AJRS
/https://albalqajournal.ammanu.edu.jo
Vol.(27) No.(2) 2024
Received: 24/04/2024
Accepted: 06/06/2024
Published: 30/06/2024

مجلة البلقاء
للبحوث والدراسات
Al-Balqa Journal
for Research & Studies

Exploring The Landscape Of Cyber Crimes Targeting Women: A Literature Review On Cybee Security Laws

Mustafa Al Atiyat[1*], Anas Ratib Alsoud[2], khalid Al-Dweri[3]

[1]Al-Ahliyya Amman University
[2]Al-Ahliyya Amman University
[3]Kuwait International Law School

Abstract

Background & Statement of the problem: As technology continues to advance and reshape our lives, the digital realm has become a breeding ground for various forms of cybercrimes, including those specifically aimed at women. With the increasing prevalence of digital technologies and internet usage, the vulnerability of women to various forms of cybercrimes has become a pressing concern.

Objectives: This research paper presents a comprehensive literature review on the landscape of cybercrimes targeting women within the context of cyber security laws aiming to explore the nature and extent of cyber crimes against women, focusing on key offenses such as online harassment, cyberstalking, non-consensual pornography, and online identity theft.

Methods: Nearly 60 articles and studies related to the specific topic were analyzed thoroughly in this paper and it highlights the evolving nature of cybercrimes against women and the need for robust legal frameworks to protect and empower them in the digital era. Additionally, the existing cyber security laws and their effectiveness in addressing these crimes were critically examined.

Results: The findings of this research emphasize the importance of comprehensive measures, including legislative updates, awareness campaigns, and enhanced law enforcement efforts, to combat cybercrimes targeting women effectively.

Conclusions (Recommendations and contributions): It is evident that existing cyber security laws need to be strengthened and adapted to effectively address these crimes and also a multi-faceted approach is needed to enhance the protection of women against cybercrimes.

Key words

Awareness, Cyber security laws, Cybercrimes against women, Cybercrimes, Defence, Method.

AJRS
/https://albalqajournal.ammanu.edu.jo
المجلد (27) العدد (2) 2024
الاستلام: 20/09/2023
القبول: 14/02/2024
النشر: 30/06/2024

مجلة البلقاء
للبحوث والدراسات
Al-Balqa Journal
for Research & Studies

قراءة في الجرائم الإلكترونية التي تستهدف الإناث: مراجعة الأدبيات المتعلقة بقوانين الأمن السيبراني

مصطفى العطيات[1]*،أنس راتب السعود[2]، خالد الدويري[3]

[1] جامعة عمان الأهلية
[2]جامعة عمان الأهلية
[3]كلية القانون الكويتية العالمية

الملخص

خلفية الدراسة ومشكلتها: مع استمرار التكنولوجيا في التقدم وإعادة تشكيل حياتنا، أصبح العالم الرّقمي أرضًا خصبة لمختلف أشكال الجرائم الإلكترونية، بما فيها تلك التي تستهدف النساء على وجه الخصوص. ومع تزايد انتشار التقنيات الرّقمية واستخدام الإنترنت، أصبح تعرض النساء لمختلف أشكال الجرائم الإلكترونية مصدر قلق مُلّح.

الأهداف: تقدم هذه الورقة البحثية مراجعة شاملة للأدبيات حول مشهد الجرائم الإلكترونية التي تستهدف النساء في سياق قوانين الأمن السيبراني، بهدف استكشاف طبيعة ومدى الجرائم السيبرانية ضد النساء، مع التركيز على الجرائم الرئيسة مثل التحرش عبر الإنترنت، والمطاردة السيبرانية، والمواد الإباحية دون الموافقة، وسرقة الهوية عبر الإنترنت.

الطرق المستخدمة: تم تحليل ما يُقارب من 60 مقالًا ودراسة تتعلق بالموضوع بشكل شامل في هذه الورقة البحثية، مما يسلط الضوء على الطبيعة المتطورة للجرائم الإلكترونية ضد النساء، والحاجة إلى أُطر قانونية قوية لحمايتهنّ وتمكينهنّ في العصر الرّقمي. بالإضافة إلى ذلك، تم فحص قوانين الأمن السيبراني الحالية وفعاليتها في التصدي لهذه الجرائم بشكل نقدي.

النتائج: تؤكد نتائج هذا البحث أهمية اتخاذ تدابير شاملة، بما في ذلك التحديثات التشريعية، وحملات التوعية، وتعزيز جهود إنفاذ القانون، لمكافحة الجرائم الإلكترونية التي تستهدف النساء بشكل فعّال.

الاستنتاجات (التوصيات والمساهمة): من الواضح أنّ قوانين الأمن السيبراني الحالية تحتاج إلى تعزيز وتكييف لمواجهة هذه الجرائم بشكل فعّال، كما أنّ هناك حاجة إلى نهج متعدد الأوجه لتعزيز حماية النساء ضد الجرائم السيبرانية.

الكلمات المفتاحية

التوعية، الجرائم الإلكترونية ضد النساء، الجرائم الإلكترونية، الدفاع، قوانين الأمن السيبراني، المنهجية.

1. Introduction

Cybercrimes targeting women have become a significant concern in the digital age. With the rise of the Internet and the widespread use of technology, women have increasingly become victims of various forms of online exploitation, harassment, and abuse. These cybercrimes have a profound impact on women's safety, well-being, and their participation in the digital space (Uma, 2017). Addressing this issue requires a comprehensive understanding of the nature and extent of cybercrimes targeting women, as well as an examination of the legal frameworks and initiatives in place to combat these crimes. The advent of the Internet has undoubtedly brought numerous benefits and opportunities for women, enabling them to connect, communicate, and access information like never before. It has opened up new avenues for education, employment, entrepreneurship, and social engagement (Datta et al., 2020). However, alongside these advancements, the online world has also witnessed the emergence of cybercrimes specifically designed to target and victimize women. These crimes encompass a wide range of malicious activities, including but not limited to online harassment, cyberstalking, non-consensual pornography, doxing, and online identity theft. The impact of cybercrimes on women is significant and multifaceted. It extends beyond the immediate harm caused by these offenses, often leading to psychological trauma, social isolation, and reputational damage. Women who experience cybercrimes may face long-lasting emotional distress and find it challenging to regain a sense of security and trust in online spaces (Bhat and Ahmad, 2022). Furthermore, the fear of victimization can deter women from fully participating in digital platforms and exercising their rights to freedom of expression and privacy. In response to the increasing prevalence of cyber crimes against women, many countries have enacted cyber security laws and regulations to provide legal protection and remedies for victims. These laws aim to establish a legal framework for prosecuting cyber offenders and deterring potential perpetrators. However, the effectiveness of these laws in addressing gender-based cybercrimes remains a subject of debate (Halder and Jaishankar, 2016). Challenges such as jurisdictional issues, lack of awareness, and the rapidly evolving nature of technology present obstacles to the successful prosecution and prevention of these crimes (Halder and Jaishankar, 2016).

Cyber security laws play a crucial role in safeguarding individuals, organizations, and nations from the growing threats posed by cybercrimes and malicious activities in the digital domain. As technology continues to advance, the need for robust legal frameworks to protect sensitive information, secure critical infrastructure, and combat cyber threats becomes increasingly imperative (Azad et al., 2017). This introduction provides an overview of cyber security laws, their objectives, and their significance in the modern digital landscape. Cyber security laws encompass a range of legal instruments, regulations, and policies that govern the protection of information systems, data privacy, and the prevention and response to cyber incidents (Boukemidja, 2018). These laws are designed to address the unique challenges posed by the interconnectedness of our digital infrastructure, including the ever-evolving nature of cyber threats, the sophistication of cyber attackers, and the potential impacts on national security, economy, and individual rights. The primary objectives of cyber security laws are manifold (Kabi et al., 2022). They aim to establish legal frameworks that define and criminalize various forms of cybercrimes, such as hacking, identity theft, malware distribution, and data breaches. These laws provide a basis for identifying, investigating, and prosecuting cyber offenders, ensuring accountability and deterrence. Cybersecurity laws focus on protecting critical infrastructure, including government systems, financial institutions, and essential services,

from cyber-attacks (Kaushik, 2014). They outline standards and regulations for organizations to implement security measures, conduct risk assessments, and develop incident response plans to mitigate the impact of cyber incidents and ensure the continuity of operations (Singh, 2015).

Cybersecurity laws often encompass provisions for protecting individuals' privacy and personal data. They set guidelines for data protection, secure handling of personal information, and the notification of data breaches (Jose, 2017). These provisions are crucial for maintaining trust in digital platforms and ensuring individuals' rights to privacy and control over their personal information (Malar, 2012). Additionally, cyber security laws may include provisions for international cooperation and information sharing to combat cross-border cyber threats effectively. Given the global nature of cybercrimes and the potential for cyber attackers to operate from different jurisdictions, international collaboration is vital for investigating cyber incidents, extraditing offenders, and sharing best practices in cyber defense (Sridevi et al., 2023). The significance of cyber security laws cannot be overstated. These laws provide a legal framework that enables governments, organizations, and individuals to protect themselves from cyber threats and respond effectively to cyber incidents. By establishing clear rules and consequences, cyber security laws create a deterrent effect and help to establish a cyber-resilient society (Ng et al., 2018).

However, the effectiveness of cyber security laws relies on several factors. The dynamic nature of technology and cyber threats necessitates regular updates and adaptations of these laws to address emerging challenges. Moreover, effective enforcement, capacity building, and international cooperation are critical to combat cybercrimes and ensure the implementation and adherence to cyber security laws (Reina, 2022). This review aims to provide a comprehensive analysis of cybercrimes targeting women and the existing legal frameworks designed to combat these offenses. By examining relevant literature, empirical studies, and case examples, this paper will shed light on the prevalence and impact of cybercrimes against women. It will critically evaluate the adequacy and effectiveness of current cyber security laws in addressing the unique challenges posed by these crimes. Additionally, it will explore the limitations and gaps in the legal frameworks, as well as highlight potential strategies and recommendations for strengthening the protection of women in the digital realm. The paper contributes to the field of cyber security laws in the following ways:

a) The paper provides a thorough examination and analysis of cybercrimes targeting women within the context of cyber security laws.

b) The paper critically evaluates the effectiveness and adequacy of existing cybersecurity laws in addressing gender-based cybercrimes.

c) The paper highlights the challenges faced by law enforcement agencies in investigating and prosecuting cybercrimes against women.

d) By consolidating relevant information, it provides a valuable resource for researchers, policymakers, and practitioners in the field.

e) The paper offers practical recommendations for policymakers, lawmakers, and law enforcement agencies to enhance the protection of women against cybercrimes.

1.2 Need for the survey

A survey is essential to gain a comprehensive understanding of the landscape of cybercrimes targeting

women and the effectiveness of cyber security laws in addressing these crimes. While existing research provides valuable insights, a survey can offer a more detailed and current assessment of the prevalence, nature, and impact of cybercrimes against women. It allows for the collection of primary data directly from victims, law enforcement agencies, and relevant stakeholders, offering first-hand accounts and experiences. Additionally, a survey can help identify the challenges and limitations faced by law enforcement agencies in investigating and prosecuting these crimes, as well as the barriers women encounter in seeking justice and support. By capturing quantitative and qualitative data, a survey can provide a holistic perspective on the various forms of cybercrimes, their consequences, and the effectiveness of legal frameworks in addressing them.

1.2 Need for the survey

A survey is essential to gain a comprehensive understanding of the landscape of cybercrimes targeting women and the effectiveness of cyber security laws in addressing these crimes. While existing research provides valuable insights, a survey can offer a more detailed and current assessment of the prevalence, nature, and impact of cybercrimes against women. It allows for the collection of primary data directly from victims, law enforcement agencies, and relevant stakeholders, offering first-hand accounts and experiences. Additionally, a survey can help identify the challenges and limitations faced by law enforcement agencies in investigating and prosecuting these crimes, as well as the barriers women encounter in seeking justice and support. By capturing quantitative and qualitative data, a survey can provide a holistic perspective on the various forms of cybercrimes, their consequences, and the effectiveness of legal frameworks in addressing them.

Moreover, a survey can serve as a platform to gauge awareness levels among women regarding their rights, existing laws, and available support systems. It can uncover the gaps in knowledge and understanding that need to be addressed through targeted awareness campaigns and educational initiatives. Additionally, a survey can identify potential areas of improvement in cyber security laws, such as the need for specific provisions or amendments to better protect women from emerging forms of cybercrimes. Furthermore, a survey can provide valuable insights into the perception of safety and trust in the digital space among women. It can shed light on their behavioral patterns, including the extent to which they engage in online activities and the precautions they take to mitigate the risks of cybercrimes. These insights can inform the development of policies, interventions, and preventive measures tailored to address the specific concerns and needs of women in the digital realm.

1.3 Scope of the survey

The scope of the survey will encompass a wide range of aspects related to cybercrimes targeting women and the effectiveness of cyber security laws. It will include but not be limited to the following areas:

Prevalence and types of cybercrimes: The survey will aim to capture data on the prevalence of various forms of cybercrimes against women, such as online harassment, cyberstalking, revenge porn, and identity theft. It will seek to understand the frequency and severity of these crimes and their impact on the victims.

Victim experiences and responses: The survey will explore the experiences of women who have been victims of cybercrimes. It will investigate their responses to the incidents, including whether they reported the crimes to law enforcement agencies, sought support from relevant organizations, or took measures to mitigate the consequences of the crimes.

Awareness of cyber security laws: The survey will assess the awareness levels among women regarding the existing cyber security laws designed to protect them. It will determine their knowledge of their rights, legal provisions, and available support systems in the event of cybercrimes.

Challenges and barriers: The survey will aim to identify the challenges faced by women in reporting cybercrimes and seeking justice. It will uncover the barriers they encounter, such as fear of retaliation, lack of trust in the legal system, or limited awareness of available resources. It will also explore the difficulties faced by law enforcement agencies in investigating and prosecuting these crimes.

Trust and safety in the digital space: The survey will gauge women's perceptions of safety and trust in the online environment. It will explore their behaviors, including the extent to which they engage in online activities, the platforms they use, and the precautions they take to protect themselves from cybercrimes.

Effectiveness of cyber security laws: The survey will assess the effectiveness of existing cyber security laws in addressing cybercrimes targeting women. It will seek feedback on the strengths and weaknesses of the legal frameworks, including suggestions for improvements or additional measures that could enhance the protection of women.

It is important to note that the scope of the survey may be further refined based on the research objectives, available resources, and the target population. The survey will be designed to provide a comprehensive understanding of the issues surrounding cyber crimes against women and the role of cyber security laws in addressing these crimes.

2. Methodology

The methodology for conducting the literature review on cybercrimes targeting women and cyber security laws involved a systematic approach. The research process began with identifying the research objectives and establishing the scope of the review. Relevant literature was searched using academic databases, scholarly journals, and conference proceedings, utilizing appropriate keywords and search terms. Inclusion and exclusion criteria were applied to select studies that aligned with the research objectives. The selected literature underwent a thorough screening and data extraction process, where key findings, methodologies, and arguments were identified. A critical analysis and synthesis of the extracted data were conducted to identify common themes and trends. The findings were then interpreted about the research objectives. The limitations of the literature review process were acknowledged, and recommendations for further research were provided. The methodology ensured a comprehensive and rigorous examination of the existing literature on cybercrimes targeting women and cyber security laws.

2.1 Understanding the landscape of cybercrimes targeting women

The review will explore the nature and extent of cybercrimes targeting women, shedding light on the prevalence, motives, and tactics employed by perpetrators. It will delve into key offenses, examining the psychological impact on victims and the broader societal implications. Additionally, the review will critically analyze the existing cybersecurity laws and their effectiveness in addressing and preventing cybercrimes against women. By synthesizing relevant literature, studies, and legal frameworks, this review seeks to identify gaps, challenges, and opportunities for strengthening cyber security laws and protection mechanisms for women. It aims to provide valuable insights for policymakers, lawmakers, law enforce-

ment agencies, and other stakeholders involved in shaping and implementing policies related to cyber security and women's rights.

Tharshini et al. (2021) explored the cybercrime threat landscape during the movement control order in Malaysia. It investigates the types of cybercrimes that were prevalent during the period and examines the impact of the movement control order on cybercrime activities in the country.

Aransiola and Asindemade (2011) focused on understanding the individuals who engage in cybercrime activities in Nigeria and examined the strategies they employ. It provides insights into the motivations and characteristics of cybercrime perpetrators in the Nigerian context.

Holt and Bossler (2008) explored the applicability of the lifestyle-routine activities theory in understanding cybercrime victimization. It investigates the factors that contribute to individuals becoming victims of cybercrimes and examines how routine activities and lifestyle choices impact the likelihood of victimization.

Swiątkowska (2020) focused on the challenges and potential strategies for tackling cybercrime in developing countries. It emphasizes the importance of addressing cybercrime to harness the digital potential of these countries and highlights the implications for economic development and growth.

Graham (2018) explored cybercrimes specifically targeted against women in India. While no specific publication details are provided, this study likely examines the various forms of cybercrimes faced by women in India, such as online harassment, cyberstalking, and the dissemination of non-consensual intimate images.

2.2 Forms of cyber crimes against women: online harassment, cyberstalking, and revenge porn

This literature review aims to provide a comprehensive understanding of online harassment, cyberstalking, and revenge porn as significant forms of cybercrimes against women. By exploring the existing research, studies, and legal frameworks, this review seeks to shed light on the prevalence, motives, and impacts of these crimes on women's lives. By synthesizing the available knowledge and identifying gaps in understanding, this literature review aims to contribute to the development of evidence-based strategies, policies, and interventions to combat these forms of cybercrimes against women. It seeks to advocate for greater awareness, legal protections, and support systems that empower women, promote digital safety, and foster a more inclusive and respectful online environment.

Lazarus (2022) et al. explored the application of feminist theory in understanding digital crimes, specifically focusing on the intersection of gender and cybercrime types. It examines how gender dynamics shape the perpetration and experience of cybercrimes, providing insights into the importance of feminist perspectives in understanding digital crime phenomena.

Lazarus (2019) highlighted the potential synergy between feminist criminology and the Tripartite Cybercrime Framework. It examines how feminist criminological perspectives can enhance the understanding and analysis of cybercrimes, emphasizing the need to consider gender dynamics in cybercrime research and prevention efforts.

Clevenger et al. (2018) explored the interpersonal cyber victimization literature, focusing on the role of technology in the perpetration of online victimization. It provides insights into the dynamics of cyberbullying, cyberstalking, and other forms of interpersonal

cyber victimization, highlighting the challenges and strategies in addressing these issues.

Ahmed (2019) involved a content analysis of gender-based offenses committed online, specifically focusing on cyberstalking. It examines the nature of cyberstalking incidents and explores the gendered dynamics within these offenses. The dissertation contributes to the understanding of cyberstalking as a form of gender-based cybercrime.

Wissink et al. (2023) examined the risk factors associated with juvenile cybercrime. It synthesizes findings from multiple studies to identify common risk factors that contribute to juvenile involvement in cybercrimes. The study provides insights into the individual, familial, and social factors that increase the likelihood of juvenile engagement in cybercriminal activities.

These studies contribute to the understanding of digital crimes and cybercrimes from different perspectives, including feminist theory, victimization literature, gender dynamics, and risk factors associated with cybercriminal behavior. They provide valuable insights into the complexities of digital crimes and highlight the importance of considering gender and social factors in understanding and addressing these phenomena.

2.3 Impact of identity theft and online fraud on women

This literature review will examine the impact of identity theft and online fraud on women from various perspectives. It will explore the financial, emotional, and psychological consequences experienced by female victims, highlighting the unique challenges they face in recovering from such crimes. The review will also delve into the social and cultural factors that contribute to women's vulnerability to identity theft and online fraud, including gender stereotypes, online behaviors, and societal pressures. Additionally, the review will discuss the existing legal and technological measures in place to prevent and address identity theft and online fraud, evaluating their effectiveness in protecting women. It will also identify gaps in knowledge and areas for improvement in policy, education, and support systems to better safeguard women's identities and mitigate the impact of these cybercrimes.

Copes et al. (2010) focus on differentiating types of identity theft victims using a national victimization survey. It examines the characteristics and experiences of identity theft victims, shedding light on variations in victimization patterns and the impact of identity theft on individuals.

Guedes et al. (2022) explored the determinants of victimization and fear of online identity theft. It investigates the factors that contribute to individuals becoming victims of online identity theft and the psychological impact it has on individuals' fear of victimization.

Cross et al. (2014) focused on the challenges faced in responding to online fraud victimization in Australia. It explores the difficulties encountered by law enforcement agencies and policymakers in addressing online fraud, highlighting the complexities of investigating and prosecuting online fraud cases.

Anderson (2006) examined the demographics of identity theft victims and the effects of demographic characteristics on victimization rates. It investigates how age, gender, income, and other demographic factors influence an individual's vulnerability to identity theft.

Reyns (2013) expanded routine activity theory to understand identity theft victimization in online contexts. It explores how individuals' online routines, such as internet usage patterns and online behaviors, contribute to their vulnerability to identity theft victimization.

These studies contribute to the understanding of identity theft, particularly victimization patterns, determinants of victimization, challenges in responding to online fraud, demographics of victims, and the role of routines in identity theft victimization. They provide insights into the dynamics of identity theft and contribute to the development of strategies and policies for prevention and intervention in this area.

2.4 Tactics and Strategies Employed by Perpetrators in exploiting women Online Cyber security Laws and Policies

Chawki et al. (2015) explored the intersection of cybercrime, digital forensics, and jurisdiction. It examines the challenges related to investigating and prosecuting cybercrimes across different jurisdictions and provides insights into the legal and technical aspects of digital forensics in cybercrime investigations.

Enein (2017) focused on the cybersecurity challenges specific to the Middle East region. It examines the evolving threat landscape, discusses the impact of geopolitical factors on cybersecurity, and explores the policy and technological measures required to address these challenges.

Airehrour et al. (2018) focused on social engineering attacks in the New Zealand banking system. It explores the techniques used by attackers to manipulate users and gain unauthorized access to sensitive information. The paper also proposes a user-reflective mitigation model to enhance security measures against social engineering attacks.

Welch (2016) explored the connection between human trafficking and terrorism, with a specific focus on preventing human trafficking within the context of the Islamic State. It discusses the role of national security resources in addressing human trafficking and highlights the importance of a comprehensive approach to combatting this crime.

Puyvelde and Brantly provided an overview of cybersecurity, focusing on the political, governance, and conflict dimensions of cyberspace. It explores the policies and strategies employed by different actors to address cybersecurity challenges and examines the role of international cooperation and conflict in shaping cybersecurity dynamics.

These publications cover a range of topics related to cybercrime, cybersecurity, digital forensics, social engineering attacks, human trafficking, and the geopolitical aspects of cybersecurity. They contribute to the understanding of these issues, providing valuable insights into the challenges and potential solutions in these domains.

2.5 Effectiveness of cyber security laws in addressing cybercrimes against women

Younies and Al-Tawil (2020) examined the impact of cybercrime laws on protecting citizens and businesses in the UAE. It explores the legal framework, policies, and regulations implemented in the UAE to combat cybercrimes and assesses their effectiveness in safeguarding individuals and organizations from cyber threats.

Chikumbi (2022) provided a critical analysis of cyber laws and cybercrimes in Zambia, with a specific focus on the Cyber Security and Cyber Crimes Act No. 2 of 2021. It examines the provisions of the act and evaluates its effectiveness in addressing cybercrimes and ensuring cybersecurity in Zambia.

Pawlak and Barmpaliou (2017) explored the politics surrounding capacity-building efforts in cybersecurity. It examines the challenges and opportunities associated with enhancing cybersecurity capabilities at the national and international levels, considering political factors that influence capacity-building initiatives.

Paul and Wang (2019) focused on determining the socially optimal investment in information technology (IT) for cybersecurity. It uses a mathematical model to analyze the trade-off between the costs and benefits of IT investment in cybersecurity and provides insights into the optimal allocation of resources to mitigate cyber risks.

Shamsi (2019) presented a case study that evaluates the effectiveness of a cyber security awareness program targeting young children in the UAE. It assesses the impact of the program in enhancing children's knowledge, skills, and behaviors related to online safety and cybersecurity.

These publications cover various aspects of cybercrime laws, cyber security awareness, cybersecurity capacity building, socially optimal IT investment for cybersecurity, and the evaluation of legal frameworks and policies in specific countries. They contribute to the understanding of the effectiveness of cybercrime laws, the challenges in implementing cybersecurity measures, and the importance of awareness and capacity building in ensuring cyber resilience.

2.6 Challenges in preventing and prosecuting cybercrimes against women

Levi et al. (2016) examined the nature and impact of economic cybercrimes, such as fraud and financial scams, on individuals, businesses, and society as a whole. The paper discusses the challenges faced by law enforcement agencies in investigating and preventing economic cybercrimes and highlights the need for effective policing strategies in the digital era.

Neira (2016) provided an in-depth exploration of identity theft from the perspective of a cybercriminal. The study delves into the motivations, techniques, and psychological factors that drive individuals to engage in identity theft. It offers insights into the mindset of cybercriminals and contributes to the understanding of this prevalent form of cybercrime.

Blazek (2016) examined the various types of cybercrimes, such as hacking, online fraud, and cyber harassment, and analyzed the efforts undertaken to combat these crimes. It sheds light on the challenges faced in addressing digital criminality and highlights the importance of effective measures to mitigate these threats.

Dokku and Kandula (2021) focused on the issues and challenges associated with the implementation of the Information Technology Act 2000 in India. It examines the legal framework for addressing cyber crimes in India and identifies the gaps and limitations that hinder effective enforcement. The paper provides insights into the need for amendments and enhancements to the existing legislation to tackle emerging cyber threats.

Levi (2017) provided an overview of economic cybercrimes, with a focus on assessing their trends, scale, and nature. It explores the various forms of economic cybercrimes, their impacts on individuals and society, and the challenges faced in combating them. The paper highlights the need for comprehensive approaches to address economic cybercrimes and improve the effectiveness of policing efforts.

These publications cover a wide range of topics related to economic cybercrime, identity theft, digital

criminality, legal challenges, and the assessment of cybercrime trends. They contribute to the understanding of the implications of economic cybercrimes, the mindset of cyber criminals, the fight against digital criminality, and the issues surrounding cybercrime legislation and enforcement.

2.7 International legal frameworks and initiatives for protecting women in cyberspace

Sebastian and Sandeep (2021) examined the data protection laws in India, with a particular focus on privacy and data protection in the digital realm. The authors critically analyze the legal framework for data protection in India and assess its effectiveness in safeguarding privacy rights. The study identifies gaps and challenges in the existing regulations and highlights the need for comprehensive and robust data protection laws to address the evolving landscape of cyberspace.

Munyolo (2021) investigated the regulatory framework for cybersecurity in the context of e-health in Kenya. The study critically analyzes the existing regulations and policies related to cybersecurity in the healthcare sector, assessing their effectiveness in protecting sensitive health data and ensuring the integrity of e-health systems. The research provides insights into the challenges faced by the regulatory framework and suggests potential improvements to strengthen cybersecurity measures in the Kenyan healthcare industry.

Zhou (2020) explored the relationship between digital labor platforms and labor protection in China. The paper examines the impact of these platforms on workers' rights, job security, and social protection measures. It discusses the challenges faced in regulating digital labor platforms and provides recommendations for enhancing labor protection in the digital economy, ensuring fair working conditions, and promoting the rights of digital platform workers.

Bentototahewa (2021) presented a framework for the acceptance and implementation of global data privacy and security policies by states, with a specific focus on Sri Lanka and the United Kingdom. The research critically examines the approaches of these two countries in addressing data privacy and security concerns and suggests strategies for the effective adoption and implementation of global policies at the national level. The study contributes to the understanding of the challenges and opportunities in harmonizing data protection practices across different jurisdictions.

Heijmans and Vosse (2021) highlighted the importance of bridging the digital divide and ensuring equitable access to digital technologies for all individuals and communities. It discusses the potential benefits of digital development cooperation in promoting socio-economic development, enhancing digital inclusion, and addressing the challenges associated with digital transformation. The research emphasizes the need for collaborative efforts among various stakeholders to promote inclusive digital connectivity as a driver of sustainable development globally.

2.8 Case studies and notable research on cybercrimes against women

Harkin et al. (2018) explored the challenges encountered by specialist police cyber-crime units. The paper presents findings from an empirical analysis, highlighting the difficulties faced by these units in effectively investigating and combating cybercrime. The study provides insights into the specific challenges and suggests potential strategies to enhance the capabilities of law enforcement agencies in addressing cybercrime.

Kabir (2018) examined cybercrime as a new form of violence against women, focusing on the case study of Bangladesh. The paper explores the various types of cyber crimes targeting women, their prevalence, and their impact on victims. It sheds light on the specific challenges faced by women in the context of cybercrime and discusses the measures needed to address this issue.

Kashif et al. (2020) highlighted the vulnerabilities and opportunities exploited by cyber-criminals during the global health crisis. It examines the types of cyber crimes that have seen a surge and provides insights into the underlying factors contributing to this increase. The study emphasizes the need for enhanced cybersecurity measures in the face of evolving cyber threats.

Pastrana et al. (2018) discussed the design and implementation of the Crimebb platform, which allows researchers to analyze and understand the activities and behaviors within these illicit online communities. It highlights the importance of such platforms for advancing cybercrime research and facilitating the development of effective countermeasures.

Le et al. (2019) provided an overview of cyber security in parallel and distributed computing environments. The book covers various concepts, techniques, applications, and case studies related to ensuring the security of parallel and distributed computing systems. It offers insights into the challenges and solutions in protecting these complex systems from cyber threats.

2.9 Emerging trends and future directions in cyber security laws for women's protection

Gupta et al. (2018) presented a taxonomy of methods for defending against phishing attacks, a prevalent form of cybercrime. They discuss current issues and challenges in combating phishing attacks and provide insights into future directions for developing effective countermeasures. The study contributes to the understanding of phishing attacks and provides a framework for improving the security of online systems and protecting users from phishing threats.

Kavanagh and Johnson (2017) provided comprehensive coverage of human resource information systems (HRIS). The book explores the basics of HRIS, and its applications in various organizational contexts, and offers insights into future directions in the field. It serves as a valuable resource for understanding the role of HRIS in managing human resources and discusses emerging trends and technologies shaping the future of HRIS.

Teraa et al. (2016) discussed the current trends in the diagnosis and management of critical limb ischemia, a severe form of peripheral artery disease. They provide insights into the advancements in treatment options and highlight the future directions for research and clinical practice in this field. The paper contributes to improving the understanding and management of critical limb ischemia, ultimately aiming to enhance patient outcomes.

Gupta et al. (2016) provided a comprehensive overview of modern cryptographic solutions for computer and cyber security. It covers various aspects of cryptography, including encryption algorithms, authentication protocols, key management, and security applications. The book serves as a valuable resource for researchers, practitioners, and professionals working in the field of computer and cyber security.

Lau and Dunn (2018) provided a comprehensive overview of therapeutic peptides, discussing their historical perspectives, current development trends, and future directions. The paper highlights the potential of

therapeutic peptides as a promising class of drugs and discusses emerging research areas and advancements in peptide-based therapeutics. The study contributes to the understanding of therapeutic peptides and provides insights into their future applications in medicine and healthcare.

3. Identifying the mismatch: evaluation of objectives and outcomes

The literature review on cyber security laws and cybercrimes targeting women has shed light on several important aspects. The evaluation of objectives and outcomes has revealed a mismatch between the existing cybersecurity laws and the challenges faced by women in the digital realm. Here are the key findings and outcomes of this research:

Mismatch in objectives: The analysis highlights a misalignment between the objectives of cyber security laws and the specific vulnerabilities and risks faced by women. Existing laws often fail to adequately address the unique nature and impact of cybercrimes targeting women.

Evaluation of objectives: The research has evaluated the objectives of cyber security laws about their effectiveness in preventing, detecting, and addressing gender-based cyber crimes. It has revealed gaps and limitations in the current legal framework.

Identification of challenges: The literature review has identified various challenges faced by law enforcement agencies in investigating and prosecuting cyber crimes against women. These challenges include the complexity of cyber crimes, limited resources and training, and issues of jurisdiction and cross-border cooperation.

Findings on gender-based cyber crimes: The review has examined different types of cyber crimes targeting women, including online harassment, stalking, revenge porn, and identity theft. It highlights the prevalence and harmful consequences of these crimes on women's safety, privacy, and well-being.

Mismatch in outcomes: Despite the existence of cyber security laws, the outcomes in terms of prevention, deterrence, and protection for women remain inadequate. The research emphasizes the need for more comprehensive and gender-sensitive approaches in addressing cybercrimes targeting women.

Based on these findings, it is evident that there is a pressing need for policy reforms and enhancements in cyber security laws to better protect women from cyber crimes. The identified mismatch between objectives and outcomes calls for a comprehensive and inclusive approach to address the gendered dimensions of cyber security. This includes raising awareness, providing specialized training to law enforcement, establishing effective reporting mechanisms, and implementing stricter penalties for offenders. Ultimately, this literature review serves as a valuable resource for researchers, policymakers, and practitioners in understanding the landscape of cybercrimes targeting women and informing future initiatives to strengthen cyber security laws and ensure the protection of women in the digital age.

4. Results and discussions

The review paper on cybercrimes targeting women provides a comprehensive analysis of the results and discusses their implications in detail. The findings of the review reveal the prevalence and impact of cybercrimes on women, as well as the limitations and gaps in existing cybersecurity laws. The results highlight that cybercrimes targeting women are a significant issue in the digital landscape. The review identifies various forms of cybercrimes, such as online harassment, stalking, revenge porn, and identity theft, which dis-

pISSN: 1684-0615 / eISSN: 2616-2814 AJRS

proportionately affect women. These crimes not only violate their privacy and personal security but also have severe emotional, psychological, and social consequences. The review underscores the urgent need for effective measures to address these gender-based cybercrimes and protect women's rights in the online space.

Furthermore, the review critically evaluates the objectives and outcomes of current cyber security laws about gender-based cybercrimes. It identifies a mismatch between the objectives of these laws and the challenges faced by women in the digital realm. The analysis reveals that existing laws often fail to adequately address the specific vulnerabilities and risks faced by women, resulting in limited protection and justice for victims. This finding emphasizes the necessity for gender-sensitive approaches in the formulation and implementation of cyber security laws to ensure comprehensive protection for women.

The review also discusses the challenges faced by law enforcement agencies in investigating and prosecuting cybercrimes against women. These challenges include the complex nature of cybercrimes, limited resources and training, and difficulties in jurisdiction and cross-border cooperation. The review emphasizes the importance of addressing these challenges through capacity building, improved coordination among law enforcement agencies, and international collaboration to effectively combat gender-based cybercrimes. In the discussion section, the review paper expands on the implications of the findings. It underscores the need for policy reforms and enhancements in cyber security laws to align them with the evolving nature of cybercrimes and the specific vulnerabilities faced by women. The discussion highlights the importance of raising awareness about cybercrimes, providing specialized training to law enforcement officers, establishing efficient reporting mechanisms, and implementing stricter penalties for offenders. Additionally, the review offers practical recommendations for policymakers, lawmakers, and law enforcement agencies to enhance the protection of women against cybercrimes.

5. Recommendations for strengthening cyber security laws and protection of women

Based on the findings and discussions in the review paper on cybercrimes targeting women, the following recommendations can be made for strengthening cyber security laws and enhancing the protection of women:

Gender-sensitive legislation: Develop and enforce cyber security laws that explicitly address gender-based cybercrimes and provide comprehensive protection for women. These laws should recognize the specific vulnerabilities and risks faced by women and ensure that adequate measures are in place to prevent, investigate, and prosecute such crimes.

Awareness and education: Promote awareness campaigns and educational programs to inform women about the risks and preventive measures related to cybercrimes. This includes educating women on safe online practices, privacy settings, and reporting mechanisms. Similarly, awareness programs should target society as a whole to foster a culture of respect and digital responsibility.

Strengthen law enforcement capabilities: Provide specialized training to law enforcement agencies on investigating and responding to gender-based cybercrimes. This includes understanding the technical aspects of cybercrimes, digital evidence collection, and victim support. Adequate resources and personnel should be allocated to effectively handle these cases.

pISSN: 1684-0615 / eISSN: 2616-2814 AJRS

Collaboration and international cooperation: Enhance cooperation among law enforcement agencies, both domestically and internationally, to address cross-border cybercrimes targeting women. Establish information-sharing mechanisms, bilateral agreements, and collaboration platforms to facilitate effective investigation and prosecution of offenders.

Victim support and rehabilitation: Establish support services for victims of gender-based cybercrimes, including counseling, legal aid, and rehabilitation programs. Ensure that victims have access to necessary resources and support to cope with the emotional and psychological impact of these crimes.

Stricter penalties: Review and strengthen penalties for perpetrators of gender-based cybercrimes to serve as a deterrent and ensure accountability. This may include imposing stricter sentences, fines, and restraining orders to protect victims.

Technology and platform accountability: Hold technology companies and online platforms accountable for addressing cybercrimes targeting women on their platforms. Encourage the development and implementation of user-friendly tools, policies, and reporting mechanisms to enable swift response and removal of offensive content.

Research and data collection: Promote research initiatives to further understand the nature and prevalence of gender-based cybercrimes, as well as their impact on women. Collect comprehensive data on these crimes to inform evidence-based policy-making and facilitate targeted interventions.

By implementing these recommendations, it is possible to strengthen cyber security laws, enhance the protection of women, and create a safer digital environment for all individuals.

6. Conclusion and Future Directions

The literature review on cybercrimes targeting women within the context of cyber security laws highlights the urgent need for comprehensive measures to address the vulnerabilities and risks faced by women in the digital realm. The findings of this research underscore the evolving nature of cybercrimes against women, including online harassment, cyberstalking, non-consensual pornography, and online identity theft, among others. Existing cyber security laws need to be strengthened and adapted to effectively address these crimes. The review paper recommends a multi-faceted approach to enhance the protection of women against cybercrimes. This includes gender-sensitive legislation that explicitly addresses gender-based cybercrimes and ensures comprehensive protection for women. It also emphasizes the importance of awareness campaigns and educational programs to inform women about the risks and preventive measures associated with cybercrimes. Furthermore, the review highlights the significance of strengthening law enforcement capabilities in investigating and responding to gender-based cybercrimes. This involves specialized training for law enforcement agencies, collaboration and international cooperation, and the establishment of victim support services and rehabilitation programs. In terms of future directions, there is a need for ongoing research to further understand the nature and prevalence of cybercrimes targeting women, as well as their impact on victims. This research can inform evidence-based policy-making and facilitate targeted interventions.

pISSN: 1684-0615 / eISSN: 2616-2814 AJRS

English References

Aboul-Enein, S., 2017. Cybersecurity challenges in the Middle East. GCSP, 17, 5-49.

Ahmed, N., 2019. Cyberstalking: a content analysis of gender-based offenses committed online (Doctoral dissertation).

Airehrour, D., Vasudevan Nair, N. and Madanian, S., 2018. Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model. Information, 9(5), 110.

Al Shamsi, A.A., 2019. Effectiveness of cyber security awareness program for young children: A case study in UAE. Int. J. Inf. Technol. Lang. Stud, 3(2), 8-29.

Anderson, K.B., 2006. Who are the victims of identity theft? The effect of demographics. Journal of Public Policy & Marketing, 25(2), 160-171.

Aransiola, J.O. and Asindemade, S.O., 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychology, Behavior, and Social Networking, 14(12), 759-763.

Azad, M.M., Mazid, K.N. and Sharmin, S.S., 2017. Cyber crime problem areas, legal areas, and cybercrime law. International Journal of New Technology and Research, 3(5), 1-6.

Bentototahewa, V., 2021. A Framework for Acceptance and Implementation of Global Data Privacy and Security Policies by States (A Case Study of Sri Lanka and United Kingdom) [Doctoral dissertation, Cardiff Metropolitan University].

Bhat, R.M. and Ahmad, P.A., 2022. Social Media and the Cyber Crimes Against Women Study. Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN 2815-0953, 2(01), 18-22.

Blazek, R., 2016. THE NEW FORMS OF DIGITAL CRIMINALITY IN SLOVAKIA AND FIGHT AGAINST THEM. U KAZNENOM PRAVU I PRAVOSUĐU Digitalization in Penal Law and Judiciary, p.17.

Boukemidja, N.B., 2018. Cyber Crimes against Women: Qualification and Means. European Journal of Social Sciences, 1(3), pp.34-44.

Chawki, M., Darwish, A., Khan, M.A. and Tyagi, S., 2015. Cybercrime, digital forensics and jurisdiction (Vol. 593). Springer.

CHIKUMBI, L., 2022. A CRITICAL ANALYSIS ON CYBER LAWS AND CYBER CRIMES IN ZAMBIA; A CASE OF CYBER SECURITY AND CYBER CRIMES ACT NO. 2 OF 2021[Doctoral dissertation, Cavendish University].

Clevenger, S.L., Navarro, J.N. and Gilliam, M., 2018. Technology and the endless "cat and mouse" game: A review of the interpersonal cyber victimization literature. Sociology Compass, 12(12), 12639.

Copes, H., Kerley, K.R., Huff, R. and Kane, J., 2010. Differentiating identity theft: An exploratory study of victims using a national victimization survey. Journal of Criminal Justice, 38(5), 1045-1052.

Cross, C., Smith, R.G. and Richards, K., 2014. Challenges of responding to online fraud victimization in Australia. Trends and issues in crime and criminal justice, (474), 1-6.

Datta, P., Panda, S.N., Tanwar, S. and Kaushal, R.K., 2020, March. A technical review report on cyber crimes in India. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 269-275). IEEE.

Dokku, S.R. and Kandula, D., 2021. A study on issues and challenges of Information Technology Act 2000 in India. Annals of Justice and Humanity, 1(1), pp.39-49.

Graham, N., 2018. Cyber crimes against women in India.

Guedes, I., Martins, M. and Cardoso, C.S., 2022. Exploring the determinants of victimization and fear of online identity theft: An empirical study. Security Journal, 1-26.

Gupta, B., Agrawal, D.P. and Yamaguchi, S. eds., 2016. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global.

Gupta, B.B., Arachchilage, N.A. and Psannis, K.E., 2018. Defending against phishing attacks: taxonomy of methods, current issues, and future directions. Telecommunication Systems, 67, 247-267.

Halder, D. and Jaishankar, K., 2016. Celebrities and cyber crimes: An analysis of the victimization of female film stars on the Internet. Available at SSRN 3049543.

Halder, D. and Jaishankar, K., 2016. Cyber crimes against women in India. SAGE Publications India.

Harkin, D., Whelan, C. and Chang, L., 2018. The challenges facing specialist police cyber-crime units: An empirical analysis. Police Practice and Research, 19(6), 519-536.

Holt, T.J. and Bossler, A.M., 2008. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant behavior, 30(1), 1-25.

Jose, T., Vijayalakshmi, Y. and Babu, S.S., 2017. Cyber-crimes in Kerala: A study. Advances in Computational Sciences and Technology, 10(5), 1153-9.

Kabi, A., Marisport, A., Gori, S. and Tomar, A.S., 2022. The Facets Of Cyber Crimes Against Women In India: Issues And Challenges. Journal of Positive School Psychology, 6(8), 10220-10248.

Kabir, N., 2018. Cyber Crime a New Form of Violence Against Women: From the Case Study of Bangladesh. Available at SSRN 3153467.

Kashif, M., Javed, M.K. and Pandey, D., 2020. A surge in cyber-crime during COVID-19. Indonesian Journal of Social and Environmental Issues (IJSEI), 1(2), 48-52.

Kaushik, N., 2014. Cyber Crimes against women. Global Journal of Research in Management, 4(1), 37.

Kavanagh, M.J. and Johnson, R.D. eds., 2017. Human resource information systems: Basics, applications, and future directions. Sage Publications.

Lau, J.L. and Dunn, M.K., 2018. Therapeutic peptides: Historical perspectives, current development trends, and future directions. Bioorganic & medicinal chemistry, 26(10), 2700-2707.

Lazarus, S., 2019. Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework. International Social Science Journal, 69(231),15-33.

Lazarus, S., Button, M. and Kapend, R., 2022. Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. The Howard Journal of Crime and Justice, 61(3), 381-398.

Le, D.N., Kumar, R., Mishra, B.K., Chatterjee, J.M. and Khari, M. eds., 2019. Cyber security in parallel and distributed computing: Concepts, techniques, applications, and case studies. John Wiley & Sons.

Levi, M., 2017. Assessing the trends, scale, and nature of economic cybercrimes: overview and Issues: In Cybercrimes, cybercriminals, and their policing, in crime, law and social change. Crime, law, and social change, 67, 3-20.

Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M.L., 2016. The implications of economic cybercrime for policing.

Malar, M.N., 2012. Impact of cyber crimes on social networking pattern of girls. international Journal of Internet of Things, 1(1), 9-15.

Munyolo, G.N.O., 2021. Cyber-security in E-health: a Critical Analysis of the Regulatory Framework in Kenya [Doctoral dissertation, University of Nairobi].

Neira, R.E., 2016. Identity theft: Inside the mind of a cybercriminal [Doctoral dissertation, Utica College].

Ng, M.H.M., Wong, C.W.E., Shen, K.W., Lam, K.T.S. and Cheung, C.L.T., 2018. Online dating scams in Hong Kong: an analysis of the victimization process of female users. HKU Theses Online (HKUTO).

Okano-Heijmans, M. and Vosse, W., 2021. Promoting open and inclusive connectivity: The case for digital development cooperation. Research in Globalization, 3, p.100061.

Pastrana, S., Thomas, D.R., Hutchings, A. and Clayton, R., 2018, April. Crimebb: Enabling cybercrime research on underground forums at scale. In Proceed-

ings of the 2018 World Wide Web Conference (pp. 1845-1854).

Paul, J.A. and Wang, X.J., 2019. Socially optimal IT investment for cybersecurity. Decision Support Systems, 122, p.113069.

Pawlak, P. and Barmpaliou, P.N., 2017. Politics of cybersecurity capacity building: conundrum and opportunity. Journal of Cyber Policy, 2(1), 123-144.

Reina, L.A.V., 2022. Review of the Book" Cyberbullying". Analysis of the Victimization of Minors in Cyberspace from the Theory of Everyday Activities.

Reyns, B.W., 2013. Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2), 216-238.

Sebastian, A.M. and Sandeep, M.N., 2021. Privacy and data protection in cyberspace–a critical analysis of data protection laws in India.

Singh, J., 2015. Violence against women in the cyber world: a special reference to India. International Journal of Advanced Research in Management and Social Sciences, 4(1), 60-76.

Sridevi, J., Mariyappan, M.S.R. and Vel, E.K., 2023, June. Safety and Legal Measures to Protect Women from Cyber Crimes. In Recent Trends in Computational Intelligence and Its Application: Proceedings of the 1st International Conference on Recent Trends in Information Technology and its Application (ICRTITA, 22) (p. 298). CRC Press.

Swiątkowska, J., 2020. Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series, (33).

Teraa, M., Conte, M.S., Moll, F.L. and Verhaar, M.C., 2016. Critical limb ischemia: current trends and future directions. Journal of the American Heart Association, 5(2), p.e002938.

Tharshini, N.K., Hassan, Z. and Mas'ud, F.H., 2021. Cybercrime Threat Landscape amid the Movement Control Order in Malaysia. International Journal of Business and Society, 22(3), 1589-1601.

Uma, S., 2017. Outlawing cyber crimes against women in India. Bharati Law Review, 5(4), 103-116.

Van Puyvelde, D. and Brantly, A.F., 2019. Cybersecurity: politics, governance, and conflict in cyberspace. John Wiley & Sons.

Welch, S.A., 2016. Human trafficking and terrorism: Utilizing national security resources to prevent human trafficking in the Islamic state. Duke J. Gender L. & Pol'y, 24, p.165.

Wissink, I.B., Standaert, J.C., Stams, G.J.J., Asscher, J.J. and Assink, M., 2023. Risk factors for juvenile cybercrime: A meta-analytic review. Aggression and Violent Behavior, p.101836.

Younies, H. and 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.

Zhou, I., 2020. Digital labor platforms and labor protection in China (No. 11). ILO Working Paper.

Declaration of conflict of interest: The researcher (or researchers) declare(s) and undertakes that there is no conflict of interest with any person or institution. This research has not been previously published in any way, whether written, read, published, visual or audio.

Funding statement: This research is funded by (mention details of the institution's name, decisionnumber), or this research did not receive any financial support.

Biography of researchers

Mustafa Al- Atiyat

PhD Commercial Law University of Cairo, Associate Professor Al-Ahliyya Amman University Present Teaching Commercial Law courses at the Faculty of Law.

Email: m.atiyat@ammanu.edu.jo
ORCID: https://orcid.org/0000-0001-6200-8735

ANAS R. ALSOUD

Professor of informatics (electronic business and commerce). Since joining AL-Ahliyya Amman University, in 2012, he has been involved with studies related to e-business, e-government, and cloud computing in developing countries

Email: a.alsoud@ammanu.edu.jo
ORCID: https://orcid.org/0000-0002-1410-8843

Khalid Al Dweri

Associate Professor of Civil Law.

Email: dr.aldwerikhalid@gmail.com