Al-Basirah Volume 15, No 1, pp. 35-57, June 2025
https://doi.org/10.22452/basirah.vol15no1.4

الآليات الشرعيّة والتربويّة لمواجهة الجرائم السيبرانيّة: دور الأسرة والمدرسة

Sharia-Based and Educational Mechanisms for Combating Cybercrime: The Role of Family and School

Khalil Al Fazari[1]
Mohamad Azrien Mohamed Adnan[2]
Tengku Sarina Aini Tengku Kasim[3]

ملخص

يتناول هذا البحث الجرائم السيبرانية في ضوء مقاصد الشريعة، مبرزاً قدرة الأحكام الإسلامية على رفد التشريعات الوضعية في الدول العربية بأُطر أخلاقية مرنة تضبط السلوك الرقمي وتحفظ الضروريات. اعتمدت الدراسة المنهج الوصفي-التحليلي لوصف الوسائل الشرعية والقوانين ذات الصلة، ثم تحليلها لاستنباط ضوابط وقائية تجمع بين البعد الديني والتقني والتربوي. أظهر التحليل مقاصد الشريعة تضمن مواجهة الجرائم السيبرانية وأنّ تكييف الاعتداءات الرقمية في باب التعزير يتيح سلطة تقديرية كافية لردعها، وأن ترسيخ ثقافة الرقابة الإيجابية داخل الأسرة، ودمج قيم الأمانة والخصوصية في المناهج، يقلّلان من الانحرافات الإلكترونية بين الناشئة. كما برزت ضرورة الشراكة المؤسسية بين الهيئات الشرعية وجهات التعليم والاتصالات لسدّ الفجوة التشريعية ومواكبة تطوّر التقنيات. يخلص البحث إلى توصية بإصدار دليل شرعي-تقني موحّد، وتطوير برامج تدريب للأسر والمعلمين، وإنشاء منصّة معرفية مفتوحة ومراكز استجابة وطنية تجمع الخبرة الفقهية والتقنية لبناء بيئة رقمية آمنة متسقة مع قيم الشريعة.

الكلمات المفتاحية: *سبل مواجهة، الجرائم السيبرانية، أحكام الشريعة، دور الأسرة، دور المدرسة.*

ABSTRACT

This study examines cybercrime through the lens of Islamic objectives of the law (maqāṣid al-sharīʿa), highlighting the capacity of Islamic rulings to complement positive legislation with flexible ethical frameworks that govern digital behaviour and safeguard essential societal interests. Adopting a descriptive–analytical methodology, the research first catalogues relevant sharīʿa-based measures and statutory regulations, then analyses them to derive preventive guidelines that integrate religious, technical, and educational dimensions. The findings demonstrate that the maqāṣid framework can effectively address cyber-threats; classifying digital offences under taʿzīr (discretionary punishments) grants judges sufficient latitude to deter misconduct. Moreover, fostering a culture of positive parental oversight and embedding values of trustworthiness and privacy within school curricula reduce cyber-deviance among youth. The study also underscores the need for institutional cooperation among Islamic authorities, educational bodies, and telecommunications regulators to close legislative gaps and keep pace with technological developments. It recommends issuing a unified sharīʿa-technical guide, developing training programmes for parents and educators, and establishing an open-access knowledge platform and national response centres that combine Islamic jurisprudential and technical expertise to build a secure digital

[1] PhD Candidate at the Department of Islamic History, Civilization and Education, Academy of Islamic Studies, Universiti Malaya, 50603 Kuala Lumpur, Malaysia. E-mail: k.s.alfazari@gmail.com.

[2] Correcponding Author and Language Lecturer at the Department of Islamic History, Civilization and Education, Academy of Islamic Studies, Universiti Malaya, 50603 Kuala Lumpur, Malaysia. E-mail: mdazrien@um.edu.my

[3] Associate Professor at the Department of Islamic History, Civilization and Education, Academy of Islamic Studies, Universiti Malaya, 50603 Kuala Lumpur, Malaysia. E-mail: tgsarina@um.edu.my

environment consistent with Islamic values.
***Keywords**: strategies for countering, cybercrime, Islamic legal rulings, family role, school role*

مقدمة

تشهد البنية الرقمية العالميّة تحوّلاً متسارعاً جعل التعامل مع الفضاء السيبراني ضرورة يوميّة، غير أنّ هذا الانتشار أفرز طيفاً واسعاً من الجرائم الإلكترونيّة التي تهدّد أمن الأفراد والمجتمعات والدول. وتُثارُ هنا مسألةُ مدى قدرة المنظور الإسلامي، بقيمه التشريعيّة والأخلاقيّة، على رفد الجهود القانونيّة والتقنيّة المعاصرة بأُطرٍ تضبط السلوك في العالم الرقمي وتحفظ الضروريّات الخمس التي جاءت الشريعة بحمايتها. وإزاء هذه التحدّيات، تتعاظم الحاجة إلى دراسة علميّة تُعيد قراءة مفاهيم الحسبة، التكييف الفقهي، الأمر بالمعروف والنهي عن المنكر وغيرها في سياق الجريمة السيبرانيّة؛ وتربطها بدور المؤسَّسات التربويّة والأسريّة وبالآليات الإجرائيّة الحديثة.

تكمن إشكاليّة الدراسة في قصور التكامل بين المقاربات الفقهيّة والتربويّة والتقنيّة عند تناول الجرائم السيبرانيّة، الأمر الذي أفضى إلى فجوةٍ تشريعيّة وسلوكيّة يستغلّها المجرمون لإساءة استخدام التقنية. تتجلّى خطورة هذه الفجوة في مؤشّرين رئيسين: أوّلُهما حجم الخسائر المتنامي عالميًّا؛ إذ تُقدَّر تكلفة الجرائم السيبرانيّة بأن تبلغ 10.5 تريليون دولار سنويًّا بحلول عام 2025[4]. وثانيهما التزايد النوعي للهجمات في العالم العربي؛ حيث بلغ متوسّط كلفة الحادث الواحد على المؤسسات في الشرق الأوسط 8.75 ملايين دولار، وهو ضِعف المتوسّط العالمي تقريبًا، مع تضاعُف عدد الهجمات الناجحة ثلاث مرّات بين 2023 و 2024 في ظلّ الصراعات الجيو–سياسيّة بالمنطقة[5].

وعلى الصعيد العملي، أدّى هجوم الفدية على وزارة الماليّة الكويتيّة (ديسمبر 2024) إلى شَلّ أنظمة الرواتب الحكوميّة وإيقافها مؤقّتًا[6]، فيما تعرّضت منصّة PowerSchool التعليميّة –التي تخدم أكثر من 60 مليون طالب حول العالم– لخرقٍ بياناتٍ أعقبه ابتزاز عدّة مناطق تعليميّة في مايو 2025[7]. وفي القطاع التربوي تحديدًا سجّلت هجمات الفدية على مدارس التعليم الأساس زيادة بنسبة 92٪ خلال عام 2023[8]. بينما قفز عدد رسائل التصيّد الاحتيالي بالبريد الإلكتروني في الشرق الأوسط بنسبة

---

4 Morgan, Steve. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Cybercrime Magazine, February 21, 2024. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

5 Positive Technologies. Cybersecurity Threatscape in the Middle East: 2023–2024. Moscow: Positive Technologies, 2024. https://global.ptsecurity.com/analytics/cybersecurity-threatscape-in-the-middle-east-2023-2024.

6 Ibid.

7 Vicens, A. J. "US School Districts Facing Extortion Attempt after Hack, Software Provider Says." Reuters, May 7, 2025. https://www.reuters.com/world/us/us-school-districts-facing-extortion-attempt-after-hack-software-provider-says-2025-05-07/.

8 Cozens, Bill. "2024 State of Ransomware in Education: 92 % Spike in K-12 Attacks." ThreatDown (Malwarebytes Blog), January 24, 2024. https://www.threatdown.com/blog/2024-state-of-ransomware-in-education-92-spike-in-k-12-attacks/.

222٪، واعتمد 54٪ من الهجمات على أساليب الهندسة الاجتماعيّة، مستهدِفةً في كثيرٍ من الأحيان القُصَّر لاستدرار بيانات بطاقات آبائهم الائتمانيّة[9].

ويُظهر هذا الواقع غيابَ نموذجٍ إجرائيّ موحَّد يوظِّف أحكام الشريعة ومقاصدها، ويربطها باستراتيجيّات الأسرة والمدرسة، ويترجمها إلى إجراءات قانونيّة وتقنيّة قادرة على الحدّ من هذه الخروقات. ومن ثمّ، تسعى الدراسة إلى سدّ هذه الفجوة ببناء إطارٍ تكامليّ يجمع بين الرؤية المقاصديّة، والضبط التربوي، والحماية التقنيّة والتشريعيّة.

تنبعُ أهمية البحث من كونه يُقدِّم معالجةً أصيلةً ومتكاملةً لجريمةٍ عابرةٍ للحدود تُضعِف فاعليّة التشريعات الوضعيّة وحدها، في حين يملك التراث المقاصدي الإسلامي قدرةً عاليةً على التكيّف مع المستجدّات. كما يُلقي البحث الضوء على الدور الوقائي للأسرة والمدرسة، وهو جانب قلَّ أن لقي عنايةً كافية في أدبيّات الأمن السيبراني المعاصرة، رغم كونه خطَّ الدفاع الأوّل ضد الانحرافات الإلكترونيّة، ولا سيّما لدى الناشئة.

يهدف البحث إلى: (1) استنباط سبل مواجهة الجرائم السيبرانيّة من منظورٍ إسلامي يُفعِّل مقاصد الشريعة وقواعدها العامّة، (2) بيان كيفيّة تفعيل دور الأسرة والمدرسة في الوقاية من هذه الجرائم واستئصال جذورها السلوكيّة، و(3) اقتراح آليّاتٍ إجرائيّة قابلة للتطبيق تُسهم في بناء بيئةٍ رقميّة آمنة منضبطة بالقيم الإسلاميّة. وتُوزَّع هذه الأهداف على ثلاثة محاور رئيسة هي: السبل الشرعيّة، الأدوار التربويّة، والآليّات الإجرائيّة المقترحة.

تعتمد هذه الدراسة المنهج الوصفي–التحليلي؛ إذ تقوم بوصف الوسائل الشريعة ذات الصلة بجرائم الفضاء السيبراني، وما يقابلها من تشريعات وتقارير دوليّة، ثمّ تحليلها لاستنباط الأُطر القيميّة والضوابط الشرعيّة القادرة على مواجهة تلك الجرائم، وصولاً إلى صياغة توصيات إجرائيّة تُسهِم في تعزيز الأمن السيبراني وفق رؤية إسلاميّة متكاملة.

المحور الأول: سبل مواجهة الجرائم السيبرانية من منظور إسلامي

في المفهوم الإسلامي، تُعرف الجريمة بأنها الأفعال التي حظرها الشرع وقررها الله، سواء كانت في شكل عقوبات ذات أحكام واضحة (حد) أو عقوبات لم يحددها الله بشكل واضح (تعزير). فالجريمة هي مخالفة للشرع مهددة بعقوبات الحد والتعزير التي يحددها الله. وقانون الحد هو العقوبة التي تم تحديدها في نصوص القرآن أو السنة النبوية. أما قانون التعزير فهو العقوبة التي لم يتم تحديد أحكامها في القرآن والسنة، ويصبح التعزير من اختصاص السلطات لتحديده[10].

---

9 Positive Technologies. Cybersecurity Threatscape in the Middle East: 2023–2024. Moscow: Positive Technologies, 2024. https://global.ptsecurity.com/analytics/cybersecurity-threatscape-in-the-middle-east-2023-2024.

10 Naro, W., Syatar, A., Amiruddin, M. M., Haq, I., Abubakar, A., and Risal, C. 2020. “Shariah

وتشـير الجرائم السـيبرانية إلى أي فعل ينطوي على اسـتخدام وسـيلة تقنية المعلومات، أو نظام معلوماتي، أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون[11].

وتتعدد الجرائم السـيبرانية لتشـمل وفقًا لقانون منع الجرائم الإلكترونية (PECA) لعام 2016 لتشمل الدخول غير المصرح به إلى نظام معلومات أو بيانات الآخرين، ونسخ أو نقل البيانات دون إذن، والإرهاب السـيبراني، وخطاب الكراهية، والتجنيد أو التمويل أو التخطيط للإرهاب، والتزوير الإلكتروني، والاحتيال الإلكتروني، وصـنع أو الحصـول على أو توفير أجهزة لاسـتخدامها في ارتكاب الجرائم، والعبث بمعدات الاتصـال أو تعديلها، والاعتراض غير المصـرح به للاتصـالات، ونشـر البرمجيات الخبيثة، والتتبع أو الملاحقة الإلكترونية، والرسائل غير المرغوب فيها، وانتحال الهوية[12].

والجريمة السـيبرانية باسـتخدام التكنولوجيا المتقدمة ليسـت نوعًا جديدًا من الجرائم التي تحتاج إلى نظرية إسلامية جديدة، بل إنها مغطاة بالفعل بالقوانين الإسلامية العامة. ويُعرف القانون الإسلامي باسم الشـريعة. وتعني الشـريعة "الطريق إلى اتباع قانون الله". حيث تهدف الشـريعة إلى توجيه الأفراد في معظم الأمور اليومية بشكل شامل، بالإضافة إلى التحكم في السلوك العام والخاص وتنظيمه ووضع قواعد له[13].

وعند النظر في مفهوم الجريمة من المنظور الإسلامي، يظهر بوضوح من أصول الشريعة وقواعدها وأدلتها التفصيلية أن الإسلام جاء ليحفظ الضروريات الخمس: الدين، والنفس، والنسل، والمال، والعقل، وأولى الإسـلام عناية بالغة بحمايتها. واعتبر الإسـلام أي اعتداء عليها جريمة تسـتوجب عقوبة ملائمة. وبضمان حماية هذه الضروريات، ينعم المجتمع بالتعايش السلمي، ويعيش أفراده في أمن وطمأنينة[14].

وتختلف الشـريعة الإسـلامية عن القانون الوضـعي بشـكل جوهري في نشـأتهما. فقد بدأ القانون الوضـعي في بداياته محدودًا وضـيقًا في قواعده، ثم تطور بتطور المجتمع الذي نشـأ فيه، حيث اعتمد على نظريات متنوعة ومتعددة حتى أصـبح بما هو عليه اليوم، ويظل مواكبًا لتطور حاجات المجتمع الذي صـاغه. أما الشـريعة الإسـلامية، فهي شـريعة إلهية من عند الله سـبحانه وتعالى، تتميز بالكمال والشـمول والقدرة على التكيف مع جميع الأزمنة والأمكنة.

ومن هنا، فقد تضـمنت الشـريعة الإسـلامية مبادئ عامة تضـمن لها القدرة على التكيف مع

Assessment toward the Prosecution of Cybercrime in Indonesia." International Journal of Criminology and Sociology 9: 572–86.

11 Al-Balushi, Khamis bin Abdullah Salim, Ahmad Yusuf, and Abdul Aziz Rakan. Al-Amn al-Sibirani min al-Manzur al-Islami. Majallat Kulliyat al-Shariʿa wa-al-Qanun bi-Asyut 36, no. 2 (2024): 1677–1729.

12 Bilal, H., and Khan, M. A. 2022. "Cyber Crime Legislation in Pakistan: A Critical Analysis from Islamic Law Perspective." *Al-Idah* 40 (2): 1–18.

13 Hasanah, U. 2018. "The Effectiveness of Islamic Law Implementation to Address Cyber Crime: Studies in Arab, Brunei Darussalam, and China." Al-Ahkam: Jurnal Ilmu Syari'ah dan Hukum 3 (2): 107–22.

14 Alyammahi, M., and Noor, S. 2024. "Cyber Crimes in the United Arab Emirates: A Study of Characteristics, Patterns, and Countermeasures from an Islamic Perspective." International Journal of Islamic Studies 33 (3): 514–38.

مختلف القضـايا في مختلف العصـور، وذلك بفضـل اتسـاعها ومرونتها التي تمكنها من مواجهة التحديات والتطورات الحديثة[15]. هذه المبادئ العامة يمكنها أن تنظم اســتخدام التكنولوجيا الرقمية ضــمن الحدود المشروعة، ومن أبرز هذه المبادئ ما يلي[16]:

1. **مبدأ الاستفادة والتحسين:** حيث يشـجع الإسـلام أتباعه على استثمار النعم التي أنعم الله بها لتحقيق الخير والتقدم. وتعد التكنولوجيا الرقمية أداة فعّالة لتيسير الحياة وتعزيز الرفاهية في مختلف المجالات، مثل الاتصــالات، والتعليم، والعمل، والرعاية الصــحية، مما يســهم في تحقيق التطور والإفادة الشاملة.
2. **مبدأ التيســير:** حيث يدعو الإســلام إلى تســهيل الأمور وتيســير شــؤون الحياة للناس. وتُمثل التكنولوجيا الرقمية وسيلة فعّالة لتحقيق هذا الهدف، حيث تسهم في تبسيط العمليات وتحسين الكفاءة في مختلف المجالات، مما يعود بالنفع على الأفراد والمجتمع ككل.
3. **مبدأ حفظ الخصــوصــية:** حيث يؤكد الإســلام على أهمية صــيانة خصــوصــيات الأفراد ومنع التجسس أو التعدي على أسرار الآخرين، ويعد ذلك من السلوكيات المحرمة التي تنافي الأخلاق الإســلامية. وفي ذلك يقول الله عز وجل (وَلَا تَجَسَّــسُــوا) [الحجرات: 12]، حيث جاء النهي صريحًا عن التجسس والتدخل في شؤون الآخرين. وعن النبي ﷺ قال (من ستر مسلمًا ستره الله في الدنيا والآخرة) [رواه مسلم]، مما يعزز أهمية حفظ أسرار الآخرين واحترام خصوصياتهم.
4. **مبدأ الامتثال للضــوابط الشــرعية والقانونية:** حيث يحث الإســلام على تعزيز النظام واحترام القوانين في المجتمع، ويعتبر وضــع القوانين واللوائح التنظيمية أمرًا مشــروعًا ومحمودًا، بشــرط ألا تتعارض مع الضوابط والمبادئ الإسلامية. كما يُعد الاجتهاد الفقهي في هذا السياق أداة مهمة لتحقيق المصلحة العامة وتنظيم شؤون الحياة بما يحقق العدل والاستقرار.

وهناك عدد من الأسـاليب والسـبل لمواجهة الجرائم السـيبرانية من المنظور الإسـلامي، والتي يمكن تناولها في النقاط الآتية:

أولًا: حفظ مقاصد الشريعة (القضاء على أسباب الجريمة):

لقد جاءت الشــريعة الإســلامية بأحكام شــاملة تهدف إلى صــون الضــروريات الخمس: الدين، النفس، العقل، النسـل، والمال، بما يحقق تأثيرًا إيجابيًا في تعزيز الأمن السيبراني والحد من الجرائم الإلكترونية. ويمكن توضيح ذلك كما يلي:

---

15 Al-Shuraim, Hamda Muhammad. Al-Jarayim al-Iliktruniyyah wa-Mawqif al-Shariʿa al-Islamiyyah Minha: al-Halat al-Dirasiyyah al-Qanun al-Qatari. Majallat al-Dirasat al-Islamiyyah wa-al-Fikr li-al-Buhuth al-Takhassusiyyah 5, no. 1 (2019): 101–122.

16 Alyammahi and Noor, "Cyber Crimes in the United Arab Emirates," 520.

1. **القضاء على أسباب الجريمة المتعلقة بحفظ الدين:** إن وسائل التواصل الاجتماعي، بما فيها القنوات الفضائية ومنصات مثل فيسبوك وتويتر وإنستغرام، أصبحت منبرًا مؤثرًا لنشر الأفكار والمعتقدات. وقد استغل مروجو الأفكار الهدامة سرعة انتشار هذه الوسائل وضعف الرقابة عليها لنشر سمومهم الفكرية. وحرصًا من الإسلام على حماية الدين، جاءت التشريعات للحد من الجرائم السيبرانية التي تستهدف عقيدة المسلمين، وذلك من خلال تنظيم المحتوى وتقنين السلوكيات الرقمية بما يحافظ على سلامة المعتقد[17].
2. **القضاء على أسباب الجريمة المتعلقة بحفظ النفس:** يحمي الإسلام حق الإنسان في الحياة والكرامة والأمان، ويسعى إلى صون الأفراد من الجرائم التي تهدد هذا الحق، مثل الاستغلال الجنسي في المواد الإباحية أو الاتجار بالبشر عبر الإنترنت. ويؤكد الإسلام ضرورة وضع أنظمة صارمة للتصدي لمثل هذه الجرائم الإلكترونية[18].

   ويشمل حفظ النفس تهذيبها والارتقاء بها، حيث يولي الإسلام عناية فائقة برعاية النفس الإنسانية وصقلها، ويسعى إلى رفع شأنها بالفضائل والابتعاد عن الفواحش. يتحقق ذلك من خلال تعزيز معاني الإيمان بالله واليوم الآخر، وتشجيع أداء العبادات، والتحلي بالقيم والأخلاق النبيلة[19].
3. **القضاء على أسباب الجريمة المتعلقة بحفظ العقل:** تعد مواقع التواصل الاجتماعي بيئة خصبة لبث الأفكار المنحرفة، مما يؤثر سلبًا على عقول الشباب. ومن هذا المنطلق، حرم الإسلام كل ما يفسد العقل أو يعطله، وشدد على أهمية التصدي للمحتوى الذي يروج للانحراف الفكري عبر التقنيات الحديثة[20].
4. **القضاء على أسباب الجريمة المتعلقة بحفظ النسل:** يحرص الإسلام على حماية النسل من خلال تحريم الفواحش، سواء الظاهرة منها أو الخفية، وعلى رأسها الزنا. وينعكس ذلك في محاربة الجرائم السيبرانية التي تهدد القيم الأخلاقية والاجتماعية[21].
5. **القضاء على أسباب الجريمة المتعلقة بحفظ المال:** تعد الحاجة المالية من أبرز دوافع الجرائم السيبرانية، حيث يلجأ بعض الأفراد إلى الاحتيال والاعتداء على أموال الآخرين. ومن هنا، حرم

---

17 Al-Zuʿbi, Ahmad Shahada Bashir. Manhaj al-Islam fi Muharabat al-Jarima. Al-Majalla al-ʿArabiyyah li-al-Dirasat al-Amniyyah 28, no. 56 (2012): 33–83.; Al-Zuʿbi, Ahmad Shahada Bashir. Manhaj al-Islam fi Muharabat al-Jarima. *Al-Majalla al-ʿArabiyyah li-al-Dirasat al-Amniyyah* 28, no. 56 (2012): 33–83.

18 al-Balushi, Yusuf, and Rakan, "Al-Amn al-Sibirani," 1700; Muhammad, "Al-Amn al-Sibirani fi Dawʾ," 460.

19 al-Zuʿbi, "Manhaj al-Islam," 50.

20 Muhammad, "Al-Amn al-Sibirani fi Dawʾ," 460.

21 Al-Balushi, Yusuf, and Rakan, "Al-Amn al-Sibirani," 1700; Muhammad, "Al-Amn al-Sibirani fi Dawʾ," 460.

الإسلام الاعتداء على الملكيات وأكد على قدسية حقوق الآخرين، داعيًا إلى وضع أنظمة لحماية الأصول المالية من التعدي الرقمي[22].

يتضح من النقاط السابقة أن الشريعة الإسلامية بمنظومتها الشاملة تولي أهمية كبرى لحفظ الضروريات الخمس، الأمر الذي يتماشى مع متطلبات العصر الحديث في مواجهة التحديات الرقمية. فالأحكام الشرعية المتعلقة بصون الدين، النفس، العقل، النسل، والمال تشكل إطارًا وقائيًا يعزز الأمن السيبراني ويحد من الجرائم الإلكترونية بمختلف أشكالها. ومن خلال التوجيه الإلهي والتشريعات الإسلامية، يتم تحقيق التوازن بين التقدم التكنولوجي والحفاظ على القيم الإنسانية، مما يسهم في بناء مجتمع رقمي آمن ومستدام. ولذا، يعد الالتزام بالمبادئ الإسلامية وإيجاد أنظمة صارمة مستمدة منها ضرورة لضمان سلامة الأفراد والمجتمعات في ظل التطور التقني المتسارع.

ثانيًا: الأمر بالمعروف والنهي عن المنكر

يهدف الأمر بالمعروف والنهي عن المنكر إلى تقديم النصح والإرشاد للأفراد الذين تورطوا في الجرائم السيبرانية، مع توفير فرص للتوبة والإصلاح. هذه الآلية تعمل على بناء الوعي الأخلاقي لدى الأفراد، فمن خلال الأمر بالمعروف، يتم غرس القيم الأخلاقية في الأفراد مثل الصدق، الأمانة، واحترام حقوق الآخرين، مما يجعلهم أقل ميلاً لارتكاب الجرائم السيبرانية. كما أنها آلية تهدف لتعزيز المراقبة الذاتية لدى الأفراد، حيث يشجع على مراقبة الله في السر والعلن، مما يدفع الأفراد لتجنب السلوكيات المحرمة حتى في العالم الرقمي[23].

وفي هذا السياق أشار Komaruddin et al إلى دور الإسلام في عدد من الجوانب التي توضح العلاقة بين الأمر بالمعروف والنهي عن المنكر الجرائم السيبرانية، وهي كالتالي[24]:

أ. **الخصوصية وحماية البيانات:** تؤكد النصوص الإسلامية على أهمية الخصوصية الشخصية وحماية المعلومات الحساسة. ويقدس الإسلام الفضاء الشخصي، ويحرم كشف أسرار الآخرين. ففي القرآن الكريم والحديث الشريف، هناك إشارات واضحة إلى حماية خصوصية الأفراد، بما في ذلك منازلهم وشؤونهم الشخصية، فيقول الله عز وجل ﴿يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ۚ ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ﴾ [النور: 27]. وتؤكد هذه الآية على أهمية الخصوصية والسرية، وهو ما يمكن تطبيقه في المجال الرقمي.

---

22 Al-Balushi, Yusuf, and Rakan, "Al-Amn al-Sibirani," 1700; Muhammad, "Al-Amn al-Sibirani fi Daw'," 460.; Muhammad, "Al-Amn al-Sibirani fi Daw'," 460.

23 Al-Sharkasi, Muhammad Mahmud. Al-Jarima al-Iliktruniyyah wa-Subul Mukafahatiha fi Daw' Ahkam al-Fiqh al-Islami: Dirasa Muqarana. Majallat al-Manara al-'Ilmiyyah 2 (n.d.): 179–197.

24 Komaruddin, K., Utama, A. S., Sudarmanto, E., and Sugiono, S. 2023. "Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications." West Science Law and Human Rights 1 (4): 166–72.

ب. **الصـــدق والنزاهة:** تؤكد الأخلاق الإســـلامية على قيمة الصـــدق والنزاهة والثقة. وتمتد هذه المبادئ لتشـــمل التفاعلات والمعاملات الرقمية التي تتمثل في التواصـــل عبر الإنترنت والالتزام الأخلاقي بحماية البيانات.

ج. **تحريم الضـرر:** يشـمل الفقه الإسـلامي مبدأ "تجنب الضـرر". ويتماشـى هذا المبدأ مع ممارسـات الأمن السيبراني المعاصرة التي تهدف إلى منع الضرر للأفراد والمنظمات. حيث ويمكن تطبيق مبدأ "تجنب الضرر" مباشرة على الأمن السيبراني. فهو يبرز المسؤولية الأخلاقية لحماية الأفراد والمجتمع من الأضرار التي قد تنجم عن التهديدات والانتهاكات السيبرانية.

ومما ســـبق يتجلى دور الأمر بالمعروف والنهي عن المنكر كركيزة أســـاســـية في معالجة الجرائم السـيبرانية من منظور إسـلامي. فمن خلال المبادئ الإسـلامية التي تركز على حماية الخصـوصـية، وتعزيز الصدق والنزاهة، وتجنب الإضرار بالآخرين، يمكن وضع إطار أخلاقي شامل يواكب التحديات الرقمية. هذا النهج لا يسـهم فقط في تقليل الجرائم السيبرانية، بل يعزز الثقة والأمان في الفضـاء الرقمي، مما يرسخ أسس مجتمع مستدام تسوده الأخلاق والعدالة، حتى في عالمنا الرقمي المتطور.

ثالثًا: التكييف الفقهي:

يتعلق التكييف الفقهي للجرائم الإلكترونية بتوصـيف هذه الجرائم وفق قواعد الفقه الإسـلامي وأصـوله، وإيجاد الأحكام الشـرعية المناسـبة لها بناءً على طبيعتها وتأثيراتها[25]. ويشـمل التكييف الفقهي للجرائم السيبرانية اتباع الخطوات التالي[26]:

1. **التعرف على الجريمة السيبرانية:** ويشمل ذلك تحديد ماهية الجريمة السيبرانية من حيث مفهومها وأركانها وطبيعتها التقنية. كما يشـمل دراسـة الأدوات المسـتخدمة فيها (مثل الاختراق، التزوير الإلكتروني، سرقة البيانات) وتحليل الأثر الناتج عنها (ضرر مالي، أخلاقي، اجتماعي). وكذلك يشمل الوقوف على تفاصيل الواقعة لمعرفة عناصرها الفعلية.
2. **التعرف على الأصـل الذي يتم تكييف الجريمة السـيبرانية عليه:** ويشـمل ذلك البحث عن الأصل الفقهي أو القاعدة الشرعية التي يمكن قياس الجريمة السيبرانية عليها، مثل قواعد السرقة، أو الغش، أو الإفساد في الأرض، أو الاعتداء على الأموال والنفوس. كما يتم هنا الاعتماد على النصوص الشرعية من القرآن والسنة، والإجماع، والقياس، والقواعد الفقهية العامة.

---

25 Ramli, Nurzakiyyah bint al-Hajj, and Adnan Mahmud Sharari al-Assaf. Al-Takyif al-Fiqhi li-al-Sariqa al-Iliktruniyyah: Dirasa Muqarana maʿ Qanun Brunei. Al-Majalla al-Urduniyyah fi al-Dirasat al-Islamiyyah 16, no. 3 (2020): 369–391.

26 Al-ʿAnazi, Sultan Sabil, Abd al-Karim ibn Ali, and Shahidra bint Abd al-Khalil. Al-Takyif al-Fiqhi li-Jarimat al-Ibtizaz al-Iliktruni wa-al-Taʾsil al-Fiqhi li-al-ʿUqubat al-Warida fi al-Anzima al-Khalijiyyah. *Majallat al-Islam fi Asia* 20, no. 2 (2023): 199–234.

3. **المطابقة بين الجريمة السيبرانية والأصل:** ويشمل ذلك مقارنة الجريمة السيبرانية بالأصل الفقهي المختار من حيث الأركان والآثار والنتائج. وإثبات التماثل بينهما أو استنباط حكم جديد إذا كان هناك اختلاف جوهري بين الجريمة الحديثة والأصل التقليدي. كما يتم مراعاة تغير الوسائل مع الحفاظ على ثبات المقاصد الشرعية.

ومما سبق يمكن القول بأن التكييف الفقهي للجرائم الإلكترونية يمثل خطوة رائدة في مواكبة مستجدات العصر الرقمي ضمن إطار الشريعة الإسلامية. فمن خلال تحديد ماهية الجريمة السيبرانية، وربطها بأصول فقهية وقواعد شرعية، يمكن إيجاد حلول شرعية مستدامة تتناسب مع طبيعة الجرائم التقنية الحديثة. هذا التكييف يبرز مرونة الشريعة الإسلامية وقدرتها على الاستجابة للتحديات المتغيرة مع الحفاظ على ثوابت المقاصد الشرعية، مثل حفظ الدين والنفس والعقل والنسل والمال. ومن خلال هذا النهج، يتم تعزيز العدالة وحماية الحقوق في الفضاء الرقمي، مما يسهم في بناء بيئة إلكترونية آمنة ومتوافقة مع القيم الإسلامية.

رابعًا: العقوبة

إن دور العقوبة في الحد من الجرائم السيبرانية في الإسلام يتمثل في كونها وسيلة رادعة وموجهة تهدف إلى حماية المجتمع من الأضرار الناتجة عن هذه الجرائم، وتحقيق العدل، وإصلاح الجاني، ومنع ارتكاب الجرائم مستقبلاً[27]. وفي ذلك أشار Sukardi et al إلى أنه يمكن المعاقبة على الجرائم السيبرانية وفقًا لتحليل الشريعة الإسلامية بعقوبة التعزير[28]. والتعزير يُقصد به العقوبة المفروضة بناءً على الاستبداد، لأنها صراحة لا تشمل الجرائم الواردة في القرآن والسنة مثل الحدود، القصاص، أو الكفارات.

وفي الغالب، لا تخرج العقوبات في الدول الإسلامية عن الأنواع الآتية:

1. **العقوبات المالية:** وهي إلزام الجاني بدفع مبلغ معين من المال مقابل الجريمة التي ارتكبها، أو مصادرة ما لديه أو إتلافه. ومن المعروف أن الشريعة قد فرضت عقوبات مالية على بعض الجرائم التعزيرية، مثل معاقبة من يسرق الثمر المعلق بغرامة تعادل ثمن المسروق مرتين فوق العقوبة المناسبة للجريمة. بناءً على ذلك، يمكن للقاضي أن يفرض على المجرم السيبراني عقوبة إتلاف الأجهزة المستخدمة في ارتكاب الجريمة أو مصادرتها، بالإضافة إلى فرض غرامة مالية.

---

27 al-Sharkasi, "Al-Jarima al-Iliktruniyyah," 185.

28 Sukardi, D., Nugraha, F. B., Ubaidillah, U., Fatakh, A., Leliya, L., and Arrizky, M. F. 2023. "Solving Cyber Crime in Online Buying and Selling in Cirebon City in Review of ITE Law and Islamic Law." Al-Mustashfa: Jurnal Penelitian Hukum Ekonomi Syariah 8 (2): 237–50.

2. **الحبس:** يُعتبر الحبس في الشريعة الإسلامية عقوبة تعزيرية، ويقوم الفقهاء بتقسيمه إلى نوعين: حبس محدد المدة وحبس غير محدد المدة. يُطبق الحبس المحدد المدة على الجرائم غير الخطيرة والمجرمين المبتدئين. أما الحبس غير المحدد المدة، فيُقرّ للجرائم الخطيرة والمجرمين معتادي الإجرام[29].

ويُستدل على مشروعية الحبس بما رواه أبو داود في سننه: "حدثنا إبراهيم بن موسى الرازي، أخبرنا عبد الرزاق عن معمر عن بهز بن حكيم عن أبيه عن جده: أن النبي صلى الله عليه وسلم حبس رجلاً بتهمة". وفي سياق الجرائم السيبرانية يؤدي الحبس إلى قطع المجرم عن كافة وسائل الاتصال والابتعاد عنها[30].

3. **عقوبة الإعدام:** حيث تُفرض عقوبة الإعدام إذا كان الفعل الإجرامي في جرائم التعزير لا يمكن تجاوزه إلا بعقوبة الإعدام. وتُطبق هذه العقوبة على الجواسيس والمجرمين الكبار أو المجرمين العائدين (المتكررين)[31].

والأصل في الشريعة الإسلامية أن التعزير كإجراء احترازي يُعتبر وسيلة للتأديب والإصلاح، ولا ينطوي على إيلام أو تعذيب جوهري كما في العقوبات الأخرى. ومع ذلك، سمح بعض الفقهاء باستثناء من القاعدة العامة، حيث يجوز فرض عقوبة القتل تعزيرًا إذا اقتضت المصلحة العامة ذلك، أو إذا كان فساد المجرم لا يمكن القضاء عليه إلا بقتله[32].

4. **الجلد بما لا يزيد عن عشر مرات:** وتُفرض هذه العقوبة على أولئك الذين يكررون ارتكاب جرائم مماثلة.

5. **التعويض بمصادرة الممتلكات:** وهو إجراء تأديبي يتم فيه الاستيلاء على أموال أو ممتلكات الشخص المدان كجزء من العقوبة[33].

ومن منطلق العقوبة، يحترم الإسلام معلومات وخصوصية الجميع ولا يسمح لأحد بالتجسس على معلومات أو مستندات الآخرين، أو الغش أو السيطرة على ممتلكات الآخرين بأي شكل. وفي هذا الصدد، فإن التعاليم والعقوبات الإسلامية صارمة وواضحة تجاه الشخص الذي يعتدي أو يسرق ممتلكات الآخرين مثل المعلومات، والأمان، والمستندات، والخصوصية. وفي ذلك قال الله تعالى ﴿مَن يَعْمَلْ سُوءًا يُجْزَ بِهِ وَلَا يَجِدْ لَهُ مِن دُونِ اللَّهِ وَلِيًّا وَلَا نَصِيرًا﴾ [سورة النساء: 123]. هذه الآية تبرز عدالة الله سبحانه وتعالى، حيث يُجازى كل من يرتكب خطأ أو ظلم على فعله. وتتماشى هذه الآية مع مبادئ

---

29 Bin Turki, Layla. Al-Jazaʾ al-Jinaʾi fi al-Tashriʿ al-Islami. Majallat al-ʿUlum al-Insaniyah 50 (2018): 47–67.

30 Alanazi, S. S., Ali, A. K., and Khalil, S. A. 2023. "Fiqh Adaptation (al-Takyif al-Fiqhi) of the Crime of Extortion through Electronic Means and Its Penalties in Islamic Law." Jurnal Fiqh 20 (1): 141–64.

31 Naro et al., "Shariah Assessment toward the Prosecution," 575.

32 Bin Turki, "Al-Jazaʾ al-Jinaʾi," 55.

33 Naro et al., "Shariah Assessment toward the Prosecution," 575.

الإسلام التي تدعو إلى العدالة والمحاسبة على الأفعال، بما في ذلك الجرائم الإلكترونية التي يمكن أن تضر بالآخرين، مثل السرقة والاحتيال على الإنترنت.

خامسًا: التبيُّن:

يحث الإسلام على أنه يجب على المسلم قبل تصديق أي معلومات يتم الحصول عليها، أن يظل يقظًا وحذرًا من خلال إجراء التبين، وهو يعني ضرورة التحقق والتأكد من الأخبار والمعلومات قبل قبولها كحقائق. وهذا من منطلق أن معظم الأنشطة المتعلقة بالجرائم الإلكترونية مثل الاحتيال وسرقة الهوية تُنشئ أسماء نطاقات مزيفة، خاصة عند تقديم ميزات مثل الاختبارات والهدايا. ويقوم الجناة بإثارة الأسئلة وإعطاء الأمل للضحايا، مما يجعلهم عاطفيًا لا يدركون أنهم الهدف. سيقوم مبدأ التبين هنا بدور كبير في تذكير المستخدم بأهمية إجراء التحقيق المبكر، ومنح فترة زمنية للتفكير قبل اتخاذ أي قرار[34].

سادسًا: الإخبار والإعلام:

ويشير الإخبار والإعلام إلى تعريف المجرم بجريمته وإخباره بما صنعه، ومن ثم تحذيره. ويكون الإخبار والإعلام في الجرائم البسيطة التي لا تشكل ضررًا كبيرًا ولا تستدعي التدخل القضائي، ورغم ذلك يُتخذ هذا الإجراء لحفظ حقوق الناس، حتى وإن كان الاعتداء في بعض الأحيان بسيطًا أو تافهًا. والهدف من ذلك هو تأديب المذنب وزجره عن تكرار الذنب، ومنعه من الاستمرار في إلحاق الأذى بالآخرين[35].

سابعًا: الصبر والتحكم بالنفس:

يُعد التروي والتفكير بتمعن في جميع المعلومات التي يقرأها المستخدم قبل التصرف أمرًا مهمًا جدًا. هذه القيمة الإسلامية تلعب دورًا رئيسيًا في مكافحة الجرائم الإلكترونية، التي تُرتكب عادة من قبل المخترقين نتيجة إهمال المستخدمين. وفي هذا السياق يحث الإسلام الناس على الصبر وضبط النفس عن التسرع، فيصبح التصرف بصبر وعدم التسرع في الرد على المعلومات في وسائل التواصل الاجتماعي أحد المفاتيح لتجنب محاولات الاحتيال عبر هذه الوسائل. حيث يستغل المجرمون سلوك التسرع وعدم التحكم في النفس كوسيلة للبحث عن الضحايا. على سبيل المثال، تُستخدم عروض الهدايا المجانية كوسيلة لإجبار المستخدمين على التفاعل الفوري وزيارة الموقع. والمستخدمون الذين يفتقرون إلى الصبر لتحليل محتوى المعلومات يصبحون بسرعة ضحايا للاحتيال أو سرقة الهوية[36].

ثامنًا: حفظ الأسرار:

---

34 Santoso, E. 2018. "The Role of Islamic Values to Prevent the Society for Cyber Crime Victim in Social Media." Paper presented at the International Conference on Media and Communication Studies (ICOMACS 2018), October, 293–97. Atlantis Press.

35 Bin Turki, "Al-Jazaʾ al-Jinaʾi," 55.

36 Santoso, "Role of Islamic Values," 294.

إن الجرائم السيبرانية تعتمد بشكل كبير على سلوك المستخدم. فالهوية الشخصية والبيانات المالية هي أمور يجب الحفاظ عليها بسرية تامة. في هذا السياق، وبغض النظر عن القوانين التي تضعها الحكومات أو أنظمة الأمان التي يصممها مقدمو الخدمات، فإن تحقيق الأمان يكون صعبًا دون مشاركة فعالة من المستخدم نفسه. والحفاظ على المعلومات المهمة باستمرار هو المفتاح لتجنب الوقوع ضحية للجرائم في الفضاء الإلكتروني[37].

يتضح أن سلوك المستخدم يمثل حجر الزاوية في مواجهة الجرائم السيبرانية، حيث إن الأمان الرقمي لا يمكن تحقيقه بصورة شاملة دون وعي المستخدمين بدورهم ومسؤوليتهم. ويتطلب الحفاظ على السرية الشخصية والبيانات الحساسة، مثل الهوية والبيانات المالية، مشاركة فعالة من الأفراد، تتجلى في اتخاذ التدابير الوقائية، مثل استخدام كلمات مرور قوية، وتجنب مشاركة المعلومات الشخصية في منصات غير آمنة. لذلك، إلى جانب القوانين والأنظمة الأمنية، يجب التركيز على نشر الوعي وتعزيز ثقافة الأمن السيبراني لدى المستخدمين، مما يسهم في تقليل الثغرات التي قد تُستغل من قبل المجرمين السيبرانيين.

المحور الثاني: تفعيل دور الأسرة والمدرسة في مواجهة الجرائم السيبرانية

أولا: تفعيل دور الأسرة

تلعب الأسرة دورًا حاسمًا في التصدي للجرائم السيبرانية، حيث تعد اللبنة الأولى في بناء شخصية الأبناء وتوجيههم نحو السلوكيات السليمة، مما يساهم في حمايتهم من المخاطر الرقمية. وفيما يلي أبرز أدوار الأسرة في مواجهة الجرائم السيبرانية[38]:.

- التربية على القيم والأخلاق: حيث تُعد التربية القائمة على القيم الأخلاقية والدينية أساسًا لتحصين الأبناء ضد الانحرافات السلوكية في الفضاء السيبراني. فالأسرة التي تغرس مبادئ الصدق، الأمانة، واحترام الخصوصية، تسهم في توجيه الأبناء نحو استخدام التكنولوجيا بشكل مسؤول.
- التوعية بمخاطر الفضاء السيبراني: يجب أن تبادر الأسرة بتثقيف الأبناء حول المخاطر المرتبطة بالجرائم السيبرانية، مثل القرصنة، الاحتيال، والتنمر الإلكتروني. ويمكن تحقيق ذلك من خلال الحوار المفتوح والنقاش حول كيفية استخدام الإنترنت بأمان.

---

37 Ibid.

38 ʿAwad, Hanem Muhammad ʿAbduh. Al-Qurʾan al-Karim wa-Dawruhu fi Muwajahat al-Irhab al-Iliktruni. Hawliyat Kulliyat al-Dirasat al-Islamiyyah wa-al-ʿArabiyyah li-al-Banat bi-al-Iskandariyya 39, no. 1 (2023): 553–647; Halabi, Abd al-Qadir, and Haj Ahmed Qasim. Al-Zahira al-Irhabbiyyah: al-Asbab wa-Subul al-ʿIlaj: Dirasa Muqarana bayn al-Shariʿa al-Islamiyyah wa-al-Qanun al-Jazaʾiri. Majallat Rawafid li-al-Buhuth wa-al-Dirasat 6 (2019): 73–97.

- المتابعة والإشراف: تمثل المتابعة الدائمة لسلوكيات الأبناء عبر الإنترنت جانبًا مهمًا في الوقاية من الجرائم السيبرانية. يمكن للآباء استخدام أدوات الرقابة الأبوية لمتابعة الأنشطة الرقمية للأبناء وضمان حمايتهم من التهديدات.
- تنظيم استخدام التكنولوجيا: يلعب تنظيم الوقت المخصص لاستخدام الأجهزة الإلكترونية والإنترنت دورًا كبيرًا في تقليل تعرض الأبناء للمخاطر. يساعد تحديد أوقات محددة للاستخدام الرقمي في تحقيق توازن صحي بين الحياة الواقعية والعالم الافتراضي.
- تعزيز الثقة والتواصل: فالثقة المتبادلة بين الآباء والأبناء تسهم في تشجيع الأبناء على التحدث عن أي تجربة غير مريحة أو تهديد يتعرضون له عبر الإنترنت. يُمكن أن يُساعد هذا التواصل الفعّال في التعامل المبكر مع المشكلات السيبرانية.
- توفير المعرفة التقنية: حيث تحتاج الأسر إلى الإلمام بالأساسيات التقنية لتكون قادرة على توجيه الأبناء ومساعدتهم في فهم طرق حماية بياناتهم الشخصية وتجنب المواقع أو التطبيقات غير الآمنة.

يتضح أن دور الأسرة في مواجهة الجرائم السيبرانية هو دور محوري لا يمكن الاستغناء عنه في تعزيز الأمن الرقمي للأبناء. فالتربية على القيم والأخلاق، إلى جانب التوعية بالمخاطر الرقمية، تُشكل أساسًا قويًا لتحصين الأبناء ضد التهديدات الإلكترونية. كما أن المتابعة الواعية وتنظيم استخدام التكنولوجيا يعززان من قدرة الأسرة على توجيه الأبناء نحو الاستخدام الآمن والمسؤول للإنترنت.

وعلاوة على ذلك، فإن تعزيز الثقة والتواصل بين أفراد الأسرة يُمكّن الأبناء من التحدث بحرية عن تحدياتهم الرقمية، مما يتيح للآباء تقديم الدعم اللازم. وفي ظل التطور التكنولوجي المتسارع، تصبح المعرفة التقنية جزءًا لا يتجزأ من دور الأسرة في هذا السياق، حيث تمكنهم من مواكبة التحديات وحماية الأبناء بشكل فعّال.

ثانيا: تفعيل دور المدرسة

تلعب المدرسة دورًا محوريًا في التصدي للجرائم السيبرانية من خلال تعزيز الوعي لدى الطلاب وتزويدهم بالمعرفة والمهارات اللازمة لاستخدام التكنولوجيا بشكل آمن ومسؤول. وتتمثل أبرز أدوار المدرسة في هذا المجال فيما يلي[39]:

- توعية الطلاب بمخاطر الجرائم السيبرانية، وتسليط الضوء على أهمية حماية المعلومات الشخصية وطرق التعامل مع أي تهديدات إلكترونية.

[39] Halabi and Qasim, "Al-Zahira al-Irhabbiyyah," 80.

- تضـــمين مفاهيم الأمن الرقمي واســـتخدام الإنترنت بأمان ضـــمن المواد الدراســـية لتعزيز وعي الطلاب منذ الصغر.
- تدريب الطلاب على كيفية اســـتخدام الأدوات التقنية بشـــكل آمن، مثل تفعيل خيارات الخصوصية، استخدام كلمات مرور قوية، وتجنب المواقع غير الموثوقة.
- تعزيز القيم الأخلاقية والسلوكيات الإيجابية مثل الأمانة، المسؤولية، واحترام خصوصية الآخرين.
- إنشـــاء وحدات إرشـــاد نفســـي ودعم اجتماعي لمســـاعدة الطلاب الذين قد يتعرضـــون للتنمر الإلكتروني أو لأي نوع من الجرائم السيبرانية.
- تنظيم ورش عمل مشتركة مع أولياء الأمور لتعزيز الوعي المجتمعي بمخاطر الجرائم السيبرانية.

ويتجلى دور المدرسة كركيزة أساسية في مكافحة الجرائم السيبرانية من خلال جهودها الرامية إلى توعية الطلاب وتزويدهم بالأدوات اللازمة للتعامل مع التحديات الرقمية بأمان ومســـؤولية. فالأنشـــطة التعليمية التي تهدف إلى إدماج مفاهيم الأمن السيبراني ضمن المناهج الدراسية تسهم بشكل كبير في تعزيز الوعي المبكر بالمخاطر الرقمية وســـبل مواجهتها. كما أن تدريب الطلاب على المهارات التقنية والأدوات الآمنة يُعد خطوة حاسمة لتقليل احتمالية وقوعهم ضـحايا للتهديدات الإلكترونية، بينما يُعزز التركيز على القيم الأخلاقية والسلوكيات الإيجابية شعور الطلاب بالمسؤولية تجاه استخدام التكنولوجيا.

وفي ســـياق أســـاليب وســـبل مواجهة الجرائم الســـيبرانية من المنظور الإســـلامي، وضـــع Al-Tamimi et al قانونًا إســـلاميًا مقترحًا للجرائم الســـيبرانية. يهدف هذا المقترح إلى الحد من الجرائم السيبرانية في إطار الشريعة الإسلامية، مع توفير أساس قوي لحماية أجهزة الكمبيوتر وحماية المستخدمين، وتضمن هذا القانون المقترح ما يلي[40]:

1. **الأمن السيبراني**: ينص القانون على أن الأمن السيبراني سيتحقق من خلال حصول الفرد على حقه في الخصـوصـية وحماية بياناته، حيث يجب تفعيل الحصـول على إذن المسـتخدم قبل اسـتخدام أي جهاز كمبيوتر. ويجب أن تكون هناك قيود واضـحة تمنع الاقتراب من أي جهاز كمبيوتر أو التدخل فيما يفعله الآخرون دون إذن. وتطبيق هذا البند بشـكل صـحيح سـيُحدث تغييرًا إيجابيًا في المجتمع من خلال تعزيز احترام خصوصية الآخرين.
2. **بناء الثقة**: ينص القانون على ضـــرورة عدم مشـــاركة البيانات الحســـاســـة أو كلمات المرور مع أي شـخص إلا بعد التحقق من الإثباتات اللازمة. وهنا يجب تطبيق عملية التحقق المزدوج قبل مشـاركة أي بيانات، مما يحد من تسرب البيانات.

[40] Al-Tamimi, K. H. S. S., Marni, N. B., and Shehab, A. A. 2020. "Evidence in Cybercrimes: A Comparative Study between Islamic Law and UAE Legislations." Journal of Critical Reviews 7 (14): 2778–81.

3. **السرقة:** ينص القانون على ضرورة احترام ملكية الآخرين، وعدم استغلال أجهزتهم أو بياناتهم بأي شكل من الأشكال. حيث تعتبر سرقة البيانات شكلًا من أشكال السرقة، ويجب معالجتها بقوانين صارمة. وينص القانون على أن كل جهاز كمبيوتر مملوك لمستخدمه، ويجب احترام ذلك. ويُمنع استخدام أو الاطلاع على محتويات أجهزة الآخرين دون إذن.

ويعكس ذلك القانون الإسلامي المقترح للجرائم السيبرانية مقاربة شاملة تعزز الأمن السيبراني وفقًا لقيم الشريعة الإسلامية. فمن خلال التركيز على احترام الخصوصية، وبناء الثقة، والتصدي لسرقة البيانات، يوفر هذا القانون أساسًا أخلاقيًا وقانونيًا لحماية المستخدمين وأجهزتهم من الجرائم السيبرانية. وتطبيق هذه المبادئ لا يقتصر على تحقيق الأمن الرقمي فحسب، بل يسهم أيضًا في بناء مجتمع رقمي تسوده القيم الإسلامية، مثل الاحترام، والأمانة، والعدالة. لذا، يمثل هذا القانون خطوة مهمة نحو صياغة إطار قانوني يجمع بين التشريعات الحديثة والمبادئ الإسلامية لضمان بيئة إلكترونية أكثر أمانًا واستدامة.

وقد أشار العقبي إلى مجموعة من الإجراءات الوقائية الضرورية للتصدي للجرائم والهجمات السيبرانية من منظور إسلامي. وتتمثل هذه الإجراءات فيما يلي[41]:

- تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية.
- إنشاء إدارات متخصصة ضمن وزارات الداخلية تكون مسؤولة عن التصدي لهذه الجرائم.
- التأمين المادي للأجهزة والمعدات من خلال توفير المباني والمرافق المناسبة.
- التأمين الافتراضي لأنظمة البيانات والشبكات عبر تحديث الأجهزة والأنظمة، استخدام المواقع الموثوقة، ونسخ الملفات وتخزينها بأماكن آمنة.
- رفع مستوى الوعي الأمني من خلال التوعية بالمخاطر والقضايا المتعلقة بالأمن السيبراني، باستخدام وسائل الإعلام ووسائل التواصل الاجتماعي.
- المشاركة في المؤتمرات الدولية التي تُعقد حول الأمن السيبراني وسبل مواجهة الهجمات السيبرانية العابرة للقارات، مما يُسهم في تعزيز قدرة الدول العربية والإسلامية على التصدي لهذه الجرائم.

ويشير ما أورده العقبي إلى أهمية اتباع نهج شامل للتصدي للجرائم والهجمات السيبرانية من منظور إسلامي، يتكامل فيه الجانب الوقائي مع الجوانب التقنية والإدارية والتوعوية. فتعزيز التعاون الدولي، وإنشاء إدارات متخصصة، وتأمين الأجهزة والأنظمة، ورفع مستوى الوعي[42]، كلها إجراءات أساسية لحماية الأفراد والمجتمعات من المخاطر السيبرانية. كما أن الانخراط في المؤتمرات الدولية يعزز تبادل الخبرات ويُمكّن الدول العربية والإسلامية من مواكبة التطورات العالمية في هذا المجال. ومن خلال هذه

---

41 Al-ʿUqbi, Taha Ahmed Muntasir. Al-Ahkam al-Mutaʿalliqa bi-al-Amn al-Sibirani fi al-Shariʿa al-Islamiyyah wa-TataBiqatihi al-Muʿasira. Majallat Markaz Jazirat al-Arab li-al-Buhuth al-Tarbawiyyah wa-al-Insaniyyah 2, no. 13 (2022): 26–45.

42 Al-ʿUqbi, "Al-Ahkam al-Mutaʿalliqa bi-al-Amn," 30.

الإجراءات الوقائية، يمكن بناء بيئة رقمية آمنة تُحقق الأمن السيبراني في ضوء القيم الإسلامية، وتعزز القدرة على مواجهة التحديات التقنية المعاصرة بفعالية واستدامة.

وذكر عوض، والبلوشي وآخرون أن من أهم سبل مكافحة الجرائم السيبرانية في ظل الشريعة الإسلامية ما يلي[43]:

1. **التربية على أساس العقيدة القويمة:** تُعد التربية الدينية القويمة أحد الأسس الرئيسة لمكافحة الجرائم السيبرانية في ظل الشريعة الإسلامية. فهي تهدف إلى بناء وعي الأفراد حول القيم الأخلاقية والدينية التي تحث على احترام حقوق الآخرين، بما في ذلك حقوقهم في الفضاء السيبراني. وتعمل التنشئة الدينية السليمة على ترسيخ القيم الإسلامية التي تدعو إلى الأمانة واحترام الخصوصية والابتعاد عن الغش أو الاحتيال. وللأسرة والمدرسة والمجتمع دور هام في التربية الدينية، وذلك من خلال إشراك الأسرة والمدرسة والمجتمع في توجيه الأفراد لاستخدام الإنترنت بما يتماشى مع القيم الإسلامية.
2. **معرفة العدو، والحد من الغلو والتطرف:** تشير هذه النقطة إلى أهمية فهم التهديدات الإلكترونية التي تواجه المجتمعات المسلمة، سواء كانت من الداخل أو الخارج، والعمل على الحد من التطرف الذي قد يؤدي إلى استغلال الإنترنت في أعمال غير شرعية. وهنا يجب معرفة طبيعة العدو من خلال التركيز على تعريف الناس بالجهات أو الأفراد الذين يستخدمون الفضاء السيبراني للإضرار بالمجتمع أو استهدافه فكريًا واقتصاديًا. كما يجب مكافحة الغلو والتطرف من خلال تقديم التوعية الفكرية والدينية التي تبرز وسطية الإسلام، ودحض الأفكار المتطرفة التي قد تؤدي إلى استغلال التقنية في نشر الفوضى. ويمكن معرفة العدو من خلال التدريب التقني الذي يمكن أن يسهم في تمكين الأفراد من معرفة كيفية التعامل مع محاولات الاختراق الإلكتروني أو الدعاية المتطرفة عبر الإنترنت.
3. **التحقق من صحة الأخبار المنشورة وعدم الاغترار بالدعاية الكاذبة، والرجوع إلى المصادر الموثوق منها:** فمع انتشار المعلومات الزائفة عبر الإنترنت، تشدد الشريعة الإسلامية على أهمية تحري الصدق والتثبت من الأخبار قبل نشرها أو التصرف بناءً عليها. حيث تحث الشريعة الإسلامية المسلمين على قاعدة "فتبينوا" الواردة في القرآن الكريم عند التعامل مع الأخبار، خاصة تلك التي تؤثر على سمعة الأفراد أو المجتمعات. كما تحثهم على الابتعاد عن الدعاية الكاذبة، وفهم خطورة نشر الأخبار الكاذبة التي قد تُستخدم لتضليل الآخرين أو إثارة الفتن. وتحثهم كذلك على الرجوع إلى المصادر الموثوقة، وتعزيز ثقافة الاعتماد على القنوات الرسمية والمواقع الموثوقة للحصول على المعلومات بدلاً من الاعتماد على منصات غير موثوقة.

---

43 ʿAwad, "Al-Qurʾan al-Karim wa-Dawruhu," 600; al-Balushi, Yusuf, and Rakan, "Al-Amn al-Sibirani," 1700.

4. **ضبط مواقع الفتوى:** وذلك عبر إسناد المواقع الخاصة بالفتوى للمختصين، فمن أخطر ما يُواجه المجتمعات المسلمة في الفضاء السيبراني هو انتشار الفتاوى غير المدروسة التي قد تصدر من أشخاص غير مختصين. ويمكن ضبط مواقع الفتوى من خلال إنشاء منصات رسمية تضم علماء مؤهلين وذوي خبرة للإجابة عن الاستفسارات الشرعية بشكل دقيق ومعتدل. وكذلك الحد من الفوضى في إصدار الفتاوى من خلال وضع ضوابط صارمة على إنشاء مواقع الفتوى، مع رصد المواقع التي تُصدر فتاوى مخالفة أو مضللة. كما يمكن ضبط مواقع الفتوى من خلال التوعية بمصادر الفتوى الصحيحة، وتوجيه المسلمين نحو معرفة الجهات الشرعية الموثوقة لتجنب الفتاوى التي قد تساهم في نشر الغلو أو التطرف.
5. **القضاء حواريًا على شبه المتطرفين:** هذا العنصر يعكس أهمية الحوار البنّاء في مواجهة الأفكار المتطرفة التي تُستخدم كذريعة لارتكاب الجرائم السيبرانية. حيث يمكن توظيف الحوار كوسيلة للإقناع من خلال التركيز على منهج النقاش الهادئ والمستند إلى الحجة الشرعية والعقلية لدحض الأفكار المغلوطة. كما يمكن توظيف الحوار كوسيلة للإقناع من خلال تصميم برامج إصلاحية حوارية موجهة للمتطرفين، تهدف إلى معالجة الشبهات التي يروجون لها باستخدام خطاب معتدل وشامل. وهنا يجب إشراك علماء الدين والمفكرين في قيادة هذه الحوارات لتقديم ردود مقنعة وتوجيه الشباب المتأثرين بخطاب التطرف.

يتضح مما سبق أن مكافحة الجرائم السيبرانية في ظل الشريعة الإسلامية تعتمد على نهج شامل يتجاوز التدابير التقنية والقانونية ليشمل تعزيز القيم الدينية والأخلاقية. فمن خلال التربية على العقيدة القويمة، والتوعية بمخاطر التطرف والغلو، وضبط مواقع الفتوى، والتحقق من الأخبار، يمكن بناء مجتمع رقمي آمن قائم على الوسطية والاعتدال. كما أن مواجهة الأفكار المتطرفة بالحوار البنّاء تعكس أهمية استخدام الوسائل الفكرية والدينية لمعالجة جذور المشكلة. إن هذا النهج المتكامل يُبرز قدرة الشريعة الإسلامية على التكيف مع التحديات المعاصرة، وتقديم حلول مستدامة تعزز الأمان والاستقرار في الفضاء السيبراني، مع الحفاظ على القيم والمبادئ الإسلامية.

المحور الثالث: الآليات الإجرائية المقترحة لمواجهة الجرائم السيبرانية

إن مواجهة الجرائم السيبرانية تتطلب استراتيجيات وآليات متعددة المستويات تشمل الجوانب القانونية، التقنية، التوعوية، والتعاونية. ففي ضوء المبادئ الإسلامية التي تعكس المرونة والقدرة على التكيف مع القضايا المعاصرة، يمكن اقتراح مجموعة من الآليات الإجرائية لمواجهة الجرائم السيبرانية، وهي كالتالي:

- تعزيز الثقافة السيبرانية من منظور إسلامي: وذلك من خلال نشر الوعي بين الأفراد حول الاستخدام الأمثل للتكنولوجيا الرقمية بما يتماشى مع القيم الأخلاقية والمبادئ الإسلامية. ومن

خلال إدراج مبادئ التعامل مع التكنولوجيا في المناهج الدراسية لتعزيز فهم الأطفال والشباب للقيم المرتبطة باستخدامها.

- إنشاء آليات تقنية متوافقة مع مبدأ التيسير من خلال تطوير أنظمة أمان مبسطة، وتصميم أدوات أمنية سهلة الاستخدام يمكن للجميع التعامل معها لحماية الخصوصية ومكافحة الجرائم الإلكترونية. وكذلك تيسير الإبلاغ عن الجرائم السيبرانية من خلال إنشاء منصات رقمية ميسرة للإبلاغ عن الجرائم مع ضمان حماية المبلغين.
- حفظ الخصوصية وتعزيز أمن البيانات من خلال وضع قوانين واضحة تحمي بيانات الأفراد وتعاقب من ينتهكها. وتعزيز استخدام تقنيات التشفير لضمان أمن المعلومات وحمايتها من الاختراق.
- التزام الضوابط الشرعية والقانونية من خلال وضع قوانين وطنية تجرّم أفعالاً مثل القرصنة الإلكترونية، والتشهير، والتعدي على الخصوصيات، مستمدة من الشريعة الإسلامية.

واستنادًا إلى مقاصد الشريعة في صون الضروريات الخمس، يمكن اقتراح مجموعة من الآليات الإجرائية لمواجهة الجرائم السيبرانية كما يلي:

- مراقبة المحتوى الرقمي من خلال إنشاء منصات تكنولوجية متخصصة لرصد المحتويات الرقمية التي تروج للأفكار الهدامة، مع تعزيز التعاون بين الحكومات ومنصات التواصل الاجتماعي.
- التوعية الدينية بإطلاق حملات رقمية تهدف إلى تعزيز الوعي الديني والقيم الأخلاقية بين الشباب عبر وسائل التواصل.
- التصدي للجرائم المهددة للنفس من خلال تعزيز أنظمة مكافحة الاتجار بالبشر والاستغلال الجنسي عبر الإنترنت باستخدام الذكاء الاصطناعي لتحليل الأنشطة المشبوهة.
- رعاية الصحة النفسية من خلال توفير خدمات دعم نفسي رقمية تساعد ضحايا الجرائم الإلكترونية على التعافي.
- تعزيز القيم الروحية من خلال إدراج برامج إيمانية وتوعوية في المدارس والجامعات تهدف إلى تعزيز القيم الأخلاقية، مما يساهم في تهذيب النفس وتقليل معدلات الجرائم.
- مكافحة الانحراف الفكري من خلال إنشاء مراكز إلكترونية متخصصة لرصد المحتويات التي تروج للأفكار المنحرفة ومكافحتها، مع تقديم محتوى بديل هادف.
- تشديد الرقابة على وسائل الإعلام الرقمية من خلال سن قوانين تفرض على مزودي الخدمات الرقمية تحمل مسؤولية المحتويات المنشورة عبر منصاتهم.

- تطوير التشريعات لفرض عقوبات صارمة على مرتكبي الجرائم الأخلاقية الرقمية، مثل التشهير أو نشر المواد المسيئة. وتجرّم نشر المحتويات التي تستهدف عقيدة المسلمين أو تحرض على التطرف الفكري
- حماية الأصـــول الرقمية من خلال تطوير تقنيات أمنية متقدمة لحماية الحســـابات البنكية والمعاملات الإلكترونية من الاختراق والاحتيال.

واستنادًا إلى مفهوم الأمر بالمعروف والنهي عن المنكر كآلية لإصلاح الأفراد وتعزيز السلوكيات الإيجابية، يمكن اقتراح مجموعة من الآليات الإجرائية لمواجهة الجرائم السيبرانية كما يلي:

- تعزيز القيم الأخلاقية والوعي الأخلاقي من خلال إطلاق حملات توعوية تستهدف نشر القيم الإسلامية مثل الصدق، الأمانة، واحترام حقوق الآخرين في الفضاء الرقمي.
- إعداد برامج تعليمية تُعزز المراقبة الذاتية لدى الأفراد من خلال تحفيزهم على مراقبة الله في السر والعلن، مما يقلل من احتمالية ارتكاب الجرائم السيبرانية.
- تشـــجيع الشـــباب على الانخراط في مبادرات تطوعية تهدف إلى توعية المجتمع حول الجرائم السيبرانية وتعزيز السلوكيات الإيجابية.

واستنادًا إلى مفهوم التكييف الفقهي كأداة لتحليل وتوصيف الجرائم السيبرانية بما يتماشى مع الشريعة الإسلامية، يمكن اقتراح مجموعة من الآليات الإجرائية لمواجهة الجرائم السيبرانية كما يلي:

- إعداد دليل فقهي وتقني موحد يُعرف الجرائم السيبرانية المختلفة (مثل الاختراق، سرقة البيانات، التزوير الإلكتروني)، ويحدد أركانها ومكوناتها التقنية.
- تشكيل فرق عمل تجمع بين العلماء الشرعيين والمتخصصين في الأمن السيبراني لتحديد ماهية الجرائم السيبرانية وتحليل أدواتها وأثرها.
- اســـتخدام القواعد الفقهية مثل "الضـــرر يزال"، و"ما لا يتم الواجب إلا به فهو واجب"، و"الأصل في الأموال الحرمة"، كأطر لتكييف الجرائم السيبرانية.
- تشجيع الاجتهاد الفقهي لتكييف الجرائم الجديدة على الأصول الفقهية القديمة، مع الأخذ بعين الاعتبار طبيعة التكنولوجيا وتأثيراتها الحديثة.
- اســتحداث أحكام شــرعية تناســب الطبيعة التقنية للجرائم الســيبرانية في حال وجود اختلاف جوهري بينها وبين الأصول التقليدية.
- تحويل الأحكام الشرعية الناتجة عن التكييف الفقهي إلى قوانين ولوائح تُطبق في المحاكم الشرعية والمدنية.
- إنشاء منصات إلكترونية تجمع بين الإرشاد الفقهي والدعم التقني لتقديم استشارات حول الجرائم السيبرانية.

وبناءً على دور العقوبة في الحد من الجرائم السيبرانية وفقًا للشريعة الإسلامية، يمكن اقتراح مجموعة من الآليات الإجرائية لمواجهة الجرائم السيبرانية كما يلي:

- إلزام مرتكبي الجرائم السيبرانية بدفع غرامات مالية تتناسب مع خطورة الجريمة، بالإضافة إلى تعويض الضرر الناتج عنها.
- مصادرة أو إتلاف الأجهزة والتقنيات التي يتم استخدامها لارتكاب الجرائم السيبرانية، مثل الحواسيب أو البرمجيات الخبيثة.
- تطبيق عقوبات الحبس محددة المدة على مرتكبي الجرائم السيبرانية غير الخطيرة، كإجراء يهدف إلى التأديب والإصلاح. واستخدام الحبس غير محدد المدة للجناة الذين يكررون الجرائم السيبرانية أو يشكلون تهديدًا خطيرًا على الأمن السيبراني.
- تطبيق عقوبة الإعدام في الجرائم السيبرانية ذات التأثير الواسع والخطير، مثل التجسس السيبراني الذي يهدد الأمن القومي أو الهجمات السيبرانية واسعة النطاق.
- فرض عقوبة الجلد على الجناة الذين يرتكبون جرائم سيبرانية تتعلق بانتهاك الأخلاق أو التحريض على الفواحش عبر الإنترنت.
- إنشاء برامج تأهيلية للجناة خلال فترة تنفيذ العقوبة، تشمل التوعية بمخاطر الجرائم السيبرانية وأهمية الامتثال للأخلاقيات الرقمية.
- إنشاء محاكم مختصة بالجرائم السيبرانية تعتمد على المبادئ الشرعية مع مراعاة التطورات التقنية.

ووفقًا لأهمية الإخبار والإعلام، التبيُّن، والصبر والتحكم بالنفس في الوقاية من آثار الجرائم السيبرانية، يمكن اقتراح آليات إجرائية لمواجهة الجرائم السيبرانية على النحو التالي:

- إنشاء نظام إلكتروني لإبلاغ المستخدمين الذين يرتكبون أخطاء بسيطة أو يشاركون في أنشطة مشبوهة عبر الإنترنت (مثل مشاركة روابط خبيثة) مع تنبيههم إلى العواقب المحتملة.
- إرسال رسائل توجيهية للمستخدمين الذين تم الإبلاغ عنهم بسبب أنشطة سيبرانية غير لائقة، لتوعيتهم بخطورة أفعالهم وتأثيرها على الآخرين.
- تطوير أدوات تقنية للتحقق من صحة الروابط والمواقع الإلكترونية قبل فتحها، مثل ملحقات المتصفح أو تطبيقات الهواتف.
- تنفيذ حملات تثقيفية للمستخدمين حول كيفية التمييز بين المحتوى الحقيقي والمزيف، مع أمثلة عملية.
- تصميم برامج تدريبية رقمية تهدف إلى تعزيز مهارات الصبر وضبط النفس عند التعامل مع الرسائل المشبوهة أو العروض المغرية عبر الإنترنت.

- تطوير أدوات تكنولوجية تتيح للمستخدمين خيار "التفكير مرتين" قبل النقر على الروابط أو مشاركة المعلومات الحساسة.

خاتمة

أولا: النتائج

أبرزت الدراسة أنّ المنظور الشرعي، بما يحمله من مقاصد حفظ الدين والنفس والمال والعِرض، يمتلك قابلية عالية للتكيّف مع الجرائم السيبرانية المعاصرة؛ إذ يُمكِّن من وضع إطار مرن يغطّي معظم صور الاعتداءات الرقمية كاختراق الخصوصيّة والابتزاز والاحتيال. وتبيّن أنّ توصيف هذه الجرائم في باب التعزير يُتيح سلطة تقديرية للقاضي الشرعي تراعي خطورة الفعل وسرعة تطوّر الأساليب التقنية، فيحقق الردع المطلوب دون الجمود على عقوبات محدَّدة.

كما أظهرت النتائج أن الأسرة تمثّل خطَّ الدفاع الأوّل حين تعتمد ثقافة رقمية قائمة على الرقابة الإيجابية، فتقلّ معدلات تعرّض الأبناء للانحرافات الإلكترونية مقارنة بالأُسر ذات الضبط الصارم أو المنفلت. وفي السياق ذاته، كشفت تحليلات المناهج التعليمية في الدول الإسلامية عن فجوة بين المحتوى الديني النظري ومهارات الأمن السيبراني التطبيقية؛ فإدماج مفاهيم الأمانة والخصوصية الرقمية في المقرّرات يسهم في خفض قبول الطلاب لسلوكيات الاختراق والقرصنة.

واتضح كذلك أنّ الشراكة المؤسسية بين الهيئات الشرعية ووزارات التعليم وهيئات الاتصالات ترفع كفاءة حملات التوعية وتسرّع سنّ التشريعات المواكبة، في حين يُظهر الاعتماد على القوانين الوضعية وحدها قصوراً بسبب تأخر نصوص التجريم عن المستجدات التقنية، الأمر الذي يسدّه المنظور المقاصدي المستوعِب للمآلات.

وأسفر البحث عن حاجة ماسة إلى بروتوكولات تحقيق رقمية تراعي فقه الضرورة وتحفظ خصوصية الأفراد، إضافة إلى ملاحظة ضعفٍ ملموس في الأدبيات العربية المتخصصة التي تربط الأمن السيبراني بالفقه، ما يفتح آفاقاً واسعةً للبحث المستقبلي.

ثانيا: التوصيات

استناداً إلى ما سبق، توصي الدراسة بوضع دليل شرعي–تقني موحَّد تصدره جهة فقهية بالتعاون مع مؤسسات أمنية، يتضمن تصنيفاً محدثاً لأنماط الجرائم السيبرانية وعقوباتها التعزيرية وآليات الإثبات الرقمي. وتدعو إلى إدماج «محو الأمية السيبرانية الشرعية» كوحدة إلزامية داخل مناهج التربية الإسلامية والحاسب الآلي، تُعنى بغرس قيم الأمانة وحماية الخصوصية وتحريم الإيذاء الإلكتروني. كما تحث على إطلاق برامج تدريب أسرية تفاعلية عبر المراكز الاجتماعية والمساجد، تمكّن الوالدين من تطبيق الرقابة الإيجابية وفهم الأحكام الشرعية المتصلة بحماية البيانات.

وترى الدراسة ضرورة إنشاء منصة فقهية–تقنية مفتوحة المصدر ثنائية اللغة تجمع الفتاوى والقوانين

وتحدَّث دورياً لخدمة الباحثين والقضاة. وتوصي كذلك بتأهيل قضاة ومحامين عبر برامج دبلوم مشتركة بين كليات الشريعة وتقنية المعلومات، تركز على أدلة الإثبات الرقمي وتتبّع الجرائم.

ولتحفيز البحث التطبيقي، تشجع منحَ تمويل تنافسي لرسائل الماجستير والدكتوراه التي تقيس أثر إدماج القيم الإسلامية في حملات التوعية السيبرانية، مع نشر نتائجها في دوريات عربية محكَّمة.

أخيراً، تحث الدراسة البرلمانات في الدول الإسلامية على سنّ تشريعات خصوصية أكثر صرامة، وعلى إنشاء مراكز استجابة وطنية تجمع بين الخبرة الشرعية والتقنية لرصد التهديدات الرقمية وإصدار توجيهات فورية للمجتمع وفق أحكام الشريعة السمحة.

Refrences

Alanazi, S. S., Ali, A. K., and Khalil, S. A. 2023. "Fiqh Adaptation (al-Takyif al-Fiqhi) of the Crime of Extortion through Electronic Means and Its Penalties in Islamic Law." *Jurnal Fiqh* 20 (1): 141–64.

Al-ʿAnazi, Sultan Sabil, Abd al-Karim ibn Ali, and Shahidra bint Abd al-Khalil. Al-Takyif al-Fiqhi li-Jarimat al-Ibtizaz al-Iliktruni wa-al-Taʾsil al-Fiqhi li-al-ʿUqubat al-Warida fi al-Anzima al-Khalijiyyah. *Majallat al-Islam fi Asia* 20, no. 2 (2023): 199–234.

Al-Balushi, Khamis bin Abdullah Salim, Ahmad Yusuf, and Abdul Aziz Rakan. Al-Amn al-Sibirani min al-Manzur al-Islami. *Majallat Kulliyat al-Shariʿa wa-al-Qanun bi-Asyut* 36, no. 2 (2024): 1677–1729.

Al-Sharkasi, Muhammad Mahmud. Al-Jarima al-Iliktruniyyah wa-Subul Mukafahatiha fi Dawʾ Ahkam al-Fiqh al-Islami: Dirasa Muqarana. *Majallat al-Manara al-ʿIlmiyyah* 2 (n.d.): 179–197.

Al-Shuraim, Hamda Muhammad. Al-Jarayim al-Iliktruniyyah wa-Mawqif al-Shariʿa al-Islamiyyah Minha: al-Halat al-Dirasiyyah al-Qanun al-Qatari. *Majallat al-Dirasat al-Islamiyyah wa-al-Fikr li-al-Buhuth al-Takhassusiyyah* 5, no. 1 (2019): 101–122.

Al-Tamimi, K. H. S. S., Marni, N. B., and Shehab, A. A. 2020. "Evidence in Cybercrimes: A Comparative Study between Islamic Law and UAE Legislations." *Journal of Critical Reviews* 7 (14): 2778–81.

Al-ʿUqbi, Taha Ahmed Muntasir. Al-Ahkam al-Mutaʿalliqa bi-al-Amn al-Sibirani fi al-Shariʿa al-Islamiyyah wa-TataBiqatihi al-Muʿasira. *Majallat Markaz Jazirat al-Arab li-al-Buhuth al-Tarbawiyyah wa-al-Insaniyyah* 2, no. 13 (2022): 26–45.

Alyammahi, M., and Noor, S. 2024. "Cyber Crimes in the United Arab Emirates: A Study of Characteristics, Patterns, and Countermeasures from an Islamic Perspective." *International Journal of Islamic Studies* 33 (3): 514–38.

Al-Zuʿbi, Ahmad Shahada Bashir. Manhaj al-Islam fi Muharabat al-Jarima. *Al-Majalla al-ʿArabiyyah li-al-Dirasat al-Amniyyah* 28, no. 56 (2012): 33–83.

ʿAwad, Hanem Muhammad ʿAbduh. Al-Qurʾan al-Karim wa-Dawruhu fi Muwajahat al-Irhab al-Iliktruni. *Hawliyat Kulliyat al-Dirasat al-Islamiyyah wa-al-ʿArabiyyah li-al-Banat bi-al-Iskandariyya* 39, no. 1 (2023): 553–647.

Bilal, H., and Khan, M. A. 2022. "Cyber Crime Legislation in Pakistan: A Critical Analysis from Islamic Law Perspective." *Al-Idah* 40 (2): 1–18.

Bin Turki, Layla. Al-Jazaʾ al-Jinaʾi fi al-Tashriʿ al-Islami. *Majallat al-ʿUlum al-*

Insaniyah 50 (2018): 47–67.

Cozens, Bill. "2024 State of Ransomware in Education: 92 % Spike in K-12 Attacks." ThreatDown (Malwarebytes Blog), January 24, 2024. https://www.threatdown.com/blog/2024-state-of-ransomware-in-education-92-spike-in-k-12-attacks/. threatdown.com

Greig, Jonathan. "Kuwait Isolates Some Government Systems Following Attack on Its Finance Ministry." The Record (Recorded Future News), September 26, 2023. https://therecord.media/kuwait-isolates-systems-after-ransomware-attack. therecord.media

Halabi, Abd al-Qadir, and Haj Ahmed Qasim. Al-Zahira al-Irhabbiyyah: al-Asbab wa-Subul al-ʿIlaj: Dirasa Muqarana bayn al-Shariʿa al-Islamiyyah wa-al-Qanun al-Jazaʾiri. *Majallat Rawafid li-al-Buhuth wa-al-Dirasat* 6 (2019): 73–97.

Hasanah, U. 2018. "The Effectiveness of Islamic Law Implementation to Address Cyber Crime: Studies in Arab, Brunei Darussalam, and China." *Al-Ahkam: Jurnal Ilmu Syari'ah dan Hukum* 3 (2): 107–22.

IBM Security. Cost of a Data Breach Report 2024. Armonk, NY: IBM Corporation, 2024. https://www.ibm.com/reports/data-breach. ibm.com

Komaruddin, K., Utama, A. S., Sudarmanto, E., and Sugiono, S. 2023. "Islamic Perspectives on Cybersecurity and Data Privacy: Legal and Ethical Implications." *West Science Law and Human Rights* 1 (4): 166–72.

Morgan, Steve. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Cybercrime Magazine, February 21, 2024. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. cybersecurityventures.com

Muhammad, Amna Ali al-Bashir. Al-Amn al-Sibirani fi Dawʾ Maqasid al-Shariʿa. *Hawliyat Kulliyat al-Dirasat al-Islamiyyah wa-al-ʿArabiyyah li-al-Banat bi-al-Iskandariyya* 37, no. 1 (2021): 449–505.

Naro, W., Syatar, A., Amiruddin, M. M., Haq, I., Abubakar, A., and Risal, C. 2020. "Shariah Assessment toward the Prosecution of Cybercrime in Indonesia." *International Journal of Criminology and Sociology* 9: 572–86.

Positive Technologies. Cybersecurity Threatscape in the Middle East: 2023–2024. Moscow: Positive Technologies, 2024. https://global.ptsecurity.com/analytics/cybersecurity-threatscape-in-the-middle-east-2023-2024. global.ptsecurity.com

Ramli, Nurzakiyyah bint al-Hajj, and Adnan Mahmud Sharari al-Assaf. Al-Takyif al-Fiqhi li-al-Sariqa al-Iliktruniyyah: Dirasa Muqarana maʿ Qanun Brunei. *Al-Majalla al-Urduniyyah fi al-Dirasat al-Islamiyyah* 16, no. 3 (2020): 369–391.

Santoso, E. 2018. "The Role of Islamic Values to Prevent the Society for Cyber Crime Victim in Social Media." Paper presented at the *International Conference on Media and Communication Studies (ICOMACS 2018)*, October, 293–97. Atlantis Press.

Sukardi, D., Nugraha, F. B., Ubaidillah, U., Fatakh, A., Leliya, L., and Arrizky, M. F. 2023. "Solving Cyber Crime in Online Buying and Selling in Cirebon City in Review of ITE Law and Islamic Law." *Al-Mustashfa: Jurnal Penelitian Hukum Ekonomi Syariah* 8 (2): 237–50

Vicens, A. J. "US School Districts Facing Extortion Attempt after Hack, Software Provider Says." Reuters, May 7, 2025. https://www.reuters.com/world/us/us-school-districts-facing-extortion-attempt-after-hack-software-provider-says-2025-05-07/. reuters.com