مجلة الكندي

مجلة قانونية سياسية مختصة بنشر الابحاث والدراسات القانونية والدولية المعاصرة

العدد الثالث - السنة الاولى - المجلد الاول /رمضان 1447 الموافق اذار 2026

توجه جميع الملاحظات الى رئيس لجنة التحرير على العنوان

مجلة الكندي - أربيل - العراق

الهاتف : 9647500100017+

البريد الالكتروني : alkindi-journal.com

تتوفر نصوص البحث على الموقع التالي

alkindi-journal.com

رقم الايداع ISSN : 3005 -6578-2693

مجلة الكندي

مجلة قانونية سياسية تختص بنشر الأبحاث والدراسات القانونية والدولية المعاصرة

مجلة الكندي
دراسات قانونية برؤية مستقبلية

رئيس التحرير:

أ.د مالك دحام متعب حمادي الجميلي
جامعة المشرق – العراق

مدير التحرير:

أ.د أحمد سمير محمد ياسين الجبوري
جامعة كركوك – العراق

هيئة التحرير:

أ.د. عصمت عبد المجيد بكر
أستاذ قانون محاضر في عدد من الجامعات–العراق
أ.د.عمر محمد شحادة
الجامعة اللبنانية – لبنان
أ.د. محمد رياض دغمان
الجامعة اللبنانية – لبنان
د. رواد غالب سليقة
جامعة بيروت العربية – لبنان
د. عمار ممدوح البيك
جامعة حلب – سورية
أ.د. حسن فضالة موسى حسن التميمي
الجامعة العراقية – العراق
أ.د. أحمد نوار نصيف
جامعة تكريت – العراق

أ.د رشيد مجيد محمد الربيعي
جامعة بغداد–العراق
أ.د. بشير سعد زغلول
جامعة قطر – قطر
أ.د. محمد حمد مصطفى القطاطشة
الجامعة الأردنية – الأردن
د. محمد بن طريف
جامعة عمان العربية – الأردن
أ. د. وسام حسين غياض
الجامعة اللبنانية – لبنان
أ.م.د. مروان عامر نصيف جاسم
جامعة تكريت – العراق

سياسة النشر

تُعنى مجلة الكندي بمشاركات الأبحاث الرصينة والدراسات والتعليقات على الأحكام القضائية وملخصات رسائل الماجستير وأطاريح الدكتوراه والتقارير العلمية عن الندوات والمؤتمرات وعرض الكتب الجديدة ومراجعتها باللغة العربية والإنكليزية، كما تدعوكم المجلة للتفاعل معها وإغناء الأعداد الصادرة عنها وفق سياسة النشر الخاصة بها والمتمثلة بالآتي:

1- مجلة الكندي هي مجلة دورية تصدر شهرياً عن دار هاتريك للنشر والتوزيع في أربيل- العراق.

2- المجلة مختصة بنشر أبحاث العلوم الإجتماعية (القانونية والسياسية والاقتصادية)، أو عرض رسائل الماجستير وأطاريح الدكتوراه، أو التعليقات على الأحكام القضائية، أو التقارير العلمية عن الندوات والمؤتمرات، أو عرض الكتب الجديدة ومراجعتها في العلوم القانونية والسياسية وباللغتين العربية والإنكليزية.

3- تحتفظ المجلة بحقوق النشر والطبع كافة، كما تعبر جميع آراء المؤلفين الواردة في البحث أو المادة العلمية عن وجهة نظرهم، ولا تُعَدُّ المجلة مسؤولة عنها، استناداً لمبدأ استقلالية الرأي، وتلتزم المجلة بالحفاظ على حقوق الملكية الفكرية للمؤلفين..

4- المجلة غير ملزمة برد أصول البحوث أو التعليقات على الأحكام القضائية أو ملخصات الكتب ورسائل الماجستير أو أطاريح الدكتوراه سواء نشرت أم لم تنشر، مع خصم جميع المصاريف في حال عدم النشر.

5- تكون الأولوية بالنشر حسب الأسبقية بالحصول على قبول نشر للبحوث، وفي حال رغبة الباحث بالنشر المستعجل يستوفى مبلغ إضافي على أجور النشر النهائية للبحث، طبقاً لما متاح على موقع المجلة الإلكتروني.

6- يشترط بالمادة العلمية المراد نشرها بالمجلة، أن لا تكون قد سبق نشرها في مجلة أو دورية أو مؤتمر علمي، بتعهد يقدمه الباحث، وبخلافه يتحمل الباحث المسؤولية القانونية والمالية كافة.

7- يلتزم الباحث بعدم إرسال بحثه أو مادته العلمية إلى أي جهة أخرى لغرض النشر، حتى يصله رد المجلة بصلاحية بحثه أو مادته العلمية للنشر من عدمه خلال مدة شهرين من تاريخ استلام المجلة للبحث أو المادة العلمية، وبخلافه تحتفظ المجلة بحقوقها القانونية والمالية كافة.

8- يتعين على الباحث أن يلتزم بشروط وأسلوب النشر المعتمد من المجلة والمتاح على موقع المجلة الإلكتروني (https:// alkindijournal.com)، وبخلافه لا تتحمل المجلة مسؤولية التأخر بقبول أو نشر البحث أو المادة العلمية.

9- يجب على الباحث مراعاة الأمانة العلمية في البحث العلمي والدراسة الأكاديمية وفي مقدمتها أخلاقيات البحث العلمي وبنود لجنة أخلاقيات النشر (Committee On Publication Ethics) مثال ذلك، توثيق المراجع والمصادر والنصوص القانونية والعلمية ومراعاة الموضوعية والمنهجية في الكتابة، وبخلافه يتحمل الباحث المسؤولية القانونية والإدارية والمالية الكاملة عن أي انتهاك أو تجاوز لهذه الأخلاقيات طبقاً للقوانين والتعليمات الوطنية أو الدولية.

10- تخضع جميع البحوث العلمية المراد نشرها بالمجلة لتدقيق نسبة الانتحال (turnitin) ضماناً لعدم نشر البحوث مسروقة النص جزئياً أو كلياً، وبخلافه يتحمل الباحث المسئولية القانونية والمالية والإدارية الكاملة.

11- تخضع المادة العلمية التي تنشرها المجلة للتحكيم الشفاف والمراجعة العلمية المتخصصة (Peer-reviewed process) فضلاً عن التدقيق اللغوي (للغة العربية واللغة

الإنكليزية)، ويكون للمجلة صلاحية الموافقة على النشر فيها من عدمه استناداً إلى الآراء الأولية لهيئة تحرير المجلة أو آراء المحكمين المتخصصين.

13- يمنح كل باحث نسخة ورقية من العدد المنشور فيه بحثه، فضلاً عن نسخة مستلة عن بحثه، ولا تتحمل المجلة أجور إرسال النسخة الورقية للباحث.

14- تعمل المجلة وفق آلية وسياسة النشر المفتوح (Open Access).

15- تلتزم المجلة بمنح الباحث قبول النشر حين استكمال جميع المتطلبات على أن يذكر فيه المجلد والعدد وسنة النشر. باستثناء البحوث المستلة من رسائل الماجستير وأطاريح الدكتوراه.

مدى أهمية التعاون القانوني في تدعيم الأمن السيبراني

إعداد الطالبة: رسل نافع خلف

بإشراف الأستاذ الدكتور :محمد فرحات

مستخلص

يهدف هذا البحث إلى دراسة الجزاءات الجنائية والتدابير القانونية المفروضة على الجرائم السيبرانية في ظل التطور المتسارع للتكنولوجيا الرقمية واتساع نطاق استخدام الإنترنت .تكمن أهمية البحث في إبراز التحديات التي تواجه التشريعات الجنائية التقليدية عند التعامل مع الجرائم الإلكترونية، مثل صعوبة الإثبات، والطابع العابر للحدود، وتنوع صور الاعتداءات الرقمية .كما يسعى البحث إلى تحليل فعالية العقوبات الجنائية والتدابير الاحترازية في تحقيق الردع العام والخاص، مع التركيز على التوازن بين حماية المجتمع الرقمي وضمان الحقوق والحريات الفردية .يعتمد البحث على المنهج الوصفي التحليلي والمقارن، من خلال دراسة النصوص القانونية الوطنية والدولية واستقراء التجارب القضائية، وصولاً إلى تقديم توصيات عملية لتطوير المنظومة الجنائية في مواجهة الجريمة السيبرانية.

الكلمات المفتاحية :الجريمة السيبرانية، الجزاءات الجنائية، التدابير الاحترازية، الأدلة الرقمية، التشريع المقارن.

Abstract

This study aims to examine the criminal sanctions and legal measures imposed on cybercrime in light of the rapid development of digital technologies and the widespread use of the Internet. The significance of the research lies in highlighting the challenges faced by traditional criminal legislation when addressing cyber offenses, such as difficulties in evidence collection, the cross-border nature of cybercrime, and the diversity of digital attacks. The research seeks to analyze the effectiveness of criminal penalties and precautionary measures in achieving both general and specific deterrence, while emphasizing

Keywords:(Cybercrime, Criminal Sanctions, Precautionary Measures, Digital Evidence, Comparative Legislation.)

مقدمة

الجريمة السيبرانية الافتراضية أو جريمة فضاء الانترنت أو الجريمة الالكترونية مهما تعددت التسميات الى أن المعنى يبقى واحد وهو الاستعمال السلبي للتكنولوجيا والذي يشكل جريمة في نظر القانون يتوجب العقاب عليها، اختلفت التسمية بشأنها إلا أننا سوف نحاول سرد أهم المصطلحات القانونية التي تخصها أهم الميزات والخصائص التي تنفرد بها مقارنة مع الجرائم التقليدية التي نعرفها التي تثبت بالقرائن القانونية.

أولاً أهمية البحث

- **حماية المجتمع الرقمي** :يساهم البحث في إبراز دور القانون الجنائي في مواجهة التهديدات السيبرانية التي تستهدف الأفراد والمؤسسات والدول.
- **سد الفراغ التشريعي** :كثير من التشريعات التقليدية لم تُصمم لمواجهة الجرائم الإلكترونية، مما يجعل البحث أداة لتطوير قواعد قانونية حديثة.
- **تعزيز الأمن الوطني والاقتصادي** :الجرائم السيبرانية قد تؤدي إلى خسائر مالية ضخمة أو تهديد البنية التحتية الحيوية، وبالتالي فإن دراسة الجزاءات والتدابير تساعد في صياغة سياسات ردع فعّالة.

ثانياً إشكالية البحث:

قصور التشريعات التقليدية :هل تكفي النصوص الجنائية الحالية لمواجهة الجرائم السيبرانية أم تحتاج إلى تعديل جذري؟

ثالثاُ منهجية البحث

- **المنهج الوصفي التحليلي** :وصف النصوص القانونية القائمة وتحليل مدى فعاليتها في مواجهة الجرائم السيبرانية.
- **المنهج المقارن** :دراسة تجارب دول مختلفة (مثل الاتحاد الأوروبي، الولايات المتحدة، والدول العربية) في وضع الجزاءات والتدابير.
- **المنهج الاستقرائي** :استخلاص النتائج من حالات واقعية وأحكام قضائية متعلقة بالجرائم الإلكترونية.
- **المنهج النقدي** :تقييم الثغرات التشريعية واقتراح حلول عملية لتطوير المنظومة الجنائية.

رابعاً خطة البحث:

يتناول هذا البحث مبحثين يتضمن المبحث الاول العقوبات الأصلية وظروف التشديد والتخفيف وينقسم الى مطلبين الأول الحبس والسجن والغرامات ومعايير تقديرها في السرقة السيبرانية اما الثاني ظروف التشديد (الطابع المنظم، العابر

للحدود ، المساس بالبنية الحرجة، ظروف التخفيف ، اما المبحث الثاني التعاون الدولي في تدعيم الأمن السيبراني وينقسم الى مطلبين الأول الجهود الدولية الاتفاقية في تدعيم الأمن السيبراني والمطلب الثاني الجهود الوطنية في تدعيم الأمن السيبراني.

المبحث الأول

العقوبات الاصلية وظروف التشديد والتخفيف

الجزاء العقابي هو الأثر الذي يقرره النص الجزائي عند مخالفة الأوامر أو النواهي، ويتخذ صورتين أساسيتين هما العقوبات والتدابير الاحترازية. وتستوجب النصوص الخاصة بالجرائم الإلكترونية تضمين هذين الجزاءين أو الإحالة إلى القوانين الجزائية العامة لضمان التطبيق الفعّال..**ينقسم هذا البحث إلى مطلبين يتناول المطلب الأول الحبس والسجن والغرامات ومعايير تقديرها في السرقة السيبرانية ويتناول المطلب الثاني ظروف التشديد (الطابع المنظم. العابر للحدود. المساس بالبنية الحرجة) ظروف التخفيف.**

المطلب الأول

الحبس والسجن والغرامات ومعايير تقديرها في السرقة السيبرانية

إن السرقة السيبرانية ليست جريمة مستقلة بمعايير خاصة، بل تُكيف وفق القواعد الجنائية التقليدية وأركان الجريمة الثلاثة:

القصد الجنائي :نية الجاني الاستيلاء على بيانات الغير أو استغلالها دون حق.

الركن المادي :الدخول غير المشروع إلى الأنظمة أو الحسابات أو قواعد البيانات بهدف الاستيلاء.

الضرر : مالي كخسارة الأموال والمعاملات، أو معنوي كانتهاك الخصوصية والمساس بالسمعة.

وعلى ضوء ذلك سنقوم بتقسيم هذا الفرع الى فكرتين رئيسيتين أولهما التكييف القانوني للجريمة السيبرانية ومن بعدها سننتقل للحديث عن جريمة السّرقة الإلكترونيّة

- **أولاً التكييف القانوني للجريمة السيبرانية**

إن التكييف القانوني للحرب السيبرانية يدور بين اعتبارها حربًا بالمعنى التقليدي أو مجرد جرائم إلكترونية. إنكار صفة الحرب يعود إلى صعوبة إثبات الأدلة المادية المباشرة بسبب طبيعة الهجمات التي تُنفذ عبر شبكات معقدة وتستخدم تقنيات التمويه، بخلاف الحروب التقليدية التي تترك آثارًا واضحة يسهل توثيقها. الحرب السيبرانية تتسم بالغموض واللامادية، وقد تُحدث آثارًا خطيرة على الأنظمة والمصالح الوطنية دون أن تُثبت كـ"هجوم مسلح" بالمعنى القانوني. ومن هنا يبرز التحدي: هل تُعامل هذه الهجمات كجرائم جنائية أم كحرب تستدعي تطبيق قواعد القانون الدولي الإنساني؟ وهو ما يعكس الحاجة إلى

إطار قانوني جديد يستوعب خصوصية الحرب السيبرانية ويوازن بين الحماية وعدم التوسع في مفهوم الحرب [1].

إن الفرضية الثانية تعتبر الهجمات السيبرانية حربًا إذا ترتب عليها آثار مادية ملموسة في المجالات الاقتصادية والأمنية والعسكرية. كما أن قرار الجمعية العامة للأمم المتحدة بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات يؤكد أن لهذه الهجمات آثارًا واسعة قد تُلحق دمارًا بمختلف جوانب الحياة، لكن رغم الاعتراف بخطورتها لا يزال التعامل معها يتم في إطار محدود دون وجود اتفاقية دولية واضحة تحدد أو تقيد آثارها.[2].

- **ثانياً: جريمة السّرقة الإلكترونيّة**

إنّ جريمة السّرقة الإلكترونيّة لا تمثّل جريمة ذات طبيعة، أو كيان خاص يقتضي إخضاعها لقواعد خاصة، إذ تعدُّ من جرائم القانون العام، ولا تجعل منها وسيلة ارتكابها بجهاز إلكتروني جريمة جديدة. فمن الخطأ النظر إلى الجرائم الإلكترونيّة على أنها نوع خاص من الجرائم.

---

[1] رامي متولي القاضي، مكافحة جرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، ط1، دار النهضة العربية، القاهرة، 2011، ص66.

[2] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002، ص45.

استنادًا الى ذلك تعدُّ الجرائم الإلكترونيّة من جرائم القانون من جهة طبيعتها وأركانها العامّة، وهي ملحقة بالقسم الخاص من قانون العقوبات العام، وإن كان لها ذاتيّتها الخاصّة كسائر جرائم القسم الخاص.

تُعد عقوبة السرقة الإلكترونية من أبرز القضايا التي تختلف باختلاف التشريعات الوطنية، إذ إن كل دولة تضع إطارًا قانونيًا خاصًا بها لمواجهة هذه الجرائم وفقًا لخطورتها وتأثيرها على المجتمع. ففي بعض الدول، قد تقتصر العقوبة على الغرامات المالية أو الحبس لفترات قصيرة إذا كانت الجريمة بسيطة، بينما قد تصل العقوبة في حالات أخرى إلى السجن المؤبد، خاصةً إذا ارتبطت الجريمة بالاستيلاء على مبالغ مالية ضخمة أو الاعتداء على بيانات رسمية ذات أهمية استراتيجية.

وتتفاوت العقوبة أيضًا بحسب طبيعة الجريمة: فالجرائم البسيطة مثل اختراق البريد الإلكتروني أو تزوير حسابات على مواقع التواصل الاجتماعي غالبًا ما تُعاقب بعقوبات أقل شدة، بينما الجرائم المتوسطة مثل الاحتيال الإلكتروني وسرقة البيانات والابتزاز تُواجه بعقوبات أشد وفقًا للمواد القانونية. أما الجرائم الخطيرة، مثل اختراق مواقع أجهزة الدولة أو الإضرار بالأنظمة المعلوماتية الحيوية أو ارتكاب جرائم تهدد النظام العام والأمن القومي، فإنها قد تؤدي إلى السجن لسنوات طويلة أو حتى السجن المؤبد، نظرًا لما تشكله من تهديد مباشر لاستقرار الدولة ومصالحها الحيوية.

المطلب الثاني

ظروف التشديد (الطابع المنظم. العابر للحدود. المساس بالبنية الحرجة)

ظروف التخفيف

ظروف التشديد في الجريمة السيبرانية هي حالات تزيد من خطورة الفعل الإجرامي وتؤدي إلى عقوبات أشد، وتتضمن استغلال الوظيفة العامة، أو استغلال القُصّر، أو ارتكاب الجريمة عبر عصابة منظمة، أو استهداف بنى تحتية حيوية، أو استخدام تقنيات معقدة مثل الشبكات الآلية، الهدف من التشديد هو حماية المجتمع من الآثار السلبية لتلك الجرائم وردع مرتكبيها عن طريق زيادة العقوبة لتناسب خطورة الفعل وتأثيره.

أولاً: ظروف التشديد في الجرائم السيبرانية

أ- **الطابع المنتظم**

في الجريمة السيبرانية يشير إلى تكرار الهجمات والانتهاكات باستخدام أساليب وتقنيات متطورة ومنظمة، حيث يقوم مرتكبوها بالتخطيط والتنفيذ عن بُعد باستخدام شبكات الإنترنت، مما يجعلها ذات خطورة متزايدة ويصعّب اكتشافها وإثباتها. تُظهر الجريمة السيبرانية طابعًا منتظمًا من خلال الأنماط المتكررة في الأدوات المستخدمة، مثل البرمجيات الخبيثة والهجمات الموجهة، والطبيعة المستمرة للأهداف، والتي تشمل سرقة المعلومات، تعطيل الأنظمة، ونشر البرامج الضارة.

ب–العابر للحدود

الجرائم السيبرانية العابرة للحدود هي جرائم إلكترونية يمتد أثرها بين دول مختلفة، مما يخلق تحديات قانونية ومؤسساتية بسبب اختلاف التشريعات وصعوبة تتبع الأدلة الرقمية. وتتميز بخطورتها على الأمن القومي والاقتصاد الرقمي، إذ قد تُرتكب في دولة وتُحدث ضررًا في أخرى أو بالتنسيق بين عدة جهات دولية [1].

ج – المساس بالبنية الحرجة

إن بناء فضاء سيبراني آمن يتطلب خططًا وطنية لمكافحة الجرائم الإلكترونية عندما تكون الأفعال مجرّمة قانونًا، وخططًا للأمان السيبراني لمنع الهجمات والمضايقات غير المجرّمة رغم أضرارها، باعتبارها سلوكًا غير ملائم [2].

الحوسبة السحابية تُعد عنصرًا أساسيًا في الحفاظ على السيادة السيبرانية، إذ توفر أدوات لحماية البيانات والخصوصية. وتستند في ذلك إلى اتفاقية الجات (GATS)التي تمنح استثناءات خاصة لحماية السجلات والحسابات الفردية. كما أن تحليل التهديدات السيبرانية يكشف عن جانب داخلي يتمثل في سيطرة

---

[1] جنان فايز الخوري، الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود، مكتبة صادر للنشر، بيروت، 2009، ص202.

[2] وسيم الحجار، النظام القانوني لوسائل التواصل الجماعي، دراسة قانونية مقارنة حو الخصوصية والحرية الشخصية والمسؤولية والاختصاص، المركز العربي للبحوث القانونية والقضائية، بيروت، 2017، ص4.

الدولة على إقليمها واستخدامها الشرعي للقوة. فقد كان الجيش والشرطة يحتكران مواجهة التهديدات الداخلية، مع منع مشاركة المدنيين في هذه المهام. وتكفل القواعد القانونية الدولية حماية المدنيين من أي اعتداء وضمان عدم تعرضهم للإصابة. [1].

2 – التهديدات الخارجية: إن أغلب التهديدات التي تستهدف الدولة في الأصل خارجية، تختلف مداها وأثرها ودوافعها وتتوقف على المهاجمين وأدواتهم وقد أصبح الأمر مختلفا بعد ظهور الفضاء السيبراني، فالشبكة ليس لها مقر في دولة معينة، ولا تخضع للرقابة ولا سيطرة لدولة ما عليها، ولا يوجد قانون جنائي موحد نافذ فيها، إذ إن القوانين العقابية والإجرائية تتعدد بعدد الدول، فالتعري بالنسبة لامرأة على شبكة الإنترنيت مباح في أمريكا وفرنسا مثلاً، بينما يعتبر جريمة في تشريع جمهورية مصر العربية أو دولة الإمارات العربية المتحدة[2].

---

[1] احمد عبد الكريم سلامة، الانترنيت والقانون الدولي الخاص فراق ام تلاقي، الطبعة الثالثة، بحوث مؤتمر القانون والكمبيوتر والانترنيت المنعقد بتاريخ 31 مايو 2000 جامعة الإمارات العربية المتحدة كلية الشريعة والقانون المجلد الأول، الامارات، 2004، ص 26.

[2] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دار النهضة العربية، مصر، 2009، ص577.

المبحث الثاني

التعاون الدولي في تدعيم الأمن السيبراني

إن التحديات التي يفرضها العنصر العابر للحدود الوطنية عند التحقيق في الجرائم السيبرانية مماثلة لتلك التحديات التي ترتبط بجرائم عبر وطنية أخرى، ونتيجة لمبدأ السيادة الوطنية الذي بمقتضاه لا يمكن إجراء أي تحقيقات في إقليم دولة أجنبية أخرى بدون إذن من السلطات المحلية الأخرى، فان التعاون الوثيق بين الدول المعنية أمر بالغ الأهمية في تحقيقات الجرائم السيبرانية[1] . **وينقسم هذا المبحث إلى مطلبين يتناول المطلب الأول الجهود الدولية الاتفاقية في تدعيم الأمن السيبراني والمطلب الثاني الجهود الوطنية في تدعيم الأمن السيبراني.**

المطلب الأول

الجهود الدولية الاتفاقية في تدعيم الأمن السيبراني

سنعالج هذا المطلب موضوع القانون الذي هو الأساس الذي يستند إليه كل طلب لالتماس المساعدة القانونية المتبادلة أو تسليم المجرمين ويقصد بالأساس القانوني تحديد النصوص القانونية التي تستند إليها الدول في تنفيذ طلب المساعدة المتبادلة أو تسليم المجرمين، وفق الفقرات التالية:

أولاً: الاتفاقيات الدولية ذات الصفة العامة المتصلة بالتعاون بين الدول:

---

[1] جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، مكتبة السنهوري، بغداد، 2012، ص 54.

في غياب الاتفاقيات الثنائية أو التشريعات الداخلية، تعجز السلطات الوطنية عن تقديم المساعدة القانونية وتسليم المجرمين، بينما توفر الاتفاقيات الدولية أساسًا للتعاون الجنائي المشترك. وتمتاز هذه الصكوك الدولية باتساع نطاقها الجغرافي، مع مراعاة الخصوصيات الإقليمية والنظم القانونية لضمان فعالية التعاون[1] .

ثانياً: الأساس القانوني للتعاون الدولي في معاهدة بودابست 2001.

التعاون الدولي لمكافحة الجريمة يقوم على تبادل المساعدة وتضافر الجهود بين الدول لمواجهة التهديدات الإجرامية وتجاوز مشكلات الحدود والسيادة. وقد أرست اتفاقية بودابست لمكافحة الجرائم السيبرانية أسسًا قانونية ومبادئ فعالة لضمان تعاون دولي مشترك [2]:

1- المبادئ العامة ذات الصلة بالتعاون الدولي:

- تنص المادة (23) من اتفاقية بودابست على مبدأ التعاون الدولي بأوسع نطاق ممكن وتذليل العقبات أمام تبادل المعلومات والأدلة. كما توسع نطاق التعاون

[1] دليل التعاون الدولي في المسائل الجنائية لمكافحة الإرهاب، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، منشورات الأمم المتحدة، نيويورك، 2009، ص 21.

[2] إمام حسنين عطا الله، جرائم تقنية المعلومات في التشريعات والصكوك العربية، دار جامعة نايف للنشر، الرياض، 2017، ص 198.

ليشمل الجرائم السيبرانية والجرائم التقليدية المرتبطة بالأدلة الرقمية، مع إضافة مبدأ آخر في المادة(24) [1].

- مبدأ التعاون الفعال في المسائل الجنائية، تبين الاتفاقية إن الشروط الوارد ذكرها في القواعد القانونية للاتفاقية المتعلقة بالتعاون لا تبطل شروط الوثائق الدولية المتعلقة بالتعاون بالنص على أن التعاون في المادة (23) يتم من خلال تطبيق الصكوك الدولية ذات الصلة والخاصة بالتعاون الدولي الفعال وبالترتيبات المتفق عليها بمقتضى التشريعات الموحدة أو ذات الصلة بالمعاملة بالمثل والقوانين الوطنية
- مبدأ كفاية الأدلة وازدواجية التجريم: يتطلب إعداد طلبات المساعدة القانونية وجود أدلة إثبات كافية لتقديمها، ومقدار هذه الأدلة يكون مبنياً جزئياً في التشريعات القانونية الصادرة عن الدولة متلقية الطلب فضلا عن ازدواجية التجريم الذي يقتضي أن يكون تصرف الشخص محرم في الدول التي تبتغي التعاون الدولي، ونجد هذا المبدأ بنص المادة (24) بنصها شريطة أن يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين [2].

2- الأساس القانوني للتعاون الدولي:

---

[1] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنيت، دار المطبوعات الجامعية، الإسكندرية، 2008، ص 365.

[2] أمير فرج يوسف، مكافحة جريمة الإرهاب الإلكتروني، الإرهاب الرقمي في ظل اتفاقية دول مجلس التعاون لمكافحة الإرهاب، الطبعة الأولى، دار الكتب والدراسات العربية، الإسكندرية، 2015، ص 231.

المادة (24) من اتفاقية بودابست تُعد أساسًا قانونيًا للتعاون الدولي في مجال تسليم المجرمين، إذ تلزم الدول الأطراف بتسليم مرتكبي الجرائم المنصوص عليها في المواد .(11–2) كما تتيح الاتفاقية اعتبارها أساسًا قانونيًا للتسليم حتى في حال عدم وجود معاهدة ثنائية بين الدول .وتوفر الاتفاقية قواعد كافية للتعاون المشترك، مع التأكيد على المبادئ العامة للمساعدة المتبادلة .المادة (25) تلزم الدول الأعضاء بتقديم المساعدة على أوسع نطاق ممكن في القضايا الجنائية . وفي حال غياب اتفاق دولي، نصت الاتفاقية على تعيين سلطة مركزية مسؤولة عن تلقي وإرسال طلبات المساعدة.

المطلب الثاني

الجهود الوطنية في تدعيم الأمن السيبراني

إن استراتيجيات مواجهة الجرائم السيبرانية تبدأ من داخل الدولة ومن صلب قوانينها الجنائية، إذ أن التشريع الجنائي مسألة ضرورية للحد من الجرائم السيبرانية، ومع ذلك توجد العديد من المشاكل تجعل التشريع الوطني وحده غير كافياً في حد ذاته ويحتاج إلى ما يدعمه من الناحية الدولية بالأخص في الجرائم العابرة للحدود الوطنية[1] . ويثور سؤال حول أي جانب من جوانب القوانين الجنائية التي يجب مواءمتها من قبل الدول مع القواعد الإقليمية والدولية، وهل

(1) محمد شوقي وآخرون، الجرائم الإلكترونية والطب الشرعي الرقمي والسلطة القضائية، نشرته مركز ابحاث سبرينغر، 2015، ص 21.

هناك مبادئ يجب مراعاتها عند سن التشريعات في مواجهة هذه الظاهرة؟ هذا ما سيتم الإجابة وفق الفقرات التالية:

أولاً: مواءمة التشريعات الموضوعية

إن مواجهة الجرائم السيبرانية تتطلب وجود تشريعات وطنية تجرّم إساءة استخدام الحاسوب، مع ضرورة مواءمة هذه التشريعات بين الدول لتسهيل التحقيقات، تسريع المساعدة القانونية، وتسليم المجرمين. الاتساق مطلوب على المستوى الدولي والوطني، سواء في القوانين الجنائية أو السياسات المرتبطة بتكنولوجيا المعلومات، ويُعد تحديث القانون الجنائي أمراً أساسياً لاستيعاب الطبيعة الخاصة لهذه الجرائم(1) ..

بالنسبة للتشريع العراقي فقد كفل الدستور العراقي لعام 2005 الحق في التعبير والحق في الخصوصية بشكل شامل، والتي بينت بأن لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين[2]، أيضاً كفل الدستور حرية التعبير عن الرأي بكافة الوسائل وكذلك حرية الصحافة والإعلام والنشر[3] كذلك نجد فيه أن حرية الاتصالات والمراسلات وعدم جواز مراقبتها أو الكشف

---

[1] إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الالكترونية، بودابست عام 2001 والبروتوكول الملحق بها، دار النهضة العربية، القاهرة، 2009، ص28 – 32.

[2] المادة (17) من الدستور العراقي النافذ 2005.

[3] في المادة (38) الدستور العراقي النافذ 2005.

عنها[1]، كما نص على حرية الفرد في الفكر والضمير والعقيدة[2]، تعد هذه المواد الدستورية حماية لحرية التعبير والحق في الخصوصية، إلا إن في مجال قانون العقوبات نجد إن العراق لم يتجه في الوقت الحاضر إلى اتخاذ وجه معينة بصدد تحديث القواعد القانونية العقابية، فلم يسن المشرع العراقي قانون خاص بالجرائم السيبرانية بوجه عام، وما يرتكب من جرائم يرجع في معالجتها إلى القواعد العامة المنصوص عليها في قانون العقوبات رقم 111 لسنة 1969 المعدل.

ثانياً: مواءمة التشريعات الإجرائية:

لتمكين أجهزة إنفاذ القانون من جمع الأدلة على الصعيد العالمي، تعتبر المواءمة بين القوانين الإجرائية متطلبا ثانياً ضرورياً للتعاون الدولي الفعال ومن المهم التمييز بين المبادئ والإجراءات في مناسبة مناقشة تحديث التشريعات الإجرائية. فقاموس ويبستر (Merriam – Webster online dictionary) يعرف المبدأ بأنه: شامل وقانون أساسي، أو النظرية أو الافتراض أو القاعد»، أما الإجراء فهو طريقه خاصة لإنجازه ومن هنا يمكن فهم الفرق بأن المبدأ هو حقيقة أساسية تحكم مسعى محدد والإجراء هو طريقة لإنجاز شيء ما[3] .

---

[1] في المادة (40) الدستور العراقي النافذ 2005.

[2] في المادة (42) الدستور العراقي النافذ 2005.

[3] كيفن كاردويل وآخرون، الجرائم الإلكترونية والطب الشرعي الرقمي، نشرته سبرينغر، نيويورك، 2007، ص 54.

ومن أهم المبادئ التي يجب إن تحويها التشريعات الإجرائية في مواجهة الجرائم السيبرانية ما يلي:

1- مبدأ اليقين: اليقين في النظم الإجرائية يتطلب أن تكون الأدلة الرقمية حقيقية وموثوقة رغم قابليتها للتعديل أو الحذف، لذا يجب التحقق من مصدرها وسلامتها قبل عرضها على المحكمة واعتمادها في الحكم[1] ...

2- مبدأ المشروعية: إن مشروعية الدليل الجنائي تعني ضرورة اتفاق الإجراء مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع، فضلا عن مراعاة إعلانات حقوق الإنسان والمواثيق والاتفاقات الدولية وقواعد النظام العام ومبادئ المحكمة العليا[2] .

3- مبدأ المشاركة: إن نجاح التحقيقات في الجرائم السيبرانية يتطلب تعاون القطاع الخاص في مجال الاتصالات والتكنولوجيا، خصوصاً في توفير بيانات المشتركين وحركة المرور والمحتوى. هذا التعاون يجب أن يكون منظماً بقانون لضمان عدم تركه لمشيئة الشركات أو استغلاله من قبل السلطات، وليكون معترفاً به أمام القضاء

---

[1] إيوغان كيسي، الدليل الرقمي وجرائم الكمبيوتر، الطبعة الثالثة، نشرته السفير، ماريلاند، 2011، ص 68.

[2] عبد الله احمد هلالي، حجية المخرجات الكمبيوترية في المواد الجنائية، مصدر سابق، ص 751 - 754.

خاتمة

إن التعاون القانوني الدولي يشكّل ركيزة أساسية في تدعيم الأمن السيبراني، إذ يتيح مواجهة الجرائم الإلكترونية ذات الطابع العابر للحدود بفعالية أكبر. فالتنسيق بين التشريعات الوطنية والاتفاقيات الدولية يعزز من قدرة الدول على تبادل المعلومات والأدلة الرقمية، ويحد من الملاذات الآمنة للمجرمين السيبرانيين. كما أن هذا التعاون يسهم في بناء منظومة ردع متكاملة، تحقق التوازن بين حماية المجتمع الرقمي وضمان الحقوق الفردية، وتدعم الثقة في الفضاء الإلكتروني العالمي.

النتائج

1. أثبتت الجرائم السيبرانية أنها تتجاوز الحدود الجغرافية، مما يجعل التعاون القانوني ضرورة لا خياراً.
2. وجود تفاوت بين التشريعات الوطنية يضعف فعالية مكافحة الجرائم الإلكترونية.
3. التعاون القضائي الدولي يسهل تبادل الأدلة الرقمية ويعزز سرعة التحقيقات.
4. الأمن السيبراني لا يمكن تحقيقه بشكل كامل دون إطار قانوني دولي منسق.

التوصيات

1. تعزيز الاتفاقيات الدولية الخاصة بمكافحة الجرائم السيبرانية وتحديثها بما يتناسب مع التطور التقني.
2. إنشاء آليات دائمة لتبادل المعلومات والأدلة الرقمية بين الدول بشكل آمن وسريع.
3. توحيد المعايير القانونية المتعلقة بالأدلة الرقمية لضمان قبولها أمام المحاكم المختلفة.
4. دعم بناء قدرات الأجهزة القضائية والأمنية عبر التدريب المستمر في مجال التحقيقات السيبرانية.

قائمة المصادر والمراجع

المراجع العربية

1. أحمد عبد الكريم سلامة، الانترنيت والقانون الدولي الخاص: فراق أم تلاقي . الطبعة الثالثة، بحوث مؤتمر القانون والكمبيوتر والانترنيت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول، الإمارات، 2004.
2. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الالكترونية، بودابست عام 2001 والبروتوكول الملحق بها .القاهرة: دار النهضة العربية، 2009.
3. جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها .بغداد: مكتبة السنهوري، 2012.
4. جنان فايز الخوري، الجرائم الاقتصادية الدولية والجرائم المنظمة العابرة للحدود .بيروت: مكتبة صادر للنشر، 2009.
5. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي .القاهرة: دار النهضة العربية، 2002.
6. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت . مصر: دار النهضة العربية، 2009.

7. وسيم الحجار، النظام القانوني لوسائل التواصل الجماعي: دراسة قانونية مقارنة حول الخصوصية والحرية الشخصية والمسؤولية والاختصاص . بيروت: المركز العربي للبحوث القانونية والقضائية، 2017.

8. عبد الله أحمد هلالي، حجية المخرجات الكمبيوترية في المواد الجنائية.

القوانين

9. الدستور العراقي النافذ لسنة 2005، المادة.(17)

10. الدستور العراقي النافذ لسنة 2005، المادة.(38)

11. الدستور العراقي النافذ لسنة 2005، المادة.(40)

12. الدستور العراقي النافذ لسنة 2005، المادة.(42)

المراجع الأجنبية

13. Cardwell, Kevin, et al. Cybercrime and Digital Forensics. New York: Springer, 2007.

14. Casey, Eoghan. Digital Evidence and Computer Crime. 3rd ed. Maryland: Elsevier, 2011.

15. Shoukry, Mohamed, et al. Cybercrime, Digital Forensics, and the Judicial Authority. Springer Research Center, 2015.