.

Checking your financial account regularly: This is an important activity of self-defense against being scammed in finances. Individuals are advised to scrutinize their bank accounts, online wallet transactions and investment accounts on a frequent basis to identify suspicious and illegal activities. Even the slightest, unaccounted charge might be an indicator of abuse in earlier years. By learning about an issue at the first stage, you can react immediately, e.g., by notifying banks, freezing accounts, or initiating a lawsuit. This will aid in losing less money.

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

Secured Transactions and Disinterested checks: Individuals are advised to only apply secure and verified channels of transaction of any financial transaction be it investment, loan or transfer. Do not transact through chat programs, third parties, and unverified Internet connections. All these are unofficial and unsafe methods of doing business. The other thing that should be considered is to ensure that everyone involved in a financial transaction is as they claim. This is in terms of verifying credentials, ensuring that business or personal claims are authentic and ensuring that investment opportunities are authentic.

Checks and Balances in Workplace: Financial abuse can present as a normal business at the workplace, or as a company partner. In an effort to prevent such exploitation, companies and individuals are expected to ensure that they establish their checks and balances. A single individual should not possess the entire management of big deals or private financial information. Hierarchy of approvals, two step authentication and frequent auditing all help in ensuring that individuals are responsible and have fewer chances of being fooled or swindled.

Knowing how you feel, and knowing how to spend your money: When money gets into your head, people who fall into honeytraps are generally duped into emotional financial choices. What is equally important is being aware of this mental pressure in the same way that it is of actually making actions to defend yourself. One should never decide to make huge financial choices under the impulse of the moment, particularly when making the decision out of love, the need to, or the duress. Stepping out and thinking objectively about the problem, seeking advice of individuals you are close to, like friends, family or financial advisers and documenting all the agreements or communications can be effective steps to safeguard your financial and emotional health. Careful monitoring, safe methods of transactions, independent checks, and organizational controls can significantly reduce the chances of falling into financial exploitation by people. This happens despite the existence of emotional or digital manipulation. The proactive financial protection is a significant means to protect yourself against the schemes that are complex and often overlapping to each other in honey trap.

"Screenshots and Records often speak louder than memories in law"

Record keeping and documentation: In the case of emotional, financial or digital abuse, having specific records and proper documentations can be one of the most effective methods of ensuring that this does not occur again and also to achieve justice. Recording all the interactions chronologically and keeping accurate records assists individuals in narrating a consistent story regarding what transpired and these patterns depict patterns of lying, coercion or manipulation. This includes recording messages, emails, telephone calls or face-to-face discussions and notes down the date and time and situation where possible. Maintaining a good record would assist the victim in making good decisions and viewing the problems in perspective when he or she feels bad.

Retention of Digital Evidence: In the modern world, screenshots, chat logs, emails and digital receipts are all significant evidence. These facts could support the accusations of dishonesty, giving money or threats. As an illustration, chat archives of social media, messaging services, or dating markets can indicate that some person was attempting to defraud or compel you to make a decision. Storing copies of contracts, agreements or confirmation of transactions may also assist in civil claims under the Indian Contract Act or other similar acts. Storing these records in a secure place preferably in more than one format or device reduces the possibility of them being removed or altered accidentally.

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

In case of *Anwar P.V Vs. P.K Basheer (2014)*[14]*:* Established strict rule for admissibility of electronic evidence, mandating a section 65B Certificate under the Indian evidence act for any electronic record, to be accepted as proof, thereby over ruling prior interpretation, that allowed oral testimony or lessor proof.

Documentation of Threats and Harassment: In case there is exploitation accompanied by threats, harassment, or intimidation, then it is worth noting each episode down on paper. Individuals must document the nature of the threat and the manner in which it was presented as well as the response or reactions. It involves making screenshots of intimidating messages, recording threatening calls, or writing down what was said during in-person interaction. Such evidence may be provided subsequently to the police, cybercrime departments or even civil courts and treated as evidence of what the individual did and to help in asserting claims in the BNS or IT Act.

Chronology and Organization: It is more credible to place documents in sequence as it demonstrates a type of mischief inseparable with time rather than a few acts. Listing files by labels and indexing them with the date and situation helps to locate them when you require it in an investigation or a court case. Storing the backups in a secure storage or cloud services can ensure that the evidence still exists, even in the case when the primary devices are breached.

The maintenance of detailed documents helps to not only enhance the legal grounds of the victims, but also provide them with clarity and control over the matter. Documentation transforms emotions of manipulation that cannot be established into demonstrations that may be utilized in the court. This bridges the divide between emotions and the law. Simply put, records are not only a means to guard against being cheated the second time but also a means to ensure that justice is achieved.

CONCLUSION

The contemporary personal, professional and online world have entirely altered the manner of trust, intimacy and exploitation functions. The dark secrets of honeytraps and relationship-related cons demonstrate a bitter lesson: in age of the internet, emotional vulnerability can be exploited in the most outrageous way, and victims are not only deprived of their money, but mentally traumatized, socially vulnerable, and alone. It is not only money that becomes lost, but emotional betrayal, damaged reputation, deprivation of personal freedom and long-term consequences on mental health, and even job and social life issues are also impacted. Such effects demonstrate the necessity of developing a broader definition of the concept of in harm in relation and cyber exploitation including the psychological, social and financial levels.

The legislation of India, which encompasses Bharatiya Nyaya Sanhita (BNS), the Information Technology Act of 2000 and civil remedies listed in family and contract law, contains useful provisions in addressing these complex issues. The BNS includes penalties against lying, extortion and coercion whereas cyber laws safeguard digital privacy, identity, and personal information. Additional avenues of restitution are available under the civil remedies, like rescission of contracts, fraudulent marriages, claims of emotional and pecuniary loss. Nevertheless, the fact that such laws are fragmented and intersect, as well as the issue of evidence, jurisdiction, and social stigma, demonstrate how poorly they should be transformed, simplified, and implemented, in a more consistent and efficient manner. More and more digital technologies, transnational platforms, and AI-based tools are being utilized in honeytrap crimes. This implies that the law and the police must

[14] *Anwar P.V Vs. P.K Basheer (2014) AIR 2015 Supreme Court 180*

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

be capable of utilizing these tools and be conversant with the law.

It is important to be cautious, prepared, and in action to anyone who may be victims. In order to transform the weaknesses into strengths, it is essential to be sensitive to the red flags, make good records of the experiences, spend the money wisely, and pay a close attention to the online footprint. Early legal advice will ensure the effective prosecution of criminal, civil, and cyber redress, will help in the protection of rights, damages recalculation, and avoid any further exploitation. Individuals should also be mentally fit, emotionally intelligent, and capable of behaving morally on the internet to manage the complexity of contemporary relationships.

Honeytraps demonstrate that we should be more cautious about morality, we should know how to utilize technology and we should have backup systems. Education campaigns in the community, counselling services and community support networks can be used to assist individuals who are in trouble and prevent them being exploited. To prevent professional and financial manipulation, companies and organizations need to introduce very strict rules of work, ensure that no one is unaware of what they are doing, and they provide training programs. Legal, technological as well as societal interventions should work together in addressing the causes and the effects of honeytraps plans.

The world is evolving at a rapid pace, and this makes it difficult in a certain sense. The use of AI in social engineering and deep fake materials, virtual avatars, virtual reality systems, the metaverse, and scams of cryptocurrencies complicate the discovery, gathering, and presentation of evidence in court. Blockchain and encrypted systems ensure privacy and security, yet, they complicate the process of police following money and understanding what one had to do. Laws have to keep on evolving, therefore, to accommodate cyber forensics, AI surveillance, digital evidence standards as well as inter-country collaboration to ensure that individuals are answerable. The exploitation can be prevented at the source with the help of ethical digital design, platform protection, and educating users on how to safeguard themselves.

Greater concerns of morality and society are also raised in honeytraps. They demonstrate the relationship between trust, technology and morality in the way people interrelate with one another today. Laws and technology are not enough to prevent exploitation. We must also have a culture of awareness, being ethical, and responsible on our actions. Educating people on how to operate technology, think and feel about themselves is significant to enable them to be smart and strong enough to identify and prevent the manipulation processes.

Finally, protecting trust - the weakest and most valuable in human relations - requires a forward-looking with multiple components approach. The law, technology, and psychological preparedness, and awareness of the society need to work in harmony to address the changing challenges posed by honeytraps. By taking action, having strong legal alternatives, adhering to organizational rules, and participating in their community, individuals can gain control over their emotional, financial and personal life and are less susceptible to relational and digital deception. Maintaining the balance of digital intimacy, social connectivity, and technical progress, the task of fighting honeytraps should be a collective effort of lawyers, engineers, psychologists, policymakers, and teachers as society still works out the new set of rules. It requires the future hazards to be envisaged, preventative measures to be integrated, and the development of ethical, knowledgeable, and strong societies. Through raising awareness, preparedness, and multi-dimensional intervention, the society is able to transform how individuals interact with one another and with technology, transit trust is not only secure, but also lasting, esteemed, and valued in the 21st

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

century. Honeytraps are not only an issue of law but also an issue of social, technological as well as psychological issues which require comprehensive solutions and a culture of looking out. It is only through such collaborative efforts that the harm caused by lying, deceiving and manipulation can be really reduced and it is imperative to ensure that as human relationships, they remain founded on honesty, respect and integrity

References

Brenner, S. (2021) "Cybercrime, Trust, and Emotional Exploitation in Personal Relationships," Harvard Journal of Law & Technology.

Aggarwal, Gifty (2015), "General Awareness on Cyber Crime. "The International Journal of Advanced Research in Computer Science and Software Engineering. Volume 5, Issue 8. http://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/articleshow/59707605.cms

Anupreet Kaur Mokha. (2017) "A Study on Awareness of Cyber Crime and Security." Research in the Humanities and Social Sciences. 8(4): 459–464, October to December.

Achuthan, K., and Khobragade, S. & Kowalski, R., (2025) "Cybercrime via the public lens: A longitudinal analysis". Humanit Soc Sci Commun 12, 282. Available at: https://doi.org/10.1057/s41599-025-04459-x

Annapurna Jonnalagadda et al. (2015). "Emerging Trends in Cyber Crimes and Their Solutions". International Journal of Multidisciplinary Advanced Research Trends, Volume 4, Issue. 4(2), pp: 1-8. https://cybercrime.gov.in/Webform/CrimeCatDes.aspx

In the Lawyers Collective, "Cyber-Crime: Hardships to Curb it." 16 No. 9 (September), Vol. 1, Pati, Parthsastry (2001) pp. 26–27.

Suresh T. Vishwanathan (2001): "The Indian Cyber Laws" Bharat Law House, 3rd Edition 2022

S. Subramanian "Combating Computer Crime" in The Hindustan Times (December 18, 1995), p. 12

S. Thangamayan, Murugan Ramu, S. Selvaraju, (2023) "Cyber Crime and Cyber Law in India: A Comprehensive Study with Special Reference to Information Technology". IJRITCC 2023, 11, 2903–2906.

Smith, R. G. (2013). "Fraud and stealing someone's identity. In the Handbook of Internet Crime" (pp. 291-319). Willan.

Taneski, N., and Karovska Andonovska, B. (2020). "Legal aspects of cybersecurity. Security Dialogues–International Peer Reviewed", 11(1), 99-110

Ms. Aswathy Nair, Dr. Devashree Awasthy, Ms. Aarzoo Bishnoi, (2025) "Honey Traps in India: A Legal Analysis, Case Studies, and the Imperative for Legislative Reform." Volume 3 | Issue 5 | May 2025 ISSN: 2583-973X

Anmol Shekhar Srivastava Akhilesh Dwivedi, "Honey-Trap Espionage in India: A Psychological Perspective through Content Analysis of National-Level Cases" ISSN: 2581-6918 (Online), 2582-1792 (PRINT).

PRIME LEGAL, (2025) "Cybercrime Legislation and Enforcement Challenges in the Digital Age" Available at: https://blog.primelegal.in/cybercrime-legislation-and-enforcement-challenges-in-the-digital-age/

PRIME LEGAL, (2025) "Supreme Court Orders CBI Probe into Digital Arrest Scam Cases; Directs States to Provide Mandatory Consent" Available at: https://blog.primelegal.in/supreme-

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

court-orders-cbi-probe-into-digital-arrest-scam-cases/

PRIME LEGAL, (2025), "Compliance Risks and Obligations for Companies Under The Digital Personal Data Protection Act, 2023" Available at: https://blog.primelegal.in/compliance-risks-and-obligations-for-companies-under-the-digital-personal-data-protection-act-2023/

PRIME LEGAL, (2025), "Judicial Approach to Balancing Free Speech and Hate Speech in India" Available at : https://blog.primelegal.in/judicial-approach-to-balancing-free-speech-and-hate-speech-in-india/

PRIME LEGAL, (2025), "The Scope of the Right to Privacy in the Indian Constitution: Post-Puttaswamy Analysis" Available at: https://blog.primelegal.in/the-scope-of-the-right-to-privacy-in-the-indian-constitution-post-puttaswamy-analysis/

PRIME LEGAL, (2025), "Cyber Law – Role in Combating Dark Web Crimes" Available at: https://blog.primelegal.in/cyber-law-role-in-combating-dark-web-crimes/

Panigrahi, S. (2025). AI in HR: Impact of artiLicial intelligence on transforming human resources. *The American Journal of Management and Economics Innovations.*

Panigrahi, S. (2025). AI in HR: Impact of artiLicial intelligence on transforming human resources. *The American Journal of Management and Economics Innovations.*

Parry, E., & Battista, V. (2019). The impact of emerging technologies on work: Implications for HR. *Frontiers in Psychology, 10,* 1792.

Paul, S. (2025). Development of digital-era human resource management techniques: A review-based study. *International Journal of Psychosocial Rehabilitation.*

Paula, S. (2025). Development of digital-era HR management techniques. *International Journal of Psychosocial Rehabilitation.*

Paula, S. (2025). Development of digital-era human resource management techniques: A review-based study. *International Journal of Psychosocial Rehabilitation.*

PeopleManagingPeople. (2023). *HR digital transformation: 5-step process and best practices.* https://peoplemanagingpeople.com

Sarantis, (2024). The critical role of HRM in AI-driven digital transformation: A paradigm shift to enable Lirms to move from AI implementation to human-centric adoption. *Discover ArtiQicial Intelligence.*

Sarantis, (2024). The critical role of HRM in AI-driven digital transformation. *Discover ArtiQicial Intelligence.*

Savant, R. S. (2025). The future of work: Evolving HR strategies for a digital workforce. *Journal of Informatics Education and Research, 5*(2).

Savant, R. S. (2025). The future of work: Evolving strategies in human resource management for a digital and agile workforce. *Journal of Informatics Education and Research, 5*(2).

Shahiduzzaman, M. (2025). Digital maturity in transforming HRM in the post-COVID era. *Administrative Sciences, 15*(2), 51.

Shahiduzzaman, M. (2025). Digital maturity in transforming human resource management in the post-COVID era: A thematic analysis. *Administrative Sciences, 15*(2), 51.

Susanti, D., Rachmawati, R., & Anugrah, R. (2023). Digital transformation in HR practices and its impact on organizational performance. *Journal of Organizational Change Management, 36*(2), 245–263.

Wahdaniah, S., et al. (2023). Human resource management transformation in the digital age. *International Journal of Applied Research and Sustainable Sciences.*

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.

Wahdaniah, S., Sucianti, R., Ambalele, E., & Tellu, A. H. (2023). Human resource management transformation in the digital age: Recent trends and implications. *International Journal of Applied Research and Sustainable Sciences.*

Mahajan, N. (2025). Augmented Intelligence in Program Management: Enhancing Human Leadership with AI; PM World Journal, Vol. XIV, Issue VII, July. Available online at https://pmworldlibrary.net/wp-content/uploads/2025/07/pmwj154-Jul2025-Mahajan-Augmented-Intelligence-in-Program-Management.pdf

Mahajan, N. (2025). Governance of Cross-Functional Delivery in Scalable Multi-Vendor Agile Transformations; International Journal of Applied Mathematics, Vol. 38, No. 2s, pp. 156–167. Available online at https://doi.org/10.12732/ijam.v38i2s.75

ABOUT THE AUTHOR

ADVOCATE ANIK M IKTEAR UDDIN

When conversations begin about courage, innovation, and excellence in India's modern legal arena, one name stands out unmistakably—Advocate Anik. M. Iktear Uddin, fondly known as Advocate Anik. Based in Bangalore, he is widely celebrated not just as a brilliant lawyer, but as a visionary force shaping the future of law, technology, and justice in India.

From humble beginnings in Jalpaiguri, West Bengal, to emerging as one of India's most trusted legal minds, his journey stands as a testament to grit, passion, and unwavering commitment to the law. With over 17 years of distinguished legal experience, supported by an LL.B. and an LL.M. from Bangalore University—where he secured Second Rank—he transformed ambition into lasting impact. A lifetime alumnus of Bangalore University and a proud member of the Karnataka Bar Association, he went on to co-found Prime Legal, a nationally reputed law firm renowned for handling complex, high-stakes legal matters with precision, integrity, and authority.

With experience spanning 30,000+ cybercrime matters, landmark financial fraud disputes, and intense courtroom battles, Adv Anik has stood at the forefront of India's fastest-evolving legal challenges. He has handled prominent cases before the ED, CBI, CCB, cyber units, and other enforcement agencies throughout India. He's also served as a Special Public Prosecutor in high-profile criminal trials. Furthermore, he's provided guidance to major corporations, fintech leaders, and tech innovators during critical legal challenges, always with a steady hand and clear vision. Yet, his most significant asset isn't his influence or reputation; it's his humanity. Through his work with the District Legal Services Authority, he helped settle over 10,000 legal aid cases, making sure justice was accessible to those who needed it. His efforts in cyber safety awareness, public welfare programs, and corporate policy development have brought him national acclaim, numerous awards, and the genuine respect of law enforcement and public institutions.

A dedicated educator and a skilled author, Adv Anik brings the law to life. His published works dissect intricate topics such as cybercrime, digital justice, Muslim property law, and legal rights, striving to make the law accessible, empowering, and pertinent to people's daily experiences. His writing is marked by a blend of depth, clarity, and a clear sense of purpose, showcasing a forward-thinking intellect and a heart dedicated to justice. Advocate Anik is now a prominent figure—a lawyer, a leader, an educator, and a catalyst for change. He is unyielding in the courtroom, compassionate in his service, and a source of inspiration. He exemplifies the belief that the law is more than just a career; it's a potent tool for safeguarding, empowering, and reshaping society

Citation: Anik (2026). Deception, Honeytraps, And Financial Exploitation in Personal Relationships: Legal Pathways for Protection and Redress. *International Insurance Law Review*, 34 (S1), 79-100.