

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب

والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

Cybercrimes in Cyberspace: A Qualitative Analytical Study of Polarization and Extremism, Banking Fraud, and Intellectual Property Infringement

د. فيصل بن مونس العنزي⁽¹⁾

⁽¹⁾ أستاذ الإعلام المساعد في قسم الإعلام بجامعة الملك سعود (المسعودية)، . falanazi3@ksu.edu.

تاريخ النشر: 2025/09/30

تاريخ القبول: 2023/10/28

تاريخ الاستلام: 2025/07/22

ملخص

تتناول هذه الدراسة بالتحليل ظاهرة الجرائم الاتصالية في الفضاء السيبراني، وتأثيراتها المتنامية على منظومتي الأمن الفكري والاقتصادي، وانطلاقاً من ندرة الدراسات التي تعالج هذه الجرائم كمنظومة متكاملة، يعتمد البحث على المنهج النوعي بأسلوبه الوصفي التحليلي، مقدماً قراءة نقدية لثلاثة نماذج رئيسية هي: الاستقطاب الفكري والتطرف، والاحتيال المصرفي، وانتهاك حقوق الملكية الفكرية، إذ تهدف هذه الورقة إلى دراسة الأساليب الإجرامية المستحدثة في كل نموذج، وتقييم فاعلية الأطر التشريعية الحالية في مواجهتها، وقد توصلت الدراسة إلى أن هذه الجرائم، رغم اختلاف أشكالها، تشكل منظومة تهديد واحدة ومتداخلة؛ فالأدوات والمنصات التي تُستخدم لتهديد الأمن الفكري عبر الاستقطاب هي ذاتها التي قد تُستغل لتهديد الأمن الاقتصادي عبر الاحتيال المالي، كما أظهرت النتائج وجود فجوة متزايدة بين سرعة تطور هذه الجرائم وببطء وتيرة الاستجابات التشريعية والتقنية لها. وبناءً على ذلك، توصي الدراسة بضرورة تبني استراتيجية وطنية متكاملة تجمع بين التحديث التشريعي المستمر، وتطوير الحلول التقنية المتقدمة، وتكثيف برامج التوعية المجتمعية لتحسين الفضاء السيبراني.

الكلمات المفتاحية: الجرائم الاتصالية، الفضاء السيبراني، الاستقطاب الفكري، الاحتيال المصرفي، الملكية الفكرية.

Abstract :

This study analytically addresses the phenomenon of communication crimes in cyberspace and their growing impact on the intellectual and economic security systems. Stemming from the scarcity of studies that treat these crimes as an integrated system, this research adopts a qualitative approach with its descriptive-analytical method, presenting a critical reading of three main models: intellectual and extremist polarization, banking fraud, and intellectual property infringement. This paper aims to examine the emerging criminal methods in each model and to evaluate the effectiveness of current legislative frameworks in confronting them. The study concluded that these crimes, despite their different forms, constitute a single, interconnected threat system; the tools and platforms used to threaten intellectual security through polarization are the same ones that can be exploited to threaten economic security through financial fraud. The findings also revealed a growing gap between the rapid evolution of these crimes and the slow pace of legislative and technological responses. Accordingly, the study recommends the adoption of a comprehensive national strategy that combines continuous legislative modernization, the development of advanced technological solutions, and the intensification of community awareness programs to fortify cyberspace.

Keywords: Cyberspace, Intellectual Polarization, Banking Fraud, Intellectual Property.

مقدمة

شهد العالم منذ ثمانينيات القرن الماضي ثورة في تقنية المعلومات أعادت تشكيل بنية المجتمعات¹، وبينما فتحت هذه الثورة آفاقاً للنمو والابتكار، فقد أفرزت في الوقت ذاته بيئة جديدة للجريمة تُعرف بـ "الفضاء السيبراني"، حيث انتقلت الممارسات المحظورة من بيئتها الواقعية إلى الرقمية². وفي هذا الفضاء، لم تعد التهديدات تقتصر على الأصول المادية، بل امتدت لتطال ركيزتين أساسيتين للأمن الوطني والمجتمعي هما الأمن الفكري والاقتصادي.

ويمكن تعريف هذه الجرائم المستحدثة بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات"³، حيث تتميز هذه الجرائم بأنها تقع في بيئة لا يظهر فيها أثر مادي مباشر، وتمنح مرتكبها قدرة على التخفي خلف سرية الشبكة العنكبوتية⁴.

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

فعلى صعيد الأمن الفكري، استغلت حركات التطرف والاستقطاب هذه البيئة كمنصة لنشر أفكارها الهدامة وتجنيد الأتباع⁵، مستهدفة بذلك عقول الشباب وتماسك النسيج الاجتماعي⁶، وعلى صعيد الأمن الاقتصادي، أصبح الاحتيال المالي وانتهاك حقوق الملكية الفكرية من أبرز الجرائم التي تهدد المؤسسات والأفراد، وهو ما يقف عائقاً أمام الطموحات التنموية العالمية الرامية إلى بناء اقتصادات رقمية آمنة ومزدهرة.

حيث وصلت هذه التحديات إلى مستوى استراتيجي قد يرقى إلى "حرب معلوماتية" يسعى فيها كل طرف لتدمير بيانات خصمه، مما يشكل تحدياً كبيراً للمنظومات الأمنية والتقنية والقانونية ويتطلب مهارات أكثر تعقيداً من تلك اللازمة للجرائم التقليدية⁷، وانطلاقاً من هذا الواقع، تأتي هذه الدراسة لمحاولة تقديم قراءة تحليلية لهذه الظواهر سعياً من الباحث لتحليل أبعاد هذه التهديدات المتشابكة، وفهم تقاطعاتها، وتقديم رؤية متكاملة تساهم في تعزيز منظومة الأمن الفكري والاقتصادي في الفضاء السيبراني.

مشكلة الدراسة

تكمن مشكلة الدراسة في أن التحول المتسارع نحو المجتمع المعلوماتي قد أفرز تحديات جسيمة تهدد منظومة الأمن الفكري والاقتصادي في الفضاء السيبراني. فعلى صعيد الأمن الفكري، لم تعد القضية مجرد وجود محتوى ضار، بل أصبحت تتمثل في قدرة الحركات المتطرفة على توظيف استراتيجيات اتصال متقدمة ومتطورة باستمرار لاستهداف الشباب فكرياً، وهو ما أكدته دراسة⁸، ومما يساهم في تفاقم هذا الخطر الذي يؤدي⁹ إلى التدفق الهائل للمعلومات عبر مصادر الويب غير الموثوقة يعد سبباً رئيسياً للانحراف الفكري.

وعلى صعيد الأمن الاقتصادي، تتعرض الاقتصادات لخطر الخسائر الفادحة نتيجة لجرائم الاحتيال المصرفي وانتهاكات حقوق الملكية الفكرية، وتتفاقم هذه المشكلة في ظل ما

¹⁰ وجود تحديات كبيرة تجعل من الصعب السيطرة على هذه الجرائم، أبرزها قصور التشريعات وصعوبة تحديد مرتكبيها. وهو ما يقف عائقاً أمام تحقيق الاستفادة الكاملة من إمكانات الاقتصاد الرقمي. وبالتالي، فإن جوهر المشكلة يكمن في الفجوة المتزايدة بين سرعة تطور الأساليب الإجرامية في الفضاء السيبراني، وبطء وتيرة تطور الاستجابات التشريعية والتقنية القادرة على مواجهتها بفعالية. وعليه، يتمثل التساؤل الرئيسي للدراسة في الآتي:

ما التهديدات التي تفرضها جرائم الاستقطاب والتطرف، والاحتيال المصرفي، وانتهاك الملكية الفكرية، على منظومة الأمن الفكري والاقتصادي في الفضاء السيبراني؟

أهمية الدراسة

الأهمية العلمية:

تكمن الأهمية العلمية للدراسة في محاولتها سد فجوة معرفية عبر تقديم تحليل يربط بين جرائم الأمن الفكري (كالاستقطاب) وجرائم الأمن الاقتصادي (كالاحتيال) في الفضاء السيبراني ضمن إطار مفاهيمي موحد.

الأهمية التطبيقية:

أما الأهمية التطبيقية، فتتمثل في إمكانية أن تقدم نتائجها رؤى مفيدة لصناع القرار والجهات التشريعية والأمنية والتقنية، للمساهمة في تطوير استراتيجيات مواجهة أكثر فاعلية لهذه التهديدات المستجدة.

أهداف الدراسة

يكمن الهدف الرئيسي لهذه الدراسة في الكشف عن طبيعة وأبعاد التهديدات التي تفرضها جرائم الاستقطاب والتطرف، والاحتيال المصرفي، وانتهاك الملكية الفكرية، على منظومة الأمن الفكري والاقتصادي في الفضاء السيبراني. وتنبتق عن هذا الهدف الرئيسي، الأهداف الفرعية التالية:

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

- تحليل الأساليب التقنية والنفسية التي تستخدمها حركات التطرف في عمليات الاستقطاب الفكري عبر الإنترنت.
- رصد أثر التحول الرقمي في القطاع المالي على طبيعة وحجم جرائم الاحتيال المصرفي.
- تحديد أبرز التحديات القانونية المستجدة التي تواجه حماية حقوق الملكية الفكرية في البيئة الرقمية.
- تقييم مدى فاعلية الأطر التشريعية الحالية في مواجهة الأشكال الجديدة للجرائم السيبرانية والمساهمة في بناء فضاء سيبراني آمن.

تساؤلات الدراسة

للإجابة على مشكلة الدراسة، والحالات الرئيسية التي يركز عليها البحث، يكون التساؤل الرئيسي للدراسة هو: ما التهديدات التي تفرضها جرائم الاستقطاب والتطرف، والاحتيال المصرفي، وانتهاك الملكية الفكرية، على منظومة الأمن الفكري والاقتصادي في الفضاء السيبراني؟ وتنبثق عن هذا التساؤل الرئيسي، التساؤلات الفرعية التالية:

س1 ما أبرز الأساليب التقنية والنفسية التي تستخدمها حركات التطرف في عمليات الاستقطاب الفكري عبر الإنترنت؟

س2 كيف أثر التحول الرقمي في القطاع المالي على طبيعة وحجم جرائم الاحتيال المصرفي؟

س3 ما التحديات القانونية المستجدة التي تواجه حماية حقوق الملكية الفكرية في البيئة الرقمية؟

س4 ما مدى فاعلية الأطر التشريعية الحالية في مواجهة الأشكال المستجدة للجرائم السيبرانية والمساهمة في بناء فضاء سيبراني آمن؟

تعريفات مصطلحات الدراسة

يعكس التاريخ التشريعي لمواجهة الجرائم الاتصالية مساراً تدريجياً بدأ في الدول الغربية، حيث كانت السويد سباقة بإصدار قانون خاص عام 1973م، تلتها الولايات المتحدة (1976م) وبريطانيا (1981م). وانتقلت هذه الجهود لاحقاً إلى المنطقة العربية، حيث برزت تشريعات مبكرة كنظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية (2007م) والقانون الاتحادي في الإمارات العربية المتحدة (2006م)، مما يوضح الاهتمام المتزايد بهذه الظاهرة على المستوى العالمي (العمر، 2012).

وتُعرف الجرائم الاتصالية بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات" ¹¹ وتتميز هذه الجرائم بخصائص عدة أبرزها أنها عابرة للحدود، وصعبة الإثبات لعدم تركها أثراً مادياً، ويسهل فيها إخفاء الأدلة ¹² إذ تستهدف هذه الجرائم بشكل أساسي الأموال الشخصية والمؤسسية، والمعلومات والبيانات التجارية، والملكية الفكرية، بالإضافة إلى المواقع الإلكترونية وأخلاقيات المجتمع ¹³، وبناء على ذلك يعرفها الباحث إجرائياً بأنها: كافة الأفعال غير المشروعة التي تُرتكب عبر الفضاء السيبراني، وتهدد منظومة الأمن الفكري والاقتصادي، وتتمثل في هذه الدراسة من خلال نماذجها الرئيسية المتمثلة في جرائم الاستقطاب والتطرف، والاحتيال المصرفي، وانتهاك الملكية الفكرية.

الدراسات السابقة

يستعرض الباحث في هذا الجزء أحدث الأدبيات العلمية التي تناولت جوانب متعددة من الجرائم السيبرانية وتأثيراتها على الأمن الفكري والاقتصادي، تمهيداً لتحديد فجوة البحث التي تسعى هذه الدراسة لمعالجتها، وسيقوم الباحث بترتيبها من الأحدث إلى الأقدم، وهي على النحو الآتي:

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

هدفت دراسة (Evans et al., 2025) إلى تقييم فاعلية أنظمة كشف الاحتيال المعتمدة على الذكاء الاصطناعي في الخدمات المصرفية الرقمية، مع دراسة آثارها الأخلاقية، وقد اعتمدت الدراسة على تصميم بحثي مختلط يجمع بين التحليل الكمي لنماذج تعلم الآلة والتحليل الكيفي للمقابلات مع الخبراء، وكشفت النتائج أن الأنظمة المعتمدة على الذكاء الاصطناعي تفوقت بشكل كبير على الأنظمة التقليدية، حيث حققت دقة تصل إلى 97.5%، وقللت من الإنذارات الكاذبة بنسبة 30%. وخلصت الدراسة إلى أنه رغم هذه الفاعلية، فإن هناك تحديات أخلاقية تتعلق بخصوصية البيانات والتحيز الخوارزمي، وأوصت بضرورة تبني استراتيجيات للتخفيف من هذا التحيز واستخدام تقنيات الذكاء الاصطناعي التي تحافظ على الخصوصية.

وسعت دراسة (يوسفي ومسعودي، 2024) إلى استكشاف مساهمة الأمن السيبراني في تعزيز الأمن الفكري، واعتمدت الدراسة على منهج تحليلي شامل للمقالات العلمية والتقارير الحكومية، وكشفت نتائجها أن الأمن السيبراني يؤدي دوراً حيوياً في حماية البيانات والمعلومات الحساسة، ويوفر الإطار القانوني والتقني لمكافحة الجرائم السيبرانية، وخلصت الدراسة إلى أن تبني استراتيجيات الأمن الفكري المناسبة يمكّن من تقليل التهديدات السيبرانية وتحقيق الثقة في العالم الرقمي.

وتناولت دراسة (فاخر، 2024) العلاقة بين الاستغراق في المحتوى الرقمي وحدوث الاستقطاب السياسي والعاطفي، واستخدمت الدراسة منهج المسح، بتطبيق استبيان على عينة قصدية مكونة من 180 فرداً من بغداد، وأظهرت النتائج أن السلوك الرقمي للشخص المنغمس في المحتوى يدفعه للبقاء لمدة طويلة مع محتويات محددة، وأن من تداعيات هذا الاستقطاب هو تكوين نظرة سلبية تجاه زعماء الأحزاب الأخرى، وأوصت الدراسة بشكل ضمني بضرورة فهم آليات حدوث الاستقطاب لتجنب أضراره والانقسام الاجتماعي.

وهدفت دراسة (منخرفيس، 2023) إلى تحليل الجرائم الإلكترونية ذات الأبعاد الاجتماعية والأخلاقية عبر مواقع التواصل الاجتماعي، واعتمدت الدراسة على المنهج الوصفي التحليلي، وكشفت نتائجها أن استغلال مواقع التواصل أدى لانتشار جرائم تمس الأفراد وسمعتهم كالسب والقذف وانتحال الشخصية، ولها آثار خطيرة على الضحية والمجتمع، وأوصت الدراسة بتفعيل قوانين ردع صارمة، والرقابة الأسرية، وتكثيف حملات التوعية الإعلامية.

وتناولت دراسة (القاضي، 2023) ظاهرة التسول الإلكتروني كنموذج للجريمة الاقتصادية المستحدثة، واعتمدت الدراسة على المنهج الوصفي التحليلي، بتطبيق استبيان على عينة عشوائية مكونة من 72 فرداً، وكشفت نتائجها أن أغلبية العينة تعتبر التسول الإلكتروني نمطاً جديداً من الاحتيال وليس قضية تستدعي التضامن العاطفي، وأوصت الدراسة بضرورة تدخل المشرع لتعديل قانون الجريمة الإلكترونية، وإدراج "التسول الإلكتروني" بشكل صريح ضمن السلوكيات الإجرامية، مع الاستفادة من التجارب التشريعية الدولية والعربية في هذا المجال.

وهدفت دراسة (عبد الرحمن، 2022) إلى الكشف عن أبرز مهددات الأمن الفكري في المجتمع الرقمي، واعتمدت الدراسة على المنهج الوصفي التحليلي، بتطبيق استبيان على عينة مكونة من 150 مفردة من أعضاء هيئة التدريس بجامعة الفيوم، وتوصلت الدراسة إلى أن الشائعات والتطرف الفكري وخطاب الكراهية هي من أهم الظواهر التي تهدد الأمن الفكري، وأوصت الدراسة بضرورة عودة مؤسسات التنشئة الاجتماعية للقيام بأدوارها، إلى جانب قيام المؤسسات الأمنية بملاحقة أصحاب الأفكار الهدامة.

وسعت دراسة (الحوامدة، 2022) إلى تحليل جريمة الإرهاب الإلكتروني في التشريعات الجنائية بشكل مقارن، واعتمدت الدراسة على المنهج الوصفي التحليلي والمقارن للنصوص

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

القانونية، وكشفت نتائجها عن وجود قصور في التشريعات الحالية التي تخلط بين الإرهاب التقليدي والإلكتروني، وأوصت الدراسة بضرورة إيجاد تشريع مستقل لمكافحة الإرهاب الإلكتروني واستحداث مركز عربي متخصص في هذا المجال.

وهدف دراسة (الدبس، 2022) إلى التعرف على علاقة إدارة الأمن السيبراني بالحد من الجرائم الإلكترونية، واعتمدت الدراسة على منهج المسح، بتطبيق استبيان على عينة من 24 عاملاً في مركز الأمن السيبراني بالأردن، وكشفت نتائجها عن وجود علاقة إيجابية بين إدارة الأمن السيبراني والحد من الجرائم، وأوصت الدراسة بزيادة الأبحاث المتعلقة بهذا الموضوع لقلتها.

وسعت دراسة (شحاته، 2020) إلى تحليل مضامين الجريمة عبر مواقع التواصل الاجتماعي ورصد انعكاساتها النفسية والاجتماعية على الشباب، واعتمدت الدراسة على منهج المسح، بتطبيق استبيان على 150 شاباً بالإضافة إلى عقد مجموعة نقاش بؤرية، وكشفت الدراسة أن التعرض لمضامين الجريمة قد يثير مشاعر القلق والخوف، ولكنه في المقابل قد يدفعهم لاتخاذ الحيطة والحذر والابتعاد عن المواقف التي قد تسبب وقوع الجريمة، مما يساهم في نشر الوعي الأمني بينهم.

وهدف دراسة (بلحسين ومالكي، 2020) إلى تحليل التحديات التي تواجه حقوق المؤلف في حماية المصنفات الرقمية عبر شبكة الإنترنت، واعتمدت الدراسة على المنهج الوصفي التحليلي للقوانين والاتفاقيات الدولية، وكشفت نتائجها أن البيئة الرقمية قد طرحت تهديدات جديدة لحقوق المؤلف بسبب سهولة القرصنة، وأوصت الدراسة بضرورة الدمج بين التشريعات الحديثة والتدابير التقنية المتقدمة.

وتناولت دراسة (مطر، 2018) إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية، واعتمدت الدراسة على المنهج التحليلي للنصوص القانونية، وأظهرت نتائجها الصعوبات الكبيرة التي تواجه التحقيق في هذه الجرائم، مثل سهولة محو الأدلة الرقمية، وأوصت الدراسة بضرورة إصدار تشريع خاص ومستقل للجرائم الإلكترونية وإنشاء هيئات تحقيق متخصصة.

التعليق على الدراسات السابقة

من خلال استعراض الدراسات السابقة، يتضح وجود اهتمام بحثي متنوع بمعالجة هذه الظواهر، وينعكس هذا التنوع في تعدد المناهج العلمية المستخدمة، فقد اعتمد عدد من الباحثين على المنهج الميداني باستخدام الاستبيان للوصول إلى نتائج كمية، حيث تنوعت العينات لتشمل الأكاديميين كما في دراسة (عبد الرحمن، 2022)، والجمهور العام كما في دراسة (فاخر، 2024)، وعينات من الشباب والجمهور العام كما في دراسات (شحاته، 2020) و (القاضي، 2023)، بالإضافة إلى عينة متخصصة من العاملين في الأمن السيبراني كما في دراسة (الدبس، 2022). وفي المقابل، اتجهت دراسات أخرى إلى المنهج التحليلي النظري لدراسة الأبعاد القانونية والإجرائية، وذلك بتحليل النصوص التشريعية والاتفاقيات الدولية كما في دراسات (يوسف ومسعودي، 2024)، (الحوامدة، 2022)، (بلحسين ومالكي، 2020)، (منخرفيس، 2023)، و (مطر، 2018)، ورغم هذا الثراء المنهجي والتنوع في العينات، تكمن فجوة البحث الحالية في ندرة الدراسات التي تتعامل مع هذه التهديدات كمنظومة واحدة ومتربطة، فالغالبية العظمى من الدراسات تتناول جانباً واحداً من المشكلة (فكرياً، أو اقتصادياً، أو قانونياً) دون التعمق في تقاطعاته مع الأبعاد الأخرى للمشكلة البحثية، لذلك، تسعى هذه الدراسة لسد هذه الفجوة عبر تقديم قراءة تحليلية موحدة تربط بين هذه الجرائم المختلفة تحت مظلة الأمن الفكري والاقتصادي في الفضاء السيبراني.

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

منهجية الدراسة

تعتمد هذه الدراسة على المنهج النوعي لتحقيق هدفها الرئيس، حيث تم تطبيق هذا المنهج من خلال استخدام الأسلوب الوصفي التحليلي الذي يعتمد على استقراء الأدبيات العلمية والأبحاث السابقة المتعلقة بالجرائم الاتصالية وتأثيراتها، ووصف الظواهر المختلفة المرتبطة بها، ثم تحليلها بشكل نقدي لربطها بالإطار المفاهيمي للدراسة المتمثل في "الأمن الفكري والأمن الاقتصادي"، كما تم الاعتماد على أسلوب "دراسة الحالة" من خلال التركيز على ثلاثة نماذج رئيسية هي: الاستقطاب الفكري، والاحتيال المصرفي، وانتهاك الملكية الفكرية، وذلك لتحليل أبعادها المختلفة وتقديم رؤية متكاملة حولها.

دراسة الحالات

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها، سيقوم الباحث في هذا الجزء بتحليل ثلاث حالات رئيسية كنماذج علمية، تمثل كل منها أحد الأبعاد الرئيسية للتهديدات التي تواجه الأمن الفكري والاقتصادي في الفضاء السيبراني، وهي على النحو الآتي:

■ الاستقطاب الفكري في البيئة الرقمية

تُعزى خطورة البيئة الرقمية إلى مجموعة من الخصائص المتأصلة فيها؛ فهي بطبيعتها لا تخضع للرقابة التقليدية، وتتميز بنموها السريع، ويضاف إلى ذلك الكم الهائل من المعلومات المتاحة من مصادر متعددة لا يمكن التحكم فيها أو متابعتها¹⁴، كما أن قدرة هذه الشبكة على تجاوز الحدود الجغرافية وتوفير ميزة التخفي وإخفاء هوية المستخدمين، يجعل منها بيئة خصبة للمؤثرات الفكرية التي قد تؤدي إلى الانحراف الفكري¹⁵، وفي هذا الفضاء، وجدت حركات التطرف أدوات فعالة، حيث تسعى لبناء منظومة من القناعات الفكرية وبث الكراهية والترويج للأفكار الإجرامية، وتشويه صورة من يعارض فكرها¹⁶. وعلى الجانب الآخر، ظهرت تيارات تدعو للتحرر من القيود الدينية والاجتماعية، وتسعى للتمرد على الواقع عبر المطالبة

بالحرية المطلقة¹⁷، وقد استغلت هذه الحركات التطور التكنولوجي في التعبئة والتجنيد والتمويل، وإنشاء "مراكز تدريب رقمية" تقدم مواداً عن الأسلحة وصناعة المتفجرات، وتوفر للمجندين ميزة التخفي عن أعين السلطات¹⁸، حيث تطورت هذه الأساليب بشكل كبير، فبعد أن كان الاعتماد على إنشاء وتصميم مواقع إلكترونية لنشر الأفكار والتلقين الإلكتروني (جعفر، 2013)؛ أصبحت التنظيمات الإرهابية الحديثة تستغل منصات التواصل الاجتماعي بشكل احترافي. وتعمل هذه الجماعات بشكل أساسي على التأثير النفسي، إذ تستهدف إحداث ما يُعرف بـ "الانغماس في المحتوى الرقمي"، وهو ما يؤدي بدوره إلى "الاستقطاب العاطفي"، بحيث يكون الفرد المنغمس في هذا المحتوى نظرة سلبية وعدائية تجاه مخالفه في الرأي (فاخر، 2024)، كما تستغل هذه الجماعات تعاطف المستخدمين وتجذب الشباب بعبارات حماسية ومؤثرة، خاصة عبر غرف الدردشة والمنصات التفاعلية (فاهد، 2012)، مما يترك انعكاسات نفسية واجتماعية خطيرة عليهم (شحاته، 2020). وفي النهاية، يمكن القول إن الإرهاب الإلكتروني يُمارس من خلال ما يسمى بـ "القوى الرمزية اللينة" التي تعمل بال جذب والترغيب لا بالقوة، بهدف انتزاع الإرادة الجماعية وزرع الآراء (الطائي، 2010). وبهذا، يتضح أن الاستقطاب الفكري عبر الفضاء السيبراني لا يمثل مجرد خلاف في الآراء، بل قد يشكل تهديداً منظماً وممنهجاً للأمن الفكري والتماسك الاجتماعي (عبد الرحمن، 2022؛ يوسف ومسعودي، 2024)، الأمر الذي يتطلب استراتيجيات شاملة لمواجهته، تركز على تحصين الشباب فكرياً وتوعية المجتمع بمخاطر هذا النوع من الجرائم المستحدثة.

■ الاحتيال المصرفي في البيئة الرقمية

أدى التحول الرقمي إلى إحداث تغييرات جذرية في القطاع المصرفي، وبينما وفرت التقنيات الحديثة كفاءة وسرعة غير مسبوقة، فقد فتحت الباب في الوقت ذاته أمام مخاطر جديدة تهدد استقرار المصارف والنظام المالي ككل (عواودة، 2025)، حيث يُمثل الاحتيال

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

المصرفي أحد أبرز الجرائم الاتصالية التي تهدد الأمن الاقتصادي في الفضاء السيبراني، ويشير المفهوم في أبسط صوره إلى استخدام وسائل الخداع الإلكتروني، كالرسائل المخادعة، بهدف الاستيلاء على بيانات المستخدمين المالية (العمر، 2012)، وقد تحولت منافذ الصرف وبطاقات الائتمان مع التوسع في الخدمات الرقمية إلى مراكز جذب رئيسية للأنشطة الإجرامية، التي تتسم بطابعها العابر للحدود مما يزيد من صعوبة ملاحقة مرتكبها (الطائي، 2010)، إذ تتخذ هذه الجرائم أشكالاً متعددة بدءاً من انتحال صفة جهات رسمية (الكعبي، 2009)، وصولاً إلى أنماط مستحدثة تعتمد على الهندسة الاجتماعية مثل "التسول الإلكتروني" الذي أظهرت الدراسات الميدانية أنه يُصنف كشكل من أشكال الإجرام والاحتيال (القاضي، 2023)، ومع تطور أساليب المحتالين، أصبحت أنظمة كشف الاحتيال التقليدية القائمة على القواعد (Rule-based systems) تكافح لمواكبة التهديدات المتطورة (Evans et al., 2025)، هذا القصور دفع المؤسسات المالية للتوجه نحو حلول الذكاء الاصطناعي (AI) وتعلم الآلة. وفي هذا السياق، كشفت الدراسات الحديثة عن فاعلية هذه التقنيات بشكل لافت؛ فقد أظهرت دراسة (Nair et al., 2025) أن استخدام خوارزميات تعلم الآلة المتقدمة يمكن أن يصل بدقة كشف الاحتيال (Precision) إلى نسبة 98.4%. وفي دراسة أخرى، وُجد أن الأنظمة المعتمدة على الذكاء الاصطناعي تفوقت على الأنظمة التقليدية محققة دقة تصل إلى 97.5%، مع تقليلها للإنذارات الخاطئة بنسبة 30%، إلا أنها في المقابل تثير تحديات أخلاقية جديدة تتعلق بالتحيز الخوارزمي وخصوصية البيانات (Evans et al., 2025)، وعلى الرغم من هذه القفزات التكنولوجية في "الوقاية"، لا تزال هناك تحديات إجرائية وقانونية كبيرة في مرحلة "الملاحقة"، فقد بينت دراسة (مطر، 2018) الصعوبات الكبيرة التي تواجه التحقيق في هذه الجرائم، مثل سهولة محو الأدلة الرقمية وطابعها الدولي، وأوصت بضرورة إصدار تشريعات خاصة وإنشاء هيئات تحقيق متخصصة، وهو ما يؤكد أن التطور التقني وحده لا يكفي دون مواكبة تشريعية وقضائية فعالة.

1. حقوق الملكية الفكرية في البيئة الرقمية

يمثل انتهاك حقوق الملكية الفكرية وجهاً آخر للتهديدات التي تواجه الأمن الاقتصادي في الفضاء السيبراني. فبينما نالت قوانين حماية المصنفات المطبوعة حقها من العناية، تظل الإشكالية كامنة في المصادر الإلكترونية، حيث يكتنف الغموض القوانين الخاصة بها نتيجة لتعقد ظاهرة الجرائم المعلوماتية (جمعية المكتبات والمعلومات السعودية، 2010)، وتؤكد الدراسات الحديثة أن تحولات البيئة الرقمية قد خلقت أبعاداً جديدة للاعتداء على الملكية الفكرية، مما يتطلب تحديثاً مستمراً للبنية التشريعية (الفريجي، 2020)، فقد أدت سهولة الاستنساخ غير المحدود وبلا تكلفة، والتوزيع العالمي الفوري للمصنفات الرقمية (من برامج حاسوبية وكتب وأفلام)، إلى انتشار هائل لعمليات القرصنة وانتهاك الحقوق المادية والأدبية للمؤلفين (فاهد، 2012)، وهو ما يطرح تحديات جسيمة أمام العدالة الجنائية (المطيري وآخرون، 2023)، وتعود جذور حماية الملكية الفكرية إلى ما قبل العصر الرقمي بقرون، لكن التحدي المعاصر يكمن في أن القوانين التقليدية لم تعد كافية لمواجهة هذه التهديدات المستجدة (بلحسين ومالكي، 2020)، فالنشر المفتوح على الإنترنت دون ضوابط ساهم في هدر حقوق المؤلفين، مما يستدعي إعادة النظر في القوانين الحالية (فاهد، 2012)، ويترتب على هذا الانتحال والسطو على أفكار الآخرين آثار سلبية تتجاوز الجانب المادي، لتشمل تدني مستوى التعلم وإعاقة إثراء المعرفة البشرية (العمر، 2012). ولمواجهة هذه التحديات، برز اتجاهان رئيسيان للحلول هما: الاتجاه الأول هو الحماية القانونية، عبر تحديث التشريعات الوطنية لتتوافق مع الاتفاقيات الدولية (مثل اتفاقيات منظمة "ويبو")، وتفعيل دور الهيئات الوطنية (مثل الهيئة السعودية للملكية الفكرية) في تسجيل الحقوق وإنفاذها (الفريجي، 2020)، أما الاتجاه الثاني فهو الحماية بالتقنية، حيث لم يعد من الممكن الاعتماد على القوانين وحدها، وتوصي الدراسات الحديثة بضرورة الدمج بين التشريعات المحدثه والتدابير التقنية المتقدمة كالتشفير، والتوقيع الإلكتروني، والعلامات المائية الرقمية، وأنظمة إدارة

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

الحقوق الرقمية (DRM) لضمان حماية فعالة للملكية الفكرية في العصر الرقمي (بلحسين ومالكي، 2020؛ المطيري وآخرون، 2023؛ لواعر، 2023)، وبذلك، يكمن التحدي الأبرز في هذا المجال في تحقيق التوازن الدقيق بين حماية الحقوق الحصرية للمبدعين من جهة، وبين ضمان حق المجتمع في الوصول للمعرفة وتداولها وفقاً لمبدأ الاستخدام العادل من جهة أخرى.

النتائج والمناقشة

بعد استعراض الأدبيات العلمية وتحليل الحالات الرئيسية، يتضح أن الفضاء السيبراني قد تحول بالفعل إلى ساحة صراع جديدة، لا تقتصر على المواجهات التقنية بين المؤسسات، بل تمتد لتشمل صراعات فكرية واقتصادية واسعة النطاق، فالخصائص الفريدة للبيئة الرقمية، من تجاوز للحدود وغياب للرقابة، جعلتها مسرحاً مثالياً لهذه الصراعات بدرجة تفوق البيئة التقليدية. ومن خلال التحليل، تبرز عدة استنتاجات رئيسية:

أولاً: ترابط التهديدات الفكرية والاقتصادية في البيئة الرقمية كجريمة اتصالية

إن أهم ما توصلت إليه هذه الدراسة هو أن النظر إلى جرائم الاستقطاب الفكري والاحتيال المصرفي وانتهاك الملكية الفكرية كقضايا منفصلة هو قراءة قاصرة للواقع، فالقراءة المتعمقة لهذه الحالات يوضح أنها ليست مجرد جرائم متفرقة، بل هي أوجه مختلفة لمنظومة تهديد واحدة ومتراطة تستهدف الأمن الشامل للمجتمعات. فالجماعات المتطرفة التي تمارس الاستقطاب الفكري لتهديد الأمن الفكري (عبد الرحمن، 2022؛ فاخر، 2024)، قد تستخدم نفس الأدوات والشبكات لتمويل عملياتها عبر الاحتيال المالي وانتهاك حقوق الملكية الفكرية، مهددة بذلك الأمن الاقتصادي. وبهذا، تتحول هذه الجرائم إلى "قوى رمزية لينة" تعمل على انتزاع الإرادة الجماعية وزعزعة الاستقرار (الطائي، 2010)، مما يؤكد أن حماية الفضاء السيبراني تتطلب رؤية متكاملة تعالج الأمن بشقيه الفكري والاقتصادي معاً،

وهو ما يتفق مع ما أوصت به دراسة (يوسف ومسعودي، 2024)، بضرورة بناء استراتيجية شاملة تركز على التشريع والتوعية والتدريب لتعزيز الثقة في الفضاء الرقمي.

ثانياً: الفجوة بين تطور الجرائم الاتصالية والاستجابات التشريعية والتقنية لها

يتضح وجود فجوة متزايدة بين سرعة تطور الأساليب الإجرامية وبطء وتيرة تطور الاستجابات لها، فالدراسات الحديثة كشفت عن نماذج إجرامية مستحدثة باستمرار، مثل "التسول الإلكتروني" كشكل من أشكال الاحتيال (القاضي، 2023)، والجرائم التي تمس الأخلاق والقيم الاجتماعية (منخرفيس، 2023). وفي المقابل، لا تزال الأطر التشريعية تحاول مواكبة هذا التطور، حيث أشارت دراسة (مطر، 2018) إلى الصعوبات الكبيرة في جمع الأدلة الرقمية، وأوصت دراسة (الحوامدة، 2022) بضرورة إصدار تشريعات مستقلة لمواجهة الجرائم المستجدة كالإرهاب الإلكتروني. وحتى مع وجود الحلول التقنية المتقدمة كاستخدام الذكاء الاصطناعي في كشف الاحتيال (Evans et al., 2025; Nair et al., 2025)، فإنها تفرز تحديات أخلاقية وقانونية جديدة تحتاج إلى تنظيم.

ثالثاً: اختلال توازن الاهتمام البحثي في دراسة التيارات الفكرية

يُلاحظ من خلال مراجعة الأدبيات أن التركيز البحثي ينصب بشكل كبير على الحركات المتطرفة ذات الطابع الديني أو السياسي، بينما لا تحظى التيارات الفكرية الأخرى، كالدعوات للتححر المطلق من القيم المجتمعية، بنفس القدر من الاهتمام، رغم أنها قد تشكل خطراً موازياً على التماسك الاجتماعي والأمن الفكري، وهذا يمثل فجوة بحثية تستدعي اهتمام الباحثين في المستقبل.

رابعاً: الوعي الرقمي ركيزة أساسية لمواجهة الجرائم الاتصالية

أخيراً، يتضح أن مواجهة الجرائم الاتصالية لا تعتمد فقط على الحلول الأمنية والتشريعية، بل تنطلق بشكل أساسي من المتلقي نفسه، فالشخص الذي يمتلك مهارات

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

التفكير النقدي، ويستقي معلوماته من مصادر متعددة، يكون أكثر حصانة ضد محاولات السيطرة الفكرية، وهو ما يؤكد على أن برامج التوعية وتعزيز "الوعي الرقمي" لدى الشباب والمجتمع هي حجر الزاوية في أي استراتيجية فعالة، خاصة وأن التعرض لمضامين الجريمة قد يثير القلق والخوف لدى الشباب¹⁹، مما يستدعي تحصينهم فكرياً²⁰.

الخاتمة

بناءً على ما سبق، توصي الدراسة بضرورة تبني استراتيجية شاملة لمواجهة هذه التهديدات، تركز على المسارات التالية:

أولاً: تحديث وصياغة تشريعات وقوانين متكاملة ومستقلة للجرائم الإلكترونية، تتجنب الخلط بين الجرائم التقليدية والمستحدثة، وتواكب التطورات التقنية المستمرة، مع تعزيز التعاون الدولي والإقليمي لوضع اتفاقيات موحدة تعالج الطبيعة العابرة للحدود لهذه الجرائم وتسهل عمليات الملاحقة القضائية.

ثانياً: إنشاء هيئات ووحدات تحقيق متخصصة في الجرائم الإلكترونية، وتزويدها بالكوادر البشرية المؤهلة والتقنيات اللازمة، وتشجيع المؤسسات المالية على تبني الحلول التقنية المتقدمة كأنظمة كشف الاحتيال المعتمدة على الذكاء الاصطناعي، مع وضع أطر أخلاقية وقانونية لضمان حماية خصوصية البيانات.

ثالثاً: إدراج مقررات "الوعي الرقمي" و"التفكير النقدي" ضمن المناهج التعليمية في مختلف المراحل، لتحصين الشباب ضد مخاطر الاستقطاب الفكري والاحتيال، بالإضافة إلى تكثيف حملات التوعية الإعلامية الموجهة لكافة شرائح المجتمع لتوضيح مخاطر الجرائم الاتصالية وكيفية حماية البيانات الشخصية.

رابعاً: دعوة المؤسسات الأكاديمية ومراكز الأبحاث إلى تكثيف الدراسات البينية التي تتناول الجرائم الاتصالية من منظور متكامل، وتشجيع الأبحاث التي تربط بين مهددات الأمن الفكري

والأمن الاقتصادي، لسد الفجوة المعرفية الحالية وتقديم رؤى أعمق تساعد في بناء استراتيجيات مواجهة أكثر شمولية وفاعلية.

خامساً: تشكيل لجان وطنية أو هيئات استشارية مشتركة تضم خبراء من القطاعات الأمنية، والقانونية، والتقنية، بالإضافة إلى ممثلين عن القطاع الخاص والمجتمع المدني، بحيث يكون الهدف من هذه اللجان هو بناء استراتيجية وطنية موحدة ومستدامة للأمن السيبراني، تضمن التنسيق بين الجهات المختلفة، وتعمل على تقييم المخاطر بشكل دوري، وتطوير حلول عملية تتناسب مع خصوصية كل مجتمع.

المراجع

2. إبراهيم، خالد. (2008). أمن الجريمة الإلكترونية (الطبعة الأولى). الدار الجامعية. البقمي، ناصر. (2009). أثر التحول إلى مجتمع معلوماتي على الأمن الفكري. في المؤتمر الوطني الأول للأمن الفكري: المفاهيم والتحديات. كرسي الأمير نايف بن عبدالعزيز لدراسات الأمن الفكري، جامعة الملك سعود، الرياض.
3. بلحسين، فاطمة الزهراء، ومالكي، طارق. (2020). حقوق المؤلف وحماية مصنفااته الرقمية في شبكة الإنترنت. في المؤتمر الدولي المحكم: الملكية الفكرية على المؤلفات (ص. 55-87). مركز جيل للبحث العلمي.
4. جعفر، علي. (2013). جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة (الطبعة الأولى). منشورات زين الحقوقية. جمعية المكتبات والمعلومات السعودية. (2010). الأمن المعلوماتي (الطبعة الأولى). مكتبة الملك فهد الوطنية. الحوامة،

الجرائم الاتصالية في الفضاء السيبراني: دراسة نوعية تحليلية لجرائم الاستقطاب والتطرف، الاحتيال المصرفي، وانتهاك الملكية الفكرية

5. الحوامدة، لورنس سعيد. (2022). جريمة الإرهاب الإلكترونية في التشريعات الجنائية: دراسة تحليلية مقارنة. مجلة كلية الشريعة والقانون، 24(1)، 469-506.
6. الدبس، هاني ضيف الله. (2022). علاقة إدارة الأمن السيبراني بالحد من الجرائم الإلكترونية من وجهة نظر العاملين لدى مركز الأمن السيبراني. مجلة المشكاة للعلوم الإنسانية والاجتماعية، 9(2)، 415-451.
7. شحاته، أحمد. (2020). مضامين الجريمة عبر مواقع التواصل الاجتماعي وانعكاساتها النفسية والاجتماعية على الشباب. المجلة العربية لبحوث الإعلام والاتصال، 31(3)، 548-591.
8. صلاح، مها. (2010). استراتيجية الاتصال في مواقع الجماعات المتطرفة على شبكة الأنترنت. في ندوة استعمال الأنترنت في تمويل الإرهاب وتجنيد الإرهابيين. جامعة نايف العربية للعلوم الأمنية وجامعة القاهرة، الرياض. الطائي، جعفر. (2010). جرائم تكنولوجيا المعلومات: رؤية جديدة للجريمة الحديثة (الطبعة الأولى). دار البداية ناشرون وموزعون.
9. عبد الرحمن، إصلاح عبد الناصر. (2022). الأمن الفكري في المجتمع الرقمي: نحو هندسة اجتماعية بناءة. مجلة كلية الآداب، جامعة الفيوم، 14(2)، 1542-1604.
10. العمر، معن. (2012). جرائم مستحدثة (الطبعة الأولى). دار وائل للنشر والتوزيع. عواودة، ماريه وصفي. (2025). إدارة المخاطر المصرفية في ظل التحول الرقمي. مجلة رماح للبحوث والدراسات، 116(2)، 550-568.
11. فاخر، علي. (2024). الاستقطاب العاطفي وعلاقته بالاستغراق بالمحتوى الرقمي Lark Journal، 16(4)، 503-535.
12. فاهد، عبدالله. (2012). مكافحة الجرائم المعلوماتية (الطبعة الأولى). مطابع الحميضي. الفريجي، رياض بن ناصر. (2020). تحولات البيئة الرقمية في مجتمع المعرفة وانعكاساتها على حقوق الملكية الفكرية بالمملكة العربية السعودية. المجلة المصرية لبحوث الاتصال الجماهيري، 1(1)، 230-260.
13. القاضي، نادية. (2023). التسول الإلكتروني في الجزائر بين استقطاب التضامن الاجتماعي ومؤشرات الاحتيال الافتراضي. مجلة العلوم الإنسانية والاجتماعية، 9(2)، 236-254.
14. الكعبي، محمد. (2009). الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت (الطبعة الثانية). دار النهضة العربية. لواعر، فاطمة. (2023). الملكية الفكرية في البيئة الرقمية. مجلة الحوكمة والقانون الاقتصادي، 7-31.
15. مطر، حسين خليل. (2018). إجراءات التحقيق وجمع الأدلة في الجرائم الإلكترونية. مجلة الكوفة للعلوم القانونية والسياسية، 11(36)، 395-410.

16. المطيري، أنوار رفاع، وعبد الجواد، سامح زينهم، والليثي، هدى عبد الباسط. (2023). الملكية الفكرية في العصر الرقمي. مجلة بنها للعلوم الإنسانية، 2(3)، 15-34 .
17. منخرفيس، يمينة. (2023). الجرائم الالكترونية عبر مواقع التواصل الاجتماعي ذات الأبعاد الاجتماعية والأخلاقية. مجلة الحقوق والعلوم الإنسانية، 16(1)، 1299-1313 .
18. المويشر، تركي. (2009). بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته [أطروحة دكتوراه غير منشورة]. جامعة نايف العربية للعلوم الأمنية. يوسف، سفيان، ومسعودي، كلثوم. (2024). الأمن الفكري وتحديات الأمن السيبراني: دراسة نظرية. مجلة الباحث، 16(2)، 647-668.
19. Evans, G., Blues, J., John, A., & Chans, P. (2025). AI-Powered Fraud Detection and Prevention in Digital Banking: Evaluating the Effectiveness and Ethical Implications. Article.
20. Nair, S. S., Lakshmikanthan, G., Belagalla, S., Ahmad, S. K., Belagalla, N., & Farooqi, S. A. (2025). Leveraging AI and Machine Learning for Enhanced Fraud Detection in Digital Banking System: A Comparative Study. In 2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT) (pp. 1278-1282).