Journal DOI: https://doi.org/10.64184

Journal Email: info@ashurjournal.com

Journal home page: https://ashurjournal.com/index.php/AJLPS/about

This journal is open access & Indexed in

IRAQI Academic Scientific Journals | Google الباحث العلمي | Crossref

Article Info.	
Sections: Law.	**Received: 2025 July 4**
Accepted: 2025 July 29	**Publishing: 2025** September **1**

Self-Cybercrime and Cybersecurity

Mohammed Zaidoun Khalaf Jabbar, Dr. Haider Ghazi Faisal

Al-Mustansiriya University

mohammed.zd@uomustansiriyah.edu.iq, l1121194@uomustansiriyah.edu.iq

Abstract

This study focuses on the problem of conceptual confusion between digital crimes and traditional and economic crimes on the one hand, and between cybersecurity, information security and digital privacy on the other hand, a confusion that results in a lack of understanding of the legal nature of these phenomena and a lack of clarity in the mechanisms to confront them. The importance of this study is manifested in its scientific aspect by contributing to the control of terminology and identifying the essential differences between them in order to enhance the theoretical construction in criminal jurisprudence, and in its practical aspect by guiding the legislator and decision makers towards the development of legislation more accurate and appropriate to the nature of the digital environment.

The study adopted the descriptive analytical approach by extrapolating legal texts and doctrinal opinions and analyzing them in the light of contemporary technical developments. The results concluded that digital crimes represent an independent criminal phenomenon with a special technical environment, while cybersecurity remains a broad preventive framework that differs in content from information security and digital privacy, which requires the formulation of precise legislative treatments to accommodate these differences and achieve integrated protection of digital security.

Key words: Digital crimes, Cyber security, Traditional crimes, Economic crimes Information security, Digital privacy.

DOIالمجلة : https://doi.org/10.64184

ايميل المجلة: info@ashurjournal.com

رابط الصفحة الرئيسية للمجلة: https://ashurjournal.com/index.php/AJLPS/about

هذه المجلة مفتوحة الوصول و جميع البحوث مفهرسة في هذه

Crossref Google الباحث العلمي IRAQI Academic Scientific Journals

معلومات البحث	
تاريخ الاستلام: ٤ يوليو ٢٠٢٥	القسم: القانون
تاريخ القبول: ٢٩ يوليو ٢٠٢٥	تاريخ النشر: ١ سبتمبر ٢٠٢٥

ذاتية الجرائم الرقمية والامن السيبراني

محمد زيدون خلف جبار، د. حيدر غازي فيصل

الجامعة المستنصرية

l1121194@uomustansiriyah.edu.iq، mohammed.zd@uomustansiriyah.edu.iq

الملخص

تتمحور هذه الدراسة حول إشكالية الخلط المفاهيمي بين الجرائم الرقمية والجرائم التقليدية والاقتصادية من جهة، وبين الأمن السيبراني وأمن المعلومات والخصوصية الرقمية من جهة أخرى، وهو خلط يترتب عليه قصور في فهم الطبيعة القانونية لهذه الظواهر وعدم وضوح في آليات مواجهتها. وتتجلى أهمية هذه الدراسة في جانبها العلمي من خلال الإسهام في ضبط المصطلحات وتحديد الفوارق الجوهرية بينها بما يعزز البناء النظري في الفقه الجنائي، وفي جانبها العملي من خلال توجيه المشرع وصناع القرار نحو وضع تشريعات أكثر دقة وملائمة لطبيعة البيئة الرقمية.

وقد اعتمدت الدراسة المنهج الوصفي التحليلي عبر استقراء النصوص القانونية والآراء الفقهية وتحليلها في ضوء التطورات التقنية المعاصرة. وخلصت النتائج إلى أن الجرائم الرقمية تمثل ظاهرة إجرامية مستقلة ذات بيئة تقنية خاصة، بينما يظل الأمن السيبراني إطارًا وقائيًا واسعًا يختلف في مضمونه من أمن المعلومات والخصوصية الرقمية، الأمر الذي يستدعي صياغة معالجات تشريعية دقيقة تستوعب هذه الفوارق وتحقيق حماية متكاملة للأمن الرقمي.

الكلمات المفتاحية: الجرائم الرقمية، الامن السيبراني، الجرائم التقليدية، الجرائم الاقتصادية، امن المعلومات، الخصوصية الرقمية.

المقدِّمـة

أولا: التعريف بموضوع البحث

يشهد العالم المعاصر تحولًا عميقًا بفعل الثورة الرقمية، إذ أصبح الفضاء السيبراني جزءً لا يتجزأ من مختلف الأنشطة الاقتصادية والاجتماعية والسياسية. ومع هذا التطور برزت الجرائم الرقمية بوصفها شكلًا جديدًا من الجريمة، يختلف عن الجرائم التقليدية من حيث أدوات التنفيذ وبيئة ارتكابها ونتائجها. وقد تناول البحث في أحد أقسامه موضوع تمييز الجرائم الرقمية عن الجرائم التقليدية، من خلال بيان أوجه التشابه المتمثلة بالقصد الجنائي والضرر المترتب، وأوجه الاختلاف التي تتعلق بعنصر المكان والزمان والأثر المادي وأساليب التنفيذ والأدوات والقوانين المطبقة. كما تناول البحث جانبًا آخر يخص المقارنة بين الجرائم الرقمية والجرائم الاقتصادية، حيث أبرزت أوجه التشابه بينهما كالارتباط بالدوافع الاقتصادية والتأثير المالي والاستفادة من التكنولوجيا، مقابل أوجه الاختلاف من حيث الزمان والمكان وأساليب التنفيذ والأدوات القانونية المستخدمة في المعالجة.

وفي جانب آخر، ركز البحث على موضوع الأمن السيبراني بعدّهِ خط الدفاع الأول ضد التهديدات الرقمية، إذ تم التمييز بينه وبين أمن المعلومات من خلال بيان نقاط الالتقاء مثل حماية البيانات وإدارة المخاطر، إلى جانب أوجه الاختلاف التي تتعلق بالنطاق والأهداف والأدوات. كما تطرقت الدراسة إلى التمييز بين الأمن السيبراني والخصوصية الرقمية، مبينة أن الأول يرتبط بحماية الأنظمة والبنى التحتية الرقمية من الهجمات، بينما الثانية تتمحور حول حماية الحقوق الفردية والبيانات الشخصية ومنع استغلالها. وبذلك، فإن البحث يسعى إلى تقديم رؤية شاملة لخصائص الجرائم الرقمية والأمن السيبراني وما يتقاطع معهما من مفاهيم أخرى، من خلال تحليل أوجه التشابه والاختلاف بشكل يعزز الفهم القانوني والعملي لهذه الظواهر المستحدثة.

ثانيا: أهمية البحث:

تبرز أهمية موضوع البحث من جانبين رئيسيين:

أ: الأهمية العلمية

تتجلى الأهمية العلمية للبحث في تسليط الضوء على التمييز بين الجرائم الرقمية والجرائم التقليدية، والجرائم الاقتصادية، مع بيان أوجه التشابه والاختلاف. كما توضح الدراسة الاختلاف بين الأمن السيبراني وأمن المعلومات والخصوصية الرقمية، بما يساهم في إثراء المعرفة القانونية والأكاديمية حول هذه المفاهيم المتداخلة، وتوضيح أبعادها النظرية والعملية في البيئة الرقمية.

ب: الأهمية العملية

تظهر الأهمية العملية للبحث من خلال المساهمة في توعية المشرعين وأجهزة إنفاذ القانون بأهمية وضع أطر قانونية وتشريعية متخصصة للتعامل مع الجرائم الرقمية والتهديدات السيبرانية. كما تتيح نتائج البحث لمتخذي القرار والمهنيين في المجال الأمني فرص تطوير استراتيجيات فعالة لمكافحة الجرائم الرقمية وحماية البيانات والأنظمة، بما يضمن تعزيز الأمن الوطني والمجتمعي.

ثالثا: اشكالية البحث

تكمن إشكالية البحث في غياب وضوح كاف في التمييز بين الجرائم الرقمية والجرائم التقليدية والجرائم الاقتصادية من جهة، وبين الأمن السيبراني وأمن المعلومات والخصوصية الرقمية من جهة أخرى، وهو ما يستدعي الوقوف على خصائص كل منها وبيان الفوارق الجوهرية فيما بينها.

رابعا: أهداف البحث

يهدف بحثنا عن موضوع الذاتية للجرائم الرقمية والأمن الأمن السيبراني إلى تحقيق أهداف عدة ومنها:

١. تمييز الجرائم الرقمية عن الجرائم التقليدية.

٢. تمييز الجرائم الرقمية عن الجرائم الاقتصادية.

٣. تمييز الأمن السيبراني عن أمن المعلومات.

٤. تمييز الأمن السيبراني عن الخصوصية الرقمية.

خامسا: منهجية البحث

اعتمد البحث على المنهج الوصفي التحليلي، عبر تحليل النصوص والآراء المتعلقة بالجرائم الرقمية والأمن السيبراني ومقارنتها بالجرائم التقليدية والاقتصادية وأمن المعلومات والخصوصية الرقمية.

سادسا: هيكلية البحث:

إن دراسة هذا الموضوع تفرض علينا ان نتناول الموضوع ضمن خطة بحثية مكونة من مبحثين, نتكلم في المبحث الاول عن موضوع ذاتية الجرائم الرقمية, ضمن مطلبين, نتكلم في المطلب الأول عن موضوع تمييز الجرائم الرقمية من الجرائم التقليدية, ونتناول في المطلب الثاني موضوع تمييز الجرائم الرقمية من الجرائم الاقتصادية.

أما في المبحث الثاني سوف يكون لموضوع ذاتية الأمن السيبراني, ضمن مطلبين, نتكلم في المطلب الأول عن تمييز الأمن السيبراني من أمن المعلومات, ويكون المطلب الثاني مخصص لموضوع تمييز الامن السيبراني من الخصوصية الرقمية.

المبحث الاول : ذاتية الجرائم الرقمية

أصبحت الرقمنة (التحول الرقمي) من الأمور الجوهرية في جميع المعاملات الاقتصادية والاجتماعية والأمنية، والكثير من التعاملات بشكل عام، سواء أكان على المستوى المحلي أو على المستوى الدولي، وأصبح أمر تفرضه الحداثة والتقدم الذي يجب الأخذ به لمن أراد أن يواكب التقدم العالمي، بل إن دول العالم باتت تتسابق في التطبيقات الرقمية، والتحول من الأساليب التقليدية إلى الأساليب الرقمية، وعندما سادت الثورة التكنولوجية الرقمية وباتت محلا لتطبيقات إنهاء المعاملات التجارية وغيرها واستخدمت على نطاق واسع في إدارة المؤسسات والهيئات والحكومات، ظهر للعالم مفهوم جديد للجرائم بشكل عام[١]، وجرائم السرقات والتلصص والابتزاز والتسول والنصب والاحتيال والتهديدات والتشهير بشكل خاص تعارف العالم أن يطلق عليها اسم الجرائم الرقمية وهذه الجرائم شملت كل القطاعات من دون استثناء سواء الاقتصادية أو الأمنية مثلها مثل الجرائم التقليدية، ومع ظهور هذا النوع من الجرائم ظهرت معه أساليب حديثة لمكافحتها ومحاربتها عند الفشل في منعها ، وأصبحت الجرائم الرقمية، لا تستخدم من قبل عقول إجرامية مخربة فقط بل امتدت لتستخدمها منظمات وهيئات من أجل الوصول لتحقيق أهدافها، وكذلك أصبحت أداء تستخدمها دول للتأثير على دول أخرى وإخضاعها لسطوتها وسيطرتها، حتى أصبحت أداة من أدوات الحروب الحديثة [٢].

(١) أحمد حسن أبو الحسن، مدى تأثير الرقمنة على خطورة الجرائم الاقتصادية، بحث منشور في مجلة جامعة أسوان للعلوم الإنسانية، المجلد (٤)، العدد (١)، كلية الحقوق – جامعة أسوان، ٢٠٢٤، ص٢٤.

(٢) أحمد حسن أبو الحسن ، مصدر سابق، ص٢٤.

وعلى ضوء ما تقدم، تُعدُّ الجرائم الرقمية من المواضيع القانونية الحديثة والمعقدة التي تكتسب أهمية متزايدة مع التطور السريع للتكنولوجيا وانتشار الإنترنت في جميع جوانب الحياة اليومية. وقد أسهم هذا التطور في ظهور نوع جديد من الجرائم يتميز بخصائص وسمات تختلف عن الجرائم التقليدية والجرائم الاقتصادية. لذا إن دراسة ذاتية الجرائم الرقمية تسعى إلى فهم هذه الخصائص وتوضيح كيفية تمييز هذه الجرائم من الأنواع الأخرى، وهو ما سنوضحه في هذا المبحث إذ سنميز الجرائم الرقمية من الجرائم التقليدية فضلًا عن تمييزها من الجرائم الاقتصادية وكلً منهما في مطلب مستقل وبحسب الآتي:

المطلب الأول: تمييز الجرائم الرقمية من الجرائم التقليدية

تُعدُّ الجرائم الرقمية من الظواهر الحديثة التي برزت نتيجة للتطور التكنولوجي وانتشار الإنترنت، وتتميز بخصائص تجعلها تختلف بشكل جذري عن الجرائم التقليدية. فالجرائم التقليدية مثل السرقة، والقتل، والاعتداءات الجسدية، عادة ما تتسم بوجود مادي واضح يتعلق بالمكان والزمان، إذ يتم تنفيذ الجريمة في بيئة مادية يمكن للأجهزة الأمنية ملاحظة الأدلة فيها بسهولة. أما الجرائم الرقمية، فهي تتم عبر الشبكة الرقمية باستخدام تكنولوجيا المعلومات والاتصالات، إذ غالبًا ما تكون غير مرئية في البداية ولا تترك آثارًا ملموسة، مما يعقد عملية اكتشافها وملاحقتها.

وعلى ضوء ما تقدم، سوف نتطرق لبيان أوجه التشابه والاختلاف بين الجرائم الرقمية والجرائم التقليدية وسوف نخصص لبحث كل منهما في فرع مستقل وكما يأتي:

الفرع الاول: أوجه التشابه بين الجرائم الرقمية والجرائم التقليدية

على الرغم من أن الجرائم الرقمية تحدث في بيئة غير مادية، إلّا أن هناك بعض أوجه التشابه الأساسية بينها وبين الجرائم التقليدية، إذ تشترك الجرائم الرقمية مع الجرائم التقليدية في بعض الجوانب الجوهرية مثل:

١. القصد الجنائي :

عرَّفت الفقرة الأولى من المادة (٣٣) من قانون العقوبات العراقي القصد الجنائي، إذ نصت بأنه (القصد الجرمي هو توجيه الفاعل ارادته الى ارتكاب الفعل المكون للجريمة هادفًا الى نتيجة الجريمة التي وقعت أو أية نتيجة جرمية أخرى). ويتضح من التعريف أعلاه أن للقصد الجنائي عناصر وهي العلم والارادة. والعلم هنا هو قدر من الوعي يسبق تحقق الإرادة أي أن يكون الشخص مدرك الأمور على

نحو صحيح ومطابق للواقع[١] وأما الإرادة فهي القوة النفسية التي تتحكم في سلوك الانسان التي تصدر عن وعي وإدراك لبلوغ هدف معين.

وعلى ضوء ما تقدم، يمكننا ملاحظة أن في كلا النوعين من الجرائم، يوجد القصد الجرمي لدى الجاني، سواء أكان الهدف هو السرقة، الاحتيال، التسلل إلى الأنظمة أم التسبب في أضرار. هذا القصد يُعدُّ العامل المشترك بين جميع أنواع الجرائم.

إذ يتشابه القصد الجنائي في الجريمة التقليدية والرقمية في أنه يجب أن تكون هناك إرادة لارتكاب الجريمة، سواء أكان الهدف السرقة أم الاحتيال أم الإضرار بالآخرين. ففي الجريمة التقليدية (مثل السرقة المادية) ويكون القصد هنا هو اختلاس الممتلكات، وإن في الجرائم الرقمية(مثل اختراق الحسابات) يكون القصد هنا هو الاستيلاء على بيانات أو أموال بشكل غير قانوني.

٢. الضرر المترتب على الجريمة :

تبرز معالم التشابه بين الجرائم الرقمية والتقليدية كذلك من حيث أن النتيجة النهائية للجريمة هي إلحاق الضرر بالمجني عليه. ففي كلا النوعين من الجرائم يكون هناك ضرر اقتصادي مثل (سرقة الأموال أو فقدان معلومات وأوراق مهمة تؤدي لأضرار اقتصادية بالمجنى عليه) ، فضلاً عم أن هناك اضرار معنوية مثل (السب والقذف والتشهير)[٢].

الفرع الثاني: أوجه الاختلاف بين الجرائم الرقمية والجرائم التقليدية

تختلف الجرائم الرقمية عن الجرائم التقليدية في بيئة تنفيذها وأدواتها وآثارها، فبينما ترتكب الجرائم التقليدية في العالم المادي بحدود زمانية ومكانية، في حين أن الجرائم الرقمية ترتكب من خلال الفضاء الرقمي باستخدام التقنيات الحديثة، مما يسمح بانتشارها الفوري عبر الحدود وتنفيذها عن بُعد، وصعوبة تعقب الأدلة الرقمية مقارنة بالأدلة التقليدية الملموسة في الجرائم التقليدية.

وعلى ضوء ما تقدم سنبين أوجه الاختلاف بين الجرائم الرقمية والجرائم التقليدية بحسب الآتي:

١. من حيث المكان والزمان:

---

(١) عبد الله سليمان، شرح قانون العقوبات (القسم العام– الجريمة)، ديوان المطبوعات الجامعية، لبنان، ١٩٩٨، ص٢٣١.

(١) د. ذياب موسى البداينة، الجرائم الالكترونية: المفهوم والأسباب، ورقة علمية قدمت في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن، عمان، ٢٠١٤، ص٧.

توجد هناك اختلافات عدة بين الجرائم الرقمية والجرائم التقليدية من حيث المكان والزمان وسوف نبين أبرز هذه الاختلافات كالآتي:

من حيث المكان:

- تختلف الجرائم الرقمية عن الجرائم التقليدية من حيث المكان، ففي الجرائم الرقمية يُلحظ أنها تتم عبر الانترنت باستخدام تكنولوجيا المعلومات، والجاني قد يكون في دولة مختلفة عن الضحية أو في مكان غير معروف، ويستخدم أدوات مثل VPN لإخفاء الموقع، مما يصعب تحديد المكان [١].
- أما بالنسبة للجرائم التقليدية فإنها تقع في مكان مادي معروف، إذ يتواجد الجاني والضحية في نفس الموقع الجغرافي، مع وجود أدلة مادية واضحة.

أما من حيث الزمان

- تختلف الجرائم الرقمية عن الجرائم التقليدية من حيث الزمان، ففي الجرائم الرقمية يُلحظ أنها يمكن أن تحدث بسرعة فائقة أو تتم برمجتها للتنفيذ لاحقًا، وتكون أحيانًا مستمرة على مدى شهور، مع وجود إمكانية لحذف أو تعديل الأدلة الرقمية لتغيير توقيت الجريمة[٢].
- أما بالنسبة للجرائم التقليدية فإنها تحدث في فترة زمنية محددة وواضحة، مثل سرقة في ساعة معينة، مما يسهل تحديد وقت ارتكابها.

٢. التأثير المادي:

ففي مجال الجرائم الرقمية يُلحظ أنها لا تترك عادة آثارًا مادية واضحة. على سبيل المثال، يمكن أن يتم اختراق الأنظمة الرقمية أو سرقة البيانات عبر الإنترنت من دون أن تلحظ أي تغييرات مادية في المكان الذي تمت فيه الجريمة، مما يجعل اكتشاف الجريمة أمرًا صعبًا في البداية[٣].

أما في الجرائم التقليدية يُلحظ أنها تؤدي إلى أضرار مادية أو جسدية واضحة، مثل السرقة أو الاعتداء الجسدي، مما يجعل آثار الجريمة مرئية للسلطات الأمنية [٤].

---

(١) حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، بحث منشور في مجلة دراسات وأبحاث، المجلد (٢٠٠٩)، العدد (١)، جامعة ٢٠ أوت ١٩٥٥ سكيكدة، ٢٠٠٩، ص ٢١٩ وما بعدها.

(٢) حكيم سياب، مصدر سابق، ص٢١٩ وما بعدها.

(٣) موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الانترنت، بحث منشور في مجلة دراسات قانونية، جامعة بنغازي – كلية القانون، العدد ١٧، ٢٠٠٨، ص٨٩.

(٤) د.مينا فايق، الفرق بين الجرائم المعلوماتية والجرائم التقليدية، مقال متوفر على الرابط الآتي: https://www.menafayq.com/cybercrime-vs-traditional-crime/?utm_source=chatgpt.com

٣. طرق التنفيذ:

ففي الجرائم الرقمية يُلحظ أنها تتم عن بُعد باستخدام تقنيات متقدمة مثل البرمجيات الخبيثة، والفيروسات، والاختراقات الأمنية، إذ يمكن للجاني أن يهاجم أنظمة الحاسوب أو الشبكات من أي مكان في العالم من دون أن يتواجد فعليًا في مكان الجريمة [١].

وأما في الجرائم التقليدية يُلحظ أنها تتطلب تفاعلًا مباشرًا بين الجاني والمجني عليه. على سبيل المثال، في حالة السرقة، يدخل الجاني مكان الضحية ليأخذ ممتلكاته.

٤. التكنولوجيا والأدوات:

ففي الجرائم الرقمية يُلحظ أنها تعتمد على التكنولوجيا الرقمية مثل الإنترنت، والحواسيب، والهواتف الذكية، والبرمجيات الخبيثة، إذ يمكن للمجرم استخدام أدوات تكنولوجية معقدة للوصول إلى البيانات الحساسة أو التسلل إلى الأنظمة [٢].

وأما الجرائم التقليدية يُلحظ انها تعتمد على الأدوات التقليدية التي قد تشمل الأسلحة النارية، المتفجرات، المخدرات[٣]، أو الوسائل المادية لارتكاب الجريمة (مثل أدوات السرقة أو العنف).

٥. من حيث القانون الواجب التطبيق :

ففي الجرائم الرقمية تخضع الى قوانين خاصة بشأن التعامل مع الأفعال الإجرامية التي تتم في الفضاء الرقمي، إذ قد تتنوع القوانين بين الدول وفقًا للتكنولوجيا المستخدمة ونوعية الجريمة، فعلى سبيل المثال نجد أن الاتحاد الأوروبي لديه قانون GDPR وهو قانون خاص بالجرائم والحقوق على شبكات الانترنت[٤].

تاريخ الزيارة ٢٠٢٥/٢/١٦.

(١) منصور فهيد سعيد الحارثي، معوقات إثبات الجرائم المتعلقة بتقنية المعلومات، بحث منشور في المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، مجلة علمية محكمة، المجلد (١٥)، العدد (٤)، ٢٠٢٣، ص١٠٨٢.

(٢) د. مينا فايق، مصدر سابق.

(٣) منصور فهيد سعيد الحارثي، مصدر سابق، ص١٠٥٤.

(٤) مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، قسم المختبر والشؤون العلمية لمكتب الأمم المتحدة المعني بالمخدرات و الجريمة في فيينا، مسرح الجريمة والادلة المادية (توعية الموظفين غير المتخصصين في التحليل الجنائي)، ٢٠٠٩، ص١٣وما بعدها .

وأما الجرائم التقليدية يُلحظ أنها تحكمها القوانين الجنائية التقليدية التي تحدد الأفعال الإجرامية في بيئة مادية، مثل السرقة والقتل، إذ إن هذه القوانين تطبق منذ عقود مما يجعلها أكثر استقرارا وسهلة التفسير أكثر من التشريعات الخاصة بالجرائم الرقمية.

المطلب الثاني: تمييز الجرائم الرقمية من الجرائم الاقتصادية

على الرغم من ترابط الجرائم الرقمية مع الجرائم الاقتصادية في مجالات عدة ، إلّا أن هناك اختلافات بينهما في عالم الإجرام. إذ تركز الجرائم الرقمية على استغلال العالم الرقمي والتكنولوجيا والتقنيات الحديثة لتنفيذ هجمات رقمية تمس البيانات والشبكات والاتصالات والخصوصية، فيما تركز الجرائم الاقتصادية بشكل خاص على الأفعال غير المشروعة التي تستهدف الأموال والاستقرار المالي عبر وسائل تقليدية أو رقمية.

فضلًا عن ذلك أن الجريمة الاقتصادية تشمل الأعمال أو الامتناعات التي تخالف القواعد التنظيمية أو القانونية التي تحمي السياسة الاقتصادية للدولة، وهي تتعلق بالربح غير المشروع على حساب الاقتصاد الوطني، وتؤثر على الالتزامات الاقتصادية والثقة المالية العامة، وتُعدُّ من الجرائم التي تضر بالاقتصاد القومي [١].

أما الجرائم الرقمية، فهي تختلف عن الاقتصادية بشكل رئيسي، إذ تتركز غالبًا على الانتهاكات المرتبطة بالفضاء الرقمي أو الإنترنت، مثل الاختراقات والاحتيال الإلكتروني، على الرغم من أن كلاهما يسبب أضرارًا اقتصادية ويهدف إلى المكاسب غير المشروعة. أما من حيث الاختلاف بينهما يكمن في الأدوات المستخدمة وطبيعة التنفيذ، إذ تُعدُّ الجرائم الاقتصادية أكثر ارتباطًا بالأنشطة المالية والممتلكات، بينما تركز الجرائم الرقمية على الانتهاكات التقنية في العالم الافتراضي[٢].

وعلى ضوء ما تقدم، سنوضح أوجه التشابه ومن ثم أوجه الاختلاف وكلآ في فرع مستقل وحسب الآتي:

الفرع الاول: أوجه التشابه بين الجرائم الرقمية والجرائم الاقتصادية

---

(٢) غسان رباح، قانون العقوبات الاقتصادي، منشورات الحلبي الحقوقية، بيروت – لبنان، ط ٢٠١٢، ص٩.

(٢) أحمد فاضل المعموري، الجرائم الإلكترونية في مواقع التواصل الاجتماعي حدود الشكوى والعقوبة والنقص التشريعي في القانون العراقي، الحوار المتمدن، العدد (٥٠٦٠)، ٢٠١٦/١/٣٠ ، https://www.ahewar.org تاريخ الزيارة، ١٢/ ١٢/ ٢٠٢٤.

هناك جوانب عدة تتشابه بها الجرائم الرقمية مع الجرائم الاقتصادية ، منها جوانب اقتصادية، وتأثيرات مالية، وجانب التكنولوجيا، وسنوضح ذلك تباعًا.

١. الدافع الاقتصادي:

ففي الجرائم الرقمية على الرغم من تنوع الأهداف والأساليب، إلّا أن العديد منها يكون مدفوعًا بدافع اقتصادي(١)، مثل عمليات الاحتيال عبر الإنترنت، أو سرقة المعلومات الحساسة بهدف بيعها أو ابتزاز الضحايا من أجل الحصول على الأموال، وكذلك استغلال الثغرات في الأنظمة الأمنية لتحقيق مكاسب مالية. فضلًا عن أنه يمكن أن تتم عملية الاحتيال إلكترونيًا مثل الاحتيال عن طريق البريد الإلكتروني لخداع الضحية وتحويل الأموال(٢).

وكذلك الحال في الجرائم الاقتصادية فإنها تتعلق بالأنشطة التي تستهدف المال أو الممتلكات، مثل التلاعب في أسواق المال، والتزوير المالي، والتهرب الضريبي لغرض زيادة الارباح أو لتقليل الخسائر بطريقة غير قانونية، وعمليات الاحتيال التجارية. إذ إن العوامل الاقتصادية التي تتمثل بالفقر والبطالة من ناحية، ومن ناحية أخرى تتمثل بالتحولات الاقتصادية التي تصيب النظام الاقتصادي للبلد بشكل عام، مما تسبب، إما الإثراء أو الفقر مثل تحول المجتمعات من زراعية إلى صناعية، إذ أفرزت هذه التحولات الاقتصادية العديد من الجرائم الاقتصادية وانتشرت جرائم الغش والتهريب وتزييف العملة وتزوير الفواتير والمستندات المالية أو إنشاء شركات وهمية لسرقة الأموال(٣).

٢. التأثير المالي:

ففي الجرائم الرقمية تؤدي إلى خسائر مالية فادحة سواء للأفراد أو الشركات، كما في حالات الاحتيال المالي عبر الإنترنت أو الهجمات الرقمية على الأنظمة البنكية وسرقة أموالها، وهناك خسائر مالية بسبب توقف الأنظمة عن العمل نتيجة للهجمات الرقمية، فضلًا عن الخسائر المالية للأفراد بسبب عمليات الابتزاز وطلب الفدية(٤). فضلًا عن ذلك هناك خسائر مالية بسبب نزول أسهم الشركات التي

---

(٢) سعد فهد سعد ادبيس المطيري مفهوم الجرائم الإلكترونية وسماتها، بحث منشور في المجلة القانونية (مجلة علمية محكمة نصف سنوية) المجلد ١٦، العدد ٥ ٢٠٢٣، ص ١٢٥٤.

(٢) عبد الله حسين على محمود: سرقة المعلومات المخزنة في الحاسوب – رسالة ماجستير، كلية الحقوق– جامعة عين شمس، ٢٠٠١ ، ص ١٦٥.

(٣) محمد نعمة كاظم، اتجاهات السياسة الجنائية في مكافحة الجريمة الاقتصادية، رسالة ماجستير، الجامعة المستنصرية – كلية القانون، العراق، بغداد، ٢٠٢١، ص٥٢، ص٥٥.

(٤) عبد الله حسين على محمود: سرقة المعلومات المخزنة في الحاسوب ، مصدر سابق، ص١٦٥ .

تتعرض للاختراق وتسريب معلوماتها وبيانات العملاء فضلًا عن أعمال الصيانة التي تضطر الشركات لعملها من أجل اصلاح الثغرات الأمنية وتعزيز الحماية لأنظمتها وتوظيف الخبراء بهذا المجال وحتى تدريبهم، كل هذه الأسباب لها تأثير مادي سلبي وتسبب خسائر مادية بالغة.

وكذلك الحال بالنسبة للجرائم الاقتصادية فإنها تؤثر أيضًا على الاقتصاد بشكل عام، مثل سرقة الأموال من خلال التلاعب في القوائم المالية أو إنشاء الشركات الوهمية، والتهرب الضريبي وغسيل الأموال يسبب خسائر فادحة لاقتصاد الدولة، ناهيك عن تدمير الشركات أو التلاعب بأسواق الأسهم، مما يؤدي إلى خسائر مالية للضحايا وللاقتصاد ككل(١).

فضلًا عن ذلك يترتب على الجرائم الاقتصادية خسائر مادية آنية فضلًا عن خسائر لاحقة من خلال تعويض المتضررين من الأفراد وتشويه سمعة الأسواق المالية وانخفاض السيولة النقدية بها بسبب تضرر سمعتها وفقدان الثقة فيها.

٣. الإفادة من التكنولوجيا:

ففي الجرائم الرقمية نلحظ أنها تتطلب تكنولوجيا معلومات متقدمة لتنفيذ الجريمة مثل الهجمات الرقمية، البرمجيات الخبيثة (من خلال استخدام فيروسات خبيثة لقرصنة الأنظمة)، أو الاحتيال الرقمي (من خلال إنشاء مواقع إلكترونية أو رسائل بريدية مزيفة لخداع الضحايا)، كذلك استغلال الثغرات الأمنية لاختراق الضحايا ، او التجسس عليهم، او الحاق الضرر ببيانات وبرامج الحاسوب وافسادها (٢) .

وكذلك الحال بالنسبة للجرائم الاقتصادية يمكن أن تتضمن استخدام التكنولوجيا لكن بشكل جزئي، كما في الجرائم الاقتصادية الحديثة مثل التلاعب بالبيانات المالية أو تزويرها، او التحويل الالكتروني غير المشروع للأموال واختراق بطاقات الائتمان، فضلا عن ذلك القمار وغسيل الاموال من خلال الانترنت، إذ يتم ذلك من خلال تحويل الأموال غير المشروعة عبر منصات خاصة بالعملات الرقمية. كذلك السطو على اموال البنوك بغاية الربح المادي وكسب الاموال (٣).

الفرع الثاني: أوجه الاختلاف بين الجرائم الرقمية والجرائم الاقتصادية

---

(١) قسمية محمد، مصادر وأساليب عمليات تبييض الأموال، مجلة الدراسات والبحوث القانونية، المجلد ٩، العدد ١، ٢٠٢٤ ، ص ١٧١-١٧٣.

(٢) فيصل جعيلان العازمي، إشكالية الملاحقة الجنائية في الجرائم الإلكترونية، بحث منشور في مجلة كلية الشريعة والقانون بطنطا، المجلد (٣٩)، العدد (٢)، جامعة القاهرة ، مصر، ٢٠٢٤، ص ٧٨٥.

(٣) زياد عبد الرزاق، مصطفى زغيبي، الجرائم الالكترونية الاقتصادية، المفهوم والدوافع، بحث منشور في مجلة دراسات قانونية واقتصادية، المجلد (٧)، العدد (١)، الجزائر، ٢٠٢٤، ص ٤٠٦.

تختلف الجرائم الرقمية عن الجرائم الاقتصادية في مجالات عدة منها، الاختلاف في جانب الزمان والمكان، الأدوات التي تستخدم في تنفيذ الجريمة، وأساليب التنفيذ. وسنقوم بتوضيح هذه الاختلافات تباعًا.

١. المجال الزمني والمكاني:

من ناحية المكان: ففي الجرائم الرقمية نلحظ أنها تتم في الفضاء الرقمي أو عبر الإنترنت، مما يعني أن الجريمة يمكن أن تحدث فقط عن طريق العالم الرقمي، ويمكن للمجرم أن ينفذ الجريمة من أي مكان في العالم من دون الحاجة للتواجد الفعلي في مكان الجريمة[١]، أما في الجرائم الاقتصادية عادة ما تحدث في بيئة مادية ومحددة، مثل الشركات أو الأسواق المالية، على الرغم من أن بعض الجرائم الاقتصادية قد تستخدم التكنولوجيا، إلّا أنها تتطلب عادة وجود المجرم في مكان معين لتطبيق الجريمة، مثل مكاتب الشركات أو الأسواق المالية [٢].

أما من ناحية الزمان: ففي الجرائم الرقمية نلحظ أنها تتم في أي وقت طالما أن هناك وصول إلى شبكة الإنترنت أي يمكن للجاني تنفيذها في كل أيام السنة سواء أكانت أيام العطل الرسمية أو أيام المناسبات وفي أي ساعة يمكنه تنفيذها ولا يهم سواء ليلًا أو نهارًا[٣].

وأما في الجرائم الاقتصادية عادة ما تتطلب قيام الجريمة في وقت محدد لانتهاز الفرصة المناسبة أو لضمان عدم اكتشاف الجريمة وإمكانية الهروب لتحقيق مكسب مالي أكبر [٤].

٢. أساليب التنفيذ:

ففي الجرائم الرقمية يُلحظ أنها تتم باستخدام تقنيات متقدمة مثل البرمجيات الخبيثة، الفيروسات، الاختراقات الأمنية، والتصيد الاحتيالي عبر الإنترنت، إذ يعتمد الجاني هنا على أدوات تكنولوجية للوصول إلى المعلومات أو الأنظمة[١].

---

(١) هناء مصطفي الخبيري ، الجرائم المعلوماتية وتقنين العملات الرقمية – دراسة قانونية في التشريعات والاتفاقيات الدولية، دار النهضة العربية ، ٢٠٢٢، ص ٩٥.

(١) د. زهير خريبط خلف، مواجهة الجرائم الاقتصادية في التشريع العراقي، بحث منشور في مجلة دراسات البصرة، السنة (٢٠)، العدد (٦٠)، ٢٠٢٥ ص ٢٦٤ وما بعدها

(٣) د. رحموني محمد ، خصائص الجريمة الإلكترونية ومجالات استخدامها، بحث منشور في مجلة الحقيقة للعلوم الاجتماعية والإنسانية، العدد (٤١) ، جامعة أحمد دراية – ادرار، الجزائر، ٢٠١٧، ص ٤٤١ وما بعدها.

(٣) د. نجم عبد الله حسين، التشريعات الجنائية لمكافحة الجرائم الاقتصادية في العراق، بحث منشور في مجلة دراسات قانونية، المجلد (٤)، العدد (١)، ٢٠٢١ ، رابط البحث : https://alhudamissan.com/index.php/2013-03-05-21-25-16/2013-03-05-21-25-11/5501-2021-07-24-20-57-51.html ، تاريخ الزيارة ٢٠/٢/٢٠٢٥

وأما في مجال الجرائم الاقتصادية نلحظ أن أساليب التنفيذ في هذه الجرائم تعتمد على استغلال الثغرات القانونية وبالغالب تعتمد على تعاون أطراف متعددة مثل الموظفين الفاسدين[٢]، فضلًا عن هذه الجرائم فيها العديد من الصور وكل صورة منها تختلف طريقة أسلوب تنفيذها عن غيرها فعلى سبيل المثال بيع سلعة بسعر يزيد عن سعرها المحدد، فضلا عن ذلك ازالة وتحريف تاريخ الصلاحية للسلع واعادة تغليف المنتجات التي تعرضت للتلف، او تقديم بيانات ومعلومات كاذبة بقصد الحصول على تخفيض او سماح من سعر الضريبة المفروضة [٣].

٣. الأدوات المستخدمة:

ففي الجرائم الرقمية كما سبق ان اوضحنا انها تعتمد بشكل أساس على أدوات تقنية متقدمة تكنولوجيًا، وتتمثل في الحواسيب الشخصية والخوادم التي تُستخدم لاستضافة البيانات المخترقة أو البرمجيات الخبيثة، والهواتف الذكية والأجهزة اللوحية التي تُستعمل للولوج إلى الحسابات وتنفيذ عمليات الاحتيال، فضلًا عن الإنترنت والشبكات التي تُستخدم لنقل البيانات وممارسة الأنشطة غير القانونية.

وأما في الجرائم الاقتصادية، فالأدوات تعتمد بشكل رئيس على وسائل تقليدية وأدوات محاسبية[٤]، إذ يتم التلاعب بالسجلات المحاسبية والمالية يدويًا أو إلكترونيًا، كالقيود المخادعة والبيانات والمعلومات الكاذبة من خلال، تحرير وتعديل الأرقام والتقارير المالية، ، بهدف التلاعب بالأرقام وإخفاء العمليات غير القانونية أو التهرب الضريبي. وغالبًا ما تكون الأدوات التقليدية بسيطة وسهلة الاستخدام، وتعتمد على مهارات في التزوير والتلاعب اليدوي. أو باستخدام برامج تحرير سهلة[٥].

٤. قوانين الملاحقة القانونية:

تتم معالجة الجرائم الرقمية وفقًا لقوانين الجرائم الرقمية أو قوانين تكنولوجيا المعلومات، مثل اتفاقية بودابست عام ٢٠٠١ لمكافحة الجرائم الإلكترونية، وتنظم هذه المعاهدة التعاون بين الدول

---

(١) راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث منشور في مجلة كلية الحقوق للبحوث القانونية والاقتصادية، المجلد (٢٠٠٨)، العدد (١)، جامعة الإسكندرية ، ٢٠٠٨، ص٩.

(٢) محمد علي سويلم ، الحماية الجنائية للبورصة بين الجوانب الإجرائية والأحكام الموضوعية دراسة مقارنة، مكتب الجامعي الحديث، ٢٠١٨، ص ٧٨.

(١) محمد نعمة كاظم، اتجاهات السياسة الجنائية في مكافحة الجريمة الاقتصادية، رسالة ماجستير، الجامعة المستنصرية، كلية القانون، ٢٠٢١، ص ٧٠

(٤) محمد جبريل ابراهيم المسئولية الجنائية عن جرائم الروبوت دراسة تحليلية استشرافية دار النهضة العربية ، طبعة ٢٠٢٠ ، ص١٦.

(٣) محمد نعمة كاظم، مصدر سابق، ص ٧٠ وما بعدها

الأعضاء في مجال الجرائم الرقمية ، وتجريم الأفعال غير المشروعة في الفضاء الرقمي، وفضلًا عن اتفاقية GDPR الأوروبية لحماية البيانات الشخصية للمستخدمين وتفرض غرامات مالية على مخالفتها.

وأما في مجال الجرائم الاقتصادية فيتم معالجتها وفقًا للقوانين الاقتصادية التقليدية، مثل قانون مكافحة غسل الأموال وتمويل الارهاب رقم ٣٩ لسنة ٢٠١٥ في العراق، او قانون التلاعب بالأسواق المالية، والاحتيال التجاري، في دول أخرى وهي قوانين تركز على الأنشطة المالية والمحاسبية.

المبحث الثاني: ذاتية الأمن السيبراني

يشهد مجال الأمن السيبراني تطورًا سريعًا في ظل الاعتماد المتزايد على التكنولوجيا الرقمية في مختلف جوانب الحياة، ولفهم أهمية وخصوصية هذا المجال، من الضروري التمييز بينه وبين بعض المفاهيم ذات الصلة مثل أمن المعلومات والخصوصية الرقمية، وسوف نتطرق في هذا المطلب لبيان ذاتية الأمن السيبراني، مع التركيز على الفرق بينه وبين مفاهيم أخرى قد تتداخل معه في بعض الأحيان، وسوف نخصص مطلب مستقل لكل منها، إذ سوف نتطرق للتمييز بين الأمن السيبراني وأمن المعلومات، من حيث نطاق كل منهما وأهدافه وأدواته، ومن ثم، سوف نتطرق لبيان الفرق بين الأمن السيبراني والخصوصية الرقمية، ويسلط الضوء على العلاقة بين حماية البيانات وحماية الخصوصية في الفضاء الرقمي، من خلال هذا التحليل، سيتم توضيح الأبعاد المختلفة للأمن السيبراني وكيفية تمييزه من غيره من المفاهيم المتداولة في مجال الحماية الرقمية.

المطلب الأول: تمييز الأمن السيبراني من أمن المعلومات

يُعدُّ كل من " الأمن السيبراني" و"أمن المعلومات" من المواضيع الأساسية في ظل التهديدات الرقمية المتزايدة، إذ يركز الأمن السيبراني على حماية الأنظمة والشبكات من الهجمات الرقمية، بينما يشمل أمن المعلومات حماية جميع أشكال المعلومات، سواء إلكترونية أو ورقية. وعلى الرغم من استخدام المصطلحين أحيانًا بشكل مترادف، إلّا أن الفرق يكمنُ في النطاق والأهداف، مما يتطلب من المؤسسات إدارة فعالة لضمان سلامة المعلومات واستمراريتها في مواجهة التحديات التكنولوجية[١].

وقد تعددت تعاريف أمن المعلومات، إذ عُرّف بأنه (حماية المعلومات وعناصرها المهمة بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزنها وترسلها). وعرف أيضا بأنه (هو العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها سواء كانت هذه

(1) Arina Alexei ,Anatolie Alexei ,The difference between cyber security vs information security. Journal of Engineering Science, 29(4) , 2022, p 75 – 77.

المخاطر داخلية أو خارجية وذلك من خلال توفير الأدوات والوسائل اللازمة لحمايتها والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين)[١].

وكذلك يعرف أمن المعلومات بانه (عبارة عن الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية وهو العلم الذي يدرس كيفية توفير تدابير حماية سرية وسلامة المعلومات وكيفية مكافحة الاعتداء عليها)[٢]. وعرّف امن المعلومات أيضًا بأنه (العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها). وعرّف كذلك بأنه (هي الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية). وعرف ايضا بأنه (هي محل الدراسات والتدابير اللازمة لضمان سرية وسلامة محتوى المعلومات وتوفرها ومكافحة أنشطة الاعتداء عليها أو استغلالها في ارتكاب جرائم معلوماتية) [٣].

وعلى ضوء ما تقدم ولغرض إبراز ذاتية الأمن السيبراني من خلال تمييزه من أمن المعلومات لابد من التطرق إلى أوجه التشابه ومن ثم إلى أوجه الاختلاف بينهما، وسوف نخصص فرع مستقل لكل منهما وعلى النحو الآتي:

الفرع الاول: أوجه التشابه بين الأمن السيبراني وأمن المعلومات

هناك تداخل كبير بين الأمن السيبراني وامن المعلومات من حيث الأهداف والحماية، على الرغم من اختلاف نطاق تغطيتهما. إذ يركز كلا منهما على حماية البيانات الحساسة من الوصول الغير مصرح به أو التعديل أو الاتلاف. كما يتشابهان في اعتماد اليات دفاعية متشابهة مثل التشفير والتحقق من الهوية. وسنقوم بتوضيح هذا التشابه على النحو الآتي:

١. حماية المعلومات والبيانات:

---

(١) د. علي ادهم، أمن المعلومات الجزء الثاني، مركز النهرين للدراسات الاستراتيجية، مقال منشور على الرابط الآتي: https://www.alnahrain.iq/post/392 ، تاريخ الزيارة ٢/٨/ ٢٠٢٥

(٢) رضا إبراهيم صالح، دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية مع دراسة ميدانية على الشركات المصرية، مجلة الدراسات التجارية المعاصرة ، المجلد ٦، العدد ١٠ ، الجزء الأول، ٢٠٢٠، ص١١١.

(٣) رضا إبراهيم صالح، دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية مع دراسة ميدانية على الشركات المصرية، مصدر سابق ، ص١١٢.

يهدف كلاً من الأمن السيبراني وأمن المعلومات إلى حماية البيانات من الوصول غير المصرح به، الفقدان، التلاعب أو التسريب لذا فإن كلا المفهومين يشتركان في غاية واحدة وهي الحفاظ على سرية وأمان المعلومات ضمن بيئات متعددة، فضلًا عن ذلك أن الأمن السيبراني وأمن المعلومات يسعيان لحماية البيانات والمعلومات من التهديدات والأخطار المتنوعة [١].

٢. استخدام التقنيات الحديثة:

ففي الأمن السيبراني وأمن المعلومات يتم استخدام مجموعة متنوعة من الأدوات والتقنيات مثل التشفير لحماية البيانات سواء عند نقلها أو عند تخزينها وإن التشفير هو عملية تحويل البيانات من شكلها المقروء إلى شكل غير مفهوم عن طريق خوارزميات رياضية لغرض حماية البيانات، فضلًا عن استخدام الجدران النارية، أنظمة كشف التسلل، لتأمين المعلومات وحمايتها من الهجمات الرقمية في كلا النظامين وإن الجدران النارية هي نظام امني تستخدم لمراقبة الحركة للبيانات الصادرة والواردة وتعمل كحاجز بين الشبكات الموثوقة وغير الموثوقة لحماية البيانات والأجهزة من الاختراقات. لذلك فإن الأطر الأمنية المستخدمة في كلا المجالين تشترك في تقنيات الحماية المتقدمة التي تضمن الأمان الرقمي، إذ إن في كل من الأمن السيبراني وأمن المعلومات يتم استخدام التقنيات الحديثة مثل التشفير والجدران النارية تُستخدم بشكل شائع لحماية المعلومات في كلا من الأمن السيبراني وأمن المعلومات[٢]" .

٣. إدارة المخاطر :

في كل من الأمن السيبراني وأمن المعلومات، يتطلب الأمر تنفيذ استراتيجيات إدارة المخاطر التي تضمن الحماية الفعالة من الهجمات، فضلا عن ذلك ان كل من الأمن السيبراني وأمن المعلومات يعتمد على تقييم المخاطر المحتملة لتطوير أنظمة تدابير أمان فعالة [٣].

الفرع الثاني: أوجه الاختلاف بين الأمن السيبراني وأمن المعلومات

يختلف الأمن السيبراني عن أمن المعلومات في مجالات عدة منها، شكل المعلومات المراد حمايتها، وطبيعة التهديدات، والأدوات والاستراتيجيات، إذ يركز أمن المعلومات على حماية البيانات سواء أكانت ورقية أم رقمية من أي انتهاك لها، بينما يكون اختصاص الأمن السيبراني هو الدفاع عن

(1) Hathaway, R. M., McCreight, C., & Riley, J. (2012). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press, P76.

(2) Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology , P23.

(3) Shostack, A. (2014). Threat modeling: Designing for security. Wiley, p. 507.

البنية الرقمية بالكامل من الهجمات الرقمية. وبناءً على ذلك سنقوم بتوضيح هذا الاختلاف على النحو الآتي:

١. من حيث شكل المعلومات المراد حمايتها:

إن الأمن السيبراني يركز بشكل أساسي على حماية الأنظمة والشبكات من التهديدات الرقمية، ويشمل ذلك الفضاء الإلكتروني (مثل الإنترنت، الشبكات، البرمجيات الخبيثة)، فضلًا عن ذلك فإن الأمن السيبراني يهتم بحماية البيانات الرقمية فقط من الهجمات عبر الإنترنت، كذلك يركز على تأمين الأنظمة الرقمية وحمايتها من الهجمات الموجهة عبر الإنترنت "[١]. ولا يحمي البيانات غير الرقمية.

أما أمن المعلومات : يُعنى بحماية المعلومات بغض النظر عن شكلها أو موقعها، سواء أكانت إلكترونية أم ورقية، وبهذا فإن أمن المعلومات يُعدُّ أوسع بهذه الناحية لأنه يشمل الحماية الشاملة لجميع أنواع المعلومات، سواء أكانت ورقية أم إلكترونية[٢] ".

٢. من حيث انواع التهديدات :

إن الأمن السيبراني :يُركز على التهديدات الرقمية مثل الهجمات الرقمية (البرمجيات الخبيثة، هجمات حجب الخدمة، القرصنة)، إذ إن الأمن السيبراني يتعامل بشكل رئيسي مع التهديدات على مستوى الشبكات والأنظمة، فضلًا عن ذلك أن الأمن السيبراني يتعامل مع تهديدات تتعلق بالأنظمة الرقمية والشبكات مثل الهجمات الرقمية" [٣] .

أما أمن المعلومات يركز على جميع أنواع المخاطر التي تهدد المعلومات، سواء أكانت رقمية مثل نقل البيانات عبر الشبكات والهجمات الرقمية والفيروسات الضارة أم فقدان البيانات المادية مثل السرقة المادية أم تلف الملفات أم تسريب البيانات، لذلك فإن أمن المعلومات يتعامل مع كل تهديد قد

(1) Kizza, J. M. (2017). Guide to computer network security (4th ed.). Springer P15.

(2) ISO/IEC 27001. (2013). Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization, Appendix A Item 8.2.

(3) Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in computing (5th ed.). PearsonP, p. 6 – 20.

يهدد سرية أو نزاهة المعلومات بغض النظر عن مكانها أو شكلها أي سواء أكانت في العالم الرقمي أو الواقعي[١].

٣. من حيث الأدوات والاستراتيجيات :

يركز الأمن السيبراني على حماية الأنظمة والشبكات من الهجمات الإلكترونية، ويستخدم أدوات وتقنيات متطورة مثل جدران الحماية التي تتحكم في حركة المرور بين الشبكات الموثوقة وغير الموثوقة، وبرامج مكافحة الفيروسات التي تكتشف البرمجيات الخبيثة وتزيلها، فضلًا عن أنظمة كشف التسلل التي ترصد الأنشطة المشبوهة، وإدارة الثغرات الأمنية لمعالجة نقاط الضعف قبل استغلالها من قِبَل المهاجمين. كما يعتمد على التشفير لضمان حماية البيانات أثناء النقل والتخزين.[٢]

أما أمن المعلومات، فهو يهتم بحماية سرية وسلامة وتوافر المعلومات، سواءً أكانت رقمية أم غير رقمية، ويعتمد على استراتيجيات مثل إدارة الوصول التي تحدد من يمكنه الوصول إلى المعلومات، ووضع سياسات الأمان التي تضع إطارًا تنظيميًا لحماية البيانات، بالإضافة إلى التدقيق والمراجعة لضمان الامتثال للإجراءات الأمنية، والتوعية والتدريب لرفع مستوى الوعي الأمني لدى الموظفين. كما يُعتمد على النسخ الاحتياطي كإجراء احترازي لضمان استعادة البيانات في حالة الفقدان أو التلف [٣].

كما يبرز الاختلاف الجوهري بينهما من حيث أن الأمن السيبراني يركز على حماية البنية التحتية الرقمية والأنظمة من التهديدات الإلكترونية باستخدام تقنيات دفاعية، بينما يهتم أمن المعلومات بحماية البيانات نفسها، بغض النظر عن الوسيلة أو النظام الذي تُخزن فيه، من خلال وضع سياسات وإجراءات تنظيمية وتقنية.

المطلب الثاني: تمييز الأمن السيبراني من الخصوصية الرقمية

---

(١) إيناس ابراهيم الشيتي، تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربية السعودية دراسة تطبيقية على جامعة القصيم ، ماجستير غير منشورة، جامعة القصيم، ٢٠١٩، ص ١٤ وما بعدها.

(٢) منى عبد الله السمحان، مصدر سابق. ص١١ وما بعدها .

(٣) الفرق بين الأمن السيبراني وأمن المعلومات وأهم المقارنات، للمزيد ينظر الرابط الاتي: https://horizons-edu.com/blog/%D8%A7%D9%84%D9%81%D8%B1%D9%82-%D8%A8%D9%8A%D9%86-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D9%88%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA ، تاريخ الزيارة ٢٠٢٥/٨/١.

في ظل الثورة الرقمية السريعة، برزت مفاهيم " الأمن السيبراني" و" الخصوصية الرقمية " كعناصر حيوية لحماية الأفراد والمؤسسات. إذ يركز الأمن السيبراني على حماية الأنظمة والشبكات من الهجمات الخارجية، بينما تتعلق الخصوصية الرقمية بحقوق الأفراد في حماية بياناتهم الشخصية وعدم استغلالها أو تداولها من دون إذن. وتُعدّ المادة ١٧ من الدستور العراقي لعام ٢٠٠٥ تأكيدًا على حق الخصوصية، إذ تُعدُّ الخصوصية الرقمية جزءً من مفهوم أوسع، يهدف إلى إدارة البيانات الحساسة بشكل يحافظ على سرية وسلامة المعلومات الشخصية والاتصالات والسلوكيات في البيئة الرقمية، لتحقيق توازن بين الأمان وحماية الخصوصية في العصر الحديث(١).

وإن الخصوصية الرقمية تضم المعلومات الأسمية والبيانات والمعطيات الشخصية للفرد، إذ تدل على معنى الحق الشخصي، فلكل فرد الحق في أن يتحكم بمعلوماته الخاصة(٢).

وعلى ضوء ما تقدم، سيتم تمييز الأمن السيبراني من الخصوصية الرقمية من خلال استعراض مفهومهما وأهدافهما، وتوضيح كيفية تعاملهما مع التهديدات والحفاظ على المعلومات في الفضاء الرقمي، وسوف نقوم بتخصيص فرع مستقل لكل منها وكالاتي.

الفرع الاول: التشابه بين الأمن السيبراني والخصوصية الرقمية

يرتبط الأمن السيبراني والخصوصية الرقمية في العالم الرقمي بجوانب عدة ، فكلاهما يهتمان بحماية البيانات والمعلومات من خطر الاختراقات الرقمية، وكلاهما يعتمدان على التقنيات والأدوات نفسها وإدارتهم للمخاطر. ولا يتحقق أحدهما من دون الآخر، فغياب الحماية الأمنية يعرض الخصوصية الرقمية للخطر، وإن احترام الخصوصية هو الأساس في أي نظام أمني فعّال وأخلاقي. ومعًا يشكلان الأساس المطلوب لثقة المستخدم في العالم الرقمي. وعلى ضوء ما تقدم، سوف نبين هذا التشابه على النحو الآتي:

أ. من حيث حماية المعلومات:

---

(١) بلعسل بنت نبي ياسمين، مقدر نبيل، الحق في الخصوصية الرقمية، بحث منشور في مجلة المستقبل للدراسات القانونية والسياسية، المجلد ٥، العدد١ جامعة يحيى فارس بالمدية، المدية، الجزائر ، ٢٠٢١، ص٦.

(٢) على الرغم من أن كلمة خصوصية في حد ذاتها هي ابتكار حديث نسبيا، إذ لم تكتسب معناها الحديث إلا في بدايات القرن العشرين، والخصوصية بالإنجليزية privacy هي حق للفرد ليحافظ على معلوماته الشخصية وحياته الخاصة بشكل اختياري وحر، ويقصد بها من الناحية اللغوية بأنها حالة الخصوص، ويقال خصه بشيء يخصه خصا وخصوصا وخصوصية، فالخصوص نقيض العموم، فاخصه أفرده به دون غيره، ينظر في ذلك، ابن منظور، لسان العرب، مطبعة الأميرية ببولاق الجزء ٠٨ ، الطبعة ٠١، د.س، ص ٢٩٠.

كلاً من الأمن السيبراني والخصوصية الرقمية يهدفان إلى حماية البيانات من التهديدات، ونلحظ أن في الأمن السيبراني، يتم حماية الأنظمة والشبكات من الهجمات الرقمية، كذلك في الخصوصية الرقمية، يتم حماية المعلومات الشخصية وضمان عدم استغلالها، وبذلك فإن الهدف المشترك بين الأمن السيبراني والخصوصية الرقمية هو حماية البيانات والمعلومات الحساسة من الوصول غير المصرح به[١].

ب. من حيث الاعتماد على التقنيات والأدوات:

تُستخدم تقنيات مثل التشفير والتوثيق والجدران النارية في كلا المجالين، ففي الأمن السيبراني هذه الأدوات تهدف إلى حماية الأنظمة، وكذلك في الخصوصية الرقمية تُستخدم تقنيات التشفير والجدران النارية لضمان حماية البيانات الشخصية وضمان عدم وصول أطراف ثالثة إليها، وبذلك يمكننا أن نلحظ أن في كلتا الحالتين تستخدم هذه الادوات لحماية البيانات[٢] ".

ت. من حيث إدارة المخاطر:

يعتمد المجالان على إدارة المخاطر لتحديد التهديدات وتطوير استراتيجيات للتصدي لها، مثل التحقق من وجود ثغرات امنية ووضع خطط للتخفيف منها لضمان عدم استغلال هذه الثغرات من جهات خارجية لغرض الاختراق. ونستخلص ان كل من الأمن السيبراني والخصوصية الرقمية يعتمدان على تحليل المخاطر واتخاذ تدابير وقائية لحماية المعلومات[٣].

الفرع الثاني: الاختلاف بين الأمن السيبراني والخصوصية الرقمية

يتجسد الاختلاف بين الأمن السيبراني والخصوصية الرقمية من نواح عديدة وهي:

أ. من حيث الهدف الرئيس:

يهدف الأمن السيبراني الى تأمين الأنظمة والشبكات ضد الهجمات الإلكترونية، بما في ذلك عمليات الاختراق والبرمجيات الخبيثة، وذلك لضمان سلامتها واستمراريتها وحمايتها من المخاطر السيبرانية[٤]. وأما الخصوصية الرقمية، فتنصب على حماية البيانات الرقمية الشخصية للأفراد، وضمان معالجتها وفقًا للأطر القانونية والأخلاقية، بحيث تشمل حماية المعلومات الحساسة كالأسماء والعناوين

---

(١) بلعسل بنت نبي ياسمين، مقدر نبيل، مصدر سابق، ص٦ وما بعدها.

(2) Pfleeger, C. P. (2015). Security in computing (5th ed.). Pearson P24.

(3) Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning,PP6-7.

(٤) نورة العقون، عبد الكريم باسماعيل، واقع الفضاء السيبراني وإشكالية الدفاع الوطني، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر، ورقلة، ٢٠١٩، ص٣٦-٣٨.

والبيانات الشخصية الأخرى التي قد تكون عرضة للإفشاء أو الاستغلال، وفي حين يركز الأمن السيبراني على التصدي للتهديدات التي قد تؤثر على استقرار الأنظمة الرقمية وأمنها، فإن الخصوصية الرقمية تهتم بصيانة حقوق الأفراد في التحكم ببياناتهم الرقمية، من حيث كيفية جمعها ومعالجتها ومشاركتها[١].

ب. من حيث الادوات والنطاق:

فمن حيث الأدوات يكمنُ الاختلاف بين الأمن السيبراني والخصوصية الرقمية في التركيز والنهج، فالأمن السيبراني يركز على استخدام تقنيات متطورة مثل التشفير والجدران النارية لحماية الأنظمة الرقمية والبنى التحتية من الهجمات والاختراقات، ومن حيث النطاق فنجد أن الأمن السيبراني يحمي جميع أنواع البيانات والشبكات والخوادم والأجهزة ضد التهديدات الرقمية المختلفة[٢].

بينما تهتم الخصوصية الرقمية بالالتزام بالقوانين واللوائح التنظيمية، كاللائحة العامة لحماية البيانات GDPR، لضمان حقوق الأفراد في التحكم وحماية بياناتهم الشخصية. ومن حيث النطاق فأن أن الخصوصية الرقمية تركز على حماية البيانات الشخصية للمستخدم وحماية خصوصية الأفراد وحقوقهم القانونية[٣].

---

(١) مفيدة مباركية، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، بحث منشور في مجلة الشريعة والاقتصاد، الاصدار الاول، المجلد (٧)، العدد (١٣)، جامعة الامير عبد القادر للعلوم الاسلامية، الجزائر، ٢٠١٨، ص ٤٦٤

(١) الهيئة الوطنية للامن السيبراني ، الضوابط الاساسية للامن السيبراني، المملكة العربية السعودية، الرياض، ٢٠١٨، ص ١٢

(١) د. أحمد حسني علي أشقر، الخصوصية الرقمية في عصر الذكاء الاصطناعي (قراءة في التشريعين الاردني والفلسطيني) ، بحث منشور في مجلة جامعة القدس المفتوحة، العدد٦٦، المجلد ٧، فلسطين، رام الله،،٢٠٢٥، ص ٣٦.

الخاتِمـة

خلص البحث إلى أن الجرائم الرقمية تختلف بشكل جوهري عن الجرائم التقليدية والاقتصادية، سواء من حيث بيئة التنفيذ أو الوسائل المستخدمة أو الآثار المترتبة عليها. كما تبين أن الأمن السيبراني، على الرغم من تقاطعه مع أمن المعلومات والخصوصية الرقمية، إلا أنه يتميز عنها من حيث النطاق والأهداف والأدوات.

وعلى ضوء ما تقدم، توصلنا الى جملة من الاستنتاجات والمقترحات، يمكن اجمالها بالاتي:

أولا: الاستنتاجات

١- اتضح لنا من خلال هذا البحث أن الجرائم الرقمية تشترك مع الجرائم التقليدية في القصد الجنائي والضرر، إذ يقوم الجاني في كلا النوعين بتوجيه إرادته لارتكاب فعل غير مشروع يفضي إلى نتيجة ضارة، سواء تمثلت في سرقة أو احتيال أو تسلّل إلى أنظمة رقمية. كما أن كلاهما يؤدي إلى ضرر مادي أو معنوي يصيب المجني عليه، كالخسائر المالية أو التشهير. غير أن هذه الجرائم تختلف عن التقليدية من حيث المكان والزمان، حيث ترتكب في فضاء إلكتروني عابر للحدود يمكن أن يتم عن بعد وفي أي وقت، في حين تقع الجرائم التقليدية في مكان مادي وزمن محدّد. كما يختلف الأثر المادي إذ غالبًا ما تخلو الجرائم الرقمية من دلائل مادية ملموسة، على عكس التقليدية التي تخلّف آثارًا واضحة. وتختلف ايضا في أساليب التنفيذ، فالجرائم الرقمية تتم عبر أدوات وبرمجيات وتقنيات متقدمة، بينما تتطلب الجرائم التقليدية غالبًا تواصلًا مباشرًا بين الجاني والضحية باستخدام وسائل مادية تقليدية. واخيرا، يبرز الاختلاف في القانون الواجب التطبيق، إذ تتطلب الجرائم الرقمية تشريعات خاصة ومتجددة، بينما تظل الجرائم التقليدية خاضعة لأحكام القوانين الجنائية المستقرة.

٢- تبين لنا من خلال هذا البحث أن الجرائم الرقمية والجرائم الاقتصادية يجمعهما الدافع الاقتصادي في كثير من الأحيان، فكلاهما يستهدف تحقيق مكاسب مالية غير مشروعة، سواء من خلال الاختراق والابتزاز وبيع البيانات في الجرائم الرقمية، أو من خلال التلاعب في الأسواق والتهرب الضريبي وغسل الأموال في الجرائم الاقتصادية. كما يشتركان في التأثير المالي الكبير على الأفراد والدول، إذ تتسبب الجرائم الرقمية بخسائر مباشرة وغير مباشرة، مثل سرقة الأموال وتعطيل الأنظمة وانخفاض قيمة الأسهم، فيما تؤدي الجرائم الاقتصادية إلى الإضرار بالاقتصاد الوطني وتشويه الثقة بالأسواق. كذلك نجد أن كليهما يوظف التكنولوجيا في التنفيذ، حيث تعتبر شرطًا

أساسيًا للجرائم الرقمية، بينما تُستعمل كأداة مساعدة في الجرائم الاقتصادية. ومع ذلك، تختلف الجرائم الرقمية عن الاقتصادية من حيث الزمان والمكان، فالرقمية تُرتكب في الفضاء الإلكتروني ويمكن تنفيذها في أي لحظة ومن أي موقع، أما الاقتصادية فتجري عادة في بيئات مادية مؤسسية مرتبطة بظروف محددة. وتختلف أيضًا في الأساليب، فالرقمية تعتمد على الهجمات التقنية، بينما الاقتصادية تستغل الثغرات القانونية والتنظيمية وتقوم على تعاون داخلي. كما تختلف الأدوات، إذ ترتبط الجرائم الرقمية بالبنية التكنولوجية والشبكات، في حين تعتمد الاقتصادية على الوثائق المحاسبية والفواتير والعقود. ويظهر الاختلاف كذلك في القوانين المنظمة، إذ تنظم الجرائم الرقمية تشريعات خاصة بالفضاء الإلكتروني، بينما تحكم الجرائم الاقتصادية قوانين مكافحة غسل الأموال والتلاعب المالي.

٣- خلص البحث الى أن الأمن السيبراني وأمن المعلومات يشتركان في الهدف المتمثل بحماية البيانات وضمان سلامتها ومنع الوصول غير المشروع إليها، كما يعتمدان على أساليب متشابهة كالتشفير والجدران النارية وإدارة المخاطر. إلا أنهما يختلفان من حيث نطاق الحماية، فالأمن السيبراني يركّز على الأنظمة الرقمية والبنى التحتية المرتبطة بالشبكات، بينما أمن المعلومات يشمل جميع أشكال المعلومات سواء كانت ورقية أو إلكترونية. كما يختلفان من حيث طبيعة التهديدات، فالأمن السيبراني يتعامل مع الهجمات الرقمية كالفيروسات والاختراقات وحجب الخدمة، بينما يتسع نطاق أمن المعلومات ليشمل المخاطر الرقمية والمادية معًا كسرقة الملفات أو تلفها. ويبرز الاختلاف أيضًا في الأدوات والاستراتيجيات، إذ يقوم الأمن السيبراني على الدفاعات التقنية المتقدمة لرصد الثغرات ومعالجتها، بينما يعتمد أمن المعلومات على مزيج من الأدوات التقنية والسياسات التنظيمية، مثل إدارة الوصول والتدقيق والتوعية والنسخ الاحتياطي.

٤- أظهر البحث أن الأمن السيبراني والخصوصية الرقمية يجتمعان في حماية البيانات والمعلومات من المخاطر والاعتداءات، حيث إن غياب الأمن يعرض الخصوصية للخطر، وانتهاك الخصوصية يضعف أي منظومة أمنية. كما يشتركان في الاعتماد على أدوات تقنية متقاربة مثل التشفير والتوثيق وإدارة المخاطر. غير أنهما يختلفان من حيث الهدف الرئيسي، فالأمن السيبراني يسعى إلى حماية الأنظمة والشبكات وضمان استمراريتها وسلامتها من الهجمات، بينما تركز الخصوصية الرقمية على صون الحقوق الفردية وضمان تحكم الأشخاص في بياناتهم الشخصية ومنع استغلالها أو تداولها دون إذن. كما يظهر الاختلاف من حيث الأدوات والنطاق، إذ يعتمد

الأمن السيبراني على حلول تقنية لحماية البنية التحتية الرقمية بأكملها، بينما تقوم الخصوصية الرقمية على الأطر القانونية والتنظيمية التي تضمن حقوق الأفراد في بياناتهم. وبذلك فإن الخصوصية الرقمية تعد امتدادًا للحقوق الدستورية في الحياة الخاصة، بينما الأمن السيبراني يمثل البعد التقني لحماية البيئة الرقمية.

ثانيا: المقترحات

١- جاءت التشريعات العراقية خالية من الإشارة للجرائم الرقمية، لذلك نقترح أن يتم وضع تعريفات قانونية واضحة للجرائم الرقمية بشكل يميزها من الجرائم التقليدية والاقتصادية، وذلك لتجنب الخلط التشريعي والعملي وضمان التطبيق الصحيح للقانون عند مواجهة هذه الأفعال المستحدثة.

٢- لم تشر التشريعات العراقية الى الامن السيبراني، ولم تشر الى المفاهيم الأخرى المشابهة له مثل، أمن المعلومات والخصوصية الرقمية، لذلك نقترح أن تعمل التشريعات على بيان الامن السيبراني، فضلا عن ذلك توضيح الحدود الفاصلة بين الأمن السيبراني وأمن المعلومات والخصوصية الرقمية، من خلال تحديد نطاق كل مفهوم بدقة، بما يسهم في تنظيم المسؤوليات والحد من التداخل بين هذه المفاهيم.

٣- نقترح تعزيز الجهود التشريعية والمؤسساتية لمكافحة الجرائم الرقمية التي تتسم بتعقيد أكبر من الجرائم التقليدية، عبر تطوير آليات فعالة لرصد هذه الجرائم والتحقيق فيها وتيسير الإثبات فيها رغم طبيعتها غير المادية.

٤- نقترح إدماج حماية الخصوصية الرقمية في السياسات الوطنية بوصفها جزءًا مكملًا للأمن السيبراني، بما يضمن تحقيق التوازن بين حماية الأنظمة والشبكات وبين صون حقوق الأفراد في بياناتهم الشخصية.

قائمة المصادر والمراجع

أولا: المعاجم اللغوية

١. ابن منظور، لسان العرب، مطبعة الأميرية ببولاق الجزء ٠٨ ، الطبعة ٠١، بدون ذكر سنة الطبع.

ثانيا: الكتب القانونية

١. عبد الله سليمان، شرح قانون العقوبات (القسم العام– الجريمة)، ديوان المطبوعات الجامعية، لبنان، ١٩٩٨.
٢. غسان رباح، قانون العقوبات الاقتصادي، منشورات الحلبي الحقوقية، بيروت – لبنان، ط ٢٠١٢
٣. محمد جبريل ابراهيم المسئولية الجنائية عن جرائم الروبوت دراسة تحليلية استشرافية دار النهضة العربية ، طبعة ٢٠٢٠.
٤. محمد علي سويلم ، الحماية الجنائية للبورصة بين الجوانب الإجرائية والأحكام الموضوعية دراسة مقارنة، مكتب الجامعي الحديث، ٢٠١٨.
٥. هناء مصطفي الخبيري ، الجرائم المعلوماتية وتقنين العملات الرقمية – دراسة قانونية في التشريعات والاتفاقيات الدولية، دار النهضة العربية ، ٢٠٢٢.
٦. الهيئة الوطنية للأمن السيبراني، الضوابط الاساسية للأمن السيبراني، المملكة العربية السعودية، الرياض، ٢٠١٨.

ثالثا: البحوث والأوراق البحثية

١. أحمد حسن أبو الحسن، مدى تأثير الرقمنة على خطورة الجرائم الاقتصادية، بحث منشور في مجلة جامعة أسوان للعلوم الإنسانية، المجلد (٤)، العدد (١)، كلية الحقوق – جامعة أسوان، ٢٠٢٤.
٢. د. أحمد حسني علي أشقر، الخصوصية الرقمية في عصر الذكاء الاصطناعي (قراءة في التشريعين الاردني والفلسطيني) ، بحث منشور في مجلة جامعة القدس المفتوحة، العدد٦٦، المجلد ٧، فلسطين، رام الله، ٢٠٢٥.

٣. بلعسل بنت نبي ياسمين، مقدر نبيل، الحق في الخصوصية الرقمية، بحث منشور في مجلة المستقبل للدراسات القانونية والسياسية، المجلد ٥، العدد١ جامعة يحيى فارس بالمدية، المدية، الجزائر ، ٢٠٢١.

٤. حكيم سياب، السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية، بحث منشور في مجلة دراسات وأبحاث، المجلد (٢٠٠٩)، العدد (١)، جامعة ٢٠ أوت ١٩٥٥ سكيكدة، ٢٠٠٩.

٥. د. ذياب موسى البداينة، الجرائم الالكترونية: المفهوم والأسباب، ورقة علمية قدمت في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن، عمان، ٢٠١٤.

٦. د. رحموني محمد ، خصائص الجريمة الإلكترونية ومجالات استخدامها، بحث منشور في مجلة الحقيقة للعلوم الاجتماعية والإنسانية، العدد (٤١) ، جامعة أحمد دراية – ادرار، الجزائر، ٢٠١٧.

٧. راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث منشور في مجلة كلية الحقوق للبحوث القانونية والاقتصادية، المجلد (٢٠٠٨)، العدد (١)، جامعة الإسكندرية ، ٢٠٠٨.

٨. رضا إبراهيم صالح، دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية مع دراسة ميدانية على الشركات المصرية، مجلة الدراسات التجارية المعاصرة ، المجلد ٦، العدد ١٠ ، الجزء الأول، ٢٠٢٠

٩. سعد فهد سعد ادبيس المطيري مفهوم الجرائم الإلكترونية وسماتها، بحث منشور في المجلة القانونية (مجلة علمية محكمة نصف سنوية) المجلد ١٦، العدد ٥ ٢٠٢٣.

١٠. فيصل جعيلان العازمي، إشكالية الملاحقة الجنائية في الجرائم الإلكترونية، بحث منشور في مجلة كلية الشريعة والقانون بطنطا، المجلد (٣٩)، العدد (٢)، جامعة القاهرة ، مصر، ٢٠٢٤.

١١. قسمية محمد، مصادر وأساليب عمليات تبييض الأموال، مجلة الدراسات والبحوث القانونية، المجلد ٩، العدد ١، ٢٠٢٤

١٢. مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، قسم المختبر والشؤون العلمية لمكتب الأمم المتحدة المعني بالمخدرات و الجريمة في فيينا، مسرح الجريمة والادلة المادية (توعية الموظفين غير المتخصصين في التحليل الجنائي)، ٢٠٠٩.

١٣. موسى مسعود ارحومة، السياسة الجنائية في مواجهة جرائم الانترنت، بحث منشور في مجله دراسات قانونية، جامعه بنغازي – كلية القانون، العدد ١٧، ٢٠٠٨.

١٤. منصور فهيد سعيد الحارثي، معوقات إثبات الجرائم المتعلقة بتقنية المعلومات، بحث منشور في المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، مجلة علمية محكمة، المجلد (١٥)، العدد (٤)، ٢٠٢٣.

١٥. د. زهير خريبط خلف، مواجهة الجرائم الاقتصادية في التشريع العراقي، بحث منشور في مجلة دراسات البصرة، السنة (٢٠)، العدد (٦٠)، ٢٠٢٥ .

١٦. زياد عبد الرزاق، مصطفى زغيبي، الجرائم الالكترونية الاقتصادية، المفهوم والدوافع، بحث منشور في مجلة دراسات قانونية واقتصادية، المجلد (٧)، العدد (١)، الجزائر، ٢٠٢٤.

رابعا: الرسائل والاطاريح

أ. الرسائل

١. إيناس ابراهيم الشيتي، تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربية السعودية دراسة تطبيقية على جامعة القصيم ، ماجستير غير منشورة، جامعة القصيم، ٢٠١٩.

٢. عبد الله حسين على محمود: سرقة المعلومات المخزنة في الحاسوب – رسالة ماجستير، كلية الحقوق– جامعة عين شمس، ٢٠٠١.

٣. عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسوب رساله ماجستير ، جامعه عين الشمس – كليه الحقوق ٢٠٠١.

٤. محمد نعمة كاظم، اتجاهات السياسة الجنائية في مكافحة الجريمة الاقتصادية، رسالة ماجستير، الجامعة المستنصرية – كلية القانون، العراق، بغداد، ٢٠٢١.

٥. نورة العقون، عبد الكريم باسماعيل، واقع الفضاء السيبراني وإشكالية الدفاع الوطني، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر، ورقلة، ٢٠١٩.

ب. الاطاريح

١. باسل فايز حمد القطاطشة، ممدوح حسن ماته، الحماية الجنائية لخصوصية البيانات الشخصية الرقمية، دراسة مقارنة، اطروحة دكتوراه، جامعة العلوم الإسلامية العالمية، عمان، ٢٠٢٢.

خامسا: المواقع الالكترونية

١. أحمد فاضل المعموري، الجرائم الإلكترونية في مواقع التواصل الاجتماعي حدود الشكوى والعقوبة والنقص التشريعي في القانون العراقي، الحوار المتمدن، العدد (٥٠٦٠)، https://www.ahewar.org
٢. د. علي ادهم، أمن المعلومات الجزء الثاني، مركز النهرين للدراسات الاستراتيجية، مقال منشور على الرابط الآتي: https://www.alnahrain.iq/post/392
٣. د.مينا فايق، الفرق بين الجرائم المعلوماتية والجرائم التقليدية، مقال متوفر على الرابط الآتي: https://www.menafayq.com/cybercrime-vs-traditional-crime/?utm_source=chatgpt.com

سادسا: المصادر الأجنبية

1. Arina Alexei ,Anatolie Alexei ,The difference between cyber security vs information security. Journal of Engineering Science, 29(4) , 2022.
2. Hathaway, R. M., McCreight, C., & Riley, J. (2012). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
3. ISO/IEC 27001. (2013). Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization, Appendix A Item.
4. Kizza, J. M. (2017). Guide to computer network security (4th ed.). Springer.
5. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in computing (5th ed.). PearsonP.
6. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology.
7. Shostack, A. (2014). Threat modeling: Designing for security. Wiley.
8. Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.

References

First: Linguistic Dictionaries

1. Ibn Manzur, Lisan al-Arab, Al-Amiriya Press, Bulaq, Volume 8, 1st Edition, no date given.

Second: Legal Books

1. Abdullah Suleiman, Explanation of the Penal Code (General Section - Crime), University Publications Office, Lebanon, 1998.
2. Ghassan Rabah, Economic Penal Code, Al-Halabi Legal Publications, Beirut, Lebanon, 2012 ed.
3. Muhammad Jibril Ibrahim, Criminal Liability for Robot Crimes: A Prospective Analytical Study, Dar Al-Nahda Al-Arabiya, 2020 edition.
4. Muhammad Ali Suwailem, Criminal Protection of the Stock Exchange: Between Procedural Aspects and Substantive Provisions: A Comparative Study, Modern University Office, 2018.
5. Hana Mustafa Al-Khubairi, Cybercrimes and the Regulation of Digital Currencies - A Legal Study in International Legislation and Agreements, Dar Al-Nahda Al-Arabiya, 2022.
6. The National Cybersecurity Authority, Basic Controls for Cybersecurity, Kingdom of Saudi Arabia, Riyadh, 2018.

Third: Research and Research Papers

1. Ahmed Hassan Abu Al-Hassan, The Extent of the Impact of Digitization on the Severity of Economic Crimes, a study published in Aswan University Journal For Humanities, Volume (4), Issue (1), Faculty of Law, Aswan University, 2024.
2. Dr. Ahmed Hosni Ali Ashqar, Digital Privacy in the Era of Artificial Intelligence (A Reading of Jordanian and Palestinian Legislation), a research published in the Journal of Al-Quds Open University, Issue 66, Volume 7, Palestine, Ramallah, 2025.
3. Balasal Bint Nabi Yasmine, Muqdad Nabil, The Right to Digital Privacy, a research published in the Al-Mustaqbal Journal for Legal and Political Studies, Volume 5, Issue 1, Yahya Fares University of Medea, Medea, Algeria, 2021.

4. Hakim Sayyab, The Distinctive Features of Cybercrimes from Traditional Crimes, a research published in the Journal of Studies and Research, Volume (2009), Issue (1), University of August 20, 1955 Skikda, 2009.
5. Dr. Dhiyab Musa Al-Badayneh, Cybercrimes: Concept and Causes, a paper presented at the Scientific Forum on Emerging Crimes in Light of Regional and International Changes and Transformations, Jordan, Amman, 2014.
6. Dr. Rahmouni Muhammad, Characteristics of Cybercrime and its Areas of Use, a study published in Al-Haqiqa Journal for Social and Human Sciences, Issue (41), Ahmed Draia University - Adrar, Algeria, 2017.
7. Rashid bin Hamad Al-Balushi, Evidence in Cybercrime, a study published in the Journal of the Faculty of Law for Legal and Economic Research, Volume (2008), Issue (1), Alexandria University, 2008.
8. Reda Ibrahim Saleh, A Study of the Impact of Information Security Management on the Success of the Accounting Information Systems Security Program with a Field Study of Egyptian Companies, Journal of Contemporary Business Studies, Volume 6, Issue 10, Part One, 2020.
9. Saad Fahd Saad Adbis Al-Mutairi, The Concept of Cybercrime and Its Characteristics, a study published in the Legal Journal (a semi-annual peer-reviewed scientific journal), Volume 16, Issue 5, 2023.
10. Faisal Ja'ilan Al-Azmi, The Problem of Criminal Prosecution in Cybercrimes, a study published in the Journal of the Faculty of Sharia and Law, Tanta, Volume (39), Issue (2), Cairo University. Egypt, 2024.
11. Qasmiya Muhammad, Sources and Methods of Money Laundering Operations, Journal of Legal Studies and Research, Volume 9, Issue 1, 2024.
12. United Nations Office on Drugs and Crime, Laboratory and Scientific Affairs Section of the United Nations Office on Drugs and Crime in Vienna, Crime Scene and Physical Evidence (Awareness-Raising for Non-Criminal Analysis Staff), 2009.
13. Musa Masoud Arhuma, Criminal Policy in Confronting Cybercrimes, a study published in the Journal of Legal Studies, University of Benghazi - Faculty of Law, Issue 17, 2008.
14. Mansour Fahid Saeed Al-Harthi, Obstacles to Proving Information Technology-Related Crimes, a study published in the Legal Journal (a specialized journal in legal studies and research), a peer-reviewed scientific journal, Volume (15), Issue (4), 2023.

15. Dr. Zuhair Khuraibat Khalaf, Confronting Economic Crimes in Iraqi Legislation, a study published in the Journal of Basra Studies, Year (20), Issue (60), 2025.
16. Ziad Abdel Razzaq, Mustafa Zaghbi, Economic Cybercrimes: Concept and Motives, a study published in the Journal of Legal and Economic Studies, Volume (7), Issue (1), Algeria, 2024.

Fourth: Theses and Dissertations

A. Theses

1. Enas Ibrahim Al-Sheety, "Evaluating Information Security and Privacy Policies in Educational Institutions in the Kingdom of Saudi Arabia: An Applied Study at Qassim University," unpublished master's thesis, Qassim University, 2019.
2. Abdullah Hussein Ali Mahmoud: "Theft of Computer-Stored Information," Master's Thesis, Faculty of Law, Ain Shams University, 2001.
3. Abdullah Hussein Ali Mahmoud, "Theft of Computer-Stored Information," Master's Thesis, Ain Shams University, Faculty of Law, 2001.
4. Muhammad Nimah Kazim, "Trends in Criminal Policy in Combating Economic Crime," Master's Thesis, Al-Mustansiriya University, College of Law, Iraq, Baghdad, 2021.
5. Noura Al-Aqoun and Abdul Karim Basmaeel, "The Reality of Cyberspace and the Problem of National Defense," Master's Thesis, University of Kasdi Merbah, Algeria, Ouargla, 2019.

B. Theses

1. Basil Fayez Hamad Al-Qattatsheh, Mamdouh Hassan Matta, Criminal Protection of Digital Personal Data Privacy: A Comparative Study, PhD Thesis, International Islamic University of Science and Technology, Amman, 2022.

Fifth: Electronic Websites

1. Ahmed Fadel Al-Maamouri, Cybercrimes on Social Media: Limits of Complaint, Punishment, and Legislative Deficiencies in Iraqi Law, Al-Hewar Al-Mutamadin, Issue (5060), https://www.ahewar.org

2. Dr. Ali Adham, Information Security, Part Two, Al-Nahrain Center for Strategic Studies, an article published at the following link: https://www.alnahrain.iq/post/392
3. Dr. Mina Fayq, The Difference Between Cybercrimes and Traditional Crimes, an article available at the following link: https://www.menafayq.com/cybercrime-vs-traditional-crime/?utm_source=chatgpt.com

Sixth: Foreign sources

1. Arina Alexei ,Anatolie Alexei ,The difference between cyber security vs information security. Journal of Engineering Science, 29(4) , 2022.
2. Hathaway, R. M., McCreight, C., & Riley, J. (2012). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
3. ISO/IEC 27001. (2013). Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization, Appendix A Item.
4. Kizza, J. M. (2017). Guide to computer network security (4th ed.). Springer.
5. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in computing (5th ed.). PearsonP.
6. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology.
7. Shostack, A. (2014). Threat modeling: Designing for security. Wiley.
8. Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.