Kufa Journal of Arts
September 2025. No. 65, P 142-174
Faculty of Arts, University of Kufa.

مجلة آداب الكوفة
العدد ٦٥، ايلول ٢٠٢٥م، ص ١٤٢-١٧٤
كلية الآداب، جامعة الكوفة

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

المسؤولية عن الجرائم الالكترونية العابرة للحدود وفقا لقواعد القانون الدولي

أ.م.د. محمد جبار جدوع العبدلي
كلية القانون - جامعة الكوفة
mohammedj.jaddoa@uokufa.edu.iq

م.م. حيدر جمعة منجي النصراوي
قسم الشؤون القانونية / جامعة الكوفة
Hayderj.alnasrawi@uokufa.edu.iq

م.م. حـــسام هاتف مسلم
قسم الشؤون القانونية / جامعة الكوفة
Hussamh.shareef@uokufa.edu.iq

م.م أنسام عبد الواحد ناصر
كلية علوم الحاسوب و الرياضيات/ جامعة الكوفة
ansama.banizuhra@uokufa.edu.iq

تاريخ الاستلام: ٢٠٢٥\٦\٨ تاريخ القبـــول: ٢٠٢٥\٧\١٣ تاريخ النشر: ٢٠٢٥/٩/١

الملخص:
يهدف هذا البحث إلى تحليل الإشكاليات القانونية المعاصرة المتعلقة بالجرائم الإلكترونية ذات الطابع العابر للحدود، في ضوء قواعد القانون الدولي الجنائي، فمع تصاعد هذه الظاهرة بات من الضروري تفكيك المفاهيم التقليدية للمسؤولية والاختصاص والسيادة، ينطلق البحث من فرضية مفادها أن النظام القانوني الدولي بصيغته الكلاسيكية يعجز عن استيعاب البنية اللاجغرافية واللامادية للجرائم الإلكترونية، ما يستلزم إصلاحاً مفاهيمياً وتشريعياً عميقاً ، ويعتمد منهجاً وصفياً تحليلاً لتفصيل الطبيعة القانونية للجرائم الإلكترونية، وتحليل أركانها، وأسس المسؤولية عنها سواء في بعدها الفردي أو الدولي، كما يسلّط الضوء على التحديات التقنية والإجرائية في الإثبات والتتبع، وغياب اتفاق دولي شامل، رغم المبادرات الأممية والإقليمية، ويختم البحث بتقديم تصور متكامل لتحديث القواعد الدولية لمساءلة مرتكبي الجرائم الإلكترونية العابرة للحدود وتفعيل قواعد المسؤولية الجزائية والمدنية بشأنها، مع التركيز على أهمية التعاون الدولي والتقنين التشريعي والتعويض الدولي، لتفادي إفلات الجناة من العقاب وضمان أمن المجتمعات الرقمية.

الكلمات المفتاحية: الجرائم الالكترونية، المسؤولية الدولية، الجرائم العابرة للحدود، الاثبات الرقمي، اركان الجريمة الالكترونية، التعويض.

Responsibility of Transnational Cybercrimes According to the Rules of International Law

Asst. Prof. Dr. Mohammed Jabbar.J. AL-Abdali
University of Kufa\Faculty of Law

Asst. Lecturer Haider J Munji Al-Nasrawi
Legal Affairs Department / University of Kufa

Asst. Lecturer Hussam h. shareef
Legal Affairs Department / University of Kufa

Asst. Lecturer Ansam Abedalwahed
Faculty of computer science and mathematics/ Universitv of Kufa

Received Date: 8/6/2025, Accepted Date: 13/7/2025, Published Date: 1/9/2025

Abstract:
This research aims to analyze the contemporary legal challenges related to transnational cybercrimes in light of the rules of international criminal law. With the escalation of this phenomenon, it has become necessary to deconstruct traditional concepts of responsibility,

DOI: https://doi.org/10.36317/kja/2025/v1.i65.20035
Kufa Journal of Arts by University of Kufa is licensed under a Creative Commons Attribution 4. 0 International License.
مجلة آداب الكوفة - جامعة الكوفة مرخصة بموجب ترخيص المشاع الإبداعي ٤,٠ الدولي.

jurisdiction, and sovereignty. The study is based on the hypothesis that the classical international legal system fails to accommodate the non-geographical and intangible nature of cybercrimes, necessitating profound conceptual and legislative reforms. The research adopts a descriptive-analytical approach to detail the legal nature of cybercrimes, analyze their elements, and the foundations of liability both individually and internationally. It also highlights technical and procedural challenges in evidence and tracking, and the absence of a comprehensive international agreement despite United Nations and regional initiatives. The study concludes by presenting a comprehensive vision for updating international rules to hold perpetrators of cybercrimes accountable, emphasizing the importance of international cooperation and legislative regulation to prevent impunity and ensure the security of digital communities.

Key words: Distance measurement, international responsibility, cross-border missiles, evidence, elements of a minor crime, digital compensation.

المقدمة

في عصرٍ تتسارع فيه التحولات الرقمية وتتلاشى فيه الحدود الجغرافية أمام شيفرات المعلومات وتدفقات البيانات، أضحت الجريمة الإلكترونية العدو اللامرئي للمنظومة القانونية الدولية، فهذه الجريمة لا تقتصر على اختراقات فردية، بل تمثل تحدياً وجودياً لفكرة السيادة، وتعيد طرح سؤال العدالة والمساءلة في فضاء لا تعترف كياناته بالحدود أو الجنسيات من هنا، يتناول هذا البحث إشكالية مركزية تتعلق بمدى فاعلية قواعد القانون الدولي الجنائي في ملاحقة الأفعال الجرمية التي تقع في بيئة سيبرانية لامادية ولا مركزية، لا يقتصر البحث على عرض المفاهيم والنصوص، بل يتجاوز ذلك إلى مساءلة جوهر المنظومة القانونية الدولية، متسائلاً عن مدى قدرتها على احتواء فاعلين رقميين غير محددي الهوية أو الموطن، ومتتبعاً حدود المسؤولية الفردية والدولية في أزمنة رقمية متشابكة، كما يتقصّى البحث العلاقة بين مبدأ السيادة ومكان وقوع الجريمة ونتيجتها، ويحلل الأطر المعيارية للمساءلة وفقاً لمشروعي مواد المسؤولية الدولية لعام ٢٠٠١، واتفاقيات مثل بودابست ٢٠٠١ واتفاقية الأمم المتحدة ٢٠٢٤، ليقدّم تصوراً قانونياً متماسكاً ومقترحاً لإعادة تشكيل منظومة العدالة الدولية في ظل العولمة الرقمية.

مشكلة البحث:

ان الجريمة الإلكترونية العابرة للحدود لا تنتهك فقط قواعد السيادة التقليدية بل تقوّض أيضاً الأسس المفهومية لمسؤولية الفرد في القانون الجنائي الدولي فضلاً عن المسؤولية الدولية، لذا تطرح الدراسة إشكالية جوهرية تتعلق بقدرة القانون الدولي الجنائي على مواكبة تحوّلات الفعل الإجرامي في الفضاء السيبراني، فكيف يواجه المشرع الوطني او الدولي جريمة لا تعترف بالجغرافية، ولا تُرتكب بجسد، بل تُبرمج بفكر وتُبث عبر شبكات لامركزية؟

وكيف تصبح مهمة القانون الدولي الجنائي مزدوجة، ليس فقط في ردع الجريمة ومعاقبة مرتكبيها، بل في إعادة التعريف والحدود ومفاهيم المسؤولية والمساءلة التي يستند إليها؟

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

أهمية البحث

لا يستهدف هذا البحث الكشف عن الشرخ بين ظاهرة الجريمة السيبرانية والاساس القانوني، بل يغوص في العمق، لان الفعل الاجرامي غير ملموس والضحية غير معروفة ولا الجاني محدد الهوية او المكان، لان الجرائم الالكترونية العابرة للحدود تضعنا امام حالة تمتحن فيها أسس المسؤولية الفردية ذاتها، لان الفاعل يتحول من مجرد عقدة الى نطاق أوسع ويتعاون مع مجموعة من الفاعلين المجهولين والمبرمجين المتخفين، وعلى أساس ذلك تتبلور أهمية البحث في تكوين صورة قانونية واخلاقية حديثة عن المسؤولية الجنائية الدولية، ومحاولة لاستنطاق القانون الجنائي الدولي في زمان تتلاشى فيه الحدود، حيث تكمن أهمية البحث حين فقدان مكان الفعل الجرمي ونهوض المسؤولية عندما يتوارى المجرم خلف الحاسوب، ويغوص في البحث عن عدالة يتم اختبارها خارج زمن تقليدي، للوصل الى العدالة المستقبلية التي تبحث عن حقيقتها في فضاءٍ حر غير معترفاً بالحدود.

فرضية البحث

يفترض هذا البحث ان القانون الجنائي الدولي بالصيغة التقليدية والتي تأسست على مفاهيم السيادة والإقليم والفاعل المادي المحدد، يُجابه قصوراً بنيوياً في التعامل مع الجرائم الإلكترونية ذات الصفة العابرة للحدود بسبب الطبيعة اللامركزية واللامادية واللامتناهية لتلك الأفعال.

ومن ثم فإن تحقيق الفاعلية القانونية في هذا المجال لا يمكن ان يقتصر على توسعة أدوات التجريم أو تعزيز التعاون الدولي، بل يتطلب إعادة نظر بشكل جذري وواسع في الإطار المفاهيمي لمسؤولية الفرد من الناحية الجنائية الدولية، مع مراعاة تداخل الأدوار الرقمية وتعدد بيئات الفعل الجرمي.

تنطلق فرضية البحث بأن التحدي الأساسي لا يكمن في غياب القواعد بل في عجزها عن إدراك طبيعة الفعل الجديد الذي قد يكون مخفياً او غير متعيّن ولا يرتبط بإقليم أو نظام قانوني واحد، مما يستدعي تفكيك الحدود التقليدية بين الجريمة والسيادة وبين الفاعلية الجنائية والمساءلة الأخلاقية في مضمار السباق الرقمي العولمي الجديد.

نطاق البحث

ينحصر نطاق البحث في دراسة الإطار القانوني للمسؤولية الجنائية حول الجرائم الإلكترونية العابرة للحدود، ضمن بُنية القانون الدولي الجنائي وفقاً لتحقق أركان الجريمة الدولية (جريمة حرب أو عدوان أو ضد الانسانية أو إبادة جماعية) في السلوك الاجرامي محل الدراسة، مع امكانية تفعيل القواعد العامة للمسؤولية الدولية عنها، والتركيز على الإشكالات النظرية والعملية المرتبطة بتحديد الفاعل الرقمي، وإسناد الفعل الجرمي في بيئة لا تعترف بالإقليم ولا تنضبط للحدود القضائية التقليدية، دون تناول الجوانب التقنية البحتة للجريمة الإلكترونية، وإنما يقتصر على الجوانب القانونية والفقهية ذات الصلة بإسناد المسؤولية، وتكييف الفعل الإجرامي، وآليات المساءلة في إطار دولي، كما لا يمتد إلى الجرائم الإلكترونية ذات البعد المحلي البحت، إلا إذا أفرزت آثاراً عبر حدود الدولة.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

منهج البحث

يعتمد البحث على المنهج الوصفي التحليلي، إذ يقوم بوصف ظاهرة الجريمة الالكترونية بوصفها عابرةً للحدود وتحليل أبعادها القانونية في ضوء قواعد القانون الدولي الجنائي، ويعتمد على تحليل النصوص الوطنية والدولية ذات الصلة، واستقراء آراء الفقه، كما يُوظّف البحث بعداً فلسفياً تأملياً، يساءل من خلاله المفاهيم التقليدية للمسؤولية الجنائية في مواجهة فاعل رقمي لا ينتمي إلى إقليم معين، ولا يخضع لمركز قانوني واضح، مما يفرض تحديات على بُنية العدالة الجنائية الدولية المعاصرة.

المبحث الأول: الإطار المفاهيمي للجرائم الإلكترونية العابرة للحدود

ولدت الجريمة الإلكترونية من رحم الحداثة التكنولوجية، لكنها سرعان ما تمردت على كل الحدود الجغرافية وتجاوزت مدارات القانون التقليدي، فهي ليست مجرد امتداد رقمي لأفعال مجرّمة سلفاً، بل نمط مغاير من الانتهاك ينتمي إلى بُنية رقمية عابرة لا تعترف بالإقليم ولا تتقيد بسيادة، ولا تخضع لحدود زمنية أو مكانية بالمعنى القانوني التقليدي.

إن الحديث عن الإطار المفاهيمي للجرائم الإلكترونية يقتضي قبل كل شيء استيعاب التحول الجذري في طبيعة الفعل الإجرامي ذاته، فلم تعد الجريمة تُرتكب بأدوات مادية في مكان معلوم ضد ضحية واضحة، بل بات يكفي نقرة زر أو سطر برمجي ليُفضي إلى إضرار جَسيم بمصلحة قانونية، سواء أكانت مالًا أو سمعة أو خصوصية أو حتى كياناً معنوياً بأكمله.

وفي ظل هذا التحول، أضحى من المحال أن تُقارب هذه الجرائم من زاوية وطنية بحتة، إذ إن أغلب الجرائم الإلكترونية اليوم تتصف بالطابع العابر للحدود، بحيث يقع الفعل في دولة وتحدث نتيجته في أخرى ويكون الفاعل متخفياً تحت غطاء افتراضي في دولة ثالثة، وربما عبر خوادم موزعة في قارات متعددة، وهنا ينهض التحدي القانوني الأكبر: كيف يُمكن الإحاطة بهذه الجرائم تشريعياً، وكيف يُمكن مساءلة فاعليها ضمن قواعد وطنية تضيق عن استيعاب أبعاد الجريمة الرقمية؟ حيث تبرز أزمة التفاوت بين الأنظمة القانونية، فبينما قطعت بعض الدول شوطاً طويلاً في سنّ تشريعات متخصصة، وشاركت في اتفاقيات دولية كاتفاقية بودابست لعام ٢٠٠١ بشأن الجرائم السيبرانية، لا تزال بعض التشريعات الوطنية تُعاني فراغاً أو قصوراً واضحاً في التعامل مع طبيعة تلك الجرائم من جانب تعريفها وانواعها وخصائها ومفهوم الطابع العابر للحدود ومكان ارتكاب الجريمة ومكان الضرر وتحديات الجرائم الالكترونية وصعوبة التتبيع والاثبات وغياب الاتفاق الدولي الشامل والازدواجية القانونية كل ذلك سيختزل ضمن المبحث الأول لمبحثنا هذا وعلى النحو الآتي:

المطلب الأول مفهوم الجرائم الإلكترونية

لقد تعددت ألفاظ ومفردات وصيغ ومصطلحات ومفاهيم الجرائم الالكترونية، فقد أطلق عليها البعض بجرائم الكمبيوتر والانترنيت وجرائم التقنية العالية (High-Tech Crimes) أو الجرائم السيبرانية (cyber crimes) أو جرائم الحاسب الآلي (computer crimes) أو

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

الجرائم الرقمية (digital crimes) أو الجرائم الناعمة (soft crimes) أو جريمة أصحاب الياقات البيض (white collar crimes) أو الجرائم النظيفة (clean crimes)، وبغض النظر عن التسمية المستخدمة سنحاول بيان تعريفها وأنواعها واهم خصائصها من خلال الفرعين الآتيين:

الفرع الأول التعريف بالجرائم الالكترونية

اولاً/ تعريف بالجرائم الالكترونية: لوحظ عدم اتفاق جمهور الباحثين والدارسين بل حتى التشريعات حول تسمية وصياغة تعريف موحد يحتوي على العناصر الاساسية للجريمة الالكترونية، حيث أطلق على التعريف عدة اسماء منهم من يسميها (الجريمة المعلوماتية) واخرون يسموها (جرائم الانترنيت) وجمع اخر يسميها (جرائم الكمبيوتر) وتوجه اخرون الى اسم (جرائم المعالجة الالية للبيانات والمعطيات)، كما تعددت المقاربات التي حاولت الإمساك بجوهر الجريمة الإلكترونية، فانبثق عن كل اتجاه تعريف يعكس زاويته المعرفية وحدود تصوره لطبيعة الفعل الجرمي المتولد من رحم البيئة الرقمية، فذهب فريق ذو النزعة التقنية يُعنى بتحديد الجريمة الإلكترونية من زاوية الأداة المستخدمة، ويرى أنها كل نشاط إجرامي يُرتكب باستخدام الحاسوب أو شبكة الإنترنت، سواء أكان ذلك الاستخدام مباشراً أو غير مباشر، طالما أن الوسيط الرقمي يشكّل جزءً من البُنية التحتية للفعل الإجرامي، ويستوجب هذا التعريف فهم المصطلحات التقنية المرتبطة به، من قبيل: الحاسب الآلي، البرامج، البيانات، الممتلكات الرقمية، الدخول غير المشروع، والخدمات الحيوية (الشكري، ٢٠٠٨).

وذهب فريق ذو النزعة القانونية الفقهية الذي انشغل بفهم الجريمة الإلكترونية بوصفها ظاهرة مستحدثة تنتمي إلى صنف خاص من الجرائم ذات الطبيعة اللاعنفية، والتي تتصف بالخفاء والدقة وسرعة التنفيذ وتكاد تنفلت من قبضة الإثبات التقليدي، إذ تخلو في الغالب من الأثر المادي المحسوس وتُمكن مرتكبها من تخريب الأدلة الرقمية بلمح البصر، فهي جريمة ذات طابع متجاوز للحدود السيادية، مما يجعل من مواجهتها أمراً عسيراً في ظل قصور التشريعات وضعف الوعي التقني لدى السلطات الضبطية والقضائية، فضلاً عن التعقيد الإثباتي الذي تفرضه بنيتها التكنولوجية (وهيب، ٢٠١٤).

أما بعض التعريفات فقد سعت لتجريد الجريمة الإلكترونية من البواعث الشخصية والغايات الربحية، مركّزة على الفعل ذاته، بوصفه انحرافاً قانونياً يستند إلى المعالجة المعلوماتية ويستدعي تدخل المشرّع والعقاب، ما يجعلها جرائم مستقلة بذاتها، لا بمجرد الوسيلة المستخدمة بل بطبيعة البُنية القانونية والرقمية التي تنطوي عليها (هجيج & سالم، دون سنة).

وذهبت منظمة التعاون الاقتصادي والتنمية لتعريف الجريمة الالكترونية في اجتماع باريس عام ١٩٨٣ والذي يعد من أقدم التعاريف وعلى النحو الاتي "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها" (الطوابلة، دون سنة).

وخلاصة القول، فإن الجريمة الإلكترونية ليست مجرد امتداد رقمي للجرائم التقليدية، بل هي نمط جديد من الاعتداءات القانونية، يتميز بسمات خاصة تنبع من الفضاء السيبراني الذي أفرزها

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

من حيث الوسيلة والمجال والأثر، ومن ثم فهي تستلزم مقاربة قانونية جديدة تراعي تعقيداتها وتداخلها مع النظام المعلوماتي المعولم، وتستوجب ملاءمة التشريعات الوطنية، كالتشريع العراقي، مع القواعد الدولية، لتوفير إطار ناظم يحقق التوازن بين حماية الأمن السيبراني واحترام الحقوق الرقمية وتحقيق العدالة في عالم تتلاشى فيه الحدود الجغرافية أمام المعطى الرقمي المتسارع.

ثانياً/ أنواع الجرائم الالكترونية: تنطوي الجرائم الإلكترونية على صور متعددة ومتنوعة، يعزى تنوعها إلى طبيعة الوسائط التقنية المستخدمة ومجالات الإضرار الناتجة عنها، ويمكن تصنيف هذه الجرائم على وجه الإجمال إلى الأنماط الآتية:

١. **الجرائم الماسة بالمعطيات الإلكترونية للحاسوب:** يُقسَّم هذا النوع من الجرائم إلى نوعين رئيسين وفقاً للمعطيات الالكترونية للحاسوب:

أ- **الجرائم الواقعة على المعطيات ذاتها**: وهي الجرائم التي تستهدف البيانات والمعلومات المخزنة في الأنظمة الإلكترونية، عبر تشويهها أو تعديلها أو إتلافها، ويُرتكب النوع هذا عبر وسائل تقنية ضارة مثل الفيروسات والبرمجيات الخبيثة.

ب- **الجرائم الواقعة على مدلول المعطيات الإلكترونية:** وهي التي تستهدف ما تمثّله تلك المعطيات من قيمة مالية أو تجارية، كأن يتم الاستيلاء على الأموال المرتبطة بالحسابات البنكية أو البطاقات الائتمانية من خلال الحاسوب، أو يتم الاتجار غير المشروع بالمعلومات المستخلصة نتيجة هذا النوع من الجرائم.(المويشير، ٢٠٠٩).

٢. **الجرائم الماسة بالمعطيات الإلكترونية ذات الطابع الشخصي:** وتتجسد الجريمة في الاعتداء على المعلومات او البيانات الشخصية المخزنة إلكترونياً، والتي تتصل بحياة الأفراد الخاصة، كالمراسلات، والصور، والمعلومات الصحية أو المالية، ما يشكّل مساساً خطيراً بالحق في الخصوصية المكفول قانوناً (عوض، ١٩٩٣).

٣. **الجرائم الماسة بحقوق الملكية الفكرية:** ويشمل هذا الصنف من الجريمة الأفعال التي تمس الحقوق الأدبية والمالية لأصحاب الابتكارات والمصنفات الفكرية، ومن أبرزها نسخ أو استخدام البرامج الإلكترونية دون ترخيص مسبق، إعادة تدوير البرمجيات أو التلاعب بمحتواها أو نسبتها زوراً، انتهاك العلامات التجارية وبراءات الاختراع باستخدام الوسائط الإلكترونية، تحميل الكتب والمصنفات الإلكترونية المحمية بحقوق المؤلف دون سداد المقابل المالي أو دون الحصول على إذن مشروع (عرب، ٢٠٠٦، ص ٩).

٤. **جرائم أخرى متعددة:** وتشمل الجرائم الالكترونية من حيث الهدف الذي تسعى الى تحقيقه:

أ- **جرائم التشهير:** وهي تلك الأفعال التي يُقصد بها تشويه سمعة الأفراد والنيل من مكانتهم الاجتماعية أو الوظيفية، عبر نشر معلومات أو صور أو أقوال مسيئة تمس شرفهم أو اعتبارهم، باستخدام المنصات الرقمية ومواقع التواصل الاجتماعي.

ب- **المطاردة الإلكترونية (Cyberstalking):** وتتمثل في تتبّع الأفراد ومراقبة تحركاتهم وأنشطتهم عبر الوسائل الإلكترونية المختلفة، سواء بغرض الإحراج العلني،

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

أو لتحقيق مكاسب غير مشروعة، كارتكاب جرائم السرقة المالية، أو ابتزاز الضحايا وتهديدهم بنشر معلومات شخصية أو حساسة تم جمعها دون رضاهم.

ت- **جرائم القذف والسبّ والشتم:** وهي الأفعال التي تتضمن توجيه عبارات أو ألفاظ تنطوي على إهانة صريحة أو اتهام بغير حق، تمس شرف الشخص أو كرامته أو تنال من اعتباره في محيطه الاجتماعي، ويزداد خطرها حين يتم تداولها أو تكرار نشرها إلكترونياً على نطاق واسع.

وتتسم هذه الجرائم بخطورة بالغة، إذ لا تقتصر آثارها على النواحي النفسية والمعنوية للضحية، بل قد تمتد إلى تهديد أمنه الشخصي واستقراره الاجتماعي، مما يُحتّم ضرورة مواجهتها بتشريعات رادعة ووسائل تقنية مضادة تكفل الحماية القانونية الفاعلة (سمارة، ٢٠٠٨).

الفرع الثاني خصائص الجرائم الإلكترونية

أضحت الفضاءات الرقمية ميداناً مفتوحاً للتواصل العابر للحدود، بمختلف أشكاله ومستوياته، إلا أن هذا الانفتاح لم يخلُ من تداعيات سلبية إذ برزت إلى السطح ظواهر إجرامية جديدة تمثّلت في انتشار الحسابات الوهمية التي يُدار بعضها من قبل أشخاص ينتهجون سلوكاً إجرامياً يستهدف الأفراد والمجتمعات على حدٍ سواء.

وأمام تصاعد وتيرة هذه الجرائم وتعقّد أساليب ارتكابها، سعت غالبية الدول، كلٌ بحسب إمكاناته، إلى تكثيف جهودها لمواجهتها والحدّ من آثارها، سواء من خلال إعداد دراسات أكاديمية رصينة، أو بحوث أمنية معمّقة تُعنى بكشف طرائق ارتكاب هذه الجرائم وتحليل الخصائص السلوكية لمرتكبيها، فضلاً عن الوقوف على الدوافع النفسية والاجتماعية المحرّكة لهم، وفي ذات السياق، بادرت العديد من الدول إلى سنّ تشريعات متخصصة تتلاءم مع خصوصية البيئة الرقمية، وتستوعب المستجدات التقنية، بما يكفل مواجهة هذه الجرائم بفعالية وعدالة. (المشهداني، ٢٠٠١، ص ٣٠).

ومن أجل التصدي المنهجي للجرائم الإلكترونية، فإن الوقوف على خصائصها الجوهرية يُعدّ مدخلاً أساسياً لفهم طبيعتها، وتتلخّص أبرز هذه الخصائص في الآتي:(الموني، ٢٠١٠، ص ٥٨)

أولاً/ جرائم يصعب إثباتها والكشف عنها: تتّسم الجرائم الإلكترونية بقدرٍ عالٍ من التعقيد والغموض، يجعل من عملية إثباتها والكشف عنها أمراً بالغ الصعوبة، ويُعزى ذلك إلى طبيعتها الرقمية المجردة، إذ إنها لا تخلّف آثاراً مادية ملموسة كما هو الحال في الجرائم التقليدية، بل تتم عبر رموز ومعطيات إلكترونية متغيرة باستمرار، يصعب تعقّبها أو الاحتفاظ بها كدليل مادي مباشر.

وغالباً ما يتم اكتشاف هذه الجرائم مصادفة، وبعد مرور فترة زمنية طويلة على ارتكابها، دون أن تترك خلفها بصمات إلكترونية كافية تُيسّر مهمة المحقق الجنائي، ويُضاف إلى ذلك أن مرتكبي هذا النوع من الجرائم غالباً ما يتحلّون بدرجة عالية من الذكاء والتمكّن التقني، مما

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

يمنحهم القدرة على إخفاء آثارهم والتلاعب بالأدلة، وهو ما يجعل الوسائل التقليدية للتحقيق، التي يعتمدها المحقق الكلاسيكي، غير كافية أو فعالة في ملاحقتهم (مراد، د.ت، ص ٣٨).

ثانياً/ جرائم عابرة للحدود: أي تتّسم بكونها لا تعترف بالحدود الجغرافية للدول، وهو ما سنتناوله بشكل اكثر تفصيل خلال المطلب الثاني.

ثالثاً/ جرائم ماسة بالقيم الأخلاقية والآداب العامة: تشكل بعض الجرائم الإلكترونية تهديداً مباشراً للمنظومة الأخلاقية للمجتمع، لا سيما من خلال نشر وتداول المواد الإباحية والمحتويات المخلة بالحياء، مما يسهم في اشاعة الفسق والفجور وتقويض القيم والضوابط الاجتماعية الراسخة (المشهداني، ٢٠٠١، ص ٣٠).

رابعاً/ الفئة العمرية لمرتكبي الجرائم الالكترونية: تشير المؤشرات الإحصائية المتوفرة إلى أن الفئة العمرية الغالبة على مرتكبي الجرائم الالكترونية تتراوح بين (١٨ - ٤٦) عاماً، مع متوسط عمري يقدّر بـ (٢٥) عاماً، وتدل هذه المعطيات على أن أغلب مرتكبي هذا النوع من الجرائم هم من فئة الشباب، وهو ما يُعزى إلى إلمامهم الواسع باستخدام تقنيات الحواسيب والأنظمة الرقمية، على خلاف الفئات الأكبر سناً التي لم تحظَ بذات الفرصة للتعامل مع الحواسيب نتيجة للتغيرات التقنية المتسارعة وحداثة الطفرة المعلوماتية، وتُعد هذه السمة مؤشراً دالاً على الطبيعة المعاصرة والمرتبطة بالتطور التكنولوجي في تكوين الجريمة المعلوماتية (الشكري، ٢٠٠٨).

خامساً/ محل الجريمة: تُوجَّه الجريمة الالكترونية أساساً إلى النيل من المعطيات الإلكترونية بصورها المختلفة، باعتبارها تمس المعنويات لا الماديات (الدسوقي، ٢٠١٠)

المطلب الثاني مفهوم الطابع العابر للحدود

أرخت الجرائم الإلكترونية بظلالها الكثيفة على المنظومة القانونية الدولية، إذ اتسمت بطابعها العابر للحدود، فغدت لا تعرف وطناً ولا تعترف بسيادة متجاوزة بذلك المفاهيم التقليدية لمكان الجريمة وزمانها، الأمر الذي أفضى إلى نشوء معضلة قانونية دقيقة تتمثل في تنازع الاختصاص بين الدول وتعارضه أحياناً مع مبدأ احترام السيادة الوطنية، وما كان يُعالَج بالأمس بأدوات التحقيق التقليدية وآليات البحث الجنائي الكلاسيكية بات اليوم قاصراً عن الإحاطة بجوانب هذه الجرائم المعقدة، التي تشهد تطوراً متسارعاً نتيجة لاحترافية مرتكبيها وتنامي قدرتهم على توظيف التكنولوجيا الحديثة بوصفها وسيلة ومسرحًا للجريمة في آنٍ واحد.

أفرز هذا الواقع تحدياً مزدوجاً، من جهةٍ هي قصور في أدوات التحقيق التقليدية، ومن جهةٍ أخرى تعقيد ناتج عن تشتت عناصر الجريمة بين كيانات رقمية وجغرافية متباعدة، ولعلّ الخطر الأعمق يكمن في أن هذه الجرائم لا تنتهك فقط أنظمة الحماية القانونية، بل تقوّض مبدأ سيادة القانون ذاته إذا لم تُواجَه برؤية قانونية عابرة للحدود، وتعاون دولي قائم على الثقة والتكامل القضائي (بن فرحات & عمري، ٢٠٢٤، ص ٦٦٢).

ومن خلال ما تقدم، سنتناول مفهوم الطابع العابر للحدود عبر فرعين، الاول ليان هذ الطبيعة، والفرع الثاني لبيان تحدياتها.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

الفرع الاول الطبيعة العابرة للحدود

أن الطبيعة العابرة للحدود للجرائم الالكترونية، كما ذكرنا ذلك بشكل مختصر خلال خصائص هذه الجرائم، يأتي من عدم تقيدها بالحدود الجغرافية للدول، فهي ترتكب عبر آلاف الأميال في لحظات معدودة وتتسبب بآثار متزامنة ممكن ان تصيب عدة دول، مما يجعل مواجهتها تحدياً قانونياً وأمنياً يتطلب الوقوف عليه، حيث تتجلى هذه الطبيعة بالتعقيد، إذ أصبحت هذه الجرائم في العصر الرقمي الحديث تتجاوز الإطار الإقليمي للدول، متمددة في فضاءٍ افتراضي لا تعترف حدوده بالجغرافية ولا تحكمه سيادة تقليدية، وبات التحقيق فيها يواجه إشكاليات جوهرية في تحديد ولاية قضائية مكانية وتطبيق القوانين الوطنية ذات الصلة، مما أفضى إلى تنازع الاختصاص بين عدة أنظمة قانونية، كلٌّ منها يدّعي لنفسه الأحقية في الملاحقة والمعاقبة

إن الطبيعة العابرة للحدود التي تتسم بها هذه الجرائم تُحتِّم مقاربةً قانونية قائمة على التوازن بين متطلبات العدالة الجنائية وضرورات احترام السيادة، بما يضمن فعالية الإجراءات من جهة، ومشروعية الوسائل من جهة أخرى (بن فرحات & عمري، ٢٠٢٤، ص ٦٦).

وتأتي الطبيعة العابرة للحدود من خلال الآتي:

أولاً/ مكان ارتكاب الجريمة: أسهم التطور التكنولوجي المتسارع في توسيع نطاق الاتصال بالحواسيب المركزية، وتعزيز ترابطها مع قواعد البيانات العالمية بوساطة الاتصالات الشبكية الحديثة ، لاسيما شبكات الهاتف وشبكة الإنترنت، الأمر الذي أفضى إلى تصاعد ملحوظ في حالات التلاعب بالأنظمة المعالجة إلكترونياً، سواء كان على مستوى البُنية التقنية أو البيانات المخزّنة، ولا يقف التلاعب عند حدود المعالجة الداخلية، بل يمتد ليطال مرحلة الإخراج النهائي للمعلومات، حيث يُعمد إلى تغيير مضمون البيانات، أو حذف أجزاء منها، أو استبدالها ببيانات مغايرة في المعنى والدلالة، ويؤدي إلى انحراف للنتائج المخرجة يُفضي إلى الغش والاحتيال المعلوماتي، ويُغيّر من القيمة القانونية أو المحاسبية أو الإدارية للمعلومة الأصلية.

وتكمن العبرة القانونية في توصيف هذا الفعل بكونه احتيالاً الكترونياً حين تُفرغ البيانات من معناها الحقيقي، لتُعاد صياغتها وفق نية جرمية تنطوي على الخداع، ولعلّ أخطر ما في هذه الجرائم في مرحلة الإخراج المتلاعب بها غالباً ما تُستخدم لطمس آثار الجريمة الإلكترونية، وتضليل أدوات التحقيق الرقمي.

ومن زاوية أخرى، فإن شبكات الاتصال الدولية تلعب دوراً مركزياً في تحويل هذه الجرائم إلى جرائم عابرة للحدود، إذ يمكن أن يُرتكب النشاط الجرمي كزرع الفيروس أو تعديل البيانات من داخل دولةٍ ما، بينما تتحقق نتائجه وأضراره في نظام معلوماتي تابع لدولة أخرى، مما يضع هذه الأفعال ضمن نطاق الجرائم العابرة للإقليم الوطني، ويستدعي تحركاً قانونياً دولياً مشتركاً لمواجهتها (قوره، ٢٠٠٥).

ثانياً/ مكان الضرر: تقع الجرائم العابرة للحدود بارتكاب أفعال إجرامية التي في أكثر من دولة أو تمتد آثارها إلى دول متعددة، وفي هذا السياق، يُعد مكان الضرر هو الدولة التي وقع فيها الأثر السلبي للجريمة، سواء كان ذلك ضرراً مادياً أو اقتصادياً أو اجتماعياً أو بيئياً، حيث تُعتبر الدولة

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

المستقبلة لأثر الجريمة هي مكان الضرر؛ لأنها تتعرض للآثار السلبية المباشرة لهذه الجريمة، ان تحديد مكان الضرر له أهمية كبيرة في القانون الدولي والجنائي، لأنه يساعد في تحديد الولاية القضائية ويسمح للدولة المتضررة بممارسة سلطتها القضائية على الجناة، وكذلك تعزيز التعاون الدولي في التحقيق والملاحقة القضائية، خاصة عندما تكون الجريمة معقدة وتشمل عدة دول لضمان إنصاف الضحايا وعدم افلات المجرمين من العقاب، وان تحديد مكان الضرر في الجرائم التقليدية يكون من خلال الموقع الجغرافي الذي وقع فيه الضرر، أما في الجرائم الإلكترونية، فقد يكون الضرر في الدولة التي يقيم فيها الضحية، فإذا تعرض مواطن في العراق للاحتيال عبر الإنترنت من جهة خارجية، يُعتبر العراق مكان الضرر، أو قد يكون في الدولة التي تستضيف الخوادم المخترقة إذا تم استهداف خوادم موجودة في دولة معينة، فتعد تلك الدولة مكان الضرر، أو يكون مكان الضرر في الدولة التي حدث فيها الأثر الاقتصادي أو الاجتماعي، فإذا تسبب هجوم إلكتروني في خسائر مالية لشركة في دولة معينة، فتعد تلك الدولة مكان الضرر (هجيج & سالم، دون سنة).

ان تحديد مكان الضرر في الجرائم الإلكترونية يواجه عدة تحديات سنحاول تسليط الضوء عليها خلال الفرع الثاني.

الفرع الثاني تحديات الجرائم الإلكترونية العابرة للحدود

تُعدّ جرائم الإنترنت من الظواهر الإجرامية المستحدثة التي تتميّز بجملة من الخصائص الفنية والموضوعية، تجعل من التصدي لها وضبط مرتكبيها مهمة شاقة أمام الأجهزة الأمنية، لاسيما على المستوى الوطني، إذ أن هذه الجرائم بطبيعتها تتجاوز الحدود التقليدية لسيادة الدولة، لتتخذ طابعاً عابراً للحدود في بيئة رقمية لا تعترف بالفواصل الجغرافية أو القيود الإقليمية، الأمر الذي يتيح لمرتكبيها تنفيذ أفعالهم الإجرامية بسهولة عبر الشبكة المعلوماتية الدولية، وهو ما يُفضي إلى تعقيد الجهود الرامية إلى مكافحتها، سواء على الصعيد الداخلي أو في أطر التعاون الدولي (بولحة & خلوفي، ٢٠١٩).

أولاً/ صعوبة التتبع والاثبات: تُعدُّ الجرائم الإلكترونية من أصعب أنماط الإجرام في الإثبات والتحقيق، لأنها تتسم بطابع غير مادي، وسرعة في التنفيذ، وقدرة عالية على إخفاء الآثار الرقمية أو طمسها دون أن تخلّف أدلة محسوسة، كما أن هذه الجرائم تقع في بيئة افتراضية لا تخضع للحدود الجغرافية التقليدية، مما يُعقّد مهمة التتبع الفني، ويستلزم تعاوناً دولياً فعّالاً يصطدم غالباً بتباين التشريعات وتفاوت مستويات الخبرة الفنية لدى جهات التحقيق، أضف إلى ذلك أن وسائل الإثبات الرقمية كالبصمات الإلكترونية وسجلات الخوادم قد تكون عرضة للتلاعب أو الإتلاف بوسائل تقنية متقدمة، ما يُضعف حجيتها أمام القضاء ويثير تحديات قانونية تتعلق بحجية الدليل الإلكتروني وإجراءات جمعه وحفظه، كما أن عدم ظهور الدليل المادي التقليدي في مثل هذه الجرائم يجعل من الاعتماد على القرائن التقنية أمراً حتمياً، مما يتطلب إعداداً قضائياً متخصصاً في فهم طبيعة الأدلة الرقمية، ويُضاف أيضاً الضعف في البنى التحتية

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

للتحقيق الإلكتروني في العديد من الدول يزيد من صعوبة الكشف عن الجناة وملاحقتهم جنائياً بصورة فعالة (الحارثي، دون تاريخ).

ثانياً/ غياب اتفاق دولي شامل: تُعدُّ الجرائم الإلكترونية من أبرز التحديات القانونية المعاصرة التي تواجه الدول والمجتمعات الدولية على حدٍّ سواء، وعلى الرغم من وجود عدد من الاتفاقيات الدولية والإقليمية التي تناولت بعض أوجه هذه الظاهرة الإجرامية، إلا أن المجتمع الدولي لا يزال يفتقر إلى اتفاق شامل وموحد يُنظِّم جميع أبعادها، ويُوفِّر إطاراً قانونياً دولياً جامعاً لمكافحتها.

١. أسباب غياب الاتفاق الدولي الشامل:

أ- **التباين التشريعي بين الدول:** تتباين النظم القانونية الوطنية في تعريف الجرائم الإلكترونية، وفي تحديد أركانها والعقوبات المقررة لها، الأمر الذي يُشكِّل عائقاً جوهرياً أمام صياغة اتفاق دولي موحد يُراعي هذا التنوع القانوني.

ب- **اعتبارات السيادة الوطنية:** تتحفظ بعض الدول على الدخول في التزامات دولية قد تقيد من صلاحياتها السيادية في ملاحقة الجرائم الإلكترونية ضمن نطاقها الإقليمي، لاسيما حينما يتعلّق الأمر بالتدخل في البُنية التحتية الرقمية أو البيانات السيادية.

ت- **الاعتبارات الاقتصادية والتكنولوجية:** تتأثر مواقف الدول بشأن الاتفاقيات الدولية بمصالحها التجارية والتكنولوجية، إذ تخشى بعض الدول من أن تفرض المعايير الدولية الموحدة قيوداً قد تُضعف تنافسيتها في سوق التكنولوجيا الرقمية (هلالي، ٢٠٠٣).

٢. الجهود الدولية المبذولة: على الرغم من غياب اتفاق دولي شامل، فقد شهد المجتمع الدولي اعداد من المبادرات والاتفاقيات هدفها تنظيم بعض أوجه الجرائم الإلكترونية، وذلك من خلال مبدأ عدم التدخل في الشؤون الداخلية للدول الذي أقره القانون الدولي بشكل صريح من خلال ميثاق الامم المتحدة وإعلان زيادة فعالية مبدأ الامتناع عن التهديد باستعمال القوة أو استعمالها في العلاقات الدولية لسنة ١٩٨٧، حيث يمكن اعتماده في عدم مشروعية الجرائم الالكترونية العابرة للحدود باعتبارها تدخلاً في شؤون الدولة المستهدفة، كما بذلت الأمم المتحدة جهوداً كبيرة لتطوير إطار قانوني دولي ينظم السلوك في الفضاء السيبراني، حيث أكدت الجمعية العامة عام ٢٠١٥ على ضرورة احترام قواعد القانون الدولي وما يرتب على ذلك من الحقوق والواجبات السيادة في استخدامها لتكنولوجيا المعلومات والاتصالات بما في ذلك الفضاء السيبراني (العزازي، دون تاريخ، ص ٤٩٩).لينتهي الأمر بإقرار الأمم المتحدة اتفاقية لمكافحة الجريمة السيبرانية عام ٢٠٢٤ التي تدخل حيز النفاذ بعد مرور (٩٠) يوم على إيداع الوثيقة الاربعين للتصديق او القبول او الاقرار او الانضمام وفقًا للمادة ٦٥ من اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية (٢٠٢٤). لتمثل خطوة مهمة على صعيد تعزيز العمل الدولي في مكافحة الجرائم الالكترونية العابرة للحدود، كما عملت العديد من المنظمات الإقليمية على تطوير قواعد ومعايير لمكافحة الجرائم الالكترونية العابرة للحدود وحماية البنية التحتية الحيوية وتعزيز

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

التعاون الدولي كاتفاقية بودابست والمعروفة أيضاً باسم اتفاقية مجلس أوروبا بشأن الجريمة الإلكترونية لعام ٢٠٠١، وهي مراجعة جماعية لمواجهة الجرائم الالكترونية من قبل الدول الاعضاء في مجلس اوربا وغيرها، عبر تجريم قائمة من الهجمات ضد أجهزة الكمبيوتر وتحديد أدوات القانون الإجرائي للتحقيق في الجرائم الإلكترونية وتأمين الأدلة الإلكترونية والتعاون الدولي بشأن تلك الجرائم وادلتها (قطاف & بوقرين، ٢٠٢٢، ص ٣٣٧).

إن غياب اتفاق دولي موحد يُضعف من فاعلية الجهود المبذولة في مواجهة الجريمة الالكترونية ويؤدي إلى تشتت المعايير وتضارب الإجراءات القانونية بين الدول، ومن ثم فإن الضرورة باتت ملحة لتكثيف التعاون الدولي، والتوصل إلى اتفاق شامل يُنظِّم سُبل الوقاية والملاحقة القضائية، ويوفّر أدوات قانونية موحدة لمواجهة هذا التحدي العابر للحدود (حجازي، ٢٠٠٧).

المبحث الثاني: أحكام مسؤولية الأفراد عن الجرائم الالكترونية العابرة للحدود

تمثل الجرائم الالكترونية العابرة للحدود تحدياً متزايداً لقواعد المسؤولية في القانون الدولي، حيث تسبب آثاراً خطيرة على مستوى العلاقات الدولية قد تصل لدرجة تهديد السلم والأمن الدوليين, وتشمل هذه الآثار مجموعة واسعة من العواقب القانونية والعملية كتهديد السيادة الوطنية (الجبوري، ٢٠٢٤) في ظل تحديات تواجه المجتمع الدولي نتيجة استخدام تكنولوجيا المعلومات ليس فقط من قبل الدول بل أيضاً من قبل جماعات غير حكومية غالباً ما تعلن مسؤوليتها عن تلك الجرائم أو الهجمات التي تلحق أضراراً بالغة بالقطاعات الضرورية للحياة البشرية (صادق، ٢٠٢٤، ص ٩٣).

وقد تكون الجرائم الالكترونية ضمن نزاع مسلح لتكون مسؤولية مرتكبيها بشكل فردي وفقاً لقواعد القانون الدولي الانساني باعتبارها جريمة دولية، او قد تكون هناك دول راعية او داعمة او متسترة على مرتكبيها فيتم النظر إليها في إطار المسؤولية عن الأعمال غير المشروعة دولياً، وقد تعتبر الجرائم الالكترونية العابرة للحدود جرائم إرهابية في حال كان تنفيذها بهدف إدخال الرعب أو الخوف والفزع بين الناس أو إثارة الفوضى وزعزعة الاستقرار السياسي أو إلحاق أضرار جسيمة، لتُطبق بشأنها القوانين المتعلقة بمكافحة الإرهاب

وسنتناول المسؤولية الدولية عن الانتهاكات السيبرانية لسيادة الدول من خلال مطلبين، الاول لمحددات هذه المسؤولية، والمطلب الثاني لبيان آثارها.

المطلب الاول محددات المسؤولية عن الجرائم الإلكترونية العابرة للحدود

تعد فكرة السيادة حديثة نسبياً ظهرت في القرن السادس عشر على يد الفقيه الفرنسي (جان بودان) في مؤلفه الكتب الستة للجمهورية عام ١٥٧٧، جاعلاً منها عنصراً جوهرياً لمفهوم الدولة، فمن غير الممكن ان تكون الدولة دون سيادة (الحديثي، ١٩٨١، ص. ٢٠).

فهي الأساس التي تستند عليها الدولة في تعاملها الخارجي مع الدول الأخرى وفي تطبيقها داخل الدولة (شبر، ٢٠٠٦، ص. ٧). وأحدث ظهور الفضاء الالكتروني تحولات جوهرية في مفهوم

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

السيادة التقليدية، مما أثار تساؤلات حول آثار تلك السيادة بمفهومها الجديد وقدرة الدول في الحفاظ على سيادتها في ظل تحديات يفرضها الفضاء الرقمي المتنامي مما يجعله أداة قوية في الصراعات الحديثة (عبادة، ٢٠٢٣). وبالتالي يتوجب بيان الاساس القانوني للمسؤولية عن الجرائم الإلكترونية العابرة للحدود وكذلك بيان اركان هذه الجريمة من خلال الفرعين الآتيين:

الفرع الأول الأساس القانوني للمسؤولية عن الجرائم الالكترونية العابرة للحدود

يمكن أن يكون الاساس القانوني للمسؤولية عن الجرائم الإلكترونية العابرة للحدود في عدة مبادئ للقانون الدولي كحظر استخدام القوة او عدم التدخل في الشؤون الداخلية للدول.

أولاً/ حظر استخدام القوة او التهديد بها: أشار ميثاق الامم المتحدة إلى حظر استخدام القوة او التهديد بها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة (ميثاق الأمم المتحدة، ١٩٤٥، المادة ٢، الفقرة ٤) وأثار تفسير (القوة) في المبدأ المذكور جدلاً دولياً وفقهياً واسعاً حول مدى شمولها لغير الاسلحة التقليدية كالوسائل الالكترونية، فتمسكت الدول المتفوقة بهذه الوسائل كالولايات المتحدة وروسيا بالتفسير الضيق للقوة بحجة يتقيّد بديباجة الميثاق والفقرة (٤) من المادة (٢) منه فضلاً عن الاعمال التحضيرية لصياغتها، والتي اشارت جميعها إلى قصر الحظر على القوة المسلحة (فرج الله، ١٩٨٦، ص. ٢١٨).

في حين هناك اتجاه آخر يتمسك بالتفسير الواسع لمعنى القوة المحظورة لتشمل كذلك القوة السيبرانية عند تحقيقها لآثار مادية ملموسة، مدنية أو عسكرية، حيث أكدت الأعمال التحضيرية لمؤتمر سان فرانسيسكو، الذي سبق اعتماد الميثاق، على أن تحديد حظر استخدام القوة الواردة في المادة (٢) من الميثاق جاء على سبيل المثال لا الحصر بقصد التوضيح لا التضييق من نطاق الحظر في العلاقات الدولية (بوراس، ٢٠٠٩، ص. ١٣٠).ولا يوجد مبرر قانوني لقصره على القوة المسلحة، فيجب أن تشمل أي وسيلة تهدد استقلال الدول وتعرض مصالحها للخطر او تقيد قدراتها في صد الاعتداء الموجه ضدها لحماية امنها القومي (العاني، ١٩٩٧، ص. ٦١٢).

وأشارت الجمعية العام للأمم المتحدة في قرارها بخصوص مكافحة الاساءة من استخدام تكنولوجيا المعلومات لغرض اجرامي لعام ٢٠٠١ إلى ضرورة منع ومكافحة هذا الاستعمال السيء لتكنلوجيا المعلومات لتحقيق أهداف إجرامية (الأمم المتحدة، ٢٠٠١). كما أقرت الجمعية العامة عام ٢٠٠٥ إعلان بانكوك في نطاق منع الجريمة والعدالة الجنائية، المتضمن منع إساءة استعمال نظم الاتصالات والشبكات الحاسوبية لأغراض إجرامية وضرورة التحقيق في الجرائم الالكترونية وملاحقة مرتكبيها قضائياً (الأمم المتحدة، ٢٠٠٥).

وأصدرت الجمعية أيضاً عام ٢٠٠٩ قراراً يقضي بضرورة التعاون في مكافحة إساءة استخدام التكنولوجيا لأغراض إجرامية والتحقق فيما إذا كانت التشريعات كافية للتحقيق في جرائم الفضاء الإلكتروني ومحاكمة مرتكبيها (الأمم المتحدة، ٢٠١٠)

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

ووفقاً لما تقدم، فإن المسؤولية عن ارتكاب الجرائم الالكترونية العابرة للحدود يمكن أن يكون لانتهاك تلك الجرائم لمبدأ حظر استخدام القوة او التهديد بها في العلاقات الدولية.

ثانياً/ مبدأ عدم التدخل في الشؤون الداخلية للدول: يقصد بهذا المبدأ حق كل دولة في إدارة شؤونها الداخلية دون تدخل خارجي، وقد تضمنه ميثاق الامم المتحدة (ميثاق الأمم المتحدة، ١٩٤٥، المادة ٢، الفقرة ٧)

لكن تعرض المبدأ لتحديات جديدة نتيجة التوسع في استخدام التكنولوجيا في الصراعات وظهور أشكال جديدة من التهديدات مثل الجرائم الالكترونية نتيجة الصعوبة في تحديد الجهة المسؤولة عنها وصعوبة جمع الأدلة في الفضاء الرقمي، ولتجاوز هذه التحديات يجب على المجتمع الدولي أن يعمل على تطوير إطار قانوني دولي أكثر شمولاً يحدد بوضوح السلوك المقبول, كما يجب تعزيز التعاون الدولي بين الدول لضمان تنفيذ هذا الإطار القانوني، مما يتضح إن حماية مبدأ عدم التدخل في الشؤون الداخلية للدول أمر حيوي للحفاظ على استقرار العلاقات الدولية، خاصة في ظل التطورات المتسارعة في العالم المعاصر وتطوير آليات جديدة لضمان تطبيقه الفعال (امين ، بدون تاريخ)

ويمكن إيجاد حظر الجرائم الالكترونية العابرة للحدود باعتبارها انتهاكاً لمبدأ عدم التدخل في الشؤون الداخلية للدول، حيث أكدت ديباجة إعلان بشأن زيادة فعالية مبدأ الامتناع عن التهديد باستعمال القوة أو استعمالها في العلاقات الدولية الذي اقرته الجمعية العامة للأمم المتحدة بموجب قرارها المرقم (٢٢/٤٢) لسنة ١٩٨٧ على (حق كل دولة، غير القبل للتصرف، في أن تختار نظامها السياسي الاقتصادي والاجتماعي والثقافي دون أي شكل من أشكال التدخل من جانب دولة أخرى) وأشار إلى أن "على الدول التزاماً بعدم التدخل، بشكل مباشر أو غير مباشر ولأي سبب كان، في الشئون الداخلية أو الخارجية لأي دولة أخرى"، كما ألزم الدول بالامتناع عن (التدخل المسلح وجميع أشكال التدخل أو محاولات التهديد الأخرى التي تستهدف شخصية الدولة أو عناصرها السياسية والاقتصادية والثقافية) ، وبالتالي يمكن أن تكون تلك الجرائم محلاً للمسؤولية الدولية، رغم مطالبة دول أخرى مثل الصين وروسيا بسيادة مطلقة على الفضاء الالكتروني توازي سيادتها الإقليمية، لكن تلك المطالبات تسعى الى فرض "قبضة حديدية" على هذا الفضاء، فسيادة الدولة في الفضاء الالكتروني مقيدة بضرورة احترام الحريات الأساسية، وفي مقدمتها الحق في الخصوصية وحرية التعبير (عبد الحمزة, ٢٠٢٢).

الفرع الثاني اركان المسؤولية عن الجرائم الالكترونية العابرة للحدود

تُعدّ الأركان القانونية أساساً لا غنى عنه لقيام المسؤولية الجنائية عن الجرائم الإلكترونية، شأنها في ذلك شأن الجرائم التقليدية، غير أن خصوصية هذا النمط من الإجرام من حيث بيئته الرقمية وطابعه العابر للحدود، تفرض إعادة النظر في كيفية تحقق أركانه، سواء على المستوى المادي أو المعنوي.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

وفي هذا السياق، سنتناول في هذا المطلب تحليل الركنين المادي والمعنوي للجريمة الإلكترونية العابرة للحدود من خلال بيان النشاط الإجرامي في البيئة الرقمية، واسناده الى الجناة وكذلك النتيجة الإجرامية المتمثلة بالضرر.

أولاً/ الفعل غير المشروع: يتمثّل الفعل غير المشروع في السلوك الخارجي الذي يأتيه الجاني، والذي يُشكّل مخالفة لقاعدة قانونية تحظر فعلاً أو تأمر به، وفي سياق الجرائم الإلكترونية، يكتسب هذا الركن خصوصية نابعة من طبيعة الفضاء الرقمي الذي تُرتكب فيه الأفعال الجرمية، بعيداً عن الوسائل المادية التقليدية، حيث لا تقتصر الجريمة الإلكترونية على الأفعال الصريحة التي يُقدم فيها الفاعل على اقتحام الأنظمة المعلوماتية أو العبث ببياناتها، بل تشمل أيضاً صوراً خفية من الإخلال بالواجبات القانونية والمهنية، قد يكون أثرها أشد خطراً ، فالتصرف الإجرامي قد يتجلى في صورة عمل إيجابي واضح، كأن يتعمد شخص ما اختراق شبكة معلومات محمية دون ترخيص، أو يلج إلى بيانات رقمية لا يملك حق الاطلاع عليها، مستغلًا أدوات تقنية متقدمة بقصد الإضرار أو الاستحواذ.

ويُعد هذا التمدد في نطاق الأفعال المجرّمة انسجاماً مع ما تفرضه البيئة الرقمية من تعقيد تقني وتشابك مسؤوليات، حيث لم تعد الجريمة محصورة في فعل مادي تقليدي، بل باتت تشمل أنماطاً متداخلة من الأفعال والتراخي الوظيفي، تتطلّب من التشريعات والسلطات القضائية قراءة جديدة للوقائع، تستوعب التطور السريع للوسائل التقنية وتُحسن تكييف الوقائع في إطار القواعد العامة للقانون الجنائي (قوره، ٢٠٠٥)

ثانياً/ الإسناد في الجرائم الكترونية العابرة للحدود: يشترط هذا الركن نسبة الجريمة الالكترونية إلى مرتكبها ليكون مسؤولاً عن آثارها، وهو أمر يواجه عدة تحديات، اشرنا لها مسبقاً خلال الدراسة، ويتوجب ان يكون الجاني قاصداً ارتكاب الفعل غير المشروع وراغباً بتحقيق نتيجتها، ويعرف بالجرائم الجزائية بالركن المعنوي للجريمة، باعتباره الرابط بين العناصر المادية للجريمة وشخصية مرتكبها، وتتخذ هذه الإرادة صوراً متعددة، فقد تتجسد في القصد الجنائي، وفي هذه الحالة تُعد الجريمة عمدية، أو قد تقوم على الخطأ غير العمدي، فتكون الجريمة غير عمدية (حسني، ١٩٧١، ص ٩٠)

وفي إطار الجرائم الإلكترونية، تُعد جريمة الدخول غير المشروع إلى نظم المعلومات مثالًا نموذجياً على الجرائم العمدية التي لا تقوم إلا بتوافر القصد الجنائي العام، والذي يتطلب اجتماع عنصرين:

١. العلم: أي أن يكون الجاني مدركاً تماماً أن دخوله إلى النظام المعلوماتي أو بقاؤه فيه مخالف للقانون، ويتم دون إذن أو ضد إرادة صاحب النظام أو من يملك السيطرة عليه، أو أن دخوله تجاوز حدود الصلاحية الممنوحة له.
٢. الإرادة: أي أن تتجه إرادته الحرة إلى ارتكاب هذا الفعل رغم علمه بعدم مشروعيته.

أما فيما يتعلق بـ جريمة التعدي على البيانات والمعلومات الإلكترونية، كجرائم الاحتيال المعلوماتي، فإنها تتطلب، إضافة إلى القصد الجنائي العام، توافر قصد جنائي خاص، يتمثل في

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

نية الإضرار بالغير أو تحقيق غرض غير مشروع، ويكفي لقيام هذا الركن أن يكون الفاعل عالماً بأن ما يقوم به يُشكّل اعتداءً على النظام أو البيانات، وأن يهدف من وراء فعله إلى إيقاع المجني عليه في الخداع أو التضليل، لحمله على تسليم مال أو منفعة أو كشف معلومات.

تتنوع صور المسؤولية الجنائية في الجرائم الإلكترونية باختلاف درجة إدراك الفاعل ونيته تجاه النظام الذي يخترقه أو يتجاوزه، ففي حالات يكون فيها الدخول إلى نظام معلوماتي مشروعاً، لكن مع تجاوز الصلاحيات المصرح بها، يُحتمل تصنيف هذا التصرف على أنه خطأ غير عمدي، خصوصاً إذا كان ذلك ناجماً عن خلل تقني أو قصور في إعدادات الأمان بالشبكة المعنية، ففي هذه الظروف، يُعفى الفاعل من المسؤولية الجنائية لعدم توافر عنصر القصد الجنائي، وعلى النقيض، يُعدّ ثبوت التعمد في التعدي على الصلاحيات المحظورة أمراً حاسماً لإثبات القصد الجنائي، وهو ركن أساسي لقيام الجريمة الإلكترونية (زعتر، ٢٠٢٣). فقد أقر القضاء الأمريكي بأن تحقق القصد الجنائي يتطلب توفر العلم بالدخول غير المشروع، إلى جانب الإرادة الصريحة في ارتكاب الفعل، مما يُشكل القصد الخاص الذي يعزز من شدة العقوبة، بينما اتجه القضاء الفرنسي إلى تقليص متطلبات القصد، مكتفياً بإثبات وجود سوء النية لدى الجاني، وهو معيار أقل حدة لكنه يظل كافياً لتأسيس المسؤولية الجنائية.

وفيما يتعلق بالتقصير التقني، فإن مظاهره قد تتجسد في الإهمال في تطبيق تحديثات الأمان الدورية أو ضعف الرقابة على الأنظمة الحاسوبية، ويفسح المجال أمام الثغرات الأمنية لاستغلالها من قبل جهات خبيثة، فمثلًا قد يؤدي عدم مراقبة سجلات الدخول أو الفشل في رصد محاولات الاختراق المستمرة إلى وقوع أضرار جسيمة، كاختراق بيانات حساسة أو تعطيل خدمات إلكترونية حيوية، وفي هذه الحالات يُعد التقصير التقني بمثابة إخلال جسيم بواجبات الحماية والتأمين، ما يؤدي إلى تحميل المسؤولين عن ذلك المسؤولية الجنائية.

وبذلك، فإن التقييم القضائي لمسألة التقصير التقني يجب أن يأخذ في الاعتبار مدى الالتزام بمعايير الأمن السيبراني المتعارف عليها في القطاع المعني، ومدى جدية التدابير المتخذة للوقاية من المخاطر الإلكترونية، وهو ما يعكس تعقيد التداخل بين القانون والتقنية في إطار مكافحة الجرائم الإلكترونية.

ثالثاً/ ضرر الجرائم الكترونية العابرة للحدود: تُعد النتيجة الإجرامية في الجرائم الإلكترونية تجسيداً للضرر الذي يترتب على الفعل غير المشروع، وهي تمثل إحدى الدعائم الجوهرية لقيام الركن المادي، ويختلف هذا الضرر في طبيعته وحدّته باختلاف صورة الجريمة وظروفها، فقد يبلغ أقصى درجاته عندما يتّخذ طابعاً مفضياً إلى الموت، كقيام طبيب عن عمد، بالولوج إلى قاعدة بيانات أحد المستشفيات وتعديل تركيب دواء مخصص لمريض، بقصد إحداث الوفاة، وفي هذه الحالة، تمتد الجريمة الإلكترونية إلى المساس بحق الإنسان في الحياة، بما يرتّب أخطر صور المسؤولية، وقد يكون الضرر ذا طبيعة مادية، كخسائر ناجمة عن إتلاف الأجهزة أو محو البيانات الحساسة، أو يتخذ شكلاً معنوياً يتمثل في الإساءة إلى السمعة، أو القذف والتشهير عبر

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

منصات التواصل الاجتماعي، وهو ما يُحدث أثراً اجتماعياً بالغ الخطورة، لا يقلّ عن الأضرار المالية.

أما ما يتعلق بالرابطة القانونية التي تربط الفعل بالضرر الناجم عنه، فإن ما يُعرف بـ الرابط المؤدي إلى تحقق النتيجة، يُعد عنصراً لا غنى عنه في إثبات المسؤولية الجنائية، فلا يكفي وقوع فعل محظور، ولا مجرد تحقق الضرر، ما لم يُثبت أن ذلك الضرر كان ناتجاً بصورة مباشرة ومعتبرة عن التصرف غير المشروع الذي ارتُكب في البيئة الرقمية.

ومن نافلة القول يتبين لنا ان الجريمة الالكترونية العابرة للحدود لا يمكن ان تكتمل الا بتحقق نتيجة للسلوك الاجرامي الذي يمكن ان يقسم الجرائم من حيث النتيجة الى جرائم خطر التي تتحقق بمجرد ارتكاب السلوك الجرمي اما جرائم ضرر فلا يمكن الاكتفاء بذلك السلوك وانما يتم البحث عن النتيجة المترتبة او الأثر الناجم عن ذلك السلوك لكون هذا الضرر هو التمثيل الحقيقي للركن المادي للسلوك الاجرامي الذي قد يقع بشكل اعتداء في الوقت الحالي او في المستقبل على مصلحة او محل حق تحت الحماية الجنائية (ممدوح، ٢٠١٩، ص ١٩٠).

المطلب الثاني آثار المسؤولية عن الجرائم الالكترونية العابرة للحدود

تُعتبر الجرائم الإلكترونية العابرة للحدود من أبرز التحديات القانونية في العصر الحديث، نظراً لطبيعتها المعقدة التي تتجاوز الحدود الجغرافية والسياسية للدول، وتداخلها مع مظاهر السيادة الوطنية والتعاون الدولي، تؤثر هذه الجرائم بشكل مباشر على الأفراد والمجتمعات والدول، سواء من خلال المساس بالأمن السيبراني أو الإضرار بالمصالح الاقتصادية والاجتماعية، مما يفرض ضرورة التطرق إلى آثار المسؤولية القانونية المترتبة على مرتكبيها.

في هذا السياق، يتناول المطلب الثاني من هذا البحث آثار مسؤولية الأفراد عن الجرائم الإلكترونية العابرة للحدود، من خلال فرعين أساسيين يسلطان الضوء على الجانبين الجزائي والمدني لهذه المسؤولية:

الفرع الاول المساءلة الجزائية للأفراد عن الجرائم الإلكترونية العابرة للحدود

ان المسؤولية الجزائية هي "عبارة عن الالتزام بتحمل الجزاء الذي ترتبه القواعد القانونية كأثر للفعل الذي يرتكب خروجاً على أحكامها " (حنش، ٢٠٢٠، ص ١١).وفي ظل مبدأ الشرعية (مبدأ لا جريمة ولا عقوبة إلا بنص)، تواجه الأجهزة القضائية تحدياً ليس يسيراً في تحديد النصوص العقابية اللازمة لمعاقبة مرتكبي الانتهاكات السيبرانية، خاصة عند عدم وجود تشريعات تعالج تلك الانتهاكات بشكل صريح وواضح، ليتم اللجوء حينها إلى القواعد العامة لتطبيقها على مرتكبي تلك الانتهاكات على نحو لا يسمح لهم بالإفلات من العقاب، ويمكن الوقوف على آثار المسؤولية عن الجرائم الالكترونية العابرة للحدود من خلال احكام القوانين الجزائية الوطنية أو من خلال القانون الجنائي الدولي.

أولاً/ القوانين الجنائية الوطنية: يتوافق التشريع العراقي مع الاتفاقيات الدولية في اعتماد مبدأ الاختصاص الإقليمي كأحد الضوابط الأساسية لتحديد ولاية القضاء الجنائي، وذلك وفقاً لأحكام

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

المادة (٦) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل، والتي تقر بأن جميع الجرائم المرتكبة داخل العراق تخضع لولاية القضاء الوطني بغض النظر عن جنسية أو صفة مرتكبها، كما يعتبر الفعل الجرمي واقعاً في العراق إذا وقع فيه أحد العناصر المكونة له، أو تحققت نتيجته، أو كان مقصوداً أن تتحقق داخله، وهو ما يكفل للدولة السيطرة القانونية الكاملة على الجرائم ذات الطابع الإقليمي، وإلى جانب ذلك يمتد نطاق الاختصاص الإقليمي ليشمل جميع أراضي جمهورية العراق، بما فيها المياه الإقليمية والفضاء الجوي التابع لها، مما يضمن شمولية التطبيق القضائي للجرائم الالكترونية الواقعة ضمن هذه الحدود، وقد تبنّى المشرّع العراقي أيضاً مبدأ الاختصاص العيني بموجب المادة (٩) بإخضاع الجرائم التي تمس أمن الدولة الداخلي والخارجي لولاية القضاء العراقي بغض النظر عن مكان وقوعها أو جنسية مرتكبها، كما أخذ بالاختصاص الشخصي في المادة (١٠)، حيث يُخضع القانون العراقي أي مواطن عراقي ارتكب جريمة خارج البلاد للمساءلة وفق أحكامه، بشرط أن يكون الفعل معاقباً عليه بموجب قانون الدولة التي وقع فيها، وأن يكون الجاني موجوداً داخل العراق.

أما فيما يتعلق بالاختصاص الشامل، فقد تم تكريسه بموجب المادة (١٣) من قانون العقوبات، حيث تخضع لولاية القضاء العراقي كل شخصية تُضبط داخل الدولة بعد ارتكابها خارج البلاد جرائم تمس الأمن الدولي، مثل تخريب أو تعطيل وسائل الاتصالات والمواصلات الدولية، أو الاتجار بالبشر والرقيق والمخدرات.

يتمتع القضاء العراقي بولاية قضائية كاملة لملاحقة مرتكبي الجرائم الالكترونية داخل البلاد، بغض النظر عن جنسيتهم أو موقع الجريمة، مستنداً إلى التشريعات الوطنية والاتفاقيات الدولية التي تنظم التعاون القضائي بين الدول، ومع ذلك ونظراً للاتساع المتزايد للأنشطة الالكترونية العابرة للحدود، فإن الحاجة إلى تعديل المادة (١٣) باتت ضرورية، بحيث تشمل الجرائم الالكترونية ضمن نطاق الاختصاص الشامل، مما يتيح للقضاء العراقي ملاحقة مرتكبي هذه الجرائم على نطاق أوسع وأكثر فعالية (صالح & نوذري، ٢٠٢٥، ص ١٨).

يلاحظ ان قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل لم يشر صراحةً للجرائم الالكترونية ولكم عالج على سبيل المثال جريمة الابتزاز المالي ضمن المادة (٤٥٢) والمتضمنة: (١- يعاقب بالسجن مدة لا تزيد على سبع سنين او الحبس من حمل اخر بطريق التهديد على تسليم نقود او أشياء أخرى غير ما ذكر في المادة السابقة. ٢- وتكون العقوبة مدة لاتزيد على عشر سنين إذا ارتكبت الجريمة بالقوة او الاكراه) (قانون العقوبات العراقي، ١٩٦٩، المادة ٤٥٢).

وتناول المشرّع العراقي جريمة التهديد ضمن أحكام المواد (٤٣٠-٤٣٢) من قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل، ولكن لم يُفرد نص خاص صريح لجريمة الابتزاز، بل أوردها ضمنياً من خلال تنظيمه لحالة التهديد المقترن بطلب، كما ورد في المادة (٤٣٠) تحديداً، وباستقراء نص المادة المذكورة، يتضح أن المشرّع عمد إلى استخدام عبارات عامة وفضفاضة عند تجريم فعل التهديد، سواء وقع مجرداً أو كان مقترناً بطلب، إذ نصّت الفقرة الأولى من المادة

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

(٤٣٠) على أن: "كل من هدد آخر..."، دون أن تحدد وسيلة التهديد بشكل حصري أو مقيد، وهذا الإطلاق في الصياغة يفيد القابلية للتطبيق على مختلف الوسائل، التقليدية منها أو الحديثة، ما دام القصد الإجرامي متحققاً والأثر الإجرامي قائماً.

ومن ثم، فإن التهديد المقترن بطلب وهو الصورة التي تقوم عليها جريمة الابتزاز يمكن أن يقع باستخدام الوسائل الإلكترونية الحديثة، كالبريد الإلكتروني، أو تطبيقات المراسلة، أو غرف الدردشة، بل وحتى عبر منصات التواصل الاجتماعي، مستندين في ذلك إلى شمولية النص وعموميته المطلقة، التي تجري على إطلاقها ما لم يُقيّدها نص خاص (الدراجي، ٢٠٢٠، ص ٨٠).

وحدد قانون العقوبات العراقي عقوبة السجن المؤبد أو المؤقت لمجموعة أفعال ممكن أن تكون ضمن الجرائم الالكترونية العابرة للحدود التي تحدث (تخريب او اتلاف او تعطيل القواعد والمنشآت العسكرية او المصالح.. او الأسلحة او العتاد او المؤن او الأدوية والمواد الحربية وغير ذلك مما أعد لاستعمال القوات المسلحة او الدفاع عن العراق او مما يستعمل في ذلك) (قانون العقوبات العراقي، ١٩٦٩، المادة ١٦٣).

كما حدد عقوبة السجن مدة لا تزيد عن سبع سنوات أو الحبس كل (من أحدث كسر او تلف او نحو ذلك في الآلات او الأنابيب او الأجهزة الخاصة بمرفق المياه او الكهرباء او الغاز او غيرها من المرافق العامة) (قانون العقوبات العراقي، ١٩٦٩، المادة ١/٣٥٣).

وكذلك لمن يعطّل عمداً (سير وسيلة من وسائل النقل العام البرية او المائية او الجوية) قانون العقوبات العراقي. (١٩٦٩، المادة ٣٥٨) أو (وسيلة من وسائل الاتصال السلكية او اللاسلكية المخصصة لمنفعة عامة او قطع او اتلف شيئاً من اسلاكها او اجهزتها او حال عمدا دون اصالحها) (قانون العقوبات العراقي، ١٩٦٩، المادة ٣٦١).

أما إذا نُفذت الجرائم الالكترونية العابرة للحدود لتحقيق اهداف ارهابية كإدخال الرعب أو الخوف والفزع بين الناس أو إثارة الفوضى وزعزعة الاستقرار السياسي أو إلحاق أضرار جسيمة، فتُعد أعمالاً إرهابية وتطبق بشأنها القوانين المتعلقة بمكافحة الإرهاب ، حيث حدد قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥ الأفعال الإرهابية التي يمكن أن تقع من خلال الجرائم الالكترونية العابرة للحدود كالعنف الذي يهدف إلى إلقاء الرعب بين الناس أو تعريض حياة الناس وحرياتهم وأمنهم للخطر، وكذلك افعال التخريب أو الهدم أو الإتلاف أو الإضرار العمدي للمباني أو الأملاك العامة أو المصالح الحكومية والمرافق العامة أو القطاع الخاص.. بباعث زعزعة الأمن والاستقرار (قانون مكافحة الإرهاب العراقي، ٢٠٠٥، المادة ٢)

يُعد العراق من الدول التي واجهت تحديات الجرائم الإلكترونية، حيث أعدت الحكومة العراقية مشروع قانون للجرائم المعلوماتية يتكون من (٣١) مادة موزعة على أربعة فصول تتناول التعاريف والأهداف والعقوبات وإجراءات جمع الأدلة والتحقيق والمحاكمة، وتم تقديم هذا المشروع إلى مجلس النواب عام ٢٠١١ وقُرِء قراءة أولى، ولكنه لا يزال قيد التشريع حتى الآن

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

رغم الحاجة الملحّة إليه في ظل التطورات الرقمية المتسارعة (صالح & حسين، ٢٠٢٢، ص ١١)

وقد أوضح المشرّع العراقي اهدافاً أساسية للمشروع ، حيث يسعى إلى توفير الحماية القانونية اللازمة للاستعمال المشروع للحواسيب وشبكات الإنترنت، وفرض العقوبات بحق مرتكبي الأفعال غير المشروعة التي تشكّل اعتداءً على حقوق المستخدمين، سواء كانوا أشخاصاً طبيعيين أو معنويين، كما يعمل القانون على الحدّ من إساءة استعمال تقنيات حديثة في ارتكاب الجرائم الالكترونية ، لا سيما تلك المرتبطة بسرقة البيانات، اختراق الأنظمة المصرفية، التطفل الإلكتروني، الابتزاز، التنصت غير القانوني على الاتصالات، والترويج غير المشروع للمخدرات.

ونص المشروع على الإجراءات الواجب اتباعها في حال وقوع جريمة معلوماتية، حيث خُصص الفصل الثالث لمعالجة هذه الجوانب تحت عنوان "إجراءات جمع الأدلة والتحقيق والمحاكمة ."كما جاءت المادة (٢٤) لتحدد الجهات المختصة بالنظر في هذه الجرائم، حيث منح المشرّع العراقي لقاضي التحقيق أو المحقق المختص سلطة مباشرة إجراءات الضبط وجمع الأدلة وفقاً لأحكام قانون أصول المحاكمات الجزائية، أما المادة (٢٥/البند أولاً) من المشروع فقد نصّت على اختصاص محكمة جنح أو جنايات الرصافة بالنظر في الجرائم المعلوماتية المنصوص عليها في هذا القانون، وذلك لمدة ثلاث سنوات من تاريخ نفاذه، مع استمرار هذه المحكمة في نظر القضايا ذات الصلة حتى صدور الأحكام القطعية واكتسابها درجة البتّات، إضافة إلى ذلك أكّد المشروع على ضرورة أن يكون القاضي الذي ينظر في الجرائم المعلوماتية ممن يتمتعون بالخبرة والتخصص في الجرائم الالكترونية ، مع تلقيهم التدريبات اللازمة لضمان دقة الفصل في القضايا المتعلقة بالجرائم السيبرانية. (مجلس النواب العراقي، ٢٠١١)

وهذا ان دل على شيء انما يدل على إن المشرّع العراقي قد احسن بالإحاطة ببعض الجوانب الاجرائية للجريمة الالكترونية كتحديد الجهة القضائية المختصة للنظر في هذه الجرائم، كما نرى إن المادة (٢٤) في بندها الثاني قد اشارت إلى عدم جواز المباشرة بإجراءات التفتيش الا بأمر من القاضي المختص، وهذه إشارة واضحة للتأكيد على مبدأ الشرعية الاجرائية في اطار الاجراءات الجنائية، كما انها إشارة على حماية الحياة الخاصة التي اكد الدستور العراقي لسنة ٢٠٠٥ عليها في المادة (١٧) منه، بالإضافة إلى إنه فوض للقاضي الاستعانة بالخبرة الفنية لتجاوز بعض الصعوبات التي قد يواجهها القاضي المختص في مرحلتي التحقيق والمحاكمة.

لقد أفرز التطور الرقمي مصطلحات جديدة لم تكن القوانين التقليدية قادرة على استيعابها، مثل: الحواسيب، المعالجة الآلية للبيانات، بيانات الحاسوب، البرامج الإلكترونية، جهات تزويد الخدمات المعلوماتية، بيانات المرور، بيانات الاشتراك، البطاقات الإلكترونية، شبكات المعلومات، التوقيع الإلكتروني، الوسائل الرقمية، المحررات الإلكترونية، نظام معالجة المعلومات، شهادات التصديق الإلكتروني، الإرهاب المعلوماتي، تهكير المواقع الرسمية، اختراق الحواسيب الشخصية، إساءة استخدام البطاقات الائتمانية، اعتراض المعلومات،

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

والتلاعب بالبيانات الرقمية، الأمر الذي يدلل على اهمية تبنّي تشريعات تواكب تلك التطورات ولا تسمح بإفلات مرتكبي الجرائم الالكترونية العابرة للحدود من العقاب وتسمهم في إنصاف الضحايا وتحقيق العدالة وحماية الدول لسيدتها.
وفي إطار المساعي العربية لمواجهة التحديات المستجدة في ميدان الجريمة الالكترونية ، بذلت البلدان العربية جهوداً حثيثة لمواكبة التطورات التقنية المتسارعة، وذلك من خلال تبني تشريعات متخصصة ترمي إلى تجريم الأفعال المستحدثة في مجال تقنية المعلومات، وقد تُوّجت هذه الجهود الجماعية بإصدار **القانون العربي النموذجي الموحد لمكافحة جرائم تقنية المعلومات لسنة ٢٠٠٣**، الذي يُعد خطوة تشريعية رائدة تهدف إلى توحيد الرؤى القانونية بين الدول العربية في مواجهة هذه الجرائم العابرة للحدود، وفي السياق ذاته أناط المشرّع المصري على وجه الحصر **بالجهاز القومي لتنظيم الاتصالات** مهمة الإشراف والرقابة على قطاع الاتصالات، انطلاقاً من دوره المحوري في تنظيم هذا القطاع وضمان حسن استخدامه، باعتبار هذا الجهاز كياناً حكومياً يتبع وزارة الاتصالات وتكنولوجيا المعلومات، صلاحيات واسعة تهدف إلى حماية حقوق المستخدمين وتعزيز أمن المعلومات وضبط أداء مزوّدي الخدمات في ظل ما يشهده العصر الرقمي من تطورات متلاحقة (السلامي، ٢٠٢٣).

وأدرك المشرّع الكويتي مبكراً خطورة الجرائم الإلكترونية وما تحمله من تهديد مباشر للخصوصية والأمن المجتمعي، لا سيما في ظل التوسع المطّرد في استخدام الشبكة الدولية للمعلومات في مختلف مناحي الحياة، وما رافقه من إساءة الاستعمال من قِبل بعض الأفراد ممّن استغلوا هذه الوسائل التقنية للإضرار بالغير والاعتداء على حقوقهم. وإزاء ذلك، صدر **قانون مكافحة جرائم تقنية المعلومات رقم (٦٣) لسنة ٢٠١٥**، بوصفه استجابة تشريعية لما أفرزته البيئة الرقمية من مظاهر إجرامية مستحدثة ووسيلة لضبط السلوك الإنساني في الفضاء السيبراني، لتحقيق التوازن بين حرية الاستخدام ومتطلبات الحماية القانونية، وتضمن هذا القانون نصوصاً جزائية واضحة تتناول الأفعال المجرّمة والعقوبات المقررة بحق مرتكبيها ومن بين هذه النصوص ما ورد في الفقرة (٤) من المادة **(٣)** التي جاء فيها "يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تتجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: استعمل الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه" (الدراجي، ٢٠٢٠، ص ٩٨).

ويُستشف من هذا النص أن المشرّع الكويتي قد تبنّى نهجاً يوازن بين الحزم والمرونة، إذ **حدد سقف العقوبة السالبة للحرية دون أن يُقيد القاضي بحد أدنى،** مما يمنحه هامشًا تقديريًا لتقدير الجزاء الأنسب بحسب ظروف كل واقعة وملابساتها. وهذا التوجه يعكس فلسفة تشريعية رشيدة تهدف إلى **تحقيق الردع الخاص والعام دون الوقوع في غلو العقوبة أو جمود النص،** وهو ما

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

يُجسد أحد أوجه التكيف التشريعي مع طبيعة الجريمة الإلكترونية كجريمة متجددة ومتعددة الأشكال.

وتناول المشرع الفرنسي جريمة الابتزاز الإلكتروني ضمن نطاق المادة (٣١٢) من قانون العقوبات الفرنسي رقم ٩٢-٦٨٣ الصادر بتاريخ ٢٢ يوليو/تموز ١٩٩٢، حيث فصّل صور هذه الجريمة وميّز بينها على نحو يعكس دقة تشريعية في تقدير خطورة الفعل الإجرامي باختلاف وسائله وآثاره، وقد وردت أحكام الابتزاز في الفقرات (١- ١٢) ، فجاء النص مبيّناً صورتين رئيستين للابتزاز: أحدهما يتأسس على التهديد بالإيذاء المادي، والثاني يقوم على التهديد بالإيذاء المعنوي المرتبط بالشرف والاعتبار، ففي الفقرة الأولى، نص المشرع على ما يلي: "إن الابتزاز هو الحصول عن طريق التهديد بالعنف أو الإكراه على توقيع التزام أو تنازل أو كشف عن سر أو تسليم أموال أو قيم أو على أي ممتلكات أخرى، ويعاقب على الابتزاز السجن بسبع سنين وغرامة قدرها ١٠٠ الف يورو، أما في الفقرة العاشرة، فقد ورد النص الآتي: "الابتزاز هو الحصول عن طريق التهديد بكشف أو ادعاء وقائع من شأنها أن تضر بالشرف أو السمعة أو الاعتبار على توقيع أو تعهد أو تنازل أو كشف عن سر أو تحويل مال أو اوراقاً مالية أو أي سلعاً أخرى، ويعاقب على الابتزاز بالسجن خمس سنوات وغرامة قدرها ٧٥ ألف يورو".

يتبيّن من هذا التدرج في العقوبة أن المشرع الفرنسي قد أقام تمييزاً دقيقاً بين صور الابتزاز وفقاً لدرجة جسامة التهديد، فشدد العقوبة في حالة الابتزاز القائم على الإكراه الجسدي أو العنف المادي، إذ اعتبره أشد خطراً وأبلغ أثراً في تقييد إرادة الضحية، فعاقب مرتكبه بالسجن لمدة سبع سنوات وغرامة مقدارها مئة ألف يورو، أما إذا كان التهديد ذا طبيعة معنوية تمس السمعة أو الشرف أو الاعتبار، فقد قُدِّرت خطورته بدرجة أدنى، فجاءت العقوبة أخف: خمس سنوات سجن وغرامة قدرها خمسة وسبعون ألف يورو (المعموري & عجيل، ٢٠١٧، ص ٢٧٥).

المطلب الثاني آثار المسؤولية عن الجرائم الالكترونية العابرة للحدود

تُعتبر الجرائم الإلكترونية العابرة للحدود من أبرز التحديات القانونية في العصر الحديث، نظراً لطبيعتها المعقدة التي تتجاوز الحدود الجغرافية والسياسية للدول، وتداخلها مع مظاهر السيادة الوطنية والتعاون الدولي، تؤثر هذه الجرائم بشكل مباشر على الأفراد والمجتمعات والدول، سواء من خلال المساس بالأمن السيبراني أو الإضرار بالمصالح الاقتصادية والاجتماعية، مما يفرض ضرورة التطرق إلى آثار المسؤولية القانونية المترتبة على مرتكبيها.
في هذا السياق، يتناول المطلب الثاني من هذا البحث آثار مسؤولية الأفراد عن الجرائم الإلكترونية العابرة للحدود، من خلال فرعين أساسيين يسلطان الضوء على الجانبين الجزائي والمدني لهذه المسؤولية:

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

الفرع الاول المساءلة الجزائية للأفراد عن الجرائم الإلكترونية العابرة للحدود

ان المسؤولية الجزائية هي "عبارة عن الالتزام بتحمل الجزاء الذي ترتبه القواعد القانونية كأثر للفعل الذي يرتكب خروجاً على أحكامها " (حنش، ٢٠٢٠، ص ١١).وفي ظل مبدأ الشرعية (مبدأ لا جريمة ولا عقوبة إلا بنص)، تواجه الأجهزة القضائية تحدياً ليس يسيراً في تحديد النصوص العقابية اللازمة لمعاقبة مرتكبي الانتهاكات السيبرانية، خاصة عند عدم وجود تشريعات تعالج تلك الانتهاكات بشكل صريح وواضح، ليتم اللجوء حينها إلى القواعد العامة لتطبيقها على مرتكبي تلك الانتهاكات على نحو لا يسمح لهم بالإفلات من العقاب، ويمكن الوقوف على آثار المسؤولية عن الجرائم الالكترونية العابرة للحدود من خلال احكام القوانين الجزائية الوطنية أو من خلال القانون الجنائي الدولي.

أولاً/ القوانين الجنائية الوطنية: يتوافق التشريع العراقي مع الاتفاقيات الدولية في اعتماد مبدأ الاختصاص الإقليمي كأحد الضوابط الأساسية لتحديد ولاية القضاء الجنائي، وذلك وفقاً لأحكام المادة (٦) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل، والتي تقر بأن جميع الجرائم المرتكبة داخل العراق تخضع لولاية القضاء الوطني بغض النظر عن جنسية أو صفة مرتكبها، كما يعتبر الفعل الجرمي واقعاً في العراق إذا وقع فيه أحد العناصر المكونة له، أو تحققت نتيجته، أو كان مقصوداً أن تتحقق داخله، وهو ما يكفل للدولة السيطرة القانونية الكاملة على الجرائم ذات الطابع الإقليمي، وإلى جانب ذلك يمتد نطاق الاختصاص الإقليمي ليشمل جميع أراضي جمهورية العراق، بما فيها المياه الإقليمية والفضاء الجوي التابع لها، مما يضمن شمولية التطبيق القضائي للجرائم الالكترونية الواقعة ضمن هذه الحدود، وقد تبنّى المشرّع العراقي أيضاً مبدأ الاختصاص العيني بموجب المادة (٩) بإخضاع الجرائم التي تمس أمن الدولة الداخلي والخارجي لولاية القضاء العراقي بغض النظر عن مكان وقوعها أو جنسية مرتكبها، كما أخذ بالاختصاص الشخصي في المادة (١٠)، حيث يُخضع القانون العراقي أي مواطن عراقي ارتكب جريمة خارج البلاد للمساءلة وفق أحكامه، بشرط أن يكون الفعل معاقباً عليه بموجب قانون الدولة التي وقع فيها، وأن يكون الجاني موجوداً داخل العراق.

أما فيما يتعلق بالاختصاص الشامل، فقد تم تكريسه بموجب المادة (١٣) من قانون العقوبات، حيث تخضع لولاية القضاء العراقي كل شخصية تُضبط داخل الدولة بعد ارتكابها خارج البلاد جرائم تمس الأمن الدولي، مثل تخريب أو تعطيل وسائل الاتصالات والمواصلات الدولية، أو الاتجار بالبشر والرقيق والمخدرات.

يتمتع القضاء العراقي بولاية قضائية كاملة لملاحقة مرتكبي الجرائم الالكترونية داخل البلاد، بغض النظر عن جنسيتهم أو موقع الجريمة، مستنداً إلى التشريعات الوطنية والاتفاقيات الدولية التي تنظم التعاون القضائي بين الدول، ومع ذلك ونظراً للاتساع المتزايد للأنشطة الالكترونية العابرة للحدود، فإن الحاجة إلى تعديل المادة (١٣) باتت ضرورية، بحيث تشمل الجرائم الالكترونية ضمن نطاق الاختصاص الشامل، مما يتيح للقضاء العراقي ملاحقة مرتكبي هذه الجرائم على نطاق أوسع وأكثر فعالية (صالح & نوذري، ٢٠٢٥، ص ١٨).

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

يلاحظ ان قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل لم يشر صراحةً للجرائم الالكترونية ولكم عالج على سبيل المثال جريمة الابتزاز المالي ضمن المادة (٤٥٢) والمتضمنة: (١- يعاقب بالسجن مدة لا تزيد على سبع سنين او الحبس من حمل اخر بطريق التهديد على تسليم نقود او أشياء أخرى غير ما ذكر في المادة السابقة. ٢- وتكون العقوبة مدة لاتزيد على عشر سنين إذا ارتكبت الجريمة بالقوة او الاكراه) (قانون العقوبات العراقي، ١٩٦٩، المادة ٤٥٢).

وتناول المشرّع العراقي جريمة التهديد ضمن أحكام المواد (٤٣٠-٤٣٢) من قانون العقوبات رقم ١١١ لسنة ١٩٦٩ المعدل، ولكن لم يُفرد نص خاص صريح لجريمة الابتزاز، بل أوردها ضمنياً من خلال تنظيمه لحالة التهديد المقترن بطلب، كما ورد في المادة (٤٣٠) تحديداً، وباستقراء نص المادة المذكورة، يتضح أن المشرّع عمد إلى استخدام عبارات عامة وفضفاضة عند تجريم فعل التهديد، سواء وقع مجرداً أو كان مقترناً بطلب، إذ نصّت الفقرة الأولى من المادة (٤٣٠) على أن: "كل من هدد آخر..."، دون أن تحدد وسيلة التهديد بشكل حصري أو مقيد، وهذا الإطلاق في الصياغة يفيد القابلية للتطبيق على مختلف الوسائل، التقليدية منها أو الحديثة، ما دام القصد الإجرامي متحققاً والأثر الإجرامي قائماً.

ومن ثم، فإن التهديد المقترن بطلب وهو الصورة التي تقوم عليها جريمة الابتزاز يمكن أن يقع باستخدام الوسائل الإلكترونية الحديثة، كالبريد الإلكتروني، أو تطبيقات المراسلة، أو غرف الدردشة، بل وحتى عبر منصات التواصل الاجتماعي، مستندين في ذلك إلى شمولية النص وعموميته المطلقة، التي تجري على إطلاقها ما لم يُقيّدها نص خاص (الدراجي، ٢٠٢٠، ص ٨٠).

وحدد قانون العقوبات العراقي عقوبة السجن المؤبد أو المؤقت لمجموعة أفعال ممكن أن تكون ضمن الجرائم الالكترونية العابرة للحدود التي تحدث (تخريب او اتلاف او تعطيل القواعد والمنشآت العسكرية او المصالح.. او الأسلحة او العتاد او المؤن او الأدوية والمواد الحربية وغير ذلك مما أعد لاستعمال القوات المسلحة او الدفاع عن العراق او مما يستعمل في ذلك) (قانون العقوبات العراقي، ١٩٦٩، المادة ١٦٣).

كما حدد عقوبة السجن مدة لا تزيد عن سبع سنوات أو الحبس كل (من أحدث كسر او تلف او نحو ذلك في الآلات او الأنابيب او الأجهزة الخاصة بمرفق المياه او الكهرباء او الغاز او غيرها من المرافق العامة) (قانون العقوبات العراقي، ١٩٦٩، المادة ١/٣٥٣).

وكذلك لمن يعطّل عمداً (سير وسيلة من وسائل النقل العام البرية او المائية او الجوية) قانون العقوبات العراقي. (١٩٦٩، المادة ٣٥٨) أو (وسيلة من وسائل الاتصال السلكية او اللاسلكية المخصصة لمنفعة عامة او قطع او اتلف شيئاً من اسلاكها او اجهزتها او حال عمدا دون اصالحها) (قانون العقوبات العراقي، ١٩٦٩، المادة ٣٦١).

أما إذا نُفذت الجرائم الالكترونية العابرة للحدود لتحقيق اهداف ارهابية كإدخال الرعب أو الخوف والفزع بين الناس أو إثارة الفوضى وزعزعة الاستقرار السياسي أو إلحاق أضرار

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

جسيمة، فتُعد أعمالاً إرهابية وتطبق بشأنها القوانين المتعلقة بمكافحة الإرهاب ، حيث حدد قانون مكافحة الإرهاب العراقي رقم (١٣) لسنة ٢٠٠٥ الأفعال الإرهابية التي يمكن أن تقع من خلال الجرائم الالكترونية العابرة للحدود كالعنف الذي يهدف إلى إلقاء الرعب بين الناس أو تعريض حياة الناس وحرياتهم وأمنهم للخطر، وكذلك افعال التخريب أو الهدم أو الإتلاف أو الإضرار العمدي للمباني أو الأملاك العامة أو المصالح الحكومية والمرافق العامة أو القطاع الخاص.. بباعث زعزعة الأمن والاستقرار (قانون مكافحة الإرهاب العراقي، ٢٠٠٥، المادة ٢)

يُعد العراق من الدول التي واجهت تحديات الجرائم الإلكترونية، حيث أعدت الحكومة العراقية مشروع قانون للجرائم المعلوماتية يتكون من (٣١) مادة موزعة على أربعة فصول تتناول التعاريف والأهداف والعقوبات وإجراءات جمع الأدلة والتحقيق والمحاكمة، وتم تقديم هذا المشروع إلى مجلس النواب عام ٢٠١١ وقُرِء قراءة أولى، ولكنه لا يزال قيد التشريع حتى الآن رغم الحاجة الملحّة إليه في ظل التطورات الرقمية المتسارعة (صالح & حسين، ٢٠٢٢، ص ١١)

وقد أوضح المشرّع العراقي اهدافاً أساسية للمشروع ، حيث يسعى إلى توفير الحماية القانونية اللازمة للاستعمال المشروع للحواسيب وشبكات الإنترنت، وفرض العقوبات بحق مرتكبي الأفعال غير المشروعة التي تشكّل اعتداءً على حقوق المستخدمين، سواء كانوا أشخاصاً طبيعيين أو معنويين، كما يعمل القانون على الحدّ من إساءة استعمال تقنيات حديثة في ارتكاب الجرائم الالكترونية ، لا سيما تلك المرتبطة بسرقة البيانات، اختراق الأنظمة المصرفية، التطفل الإلكتروني، الابتزاز، التنصت غير القانوني على الاتصالات، والترويج غير المشروع للمخدرات.

ونص المشروع على الإجراءات الواجب اتباعها في حال وقوع جريمة معلوماتية، حيث خُصص الفصل الثالث لمعالجة هذه الجوانب تحت عنوان "إجراءات جمع الأدلة والتحقيق والمحاكمة ."كما جاءت المادة (٢٤) لتحدد الجهات المختصة بالنظر في هذه الجرائم، حيث منح المشرّع العراقي لقاضي التحقيق أو المحقق المختص سلطة مباشرة إجراءات الضبط وجمع الأدلة وفقاً لأحكام قانون أصول المحاكمات الجزائية، أما المادة (٢٥/البند أولاً) من المشروع فقد نصّت على اختصاص محكمة جنح أو جنايات الرصافة بالنظر في الجرائم المعلوماتية المنصوص عليها في هذا القانون، وذلك لمدة ثلاث سنوات من تاريخ نفاذه، مع استمرار هذه المحكمة في نظر القضايا ذات الصلة حتى صدور الأحكام القطعية واكتسابها درجة البتّات، إضافة إلى ذلك أكّد المشروع على ضرورة أن يكون القاضي الذي ينظر في الجرائم المعلوماتية ممن يتمتعون بالخبرة والتخصص في الجرائم الالكترونية ، مع تلقيهم التدريبات اللازمة لضمان دقة الفصل في القضايا المتعلقة بالجرائم السيبرانية. (مجلس النواب العراقي، ٢٠١١)

وهذا ان دل على شيء انما يدل على إن المشرّع العراقي قد احسن بالإحاطة ببعض الجوانب الاجرائية للجريمة الالكترونية كتحديد الجهة القضائية المختصة للنظر في هذه الجرائم، كما نرى إن المادة (٢٤) في بندها الثاني قد اشارت إلى عدم جواز المباشرة بإجراءات التفتيش الا بأمر

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

من القاضي المختص، وهذه إشارة واضحة للتأكيد على مبدأ الشرعية الاجرائية في اطار الاجراءات الجنائية، كما انها إشارة على حماية الحياة الخاصة التي اكد الدستور العراقي لسنة ٢٠٠٥ عليها في المادة (١٧) منه، بالإضافة إلى إنه فوض للقاضي الاستعانة بالخبرة الفنية لتجاوز بعض الصعوبات التي قد يواجهها القاضي المختص في مرحلتي التحقيق والمحاكمة.

لقد أفرز التطور الرقمي مصطلحات جديدة لم تكن القوانين التقليدية قادرة على استيعابها، مثل: الحواسيب، المعالجة الآلية للبيانات، بيانات الحاسوب، البرامج الإلكترونية، جهات تزويد الخدمات المعلوماتية، بيانات المرور، بيانات الاشتراك، البطاقات الإلكترونية، شبكات المعلومات، التوقيع الإلكتروني، الوسائل الرقمية، المحررات الإلكترونية، نظام معالجة المعلومات، شهادات التصديق الإلكتروني، الإرهاب المعلوماتي، تهكير المواقع الرسمية، اختراق الحواسيب الشخصية، إساءة استخدام البطاقات الائتمانية، اعتراض المعلومات، والتلاعب بالبيانات الرقمية، الأمر الذي يدلل على اهمية تبنّي تشريعات تواكب تلك التطورات ولا تسمح بإفلات مرتكبي الجرائم الالكترونية العابرة للحدود من العقاب وتسمهم في إنصاف الضحايا وتحقيق العدالة وحماية الدول لسيدتها.

وفي إطار المساعي العربية لمواجهة التحديات المستجدة في ميدان الجريمة الالكترونية ، بذلت البلدان العربية جهوداً حثيثة لمواكبة التطورات التقنية المتسارعة، وذلك من خلال تبني تشريعات متخصصة ترمي إلى تجريم الأفعال المستحدثة في مجال تقنية المعلومات، وقد تُوّجت هذه الجهود الجماعية بإصدار **القانون العربي النموذجي الموحد لمكافحة جرائم تقنية المعلومات لسنة ٢٠٠٣**، الذي يُعد خطوة تشريعية رائدة تهدف إلى توحيد الرؤى القانونية بين الدول العربية في مواجهة هذه الجرائم العابرة للحدود، وفي السياق ذاته أناط المشرّع المصري على وجه الحصر **بالجهاز القومي لتنظيم الاتصالات** مهمة الإشراف والرقابة على قطاع الاتصالات، انطلاقاً من دوره المحوري في تنظيم هذا القطاع وضمان حسن استخدامه، باعتبار هذا الجهاز كياناً حكومياً يتبع وزارة الاتصالات وتكنولوجيا المعلومات، صلاحيات واسعة تهدف إلى حماية حقوق المستخدمين وتعزيز أمن المعلومات وضبط أداء مزوّدي الخدمات في ظل ما يشهده العصر الرقمي من تطورات متلاحقة (السلامي، ٢٠٢٣).

وأدرك المشرّع الكويتي مبكراً خطورة الجرائم الإلكترونية وما تحمله من تهديد مباشر للخصوصية والأمن المجتمعي، لا سيما في ظل التوسع المطّرد في استخدام الشبكة الدولية للمعلومات في مختلف مناحي الحياة، وما رافقه من إساءة الاستعمال من قِبل بعض الأفراد ممّن استغلوا هذه الوسائل التقنية للإضرار بالغير والاعتداء على حقوقهم. وإزاء ذلك، صدر **قانون مكافحة جرائم تقنية المعلومات رقم (٦٣) لسنة ٢٠١٥**، بوصفه استجابة تشريعية لما أفرزته البيئة الرقمية من مظاهر إجرامية مستحدثة ووسيلة لضبط السلوك الإنساني في الفضاء السيبراني، لتحقيق التوازن بين حرية الاستخدام ومتطلبات الحماية القانونية، وتضمن هذا القانون نصوصاً جزائية واضحة تتناول الأفعال المجرّمة والعقوبات المقررة بحق مرتكبيها ومن

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

بين هذه النصوص ما ورد في الفقرة (٤) من المادة **(٣)** التي جاء فيها "يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تتجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: استعمل الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه" (الدراجي، ٢٠٢٠، ص ٩٨).

ويُستشف من هذا النص أن المشرّع الكويتي قد تبنّى نهجاً يوازن بين الحزم والمرونة، إذ **حدد سقف العقوبة السالبة للحرية دون أن يُقيد القاضي بحد أدنى،** مما يمنحه هامشًا تقديريًا لتقدير الجزاء الأنسب بحسب ظروف كل واقعة وملابساتها. وهذا التوجه يعكس فلسفة تشريعية رشيدة تهدف إلى **تحقيق الردع الخاص والعام دون الوقوع في غلو العقوبة أو جمود النص،** وهو ما يُجسد أحد أوجه التكيف التشريعي مع طبيعة الجريمة الإلكترونية كجريمة متجددة ومتعددة الأشكال.

وتناول المشرع الفرنسي جريمة الابتزاز الإلكتروني ضمن نطاق المادة (٣١٢) من قانون العقوبات الفرنسي رقم ٩٢-٦٨٣ الصادر بتاريخ ٢٢ يوليو/تموز ١٩٩٢، حيث فصّل صور هذه الجريمة وميّز بينها على نحو يعكس دقة تشريعية في تقدير خطورة الفعل الإجرامي باختلاف وسائله وآثاره، وقد وردت أحكام الابتزاز في الفقرات (١- ١٢) ، فجاء النص مبيّناً صورتين رئيستين للابتزاز: أحدهما يتأسس على التهديد بالإيذاء المادي، والثاني يقوم على التهديد بالإيذاء المعنوي المرتبط بالشرف والاعتبار، ففي الفقرة الأولى، نص المشرع على ما يلي: "إن الابتزاز هو الحصول عن طريق التهديد بالعنف أو الإكراه على توقيع التزام أو تنازل أو كشف عن سر أو تسليم أموال أو قيم أو على أي ممتلكات أخرى، ويعاقب على الابتزاز السجن بسبع سنين وغرامة قدرها ١٠٠ الف يورو، أما في الفقرة العاشرة، فقد ورد النص الآتي: "الابتزاز هو الحصول عن طريق التهديد بكشف أو ادعاء وقائع من شأنها أن تضر بالشرف أو السمعة أو الاعتبار على توقيع أو تعهد أو تنازل أو كشف عن سر أو تحويل مال أو اوراقاً مالية أو أي سلعاً أخرى، ويعاقب على الابتزاز بالسجن خمس سنوات وغرامة قدرها ٧٥ ألف يورو".

يتبيّن من هذا التدرج في العقوبة أن المشرع الفرنسي قد أقام تمييزاً دقيقاً بين صور الابتزاز وفقاً لدرجة جسامة التهديد، فشدد العقوبة في حالة الابتزاز القائم على الإكراه الجسدي أو العنف المادي، إذ اعتبره أشد خطراً وأبلغ أثراً في تقييد إرادة الضحية، فعاقب مرتكبه بالسجن لمدة سبع سنوات وغرامة مقدارها مئة ألف يورو، أما إذا كان التهديد ذا طبيعة معنوية تمس السمعة أو الشرف أو الاعتبار، فقد قُدِّرت خطورته بدرجة أدنى، فجاءت العقوبة أخف: خمس سنوات سجن وغرامة قدرها خمسة وسبعون ألف يورو (المعموري & عجيل، ٢٠١٧، ص ٢٧٥).

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

أولاً/ الاستنتاجات

١. تعد الجرائم الالكترونية العابرة للحدود ضمن الجرائم العالمية التي تمتد تأثيراتها عبر حدود دولتين أو أكثر، كما يمكن أن تكون جرائم دولية وفقاً للمادة (٣٦) من البروتوكول الإضافي الأول (١٩٧٧)، المتضمنة نصاً عاماً يشمل أي أساليب أو وسائل قتال يمكن اكتشافها في المستقبل، لتكون محكومة بقواعد القانون الدولي الانساني خلال النزاعات المسلحة. وبالتالي يمكن تكييف الانتهاكات السيبرانية لسيادة الدول ضمن الجرائم الدولية وفقاً لتحقق أركان الجريمة الدولية (جريمة حرب أو عدوان أو ضد الانسانية أو إبادة جماعية) في السلوك غير المشروع للانتهاكات السيبرانية، لتكون مسؤولية الجناة متحققة بمحاسبتهم وفقاً لأحكام القضاء الجزائي الدولي.
٢. تشكّل الجرائم الإلكترونية العابرة للحدود تهديداً مباشراً للسيادة الوطنية، وتُحدث فراغاً قانونياً في منظومة القانون الدولي الجنائي التقليدي، حيث يتطلب الأمر النص صراحةً عليها في نظام روما الاساسي لعام ١٩٩٨.
٣. غياب الإقليم المحدد والهوية المعروفة للجناة يجعل من تطبيق قواعد المسؤولية الجنائية الدولية أمراً بالغ التعقيد، مما يوجب وضع قواعد اجرائية تتلاءم مع طبيعتها.
٤. تعاني المنظومة القانونية من قصور في أدوات الإثبات والتحقيق الرقمي، ما يحدّ من فاعلية مساءلة الفاعلين الرقميين، الأمر الذي يتطلب معالجتها صراحةً في التشريعات الوطنية ونظام روما الاساسي لعام ١٩٩٨.
٥. الاتفاقيات الدولية الحالية تشكّل بداية جيدة، لكنها لا تغني عن الحاجة إلى ميثاق دولي موحد لمكافحة الجريمة السيبرانية.
٦. يتطلب إسناد الجريمة الإلكترونية إلى دولة أو فرد إثبات الركنين المادي والمعنوي في بيئة رقمية لا تعترف بالحدود، وهو تحدٍّ يتطلب تطوير أدوات قانونية وتقنية جديدة.
٧. تنوع صور الجريمة، من الاحتيال إلى الإرهاب السيبراني، يُحتّم تعددية المقاربات القانونية وعدم الاكتفاء بالتجريم المحلي.
٨. اصبح لازماً في الوقت الحالي توسيع مفهوم السيادة ليشمل الفضاء السيبراني لضمان الحماية القانونية للدول والمجتمعات.
٩. يجب الانتقال من النظرة الضيقة للاختصاص الجنائي إلى نظرة شاملة تأخذ بعين الاعتبار مكان الفعل، والنتيجة، والمصلحة المعتدى عليها، وهو ما يجب ان يلتفت اليه المشرع الوطني والدولي الجنائي.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

ثانياً/ التوصيات

١. ضرورة معالجة الجرائم الإلكترونية العابرة للحدود بشكل صريح في التشريعات الوطنية ونظام روما الاساسي لعام ١٩٩٨، فالقانون الدولي التقليدي غير كافٍ لوحده لضبط الجرائم الإلكترونية الحديثة، ويحتاج إلى تطوير مفاهيمي وإجرائي.

٢. رغم وجود اتفاقيات كاتفاقية بودابست واتفاقية الأمم المتحدة لعام ٢٠٢٤، إلا أن غياب اتفاق دولي شامل يُضعف قدرة الدول على التجريم والعقاب الفعّال، الأمر الذي يتطلب العمل على إبرام اتفاق دولي شامل وملزم لمكافحة الجرائم الإلكترونية العابرة للحدود، يتضمن تجريماً موحداً وآليات للتعاون القضائي الدولي.

٣. تعديل التشريعات الوطنية، لا سيما في العراق، لاستيعاب الجريمة الإلكترونية بنصوص صريحة وفعّالة، وإقرار قانون الجرائم المعلوماتية.

٤. ضرورة تدريب القضاة والمحققين على الأدلة الرقمية، وتطوير نظم العدالة الجنائية لمواكبة الفضاء الإلكتروني.

٥. ضرورة إنشاء وحدات تحقيق رقمي متخصص داخل النيابات العامة والمحاكم، وتدريب القضاة على استخدام الأدلة الرقمية.

٦. لا بد من تعزيز مبدأ السيادة السيبرانية بشكل يتوازن مع احترام الحريات الأساسية وحقوق الإنسان الرقمية.

٧. ضرورة تبني التشريعات الوطنية والدولية المعنية نموذج "العدالة الشبكية" الذي يربط المسؤولية بالفاعلية التقنية والرقمية، لا بالهوية الجغرافية فقط.

1- Data Availability Statement: (The manuscript includes all the data used in the study.)

2- Conflict of Interest Statement: (The authors confirm that there are no conflicts of interest that could affect the content of this research.)

3- Funding Statement: This research was fully funded by the authors without any financial support from other entities.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

المصادر والمراجع

أولاً/ الكتب:

(١) المشهداني، أ. ع. (٢٠٠١) .الجرائم التكنولوجية (الطبعة الأولى). شركة الرفاق للطباعة.

(٢) المومني، ن. ع. (٢٠١٠) .الجرائم المعلوماتية (الطبعة الثانية). دار الثقافة للنشر والتوزيع.

(٣) الجبوري، م. خ. ع. (٢٠٢٤). الأمن السيبراني وواجب الدولة في حمايته (أطروحة دكتوراه غير منشورة). كلية القانون، جامعة بغداد، العراق.

(٤) الدسوقي، م. ك. م. (٢٠١٠) .*الحماية الجنائية لسرية المعلومات الإلكترونية* . المنصورة: دار الفكر والقانون للنشر والتوزيع.

(٥) الطوابلة، ع. ح. (دون سنة) .أبحاث في جرائم تقنية المعلومات: التعاون القضائي الدولي لمكافحة الجريمة المعلوماتية .دار الكتب والدراسات العربية.

(٦) العاني، إ. (١٩٩٧) .حرب الشرق الأوسط ونظام الأمن الجماعي (الطبعة الأولى). المطبعة العربية الحديثة.

(٧) العطية، ع. (٢٠٠٨) .القانون الدولي العام (الطبعة الثامنة). بغداد: مكتبة النهضة.

(٨) الغنّام، م. ح. (١٩٦٧) .قواعد القانون الدولي العام .القاهرة: دار النهضة العربية.

(٩) المشهداني، أ. ع. (٢٠٠١) .الجرائم التكنولوجية (الطبعة الأولى). شركة الرفاق للطباعة.

(١٠) المومني، ن. ع. (٢٠١٠) .الجرائم المعلوماتية (الطبعة الثانية). دار الثقافة للنشر والتوزيع.

(١١) بوراس، ع. ق. (٢٠٠٩) .التدخل الدولي الإنساني وتراجع مبدأ السيادة الوطنية .دار الجامعة الجديدة.

(١٢) حجازي، ع. ف. ب. (٢٠٠٧) .الإثبات الجنائي في جرائم الكمبيوتر والإنترنت.دار الكتب القانونية.

(١٣) حسني، م. ن. (١٩٧١) .النظرية العامة للقصد الجنائي (الطبعة الثانية). دار النهضة العربية.

(١٤) شبر، ح. (٢٠٠٦) .السيادة في عالم متغير (الطبعة الأولى). منشورات الفكر والتوعية في الاتحاد الوطني الكردستاني.

(١٥) علوان، ع. ك. (٢٠١٠) .الوسيط في القانون الدولي العام .عمان: دار الثقافة.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

(١٦) غانم، م. ح. (١٩٦٧). قواعد القانون الدولي العام. القاهرة: دار النهضة العربية.

(١٧) مراد، ع. ف. (دون تاريخ). شرح جرائم الكمبيوتر والإنترنت. دار الكتب والوثائق المصرية.

(١٨) ممدوح، م. (٢٠١٩) مكافحة الجريمة المعلوماتية عبر شبكات الإنترنت، والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الإنترنت. الجيزة: مركز الدراسات العربية للتوزيع والنشر.

ثانياً/ الأطاريح والرسائل الجامعية:

(١) الدراجي، ب. غ. ح. (٢٠٢٠). المسؤولية الجنائية الناشئة عن الابتزاز الإلكتروني: دراسة مقارنة (رسالة ماجستير، جامعة البصرة، العراق).

(٢) المويشير، ت. ب. ع. (٢٠٠٩). بناء أنموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته (رسالة ماجستير غير منشورة). جامعة نايف العربية للعلوم الأمنية، الرياض.

(٣) حنش، س. م. (٢٠٢٠). المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية: دراسة مقارنة (رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط).

(٤) صادق، م. ع. (٢٠٢٤). الحماية الدولية للمواقع ذات القوى الخطرة من الهجمات السيبرانية (رسالة ماجستير غير منشورة). معهد العلمين للدراسات العليا.

(٥) عبادة، ع. ج. (٢٠٢٣). *توظيف القدرات السيبرانية في الصراعات الدولية* (أطروحة دكتوراه). معهد العلمين للدراسات العليا.

(٦) محمد، ز. ع. (٢٠١٦). *المسؤولية الدولية الناشئة عن الهجمات السيبرانية* (رسالة لنيل شهادة الماجستير لم تنشر، جامعة الكوفة، العراق).

ثالثاً/ البحوث والدوريات:

(١) الشكري، ع. ي. ع. (٢٠٠٨). الجريمة المعلوماتية وأزمة الشرعية الجزائية. مجلة مركز دراسات الكوفة، ٥(7)، 111–132.

(٢) العزازي، ه. م. خ. (دون تاريخ). النظام القانوني الدولي لمكافحة المخاطر السيبرانية. مجلة مصر المعاصرة، ١١٤(٥٤٩)، 499. الجمعية المصرية للاقتصاد السياسي، دار الفكر العربي.

(٣) الفتلاوي، أ. ع. ن. (٢٠١٥). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. مجلة المحقق الحلي، كلية القانون، جامعة بابل.

(٤) الكاشي، ح. أ. (٢٠٠٦). الترضية في المسؤولية الدولية. مجلة القانون المقارن، جمعية القانون المقارن العراقي، بغداد، العراق.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

(٥) المعموري، م. إ. إ.، و عجيل، ح. خ. (٢٠١٧). السياسة الجنائية في تنفيذ العقوبات الأصلية: دراسة مقارنة .مجلة المحقق الحلي للعلوم القانونية والسياسية، ٩(3)، 273–323.

(٦) أمين، ص. م. (بدون تاريخ). مبدأ عدم جواز التدخل في شؤون الدول في اطار القانون الدولي الإنساني المركز الديمقراطي العربي . https://democraticac.de/?p=38854(تاريخ الزيارة: ٢ يناير، ٢٠٢٥)

(٧) بن فرحات، ن.، و عمري، ع. ق. (٢٠٢٤). الطابع العابر للحدود للجرائم الإلكترونية وأثره على عمليات التحقيق الجنائي .مجلة أبحاث قانونية وسياسية، ٩(1)، 673–660جامعة يحيى فارس، المدية، الجزائر.

(٨) بولحة، ش.، و خلوفي، ر. (٢٠١٩). تحديات الجريمة الإلكترونية في الجزائر . مجلة الأستاذ الباحث للدراسات القانونية والسياسية، ٤(2)، 1974–2003.

(٩) حيدر، أ. أ. الكاشي. (٢٠٠٦). الترضية في المسؤولية الدولية .مجلة القانون المقارن، جمعية القانون المقارن العراقي، بغداد، العراق.

(١٠) رمضان، إ. س. أ. (٢٠٢٥). مواجهة الهجمات السيبرانية في ضوء أحكام القانون الدولي .مجلة العلوم القانونية والاقتصادية، العدد الأول، السنة السابعة والستون.

(١١) زعتر، ه. أ. م. (٢٠٢٣). الإشكاليات القانونية للجرائم الإلكترونية العابرة للحدود وسبل مواجهتها .مجلة البحوث القانونية والاقتصادية، (٨٤)، 59–132.

(١٢) صالح، ي. ع.، و نوذري، م. (٢٠٢٥). أسس وخصائص السياسة الجنائية في الجرائم العابرة للحدود .مجلة الجامعة العراقية، ٧٣(3).

(١٣) صالح، م. م.، و حسين، ج. ع. (٢٠٢٢). الجريمة الإلكترونية وسبل مهاجمتها على المستويين الوطني والدولي .مجلس النواب العراقي، دائرة البحوث، قسم الدراسات القانونية والصياغة التشريعية.

(١٤) سمارة، م. (٢٠٠٨). الجريمة الإلكترونية .مجلة المعلوماتية، (٢٩).

(١٥) عبد الحمزة، س. م. (٢٠٢٢). مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني: دراسة في ضوء تقرير فريق الخبراء الدولي لعام ٢٠٢١ .مجلة مركز دراسات الكوفة، جامعة الكوفة، ١٧(٦٧)، 333.

رابعاً/ الاتفاقيات والوثائق الدولية والتشريعات الوطنية:

(١) الأمم المتحدة. (١٩٤٥) .ميثاق الأمم المتحدة .المادة ٢، الفقرة ٤ . https://www.un.org/ar/about-us/un-charter

(٢) البروتوكول الإضافي الأول إلى اتفاقيات جنيف لعام ١٩٧٧.

(٣) نظام روما الأساسي للمحكمة الجنائية الدولية، ١٩٩٨.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317

(٤) الأمم المتحدة. (٢٠٠١). قرار الجمعية العامة بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.(A/RES/56/121)
(٥) اللجنة الدولية للقانون الدولي. (٢٠٠١) .مشروع مواد بشأن مسؤولية الدول عن الأفعال غير المشروعة دولياً: المواد ٣٦-٣٧- ٣٨: .
https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf
(٦) الأمم المتحدة. (٢٠٠٥). قرار الجمعية العامة رقم ١٧٧/٦٠ [الوثيقة A/RES/60/177]. الجمعية العامة للأمم المتحدة.
(٧) الأمم المتحدة. (٢٠١٠). قرار الجمعية العامة رقم ٢١١/٦٤ [الوثيقة A/RES/64/211]. الجمعية العامة للأمم المتحدة.
(٨) الأمم المتحدة. (٢٠٢٤) .اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية.
(٩) قانون العقوبات العراقي، رقم ١١١ لسنة ١٩٦٩.
(١٠) قانون مكافحة الإرهاب العراقي، رقم ١٣ لسنة ٢٠٠٥.

خامساً/ المؤتمرات:

(١) عرب، ي. (٢٠٠٦). تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية .ورقة عمل مقدمة لمؤتمر هيئة تنظيم الاتصالات، ٢–٤ أبريل ٢٠٠٦، مسقط، سلطنة عمان.هيئة تنظيم الاتصالات.
(٢) عوض، م. م. (١٩٩٣). مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات. ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة.

ISSN (Print): 1994-8999, ISSN (online): 2664-469X. DOI Prefix: 10.36317