ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

CYBERCRIME PREVENTION ACT OF 2012: AWARENESS, IMPACT, AND CHALLENGES ENCOUNTERED

Lentejas III, Virgilio J.,
Philippine College of Criminology - Graduate School

ABSTRACT

This study examined the awareness, impact, and challenges encountered in relation to the implementation of the Cybercrime Prevention Act of 2012. Guided by the objective of understanding how individuals and institutions perceive and respond to the law, the research explored three core dimensions: the extent of public awareness of the Act's provisions, its perceived impact on online safety and regulation, and the challenges experienced in its enforcement and compliance. A mixed-methods design was employed. Findings revealed that while most respondents demonstrated basic familiarity with the law – particularly its coverage of cyber libel, hacking, identity theft, and online fraud – awareness of penalties and enforcement mechanisms remained limited. The impact of the Act was noted in terms of increased caution in online behavior and recognition of legal safeguards, yet challenges persisted in areas such as inadequate dissemination, inconsistent enforcement, limited technological infrastructure, and gaps in digital literacy. Qualitative results further highlighted concerns about privacy, due process, and the difficulty of balancing freedom of expression with regulation. These findings suggest that although the Cybercrime Prevention Act provides a critical legal framework for addressing online threats, its effectiveness is hindered by awareness gaps, enforcement limitations, and resource constraints.

KEYWORDS: *Awareness, Challenges, Cybercrime, And Impact*

INTRODUCTION

The rapid advancement of digital technology has transformed the way individuals communicate, access information, and participate in social, economic, and political activities. While the internet and related technologies have brought unprecedented convenience and connectivity, they have also given rise to new forms of crime that transcend geographical boundaries (Wall, 2024). Recognizing the growing threats in cyberspace, the Philippine government enacted Republic Act No. 10175, otherwise known as the Cybercrime Prevention Act of 2012, to define, prohibit, and penalize offenses committed through information and communications technologies. Among its key provisions is the criminalization of cyber libel, a digital counterpart to traditional defamation, which has sparked significant discussion regarding freedom of expression, responsible online behavior, and the role of law enforcement in cyberspace (Mahmud et al., 2024; Zukić & Zukić, 2025).

The law seeks to protect individuals and institutions from various forms of cybercrime, including offenses against the confidentiality, integrity, and availability of computer data and systems; content-related crimes such as cybersex, child pornography, and cyber libel; and computer-related fraud and identity theft. In doing so, it aims to uphold digital security, promote ethical online conduct, and provide a legal framework for prosecuting cyber offenders. However, its implementation has also raised debates about potential misuse, overreach, and the fine balance between safeguarding reputations and preserving constitutionally guaranteed freedoms.

Understanding the awareness, perceived impact, and challenges surrounding the Cybercrime Prevention Act of 2012 is particularly relevant for Criminology students, who are future law enforcers and legal practitioners. Their level of knowledge about the law, perceptions of its effects on digital responsibility, freedom of speech, and law enforcement, as well as the difficulties they encounter in real-world contexts, provide valuable insights into the law's effectiveness and areas for improvement.

This study, therefore, examines Criminology students' awareness of the Cybercrime Prevention Act of 2012, explores the perceived impact of its provisions—particularly those related to cyber libel—and identifies the challenges they face in applying or responding to the law in practical scenarios. The findings aim to inform the development of targeted educational interventions that will enhance students' capacity to navigate the digital landscape responsibly, ethically, and within the bounds of the law.

Literature Review

Cybercrime has expanded alongside digital transformation, which facilitates communication and commerce but also creates opportunities for intrusion, data theft, and service disruption across borders. International organizations such as INTERPOL, APEC, OECD, and the UN have emphasized awareness, cross-border cooperation, and legislative harmonization to address these transnational risks (Neethu, 2020). Frameworks like the Budapest Convention standardize offenses and procedural

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

powers, enabling faster mutual legal assistance and clearer evidentiary protocols (Tropina, 2020; Nandan, 2021). Operational responses increasingly rely on private-sector actors—cloud providers, ISPs, CERT/CSIRT teams, and platform safety units—supported by public agencies through digital forensics labs, cyber task forces, and trained personnel (Caneppele & Da Silva, 2022). Technological solutions such as machine learning enhance detection and prevention, but human-centered practices, ethical safeguards, and evidence-handling processes remain essential. Effective cybercrime prevention thus combines harmonized legal frameworks, technical capacity, public-private coordination, and individual digital responsibility, with organizations embedding privacy-by-design, layered controls, and incident-response planning into governance structures (Kikerpill, 2021; Mujtaba, 2023).

In the Philippines, RA 10175 (Cybercrime Prevention Act of 2012) defines cybercrime through specific unlawful acts targeting ICT systems, including offenses against data integrity, computer-related crimes such as fraud and identity theft, and content-related offenses such as cyber libel, cybersex, and child pornography, with jurisdiction extending to certain extraterritorial cases (Li, 2021; LawPhil, 2025). Rising internet use, smartphone penetration, and digital services have contributed to increased hacking, online fraud, identity theft, online sexual exploitation, and cyber libel incidents (The Asia Foundation, 2022; Department of Justice, 2025; Unicef, 2024). Both foreign and local literature highlight the need for a multi-layered approach combining legal harmonization, institutional capacity-building, public awareness, and technical measures, alongside individual and organizational responsibility, to ensure effective cybercrime prevention, protection of users, and preservation of trust in the digital ecosystem.

Theoretical Framework

This study is grounded in Routine Activities Theory (RAT) and General Strain Theory (GST), which together explain how crime happens and why people may choose to commit it, especially in online settings.

Routine Activities Theory explains crime as a matter of opportunity. Crime occurs when three things come together at the same time: a motivated offender, a suitable target, and the lack of effective guardianship. The theory emphasizes that crime is shaped by everyday routines, not just by a person's character. As people's daily activities change—such as how they work, shop, or use the internet—the chances for crime also change. In cyberspace, online platforms act as the "places" where offenders and victims meet. Targets may include user accounts, personal data, or online reputations, especially when they are visible, easy to access, and poorly protected. Guardianship online goes beyond police presence and includes security tools, user awareness, moderation, and platform rules. Studies show that risky online habits and weak protection increase the chances of victimization. RAT also guides prevention by encouraging safer routines, stronger security, and better supervision online.

General Strain Theory, on the other hand, focuses on why individuals may turn to crime. GST argues that people experience different kinds of stress or strain, such as failure to achieve goals, loss of important relationships, or exposure to negative treatment like bullying or discrimination. These experiences can create strong negative emotions, especially anger and frustration. When people feel that legal solutions are slow, unfair, or ineffective, crime may appear to be an easy or quick way to cope or retaliate. However, not everyone who experiences strain commits crime. Personal coping skills, moral beliefs, and support from family, school, or peers can reduce the likelihood of criminal behavior.

Together, RAT and GST provide a clearer picture of crime. RAT explains how and where opportunities for crime occur, while GST explains why individuals may respond to stress through criminal behavior. Combined, these theories help explain both online and offline crime and point to practical ways to prevent it—by reducing risky situations, strengthening protection, and helping individuals cope with stress in healthy ways.

Significance of the Study

This study holds significant value as it generates an evidence-based picture of how Republic Act No. 10175—especially its cyber-libel provisions—is understood, felt, and navigated by future criminal justice practitioners.

Primary beneficiaries are the Criminology students themselves. Findings can be translated into targeted digital-citizenship sessions, briefings on rights and responsibilities, and practical guidance on documentation, reporting, and self-protection online. Students who have experienced, been accused of, or witnessed cyber-libel incidents gain clearer pathways for help, while the broader student body benefits from clarified do's and don'ts that reduce both victimization and wrongful accusations.

Institutional stakeholders within the College of Criminal Justice and the wider HEI—including deans, program chairs, faculty, curriculum developers, Student Affairs/Guidance, and ICT/Discipline offices—can use the results to update syllabi and orientations, design focused trainings, strengthen incident-response SOPs (reporting, evidence handling, referrals), and allocate resources where gaps are greatest. The evidence base supports accreditation and quality-assurance efforts and can inform campus policies that balance free expression with protection from online harm.

Justice-sector partners—notably the PNP Anti-Cybercrime Group/Regional Anti-Cybercrime Units, campus police/security, prosecutors, and legal aid—benefit from a clearer understanding of knowledge gaps, reporting barriers, and coordination pain points on campus. This enables better community outreach, more student-friendly protocols, and tighter linkages between schools

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

and law enforcement for faster, more victim-sensitive responses to cyber-libel complaints.

Policy and advocacy stakeholders—such as CHED, DOJ/NCAC, DICT, local government councils, and civil society/NGOs working on digital literacy and press freedom—can draw on the study to refine guidance, craft awareness campaigns, and support evidence-informed adjustments to training requirements or referral mechanisms.

Finally, the study contributes to scholarship, offering a mixed-methods template, validated measures, and contextual themes that future researchers can adapt in other HEIs and regions, thereby expanding the national knowledge base on cybercrime awareness, impacts, and challenges.

Objectives of the study

The primary objective of this study is to determine the level of awareness, perceived impact, and challenges encountered by Criminology students regarding Republic Act No. 10175, otherwise known as the *Cybercrime Prevention Act of 2012*. Specifically, this study aims to:

1. Describe the profile of the Criminology students.
2. Determine the level of awareness of Criminology students regarding Republic Act No. 10175.
3. Examine whether there is a significant difference in the level of awareness of the respondents when they are grouped according to their profile variables.
4. Assess the perceived impact of cyber libel laws among Criminology students
5. Determine whether there is a significant difference in the perceived impact of cyber libel laws when respondents are grouped according to their profile.
6. Identify the challenges encountered by Criminology students in dealing with cyber libel cases, whether as victims, accused individuals, or observers.
7. Propose appropriate programs or interventions based on the findings of the study to improve awareness, understanding, and responsible engagement with cyber libel laws.

METHODOLOGY

Research Design

The study used an explanatory sequential mixed methods design, starting with a quantitative phase followed by a qualitative phase to deepen and explain the initial results. First, survey questionnaires were administered to Criminology students from different year levels in a school in Tacloban City to collect data on their profiles, awareness of R.A. 10175, and perceptions of the impact of cyber-libel laws. The data were analyzed using descriptive statistics to identify general trends and differences.

In the second phase, qualitative interviews were conducted with selected participants to explore the reasons behind the survey findings. These interviews focused on students' experiences and challenges in dealing with cyber-libel cases. The qualitative data were analyzed using thematic analysis, allowing the researcher to connect personal narratives with the quantitative results. Overall, the combined approach provided both a broad overview and a deeper understanding of awareness, perceptions, and challenges related to cyber-libel laws.

Research Method

Mixed methods research combines quantitative and qualitative approaches in one study to provide a more complete understanding of a research problem. Quantitative methods offer measurable patterns and relationships, while qualitative methods add context, meaning, and explanations of processes. Researchers decide how the two strands are timed (sequential or parallel), which has priority, and how they are integrated across design, data collection, and interpretation.

The main strengths of mixed methods include greater depth and breadth, improved validity through triangulation, and the ability to explain unexpected results. However, it also requires more time, careful alignment of samples, and deliberate integration of findings. When properly executed, mixed methods research produces results that are both statistically informative and practically meaningful, making it valuable for policy and real-world applications.

Population of the Study

The study population consisted of BS Criminology students from a College of Criminal Justice in Tacloban City. For the quantitative phase, purposive sampling was used to include students from Levels 1 to 4, both regular and irregular. The registrar's official class lists served as the sampling frame, and all eligible students were invited to participate through class announcements and program-wide notices. Inclusion criteria required participants to be currently enrolled, 18 years old or above, and willing to give informed consent. Students below 18, not currently enrolled, or unwilling to participate were excluded.

For the qualitative phase, 20 informants were selected using criterion-based sampling to ensure relevant experience with cyber-libel issues. Participants included victims, accused individuals, and observers with firsthand or practical knowledge. Selection emphasized variation in roles, year levels, and experiences to capture diverse perspectives. Semi-structured interviews explored real-life experiences, challenges, and suggestions related to cyber-libel cases. Recruitment continued until data saturation was achieved, and ethical safeguards—such as informed consent, confidentiality, and participant well-being—were strictly observed.

Data Gathering Tools

The study used a structured survey questionnaire and interviews as its primary data-gathering tools to obtain both quantitative and qualitative information related to Republic Act No. 10175. The survey questionnaire was organized into four parts to ensure

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

clarity and ease of response. The first part gathered basic profile information, specifically sex at birth and year level, to describe the respondents and allow for subgroup comparisons while minimizing the collection of sensitive personal data. The second part measured the level of awareness of the Cybercrime Prevention Act of 2012 in terms of its provisions, scope, penalties, and relevance using a four-point awareness scale. The third part focused on students' perceptions of the impact of cyber libel laws on digital responsibility, freedom of speech, and law enforcement, using a four-point impact scale to capture the degree of perceived effects. The fourth part consisted of an open-ended question that allowed respondents to describe challenges they encountered in cyber-libel situations, providing contextual insights that complemented the closed-ended items.

For the qualitative component, the researcher conducted semi-structured interviews with 20 informants who had direct experience with cyber-libel cases, including victims, accused individuals, and observers. The interview guide was developed based on survey results and open-ended responses and explored participants' experiences, understanding of RA 10175, reporting and evidence-gathering processes, interactions with school offices or law enforcement, perceived fairness and outcomes, and suggestions for improvement. To ensure the quality of the instruments, reliability was assessed using Cronbach's alpha, yielding an overall coefficient of .892, which indicates good internal consistency. Content validity was established through expert evaluation using the Content Validity Index, which resulted in a CVI of 1.00, confirming that all items were clear, relevant, and aligned with the constructs of the study.

Data Gathering Procedures

The data-gathering process began with the researcher securing written permission from the Dean of the Graduate School of the Philippine College of Criminology and the Dean of the College of Criminal Justice of the participating higher education institution in Tacloban City. After approval, coordination was made with the program chairperson and year-level advisers to schedule the survey administration, determine dissemination channels, and access class lists for monitoring coverage. A Google Form survey was then prepared, beginning with an informed consent page that explained the study's purpose, procedures, duration, eligibility, risks and benefits, confidentiality, voluntariness, and participants' rights. To ensure privacy, no identifying information was collected, and measures were applied to limit duplicate responses. The survey link was distributed through official class announcements and group messages, with faculty advisers briefly introducing the study during class time. The researcher monitored responses throughout the collection period, addressed technical concerns, and sent reminders to improve participation. After the survey period ended, the form was closed, data were exported and securely archived, and a working copy was created for analysis. All files were stored in an encrypted, access-controlled drive, and data quality checks were conducted prior to analysis, ensuring the integrity, confidentiality, and ethical handling of the collected information.

Treatment of Data

The study analyzed data using a mixed-methods approach. Quantitative data were cleaned, coded, and summarized with descriptive statistics, including frequencies for categorical variables and medians for ordinal scales. Nonparametric tests—Mann–Whitney U and Kruskal–Wallis H—were used to examine differences by sex and year level, with post hoc tests applied when needed. For the qualitative data, thematic analysis of interview transcripts identified key themes explaining or contextualizing the survey findings. Coding decisions were documented, excerpts were anonymized, and the qualitative insights were integrated with quantitative results to provide a richer, explanatory understanding of awareness, perceptions, and challenges related to cyber-libel laws.

Ethical Considerations

The study followed strict ethical procedures to protect participants. Permission was obtained from the relevant deans, and all materials were reviewed for compliance with institutional standards and the Philippine Data Privacy Act. Participation was voluntary, limited to those 18 and above, and had no impact on grades or services. Informed consent was obtained for both the survey and interviews, with participants able to skip questions or withdraw at any time. Survey responses were anonymous, and interview data were de-identified and stored securely on encrypted drives. Sensitive topics, such as experiences with cyber-libel incidents, were handled carefully using neutral prompts, optional responses, and safeguards for participant well-being, including referrals to support services if needed. No questions solicited illegal admissions, and any disclosures of imminent harm were managed according to institutional and legal guidelines.

RESULTS AND DISCUSSION

This section presents the findings of the study in accordance with the research objectives. Data are summarized in tables, followed by interpretation and discussion anchored on related literature.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

Profile of the Respondents

Table 1. ***Frequency and Percent Distribution of the Profile of the Respondents***

Indicators	Frequency	Percent
Sex		
Female	148	29.8%
Male	349	70.2%
Year Level		
1st Year	98	19.7%
2nd Year	64	12.9%
3rd Year	167	33.6%
4th Year	168	33.8%

Table 1 reveals two notable features of the respondent profile: the sex distribution and the year-level composition. The markedly male-dominated sample (70.2% male versus 29.8% female) suggests that the overall findings are likely to be influenced more by male perspectives and experiences. This imbalance may reflect the historical enrollment trends of the program or discipline, where men traditionally outnumber women. While the representation of both sexes allows for sex-disaggregated analysis, the comparatively smaller female subgroup may constrain the detection of subtle or moderate differences in perceptions, attitudes, or outcomes, thereby necessitating careful interpretation of any sex-based comparisons. From a methodological standpoint, the distribution remains sufficient for broad comparisons, yet the imbalance underscores the importance of contextualizing findings within the gender dynamics of the program.

In terms of year level, the data highlight a cohort that is disproportionately composed of upper-year students, with third- and fourth-year students making up roughly two-thirds of the sample (33.6% and 33.8%, respectively). This composition indicates that the findings may be more reflective of individuals who have greater curricular exposure, more advanced academic experiences, and deeper institutional socialization. Such students are likely to exhibit stronger familiarity with program requirements, greater confidence in their academic skills, and a more developed sense of professional identity. By contrast, first-year students (19.7%) and especially second-year students (12.9%) represent a much smaller proportion of the sample, potentially limiting the granularity of insights into the experiences of earlier cohorts. This underrepresentation may obscure differences related to transitional adjustment, foundational learning, or early engagement with institutional systems, thereby warranting caution in generalizing results across all year levels. Collectively, the profile suggests that while the dataset is robust for analyzing trends among advanced students, it may understate the perspectives of those in the early stages of the program.

Difference in the Level of Awareness of the Respondents

Table 2. ***Difference in the Level of Awareness of the Respondents***

Indicators	Sex		Year Level	
	U Statistic	p value	X^2	p value
Law's Provision	23861	0.146	25.0	<.001**
Scope	23135	0.047*	19.5	<.001**
Penalties	22747	0.023*	26.7	<.001**
Relevance	24239	0.242	10.9	0.012*

Table 2 compares awareness of RA 10175 by sex (Mann–Whitney U) and by year level (Kruskal–Wallis). By sex, no significant differences emerged for Law's Provisions (U=23,861, p=0.146) or Relevance (U=24,239, p=0.242), whereas small but significant gaps appeared for Scope (U=23,135, p=0.047) and Penalties (U=22,747, p=0.023). By year level, awareness differed significantly across all four domains—Law's Provisions (χ^2=25.0, p<.001), Scope (χ^2=19.5, p<.001), Penalties (χ^2=26.7, p<.001), and Relevance (χ^2=10.9, p=.012). Post-hoc results consistently show 4th-year students scoring higher than lower cohorts (for Provisions: higher than 1st and 3rd; for Scope and Penalties: higher than 1st–3rd; for Relevance: higher than 1st). These patterns indicate broadly similar awareness between males and females, coupled with a clear progression in awareness as students advance through the program. The use of rank-based nonparametric tests is appropriate for Likert-type awareness measures summarized with medians.

The absence of sex differences on Provisions and Relevance suggests that information campaigns or curricular touchpoints addressing what the law is and why it matters are reaching students irrespective of gender. The modest sex effects for Scope and Penalties may reflect differential exposure to courses, co-curricular activities, or media coverage that emphasize jurisdiction/extraterritoriality and sanction structures; however, the effects are small and not systematic across domains. In

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

contrast, the robust year-level gradients across all domains imply cumulative gains from coursework, practicum, case analyses, and institutional seminars that typically intensify in upper years. Pedagogically, this calls for front-loading core content on the law's scope (e.g., extraterritorial application, service-provider duties) and penal provisions earlier in the curriculum, then deepening with scenario-based analyses and compliance/reporting workflows in later years. Programmatically, institutions should scaffold legal-technical literacy (definitions, scope, penalties) with procedural literacy (reporting, evidence preservation, coordination with PNP-ACG) to translate "awareness" into informed digital citizenship and help-seeking behavior.

The observed "higher-year advantage" is consistent with Philippine studies showing that while college students generally recognize the provisions of RA 10175, their understanding remains moderate and uneven, particularly in technical areas such as jurisdictional scope, organizational liability, and service provider obligations. For example, Althibyani and Al-Zahrani (2023) reported that students demonstrated high awareness of common cybercrimes but showed weaker comprehension of procedural provisions. Similarly, Li (2021) found that while internet users were broadly aware of cybercrime threats, their grasp of specific legal mechanisms was limited. Calupit (2025) also emphasized persistent ambiguities in the enforcement of RA 10175, particularly concerning jurisdiction and interagency coordination, while Sund (2020) highlighted gaps in public awareness campaigns regarding service provider obligations and extraterritorial application. These findings are consistent with the Implementing Rules and Regulations of RA 10175, which specify not only the definitions of offenses such as cyber libel and illegal access but also obligations of service providers to preserve data and assist law enforcement (Implementing Rules and Regulations, 2015). Suminig et al. (2025) further noted that these elements—penalties, scope, and enforcement—require continuous education to translate awareness into effective digital citizenship. Together, these studies corroborate the current results that awareness deepens with educational progression, underscoring the importance of embedding RA 10175 content early in the curriculum and revisiting it progressively for greater depth.

Difference in the Respondents' Perceived Impact of Cyber Libel Laws

Table 3. ***Difference in the Respondents' Perceived Impact of Cyber Libel Laws***

Indicators	Sex		Year Level	
	U Statistic	p value	X^2	p value
Digital Responsibility	24041	0.184	6.60	0.086
Freedom of Speech	24788	0.437	4.97	0.174
Law Enforcement	25476	0.796	3.10	0.376

Table 3 examines whether perceived impacts of cyber-libel laws differ by sex (Mann–Whitney U) and by year level (Kruskal–Wallis) across three domains: Digital Responsibility, Freedom of Speech, and Law Enforcement. All tests are non-significant: by sex—Digital Responsibility (U=24,041, p=0.184), Freedom of Speech (U=24,788, p=0.437), Law Enforcement (U=25,476, p=0.796); by year level—Digital Responsibility (χ^2=6.60, p=0.086), Freedom of Speech (χ^2=4.97, p=0.174), Law Enforcement (χ^2=3.10, p=0.376). These results indicate no detectable group differences in students' perceptions: males and females report comparable impacts, and perceptions are broadly similar from first through fourth year. The choice of rank-based nonparametric tests is appropriate for Likert-type medians, supporting the validity of these inferences.

The consistently non-significant findings suggest that students encounter shared curricular and socio-digital environments that yield comparable perceptions of how cyber-libel laws shape responsibility, expression, and enforcement. In practice, this may reflect uniform exposure to institutional policies, campus seminars, or national media narratives about RA 10175 that cut across demographics. Programmatically, the absence of cohort gaps implies schools can scale common interventions (e.g., digital-citizenship modules on verification, civility, and rights-based speech; workflow guidance on reporting and evidence preservation) without heavy differentiation by sex or year level.

Comparable "no-difference" patterns appear in research where digital-citizenship competencies are shaped more by shared educational exposure than by sex or year standing. Al-Abdullatif and Gameil (2020) found digital citizenship to be linked chiefly with learning experiences (e.g., online civic engagement), not uniformly with demographic splits—consistent with broadly similar perceptions across student groups here. International studies echo this: work on digital citizenship in higher education reports that course-embedded training can homogenize responsible-use attitudes across cohorts, aligning with the present null differences (e.g., distance-learning contexts showing convergent student–faculty awareness after common training). In the Philippine legal backdrop, Columbia University (2014), in its report on Disini v. The Secretary of Justice, clarified the constitutional contours of cyber-libel while voiding several overbroad provisions—jurisprudence that has since become standard content in university briefings, plausibly contributing to a shared interpretive frame across students irrespective of demographic strata.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

CONCLUSION AND RECOMMENDATIONS

The study revealed that most respondents were male and concentrated in the upper year levels, particularly the third and fourth years, suggesting that awareness and understanding of RA 10175 (Cybercrime Prevention Act of 2012) are influenced more by academic experience than by gender. Overall, students demonstrated moderate awareness of the law's provisions, scope, penalties, and relevance, indicating recognition without full comprehension of its technical and practical applications. Awareness tended to increase with year level, highlighting the role of academic progression and exposure to institutional activities. Students perceived a moderate impact of cyber libel laws on digital responsibility, freedom of speech, and law enforcement, recognizing the law's role in promoting accountability and civility online while remaining cautious of limitations such as potential chilling effects and enforcement challenges. No significant differences in perceptions were observed across sex or year level, suggesting that shared learning environments and information sources shape a common understanding among students. The study also identified three main challenges: victims faced trauma, reputational damage, and legal hurdles; accused individuals experienced stigma, financial strain, and restrictions on speech; and observers struggled with misinformation, ethical dilemmas, and inconsistent enforcement. These findings highlight the complex and multifaceted nature of cyber-libel issues.

In response, the study proposes a holistic program aimed at raising awareness, strengthening procedural literacy, and providing support mechanisms for all stakeholders. Recommendations include integrating RA 10175 and cyber-libel awareness into general education, communication, and ethics courses through graded discussions, case analyses, and debates to foster critical understanding. Schools should partner with law firms, human rights organizations, and media watchdogs to provide practical exposure through lectures, immersion projects, or internships, while establishing streamlined referral pathways to accredited legal aid or public attorneys to address victims' legal and emotional challenges. Advocacy efforts should be pursued to improve law enforcement capacity, including digital forensics training and dedicated cyber-libel prosecution teams. Restorative justice frameworks are recommended to mediate disputes and reduce emotional and reputational impacts, and digital literacy programs should be expanded to include media analysis, fact-checking, and training in identifying misinformation and defamation boundaries. Finally, institutions are encouraged to establish research and monitoring centers to track cybercrime trends, conduct awareness studies, and guide policy interventions. Collectively, these measures aim to strengthen legal literacy, institutional support, and responsible digital citizenship, ensuring that students are equipped to navigate cyber-libel laws ethically and effectively.

ACKNOWLEDGEMENT

This study would not have been possible without the guidance, generosity, and encouragement of many individuals and institutions. I am sincerely grateful for the time, expertise, and care they extended throughout the research process—from proposal development and instrument validation to data collection, analysis, and final defense.

First and foremost, I thank my adviser, Dr. Mandy G. Gonzales, for unwavering mentorship. Your sharp questions, detailed feedback, and steady encouragement shaped the rigor and clarity of this work. I am deeply appreciative of the countless hours you devoted to reading drafts, refining the methodology, and helping me keep sight of the study's purpose and ethical obligations.

I also extend my gratitude to Atty. Joaquin R. Alva, Ph.D., Dean of the PCCR Graduate School, for your leadership and guidance. My sincere thanks to the Chairperson of the Panel of Examiners, Dr. Imelda Runas, and to the Panel Members—Dr. Vivian G. Pinkihan and Dr. Ada Marie Campos—for your insightful critiques and practical suggestions that strengthened both the analysis and presentation of findings.

I am grateful to the Dean of the College of Criminal Justice, the Program Chairperson, year-level advisers, and administrative staff of Leyte Colleges for facilitating permissions, coordinating schedules, and assisting with the distribution of the survey link. Your cooperation ensured smooth, ethical, and efficient data collection.

My heartfelt thanks go to all participants—the Criminology students who completed the survey and the key informants who shared their experiences and reflections. Your candid responses and willingness to participate made this research both meaningful and possible. I am committed to honoring your contributions by presenting the results responsibly and with respect for confidentiality.

Finally, I am deeply thankful to my family and relatives for their patience, prayers, and constant encouragement. Your understanding during long nights of writing and analysis kept me grounded and motivated. To my friends and colleagues who offered moral support and timely reminders to rest—thank you. This work is as much yours as it is mine.

REFERENCES

1. *Abubakari, Y. (2021). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. Przestrzeń Społeczna, 1(1/2021 (21).*
2. *Ahmad, R., & Thurasamy, R. (2022). A Systematic Literature Review of Routine Activity Theory's Applicability in Cybercrimes. Journal of Cyber Security and Mobility, 11(3), 405-432.*
3. *Al-Abdullatif, A., & Gameil, A. (2020). Exploring students' knowledge and practice of digital citizenship in higher education. International Journal of Emerging Technologies in Learning (iJET), 15(19), 122-142.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

4. *Al-Badayneh, D. M., Al Dosari, H. M., Al Qahtani, H. M., Alkhater, J. A., & Mehawesh, S. S. (2024). College Students Attributional Differences in Knowledge Awareness about a Cybercrimes Law. Journal of Ecohumanism, 3(6), 773-786.*
5. *Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. Heliyon, 10(12).*
6. *Almrezeq, N., Alserhani, F., & Humayun, M. (2021). Exploratory study to measure awareness of cybercrime in Saudi Arabia. Turkish Journal of Computer and Mathematics Education, 12(10), 2992-2999.*
7. *Alsaeed, H. R., Elsayad, W. A., Abd El Ghani, R. T., & Hassan, M. A. (2023). Awareness Of Cybercrime Risks And Its Relationship To Attitude Toward The Internet Use Among University Students. Journal of Positive School Psychology, 7(10).*
8. *Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. Sustainability, 15(15), 11512.*
9. *Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205-217.*
10. *Anesa, P., & Engberg, J. (2023). Investigating legal discourse in the digital. The Digital (R) Evolution of Legal Discourse: New Genres, Media, and Linguistic Practices, 10, 1.*
11. *Atrey, I. (2023). Cybercrime and its legal implications: Analysing the challenges and legal frameworks surrounding cybercrime, including issues related to jurisdiction, privacy, and digital Evidence. International Journal of Research and Analytical Reviews, 10(3).*
12. *Awinja, J. M. (2021). Online defamation: Balancing reputational harm and the freedom of expression and the media.*
13. *Bag-ao, B. V. C. (2025). 'In Number There is Strength': Multi-Agency Collaborative Strategies for Combating Online Sexual Abuse and Exploitation of Children (Osaec) in Cagayan De Oro City, Philippines. Social Inquiry into Well-Being, 23(1), 26-57.*
14. *Biswal, C. S., & Pani, S. K. (2021). Cyber-crime prevention methodology. Intelligent data analytics for terror threat prediction: Architectures, methodologies, techniques and applications, 291-312.*
15. *Blancaflor, E., Arpilleda, J. A., Garcia, A. U., Monasterial, J. A., & Sulit, R. R. (2023, March). A literature review on the various trends of digital forensics usage in combating cybercrimes. In Proceedings of the 2023 6th international conference on electronics, communications and control engineering (pp. 132-138).*
16. *Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. Social Science Computer Review, 40(4), 933-954.*
17. *Bossler, A., & Holt, T. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. International Journal of Cyber Criminology, 3(1), 400-420.*
18. *Braun, C. (2024). The Cumulative Strain Paradigm: Exploring the Nexus of Terrorism and Violence Through a Criminological Lens (Doctoral dissertation, University of Nebraska at Omaha).*
19. *Brucal, A., Abante, M. V., & Vigonte, F. (2025). Cybercrime Prevention Act of 2012 in Practice: Cybersecurity, Controversy, and the Future of Digital Rights in the Philippines. Controversy, and the Future of Digital Rights in the Philippines (May 19, 2025).*
20. *Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews, 8(1), 2025024-2025024.*
21. *Butt, J. S. (2024). A comparative study about the use of artificial intelligence (AI) in public administration of Nordic states with other European economic sectors. Euro Economica, 43(1), 40-66.*
22. *Cabazares, S. M. T. (2022). "Jurisprudential Norms without Precedence": Upholding Liberty and Prosperity amid the Obscurity of Laws in the Era of Disinformation Technology.*
23. *Cai, C. (2025). Cyber Governance in China: Balancing State Centrism and Collaborative Dynamics. Taylor & Francis.*
24. *Calupit, P. A. (2025). Exploring the PNP regional anti-cybercrime unit 5 capability on cybercrime challenges: An empirical analysis. International Journal for Multidisciplinary Research, 7(3), 1-8.*
25. *Caneppele, S., & Da Silva, A. (2022). Cybercrime. In Research handbook of comparative criminal justice (pp. 243-260). Edward Elgar Publishing.*
26. *Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime detection and prevention efforts in the last decade: an overview of the possibilities of machine learning models. Rigeo, 11(7).*
27. *Cho, D. (2025). Cyber Resilience in South Korea. Asia Policy, 20(2), 46-59.*
28. *Cleofas, J. V., & Labayo, C. C. (2024). Youth netizens as global citizens: digital citizenship and global competence among undergraduate students. Frontiers in communication, 9, 1398001.*
29. *Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588-608.*
30. *Columbia University. (2014). Disini v. The Secretary of Justice.*
31. *Concoles, C. R., Cristobal, N., Felonia, E., Tadtad, V. M., & Villafuerte, K. A. (2022). Cybercrime awareness and cybercrime prevention attitude of criminology students. Southeast Asian Journal of Multidisciplinary Studies, 1(1), 2022-2022.*
32. *Cortesi, S., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). Youth and digital citizenship+ (plus): Understanding skills for a digital world. Berkman Klein Center Research Publication, (2020-2).*
33. *DataReportal-Global Digital Insights. (2024). Digital 2024: The Philippines.*
34. *Department of Justice. (2025). Identity theft.*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

35. *Disini v. Secretary of Justice. (2014). Supreme Court ruling on cyber-libel and related provisions.*
36. *Dougherty, T., & Lastrić Đurić, N. (2022). The United States approach to the investigation and prosecution of cybercrime and cryptocurrency crime. Hrvatski ljetopis za kaznene znanosti i praksu, 29(2), 409-431.*
37. *Fortun, Narvasa and Salazar Law. (2024). What is cyber libel?*
38. *Franceschini, I., Li, L., & Bo, M. (2025). Scam: Inside Southeast Asia's Cybercrime Compounds. Verso Books.*
39. *Garcia, K. M. P., & Marcelo, P. M. T. (2023). Pursuing a Balanced Approach to Speedy Case Disposition: An Analysis of Possible Solutions and Alternative Remedies to Ensure the Speedy Disposition of Cases for the Accused, the Victims, and the State. Phil. LJ, 96, 513.*
40. *Guison, R., & Macalintal, A. (2023, June). When Cyber Libel Restrains Press Freedom: The Case of Maria Ressa. In MediAsia2023 Conference Proceedings.*
41. *Hasbullah, M. A. (2022). Identifying the effects of cybercrime on business laws: implications for businesses and consumers. International Journal of Cyber Criminology, 16(2), 119-130.*
42. *Helm, C. (2025). Educational Strain and Juvenile Recidivism: A General Strain Theory Analysis of Probation Youth (Master's thesis, The University of North Carolina at Charlotte).*
43. *International Commission of Jurists. (2020). Statement on the Ressa & Santos cyber-libel conviction and implications for expression.*
44. *Isom Scott, D. A., & Stevens Andersen, T. (2020). 'Whitelash?'status threat, anger, and white America: a general strain theory approach. Journal of crime and justice, 43(4), 414-432.*
45. *Khan, M. N. I., & Ahmed, I. (2025). A Systematic Review of Judicial Reforms and Legal Access Strategies in the Age of Cybercrime and Digital Evidence. International Journal of Scientific Interdisciplinary Research, 5(2), 01-29.*
46. *Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. F1000Research, 11, 971.*
47. *Kikerpill, K. (2021). The individual's role in cybercrime prevention: internal spheres of protection and our ability to safeguard them. Kybernetes, 50(4), 1015-1026.*
48. *LawPhil. (2025). G.R. No. 203335.*
49. *Lee, J. M., Kim, J., Hong, J. S., & Marsack-Topolewski, C. N. (2021). From bully victimization to aggressive behavior: Applying the problem behavior theory, theory of stress and coping, and general strain theory to explore potential pathways. Journal of Interpersonal Violence, 36(21-22), 10314-10337.*
50. *Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. Deviant Behavior, 37(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409*
51. *Li, J. (2021). Cybercrime in the Philippines: A case study of national security. Turkish Journal of Computer and Mathematics Education, 12(11), 4224-4231.*
52. *Magbanua, K. S. (2022). An analysis of the legal and ethical implications of online disinformation in the Philippines. Journal of Public Representative and Society Provision, 2(2), 72-79.*
53. *Mahmud, K., Ahmed, E., Islam, Z., Billah, B., Banarjee, B., & Islam, K. (2024). Freedom of Expression in Cyberspace: Society, Law and its Effects in Bangladesh's Perspective. Library of Progress-Library Science, Information Technology & Computer, 44(4).*
54. *Mambile, C., & Mbogoro, P. (2020). Cybercrimes awareness, cyber laws and its practice in public sector Tanzania. International Journal of Advanced Technology and Engineering Exploration, 7(68), 119-126.*
55. *Martzoukou, K., Kostagiolas, P., Lavranos, C., Lauterbach, T., & Fulton, C. (2022). A study of university law students' self-perceived digital competences. Journal of Librarianship and Information Science, 54(4), 751-769.*
56. *Meehan, T., Forrester, L., & Haaja, J. A. (2024). Sociological theories of crime: Strain theories. Introduction to Criminology and Criminal Justice.*
57. *Movassagh, N. (2021). Awareness and Perception of Phishing variants from Policing, Computing and Criminology students in Canterbury Christ Church University (Master's thesis, Canterbury Christ Church University (United Kingdom)).*
58. *Mujtaba, B. G. (2023). Operational sustainability and digital leadership for cybercrime prevention. International Journal of Internet and Distributed Systems, 5(2), 19-40.*
59. *Nanath, K., Kaitheri, S., Malik, S., & Mustafa, S. (2022). Examination of fake news from a viral perspective: an interplay of emotions, resonance, and sentiments. Journal of Systems and Information Technology, 24(2), 131-155.*
60. *Nandan, A. B. (2021). Cybercrimes and Its Alarming Escalation during Recent Times: An International Legal Perspective. Issue 4 Int'l JL Mgmt. & Human., 4, 2413.*
61. *Neethu, N. (2020). Role of International Organizations in Prevention of Cyber-Crimes: An Analysis. Nalsar University of Law, Hyderabad, 5-17.*
62. *Nweze-Iloekwe, N. (2022). The Legal and Regulatory Aspect of International Cybercrime and Cybersecurity: Limits and Challenges.*
63. *Office of Cybercrime. (2025). Republic Act No. 10175 – Cybercrime Prevention Act of 2012.*
64. *Pasinhon, L. G., & Donato, L. M. (2024). Capability of the Regional Anti-Cybercrime Unit-Cordillera (RACU-COR) in Handling Cybercrime Cases. Asia Pacific Journal of Advanced Education and Technology, 3(2).*
65. *Poland, B. (2024). Digital Rights in a Connected World: International Approaches to Safeguarding Freedom of Expression Online. Mayo Communication Journal, 1(1), 52-62.*
66. *Ragragio, J. L. D. (2025). Contentious press freedom: Media law and the Supreme Court in the Philippines. Media, Culture & Society, 47(2), 271-286.*
67. *Ramos, H. K. S. (2023). Judicial Accountability in Trafficking Cases: Assessing the Adjudication of Offenses Involving Government Officials and the Effectiveness of the New Anti-Trafficking Guidelines (Doctoral dissertation, De La Salle University).*
68. *Respicio & Co. (2025). Cybercrime Complaint for Hacking*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 2| February2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753|| ISI Value: 1.188

69. *Reyes, M. C. (2024). Rethinking the Cybercrime Prevention Act of 2012. Center for Integrative and Development Studies. https://www. academia. edu/123826193/Rethinking_the_Cybercrime_Prevention_ Act_of_2012.*
70. *Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. Criminal Justice and Behavior, 38(11), 1149-1169. https://doi.org/10.1177/0093854811421448*
71. *Rodrigo, M. M., Ong, R. J., Garcia, K. C., Flores, C. E., & Torres, J. M. (2024). Fighting Fire with Fire: Learning Artificial Intelligence's Latent Power Against Disinformation. Available at SSRN 5050256.*
72. *Rufino, C. D., & Moyao, W. G. (2025). Cybersecurity Awareness and Practices among Criminal Justice Students in One Higher Educational Institution in Cordillera. Technium Soc. Sci. J., 71, 215.*
73. *Serafica, R. B., & Oren, Q. C. A. (2022). Upgrading the ICT regulatory framework: Toward accelerated and inclusive digital connectivity (No. 2022-26). PIDS Discussion Paper Series.*
74. *Seyidoğlu, S. (2024). Strain, Anger and Crime: A Sociopsychological Evaluation in the Context of the General Strain Theory. Süleyman Demirel Üniversitesi İnsan ve Toplum Bilimleri Dergisi, (62), 233-264.*
75. *Shami, A. Z. A., Saleem, M., & Ashraf, J. (2025). Cybercrime and digital evidence: Investigating the challenges and opportunities in prosecuting cybercrime and handling digital evidence. Research Consortium Archive, 3(2), 401-411.*
76. *Sharma, J. (2025). Evaluating the Impact of Cybercrime Awareness: A Case Study. International Journal of Innovations in Science, Engineering And Management, 59-65.*
77. *Siregar, G., & Sinaga, S. (2021). The law globalization in cybercrime prevention. International Journal of Law Reconstruction, 5(2), 211-227.*
78. *Smith, T. (2023). An Exploratory study into the aetiology of cybercrime:: Comparing the utility of the Routine Activities Theory using a model-comparison approach. Caribbean Journal of Multidisciplinary Studies, 2(1).*
79. *Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. International Cybersecurity Law Review, 4(3), 299-323.*
80. *Sosa, G. C. (n.d.). Country report on cybercrime: The Philippines.*
81. *Stephenson, P. C. (2024). Juvenile Coping and General Strain Theory (Master's thesis, The University of Mississippi).*
82. *Suminig Jr, A., Abante, M. V., & Vigonte, F. (2025). Safeguarding Cyberspace: A Comprehensive Analysis of the Cybercrime Prevention Act of 2012 (RA 10175) and Its Role in Philippine Digital Governance. Available at SSRN 5270089.*
83. *Sund, P. (2020). The Rationality Gap between Cyber Security and Rule of Law in Extra-Territorial Processing of Classified Information on Cloud Environments.*
84. *Supreme Court E-Library. (2025). G.R. No. 203335.*
85. *Tandoc, E. C., Sagun, K. K., & Alvarez, K. P. (2023). The digitization of harassment: Women journalists' experiences with online harassment in the Philippines. Journalism Practice, 17(6), 1198-1213.*
86. *Team, I. G. P. (2025). EU general data protection regulation (GDPR): an implementation and compliance guide. Packt Publishing Ltd.*
87. *The Asia Foundation. (2022). Cybersecurity in the Philippines.*
88. *Togana, N., Caoalo, J. E., Dagdagan, M., Estigoy, R. L., Gaong, J., Neyney, L., ... & Valera, K. R. (2025). Cases and Challenges in Investigating Cybercrime: The Case of Regional Anti-Cybercrime Unit 1. Available at SSRN 5179956.*
89. *Toso, C. H. S., Jumalon, A. J. A., Magadan, J. A. R., Alvarico Jr, A. B., & Cuevas, J. F. (2023). Cybercrime Awareness Among Senior High School Students. Mediterranean Journal of Basic and Applied Sciences (MJBAS), 7(2), 160-176.*
90. *Tropina, T. (2020). Cybercrime: Setting international standards. In Routledge Handbook of International Cybersecurity (pp. 148-160). Routledge.*
91. *Tüner, T. (2023). Evolution of ASEAN's Policy on Cyber Security. Middle East Technical University, Faculty of Architecture. Retrieved from https://core. ac. uk/download/620614216.pdf.*
92. *Ueda, N. (2024). Japan's Cyber Defence: A Cyber Power Theory Perspective.*
93. *Umeugo, W. (2023). Cybercrime awareness on social media: A comparison study. International Journal of Network Security & Its Applications, 15(2), 23-35.*
94. *Unicef. (2024). Online Sexual Abuse and Exploitation of Children in the Philippines.*
95. *United Nations Office on Drugs and Crime. (2025). Cybercrime Module 2 Key Issues: Computer-related offences.*
96. *UP Center for Integrative and Development Studies. (2024). Rethinking the Cybercrime Prevention Act of 2012.*
97. *Wall, D. S. (2024). Cybercrime: The transformation of crime in the information age. John Wiley & Sons.*
98. *Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. The British Journal of Criminology, 56,(1), 21-48. https://doi.org/10.1093/bjc/azv011*
99. *Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. Societal Impacts, 1(1-2), 100013.*
100. *Yar, M., & Steinmetz, K. F. (2023). Cybercrime and society.*
101. *Younies, H., & Al-Tawil, T. N. E. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). Journal of Financial Crime, 27(4), 1089-1105.*
102. *Zukić, M., & Zukić, A. (2025). Defamation Law and Media: Challenges of the Digital Age. MAP Education and Humanities, 5, 98-109.*