Procedural and Substantive Challenges of Offenses Against Chastity in Emerging Domains

1. Ebrahim Aliyannejadi: PhD Student in Criminal Law and Criminology, Department of Law, Da.C., Islamic Azad University, Damghan, Iran
2. Davoud Dadashnejad*: Department of Law, Da.C., Islamic Azad University, Damghan, Iran
3. Mohammad Hassan Hassani: Assistant Professor, Department of Law, Damghan University, Damghan, Iran
4. Morteza Barati: Department of Law, Da.C., Islamic Azad University, Damghan, Iran

***Correspondence: Da.Dadashnejad@iau.ac.ir**

Abstract

Undeniably, these laws primarily address acts against chastity within the physical realm; however, the perpetration of such offenses has transcended the boundaries of the real world, extending into cyberspace and its emerging domains. Consequently, this necessitates a specific approach to legislation and the determination of corresponding penalties. Nevertheless, the initial response of the Iranian legislature to information technology crimes was the Amendment to the Press Law, enacted on April 18, 2000. Furthermore, in 2001, the Supreme Council of the Cultural Revolution adopted the "Regulations and Criteria for Computerized Information Networks." Pursuant to Article 7 of this bylaw, information and internet service providers, as well as public internet access centers (cybercafes), are prohibited from producing and disseminating offenses against chastity and public morals by service providers and users.

Keywords: Challenges, Procedural and Substantive, Offenses Against Chastity, Emerging Domains.

Received: 17 December 2025
Revised: 22 March 2026
Accepted: 29 March 2026
Initial Publication: 24 April 2026
Final Publication: 01 January 2027

Citation: Aliyannejadi, E., Dadashnejad, D., Hassani, M. H., & Barati, M. (2027). Procedural and Substantive Challenges of Offenses Against Chastity in Emerging Domains. *Legal Studies in Digital Age*, 6(1), 1-13.

1. Introduction

Every society, taking into account its prevailing values, norms, and laws, possesses a specific definition of offenses against chastity, reacting to them differently based on its customary, religious, cultural, social, and economic conditions. Prior to the expansion of modern media, offenses against chastity were committed in the physical realm, through social interactions and face-to-face behaviors. However, with the proliferation of the internet and the emergence of social media and its affiliated networks, the domains for committing offenses against chastity have assumed different and broader dimensions. Offenders of such crimes exhibit these acts publicly and openly, to the extent that even religious and traditional families are affected. The production, promotion, and dissemination of obscene materials and images, inviting individuals to commit criminal acts contrary to public chastity and morals, pimping, pornography, dissemination of prostitution and illicit acts, and instructing the commission of illicit crimes are among the offenses considered as crimes against chastity within the internet and social media environments.

The commission of acts against chastity is regarded as an assault on the material and spiritual lives of human beings. With the advent of modern communication and media technologies, the expansion of its dimensions in this domain, and its threatening consequences for families and society, the judicial systems of various countries have also confronted numerous challenges. These are challenges that individually create insecurity and a volatile, tense atmosphere within families, and will consequently disrupt the political, economic, and cultural order of governments.

2. Challenges of Criminalization and Penalization of Offenses Against Chastity in Emerging Domains

In this section, we will examine the procedural and substantive challenges of offenses against chastity in their modern forms from the perspectives of criminalization and penalization.

2.1. Procedural Challenges

In this discourse, we will examine the procedural challenges of criminalization and penalization regarding modern forms of offenses against chastity across four subsections, which include: the ineffectiveness of preventive methods based on increasing the offender's punishment, bypassing filtering, conflict of norms and beliefs, and the essential and sovereign interests of countries.

2.1.1. Ineffectiveness of Preventive Methods Based on Increasing the Offender's Punishment

It appears that the earliest crime prevention methods were based on increasing the punishments inflicted upon the offender (Mohammadnasl, 2024). In these methods, following the discovery of the crime and the apprehension of the criminal, efforts were made to control the crime rate in society by intensifying punishments and employing severe violence through deterrence and making an example out of the offender. Through these methods, by eliminating and excluding the offender from society, the possibility of recidivism by that individual was practically nullified. However, the passage of time indicates that the application of this method has failed to adequately prevent the occurrence of crime. This is because this ideology assumes that the offender is fully aware of the cost-benefit analysis of the crime, compares them prior to committing the act, and then makes a decision. Yet, this perspective ignores the role of social and environmental factors, viewing solely the individual's inclination to commit the crime as the primary cause of its occurrence. Furthermore, it must be noted that in these methods, the police investigate and ultimately act to arrest the criminal only after the offense has occurred; hence, the police adopt a reactive approach (Ebrahimi, 2024).

The necessity of adopting specific preventive approaches for crimes, especially those in emerging domains, is evident since traditional crime prevention methods have proven ineffective against them. Although definitive statistics in this regard have not been published in our country, research conducted by the US Federal Bureau of Investigation and the Computer Security Institute demonstrates that preventive methods for traditional crimes have not been effective in preventing crimes in emerging domains. Therefore, it seems that for a comprehensive and efficient confrontation with crimes occurring in cyberspace, the implementation of an inclusive criminal policy based on the participation of all members of society, particularly cyberspace users and non-governmental organizations, is imperative (Moradkhani et al., 2015).

2.1.2. Bypassing Filtering

Crimes committed in modern forms possess unique characteristics such as boundlessness, intangibility, easy and rapid accessibility, easy mutability, and anonymity, which have accelerated the rate of crime commission in this space. The tools used to commit crimes in these domains also have dual applications; in some areas, they safely and securely provide the ground for exploiting opportunities, while in other areas, they actualize threats and jeopardize the public and private interests of society. Among these technological tools are anti-filtering tools (VPNs). Despite their extensive application in transferring financially valuable, sensitive, and critical data (such as information and data exchange between banks, financial institutions, and the stock exchange), the possibility of misusing them to conceal identity for committing cybercrimes, transferring or accessing criminal content, and bypassing the country's filtering system has been facilitated for all cyberspace users. This issue, in addition to

complicating the crime prosecution process, increases the cost of crime detection for the judicial system and law enforcement officers.

Therefore, the necessity of keeping these domains safe by providing a suitable platform for legitimate activities on the one hand, and purging them of such threats on the other, requires the enactment of effective and deterrent regulations and criteria in this area. In this regard, the Legal and Judicial Commission of the Islamic Consultative Assembly (Parliament), by proposing an amendment to add a clause to Article 25 of the Computer Crimes Law, has attempted to meet the requirements for a deterrent legal response against the production, reproduction, publication, distribution, trading, or making VPNs accessible. Under this law, the reproduction, sale, and use of these services or unauthorized access are declared prohibited, and imprisonment alongside monetary fines have been stipulated for performing such actions. On the one hand, the enactment of this regulation will eliminate the legal loophole in this regard, but on the other hand, the type and severity of punishment for these operations warrant contemplation. It is worth noting that despite holding multiple sessions attended by representatives of competent organizations, this crucial matter has not yet reached a conclusion.

2.2. Substantive Challenges

In this discourse, we will examine the substantive challenges of criminalization and penalization regarding modern forms of offenses against chastity across three subsections, including: legislative conflicts, the divergence of Iranian criminal policy from novel and modern concepts, and the legislature's lack of adequate attention to victim protection.

2.2.1. Legislative Conflicts

The legislative system in any country strives to safeguard the prevailing values and norms of society, which are accepted by the majority of its people, through the enactment of laws and regulations. Consequently, diverse legal systems are formed with different approaches, each pursuing different objectives, which can ultimately lead to conflicts among the laws of various countries. Islamic countries, due to their religious and theological foundations, have traversed a different legislative path compared to liberal or secular countries, with their laws complying with Sharia rulings and mandates, often possessing a moral aspect as well. When a crime occurs internationally involving countries with a religious-centric approach alongside secular states, they are highly likely to encounter issues due to conflicting laws. Furthermore, when laws within a specific legal system have not been codified in a particular area, such as offenses against chastity in emerging forms, or when specific laws separate from international agreements govern, disagreements may arise among the involved states regarding the competent court and the applicable law (Sobhkhiz, 2015).

3. Challenges in Adjudicating Offenses Against Chastity in Emerging Domains

3.1. Procedural Challenges

3.1.1. Preliminary Investigations and Determination of Penalties for Emerging Offenses Against Chastity

Regarding the adjudication of new forms of offenses against chastity in domestic courts, challenges and obstacles are observed that complicate and hinder the process of tracking, prosecuting, and rendering judgments for such crimes. This difficulty in the adjudication process may begin from the very outset, namely the preliminary investigation phase, and continue through to the penalty determination phase. These problems and difficulties can be attributed to various reasons, including the unfamiliarity and novelty of cyberspace-related offenses against chastity, and generally such crimes in the realm of modern technologies, from the perspective of domestic judicial authorities and law enforcement officers. Although appropriate studies and measures have been undertaken in this field, due to the high speed of technological advancement and the expansion of the internet network and its capabilities, complete mastery over it cannot be envisioned. Therefore, in every era, a new criminal phenomenon emerges in cyberspace, challenging the judicial system. Furthermore, the specific and unique nature of offenses against chastity in cyberspace, along with its intangibility and lack of confinement to physical and geographical boundaries, exacerbates the situation (Tahmasebi & Shahmoradi, 2018).

Another point concerning the challenge of conducting preliminary investigations into crimes related to emerging technologies is that judicial authorities or their officers might encounter difficulties and ambiguities. First, many aspects of offenses against chastity in cyberspace may be novel to judges or judicial officers; thus, regardless of their knowledge and capability, they might still face ambiguity and difficulty in detecting the crime and conducting its preliminary investigations. Second, the arduous path of conducting initial investigations into cyber offenses against chastity and gathering traces and evidence related to the crime is also tied to the unique characteristics of cyberspace crimes. Hence, employing traditional and outdated methods of crime detection or preliminary investigation will not yield successful results in cyber and computer crimes. Additionally, some individuals who commit offenses against chastity in these domains are professionals and experts in the field of modern technologies and the internet; by destroying, altering, or relocating data related to the committed crime, they prevent the detection of the crime or their own identification.

Beyond the aforementioned points, in offenses against chastity, the victim, for various reasons such as fear of losing honor or jeopardizing their social standing, has no desire to disclose the crime committed against them, and may even destroy the evidence and traces of the crime. Consequently, judicial officers or investigating judges face tremendous difficulty in conducting preliminary investigations and sometimes discover no trace or evidence of the crime's commission (Sheybani, 2020).

3.1.2. Conflicts in Determining the Competent Court (Jurisdiction)

One of the major challenges in the realm of adjudicating modern crimes is the issue of jurisdictional conflict. The primary reason for complications in determining jurisdiction can be attributed to the inherent transnational nature of modern crimes. Jurisdictional conflicts can occur at two stages. In the first stage, the challenge lies in determining jurisdiction between two or more different territorial domains. In this scenario, all of them might decline to adjudicate the crime due to a lack of relevant laws, or, in the prevalent scenario, all or some of them might claim competence to adjudicate. Once this dispute is resolved, a jurisdictional problem might arise in the next stage between two or more judicial authorities within the country, each potentially claiming competence or lack thereof. The significance of this issue in domestic authorities is that, as a general rule, the public prosecutor's office or the court to which the case is referred must, prior to adjudicating the case, examine its own competence or lack thereof regarding the trial of the case, and if found lacking, it must issue an order of non-competence (Nourian, 2017).

Conflicts among different jurisdictions in adjudicating modern crimes are a common occurrence in both international law and the domestic laws of countries. This conflict may sometimes manifest negatively, which is, of course, not a prevalent assumption globally. Conversely, the possibility of a positive conflict arising among countries with a vested interest in a cybercrime also exists, which is the dominant scenario at the international level; this means that all or some of the jurisdictions involved in a case claim competence to adjudicate (Nourian, 2017).

Regarding active personality jurisdiction, which is based on the accused's nationality, most countries have attempted not to be overly stringent, provided the crime was not severe and did not jeopardize their fundamental interests, aiming to cooperate with the country of adjudication as much as possible. However, concerning passive personality jurisdiction (based on the victim's nationality), countries lack consensus and exhibit greater sensitivity toward it (Sobhkhiz, 2015). It is worth noting that in Iran's domestic laws, jurisdiction to adjudicate is strictly claimed only regarding certain victims, such as children and adolescents under 18 years of age in cyberspace; for other crimes, unless they are against the country's essential interests and territorial integrity, regulations similar to those for Iranian defendants have been established.

Generally, regarding conflicts among domestic judicial authorities concerning the adjudication of modern crimes, the critical challenge is the absence of specific provisions in the criminal procedure for computer crimes. Therefore, in light of Article 687, one must refer to the general provisions of the Criminal Procedure Code. Pursuant to Article 317 of the aforementioned law, the resolution of jurisdictional disputes between criminal authorities is governed by the regulations of the Civil Procedure Code; furthermore, concerning public prosecutor's offices, it complies with the dispute resolution rules of the court to which the prosecutor's office is attached. In a scenario where military personnel publish obscene or vulgar content in cyberspace, should a dispute arise between the military court and the general court regarding the military status of the person or whether the crime was committed in the line of military duty, pursuant to Article 28 of the Civil Procedure Code, the dispute resolution authority is the Supreme Court. Similarly, concerning the emergence of a local jurisdictional dispute between two judicial

districts, if they are within the same province, according to Article 27 of the aforementioned law, the Provincial Court of Appeal resolves it; if they are not within the same province, the dispute is resolved by the Supreme Court. Moreover, in the event of a jurisdictional conflict between a superior and an inferior court—for instance, if a person publishes obscene or vulgar content via an electronic publication uploaded to a website—considering the provisions of civil law and naturally Note 1 of Article 314 of the Criminal Procedure Code, the Provincial Criminal Court One is competent to adjudicate due to being the superior authority.

If there is a disagreement between the investigator and the prosecutor in the public prosecutor's office where the case is ongoing regarding the competence or non-competence to adjudicate the cybercrime, or the nature of the crime in terms of whether it is cyber-related or not, according to Article 272 of the Criminal Procedure Code, the competent authority for resolving the dispute is the Criminal Court Two to which the prosecutor's office is attached. The court's opinion in these matters is binding (Khaleghi, 2023).

It is noteworthy that due to the distinct characteristics and status of emerging offenses against chastity, more codified and considerably updated laws must be drafted regarding the issue of jurisdiction and the adjudication process for such crimes, to ensure that the adjudication of these offenses is conducted as swiftly and fairly as possible.

The challenges of determining the competent court consist of the physical location of the crime's occurrence, the time of the crime's occurrence, and the location and identity of the offender, each of which will be examined separately.

3.1.3. Physical Location of the Crime's Occurrence

The most significant challenge in determining the competent criminal court for offenses against chastity related to modern technologies is the location where the crime occurs. The location of the internet network and the cyber environment is so disconnected from geographical location that determining the physical location of an internet source or user is often impossible. Since knowledge of this physical location is irrelevant to the network's function and the goals of its creators, the ability to identify geographical location is rarely incorporated into a network's design (Rotenberg & Darbigi, 2001). In traditional crimes, the factors influencing the determination of the crime scene vary depending on the location where the crime commenced, the offender's location when the result occurred, the location of the evidence, and the location where the crime was discovered. In contrast, for offenses against chastity occurring in cyberspace—due to the virtual and digital nature of the commission site, as well as the vastness of the computer and telecommunications network—the multiplicity of different location-related factors manifests as a challenge. For example, an individual distributing obscene images across the internet simultaneously engages multiple countries and, effectively, millions of websites within a very brief moment. Although employing advanced techniques, methods, and redoubled efforts might physically pinpoint the location where operations commenced or content was uploaded, this identification requires, firstly, international and group collaboration on the one hand, and cooperation from information service providers on the other. Secondly, identifying this location alone is insufficient for exercising jurisdiction.

Although internet systems have addresses, these addresses define their position within the network, not their physical, real-world location. Naturally, some internet addresses contain geographic identifiers or markers that can be geographically determined. For instance, the domain extension (.au) belongs to Australia. Most internet addresses lack geographic indicators, and more importantly, all internet addresses are easily transferable, as they are not like physical addresses in the real world, but rather conventional addresses within a network. For example, a user in one geographic domain might work with a source in Tokyo today but transfer their operations along with their internet address to another service provider source in Washington tomorrow; thus, there is no coordination or alignment between cyber space and physical location (Tahmasebi & Shahmoradi, 2018).

As observed, crimes in the cyber environment, unlike crimes in the physical realm that occur in a specific and confined location such as a room, a building, or a region, may be committed in various parts of the world. They also differ in that, regarding cyber environment crimes, it is impossible to definitively select a single location as the scene of the crime, not only technically but also from the perspective of criminal law (Heidari & Milani, 2022).

Often, the location of the crime's occurrence forms the basis for determining jurisdiction and applying relevant regulations. The Convention on Cybercrime, in Section 3 (Jurisdiction), Article 22, Paragraph 1, also addresses this issue, stating: "Each

Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with … this Convention, when the offence is committed:

a. in its territory;

b. on board a ship flying the flag of that Party;

c. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence falls outside territorial jurisdiction."

Upon careful consideration of this paragraph, it appears that these clauses merely reaffirm traditional jurisdictional rules, namely territorial, active personality, and universal jurisdiction. In doing so, the drafters of the Convention treated the challenge of determining the crime scene as resolved, establishing these rules on the assumption that the location is determinable. However, such rules lack substantial practical application without establishing a suitable mechanism for pinpointing the location of the crime's commission (Foroughi & Albouali, 2012).

Therefore, for all information and content in cyberspace, one can identify a source—meaning the uploader places their intended content onto a component of this domain's infrastructure so that the downloader, the intended destination of that content, can access it. Regarding the uploading of offenses against chastity, it is argued that if the upload entails content involving illegal and illicit acts, such uploading is illegal and criminal, and naturally, its location is the scene of the crime. Downloading has also been considered the scene of the crime under the premise that until individuals download the unchaste information, no crime has practically occurred. It is true that the principal act originated from the initial offender (the uploader), but until internet users download it, the crime is not completed or fully realized (Heidari & Milani, 2022).

3.1.4. Time of the Crime's Occurrence

This challenge is also a critical issue that consistently demands attention, particularly in countries where a statute of limitations exists, or even if such an institution does not exist in the law, the time of the crime's occurrence remains a significant matter regarding the applicable governing law. This does not refer to cybercrimes that happen at a specific point in time, but rather another type of crime that occurs over a designated period. For example, a computer programmer working at a bank could adjust the program written for the bank's computers so that everything proceeds smoothly and without error for a specified duration, but after a designated period (months or years), the operational method suddenly changes, and the computer deducts a negligible amount from all bank accounts, transferring it to the programmer's account. The programmer then withdraws this massive sum and absconds, or retrieves it from another location. How can one opine on the time of occurrence for such a crime? Is the time of the crime when the program was written with malicious intent? Or when the offender's act is fully realized? Can this issue be resolved by theories such as the materialization of the actus reus? For instance, should the programmer be tried at the time the program was inputted (assuming the impossible scenario that the crime is discovered at this point) on the charge of possessing malicious intent? Meaning, we argue that malicious intent existed, the material act was already performed (writing the program), and the causal link is present, thus the criminal must be tried and convicted (even before the result is realized)? In other words, prosecuting the criminal before the crime is completed? Or should we say that such an action (trying a person before the crime is committed) contravenes justice, and logically, only prosecute the individual when the crime is fully realized? Meaning, when they have absconded with the money? Prosecuting such an individual under the title of "attempted crime" also seemingly lacks efficacy and fairness due to the disparity between the charge/punishment and the potential benefit the criminal would reap upon success; meaning the penal effects of reforming and disciplining the offender would not manifest. The problem of determining the time of crime commission is considered a challenge for designating the competent judicial authority because jurisdictional laws might undergo changes during the commission process of such crimes, thereby creating the problem of determining the applicable law subordinate to the problem of determining the time the crime was generated (Shahrabadi, 2019).

3.1.5. Location and Identity of the Offender

Another existing challenge in determining the competent court is the challenge of identifying the offender's location during or after the commission of the crime. Because cyberspace is an intangible environment and, on the other hand, a vast and

transnational one—and also considering the professionalism and expertise of perpetrators of offenses against chastity in modern technologies—offenders often hunt their prey easily and attempt to remain anonymous using specific identity-altering tricks and methods. Since the principles for determining the competent court include jurisdiction based on the offender's nationality or the jurisdiction of the court where the offender is located, establishing the competent court based on either of these principles requires identifying who the perpetrator is, which state's nationality they hold, or where in the world the offender is situated. However, as previously mentioned, no system for identity verification is conceivable in cyberspace, and individuals can easily enter telecommunications or internet networks with fake identities and conceal their true ones. Because in cyberspace, users are identified by conventional identifiers such as IP addresses—which are entirely cybernetic, unobservable, and intangible—even if the user committing the crime is identified, we have in reality identified their cyber and conventional entity, not their actual identity in the way it is processed by national police forensic identification departments (Shahrabadi, 2019).

For example, in this context, regarding the observance of children's rights in cyberspace and the prohibition of pornography and the dissemination of obscene images involving children, these actions are criminalized in countries like the United States, Canada, and the Netherlands under relevant conventions. But the question is, who are the victims of such crimes? Given the argument that obscene images must be attributable to real children, are the real children whose images were abused the victims, or, since all children are potential victims of this crime, are they all considered victims? Can Country A, where child pornography is a crime, claim jurisdiction over pornography committed in and by Country B? The answer to this question depends on proving whether the aforementioned pornography actually incites sexual deviations in perverts.

If Country A can prove that the said images created in Country B were among the causes of crimes committed against its citizens, it can claim jurisdiction over individuals residing in Country B who were responsible for publishing these obscene images. In other words, can proving a causal link between the production or dissemination of obscene images of children ("child pornography") and crimes committed against children in Country A establish the jurisdiction of that country's courts? (Alipour, 2021). This applies if the offender in Country B does not hold the nationality of Country A, or if for certain reasons, their extradition cannot be requested. This matter is considered in cybercrime conventions and serves as the foundation for universal jurisdiction in Germany. Furthermore, countries can claim jurisdiction over foreign individuals who have committed the aforementioned crime outside the borders and territorial jurisdiction of a country but reside and are domiciled in that country, even if they requested domicile or residency post-crime. This is the case in the Netherlands, where a defendant or suspect can be prosecuted even if residency was obtained after the crime was committed.

In Iran, within the Computer Crimes Law enacted in 2009, in Section Two—concerning criminal procedure regarding the jurisdiction of Iranian courts over computer or cybercrimes—Paragraph C acknowledges protective (objective territorial) jurisdiction and specifies its instances in Article 28.

3.2. Substantive Challenges

3.2.1. The Discovery Phase of Offenses Against Chastity in Emerging Forms

One of the challenges regarding offenses against chastity in the cyber domain is the difficulty of detecting these crimes. In this type of crime, due to it occurring in a virtual and non-real space, no tangible or material trace of the crime or the offender's footprint is left behind as is seen in traditional crimes. In most cases, the sparse remaining traces of the crime capable of tracking the criminal can easily be erased and purged. For this reason, it can be confidently stated that the dark figure of crime for offenses against chastity related to these domains is extremely high compared to traditional crimes. On the other hand, if an individual or organization accidentally encounters digital evidence on their system during the normal course of their professional activities, and if they proceed to collect and acquire this evidence themselves, they will face the problem that the said evidence was obtained illegally. Consequently, it will lack admissibility. Therefore, it must be disclosed to law enforcement so they can proceed to acquire the evidence. Thus, the existence of a high-speed, low-cost reporting process, similar to the telephone numbers designated for emergency services like police and ambulances, seems essential.

Measures regarding the collection and preservation of electronic evidence at the virtual scene of an offense against chastity—meaning the location where the criminal executed their illegal actions to commit the crime—are divided into two categories. First, pre-entry measures, including defining the type of target data and evidence, and obtaining the necessary warrants to

commence search and seizure. Second, post-entry measures, including deploying technical protocols, using necessary tools, and drafting relevant incident reports, all of which are conducted to preserve the evidence until presented to the judicial authority. Each phase has its own specific features and characteristics. Of course, the authority to expand the scope of the investigation is also possible in specific cases with a judicial order and execution by judicial officers.

Law enforcement agencies prioritize their duties on investigating violent crimes, placing the investigation of virtual offenses against chastity at a lower tier, whereas the damages resulting from such crimes can equal the budget of a small country. Furthermore, the dichotomy law enforcement creates between violent crimes and cyber-related offenses against chastity leads to a lack of serious pursuit of the relevant evidence. However, the reality is that computers, mobile phones, and similar technologies can also contain evidence relating to violent crimes such as kidnapping, torture, abuse, and rape. Hence, the necessity of training law enforcement officers and criminal justice experts regarding networks as sources of electronic evidence is a matter that must be addressed. Ultimately, evidence and its admissibility are among the most crucial links in the administration of judicial justice, the prerequisite for which is the proper preservation and maintenance of evidence. Given its highly specialized nature, this issue is of doubled importance concerning electronic evidence. For this reason, training judicial officers and competent judicial authorities in this field is an imperative matter (Zandi, 2015).

The adjudication of offenses against chastity in cyber domains inherently entails specific complexities due to taking place in a virtual environment and the nature of the evidence. Due to reasons such as specific complexities, the elimination of physical territory and a country's sovereign political boundaries, the concealment of the criminal's identity, the mutability of the nature of evidentiary proofs, and the highly specialized and technical nature of preliminary investigations in the cyber environment, the prosecution and adjudication of cybercrimes are fraught with difficulties. Cyber offenders continually seek to commit virtual offenses against chastity because they can operate in a secure environment with minimal costs—for example, from their home or office—inflicting harm upon the material and spiritual interests of others, damaging their reputation and honor, and reaping benefits from these actions. The jurisdiction of judicial authorities in the cyber environment based on jurisdictional rules in traditional crime adjudication is not highly effective. For instance, if cyberspace leads to a displacement of the crime scene, the first issue raised is the competent criminal authority; if this extends beyond borders, instead of domestic court disputes, one must anticipate the exercise of jurisdiction by numerous countries. Also, due to the virtual environment and the nature of electronic evidence within it, evidence is constantly at risk of destruction, deletion, or encryption, which severely limits the detection and collection of crime evidence. Therefore, for a more efficient and effective confrontation against the commission of offenses against chastity in this environment, we must first recognize the existing challenges in the realm of adjudicating offenses against chastity in modern virtual and cyber forms, and establish laws concerning criminal procedure in cyberspace capable of fulfilling the aforementioned objectives (Tahmasebi & Shahmoradi, 2018).

3.2.2. Proof of the Crime

The judicial system and law enforcement may also face arduous tasks in proving offenses against chastity in cyberspace. Proving offenses against chastity in these domains has always been one of the fundamental challenges for judges, the reasons for which can be evaluated in the following aspects:

1. Criminals committing offenses against chastity in cyberspace, due to their expertise in executing cybercrimes, can easily employ various methods—such as destroying crime evidence or altering and moving it—to leave no trace of themselves or at least prevent their identification. Furthermore, they can severely obstruct the activities of prosecuting and tracking committed crimes by employing security measures like using passwords, providing blocking instructions, and coding methods, or by transferring encrypted evidence to another part of the internet, such as dark webs, thereby practically disrupting access to crime evidence and subsequently the proof of the crime (Zivari, 2012).
2. Due to the reduced costs of using modern technology and tech tools, offenses against chastity in this sector have also increased, and individuals lacking necessary awareness of its nature might become victims in this space. Moreover, the ease and affordability of using digital documents have led to their proliferation; while this holds many advantages, during the commission of offenses against chastity, collecting and relying upon them by judicial officers and judicial authorities will be difficult. Also, due to the ease of altering and destroying such documents, the admissibility or proof of cyberspace crimes will be challenged (Bagheri, 2014). Therefore, other difficulties in proving offenses against

chastity in this domain stem from the reality that criminals can easily eliminate the evidence of the crime by deleting and purging data (Bastani, 2011).

3. Another factor is the rapid advancement of technology and modern tools, resulting in cyberspace-related offenses against chastity constantly mutating, rendering them no longer identifiable using traditional tools and regulations. Consequently, when a country fails to empower and streamline its most potent weapon against crime—namely, the law—and merely relies on archaic and outdated legislation, one cannot expect favorable results in confronting such crimes. Therefore, the country's legislature is duty-bound to exert redoubled effort and precision in criminalizing modern offenses against chastity and drafting laws and punishments commensurate with them, compared to traditional offenses against chastity.
4. Offenses against chastity in the realm of cyberspace fall into the dark figure of crime. The reasons for this are multifold. First, some victims in this space, out of fear for their honor and the loss of their personal reputation or social standing, will never disclose these crimes and may even destroy the evidence and proofs of the crime in the process. Consequently, such crimes will generally not be proven. Second, the offenders in this realm, as mentioned, easily destroy the traces and evidence of the crime, leaving nothing behind for proof. Third, women who are victims of offenses against chastity often do not report the commission of these crimes against themselves—and many even deny it—to avoid stigmatization or becoming conspicuous in their family or society. Clearly, many offenses against chastity in the technology domain might be buried within the core of this space and never be revealed or proven (Tahmasebi & Shahmoradi, 2018). It should be noted that the existence of dark figures causes confusion or miscalculation within the criminal justice system and its relevant authorities, and inaccurate statistics on offenses against chastity will hinder the deployment of appropriate and necessary measures and resources for prevention or the resocialization of offenders.
5. Prosecuting offenses against chastity in the technology domain requires extensive auditing of computer data. Most of this data is not stored in a visible format readable by humans, but rather in invisible formats readable only by machines, stored highly densely within electronic storage devices. Therefore, one of the problems faced by prosecution authorities and courts in detecting, pursuing, and ultimately proving cyber offenses against chastity is the lack of visible and comprehensible evidence. This challenge is a particularly serious issue regarding the manipulation of computer programs because full auditing of a computer program and discovering invisible and hidden programmatic routines requires spending considerable time and money, which is often economically unjustifiable (Tahmasebi & Shahmoradi, 2018).

3.2.3. Determination of Penalties in Judicial Precedent

The sentencing phase is one of the critical stages in confronting criminal phenomena. The importance of this issue is doubled regarding the method of determining penalties for offenses against chastity in cyberspace and the internet, and judges must exercise greater scrutiny. The significance of the sentencing discussion for offenses against chastity in these domains relates to their characteristics, as well as their impacts and consequences. The specific features of these crimes cause a different judicial precedent to form around them, shifting the judges' perspective from that of traditional crimes. But more important than the characteristics of cyberspace offenses against chastity are their destructive results and consequences, which, in terms of quantity and spread compared to physical world offenses against chastity, are vastly greater and can entangle a broad spectrum of society. Therefore, in determining punishments for offenses against chastity in emerging domains, judges must carefully consider factors such as the offender's personal characteristics and their aptitude for committing cybercrimes, whether the committed crime was specialized or not, the nature of the crime, the resulting consequences, and the extent of damages inflicted upon the victim and society as secondary victims. In proportion to these, they should proceed to determine the penalty and utilize mitigating institutions and leniency measures (Tohidi Nafe & Amirli, 2018). It is worth mentioning that judges must exercise redoubled precision in adjudicating modern offenses against chastity, in selecting laws, and also in choosing judicial precedent or judicial criminal policy, striving to align it with legislative criminal policy, because the closer these two are, the more satisfactory the achieved results will be.

The following verdicts illustrate the approach of judges towards offenses against chastity committed in connection with modern technologies:

The following verdict is noteworthy regarding the judge's stringent approach toward publishing images related to modeling:

"… Disregarding the inherent obscenity of the committed act of 'modeling with a semi-nude body' and its religious prohibition, [the court] considers the publication of these images in cyberspace as an instance of the subject matter of Article 14 of the Computer Crimes Law (Article 742 of the Islamic Penal Code, appended in 2009). Secondly, considering the defendant's definitive conviction to a 6th-degree Ta'zir (discretionary) imprisonment under judgments No. 2100059 dated April 13, 2015, imposing a fine of twenty million Rials for publishing personal images issued by the Hamedan Court, and No. 1200200 dated May 13, 2015, for producing and publishing vulgar works issued by the Shahriar Court, and his recidivism in committing a 6th-degree Ta'zir crime, his action constitutes an instance under Article 137 of the Islamic Penal Code enacted in 2013. While being deprived of alternative punishments to imprisonment subject to Article 66 of the Islamic Penal Code enacted in 2013 due to a definitive prior conviction of a monetary fine exceeding ten million Rials, he falls under the statutory aggravation of punishment stipulated in Article 137 up to a maximum of one and a half times; therefore, invoking Note 1 of Article 14 of the aforementioned law and Article 137 of the said law, the individual is sentenced to endure four months of Ta'zir imprisonment." (Tohidi Nafe & Amirli, 2018)

In another verdict, the judge's approach is such that, taking into account individuals' honor, a telephone number is also treated as a personal secret, and its disclosure in cyberspace is deemed punishable. In this verdict, regarding the defendant accused of publishing obscene photos to encourage the female plaintiff to commit unchaste acts and publishing her phone number based on his confession, "[the court] invoking Articles 134, 171, 211, 742, 743, and 745 of the Islamic Penal Code (Article 14, Paragraph B of Article 15, and Article 17 of the Computer Crimes Law) sentences the individual for: 1- Publishing obscene photos in cyberspace to endure two years of Ta'zir imprisonment; 2- Encouraging and inciting the plaintiff to commit unchaste acts in cyberspace to endure one year of Ta'zir imprisonment; 3- Disclosing the plaintiff's private secrets (phone number) and placing them on obscene cyberspace pages, and disseminating falsehoods via computer leading to the extensive discrediting of the plaintiff to endure two years of Ta'zir imprisonment, with the executability of the most severe punishment."

Here, the court's focus on the behaviors conducted in cyberspace and the prevalent perception that this space is prone to actions against individuals' honor led the court—while treating the phone number as a private secret and referencing the dissemination of falsehoods—to ultimately convict him under Article 745 of the Islamic Penal Code appended in 2009 for the disclosure of a secret leading to discrediting. This is despite the fact that sharing someone else's phone number is not categorized as a private secret, and depending on how it is shared, could be an instance of a non-computer crime like Qadhf (false accusation) or insult, or even computer-based dissemination of falsehoods (Tohidi Nafe & Amirli, 2018).

Considering that adolescents' inclination towards information exchange environments has a direct correlation with their capabilities—which, if uncontrolled, easily assumes a deviant and criminal nature, a factor considered by courts in determining sanctions—the following sample verdict is examined, which stipulates:

"Regarding the accusation against Mr. …, a seventeen-year-old, concerning telephone harassment of Ms. … and disseminating falsehoods via computer systems and posting the plaintiff's phone number on Facebook labeling her as a prostitute … the court, noting that the defendant was an adolescent (a mature minor under 18) at the time of the occurrence, and with the ultimate goal of rehabilitating and properly socially reintegrating the delinquent child in question, and invoking Articles 1, 3, 6, 20, 36, and 40 of the Convention on the Rights of the Child adopted November 20, 1989, and Articles 10, 19, and 89 (Paragraphs T and Th) and 134 of the Islamic Penal Code of 2013, and Article 18 of the Computer Crimes Law enacted in 2009, and Article 641 of the Islamic Penal Code (Ta'zirat section) of 1996, sentences the defendant to a fine of one million Rials for the first offense, and ten million Rials for the second offense."

Offenses against chastity, particularly a spectrum of them whose commission is difficult in the external environment, such as pornography, materialize against a backdrop of various factors. In pornography, where a direct victim is not raised, the users' appetite for obscene content and the lack of genuine external manifestation of violating public chastity and morals (which holds a real and external interpretation), causes the judge's approach to such crimes not to rest solely on unilaterally blaming the offender. Although Chapter Four of Section One of the Computer Crimes Law utilizes the phrase "crimes against public chastity and morals," it is clear that cyberspace can never reflect the role of the external environment and consequently the emergence and manifestation of chastity and morals, which hold an external and apparent status. Hence, it seems that magistrates rarely

equate the violation of moral norms in cyberspace with external requirements, and thus rarely seek severe punishments for the offender in this regard or even equate it with severe Hadd crimes like Efsad-e-fil-Arz (Corruption on Earth).

A verdict issued by the Revolutionary Court regarding the management of several Persian pornographic websites, stipulating the corruption of society and the deviance of youth, ultimately results in the determination of imprisonment and a fine, rather than a ruling of Efsad-e-fil-Arz. According to this verdict: "Regarding the accusation against Mr. … of direct commission in managing Persian pornographic websites, and considering his effective activity and management of the anti-moral and anti-religious websites 'Shahvatsara' and 'X-Persia' as the general manager of the site and overseeing all subordinate managers and members, and coordinating among pornographic websites and supervising them, and his effective and significant activity towards corrupting the Islamic society and deviating the youth, invoking Article 14 of the Computer Crimes Law, [the court] sentences him to endure two years of imprisonment, inclusive of days in detention, and the payment of forty million Rials as a fine." Aside from the fact that this verdict addresses the charge of managing pornographic websites rather than Efsad-e-fil-Arz, and was adjudicated based on the Computer Crimes Law rather than the Act on Penalizing Persons Engaging in Unauthorized Audio-Visual Activities enacted in 2007 to justify the court's jurisdiction, it is clear that the Revolutionary Court's stringent approach in confronting pornography based on cyberspace requirements—specifically the users' inclination and appetite to support sexual websites and the absence of individuals unwilling to visit these sites—ultimately makes the application of Efsad-e-fil-Arz to widespread pornography far from reality.

4. Conclusion

One of the challenges of this domain is crimes against public chastity and morals, or generally offenses against chastity, which have become capable of being committed virtually with the ubiquity of the internet. In this category of crimes, any individual from the comfort of their home anywhere in the world can easily upload videos, images, or content contrary to public chastity and morals onto modern communication networks, constantly threatening family and society through the dissemination of obscene photos and videos or pornography. The consequences of offenses against chastity related to modern technologies are such that today even children are exposed to their ensuing dangers and harms, forecasting an ambiguous future for them regarding culture and values. Among the most significant damages of the expansion of offenses against chastity in this domain, which impact the future of children, adolescents, and youth, is the destruction of moral foundations and principles and the social order, which ultimately leads to the devastation of the country's economic, political, and cultural systems. The expansion of this domain's technologies and the proliferation of immoral norm-breaking will impose damaging and irreparable consequences on families and subsequently on the foundations of society.

Identifying and preventing the distribution of crimes against public chastity and morals in these domains is difficult because there is no unified consensus on how to handle this issue. While some argue that a global internet regulation and control system is necessary, others contend that strategies such as the development of filtering technologies are more appropriate. Pursuing and adjudicating offenses against chastity on the internet has frequently created a serious challenge for the judiciary, the executive, the legislature, and law enforcement agencies due to the unique nature of this medium. The easy availability of immoral and obscene materials in digital formats, even to children, including video clips, their rapid transmission across the network, and the lack of effective filters to prevent access to indecent materials are factors exacerbating the challenge.

To preserve public chastity and morals, the legislature has criminalized three categories of behaviors in Chapter Four of the Computer Crimes Law, enacted on May 26, 2009, under the title of Crimes Against Public Chastity and Morals. Behaviors related to obscene content (Article 14 of the Computer Crimes Law) and aiding in access to obscene content (Paragraph A of Article 15 of the Computer Crimes Law)—these two behaviors actually form the foundation of the crime of pornography, for which the legislature has preferred the traditional titles of crimes against public chastity and morals and obscene content over it. Thirdly, assisting individuals in committing certain crimes against persons or instructing individuals in committing crimes (Paragraph B of Article 15 of the Computer Crimes Law). Paragraph B of the aforementioned article extends beyond the scope of pornography and constitutes a broad criminalization. Pursuant to this article, inciting, encouraging, threatening, inviting, or deceiving individuals into committing offenses against chastity, the use of narcotics or psychotropic substances, suicide, sexual deviations, or violent acts, or facilitating or instructing the commission of such acts, is deemed a crime.

Some of the major challenges arising from offenses against chastity in cyberspace examined in this research include:

Internet Infrastructure: The infrastructure of the internet makes controlling offenses against chastity extremely difficult. The internet is a decentralized system with no single controlling agency or central storage facility. Because a network of networks supports this domain, even if one route is blocked, many alternative routes can be chosen to reach the same destination. Similarly, if one website or newsgroup is shut down, there are many others that can instantly take its place. The decentralized nature of the internet and its subsequent difficulties in restricting the distribution of offenses against chastity are exemplified by peer-to-peer networks, which involve direct connections between computers without the need for a central server. Therefore, it is argued that the existence of the internet in a free sense is fundamentally uncontrollable. (Core Hypothesis)

Jurisdictional Uncertainty: The internet is an international communication tool that crosses jurisdictional borders. Not only is cooperation between law enforcement agencies essential for tracking criminals across jurisdictions, but resources must also be coordinated to avoid duplicated efforts. Parallel operations conducted from various jurisdictions might unknowingly target the same organization or criminal. It is equally challenging to determine who is responsible for investigating offenses against chastity in these domains; when there are no clues as to where these crimes originated, there is a possibility that offenses against chastity remain uninvestigated because they do not fall within the specific jurisdiction of law enforcement.

Lack of Regulations: Many responsible bodies are reluctant to introduce laws that might help control internet usage. Debates persist regarding the appropriate balance between protecting society on one hand, and freedom of expression and commercial interests on the other. There is also legal ambiguity regarding whether Internet Service Providers (ISPs) should be held liable for the content they provide or should merely be considered as conduits for that material (similar to postal services). The ultimate outcome is that the legal obligations of ISPs concerning offenses against chastity in emerging domains are often unclear, and in most cases, the emphasis has been on self-regulation.

5. Recommendations

- It is suggested that the legislature, in order to protect the victims of offenses against chastity in emerging domains, study and enact laws ensuring that offenders in this domain incur Ta'zir punishments.
- The legislature should ideally enact an appropriate legal provision rendering the use of network facilities and services for unchaste materials aimed at harassing, abusing, threatening, or bothering others illegal, and also specify appropriate punishments for committing the crime.
- It is recommended that Internet Service Providers (ISPs) and telecommunications companies provide filtering services for unchaste content utilizing a cost-recovery model. Users must be granted the right to choose whether to opt into the services.
- The government and the private sector should ideally collaborate to create awareness programs regarding unchaste content and ways to mitigate the problem.
- It is proposed that a center for handling complaints regarding unchaste materials be established and promoted to users. This center will serve as an advisory service hub for users. It can also take appropriate actions against violators.
- It is recommended that virtual business owners, as a condition of their business operating license, provide content filtering services on their channels. These services will help prevent the viewing of inappropriate content by the younger generation, particularly students. Local authorities and officials should make compliance with these conditions mandatory for these entrepreneurs.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Alipour, H. (2021). *Criminal Law of Information Technology*. Khorsandi Publications.
Bagheri, A. (2014). *Iran's Judicial Criminal Policy Toward Computer Crimes* Tarbiat Modares University]. Tehran.
Bastani, B. (2011). *Computer and Internet Crimes: A New Manifestation of Delinquency*. Behnami Publications.
Ebrahimi, S. (2024). *Criminology of Prevention, Vol. 1*. Mizan Publications.
Foroughi, F., & Albouali, A. (2012). Criminal Jurisdiction of Judicial Authorities in Cyberspace. *15*(58).
Heidari, H., & Milani, A. (2022). Comparative Study of Territorial Jurisdiction in Handling Cyber Crimes with Emphasis on the Iranian Criminal System. *Journal of Law and Modern Studies*, *3*(4).
Khaleghi, A. (2023). *Notes on the Criminal Procedure Code*. Shahr-e Danesh Publications.
Mohammadnasl, G. (2024). *Fundamentals of Crime Prevention*. Mizan Publications.
Moradkhani, A., Razavi Asl, M., Ahmadi, M., & Abedian Kalkhoran, H. (2015). Methods of Preventing Internet Theft. *Journal of Jurisprudential and Philosophical Studies*, *6*(23).
Nourian, A. (2017). *Criminal Procedure of Computer and Telecommunication Crimes*. Mizan Publications.
Rotenberg, M., & Darbigi, B. (2001). *Privacy in the Information Society: Legal, Ethical, and Social Challenges of Cyberspace*. Khaneh Ketab Publishing.
Shahrabadi, M. H. (2019). *Re-identification of Illicit Relations in Cyberspace with a Legal Approach* Payame Noor University]. Mashhad.
Sheybani, M. (2020). *Iran's Criminal Policy Toward Crimes Based on the Spread of Corruption and Prostitution in Cyberspace* Judicial Sciences and Administrative Services University]. Tehran.
Sobhkhiz, R. (2015). Legal Challenges of Cyber Crimes in International Legal System and Iranian Legal System. *Quarterly of Intelligence and Criminal Research*(3).
Tahmasebi, J., & Shahmoradi, K. (2018). Challenges and Gaps in the Process of Dealing with Cyber Crimes. *Justice Legal Journal*, *82*(104).
Tohidi Nafe, J., & Amirli, H. (2018). Requirements of Sentencing Policy in Confronting Cyber Crimes with Emphasis on Judicial Practice. *Justice Legal Journal*, *82*(101).
Zandi, M. (2015). *Preliminary Investigations in Cyber Crimes*. Jangal Publications.
Zivari, K. (2012). *Iran's Criminal Policy in Preventing Computer Crimes* Payame Noor University]. Tehran.