العدد السابع والعشرون - الجزء الثالث - يوليو - 2026 - السنة الخامسة مجلة علمية فصلية محكمة

المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية

American International Journal of Humanities and Social Sciences

الالكتروني (3085 - 4806) (ISSN) / الورقي (3085 - 4830) (ISSN)

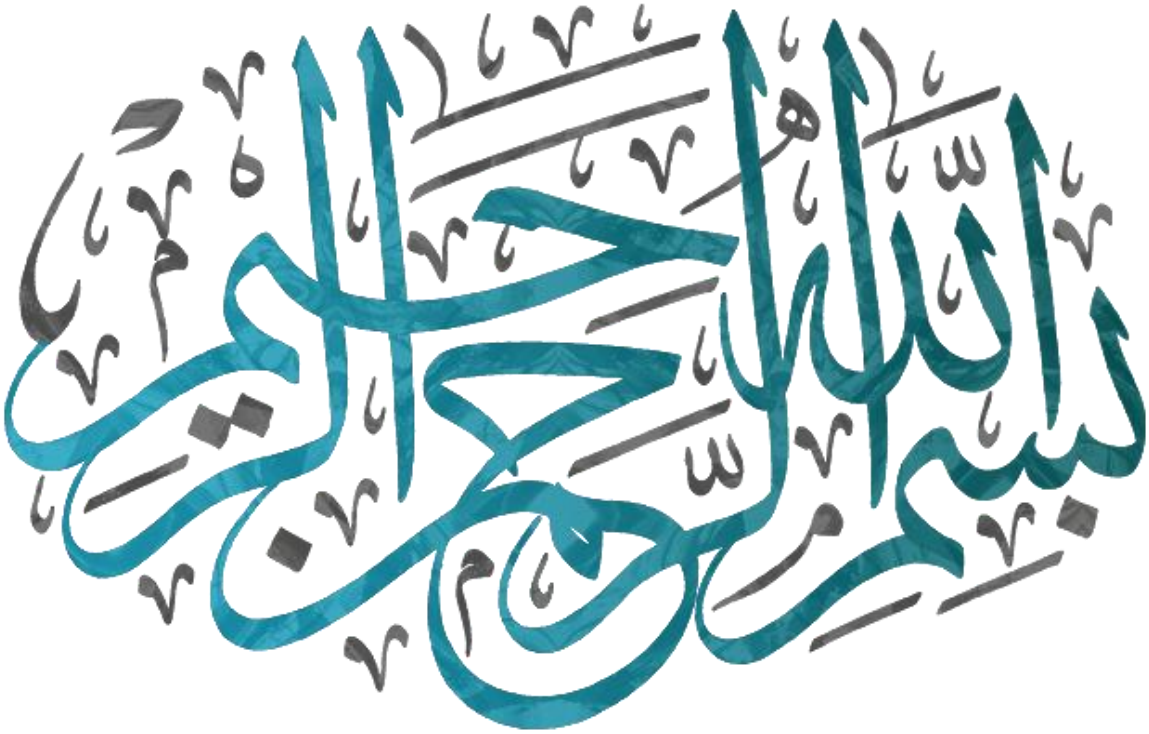
رقم الايداع القانوني في المكتبة الوطنية المغربية (2025 Pe00006)

رقم الايداع القانوني في دار الكتب والوثائق العراقية (2735)

تصدر عن الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب

ISSUED BY AMERICAN INTERNATIONAL ACADEMY OF HIGHER EDUCATION AND TRAINING

الموقع الرسمي للمجلة / www.iajphss.us


بسم الله الرحمن الرحيم

تتألف هيئة تحرير المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية من نخبة من العلماء والخبراء المتميزين من مختلف المؤسسات الأكاديمية الدولية. وتتولى الهيئة مسؤولية الحفاظ على جودة البحوث المنشورة وتقديم التوجيه الاستراتيجي لتطوير المجلة.

رئيس التحرير-أ.د.نزهة إبراهيم الصبري – نائب رئيس الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب- المملكة المغربية

نائب رئيس التحرير : أ.د. حاتم جاسم الحسون، رئيس الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب.

مدير التحرير- أ.د. هند عباس على الحمادي-أستاذ بقسم اللغة العربية وعلومها-كلية التربية للبنات-جامعة بغداد، جمهورية العراق (مدقق اللغة العربية).

https://orcid.org/my-orcid?orcid=0009-0003-0515-501X

سكرتارية التحرير

1. أ.م.د. محمد حسن أبو رحمة . وزارة التربية – فلسطين .
2. أ.سكينة إبراهيم الصبري. الشؤون الإدارية. الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب.

أعضاء هيئة التحرير

1. أ.د. حسن يوسف – استاذ اللغة العربية آدابها – جامعة قناة السويس – مصر- المدقق العام.
2. أ.د. خالد ستار القيسي ،عميد كلية الإعلام ، الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب.
3. أ. مجدي عبد الله الجايح،كلية اللغات والعلوم الإنسانية،الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب. (مدقق اللغة الإنكليزية)
4. المهندس اسماعيل المساق ، كلية علومالتقنية ،جامعة محمد الخامس ،الرباط، المملكة المغربية.

(التصميم)

5. أ.محمد تايه محمد - بك إدارة أعمال - كلية الإدارة والاقتصاد - جامعة الكوفة. (التنضيد) . https://orcid.org/0009-0003-6945-2806

أعضاء الهيئة العلمية

1. Prof. Dr Hanik Mahliatussikah - State University of Malang, Indonesia, Chairman of the Association of Arabic Language Teaching Departments in Indonesia.
2. Prof. Dr. Shamnad N - University College, Thiruvananthapuram, Kerala, India.
3. Prof.Dr.Ali H. ABDUL RASOL - KDG College - Leerexpert -England.
4. Dr.MUSTAPHA ABDUL AZIZ AKANJI - Président-Fondateur des groupes scolaires et Universitaires AKANJI En Côte d'ivoire et Nigeria.
5. Dr.Nada Al-Abidi - Educational Sciences Teaching Curricula, Methods, and E-Learning - Sweden
6. أ.د. أبكر عبد البنات آدم . مدير جامعة القرآن الكريم وتأصيل العلوم . جمهورية السودان https://orcid.org/0009-0009-8298-4464.
7. أ.د. رانيا الصاوي عبده عبد القوي – قسم علم نفس تربوي – كلية التربية – جامعة 6 اكتوبر – مصر https://orcid.org/0000-0001-7436-2774 .
8. أ.د. آمال العرباوي مهدي - رئيس قسم التربية المقارنة بكلية التربية مصر https:/://orcid.org0009-0005-3260-820X .
9. أ.د. أمل مهدي جبر- رئيس قسم العلوم التربوية والنفسية . كلية التربية للبنات . جامعة البصرة، جمهورية العراق https://orcid.org/0000-0001-7463-9876 .
10. أ.د. ناهض فالح سليمان- كلية التربية للعلوم الإنسانية . قسم اللغة الإنجليزية . جامعة ديالى . جمهورية العراق https://orcid.org/0009-0009-7896-820X .
11. 1.أ. د نور الدين زين العابدين متولي أحمد - رئيس قسم اللغة العربية وآدابها بكلية العلوم الإنسانية بجامعة بيروت العربية - لبنان https://orcid.org/0009-0006-7020-7244 .
12. أ.د. نصيف جاسم أسود سالم الأحبابي. كلية التربية للعلوم الإنسانية. قسم الجغرافية. جامعة تكريت. جمهورية العراق https://orcid.org/0009-0002-6669-4706 .
13. أ.د. نورة محمد مستغفر . أستاذ التعليم العالي مؤهل، المركز الجهوي لمهن التربية والتكوين، المملكة المغربية https://orcid.org/0009-0001-4682-2005 .
14. أ.د. هاله خالد نجم- رئيس قسم الترجمة . كلية الآداب- جامعة الموصل – جمهورية العراق). https://orcid.org/0009-0004-3687-1788).
15. أ.د. محمد خضير عباس الجيلاوي - كلية الطوسي الجامعة – النجف الاشرف – العراق. https://orcid.org/0009-0001-9668-9329
16. أ.د. محمد نهان ابراهيم رحيم الهيتي – علوم اسلامية – جامعة الانبار – العراق. 0000-0003-4092-6193
17. أ. د. سميرة شمعاوي –استاذة باحثة بمركز التوجيه والتخطيط التربوي بالرباط – المغرب. https://orcid.org/0009-0008-2452-6011

18. أ.د. برزان ميسر حامد أحمد الحميد . كلية التربية للعلوم الإنسانية. جامعة الموصل . جمهورية العراق.(https://orcid.org/0009-0003-7795-3934)

19. .أ. د.محمد ازهري - جامعة السلطان مولاي سليمان - كلية الآداب والعلوم الإنسانية. بني ملال. المغرب.

20. أ.د. تارا عمر أحمد- كلية العلوم السياسية . جامعة السليمانية . جمهورية العراق-https://orcid.org/my-orcid?orcid=0009-0003-9424-6211 .

21. أ.د.تحرير علي حسين علوان – كلية الفنون الجميلة – جامعة البصرة – جمهورية العراق. https://orcid.org/0009-0002-0076-0491

22. محمد لؤي محمد سليم البني معهد الحضارة للتأهيل والتدريب السياحي والفندقي | دمشق، سوريا. 0009-0008-2826-7088

23. أ. د. الشرقي عبد الحليم – كلية الآداب والعلوم الانسانية – سايس – جامعة - سيدي محمد بن عبد الله - فاس – المملكة المغربيةhttps://orcid.org/0000-0002-6947-5712 .

24. أ.د. داود مراد حسين الداودي . دكتوراه العلوم السياسية . مدير وحدة البحوث والدراسات . جامعة القادسية . كلية القانون . جمهورية العراقhttps://orcid.org/0009-0000-3272-5899 .

25. أ.م.د. عزيز عبدالرحمن محمد الاديمي -جامعة تعز - مدير عام بحوث التنمية الادارية والتدريب - ديوان عام محافظة تعز – اليمنhttps://orcid.org/0009-0005-2702-0495 .

26. أ.م.د. علاء الدين محمد حسين عياش – رئيس قسم تكنولوجيا الاعلام -جامعة فلسطين التقنية – فلسطينhttps://orcid.org/0000-0001-8152-9261 .

27. أ.د. سندس عزيز فارس الفارس- خبير تربوي- عميد كلية الدراسات العليا والبحث العلمي في الاكاديمية الأمريكية . جمهورية العراقhttps://orcid.org/0009-0002-7185-1059.

28. أ.د.عدنان فرحان الجوراني . أستاذ الاقتصاد . جامعة البصرة . جمهورية العراق-https://orcid.org/0009-0006-6673-5714) .)

29. د. حلا عدنان نيربي – كلية الاقتصاد – قسم المحاسبة – جامعة حلب - سوريا-https://orcid.org/0009-0006-5511-3266.

30. أ.د. ماجدولين محمد النهيبي- كلية علوم التربية . جامعة محمد الخامس . الرباط، المملكة المغربية :Orcid id. 0009-0000-1125-8689

31. د. ياسر حسن ناجي الصلوي – جامعة تعز – اليمنhttps://orcid.org/0009-0006-7335-3570 .

32. أ.د. ماهر مبدر عبد الكريم العباسي . نائب عميد كلية التربية للعلوم الإنسانية . جامعة ديالى . جمهورية العراق. 0009-0006-0681-1033

33. أ.د. حاكم موسى عبد الحسناوي - استاذ طرائق تدريس التأريخ - وزارة التربية - الكلية التربوية المفتوحة - جمهورية العراقhttps://orcid.org/0000-0002-3992-672X?lang=ar.

34. د. ليلى الادريسي – دكتوراه في القانون والعلوم السياسية – كلية العلوم القانونية والاقتصادية والاجتماعية – جامعة محمد الخامس – الراط - المغرب.
0009-0005-8175-7113

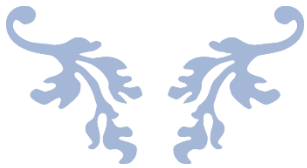
35.أ.م.د.آوان عبد الله محمود الفيضي . دكتوراه قانون خاص . كلية الحقوق . جامعة الموصل . جمهورية العراق https://orcid.org /0000-0001-8777-978x .

أعضاء الهيئة الاستشارية

1. أ.د.هالة مختار الوحش – استاذ اصول التربية الانسانية جامعة الازهر – مصر https://orcid.org/0009-0008-8680-0194 .
2. .أ.د. محمد علي عباس – علوم تربوية نفسية – الاكاديمية الامريكية الدولية للتعليم العالي والتدريب-أمريكا https://orcid.org/0009-0004-2576-8136 .
3. أ.د. حسن يوسف – استاذ اللغة العربية آدابها – جامعة قناة السويس - مصر.
4. د. عائشة الهوس – تخصص القانون العام والعلوم السياسية - المعهد المغربي للدراسات الاستراتيجية وإدارة الأزمات – المملكة المغربية https://orcid.org/0009-0000-4666-3086 .
5. أ.د. ناهض فالح سلمان - كلية التربية - جامعة ديالى - العراق https://orcid.org/0009-0009-7896-820X .
6. أ.د. رائد بني ياسين- عميد كلية الأعمال . قسم نظم المعلومات . الجامعة الأردنية- فرع العقبة . المملكة الأردنية الهاشمية(https://orcid.org/0009-0004-3687-1788) .
7. د. نادية فضيل – المركز الجهوي لمهن التربية والتكوين – بني ملال – المغرب.
8. د. هشام الميموني، دكتور في القانون العام، جامعة الحسن الثاني - الدار البيضاء ، كلية الحقوق - المحمدية(المغرب)
0000-0002-9569-3369
9. أ.م. د. سماح هادي محمد – كلية الحقوق – جامعة النهرين – جمهورية العراق https://orcid.org/0009-0006-9104-6347 .
10. أ.م.د.ايمان محمد مصطفى – كلية الدراسات العليا لتكنولوجيا النانو – مدير معمل الطاقة الشمسية – جامعة القاهرة – مصر. X575-6465-0001-0000
11. م. د. حامد شمال مصحب - كلية الحكمة الجامعة تكنولوجيا المعلومات والاتصالات والذكاء الاصطناعي – العراق https://orcid.org/0000-0002-4382-0872 .
12. أ.د. ماهر جاسب حاتم الفهد – تحصص التاريخ الحديث والمعاصر - كلية الإمام الكاظم "ع" قسم التأريخ – العراق https://orcid.org/0000-0001-5708-2527 .
13. د. نجلاء حمدان رحمة الله جادين - جامعة جازان / كلية الفنون والعلوم الإنسانية المملكة العربية السعودية https://orcid.org/0009-0008-5146-475X .

14. أ.د.علي سموم الفرطوسي - الجامعة المستنصرية / كلية التربية البدنية وعلوم الرياضة - أستاذ القياس والتقويم - الإحصاء - كرة السلة - حكم ومراقب فني دولي بكرة السلة - العراق.
ORCID : https://orcid.org/0000-0002-8598-5149
15. أ.د. مازن خلف ناصر. كلية القانون . جامعة المستنصرية . جمهورية العراق https://orcid.org/0000-0003-3754-4266 .
16. أ.م.د. محمد عبدالفتاح زهرى- رئيس قسم الدراسات الفندقية- كلية السياحة والفنادق – جامعة المنصورة- جمهورية مصر العربية(ORCID.org/0000-0002-8533-6552) .
17. م.د. محمد مولود امنكور . كلية العلوم الإدارية والمالية والاقتصادية . الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب https://orcid.org/0009-0000-8373-5528 .
18. أ.م.د. موسى إسماعيل صالح حسين - أستاذ مساعد الأدب والنقد العربي قسم اللغة العربية - جامعة جرش / الأردن https://orcid.org/0009-0007-7197-1954
19. أ.د. جاسم حسن سالم العطبي - طبيب عام - البصرة – العراق. 0009-0001-2819-1975

كلمة العدد



بسم الله الرحمن الرحيم

يسرّنا في **المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية** أن نضع بين يدي الباحثين والأكاديميين والقراء الكرام هذا الجزء الثالث من العدد السابع والعشرين، والذي خصصناه لنشر النتاج العلمي والبحوث المشتركة التي أُثري بها **المؤتمر العلمي الدولي الثالث عشر**.

يجيء هذا العدد مستجيباً للرؤية العلمية والتنسيقية التي سعى المؤتمر إلى تحقيقها، والمتمثلة في تعزيز ثقافة البحث العلمي المشترك والرصين، وتجسير الفجوات بين أرباب التخصصات المختلفة في مجالات العلوم الإنسانية والاجتماعية. إن الشراكة البحثية لم تعد مجرد خيار أكاديمي، بل أصبحت ضرورة ملحة لمواجهة التحديات المعاصرة، ورسم معالم حلول منهجية وشاملة تتعدى نطاق الرؤية الفردية إلى آفاق العمل الجماعي المتبصر.

وقد شهد هذا الجزء تنوعاً وثراءً لافتاً في الموضوعات المطروحة؛ حيث توزعت الأوراق البحثية المنشورة بين دراسات تحليلية، وميدانية، ونظرية تلامس أحدث القضايا وأشدها ارتباطاً بالواقع الإنساني والاجتماعي. وقد خضعت جميع هذه البحوث لمقاييس محكمة من التقييم والمراجعة العلمية لضمان استيفائها لأعلى معايير الرصانة والدقة والأمانة الأكاديمية المتعارف عليها دولياً.

وإذ نُقدّم هذا العدد، فإننا نتوجه بخالص الشكر والتقدير لكل الباحثين والمشاركين الذين أسهموا ببحوثهم ونتاجاتهم الفكرية في إنجاح أعمال المؤتمر وتغذية صفحات هذا العدد. كما نُثمن جهود أعضاء الهيئة الاستشارية وهيئة التحكيم ولجان المؤتمر على ما بذلوه من عمل دؤوب ودقة في الفحص والتدقيق لتقديم هذا العمل بالصورة المشرقة التي يليق بها.

وكذلك تضمن العدد بعض البحوث المنشورة لباحثين عرب خارج اعمال المؤتمر المذكور.

ختاماً، نأمل أن يشكل هذا العدد إضافة نوعية للمكتبة العربية والدولية، وأن يفتح آفاقاً جديدة أمام الباحثين لمزيد من العطاء والابتكار العلمي المشترك.

والله ولي التوفيق.

29 /2026/07 ديلاوير- الولايات المتحدة الامريكية — هيئة تحرير المجلة

الملاحظة القانونية

البحوث المنشورة في المجلة لا تعبر عن وجهة نظر المجلة، بل عن رأي كاتبها.

جدول المحتويات

دور استراتيجيات التسويق الرقمي في تحديد وتحسين تكاليف الجودة: دراسة ميدانية في مصنع النرجس للأنابيب البلاستيكية في البصرة / العراق
م.د حسن عبود معروف / م.م محمد جهاد محسن 11

أثر التدريس باستخدام الخرائط الذهنية الإلكترونية في استيعاب مفاهيم العقيدة الإسلامية لدى طلاب الإعدادية
م. د إخلاص خلف لفته..... 50

فلسفة الحياة والموت في الشعر الجاهلي
د. موسى إسماعيل حسين..... 70

الدّمج بين الثّقافة العربيّة واللّغة في مناهج تعليم النّاطقين بغيرها: تحدّيات وحلول مبتكرة
د. طلال عبد الله طافش المراشدة..... 80

الحماية القانونية للعقود الذكية في حقوق الملكية الفكرية " دراسة تحليلية في التشريعات العربية "
د. كمال الأمين محمد فضل الله الفادنى..... 98

شعرية التوحش والميتافور الحيواني – تفكيك الأنساق المضمرة والسلطة في مجموعة «مصادقة الحيتان" لحسن البصّام
م.د. مسار حميد عبد..... 138

قصيدة "أنشودة المطر" لـ بدر شاكر السياب: دراسة تحليلية في ضوء الابعاد اللغوي
م. د. موسى جاسم عجيل العبادي..... 161

المسؤولية الجزائية عن الجرائم السيبرانية
د.راسم مسير جاسم..... 178

صوت المرأة في أدب الأندلس: دراسة في السرد النسوي المغيَّب
م.م. فضيلة فاضل كريم..... 200

الدور القرآني واثره وتداعياته في سلوكيات الطفل المسلم
ختام مزهر حمد الجبوري..... 217

الوعي بالذكاء الاصطناعي وعلاقته بالكفاءة الرقمية لدى معلمي المدارس العربية في الداخل الفلسطيني
لنا جهاد عبد الرحمن حاج يحيى..... 230

التدابير السياسية والإدارية في قصة يوسف عليه السلام: دراسة تأصيلية في السياسة الشرعية ونظم الحكم من منظور أصول الدين
مختار طالب محمد الطاهر طالب..... 261

التحليل الجغرافي لواقع ومؤشرات كفاءة التعليم الأهلي في مدينة المدحتية – وفق المعايير التخطيطية

منار علي سلطان السعيدي.....271

دراسة واقع المشكلات السلوكية في درس التربية الرياضية للمرحلة الابتدائية
من وجهة نظر المعلمين والمعلمات في محافظة بابل
م . م ميادة حسن حمزة.....309

مواقع التواصل الاجتماعي والحق في الخصوصية الرقمية " التشهير نموذجا"
عواطف الازهاري.....322

تطور الفكر الواقعي في العلاقات الدولية من مورغنثاو إلى والتز
المدرس المساعد / وفاء زايد عباس.....333

School Leadership Support for Technology Integration and Its Impact on Secondary Education Quality: A Narrative Review and Conceptual Model
Ahlam Azaiza.....361

المسؤولية الجزائية عن الجرائم السيبرانية

د.راسم مسير جاسم

كلية المنصور الجامعه – العراق

rasem.mseer@muc.edu.iq

009647810052055

الملخص

يشهد العالم المعاصر تطوراً تقنياً متسارعاً جعل من الفضاء السيبراني جزءاً لا يتجزأ من حياة الأفراد والمؤسسات والدول، وأوجد في الوقت نفسه أنماطاً جديدة من السلوك الإجرامي تتجاوز الحدود الجغرافية وتستغل الطبيعة اللّامادية للبيئة الرقمية. وقد أدّى ذلك إلى بروز تحديات عميقة أمام التشريعات الجزائية التقليدية، التي وُضعت أساساً لحماية المصالح المادية والملموسة، ولم تُصمَّم للتعامل مع الاعتداءات التي تقع بواسطة الأنظمة المعلوماتية أو تستهدف البيانات الرقمية.

ينطلق هذا البحث من الحاجة الملحّة إلى دراسة المسؤولية الجزائية عن الجرائم السيبرانية في ضوء التطور التقني والفراغات التشريعية القائمة، ولا سيما في النظام القانوني العراقي. ويستعرض البحث مدى قدرة النصوص العقابية العامة على استيعاب هذه الأفعال، ويوضح مكامن القصور التي تحول دون مساءلة الجناة مساءلة فعّالة، سواء بسبب الطبيعة التقنية للجريمة، أو صعوبة تحديد مكان وقوعها والفاعل الحقيقي وراءها.

يخلص البحث إلى أن التشريعات التقليدية بما فيها التشريع العراقي غير كافية لمواجهة خطورة الجرائم السيبرانية وتطورها المستمر، وأن الحاجة باتت ملحّة لإصدار تشريع متخصص يتضمن تعريفات دقيقة، وصوراً واضحة للتجريم، وعقوبات ملائمة، وإجراءات خاصة بالإثبات والتحقيق الرقمي، مع تعزيز دور التعاون الدولي في مكافحة الجرائم العابرة للحدود.

الكلمات المفتاحية: الجرائم السيبرانية – الأمن السيبراني– الأدلة الرقمية– الاختراق الإلكتروني– البيانات الشخصية.

Criminal Liability for Cybercrimes

Rasim Masir Jasim

Al-Mansour University College

Abstract:

The contemporary world is witnessing rapid technological advancement that has made cyberspace an integral part of the lives of individuals, institutions, and states. At the same time, this development has produced new forms of criminal behavior that transcend geographical boundaries and exploit the immaterial nature of the digital environment. This situation has created profound challenges for traditional criminal legislation, which was originally designed to protect tangible and material interests and was not crafted to address offenses committed through information systems or targeting digital data.

This research stems from the urgent need to examine criminal liability for cybercrimes in light of technological progress and existing legislative gaps, particularly within the Iraqi legal system. The study explores the extent to which general criminal provisions can encompass these acts and highlights the shortcomings that hinder effective prosecution of offenders, whether due to the technical nature of the crime or the difficulty of identifying the location of the offense and the true perpetrator behind it.

The research concludes that traditional legislation—including Iraqi law—is insufficient to confront the growing seriousness and continuous evolution of cybercrimes. It emphasizes the need for a specialized legal framework that provides precise definitions, clear forms of criminalization, appropriate penalties, and specific procedures for digital evidence and cyber investigations, in addition to strengthening international cooperation in combating cross-border cybercrimes.

Keywords:

Cybercrimes, Cybersecurity, Digital Evidence, Electronic Hacking, Personal Data.

المقدمة

يتميز زمننا الرقمي الراهن بالانتشار الكثيف لتكنولوجيا المعلومات وأنظمة الاتصالات فنحن نشهد عالما تتم صياغته من جديد، حيث يتشكل عالم رقمي سيبراني تديره الشبكات الرقمية، وتلعب فيه شبكة الانترنت الدور الأساسي في إدارة الشؤون الحياتية اليومية.

وفي ظل تغلغل تكنولوجيات الاتصال الالكتروني في معظم القطاعات الحياتية الحيوية ارتفع عدد مستخدمي شبكات الانترنت على مستوى العالم وتبعاً لذلك ازدادت الهجمات والجرائم الرقمية، وأصبحت التهديدات السيبرانية أكثر خطورة، وهي ترتكب بوتيرة متسارعة.

نتيجة لهذا التطور اتجهت العديد من الدول نحو وضع استراتيجيات وطنية شاملة لضمان أمان المعلومات في الفضاء السيبراني، إذ أصبح أمان المعلومات مكوناً أساسياً يتجذر في مفهوم الأمن الوطني ويشمل المؤسسات والأفراد، وقد أدركت الدول أن التغيرات السريعة في التكنولوجيا تشكل تحديات جديدة لأمان الوطن والمواطن، مما دفعها إلى العمل على ضمان أمان المعلومات كجزء أساسي من الأمان السيبراني، فيعتمد الأمان السيبراني على مجموعة من الوسائل القانونية والتقنية لمقاومة الاستخدام غير القانوني للإنترنت وحماية نظم المعلومات ووسائل الاتصالات بهدف حماية الوطن والمواطن والمؤسسات من مخاطر الفضاء السيبراني.

أهمية البحث:

تنبع أهمية هذا البحث من أن الجرائم السيبرانية أصبحت تمثّل أحد أخطر التحديات التي تواجه المنظومات القانونية في العالم المعاصر، بعد أن تحولت الفضاءات الرقمية إلى بيئات عمل وتواصل وتبادل معلومات لا تقل خطورة وتأثيراً عن الواقع المادي. فمع تزايد الاعتماد على التكنولوجيا في المؤسسات الحكومية والقطاع الخاص والأفراد، أصبحت الأنظمة المعلوماتية والبيانات الشخصية والأصول الرقمية عرضةً لاعتداءات تتسم بالسرعة، وسهولة الإخفاء، وعبر — غالباً — حدود الدول.

وتبرز أهمية هذا البحث في عدة جوانب أساسية، منها:

1- قصور التشريعات التقليدية، وخاصة التشريع العراقي، عن استيعاب الطبيعة الخاصة لهذا النوع من الجرائم، مما يجعل من الضروري دراسة المسؤولية الجزائية للجناة وفق رؤية حديثة تتناسب مع التطور التقني.

2- تعدد صور الجرائم السيبرانية وتشابك آثارها، إذ لم تعد تقتصر على الاعتداء على البيانات والمعلومات، بل أصبحت تمس الأمن العام والاقتصاد الوطني والخصوصية الرقمية، وأحياناً تهدد الأمن السيبراني للدولة.

3- الحاجة إلى إطار جزائي فعّال قادر على ردع الجناة ومساءلتهم بما ينسجم مع خطورة الأفعال المرتكبة رقمياً، وذلك في ظل التطور الهائل لأساليب الهجوم السيبراني، ومنها: الاختراق، والتجسس الرقمي، والاحتيال الإلكتروني، والبرمجيات الخبيثة.

إشكالية البحث:

تتمثل إشكالية هذا البحث في **قصور المنظومة القانونية التقليدية عن استيعاب الطبيعة المستجدة والمعقدة للجرائم السيبرانية**، وما يرافقها من تحديات تتعلق بطبيعة الفعل الإجرامي، ووسائل ارتكابه، وكيفية اكتشافه وإثباته، وتحديد المسؤولية عنه، خصوصاً في ظل الطابع اللّامادي والعابر للحدود لهذه الأفعال.

وتتفرع هذه الإشكالية العامة إلى تساؤلات رئيسة، أهمها:

1. ما مدى قدرة التشريعات الجزائية القائمة – وبالأخص التشريع العراقي – على مواكبة الجرائم السيبرانية، وتجريم صورها المستحدثة؟
2. كيف يمكن تحديد المسؤولية الجزائية عن الأفعال السيبرانية في ظل غياب نصوص قانونية صريحة تغطي كافة صورها؟
3. هل تكفي القواعد العامة في قانون العقوبات لإسناد المسؤولية إلى الجناة في البيئة الرقمية، أم أن هذه الجرائم تحتاج إلى تنظيم خاص؟

منهج البحث:

للإلمام بموضوع البحث اتبعنا أكثر من منهج بحثي، إذ اتبعنا المنهج التحليلي وذلك من خلال تحليل نصوص قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل لبيان مدى كفايتها لتجريم الاعتداءات السيبرانية، مع بيان بعض الأحكام الواردة في مشروع قانون جرائم المعلوماتية العراقي، كما اعتمدنا المنهج المقارن لمقارنة ما توصلنا له من أحكام مع بعض الأحكام الواردة في التشريعات المقارنة كلما دعت الحاجة لذلك.

خطة البحث:

اعتمدنا في هذا البحث التقسيم الثنائي إذ قسمناه على مبحثين كالآتي:

المبحث الأول: ماهية الجرائم السيبرانية.

المبحث الثاني: الإطار القانوني للأمن السيبراني العراقي. المبحث الأول

ماهية الجرائم السيبرانية

من سمات زمننا الراهن التطور الهائل في أسلوب ارتكاب الجرائم، فلم تعد الافعال الجرمية تقتصر على استهداف الأموال والانفس فحسب، بل تعرضت حتى للمعلومات في الانظمة المعلوماتية السيبرانية، فقد اتيح للمجرم العصري ان يرتكب أشنع واخطر الجرائم في راحة تامة وحتى دون ان يتكلف عناء الانتقال من مكانه، ومن أجل فهم هذا النوع الجديد من الاجرام سنبحث في التعاريف التي اعطيت له، مع استعراض المراحل الزمنية التي مر بها.[1](**العمارات: جرائم العصر من الرقمية الى السيبرانية : 2023، ص16**) ولبيان ذلك سنقسم هذا المبحث على مطلبين، سنتطرق في المطلب الأول لدراسة تعريف الجرائم السيبرانية، أما المطلب الثاني فسنتطرق فيه لدراسة التطور الزمني للإجرام السيبراني.

المطلب الأول

تعريف الجرائم السيبرانية

إن الجرائم السيبرانية التي تتعرض للمعاملات الالكترونية هي أحدى نتائج التطور التكنولوجي الرقمي المتسارع[2](**جعفر: جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة:2013: ص20**) وقد اتخذت كظاهرة اجرامية مجالا واسعا من الدراسات التي حاولت تبيان طبيعتها، حيث سعت العديد من الدراسات الحقوقية الى اعطاء تعريف للجرائم المرتكبة بواسطة شبكة الانترنت

العالمية[1] (البداينة: **الجرائم الإلكترونية المفهوم والاسباب ورقة علمية مقدمة في الملتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية: 2022: ص 5**)

، ففي بادئ الأمر تم اعتبارها كأفعال تدخل في خانة إساءة استعمال الكمبيوتر، ومن ثم تطور الأمر وتم تصنيفها كجرائم احتيال بواسطة الكمبيوتر ومن ثم ظهر مصطلح الجرائم المعلوماتية، ومن بعدها استعمل مصطلح جرائم التقنيات العالية، او جرائم الانترنت، وأخيرا الجرائم السيبرانية.[2](**بونعاره: الجريمة الالكترونية مجلة المعيار: مجلد 2 عدد 39: جوان: 2015 : ص3: وايضا عبد العال الدربي: الجريمة الالكترونية: 2012: ص 32**)

انطلاقا مما سبق ذكره، يتضح أن المقصود من مصطلح الاجرام السيبراني، هو السلوكيات الجرمية التي تتم داخل العالم الافتراضي، والتي تخضع للقانون الجنائي[3](**القهوجي: الحماية الجائية لبرامج الحاسب الآلي : 1999، ص4**) وهو السبب الرئيسي والدافع لاستخدام مصطلح الجريمة السيبرانية في هذا البحث، حيث سنتناول تعريف الجريمة السيبرانية في فرعين سنتناول في الفرع الأول تعريف الجريمة السيبرانية وفق محل الجريمة ومعيار المعرفة أما في الفرع الثاني سنتناول تعريف الجريمة السيبرانية وفق موضوعها ومعاييرها المتنوعة.

الفرع الأول

تعريف الجريمة السيبرانية وفق محل الجريمة ومعيار المعرفة

ان حداثة الاجرام السيبراني زمنيا، واختلاف الانظمة القانونية للدول، جعل من الصعوبة بمكان الاتفاق على تعريف موحد للإجرام السيبراني[4] (**الملط: الجرائم المعلوماتية : 2006: ص 83**). لذلك نرى ان فقهاء العلم القانوني الجنائي قد افترقوا إلى اكثر من اتجاه في تعريف الجريمة السيبرانية، لكل مضمار او اتجاه الاسس التي يعتمدها ويبني عليها موقفه في اعطاء تعريف للجرائم السيبرانية، لقد جذب تعريف الجريمة السيبرانية اهتمام فقهاء القانون والباحثين المختصين في المجالات المعلوماتية، فحاول كل منهم وفق منظوره واختصاصه اعطاء تعريف مناسب لها، ويلاحظ عدم اتفاقهم على تعريف موحد يتناول هذا النوع من الجرائم المرتكبة في الفضاء السيبراني المعلوماتي عبر شبكة الانترنت، حيث سنتناول في هذ الفرع تعريف مبني على محل الجريمة أما التعريف الثاني سيكون مبني على المبني على معيار المعرفة والتحكم في التكنولوجيا وفق الآتي :

أولا: التعريف المبني على معيار "محل" الجريمة:

يرتكز أصحاب هذا التعريف على الوسيلة التي ارتكبت بواسطتها الجريمة، فمنهم من عرفها باعتبارها جرائم مرتبطة بالكمبيوتر او انها جرائم يستعمل فيها الكمبيوتر.[5](**لعتبي: الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية : 2010: ص21**)

فطالما أن الوسيلة التي يرتكب بواسطتها الجرم هي الكمبيوتر، او اية وسيلة اخرى من وسائل التقنيات المعلوماتية المتطورة الحديثة، فيعتبر عندئذ الجرم من ضمن الجرائم السيبرانية التي ترتكب عبر شبكة الانترنت[1](**الجنبيهي: جرائم الانترنت والحاسب الآلي ووسائل مكافحتها :201: ص13**). وينحو انصار هذا الاتجاه الى التضييق من نطاق هذه الجرائم السيبرانية، حيث اعتبروا انها تنال من المكونات غير المادية للحواسيب، كالبرامج والبيانات التي يتم تخزينها ضمن ذاكرتها[2] (**الدريبي: الجرائم الإلكترونية: دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت : 2012: ص42**) ووفقاً لذلك عرف مكتب التقييم التقني في الولايات المتحدة الامريكية الجريمة السيبرانية بانها "الجريمة" التي يكون فيها للبيانات الحاسوبية والبرامج المعلوماتية دوراً رئيسياً (**السعدي الحماية الجنائية لبرامج الحاسوب: 12004: ص62**)[3].

وقد تم تعريفها من قبل البعض الآخر وفق صياغة مغايرة بانها: الجرائم الناجمة عن استعمال التكنولوجيات والتقنيات المتطورة المتمثلة في الحاسوب والانترنت[4] (**قشقوش: جرائم الحاسب الالكتروني في التشريع المقارن: 2017: ص19**) في اعمال إجرامية ترمي إلى تحقيق منافع كبيرة جراء نشاطات غير شرعية، حيث يعاد ضخها في النظام المالي الدولي عبر الانترنت بإستعمال العملة الالكترونية او البطاقات الممغنطة التي يمكن بواسطتها الشراء الالكتروني، او لتداول الاسهم وممارسة الانشطة التجارية .[5](**عبد الله: جرائم المعلوماتية والانترنت: 2007 : ص15**)

وقد انتقد الاستاذ فاندرسون" هذا التعريف حيث رأى انه لا يكفي أن يستخدم الكمبيوتر في الجريمة لكي نصنفها على انها من الجرائم الرقمية السيبرانية، واضاف بانه لا يمكننا وضع تعريف للجرائم السيبرانية دون العودة إلى العوامل الاساسية المكونة لها، حيث لا يمكن الاقتصار فحسب على الوسائل المستخدمة لتحقيقها لاعتبارها كجريمة معلوماتية او سيبرانية.

ثانيا : التعريف المبني على معيار المعرفة والتحكم في التكنولوجيا

ان أنصار هذا الراي يعتمدون على المعيار الشخصي لتعريف الجريمة السيبرانية، إذ يقتضي أن يكون فاعل هذه الجرائم ملما وعالما بالتقنيات المعلوماتية، ومن نمط هذه التعريفات نرى التعريف الوارد عن الاستاذ ديفيد تومبسون للجريمة السيبرانية حيث رأى أنها الجريمة التي يتوافر لفاعلها المعرفة الوافية بتقنيات الحاسوب[6] (**رستم: الجرائم المعلوماتية أصول التحقيق الجنائي الفني:2004: ص407**)كما انبرى الفقيه "ستين سكيلبيرج" لتقديم التعريف بالجريمة السيبرانية باعتبارها مجمل الافعال غير الشرعية التي تتطلب ان تكون المعرفة بالتقنيات المعلوماتية ضرورية لارتكابها والتحقيق فيها وملاحقتها امام القضاء، ولقد اعتمدت وزارة العدل الأمريكية لهذا

التعريف في تقريرها لعام 1989 المتعلق بالجرائم الرقمية السيبرانية .[1] **(معتوق:الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن: 2012: ص 7)**

ووفق رؤية أصحاب هذا التعريف، لا بد من توافر السمات الشخصية لدى مرتكبي هذا النوع من الاجرام المعلوماتي، والمنحصرة في الإلمام الوافي بالمعارف التقنية، كما تبين مما تقدم أن الفقه القانوني قد اتجه إلى تعريف الجريمة السيبرانية وفق معيارين رئيسيين، أولهما معيار محل الجريمة الذي يركز على الوسيلة المستخدمة في ارتكاب الفعل الإجرامي، حيث يعد الحاسوب أو التقنيات المعلوماتية الأداة الأساسية لوقوع الجريمة، أما المعيار الثاني فهو معيار المعرفة والتحكم في التكنولوجيا، الذي ينظر إلى الخصائص التقنية لمرتكب الجريمة، ومع ذلك فإن كلا المعيارين لم يسلما من النقد، لكون كل منهما يركز على جانب معين دون الإحاطة الشاملة بطبيعة الجرائم السيبرانية وتطورها المستمر.

الفرع الثاني

تعريف الجريمة السيبرانية وفق موضوعها ومعاييرها المتنوعة

بعد استعراض الاتجاهات الفقهية آنفة الذكر التي تناولت تعريف الجريمة السيبرانية، قام عدد الفقهاء إلى صياغة تعريفات أخرى تأخذ بنظر الاعتبار موضوع الاعتداء المعلوماتي، في حين ذهب آخرون إلى اعتماد مقاربة مركبة تجمع بين عدة معايير لتحديد نطاق هذه الجرائم، وعليه، يمكن بيان هذه الاتجاهات من خلال عرض التعريف المبني على موضوع الجريمة، ثم التعريف القائم على الجمع بين المعايير المتنوعة وسنذكرها كما يلي :

أولاً: التعريف المبني حول "موضوع" الجريمة

يتجه أنصار هذا الاتجاه الى ان الجرائم السيبرانية ليست تلك الجرائم التي يكون الكمبيوتر محل او اداة لارتكابها، بل هي الجرائم التي تقع على الكمبيوتر او على نظامه المعلوماتي، ومن قبيل ذلك نجد التعريف الذي طرحه الفقيه روزن بالت" وعدد آخر من الاختصاصيين الآخرين، حيث رأوا أن الجرائم السيبرانية هي الجرائم التي تستلزم المباشرة نشاطات غير مشروعة موجهة لإحداث تغييرات أو حذوفات أو لنسخ أو للوصول إلى النظام المعلوماتي الرقمي المخزن داخل الحواسيب[2] **(الشوابكة: جرائم الحاسوب والانترنت، : 2004: ص19)** أو تلك النشاطات التي يتم تحويلها بواسطتها، وعلى ذات المنوال عرفها آخرون بأنها نوع من انواع الغش المعلوماتي الذي يتمثل في سلوكيات غير مشروعة تستهدف المعلومات ونقلها.[3]**(رستم : ص 407)**

ثانياً: التعريف المبني على الجمع بين معايير متنوعة

نظراً للانتقادات التي تم توجيهها للتعريفات السابقة، انبرى عدد من الشراح والفقهاء الى تقديم تعريف شامل للجرائم المرتكبة عبر الانترنت، فقد اعتبر أصحاب هذا الراي ان الجرائم السيبرانية المرتكبة عبر الانترنت هي الجرائم التي يستعمل فيها الكمبيوتر كأداة

لارتكابها، أو هي الجرائم التي يكون الكمبيوتر نفسه احد ضحاياها .[1](**حمديني: أسلوب التحقيق في الجرائم الالكترونية كآلية لمكافحتها: مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية : 2017 : ص2)**

وعلى الرغم من النقد الذي وجه لهذا الراي الذي يجمع بين عدد من المعايير من اجل تعريف الجريمة السيبرانية، لكنه واقعا يعتبر اكثر التعريفات رجاحة من الجانب العملي، نظرا لتنوع صور الجرائم الالكترونية وتطورها المرتبط بالتطور اللاحق بتقنيات المعلومات (**المرجع نفسه: ص 6**).[2]

استنادا الى ما تم عرضه فيما سبق، يتبين لنا أن الجرائم السيبرانية هي الجرائم التي تحدث بواسطة الكمبيوتر أو إحدى وسائل التقنيات المعلوماتية الرقمية المتصلة بشبكة اتصال فيما بينها.

يتضح مما سبق أن الفقه القانوني لم يستقر على معيار واحد لتعريف الجريمة السيبرانية، فذهب اتجاه إلى تعريفها بالاعتماد على موضوع الجريمة من خلال التركيز على الاعتداء الذي يقع على الأنظمة المعلوماتية والبيانات الرقمية، في حين اتجه رأي آخر إلى الجمع بين عدة معايير تأخذ بنظر الاعتبار دور الحاسوب سواء بوصفه أداة لارتكاب الجريمة أو محلاً للاعتداء عليها. ويبدو أن الاتجاه الأخير هو الأقرب من الناحية العملية، لقدرته على استيعاب التنوع والتطور المستمر في صور الجرائم السيبرانية المرتبطة بتطور تقنيات المعلومات والاتصالات.

المطلب الثاني

التطور الزمني للإجرام السيبراني

مرت الجرائم السيبرانية بعدد من المراحل وصولا الى بلوغها لمرحلة التطور الراهن حاليا، ويلاحظ ازدياد معدلاتها التصاعدية منذ بداية فترة التسعينيات، ويترابط ذلك مع التطور الهائل الذي عرفته التقنيات المستعملة في الجرائم المتعلقة بالإنترنت[3] (**حوتيه: بناء إستراتيجية لألمن المعلوماتي كمدخل لمواجهة تهديدات ومخاطر الاجرام السيبراني في الجزائر: مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق الموسوم بعنوان : الاجرام السيبراني المفاهيم والتحديات :2017 ص 7**) ولهذا سنتناول التطور الزمني للجريمة السيبرانية في فرعين حيث سنتناول في الفرع الأول المرحلة التأسيسية للجريمة المعلوماتية أما في الفرع الثاني سنتناول في الفرع الأول المرحلة التأسيسية للجريمة المعلوماتية، اما في الفرع الثاني سنتناول التحول من النظام الرقمي الى النظام السيبراني.

الفرع الأول

المرحلة التأسيسية للجريمة المعلوماتية.

ابتدأت المرحلة الأولى ببداية شيوع استعمال الكمبيوتر المرتبط بشبكة الانترنت العالمية، وامتدت هذه المرحلة منذ ستينيات القرن المنصرم إلى السبعينيات منه، ويلاحظ خلال هذه الفترة غياب الانتشار الموسع لاستخدام الكمبيوترات والتواصل عبر شبكة الانترنت وقلة عدد المستخدمين، وما تم رصده لا يتجاوز الثلاث جرائم في العام الواحد، واستهدفت هذه الجرائم البيانات المخزنة والتجسس

المعلوماتي، وقد بقيت هذه الجرائم منحصرة في إطار السلوكيات اللاأخلاقية دون ان يشملها النطاق القانوني.[1] **(نسيمة : الجريمة الالكترونية مشكلة عالمية: 2015: ص129)**

كما شهدنا في مرحلة الثمانينات إرتفاعا نسبيا ملحوظا في معدلات الجريمة السيبرانية، حيث يلاحظ بروز نوع مستجد من النشاط الاجرامي المرتبط بعمليات إقتحام انظمة الكمبيوتر عن بعد، والقيام بنشر الفيروسات عبر الانظمة المعلوماتية المتنوعة، مما ادى الى تدمير ملفات وبرامج مخزنة في ذاكرة الحواسيب المستهدفة، وقد برز وشاع في هذه الفترة "مصطلح الهاكرز"، حيث أطلق هذا المصطلح على المتسللين الذين يقتحمون الانظمة المعلوماتية، وقد ظهرت قضية دودة موريس" الشهيرة وسجلت باعتبارها من اكثر القضايا المسجلة في فترة الثمانينات اهمية، حيث استطاع الهاكر موريس تابان من القيام بنشر "فيروس إلكتروني" مستجد عرف انذاك "بدودة موريس" في أجهزة الحاسوب من خلال شبكة الانترنت، وقد دمر هذا الفيروس حوالي ستة الاف كمبيوتر.[2]**(موريس روبيرت تابان: هو أول شخص حوكم بموجب قانون الاحتيال الالكتروني الامريكي: بسبب تصميمه لفيروس سمي فيما بعد بفيروس دودة موريس يعرف من خلاله عدد المتصلين بشبكة الانترنت: ثم أضاف موريس تعليمات للفيروس ليقوم بنسخ نفسه عدة مرات ويملا كل مساحات التخزين الفارغة: وقد تسبب هذا الفيروس في خسائر كبيرة جداً)**

كما شهد الاجرام السيبراني تطوراً كبيراً في مرحلة التسعينيات من القرن المنصرم، مما ادى الى تغير ملموس في نطاق ومفهوم الجريمة السيبرانية، فقد تعرضت للهجمات بشكل نشط الكثير من مواقع الانترنت التسويقية، وظهرت حالات مستدة من الجرائم، ففي العام 1995 استطاع الهاكرز اختراق موقع البيت الأبيض الأمريكي، لتلحقها العديد من حوادث الاختراقات ونشر الفيروسات المدمرة كحالة شركة "أوميغا فيروس"، ومن أبرز الجرائم السيبرانية خطورة آنذاك قيام فتى بريطاني بالولوج الى شبكات الحواسيب العسكرية الأمريكية، حيث استطاع اختراق اكثر الاتصالات دقة وسرية، مما حدا بالمسؤولين الأمريكيين الى وصفه بأنه اخطر أنواع الاختراقات لأمن شبكات الكمبيوتر ، حيث ترك هذا الاختراق اثرا ملحوظا على الجاهزية العسكرية .[3] **(شلوش: القرصنة الإلكترونية في الفضاء السيبراني:التهديد المتصاعد لأمن الدول: 2018: ص 190)**

نلاحظ مما سبق أن الجريمة السيبرانية مرت بثلاث مراحل، حيث كانت محدودة في الستينيات والسبعينيات، ثم شهدت في الثمانينيات تزايداً مع ظهور الاختراقات والفيروسات، وفي التسعينيات اتسع نطاقها لتستهدف مواقع ومؤسسات حساسة، مما أبرز خطورتها على أمن المعلومات.

الفرع الثاني

التحول من النظام الرقمي الى النظام السيبراني

حفلت هذه المرحلة بالتزايد المتسارع في معدلات الاجرام السيبراني، وقد ترافق ذلك مع الازدياد الكبير في عدد مستعملي الانترنت عبر العالم، وما نجم من الخسائر المالية الهائلة جراء ذلك، ويلاحظ في هذه الفترة ازدياد وتطور الجهود الدولية والمحلية لمكافحة هذا النوع من الاجرام، وتميزت هذه الحقبة بظهور أنواع مستجدة من مظاهر الجريمة السيبرانية التي تتعرض للمعاملات والبيانات الرقمية، والتي تتسم بالخطورة الفائقة على أمن الأفرد والجماعات، من جراء استهدافها لشتى المجالات سواء منها المجالات الحيوية للدولة أو

للأفراد، فأصبحت الجريمة السيبرانية سلوكا يوميا معاشا في ظل التهديدات التي يشكلها الاجرام المعلوماتي على المصالح الخاصة والعامة، ونظرا لاعتماد الناس المتزايد يوما بعد يوم على تقنيات المعلومات [1] (**محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني : 2013: ص 4**) وعلى سبيل المقارنة نذكر انه في عام 2002 بلغ عدد سكان العالم حوالي ستة مليارات نسمة، وعدد المستخدمين لشبكة الانترنت حوالي ستمائة وستون مليون شخص [2] (**حميد: الأمن السيبراني – القيود والتحديات في ضوء القانون الدولي: 2021: ص 213**) وفي هذه المرحلة بزغت اتفاقية بودابست عام 2001 ، التي ركزت على مكافحة الجريمة المعلوماتية، وقد قدر عدد الجرائم السيبرانية في فرنسا لوحدها عام 2012 اكثر من سبعمائة وسبعون ألف جريمة سيبرانية.[3](**مجموعة العمل الحكومية المشتركة الفرنسية تحت عنوان حماية مستخدمي الأنترنت 2014 ص 22**

تاريخ الزيارة: http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf **(2025/12/2**

أما عام 2014، فقد بلغ عدد من يستخدم تقنيات الأنترنت معدل 35% من سكان المعمورة، بينما يستخدم ما معدله 26% من سكان الأرض مواقع التواصل الاجتماعي بشكل دائم في حياتهم اليومية، أما عدد سكان الأرض الذين يستخدمون تقنية الهاتف النقال فقد بلغ بمعدل% 93 [4] (**يراجع تقرير 2014 The Global Digital Statistic: متوفر على شبكة الإنترنت على الرابط التالي:**

http://etonpreneurs.com/uploads/Global%20Social,%20Digital%20&%20Mobile%20Statistics.%20Jan%202014.pdf **تاريخ الزيارة: 2025/12/2**) وبعد الهجمات الالكترونية الشهيرة على دولة إستونيا عام 2007، حيث انتبهت الكثير من الدول لهذا الخطر الذي يدمر البنيات التحتية للمعلومات وتقنية الاتصالات والشبكات، ويعطل كل المرافق الحيوية، فبدأت الدول التفكير بجدية في إعداد استراتيجيات الأمن السيبراني.[5] (**الموسوي: المشاركة المباشرة في الهجمات السيبرانية : 2019: ص13**)

وفي السنوات القليلة الماضية أصبحت حماية أمن المعاملات والمعلومات والاتصالات والشبكات ومواجهة الجريمة الالكترونية ذات أولوية قصوى في سياسات العديد من الحكومات[1] (**الفتلاوي: الهجمات السيبرانية: 2018: ص22**)خاصة وأن حجم الجريمة الالكترونية الرقمية يزداد بازدياد عدد مستخدمي الانترنت حول العالم.

المبحث الثاني

الإطار القانوني للأمن السيبراني العراقي

مع تزايد الاعتماد على الفضاء السيبراني في مختلف المجالات، أصبح وضع إطار قانوني فعّال للأمن السيبراني ضرورة استراتيجية لحماية المصالح الوطنية وتعزيز الأمن الرقمي. فالتشريعات الوطنية تعد الركيزة الأساسية في مواجهة التهديدات الإلكترونية، حيث تسهم في تحديد القواعد القانونية المنظمة لاستخدام الفضاء السيبراني، وتضع آليات قانونية لمكافحة الجرائم السيبرانية، وتحمي حقوق الأفراد والمؤسسات في هذا المجال. ولذلك، فإن تطوير إطار قانوني شامل للأمن السيبراني في العراق يعد خطوة أساسية لضمان الاستخدام الآمن والموثوق للتكنولوجيا الرقمية. وعلى الرغم من وجود عدة قوانين تتناول بعض جوانب الأمن السيبراني في العراق، إلا أن التشريعات الوطنية لا تزال بحاجة إلى إطار قانوني موحد يعالج جميع التحديات المرتبطة بحماية الفضاء السيبراني، ويحدد بوضوح أسس المسؤولية القانونية عن الجرائم الإلكترونية، وسبل التصدي لها وفق المعايير الدولية. كما تلعب المؤسسات الحكومية دورًا محوريا في تطبيق هذه التشريعات من خلال وضع السياسات، وتعزيز البنية التحتية الأمنية، ومواجهة المخاطر السيبرانية عبر آليات وقائية واستراتيجية فعالة.

لذلك، وبناءً عليه سنقسم هذا المبحث على مطلبين، سنتطرق في المطلب الأول لدراسة التشريعات الوطنية المتعلقة بالأمن السيبراني، أما المطلب الثاني فسنتطرق فيه لدراسة مدى انسجام التشريعات العراقية مع المعايير الدولية للأمن السيبراني

المطلب الأول

التشريعات الوطنية المتعلقة بالأمن السيبراني

يتميز النظام القانوني العراقي بإطار تشريعي واسع يشمل مختلف المجالات القانونية، ومن بينها حماية البيانات الشخصية والأمن السيبراني، وذلك لضمان تنظيم استخدامها والحفاظ عليها من أي انتهاك أو استغلال غير مشروع. وتعد هذه الحماية ضرورية في ظل التطور التكنولوجي السريع الذي يشهده العالم، حيث أصبحت البيانات الشخصية من الموارد الحساسة التي تتطلب تنظيمًا قانونيًا دقيقا للحفاظ على خصوصية الأفراد وضمان عدم التعدي عليها. وقد كفل المشرع العراقي هذا الحق من خلال عدة نصوص قانونية تسعى إلى وضع أسس قانونية لحماية البيانات الشخصية وتنظيم آلية الوصول إليها واستخدامها .[2] (**مصطفى: الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية : 2016: ص441**)

وبناء عليه سنقوم بتقسيم هذا المطلب إلى فرعين، حيث سنتناول في الفرع الأول القصور التشريعي في حماية البيانات الشخصية في العراق أما في الفرع الثاني سنتناول دور المؤسسات الحكومية في تعزيز الأمن السيبراني في العراق.

الفرع الأول

القصور التشريعي في حماية البيانات الشخصية في العراق

إن التشريعات العراقية الحالية المتعلقة بحماية البيانات الشخصية لا تزال تعاني من بعض أوجه القصور التي تتطلب تطويرًا لضمان حماية أكثر شمولا لهذه البيانات.

فعلى سبيل المثال، ينظم قانون أصول المحاكمات الجزائية بعض الجوانب المتعلقة باستخدام البيانات الشخصية في الإجراءات القانونية، لكنه لا يوفر ضمانات كافية تحول دون إساءة استخدامها أو تعرضها للانتهاك. وهذا يستدعي تحديث هذه التشريعات بما يتماشى مع التطورات الرقمية المتسارعة بحيث تتضمن نصوصًا أكثر وضوحًا لحماية خصوصية الأفراد من أي استغلال غير مشروع.[1] **(فرح: النظام القانوني لمقدمي خدمات الإنترنت دراسة تحليلية مقارنة : 2007: ص334)**

وفي هذا السياق، يمثل مشروع قانون جرائم المعلوماتية محاولة لتنظيم استخدام التكنولوجيا والحد من الجرائم السيبرانية، إلا أنه أثار جدلا واسعا بسبب بعض مواده التي قد تؤثر في الحقوق والحريات الأساسية، بما في ذلك حماية البيانات الشخصية وحرية التعبير. وقد أظهرت دراسات متخصصة أن بعض مواد المسودة، مثل المادة (19)، تتعارض مع المبادئ الدولية لحقوق الإنسان إذ إنها قد تقيد حرية التعبير وتحد من إمكانية الوصول إلى المعلومات. وبسبب هذه المخاوف، أوصت العديد من الجهات الحقوقية برفض المسودة بصيغتها الحالية، معتبرة أنها لا توفر الضمانات اللازمة لحماية حقوق الأفراد في الفضاء الرقمي .[2] **(المادة (19) من مسودة قانون الجرائم المعلوماتية العراقي)**

وقد تعرضت المسودة لانتقادات واسعة بسبب منحها السلطات صلاحيات واسعة قد تستخدم المراقبة الأفراد وفرض قيود مشددة على المحتوى الرقمي. فالمادة (3) من القانون تمنح صلاحيات لمنع أي استخدام للتكنولوجيا يمكن أن يؤثر على استقلالية الدولة وأمنها الاقتصادي والسياسي والعسكري، وهو نص عام قد يؤدي إلى تقييد حرية التعبير تحت مبررات فضفاضة. كما أن المادة (6) تحظر نشر معلومات قد تؤثر على الثقة بالنظام المالي والتجارة الإلكترونية، مما قد يحد من قدرة الأفراد والمؤسسات على انتقاد السياسات الاقتصادية والإدارية بشكل علني.[3] **(فقرة (4) من المادة (6) من مسودة قانون الجرائم المعلوماتية العراقي)**

في ظل هذه التحديات، تبرز الحاجة الملحة إلى تطوير تشريعات متوازنة تحقق الحماية الفعالة للبيانات الشخصية دون المساس بالحقوق الأساسية للأفراد. وينبغي أن تتماشى هذه التشريعات مع المعايير الدولية لضمان عدم استخدامها كأداة لتقييد الحريات أو فرض رقابة مشددة على المواطنين.

إن تحديث الإطار القانوني لحماية البيانات الشخصية، بحيث يتناسب مع التطورات التقنية الحديثة يُعد خطوة ضرورية نحو تعزيز الأمن السيبراني وبناء بيئة قانونية عادلة تحافظ على خصوصية الأفراد وتضمن استخدامًا مشروعًا وآمنا للمعلومات في المجتمع العراقي.

الفرع الثاني

دور المؤسسات الحكومية في تعزيز الأمن السيبراني في العراق

أصبح الأمن السيبراني في مختلف القطاعات أحد الأولويات الاستراتيجية التي تتطلب تدخلا حكوميًا فعالا لضمان حماية البنية التحتية الرقمية والمعلومات الحساسة تواجه الدول، بما في ذلك العراق، تهديدات سيبرانية متنامية تستهدف مؤسساتها الحكومية والخاصة، مما يجعل من الضروري تبني سياسات وأطر قانونية متكاملة لتعزيز الأمن السيبراني والتصدي للهجمات الإلكترونية التي قد تؤثر على الاستقرار الوطني والاقتصادي. ومن هذا المنطلق، تضطلع المؤسسات الحكومية بدور أساسي في تطوير استراتيجيات الحماية، ورفع مستوى الوعي، وتعزيز التعاون بين مختلف الجهات لضمان فضاء سيبراني آمن وموثوق.[1](**زهراء عماد محمد: المسؤولية الدولية الناشئة عن الهجمات السيبرانية: مكتبة القانون المقارن: العراق: 2021: ص33**)

إذ تعد وزارة الداخلية إحدى الجهات الرئيسة المسؤولة عن الأمن السيبراني، حيث تتولى مكافحة الجرائم الإلكترونية من خلال وحداتها المختصة، وتعمل على تعزيز القدرات الأمنية في رصد التهديدات الرقمية والتحقيق فيها. كما تساهم الوزارة في نشر الوعي حول المخاطر السيبرانية من خلال برامج توعوية تستهدف المؤسسات والمواطنين، مما يسهم في تعزيز الثقافة الأمنية وتقليل فرص الاختراقات الإلكترونية. بالإضافة إلى ذلك، تتعاون الوزارة مع الجهات القضائية لضمان إنفاذ القوانين المتعلقة بالجرائم السيبرانية، مما يعزز الردع القانوني ويحد من الأنشطة الإجرامية في الفضاء الإلكتروني[2](**زياد محمد العتيبي: جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها: المجلة الأكاديمية العالمية للدراسات القانونية: المجلد 3: العدد 1: 2020: ص14**) إلى جانب وزارة الداخلية، تلعب الهيئة الوطنية للأمن السيبراني دورا محوريا في وضع الاستراتيجيات والسياسات الوطنية لحماية البنية التحتية الرقمية للدولة. وعلى الرغم من أن الهيئة لا تزال في طور التطوير، فإنها تسعى إلى بناء منظومة أمنية متكاملة تعتمد على معايير دولية متقدمة، مع التركيز على تحسين قدرات الاستجابة للهجمات السيبرانية وتطوير أنظمة حماية متطورة. كما تهتم الهيئة بتعزيز التعاون بين الجهات الحكومية والقطاع الخاص، نظرًا لأن الأمن السيبراني يعد مسؤولية جماعية تتطلب تضافر الجهود بين مختلف الفاعلين في المجال الرقمي.[3] (**النقيب: الحرب الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين (الهجمات السيبرانية) : 2022: ص141**)

بدورها، تضطلع وزارة الاتصالات بمسؤولية تأمين الشبكات الحكومية وتطوير البنية التحتية التكنولوجية، حيث تشرف على مزودي خدمات الإنترنت لضمان الامتثال لمعايير الأمن السيبراني، كما تعمل على تنفيذ مشاريع تهدف إلى تعزيز أمن المعلومات في المؤسسات الحكومية. ومن خلال تبني تقنيات التشفير وأنظمة الحماية المتقدمة، تسعى الوزارة إلى الحد من التهديدات السيبرانية وضمان بيئة رقمية آمنة تدعم التحول الرقمي في البلاد. وعلى المستوى التشريعي، يقوم مجلس النواب العراقي بدور هام في وضع الأطر القانونية المنظمة للأمن السيبراني، حيث يساهم في تشريع القوانين التي تعالج قضايا أمن المعلومات وحماية البيانات. ورغم وجود بعض النصوص القانونية المتعلقة بجرائم المعلوماتية، لا يزال العراق بحاجة إلى قانون شامل يعالج مختلف جوانب الأمن السيبراني بشكل

أكثر تفصيلا، ويحدد المسؤوليات بوضوح، ويضمن انسجام التشريعات الوطنية مع المعايير الدولية المعتمدة .[1] (**جاسم: الجرائم السيبرانية وحقوق الانسان في القوانين الدولية والوطنية : 2023: ص11**)

وعلى الرغم من الجهود التي تبذلها المؤسسات الحكومية، فإن التحديات لا تزال قائمة، ومن أبرزها نقص الموارد التقنية والكوادر البشرية المؤهلة، إلى جانب ضعف التنسيق بين الجهات المعنية بالأمن السيبراني. كما أن التطور المستمر في أساليب الهجمات السيبرانية يستلزم تحديثًا دوريًا للأنظمة والسياسات الأمنية، مما يتطلب استثمارات مستمرة في هذا المجال. ولتجاوز هذه التحديات، من الضروري تعزيز التعاون مع الدول ذات الخبرة المتقدمة في الأمن السيبراني، والاستفادة من الخبرات الدولية في تطوير السياسات والبنى التحتية الرقمية.[2] (**إ هديب: الأمن السيبراني: الهجمات السيبرانية والجرائم السيبرانية : 2024: ص139**)

لذا، يمثل الأمن السيبراني حجر الأساس في حماية الأمن الوطني وتعزيز الاستقرار الرقمي في العراق، وهو مسؤولية تتطلب تنسيقًا فاعلا بين مختلف المؤسسات الحكومية. ومن خلال تطوير التشريعات، تعزيز البنية التحتية الرقمية، والاستثمار في التكنولوجيا والتدريب، يمكن للحكومة العراقية تحقيق مستوى متقدم من الحماية السيبرانية يواكب التحديات المتزايدة في العالم الرقمي.

المطلب الثاني

مدى انسجام التشريعات العراقية مع المعايير الدولية للأمن السيبراني

يشكل الأمن السيبراني محور اهتمام متزايد على المستويين الدولي والوطني، حيث أضحت التهديدات الإلكترونية أكثر تعقيدًا وانتشارًا، مما يستدعي تبني استراتيجيات قانونية وتنظيمية فعالة الحماية الفضاء الرقمي. في هذا الإطار، عملت العديد من المنظمات الدولية، مثل الأمم المتحدة والاتحاد الدولي للاتصالات(ITU) ومنظمة التعاون الاقتصادي والتنمية (OECD) ، على وضع معايير وإرشادات تهدف إلى توحيد الجهود الدولية وتعزيز قدرة الدول على التصدي للمخاطر السيبرانية. هذه المعايير لا تقتصر على وضع الأطر القانونية فحسب، بل تشمل أيضا السياسات التقنية والتدابير الوقائية التي تضمن استجابة شاملة وفعالة لمختلف التهديدات الرقمية.[3] (**الجبوري: الحماية القانونية لمعلومات شبكة الأنترنت: 2011: ص25**)

ولبيان ذلك سنقسم هذا المطلب إلى فرعين، حيث سنتناول في الفرع الأول دور دور المعايير الدولية في تعزيز الأمن السيبراني وحماية الفضاء الرقمي، وفي الفرع الثاني سنتناول أوجه التشابه والاختلاف بين التشريعات العراقية والمعايير الدولية

الفرع الأول

دور المعايير الدولية في تعزيز الأمن السيبراني وحماية الفضاء الرقمي

على الرغم من الجهود التي يبذلها العراق في هذا المجال، إلا أن الإطار القانوني للأمن السيبراني لا يزال يواجه تحديات تتعلق بمدى تكامله مع المعايير الدولية. فالمنظومة التشريعية العراقية، رغم احتوائها على بعض الأحكام المتعلقة بحماية البيانات والجرائم الإلكترونية، تفتقر إلى إطار شامل يغطي مختلف جوانب الأمن السيبراني وفقا للمعايير والممارسات العالمية. وعليه، فإن تحليل مدى توافق

التشريعات العراقية مع هذه المعايير يمثل خطوة ضرورية لتحديد الفجوات القانونية والتنظيمية واقتراح الإصلاحات اللازمة لتعزيز الأمن السيبراني في البلاد .[1] (**الجنبيهي: امن المعلومات الإلكترونية : 2005: ص7**)

ومع تزايد التهديدات السيبرانية التي تستهدف الاقتصادات والبنى التحتية الحيوية للدول، أصبحت الحاجة إلى وضع معايير دولية موحدة لتعزيز الأمن السيبراني أكثر إلحاحا من أي وقت مضى. وقد أسهمت العديد من المنظمات والهيئات الدولية في تطوير أطر قانونية وتقنية تهدف إلى مكافحة الجرائم الإلكترونية التي تتجاوز الحدود الجغرافية، مما يستدعي تنسيقًا دوليا فعالا لمواجهتها. حيث تعد الاتفاقيات الدولية إحدى الركائز الأساسية لمكافحة الجرائم السيبرانية، حيث توفر إطارا قانونيا موحدًا للدول الأعضاء لمعالجة هذه التهديدات.

ومن أبرز هذه الاتفاقيات اتفاقية بودابست لمكافحة الجرائم الإلكترونية، التي أرست الأسس القانونية لمواجهة الجرائم السيبرانية على المستوى الدولي. وتشمل هذه الجرائم اختراق الأنظمة، وسرقة البيانات، والتلاعب بالمعلومات الرقمية. كما تلزم الاتفاقية الدول الأعضاء بتحديث تشريعاتها الوطنية بما يواكب التطورات التكنولوجية، وتعزز التعاون القضائي والأمني لضمان محاسبة مرتكبي هذه الجرائم حتى عبر الحدود. إلى جانب الأطر القانونية، تلعب المعايير التقنية دورا محوريا في تعزيز الأمن السيبراني وحماية البنى التحتية الرقمية من الهجمات المتزايدة. ومن أبرز هذه المعايير معيار ISO/IEC 27001 الصادر عن المنظمة الدولية للمعايير، والذي يحدد متطلبات إدارة أمن المعلومات، بما في ذلك تقييم المخاطر، وتطبيق التدابير الوقائية، ووضع خطط استجابة للحوادث الأمنية. كما يبرز معيار ISO/IEC 27032 الذي يركز على أمن الفضاء السيبراني، حيث يقدم إرشادات لحماية الشبكات والأنظمة من الهجمات الإلكترونية المتطورة. وتساعد هذه المعايير الحكومات والمؤسسات على تبني سياسات أمنية فعالة تضمن حماية بياناتها واستمرارية عملياتها الرقمية .[2] (**سميرة بيطام: تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية : 2023: ص55**)

في السياق ذاته، يؤدي المعهد الوطني للمعايير والتكنولوجيا(NIST) دوراً محورياً في تعزيز الأمن السيبراني من خلال تطوير إطار NIST للأمن السيبراني، الذي يستند إلى خمس وظائف رئيسية: تحديد الأصول الرقمية، تطبيق التدابير الوقائية، اكتشاف التهديدات الاستجابة للهجمات والتعافي من الأضرار. ويساعد هذا الإطار المؤسسات على تطوير استراتيجيات أمنية متكاملة، مما يمكنها من التصدي للهجمات الإلكترونية بفعالية، لا سيما في القطاعات الحيوية التي تتطلب مستوى عال من الحماية .[3] (**المبادئ التوجيهية للأمم المتحدة: تنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية** http://hrlibrary.umn.edu/ **تاريخ الزيارة: 2025/12/1**)

على المستوى الدولي، يعمل الاتحاد الدولي للاتصالات(ITU) على دعم جهود تعزيز الأمن السيبراني من خلال تقديم المساعدة التقنية للدول الأعضاء، وتسهيل تبادل المعلومات حول التهديدات الإلكترونية، إلى جانب وضع استراتيجيات وطنية لحماية الأنظمة الرقمية. كما يركز الاتحاد على دعم الدول النامية في بناء بيئة إلكترونية آمنة من خلال توفير برامج تدريبية متخصصة وبناء القدرات،

مما يسهم في الحد من مخاطر الهجمات الإلكترونية التي قد تهدد استقرارها الرقمي.[1] (**نبراس الجرائم السيبرانية وأثرها على الأمن السيبراني: 2021: ص365**)

إضافة إلى الجهود القانونية والتقنية، يشكل الوعي المجتمعي عنصرًا أساسيا في تعزيز الأمن السيبراني، حيث تعتمد فعالية أي استراتيجية أمنية على مدى إدراك الأفراد والمؤسسات للمخاطر الإلكترونية وطرق الوقاية منها. ولهذا السبب، تعمل العديد من الدول على تنظيم حملات توعوية وإدراج مواد تعليمية متخصصة في المناهج الدراسية، إلى جانب توفير برامج تدريبية للموظفين والمتخصصين في مجال أمن المعلومات. ويسهم هذا النهج في تقليل الثغرات الأمنية التي قد يستغلها المهاجمون لاختراق الأنظمة الرقمية، مما يعزز الحماية على المستويين الفردي والمؤسسي .[2] (**هديب: الأمن السيبراني: الهجمات السيبرانية والجرائم السيبرانية: ص142**)

وعلى الرغم من التقدم الملحوظ في تطوير المعايير الدولية للأمن السيبراني، لا تزال هناك تحديات تعيق تطبيقها بفعالية في بعض الدول من أبرز هذه التحديات التفاوت التشريعي بين الدول، حيث تختلف القوانين الوطنية المتعلقة بمكافحة الجرائم الإلكترونية، مما قد يعرقل التعاون الدولي في ملاحقة المجرمين السيبرانيين، كما تواجه بعض الدول مشكلات في البنية التحتية الرقمية، مما يجعل أنظمتها أكثر عرضة للهجمات الإلكترونية. إضافة إلى ذلك، يشكل نقص الكفاءات المتخصصة تحديا آخر، حيث تعاني العديد من الحكومات والشركات من صعوبة في استقطاب خبراء أمن سيبراني مؤهلين لمواكبة التهديدات المتزايدة.[3] (**بيطام: تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية: ص57**)

الفرع الثاني

أوجه التشابه والاختلاف بين التشريعات العراقية والمعايير الدولية

تمثل الجرائم الإلكترونية تهديدًا متزايدًا على مستوى العالم، مما دفع العديد من الدول إلى تبني تشريعات تتماشى مع المعايير الدولية لضمان أمن الفضاء الرقمي وحماية البيانات من الهجمات السيبرانية. في هذا السياق، سعى العراق إلى تطوير منظومته القانونية لمواجهة التحديات الرقمية، إلا أن مدى انسجام هذه التشريعات مع المعايير الدولية لا يزال محل تقييم، حيث توجد بعض الجوانب التي تتوافق مع هذه المعايير، في حين أن هناك فجوات تتطلب مزيدًا من التطوير والتحديث.[4] (**أحمد: الهجمات على شبكات الحاسوب في القانون الدولي الإنساني2015: ص55**)

يتجلى أحد أوجه التشابه الرئيسة في أن التشريعات العراقية، على غرار المعايير الدولية، تجرّم العديد من الأفعال الإلكترونية غير المشروعة، مثل الاختراق غير المصرح به، وسرقة البيانات والاحتيال الإلكتروني. فهذه الجرائم تُعد انتهاكات صريحة للأمن السيبراني، وتحظى بتجريم واضح في القوانين الوطنية والدولية على حد سواء. كما تتماشى القوانين العراقية إلى حد ما مع اتفاقية بودابست للجرائم الإلكترونية، التي توفر إطارًا قانونيًا موحدًا لمكافحة التهديدات السيبرانية على مستوى العالم. وإلى جانب ذلك، تسعى الجهات العراقية المختصة إلى تعزيز التعاون الدولي عبر تبادل المعلومات حول الهجمات الإلكترونية مع الدول والمنظمات المعنية، وهو

ما يتوافق مع النهج الذي تتبعه الاتفاقيات الدولية التي تشجع الدول على تنسيق الجهود في هذا المجال.[1] (**الشمري: توظيف القوة السيبرانية في استراتيجيات الدول الكبرى: الولايات المتحدة الأمريكية وروسيا انموذجاً2022: ص109)**

وعلى الرغم من هذا التقارب، فإن التشريعات العراقية لا تزال تواجه بعض التحديات التي تعيق تحقيق انسجام كامل مع المعايير الدولية. ومن أبرز أوجه الاختلاف أن القوانين العراقية لم تواكب بعد التطورات التقنية المتسارعة، حيث تفتقر إلى نصوص صريحة تعالج الجرائم المستحدثة، مثل هجمات الفدية والتلاعب بالبيانات عبر الذكاء الاصطناعي، والتي أصبحت من أخطر التهديدات في العصر الرقمي كذلك، تظل العقوبات القانونية المفروضة على الجرائم السيبرانية في العراق أقل صرامة مقارنة بالمعايير الدولية، إذ تفرض بعض القوانين العالمية عقوبات قاسية تشمل السجن لمدد طويلة، وغرامات مالية كبيرة، وحجب الأنظمة المستخدمة في الهجمات، لضمان ردع فعّال للمجرمين الإلكترونيين[2] **(الفتلاوي: الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر: 2016:ص619)**

بالإضافة إلى ذلك، لم تنص القوانين العراقية حتى الآن على إطار شامل الحماية خصوصية المستخدمين على الإنترنت على غرار اللوائح الدولية مثل اللائحة العامة لحماية البيانات[3] **(النظام الأوربي لحماية البيانات (GDPR))** (GDPR) التي توفر ضمانات قانونية لحماية البيانات الشخصية وحقوق الأفراد في الفضاء الرقمي. وهذا القصور يفتح المجال لوجود ثغرات قد تؤثر على حقوق المستخدمين في العراق، مما يستلزم تحديثًا قانونياً يعزز من آليات حماية الخصوصية الرقمية.

ومن الجوانب الأخرى التي تحتاج إلى تطوير ضعف الموارد التقنية والبشرية اللازمة لإنفاذ القوانين المتعلقة بالأمن السيبراني. فبينما تؤكد المعايير الدولية على ضرورة الاستثمار في القدرات التكنولوجية والتدريب المستمر للعاملين في هذا المجال، لا يزال العراق بحاجة إلى تطوير بنيته التحتية الرقمية وتعزيز قدراته المؤسسية لضمان تطبيق القوانين بفعالية. وبعد توفير برامج تدريبية متخصصة للعاملين في إنفاذ القانون، وإنشاء مراكز متقدمة لرصد التهديدات والاستجابة لها، من الخطوات الأساسية التي ينبغي اتخاذها لضمان مواجهة أكثر كفاءة للهجمات الإلكترونية.

ولسد الفجوات بين التشريعات العراقية والمعايير الدولية، يصبح من الضروري العمل على تحديث القوانين الوطنية بما يضمن تغطية جميع أنواع الجرائم الإلكترونية الحديثة، وتشديد العقوبات القانونية لجعلها أكثر ردعًا للمخالفين، ووضع إطار قانوني واضح لحماية البيانات الشخصية بما يواكب المعايير العالمية. كما ينبغي تعزيز التعاون مع المنظمات الدولية المختصة، والاستثمار في تطوير القدرات الفنية والبشرية في مجال الأمن السيبراني[4] **(فرج: الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران : 2021: ص 199)** ضمان تحقيق استجابة سريعة وفعالة للتهديدات الإلكترونية المتزايدة.

وعليه، فإن تحقيق التكامل بين التشريعات العراقية والمعايير الدولية يتطلب نهجا شاملاً يشمل إصلاحات قانونية، وتحديثات تقنية، وتعزيزا للتعاون الدولي. ومن خلال هذه الجهود، يمكن للعراق أن يعزز أمنه السيبراني، ويحمي بنيته الرقمية من المخاطر المتنامية ويساهم في بناء بيئة إلكترونية أكثر أمانًا واستقرارًا، تتماشى مع التوجهات العالمية الحديثة في هذا المجال.

الخاتمة

أضحى الفضاء السيبراني اليوم مجالاً واسعاً للتفاعل البشري ولنشاط المؤسسات الحكومية والخاصة، بما يحمله من فرص هائلة للنمو والتطور، لكنه في الوقت ذاته كشف عن تحديات عميقة تتعلق بقدرة المنظومة القانونية على حماية هذا الفضاء من الانتهاكات المتزايدة. وقد أظهر هذا البحث أن الجرائم السيبرانية ليست مجرد امتداد رقمي للجرائم التقليدية، بل تمثل نمطاً جديداً من الاعتداءات يتسم بالتعقيد، والسرعة، والقدرة على إخفاء معالمه.

توصل البحث إلى أن التشريعات الجزائية التقليدية – بما في ذلك التشريع العراقي – لا تزال عاجزة عن الإحاطة بخصوصية الجرائم السيبرانية، سواء من حيث تعريفها أو تحديد صورها أو تنظيم آليات مساءلة مرتكبيها. وقد أظهر التحليل أن قصور التجريم، وضعف الأدوات الإجرائية في جمع الأدلة الرقمية والحفاظ عليها، وغياب التشريعات الخاصة بحماية البيانات الشخصية، تمثل فجوات حقيقية تؤثر في فاعلية المواجهة الجزائية، وقد توصلنا لعدد من النتائج والتوصيات لعل أهمها:

أولاً: النتائج:

1- بيّنت الدراسة أن النصوص العقابية الحالية، بما فيها القانون العراقي، وُضعت لحماية مصالح مادية ملموسة، ولا تستوعب بشكل كافٍ الطبيعة اللامادية للجرائم الإلكترونية.

2- الأمن السيبراني يعد مكوّنًا أساسيًا للأمن القومي والاقتصادي، خاصة مع التوسع في استخدام التكنولوجيا الرقمية.

3- التشريعات العراقية الحالية غير كافية لمواجهة التهديدات السيبرانية المتزايدة، مما يستدعي مراجعة شاملة لها .

4- هناك ضعف في التنسيق بين الجهات الحكومية المعنية بالأمن السيبراني، مما ينعكس سلبًا على الاستجابة الفعالة للهجمات الإلكترونية.

5- تفتقر البنية التحتية الرقمية في العراق إلى التطوير الكافي الذي يمكنها من مواجهة التحديات السيبرانية الحديثة.

ثانياً: التوصيات:

1- إصدار قانون خاص وشامل للجرائم السيبرانية، يضم تعريفات دقيقة لصور الجريمة الرقمية، ويحدّد أركانها وعقوباتها وإجراءات ضبط الأدلة الرقمية.

2- إقرار قانون لحماية البيانات الشخصية يضمن تنظيم جمع البيانات الرقمية ومعالجتها واستخدامها، ويوفّر حماية مستخدمي الإنترنت من الاعتداءات عليها.

3- النص صراحة على مسؤولية الأشخاص المعنويين ومزوّدي الخدمات الإلكترونية عند الإهمال أو التواطؤ في تهيئة البيئة لوقوع الجرائم السيبرانية.

4- إنشاء هيئة وطنية للجرائم السيبرانية تُعنى بالتحقيق الفني، وتحليل الأدلة الرقمية، وتعزيز الأمن الرقمي على مستوى الدولة.

5- تضمين النصوص العقابية إجراءات خاصة بالدليل الإلكتروني، مع الضوابط الفنية التي تضمن سلامته وقابليته للاستخدام القضائي.

6- تشديد العقوبات على الجرائم التي تستهدف البنى التحتية الرقمية أو المعلومات الحكومية أو المؤسسات المصرفية.

قائمة المصادر والمراجع

أولاً: الكتب القانونية:

1. ابتسام حمديني، أسلوب التحقيق في الجرائم الالكترونية كآلية لمكافحتها، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية، الجزائر، الموسوم بعنوان: الاجرام السيبراني المفاهيم والتحديات 2017.
2. أحمد خليفة الملط، الجرائم المعلوماتية، طبعة 2، دار الفكر الجامعي، الاسكندرية، 2006.
3. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية، ط1، منشورات زين الحقوقية، بيروت، 2018.
4. إسلام هديب، الأمن السيبراني، الهجمات السيبرانية والجرائم السيبرانية، دار مصر للنشر والتوزيع، مصر، 2024.
5. حازم جري الشمري، توظيف القوة السيبرانية في استراتيجيات الدول الكبرى، الولايات المتحدة الأمريكية وروسيا انموذجاً، دار انكي للنشر والتوزيع، العراق، 2022.
6. خالد وليد محمود، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، المركز العربي للأبحاث ودراسة السياسات، الدوحة، 2013.
7. دياب موسى البداينة، الجرائم الإلكترونية المفهوم والاسباب ورقة علمية مقدمة في الملتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، كلية العلوم الاستراتيجية، الاردن، 2022.
8. زهراء عماد محمد، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، العراق، 2021.
9. سالم نمر جاسم، الجرائم السيبرانية وحقوق الانسان في القوانين الدولية والوطنية، دار النهضة العربية، مصر، 2023.
10. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الأنترنت، منشورات الحلبي الحقوقية، لبنان، 2011.
11. عبد العال الدريبي، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والأنترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012.
12. عبد اللطيف معتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن مذكرة ماجستير، جامعة العقيد الحاج لخضر بباتنة، كلية الحقوق والعلوم السياسية قسم الحقوق، 2012.
13. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.
14. عدنان النقيب، الجرب الإلكترونية في ضوء بروتكولي سبع وسبعين الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين (الهجمات السيبرانية)، المركز العربي للنشر والتوزيع، مصر، 2022.
15. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة، طبعة أولى منشورات زين الحقوقية بيروت 2013.
16. علي عبد القادر القهوجي، الحماية الجائية لبرامج الحاسب الآلي، المكتبة القانونية، القاهرة، 1999.
17. علي محمد كاظم الموسوي، المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، بيروت، 2019.
18. عمر حوتيه، بناء إستراتيجية لألمن المعلوماتي كمدخل لمواجهة تهديدات ومخاطر الاجرام السيبراني في الجزائر، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق الموسوم بعنوان : الاجرام السيبراني المفاهيم والتحديات 2017.

19. فارس محمد العمارات جرائم العصر من الرقمية الى السيبرانية، دار الخليج للتوزيع والنشر، عمان، الأردن، 2023.
20. محمد امين الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، 2004، ص19.
21. منير محمد الجنبيهي وممدوح محمد الجنبيهي، امن المعلومات الإلكترونية، دار الفكر الجامعي، مصر، 2005.
22. منير وممدوح الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، مصر،2016.
23. هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، مصر، 2017.

ثانياً: الأبحاث والمجلات والدوريات:

1. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، كلية القانون، جامعة بابل، العدد 4، العراق، 2016.
2. أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الإنترنت دراسة تحليلية مقارنة، بحث منشور في مجلة المنارة للبحوث والدراسات، المجلد 9، العدد 13، مايو، 2007.
3. زياد محمد العتيبي، جرائم السيبرانية المرتكبة عبر الوسائط الرقمية وبيان مفهومها، المجلة الأكاديمية العالمية للدراسات القانونية، المجلد 3، العدد 1، 2020.
4. سميرة بيطام، تطور الجريمة السيبرانية والآليات القانونية للتصدي لها في ظل التحولات الجيوسياسية، مجلة كلية القانون والعلوم السياسية، العدد 22، العراق، 2023.
5. عائشة مصطفى، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم، المجلد 2، العدد 5، 2016.
6. عبد الوهاب كريم حميد، الأمن السيبراني – القيود والتحديات في ضوء القانون الدولي، مجلة العقد الاجتماعي، العدد 2، أربيل، 2021.
7. كرار عباس متعب فرج، الحرب السيبرانية: دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الأمريكية وإيران، مجلة حمورابي للدراسات القانونية، العدد 40، العراق، 2021.
8. نبراس إبراهيم مسلم، الجرائم السيبرانية وأثرها على الأمن السيبراني، مجلة القادسية للقانون والعلوم السياسية، العدد 1، العراق، 2021.
9. نسيمة سحواذ، الجريمة الالكترونية مشكلة عالمية، مجلة الشرطة للمديرية العامة للأمن الوطني، عدد 129، ديسمبر 2015.
10. نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، بحث منشور في مجلة مركز بابل للدراسات الإنسانية، المجلد 8، العدد 6، جامعة بابل، العراق، 2018.
11. هشام محمد فريد رستم الجرائم المعلوماتية أصول التحقيق الجنائي الفني، بحوث مؤتمر القانون والكمبيوتر والانترنت، جامعة الامارات المتحدة كلية الشريعة والقانون، طبعة 3، مجلد (2)، 2004.

12. واثبة السعدي الحماية الجنائية لبرامج الحاسوب، بحث منشور في مجلة العلوم القانونية، كلية القانون جامعة بغداد، مجلد 18، عدد اول، 2004.

13. ياسمين بونعاره، الجريمة الالكترونية مجلة المعيار، جامعة الأمير عبد القادر كلية أصول الدين، مجلد 2 عدد 39، جوان 2015 ، ص3؛ وايضا عبد العال الدربيي، الجريمة الالكترونية، طبعة أولى، المركز القومي للاصدارات القانونية، القاهرة، 2012.

ثالثاً: الأطاريح الجامعية:

1. سراب ثامر أحمد، الهجمات على شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوراه من متطلبات نيل درجة الدكتوراه في القانون العام، جامعة النهرين، العراق، 2015.
2. عمر العتبي، الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية اطروحة دكتواره، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2010.

رابعاً: القوانين:

1. قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.
2. مسودة قانون الجرائم المعلوماتية العراقي.
3. النظام الأوربي لحماية البيانات (GDPR).

خامساً: المواقع الإلكترونية:

1. تقرير The Global Digital Statistic 2014، متوفر على شبكة الإنترنت على الرابط التالي:
http://etonpreneurs.com/uploads/Global%20Social,%20Digital%20&%20Mobile%20Statistics.%20Jan%202014.pdf
2. تقرير مجموعة العمل الحكومية المشتركة الفرنسية تحت عنوان حماية مستخدمي الأنترنت 2014 ص 22 متوفر على الموقع الرسمي لوازرة العدل الفرنسية، الرابط الإلكتروني:
http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
3. المبادئ التوجيهية للأمم المتحدة، تنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية، الجمعية العامة، القرار 45/95. متاح على الرابط التالي:
http://hrlibrary.umn.edu/

Issue - 27 - Part 3- July - 2026 - Year 5

Refereed Quarterly Scientific Journal

American International Journal of Humanities and Social Sciences

ISSUED BY AMERICAN INTERNATIONAL ACADEMY FOR HIGHER EDUCATION AND TRAINING

QUARTERLY JOURNAL ON HUMANITARIAN AND SOCIAL AFFAIRS

(ISSN) Electronic (4806 - 3085) / (ISSN) Paper (4830 - 3085)

Legal deposit number in the Moroccan National Library (2025PE00006)

Legal deposit number in the Iraq National Library and Archives (2735)

Journal Website : https://iajphss.us/