

Cyber-Extortion between Security Enforcement and Public Consciousness: Towards a Dual Track of Repression and Prevention

Received date:14/07/2025 Accepted date:21/09/2025 Published date:28/10/2025

Samira Bechka ¹

¹ *University of Biskra , Algeria, Email: samira.bechka@univ-biskra.dz*

Abstract:

This paper examines the hazards of cyber-extortion and the twin fronts—suppression and prevention—through which it must be tackled. Treated here simultaneously as a social phenomenon and as a criminal act punishable under positive law, cyber-extortion prospers in posting and sharing space of today's Internet platforms. That permissive environment has normalized unethical conduct among certain users and made it easy for individuals to fall prey to a spectrum of online offences, foremost among them extortion. The practice, now widespread, has fractured family structures and begun to threaten both institutional stability and social order. Typical scenarios involve the creation of coercive digital material followed by threats of public release through a social-media account, through hacking of electronic profiles, or by exploiting images originally sent by third parties.

Keywords: crime; cyber-extortion; public awareness; security mechanisms.

Corresponding Author: Bechka Samira, Email: samira.bechka@univ-biskra.dz

1. INTRODUCTION

The technological surge that has swept contemporary societies has spawned an “information-technology order” whose impact on communications is both transformative and profound. Digital networks, together with a globalized economic framework, generated a rapid expansion in the range and frequency of electronic tools; in turn, these tools re-shaped social structure. The Internet emerged as a principal arena of everyday life, dissolving geographical boundaries and altering how ideas circulate. Interpersonal relations now operate in an open, boundary-light environment largely detached from traditional value systems and the informal mechanisms of social control. Within that space, a darker undercurrent—*digital anomie*—has taken root. Unethical practices once difficult to imagine have multiplied, fueled by widespread adoption of smart devices and the ever-growing constellation of social-media platforms (Facebook, Instagram, X, YouTube, TikTok, and others).

Ziouch (2017) observes that Algeria’s technological leap outpaced society’s capacity for adaptation, creating conditions in which cyber-crime thrives beyond the reach of conventional policing (Ziouche, 2017). The consequences penetrate family life and external social circles alike: individuals become exploitable, confronted by actors who manipulate digital space with ease. Offenders deploy sophisticated means—image-editing programs such as Photoshop, advanced voice-modulation software, remote-monitoring applications, and spyware able to penetrate mobile phones and harvest sensitive videos and photographs. When combined with the vast repositories available online, these tools

yield intimate data ripe for coercion. Ben Omar Yassin (2024), focusing on child victims, notes that cyber-extortion now constitutes a direct assault on private life, exploiting vulnerabilities in smart phones and in software that manipulates images, audio, and remote surveillance (Ben Omar, 2024). The offence belongs to what criminologists label “soft crimes”: it lacks overt physical violence yet still qualifies as a globally recognized category of electronic felony. By disturbing power relations, the crime undermines social security; the offender wields symbolic violence, threatening disclosure of private information and forcing the victim to satisfy demands—lawful or otherwise—to avoid scandal and social stigmatization.

Among the many manifestations of cyber-crime, cyber-extortion remains one of the most injurious. The prospect of exposing personal secrets is particularly disruptive in light of soaring user numbers and the proliferation of messaging applications. National cyber-crime units registered 3 325 cases in the first ten months of 2023, with 2 315 victims, while specialized gendarmerie teams handled more than 4 500 additional files. Data analysis reveals that 65 % of incidents originated on Facebook; state officials and senior functionaries were frequently blackmailed through doctored images (Bachouche, 2024). Similar proportions appear in Sebkhawi’s university survey, where 65 % of recorded incidents involved emotional blackmail on Facebook (Sebkhaoui, 2024).

Given this palpable threat to personal privacy and digital security, a deeper inquiry into cyber-extortion—its legal configuration and social context—is essential. Three guiding questions arise:



1. What legal-conceptual attributes distinguish cyber-extortion from its traditional counterpart?
2. Do the protective provisions contained in Algeria's Criminal Code suffice to shield individuals from this offence?
3. To what extent can heightened public awareness serve as a preventive barrier against the phenomenon?

2. Conceptual Framework

2.1 Cyber-crime

Cyber-crime has been described as “any unlawful activity involving the copying, alteration, deletion, or unauthorized access to data stored in, or transmitted through, a computer.” A parallel formulation labels it as “information fraud encompassing every illicit act connected with the processing or transfer of data.” (Centre for Security Research and Studies, 2016)

The shared core is objective: a mere reference to computers does not suffice. For conduct to qualify as cyber-crime, it must occur within an information system.

2.2 Cyber-extortion

Extortion in general: Al-Shahri defines classical extortion as “one person or a group threatening another with publication or circulation of information, news, or images the latter wishes to keep private, in order to shame, erode morale, and secure gains, concessions,

or positions that benefit the blackmailer.” (Alshahri, 2011)

The offence therefore strikes the victim’s emotional sphere, forcing compliance to protect reputation, trust, or social standing.

Cyber-extortion: Al-Anzi frames the electronic variant as “obtaining documents, photographs, or data concerning the victim—by electronic means—or threatening to publicize private material through digital tools, with the aim of achieving the blackmailer’s objectives.” (Al-Anazi, 2017)

Technology becomes the instrument of domination: privacy is violated to secure material or intangible advantage, while the offender counts on the victim’s limited capacity to resist.

Ziouche extends the idea and defines the concept as: “any act whereby an individual, using high-precision IT techniques, the Internet, and software that erases traces after the deed, carries out extortion to reach a particular end; those ends differ according to the actor and to the circumstances.” (Ziouche, 2017)

Boumami emphasizes the same coercive essence: “taking something from another without consent, the cyber-offender channeling technical ingenuity—whether for personal revenge or for hire—through modern communication tools such as computers, programs, and networks.” (Boumami, 2015)

Across these formulations, cyber-extortion remains a coercive threat aimed at the victim’s will, intended to obtain a material or moral benefit. Threat is indispensable; without it, extortion does not arise. The

act is unlawful, offends societal norms, and sits firmly within the category of information offences. Fertile ground for such behavior is found on platforms like Facebook and through electronic devices—smartphones, laptops, and similar gateways—that facilitate extortion.

2.3 Public Awareness

Al-Ruwais defines public—or community—awareness as a *mental orientation* that enables an individual to perceive self and surroundings along a spectrum of clarity and complexity. The construct embraces several layers: awareness of one’s bodily and cognitive functions; insight into the purposes that animate the external world; recognition of the self as a social actor situated within a given community; appreciation of membership in specific groups; and, finally, an understanding of how social phenomena, situations, values, and norms interact to shape personal responses (Alruwais).

Within the parameters of this study, public awareness denotes the individual’s capacity to identify and comprehend potential risks—those threatening either personal life or the welfare of close associates—and to adopt preventive strategies, whether autonomous or externally supported, aimed at avoiding entanglement in cyber-crime generally and cyber-extortion in particular. Such awareness arises from the interactive relationships the user forges in digital space through Internet-based communication channels.

2.4 Security Mechanisms

For this paper's purposes, security mechanisms refer to the suite of proactive, preventive procedures and techniques deployed by specialized institutions and security services charged with combatting cyber-crime. Their collective objective is to shield both individuals and the wider community from the diverse forms of online threat and blackmail that may materialize within the digital environment.

3. Structural Conditions Fostering the Emergence of Cyber-Extortion

Cyber-extortion ranks among the most pernicious forms of information-technology crime, given its capacity to erode public security and destabilize social order. The attendant harm touches both the individual and the collective sphere. Underlying factors vary—religious, psychological, political, economic, or social—and differ according to the victim's profile and readiness to engage online.

Motivations on the perpetrator's side likewise diverge. Yet in every scenario behavioral dysfunction remains the common thread, afflicting offender and victim alike. That dysfunction, compounded by the victim's silence and reluctance to seek familial or institutional assistance, grants the blackmailer an opening to exert control before the situation escalates and reputational damage becomes irreversible. Principal enabling conditions include the following:

3.1 Deficiencies in Conduct and Value Systems:

Beyond discrete behavioral triggers, both offender and victim are ultimately products of flawed educational practices across formative



stages. Such practices distort the individual's moral compass and shape attitudes in ways that later surface as deviant conduct. Education anchored in non-humanistic or socially injurious reference points subverts the normative framework that ought to regulate, for example, gender relations among adolescents. Ziouche (2017) underscores that weak socialization and absent value-based awareness are key drivers propelling certain individuals—whether as blackmailers or as targets—into cyber-crime (Ziouche, 2017).

Cultural legacies and strands of popular folklore may further romanticize the figure of the “hero” or, conversely, the suffering “victim.” Adolescents, eager to inhabit the heroic role, may therefore experiment with criminal patterns, particularly when digital tools offer a seemingly low-risk avenue.

Ignorance of essential facts—parental unfamiliarity with online risks, lax supervision, deficient guidance—coupled with waning informal social control, peer influence, and mere experimentation, converge to steer many into the cyber-extortion trap.

3.2 The enticement of the electronic medium

Contemporary digital tools hand would-be offenders distinct advantages, fueling a rise in on-line extortion. The virtual environment grants users sweeping control over their instruments, and extorters exploit three attributes above all:

- *Opportunity.* Crime thrives when an opening appears. In

borderless cyberspace, a victim's inattention—or feeble resistance—creates that opening.

- *Anonymity.* The web, smart devices, spoofed numbers, even a furtive Bluetooth flash allow the perpetrator to hide behind screens and keyboards.
- *Lower perceived risk.* Where an armed bank raid carries obvious danger, the same actor can operate on-line with a fraction of the exposure.

Inside many homes, satellite TV and always-on Internet have erased gender barriers while digital literacy lags. High-definition phone cameras, Bluetooth file swaps, and platforms such as YouTube give ill-intentioned users fresh avenues for extortion.

3.3 Emotional motives

Some adolescents engage in risky on-line behavior because unmet emotional needs push them toward virtual substitutes. Case files reveal persistent affective deprivation that drives them to fill the void through web-based or mobile relationships. Extorters, for their part, often view the episode as a test of their ability to exert psychological control. Parental composure—not harsh suspicion—is essential: excessive severity silences offspring and lets the situation fester. Nakib Ahmed's 2022 survey of female undergraduates confirms that weak family guidance directly increases vulnerability to image-based extortion through social media platforms (Nakib, 2022).



3.4 Economic motives

Material deprivation remains a decisive trigger. Many blackmailers justify their demands with references to unemployment, poverty, and a blunted moral compass; conversely, victims—especially young women—leave themselves open when they seek money their families cannot provide. Poverty underlies theft, embezzlement, monetary extortion, and prostitution alike. The perpetrator threatens disclosure to secure cash; the victim’s own need may be twisted into a sexual quid pro quo, such as promising a job only if she submits to the blackmailer’s demands.

3.5 Cultural motives

In many societies, perceptions of crime and deviance shift according to the offender’s or victim’s gender. Some inherited norms even excuse adolescent males while censuring females, reinforcing a “Don Juan” ideal for boys and an image of submissiveness for girls. Sabti and Abd-Nabi (2022), examining cyber-extortion and its threat to social order, report that most victims are women targeted on Facebook, Instagram, or TikTok—a pattern that mirrors broader cultural dynamics of power and sexuality in virtual space (Sabti & abd-Nabi, 2022). Romantic escapades become stories to be broadcast; certain young men recount them with relish and, at times, circulate images or recordings to amplify their status.

3.6 Media Amplification

Youths today spend long stretches before screens, absorbing a global torrent of entertainment and information that does not invariably promote pro-social values. Recent cinema and streaming content often glamorize the *hacker-hero* outwitting law-enforcement agencies, planting the notion that technical prowess, not legality, defines success. Music videos and televised dramas likewise portray intimate relationships outside accepted social frameworks, encouraging both genders to emulate risky behavior. Such narratives seldom reveal the painful fallout when those alliances unravel (Alshahri, 2011). The cumulative effect is a media landscape that normalizes—if not celebrates—illicit online conduct.

3.7 Weak Religious Restraint

Deviant online behavior might be caused by a shallow grasp of religious principles: ritual knowledge may be present, but practical ethics are missing. Parental shortcomings intensify the gap—failure to earn a lawful livelihood, to guide children, or to model integrity leaves adolescents vulnerable to the moral vacuum of cyberspace (Hamyn, 2011). The result is a fertile ground for fraud and extortion, especially inside a borderless digital ecosystem where temptations multiply and immediate supervision is scarce.

3.8 Low Preventive Awareness

A final catalyst is the community's limited grasp of basic cyber-hygiene. Large segments of the population remain unaware of the ruses

employed by online predators, granting offenders a relatively safe operating environment. Absent robust deterrent or educational mechanisms, blackmail proliferates.

Mitigation therefore begins at home: families must instill caution, protect personal data, and treat digital platforms as tools—useful yet bounded. Allowing them to fuse seamlessly with everyday life invites unnecessary exposure to harm.

4. Typology of Cyber-Extortion

4.1 Classification by the Offender’s Objective

4.1.1 Pecuniary Gain

The most common motive is straightforward enrichment. The blackmailer demands money—cash or items of equivalent value—in exchange for keeping private information from public view. The sum requested fluctuates with the victim’s perceived means, regardless of gender.

4.1.2 Sexual Gratification

Where the victim is female—especially where she is both female and a minor—the extorter often seeks sexual access or compliance. The threat may involve forcing the victim into direct involvement with the blackmailer or compelling her to engage in illicit acts with a third party. The coercion can be a single incident or repeated episodes, but patterns indicate that women constitute the bulk of targets for this variant.

4.1.3 Utilitarian Advantage

A utilitarian motive arises when the offender leverages the victim's secrets to secure some benefit unrelated to money or sex: carrying out a theft, interceding with an official, or otherwise performing an act—lawful or unlawful—contrary to the victim's will. Once coercion is established, the legal elements of extortion are satisfied (Aarab, 2021).

4.2 Classification by the Victim's Profile

Cyber-extortion has no single face. Its contours shift with the victim: a juridical person in one case, a woman in another, a man in a third. The categories set out below follow that victim-based taxonomy.

4.2.1 Juridical Persons

When the target is a government or corporate entity, the offence centers on acquiring confidential data and threatening to release it unless demands are met.

4.2.2 Minors

Under Algerian law majority commences at eighteen; anyone younger is a minor. Adolescents, drawn to digital media yet short on practical judgment, are disproportionately vulnerable. The blackmailer pressures the child by threatening to publish compromising images, videos, or chats that would diminish the minor's standing at home or in society.

4.2.3 Women



Female victims represent the archetype of cyber-extortion. Offenders—typically men—collect or fabricate intimate photographs, audio recordings, or video clips depicting illicit relations, then employ these materials to exact either cash or sexual compliance. Cases where the victim is simultaneously female and underage combine the hazards outlined above, even if the techniques differ.

4.2.4 Men

Male victims, though less discussed, are not immune. Offenders may target a man of means, threatening to publish compromising images, or exploit confidential workplace information whose disclosure would damage the victim's social or professional standing (Hamyn, 2011).

5. Consequences of Cyber-Extortion

Cyber-extortion rarely harms only the immediate victim; its repercussions spill outward, touching several circles bound to that individual. The phenomenon is therefore multi-dimensional—personal and collective—and warrants careful mapping.

5.1 Psychological Impact

Electronic offences leave a distinctive psychic residue. Victims report chronic intimidation, persistent anxiety, guilt, insomnia, recurring nightmares, poor concentration, and a pervasive fear of exposure. Some quit their employment despite financial need; irritability colors both workplace and home life, productivity drops,

and—at the extreme—nervous breakdown emerges. A subset develops a hostile view of society and contemplates self-harm. Communities, too, absorb damage: collective trust erodes, and a balanced perception of others gives way to suspicion (Alshahri, 2011).

Because the digital threat often lingers, recovery is slow. Continuous therapeutic follow-up may be required long after the victim is physically removed from the triggering environment. Social re-integration can stall; isolation becomes a coping mechanism, and personality shifts—toward aggression or antisocial traits—sometimes take root.

5.2 Security Impact

At the macro level, cyber-extortion undermines public safety. Fear for honor and reputation grows, and ancillary crimes frequently accompany the primary act: rape, fornication, alcohol or narcotics abuse, even organized prostitution and financial predation. Homicide rates can climb where families seek to “wash dishonor” through retaliatory killings. In one well-publicized episode, online vigilantes styling themselves *Swords of Honor* threatened extrajudicial violence against extorters. Such responses, while understandable in certain cultural contexts, only multiply illegality and illustrate why criminal justice—investigation, prosecution, adjudication—must remain the state’s prerogative.

5.3 Social Impact

Cyber-extortion inflicts some of the most corrosive damage found



in modern offending, and the harm radiates well beyond the immediate victim. Within the family sphere, fallout is acute. When the target is a woman—the primary caretaker and, in many settings, the linchpin of domestic stability—the offence can push her toward deviant coping strategies (Hamyn, 2011). On a wider plane, extortion operates as a disintegrative force: it erodes social cohesion, weakens interpersonal bonds, and distorts the ordinary channels of interaction that keep a community viable.

The mechanism is straightforward. Blackmail enables one segment of society to exploit another, breeding distrust, fear, and a pervasive sense of alienation. Routine exchanges freeze under the pressure of suspicion; people hesitate to engage, unsure whether new connections are safe or potentially dangerous. Over time, the fabric that knits individuals together frays. If unchecked, that dynamic threatens not merely isolated relationships but the continuity of the social order itself.

6. Security Response to Cyber-Extortion

The most effective bulwark against cyber-crime demands tools bolder than classic policing. Conscious of this, Algeria has adopted a dual strategy: (i) a rigorous penal framework and (ii) operational deployment of the police and the *Gendarmerie nationale* as the frontline defense in cyberspace.

6.1 Legislative Measures

Widespread misuse of the digital sphere has driven many jurisdictions to recalibrate their criminal codes, inserting stringent sanctions for cyber-offences now deemed uncontrollable by orthodox means. Ignoring the problem—or attempting a blanket ban—would be naïve; the proper remedy is to trace, identify, and incapacitate the offender before blackmail material reaches the public domain.

Algerian law contains no stand-alone provision entitled “cyber-extortion.” The conduct is subsumed under conventional extortion, though it unfolds in a virtual setting. Particular protection is nevertheless accorded to personal liberty and privacy. Article 303 bis of the Penal Code criminalizes exploitation of surveillance product:

“Anyone who deliberately violates another’s private life, by any technique whatsoever, shall be punished by imprisonment of six months to three years and a fine of 50 000 to 300 000 dinars, where the act consists in:

1. capturing, recording, or transmitting private or confidential conversations without the consent of the parties;
2. capturing, recording, or transmitting the image of a person in a private place without that person’s consent.” (Penal Code (amended 2015), art. 303 bis)

In practice, trial judges concentrate on the constituent acts—covert capture and use of private material—placing special weight on the *private place* requirement, which they regard as pivotal (Al-Aziz, 2016). Article 303 bis references secrecy (“private or confidential



conversations”) and tranquility (“private place”), i.e., the zone where an individual reasonably expects peace and seclusion (Ziyad, 2013).

Liability attaches to anyone who employs the illicitly obtained file—audio, image, document—under the statutory conditions, whether the use is public or private. The offence is complete once the item is stored, made accessible, or otherwise exploited in cyberspace.

A further nuance concerns public figures. Parliament recognizes that artists and other celebrities live under perpetual media glare; their expectation of privacy narrows accordingly. Yet any invasion exceeding that reduced margin still triggers civil liability. The injured party may sue for appropriate relief—monetary, specific, or symbolic. Courts enjoy broad discretion because such injuries defy exact pecuniary valuation; a fitting remedy may include an in-kind rectification, for example a public apology (Al-Arfi, 2022).

6.2 Role of the Police and the National Gendarmerie in Tackling Cyber-Extortion

Algeria has activated its police and National Gendarmerie as the principal operational shield against cyber-crime. Under domestic criminal-procedure law, the police detect offences, receive complaints, conduct preliminary enquiries, and transmit dossiers to the competent prosecutorial organ (Aicha, 2013). In practice, the General Directorate of National Security has adopted a two-track approach:

- Specialized training. Judicial-police officers now follow courses

devoted exclusively to digital offending.

- Scientific and technical laboratories. Newly equipped forensic labs extract and analyze data from electronic devices suspected of facilitating the offence, supplying investigators with probative material.

At gendarmerie level, organizational lines have been redrawn to match unit competences with crime typology. The force created the National Institute for Forensic Evidence and Criminology, an expert body charged with digital examinations, and it set up a Digital-Media Offences Unit that assigns institute experts to courts nationwide. These specialists help judges decode complex electronic evidence.

Legislative support comes from Law No. 04-09 on the special rules for preventing and suppressing offences linked to information and communication technologies. The statute established a National Authority for the Prevention of ICT-Related Offences with three core mandates:

1. Coordinate national prevention and enforcement initiatives
2. Assist judicial authorities and judicial-police services through intelligence gathering and forensic expertise.
3. Exchange information with foreign counterparts to identify and locate suspects.

Cyber-extortion, accordingly criminal under positive law, represents a new form of deviance produced by the tension between the

community's value system and technological modernity. Expansion of the digital sphere has shifted crime from physical to virtual space, giving rise to fresh modalities of domination that elude traditional social control. A responsive legal–security architecture—tailored to the emergent modus operandi—remains essential for reconstructing social order and regulating online interaction in a manner consistent with the requirements of digital-age social control.

7. Community Awareness as a Preventive Shield against Cyber-Extortion

An effective awareness strategy must operate on two planes—internal and external. The present section isolates the internal dimension; it centers on concrete practices that individual users should adopt whether they connect at work, in public venues, or at home.

7.1 Internal Safeguards

Any person who goes on-line—whether at the office, in a public setting, or on a home network—should observe a few basic safeguards. The principal measures are set out below:

- Ben Omar Yassin (2024) found that the routine posting of intimate details on social networks significantly fuels cyber-extortion. Users must therefore weigh every disclosure, particularly in public settings. When a website offers to store credentials, a single click on *yes* may lodge the password permanently—even after browser data are wiped. Passwords

should be saved only on personal devices kept at home.

- The computer is a means, not an end. Users should steer clear of suspect websites—those promising hacking tutorials, easy money through file-sharing schemes, or other forms of digital chicanery. Registering on such platforms is an open invitation to fraud.
- A thorough grasp of both the benefits and hazards of the Internet is indispensable. Home computers ought to remain under collective oversight, outside children’s bedrooms, and subject to a fixed usage schedule. A joint report by Kaspersky and the UAE Cybersecurity Council, “*Growing Up with the Internet*,” highlights variations in children’s online behavior and supplies guidance on screen time, social-media exposure, privacy threats, and cyber-bullying.
- Every household device should run antivirus programs updated daily to enrich signature databases. Kaspersky’s *Safe Kids* suite, for example, has proven effective as a parental-control solution, giving caregivers confidence that minors navigate the web with reduced risk (Abou-Taleb, 2022).
- Finally, system firewalls must remain enabled and properly configured; they intercept malicious code and prevent it from roaming freely through the machine’s architecture.

7.2 External Safeguards

The external dimension covers every immediate step a person



must take once cyber-extortion has begun. Rapid, structure action is essential.

- The victim should approach the nearest police station or *Gendarmerie nationale* post and lodge a formal complaint stating the relevant facts.
- Attempts at appeasement—whether by pleading or by partial compliance—are counter-productive, given the leverage the offender already holds through audio, images, or video files.
- Disclosing the incident to relatives secures emotional and practical support, reducing the isolation the blackmailer seeks to exploit.
- Disconnect Internet access or segment the local network so that the intruder cannot pivot to other household devices.
- Duplicate all programs and files deemed important. If a full wipe of the device or its hard drives becomes necessary, critical data remain retrievable (Ziouche, 2017).

Community awareness thus constitutes the cornerstone of any preventive strategy against cyber-extortion. Institutional efforts—governmental or civil—cannot succeed unless individuals themselves internalize the norms of safe digital conduct. Internal safeguards evidence personal responsibility: rational, informed use of the online environment. External safeguards demonstrate the user’s readiness to solicit specialized assistance the moment coercion appears. Together,

these layers promote a culture of proactive, self-directed vigilance, shifting the center of gravity from external policing to conscious self-regulation—a transition indispensable for collective resilience in the cyber age.

8. Conclusion

Rapid technological change—most visibly in Internet communications and the ever-smarter hardware riding on 3G and 4G networks—has welded mobile devices to daily life. That ubiquity opens doors not merely for legitimate exchange but also for intrusions by hackers and data thieves. A string of new social phenomena now fall under the rubric of cyber-crime; none has disrupted the domestic sphere more than cyber-extortion. Once a tangible, document-based offence, extortion now moves in a coded, symbolic environment where the threat of exposing private material is magnified by the sheer scale of social-media use. Secondary offences—fraud, drug trafficking, even homicide—frequently follow.

Faced with an assault on personal privacy of this magnitude, scholars, practitioners, and law-enforcement agencies have converged on both remedial and preventive measures: scientific symposia to craft field solutions, sharper penal provisions, and broad information campaigns. Yet, however vigilant state organs may be, comprehensive cyber-security remains elusive without sustained collaboration among all social actors—first and foremost the family, Internet-service providers, and schools. Where public awareness spreads, exposure to blackmail contracts and enforcement becomes easier.

Building on the foregoing analysis, the study advances several practical recommendations:

- Update penal statutes in step with technological advances that continually supply new tools for digital blackmail.

- Equip cyber-crime units with modern forensics and real-time monitoring technology proportional to offences committed in virtual space.

- Run periodic awareness drives in schools at every level, pairing security professionals with civil-society groups to teach young users how to report online crime.

- Expand radio and television programming that explores real-world cases, giving victims a voice and demystifying investigative procedures.

- Strengthen the family's supervisory role: install filtering software, keep devices in common areas, and cultivate open dialogue to close the gaps that offenders exploit.

- Embed digital-literacy modules in national curricula so that preventive habits form early.

- Raise statutory penalties—especially where offences undermine individual liberty or target minors—to reinforce deterrence.

9. Bibliography List:

- Aarab, M. (2021). The offence of threat and cyber-extortion. *Journal of Comparative Legal Studies*, 77(1), 1211–1212.
- Abou-Taleb, M. (2022, July 24). *Why cyber-blackmail keeps spreading*. Retrieved from Al-Masry Al-Youm:
<https://www.almasryalyoum.com/news/details/2644069>
- Aicha, B. (2013). *Criminal protection from information crime in Algerian legislation*. Algiers: Algiers.
- Al-Anazi, M. R. (2017). Criminal protection of the victim against extortion. *Arab Journal for Security Studies*.
- Al-Arfi, F. (2022). Evidentiary value of digital proof in establishing cyber-extortion under Algerian law. *Journal of Legal Studies*.
- Al-Aziz, N. A. (2016). *Special criminal protection in Algerian and French law*. Algiers: Houmah.
- Alruwais, F. B. (n.d.). Social awareness of cyber-extortion among Saudi families: A field assessment. *Journal of Arts and Humanities*.
- Alshahri, F. (2011). Civil-society responses to extortion: The cyber variant as test case. *Bāḥithāt Centre for Women's Studies*.
- Bachouche, N. (2024, February 14). *Fourteen thousand cyber-crimes recorded in 2023*. Retrieved from Echorouk Online: <https://www.echoroukonline.com>
- Ben Omar, Y. (2024). Child cyber-extortion in Algerian legislation. . *Notebooks of Politics and Law*, 16(2).

- Boumami, A. (2015). Cyber-crime as a spin-off of social-network platforms. *Jil Journal of Human and Social Sciences*.
- Centre for Security Research and Studies. (2016). *Cyber-crime in Gulf society and how to confront it*. Muscat: Sultan Qaboos Academy for Police Sciences.
- Hamyn, A. (2011). Extortion and the role of the General Presidency for the Promotion of Virtue and the Prevention of Vice in combatting it. *Extortion: Concept, causes, remedies*.
- Nakib, A. (2022). *Cyber-extortion targeting female university students on social networks. Master's thesis*. Tizi Ouzou: University of Tizi-Ouzou.
- Sabti, A. ..., & abd-Nabi, M. N. (2022). Cyber-extortion and its threat to society. *Journal of Tikrit University for the Humanities*, 29(1).
- Sebkhaoui, K. (2024). Cyber-extortion: A field study among students of Blida-2 University. *Journal of Legal and Social Sciences, Djelfa*, 9(1).
- Ziouche, S. (2017). Cyber-extortion and preventive strategies: A sociological Reading and Theoretical stances. *Journal of Social Sciences*.
- Ziyad, A. A. (2013). *The right to privacy in Algerian criminal legislation*. Batna.