Ashur Journal of Legal and political Sciences (AJLSP) is published by the Iraqi Association for Legal Sciences
ISSN: 3005-3269, Vol 3(No.3), pages: 947 -974 (2026)
https://ashurjournal.com/index.php/AJLPS/about

General Elements of Cybercrime and Their Applications: Cyber Extortion as a Model A Comparative Analytical Study in Iraqi, Egyptian, and Saudi Legislation

Assistant Lecturer Jamal Sadoon Murir

University of Fallujah / College of Applied Sciences , jamal.s.murir@uofallujah.edu.iq

ARTICLE INFORMATION

Received: 2 Jul 2026
Accepted: 14 Aug 2026
Published:1 Sep 2026

Keywords:

-Cybercrime
- Electronic Blackmail
- Criminal Liability
- Legal Elements of Crime
- Digital Evidence
- Iraqi Penal Code

ABSTRACT

This research examines the general elements of cybercrime and their applications, with a particular focus on electronic blackmail as a practical model. The study seeks to clarify the legal structure of cybercrime and to determine the position of the requirements of the legal model within the general structure of the crime, while examining the extent to which the general rules of criminal law can accommodate criminal acts committed through digital means. The research adopts an analytical and comparative approach by examining the Iraqi legal framework, particularly the Iraqi Penal Code No. (111) of 1969, as amended, and comparing it with the Egyptian Information Technology Crimes Law No. (175) of 2018 and the Saudi Anti-Cyber Crime Law issued by Royal Decree No. (M/17) of 1428 AH. The study also addresses the legislative developments in Iraq concerning proposed laws on cybercrime and information crimes.The research concludes that the digital environment does not constitute a fourth independent element of the crime. Rather, it may be connected, depending on the nature of the offense, with the specific requirements of the legal model, whether in relation to the object of the criminal conduct or the means by which the act is committed. The study further finds that the absence of a special and independent Iraqi legislation regulating cybercrime does not necessarily prevent criminal liability where the facts can be brought within an existing criminal provision without expanding or analogizing criminalization beyond the limits of the law.

With regard to electronic blackmail, the study demonstrates that its legal characterization depends on the actual elements of the conduct and the applicable criminal provision, rather than merely describing the act as "electronic blackmail." Article (430) of the Iraqi Penal Code may apply to certain forms of electronic threats when its legal elements are satisfied, while Article (456) should not be applied merely because a financial demand is present, since the elements of fraud required by that provision must first be established.

The study also finds that one of the principal practical difficulties in electronic blackmail cases is establishing the attribution of the digital conduct to the accused. The existence of a message, account, telephone number, or digital content alone may not be sufficient to establish authorship or actual use by the accused. Therefore, digital evidence should be assessed within an integrated evidentiary framework supported by technical and objective evidence.The research recommends the adoption of specialized Iraqi legislation regulating cybercrime, including electronic blackmail, with precise definitions and clear criminal elements. It also recommends establishing comprehensive rules for the collection, preservation, examination, and presentation of digital evidence before the courts, while maintaining a proper balance between protecting individuals from digital blackmail and safeguarding the procedural and legal guarantees of the accused.

مجلة آشور للعلوم القانونية والسياسية تصدر عن الجمعية العراقية للعلوم القانونية
المجلد الثالث (العدد الثالث)، الصفحات: 947 – 974، (2026) ISSN: 3005-3269
https://ashurjournal.com/index.php/AJLPS/about

الأركان العامة للجريمة الإلكترونية وتطبيقاتها جريمة الابتزاز الإلكتروني أنموذجاً

دراسة تحليلية مقارنة في التشريع العراقي والمصري والسعودي

م. م. جمال سعدون مرير

جامعة الفلوجة / كلية العلوم التطبيقية ، jamal.s.murir@uofallujah.edu.iq

معلومات المقالة

تاريخ الاستلام : ٢ تموز ٢٠٢٦
تاريخ القبول : ١٤ اب ٢٠٢٦
تاريخ النشر : ١ ايلول ٢٠٢٦

الملخص

تتناول هذه الدراسة الأركان العامة للجريمة الإلكترونية، من خلال بيان مفهومها وتمييزها عن المصطلحات المتداخلة معها، ثم تحليل متطلبات نموذجها القانوني في ضوء القواعد العامة في قانون العقوبات، مع تطبيق ذلك على جريمة الابتزاز الإلكتروني بوصفها من أبرز صور الاعتداء التي تستغل الوسائل والتقنيات الرقمية. وتركز الدراسة بصورة خاصة على مدى ملاءمة القواعد العامة في قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل لتجريم أفعال الابتزاز المرتكبة باستخدام الوسائل الإلكترونية، في ظل عدم وجود تشريع عراقي خاص ومستقل ينظم الجرائم الإلكترونية بصورة شاملة وتنطلق الدراسة من إشكالية تتمثل في مدى كفاية القواعد الجنائية العامة لاستيعاب الخصائص التي تميز الجريمة الإلكترونية، ولا سيما ما يتعلق بالركن الشرعي والركن المادي والركن المعنوي، فضلاً عن متطلبات النموذج القانوني للجريمة التي تفرضها طبيعة البيئة الرقمية ومحل السلوك الإجرامي. كما تبحث الدراسة مدى انطباق هذه العناصر على جريمة الابتزاز الإلكتروني، وحدود التكييف القانوني للأفعال المرتكبة في هذا المجال وفق النصوص العقابية التقليدية واعتمدت الدراسة المنهج التحليلي من خلال تحليل النصوص القانونية والآراء الفقهية ذات الصلة، والمنهج المقارن لمقارنة الموقف العراقي ببعض التشريعات العربية، ولا سيما التشريع المصري والسعودي، فضلاً عن الاستعانة بالمدخل التاريخي في حدود ما يلزم لبيان تطور محاولات التشريع العراقي في مجال الجرائم الإلكترونية وتوصلت الدراسة إلى أن القواعد العامة في قانون العقوبات العراقي توفر أساساً مؤقتاً لمواجهة بعض صور الابتزاز المرتكب بوسائل إلكترونية، إلا أن الاعتماد عليها بصورة مستمرة يثير إشكالات تتصل بمبدأ الشرعية الجنائية وخصوصية السلوك الرقمي وطبيعة الدليل الإلكتروني. كما خلصت إلى أن وجود تنظيم تشريعي خاص أصبح ضرورة لمعالجة الخصائص الفنية والقانونية لهذه الجرائم، وبخاصة ما يتعلق بتحديد الأفعال المجرّمة، وتنظيم حجية الدليل الرقمي، وضبط إجراءات جمعه والمحافظة عليه.

الكلمات المفتاحية:

- الجريمة الإلكترونية
- الابتزاز الإلكتروني
- الأركان العامة للجريمة
- النموذج القانوني للجريمة
- قانون العقوبات العراقي
- الدليل الرقمي

المقدمة

أحدث التطور المتسارع في تقنيات المعلومات والاتصالات تحولاً عميقاً في مختلف مجالات الحياة، وأصبحت الوسائل الرقمية جزءاً أساسياً من المعاملات والاتصالات وتبادل المعلومات. وقد صاحب هذا التطور ظهور أنماط جديدة من السلوك الإجرامي تستفيد من خصائص البيئة الرقمية، سواء من خلال استخدام الوسائل الإلكترونية أداةً لارتكاب أفعال مجرّمة، أو من خلال استهداف الأنظمة والبيانات والمعلومات ذاتها[1].وقد أدى هذا التحول إلى بروز ما اصطلح على تسميته في الفقه والتشريعات بـ الجريمة الإلكترونية أو الجريمة المعلوماتية، وهي تسميات تتعدد بحسب زاوية النظر إلى محل الجريمة أو وسيلة ارتكابها. ولأغراض هذه الدراسة، يُستخدم مصطلح الجريمة الإلكترونية بوصفه المصطلح الرئيس، ويُستعمل مصطلح الجريمة المعلوماتية عند الإشارة إلى تسمية تشريعية أو فقهية محددة، دون اعتبار اختلاف المصطلحات اختلافاً في موضوع الدراسة[2] وتتميز الجريمة الإلكترونية عن كثير من صور الإجرام التقليدي بطبيعة الوسيلة التي ترتكب من خلالها، وبسرعة تنفيذها، وإمكانية إخفاء آثارها أو تغييرها، فضلاً عن إمكان امتداد آثارها إلى أكثر من دولة. إلا أن هذه الخصائص لا تعني بالضرورة قيام نظرية مستقلة تماماً عن النظرية العامة للجريمة؛ إذ تظل الجريمة الإلكترونية خاضعة، من حيث الأصل، للقواعد العامة المتعلقة بالتجريم والعقاب، مع مراعاة الخصائص التي تفرضها طبيعة الوسائل والبيانات والأنظمة الرقمية [3] .

وتبرز أهمية هذا الأمر بصورة أوضح عند دراسة الابتزاز الإلكتروني، الذي يقوم في صورته الشائعة على استغلال معلومات أو صور أو مراسلات أو بيانات ذات صلة بالمجني عليه، ثم استعمالها أو التهديد باستعمالها لحمله على القيام بفعل أو الامتناع عنه أو تقديم منفعة للجاني. وهنا تظهر إشكالات قانونية متعددة تتعلق بتحديد النص العقابي المنطبق، ومدى استيعاب النصوص التقليدية للسلوك المرتكب بواسطة الوسائل الإلكترونية، فضلاً عن إثبات نسبة الحساب أو الرسالة أو المحتوى الرقمي إلى الشخص المتهم[4] .

وتتحدد مشكلة الدراسة في البحث عن مدى قدرة القواعد العامة للجريمة والنصوص العقابية العراقية القائمة على استيعاب الخصائص القانونية للابتزاز الإلكتروني، ولا سيما في ظل عدم وجود قانون عراقي خاص ومستقل ينظم الجرائم الإلكترونية بصورة متكاملة. ولا تقتصر المشكلة على تحديد النص العقابي المناسب، وإنما تمتد إلى بيان عناصر الجريمة ومتطلبات نموذجها القانوني، وإلى مدى كفاية وسائل الإثبات التقليدية في التعامل مع الأدلة الرقمية[5] ومن هنا تركز الدراسة على تحليل الأركان العامة للجريمة الإلكترونية، ثم تطبيقها على جريمة الابتزاز الإلكتروني، مع الوقوف على موقف التشريع العراقي وبعض التشريعات المقارنة من هذه الجريمة، وصولاً إلى تحديد أوجه القصور التي تحتاج إلى معالجة تشريعية.

أولاً: أهمية البحث

تنبع أهمية الدراسة من كونها تتناول إشكالية قانونية عملية ترتبط بالتطور التقني وتأثيره في قواعد التجريم والعقاب، ويمكن بيان أهميتها في جانبين:

1 .الأهمية العلمية:

تتمثل في محاولة ضبط مفهوم الجريمة الإلكترونية وتوحيد المصطلح المستخدم في الدراسة، وبيان مدى خضوعها للأركان العامة للجريمة، مع التمييز بين هذه الأركان وبين متطلبات النموذج القانوني للجريمة التي تفرضها طبيعة محل السلوك أو البيئة الرقمية.

كما تسعى الدراسة إلى بيان الخصائص القانونية للابتزاز الإلكتروني باعتباره نموذجاً تطبيقياً، بدلاً من التوسع في دراسة جميع صور الجرائم الإلكترونية التي قد تشتت موضوع البحث.

2 .الأهمية العملية:

تتجلى في بحث مدى ملاءمة النصوص العقابية العراقية القائمة لمواجهة الابتزاز الإلكتروني، وبيان الإشكالات التي يثيرها التكييف القانوني لهذه الأفعال، فضلاً عن دراسة الصعوبات المرتبطة بإثبات الجريمة الرقمية ونسبة السلوك الإلكتروني إلى مرتكبه.

ثانياً: إشكالية البحث

تتمحور إشكالية البحث حول السؤال الرئيس الآتي:

إلى أي مدى تستوعب القواعد العامة للجريمة والنصوص العقابية في قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل الخصائص القانونية لجريمة الابتزاز الإلكتروني، في ظل غياب تنظيم تشريعي عراقي خاص ومستقل للجرائم الإلكترونية(6)

ويتفرع عن هذا السؤال عدد من التساؤلات، أهمها:

1 .ما المقصود بالجريمة الإلكترونية، وما مدى الحاجة إلى توحيد المصطلحات المستخدمة في التعبير عنها؟

2 .ما مدى خضوع الجريمة الإلكترونية للأركان العامة للجريمة، وما المقصود بمتطلبات نموذجها القانوني؟

3 .كيف تتجسد الأركان العامة ومتطلبات النموذج القانوني في جريمة الابتزاز الإلكتروني؟

4 .إلى أي مدى يمكن تطبيق النصوص العامة في قانون العقوبات العراقي على أفعال الابتزاز المرتكبة باستخدام الوسائل الإلكترونية؟

5 .ما موقف بعض التشريعات المقارنة من الابتزاز الإلكتروني، وما الذي يمكن الاستفادة منه في معالجة النقص التشريعي العراقي؟

6 .ما أبرز الإشكالات التي يثيرها الدليل الرقمي في إثبات جريمة الابتزاز الإلكتروني([7])؟

ثالثاً: أهداف البحث

تهدف الدراسة إلى تحقيق مجموعة من الأهداف، أهمها:

1 .تحديد مفهوم الجريمة الإلكترونية واعتماد مصطلح موحد داخل الدراسة.

2 .بيان مدى خضوع الجريمة الإلكترونية للأركان العامة للجريمة وفق النظرية العامة للقانون الجنائي.

3 .التمييز بين الأركان العامة للجريمة وبين متطلبات النموذج القانوني للجريمة الإلكترونية.

4 .تحليل جريمة الابتزاز الإلكتروني بوصفها نموذجاً تطبيقياً للأركان العامة ومتطلبات النموذج القانوني.

5 .بيان مدى ملاءمة النصوص العقابية العراقية النافذة لتجريم الابتزاز المرتكب بواسطة الوسائل الإلكترونية.

6 .مقارنة الموقف العراقي ببعض التشريعات العربية التي عالجت الجرائم الإلكترونية بنصوص خاصة.

7 .تحديد أبرز الإشكالات المرتبطة بالإثبات الرقمي في جرائم الابتزاز الإلكتروني([8]).

رابعاً: فرضية البحث

تنطلق الدراسة من فرضية مفادها أن القواعد العامة في قانون العقوبات العراقي يمكن أن توفر أساساً مؤقتاً لتجريم بعض صور الابتزاز المرتكب باستخدام الوسائل الإلكترونية، إلا أن الاعتماد عليها لا يوفر معالجة تشريعية متكاملة تتلاءم مع الخصائص الفنية والقانونية للجريمة الإلكترونية، الأمر الذي يستدعي تنظيماً تشريعياً خاصاً يحدد صور السلوك المجرّم ويعالج خصوصية الدليل الرقمي وإجراءات الحصول عليه والمحافظة عليه([9]).

خامساً: مناهج البحث

اعتمدت الدراسة على:

1 .المنهج التحليلي:

وذلك بتحليل النصوص القانونية والقواعد العامة المتعلقة بالجريمة والتهديد والابتزاز، وبيان مدى انطباقها على السلوك المرتكب باستخدام الوسائل الإلكترونية.

2 .المنهج المقارن:

وذلك من خلال مقارنة الموقف العراقي ببعض التشريعات العربية، وبخاصة التشريع المصري والسعودي، في حدود ما يخدم موضوع الابتزاز الإلكتروني.

3 .المدخل التاريخي:

استُعين به في حدود ضيقة لتتبع تطور محاولات التشريع العراقي في مجال الجرائم الإلكترونية، دون اعتباره منهجاً مستقلاً من مناهج البحث المستخدمة في الدراسة.

هذه الصياغة تعالج الملاحظة رقم (2) مباشرة؛ فلا نقول إن «المنهج التتبعي» منهج رئيس، بل نقول المدخل التاريخي واستخدامه محدود.

سادساً: هيكلية البحث

لتحقيق أهداف الدراسة والإجابة عن إشكاليتها، قسمت إلى مبحثين يسبقهما تمهيد يتضمن عناصر الدراسة الأساسية، وتعقبهما خاتمة تتضمن أهم النتائج والمقترحات.

المبحث الأول:الإطار العام للجريمة الإلكترونية ومتطلبات نموذجها القانوني

ويتضمن مطلبين:

المطلب الأول: مفهوم الجريمة الإلكترونية وتطور تنظيمها التشريعي في العراق

*الفرع الأول: مفهوم الجريمة الإلكترونية وتمييزها عن المصطلحات المتداخلة.

*الفرع الثاني: التطور التشريعي العراقي في مجال الجرائم الإلكترونية.

المطلب الثاني: الأركان العامة ومتطلبات النموذج القانوني للجريمة الإلكترونية

*الفرع الأول: الركن الشرعي ومبدأ المشروعية.

*الفرع الثاني: الركن المادي وعناصره.

*الفرع الثالث: الركن المعنوي والقصد الجنائي.

*الفرع الرابع: متطلبات النموذج القانوني للجريمة الإلكترونية.

المبحث الثاني: جريمة الابتزاز الإلكتروني وتكييفها القانوني وإثباتها

ويتضمن مطلبين:

المطلب الأول: البناء القانوني لجريمة الابتزاز الإلكتروني

*الفرع الأول: متطلبات النموذج القانوني لجريمة الابتزاز الإلكتروني.

*الفرع الثاني: الركن المادي لجريمة الابتزاز الإلكتروني.

*الفرع الثالث: الركن المعنوي لجريمة الابتزاز الإلكتروني.

المطلب الثاني: التكييف القانوني والمواجهة التشريعية والقضائية للابتزاز الإلكتروني

*الفرع الأول: التكييف القانوني للابتزاز الإلكتروني في التشريع العراقي والمقارن.

* الفرع الثاني: الموقف القضائي وإشكالات الإثبات الرقمي

المبحث الأول

الإطار العام للجريمة الإلكترونية ومتطلبات نموذجها القانوني

تثير الجريمة الإلكترونية إشكالات قانونية تتصل بمدى قدرة القواعد العامة في القانون الجنائي على استيعاب الأفعال التي ترتكب باستخدام التقنيات الرقمية أو تستهدف الأنظمة والبيانات والمعلومات الإلكترونية. ولا ترجع خصوصية هذه الجرائم إلى انفصالها عن النظرية العامة للجريمة، وإنما إلى طبيعة الوسيلة أو المحل الذي يتصل به السلوك الإجرامي، وما يترتب على ذلك من آثار في تحديد النص الواجب التطبيق وإثبات الواقعة ونسبتها إلى مرتكبها. وعليه، يقتضي تحديد البناء القانوني للجريمة الإلكترونية البدء ببيان المقصود بها وتمييزها عن المصطلحات المتداخلة معها، ثم الوقوف على تطور التنظيم التشريعي العراقي في هذا المجال. وبعد ذلك يتم تحليل الأركان العامة للجريمة، وهي الركن الشرعي والركن المادي والركن المعنوي، مع بيان متطلبات النموذج القانوني التي تفرضها طبيعة الجريمة الإلكترونية دون الخلط بينها وبين الأركان العامة.

وينقسم هذا المبحث إلى مطلبين؛ يتناول الأول مفهوم الجريمة الإلكترونية وتطور تنظيمها التشريعي في العراق، بينما يخصص الثاني لدراسة الأركان العامة ومتطلبات النموذج القانوني للجريمة الإلكترونية.

المطلب الأول

مفهوم الجريمة الإلكترونية وتطور تنظيمها التشريعي في العراق

تحديد مفهوم الجريمة الإلكترونية يمثل نقطة البداية في دراسة أحكامها؛ لأن تعدد المصطلحات المستخدمة في هذا المجال قد يؤدي إلى اختلاف في تحديد نطاق الدراسة وما يدخل فيها من أفعال. كما أن غياب تعريف تشريعي جامع في بعض التشريعات يجعل من الضروري الاستناد إلى المعايير الفقهية والقانونية لبيان مدلول المصطلح المعتمد.

وعلى هذا الأساس، يتناول هذا المطلب مفهوم الجريمة الإلكترونية وتمييزها عن المصطلحات المتداخلة معها، ثم يعرض بصورة موجزة تطور محاولات التنظيم التشريعي العراقي للجرائم الإلكترونية بالقدر الذي يخدم موضوع الدراسة[10].

الفرع الأول

مفهوم الجريمة الإلكترونية وتمييزها عن المصطلحات المتداخلة

اختلفت التسميات التي استخدمت للتعبير عن الأفعال الإجرامية المرتبطة بالتقنيات الحديثة، ومن أبرزها: الجريمة الإلكترونية، والجريمة المعلوماتية، والجريمة السيبرانية، وجرائم الحاسوب. ولا يعني تعدد هذه التسميات بالضرورة وجود أنواع مستقلة من الجرائم، إذ قد تعبر في كثير من الاستخدامات عن نطاق متقارب، مع اختلاف زاوية التركيز التي ينطلق منها كل مصطلح ويقصد بالجريمة الإلكترونية، في نطاق هذه الدراسة، كل سلوك غير مشروع ومعاقب عليه قانوناً يرتكب باستخدام وسيلة إلكترونية أو تقنية رقمية، أو يستهدف نظاماً معلوماتياً أو بيانات أو معلومات إلكترونية، متى توافرت في الفعل أركان الجريمة ومتطلبات نموذجها القانوني ويتميز هذا التعريف بأنه لا يقصر الجريمة الإلكترونية على الحالات التي يكون فيها الحاسوب أو النظام المعلوماتي محلاً للاعتداء، وإنما يشمل أيضاً الحالات التي تستخدم فيها الوسائل الإلكترونية أداة لارتكاب جريمة يكون محلها شخصاً أو مالاً أو حقاً من الحقوق، كما هو الحال في الابتزاز الإلكتروني ومن ثم يمكن التمييز بين اتجاهين رئيسين في تحديد مفهوم الجريمة الإلكترونية؛ أولهما يركز على محل الاعتداء، فيدخل ضمن المفهوم الأفعال التي تستهدف البيانات أو البرامج أو الأنظمة المعلوماتية، وثانيهما يركز على الوسيلة المستخدمة في ارتكاب الجريمة، فينظر إلى الجريمة باعتبارها فعلاً إجرامياً استُخدمت في ارتكابه تقنية إلكترونية ويبدو أن الاقتصار على أحد الاتجاهين يؤدي إلى تضييق نطاق المفهوم؛ فالابتزاز الإلكتروني، على سبيل المثال، قد لا يستهدف النظام المعلوماتي ذاته، وإنما يستعمل وسيلة إلكترونية للتهديد بنشر صور أو معلومات خاصة بالمجني عليه. ومن هنا يكون الاتجاه الذي يجمع بين الوسيلة والمحل أكثر ملاءمة لموضوع الدراسة، لأنه يستوعب صور الجرائم التي تكون التقنية فيها محلاً للاعتداء، وكذلك الجرائم التي تستخدم التقنية أداة لتنفيذ السلوك الإجرامي وعليه، تعتمد هذه الدراسة مصطلح الجريمة الإلكترونية بوصفه المصطلح الرئيس، على أن يرد مصطلح الجريمة المعلوماتية عندما يكون استعماله مرتبطاً باسم تشريع أو مشروع قانون أو رأي فقهي محدد. أما مصطلح الابتزاز الإلكتروني فيستخدم حصراً للدلالة على الصورة الإجرامية محل التطبيق في المبحث الثاني[11].

وهذا التوحيد الاصطلاحي يهدف إلى منع الخلط بين المفهوم العام للجريمة الإلكترونية وبين الابتزاز الإلكتروني الذي يمثل إحدى صورها، فضلاً عن تجنب استعمال المصطلحات المختلفة وكأنها تشير إلى موضوعات مستقلة دون بيان العلاقة بينها.

الفرع الثاني

التطور التشريعي العراقي في مجال الجرائم الإلكترونية

لم يتجه المشرع العراقي، خلال الفترة التي يتناولها البحث، إلى وضع تنظيم تشريعي واحد ومستقل يستوعب جميع صور الجرائم المرتبطة بالتقنيات الرقمية، الأمر الذي أدى إلى الاعتماد في بعض الحالات على النصوص العامة في قانون العقوبات النافذ. وفي مقابل ذلك، شهدت السنوات الماضية محاولات تشريعية متعددة هدفت إلى وضع إطار خاص لمواجهة الجرائم الإلكترونية ويقتضي تناول هذا التطور عدم الاسترسال في عرض المراحل التاريخية للمشاريع التشريعية، وإنما الاقتصار على أبرز المحطات التي تكشف عن تطور النظرة التشريعية إلى الجريمة الإلكترونية ومدى الانتقال من الاعتماد على القواعد التقليدية إلى محاولة وضع تنظيم خاص فقد ظهر مشروع قانون مكافحة الجرائم الإلكترونية لسنة 2011 بوصفه إحدى المحاولات المبكرة لمعالجة الجرائم المرتبطة باستخدام التقنيات الحديثة. وقد تضمن المشروع أحكاماً تتعلق بعدد من الأفعال المرتكبة باستخدام الوسائل الإلكترونية، إلا أن المشروع واجه ملاحظات وانتقادات تتعلق باتساع نطاق بعض النصوص والعقوبات، ومدى توافقها مع الضمانات الدستورية والحريات العامة[12] ثم ظهرت محاولات تشريعية لاحقة، من بينها مشروع قانون الجرائم المعلوماتية لسنة 2019، الذي اتجه إلى صياغة أكثر ارتباطاً بالمفاهيم التقنية، ومحاولة تحديد صور الاعتداء على الأنظمة والبيانات والمعلومات بصورة أكثر تفصيلا[13] وفي سنة 2021 برز مشروع آخر لمكافحة الجرائم الإلكترونية، اتجه إلى تطوير التصنيف القانوني للأفعال المرتكبة في البيئة الرقمية، مع الاهتمام بصورة أكبر بالاعتداءات التي تستهدف الأفراد والبيانات والأنظمة المعلوماتية[14] ويكشف هذا التسلسل، في حدود ما يخدم موضوع الدراسة، عن استمرار الحاجة إلى إطار تشريعي خاص، ولا سيما أن التطور التقني المستمر يؤدي إلى ظهور صور جديدة من السلوك الإجرامي يصعب أحياناً استيعابها بصورة دقيقة من خلال النصوص التقليدية ومن ثم، فإن أهمية هذه المشاريع لا تكمن في مجرد تتبع تواريخها، وإنما في كونها تكشف عن الفجوة بين التطور التقني والحاجة إلى نصوص جنائية محددة، وهي الفجوة التي تظهر بصورة واضحة عند محاولة تكييف الابتزاز المرتكب بواسطة الوسائل الإلكترونية وفق نصوص وضعت أصلاً لصور تقليدية من التهديد أو الاحتيال.

وعليه، لن تتوسع الدراسة في تحليل كل مشروع تشريعي أو سرد تفاصيله، وإنما ستستفيد من هذا التطور في تحديد الإشكالية الأساسية للبحث، وهي مدى كفاية القواعد العقابية النافذة إلى حين وجود تنظيم تشريعي خاص.

المطلب الثاني

الأركان العامة ومتطلبات النموذج القانوني للجريمة الإلكترونية

تخضع الجريمة الإلكترونية، من حيث الأصل، للقواعد العامة التي تحكم قيام المسؤولية الجنائية، فلا يكفي أن يكون الفعل قد ارتكب بواسطة وسيلة إلكترونية حتى يكتسب وصف الجريمة، وإنما يجب أن تتوافر فيه عناصر

التجريم التي يتطلبها القانون وتبرز خصوصية الجريمة الإلكترونية في أن الوسيلة الرقمية قد تغير من صورة السلوك الإجرامي أو طريقة تحقق النتيجة أو كيفية إثبات العلاقة بين الفعل ومرتكبه، كما قد يفرض النموذج القانوني للجريمة محل الدراسة وجود محل أو وسيلة أو ظرف محدد يرتبط به التجريم ومن الضروري هنا التمييز بين الأركان العامة للجريمة وبين متطلبات النموذج القانوني للجريمة؛ فالركن الشرعي والركن المادي والركن المعنوي تمثل الأساس العام لقيام الجريمة، أما العناصر التي يشترطها النص الخاص في جريمة معينة فتتحدد وفقاً لذلك النص ولا يصح جعلها ركناً عاماً رابعاً لمجرد اتصالها بالبيئة الرقمية.

وعلى هذا الأساس، يتناول هذا المطلب الركن الشرعي، ثم الركن المادي، ثم الركن المعنوي، وأخيراً متطلبات النموذج القانوني للجريمة الإلكترونية.

الفرع الأول

الركن الشرعي ومبدأ المشروعية

يقوم الركن الشرعي للجريمة على مبدأ المشروعية الجنائية الذي مؤداه أنه لا جريمة ولا عقوبة إلا بنص قانوني سابق يقرر التجريم والعقاب. ويشكل هذا المبدأ ضمانة أساسية للحرية الفردية، إذ يمنع إنشاء الجرائم والعقوبات بطريق القياس أو التوسع غير المشروع في تفسير النصوص الجنائية.

وتزداد أهمية هذا المبدأ في مجال الجرائم الإلكترونية بسبب سرعة التطور التقني وتنوع صور السلوك المرتكب باستخدام الوسائل الرقمية؛ فقد تظهر أفعال جديدة لا يكون لها مقابل واضح في النصوص التي وضعت قبل ظهور هذه التقنيات وفي العراق، يستند مبدأ الشرعية الجنائية إلى الإطار الدستوري والقانوني، كما يقرره قانون العقوبات رقم (111) لسنة 1969 المعدل في مادته الأولى، التي تقرر مبدأ عدم العقاب على فعل أو امتناع إلا بناءً على نص قانوني[15].

وتثير الجرائم الإلكترونية في هذا المجال إشكالية تتعلق بحدود قدرة النصوص التقليدية على استيعاب السلوك الرقمي. فليس كل اختلاف في وسيلة ارتكاب الجريمة يمنع تطبيق النص الجنائي، لكن لا يجوز في المقابل تجاوز حدود النص بحيث يؤدي ذلك إلى إنشاء جريمة جديدة بطريق القياس.ومن هنا فإن تطبيق النصوص التقليدية على بعض صور الابتزاز الإلكتروني يجب أن يخضع لضابط أساسي، وهو وجود تطابق بين عناصر السلوك الواقعي والعناصر التي يتطلبها النص العقابي، بحيث تكون الوسيلة الإلكترونية مجرد طريقة ارتكاب لا تغير من الطبيعة القانونية للعناصر التي جرمها المشرع.أما إذا كان السلوك الرقمي يتضمن عناصر لا يمكن إدخالها ضمن مدلول النص التقليدي دون توسع غير جائز، فإن معالجة ذلك ينبغي أن تكون عن طريق التشريع، لا عن طريق التوسع في التفسير على حساب مبدأ الشرعية وتظهر أهمية هذه القاعدة بصورة خاصة في جريمة الابتزاز الإلكتروني؛ إذ يجب التحقق من مدى انطباق النص العقابي على التهديد الموجه عبر وسيلة إلكترونية، دون

افتراض أن مجرد استخدام الهاتف أو إحدى منصات التواصل ينشئ وصفاً جرمياً مستقلاً ما لم يكن القانون قد قرر ذلك.

الفرع الثاني

الركن المادي وعناصره

يمثل الركن المادي المظهر الخارجي للجريمة، ويتحقق بالسلوك الذي يصدر عن الجاني والنتيجة التي يرتبها القانون عليه، فضلاً عن العلاقة السببية متى كانت النتيجة عنصراً لازماً لتمام الجريمة[16].ولا تختلف الجريمة الإلكترونية من حيث الأصل عن الجريمة التقليدية في ضرورة وجود سلوك مادي قابل للإسناد إلى الفاعل، وإنما تكمن الخصوصية في الصورة التي يظهر بها هذا السلوك والوسائل المستخدمة في تنفيذه[17].

أولاً: السلوك الإجرامي الإلكتروني

قد يكون السلوك الإجرامي فعلاً إيجابياً، مثل إرسال رسالة تتضمن تهديداً، أو الدخول بصورة غير مشروعة إلى نظام معلوماتي، أو إرسال ملف أو صورة أو برنامج ضار. وقد يتحقق في بعض الجرائم عن طريق الامتناع متى كان القانون يرتب المسؤولية على الامتناع وتوافرت شروطه وفي جريمة الابتزاز الإلكتروني، يتمثل السلوك بصورة أساسية في استعمال وسيلة إلكترونية لتوجيه تهديد إلى المجني عليه، كإرسال رسالة أو تسجيل أو صورة أو غير ذلك من المحتويات الرقمية، بحيث يتضمن السلوك تهديداً يكشف عن إرادة الجاني في إخضاع المجني عليه لمطلب معين([18]) ولا تكمن أهمية الوسيلة الإلكترونية في ذاتها، وإنما في أثرها على طريقة تنفيذ السلوك وإثباته؛ فالرسالة الإلكترونية قد تمثل وسيلة للتهديد، كما يمكن أن تكون في الوقت ذاته دليلاً على وقوع السلوك، إذا أمكن التحقق من صحتها ونسبتها إلى صاحب الحساب أو الجهاز المستخدم.

ثانياً: النتيجة الإجرامية

تتمثل النتيجة الإجرامية في الأثر الذي يرتبه السلوك متى كان القانون يشترط تحقق نتيجة معينة لقيام الجريمة[19].

وفي الجرائم التي تمس حرية المجني عليه عن طريق التهديد، قد تتمثل النتيجة في التأثير في إرادته وإحداث حالة من الخوف أو الضغط تدفعه إلى الاستجابة لمطلب الجاني ولا يشترط في كل صورة من صور الابتزاز الإلكتروني أن تتحقق النتيجة التي يسعى إليها الجاني فعلاً؛ إذ يتوقف ذلك على طبيعة النص العقابي وأركان الجريمة المحددة فيه. ومن ثم يجب التمييز بين تمام السلوك المجرّم وبين تحقق الغاية التي كان الجاني يستهدفها[20].

ثالثاً: العلاقة السببية

تظهر العلاقة السببية عندما يشترط القانون نتيجة معينة، بحيث يجب إثبات أن النتيجة التي يعتد بها القانون قد ترتبت على السلوك المنسوب إلى الجاني[21].وتكتسب العلاقة السببية في الجرائم الإلكترونية أهمية خاصة بسبب إمكانية استخدام حسابات متعددة أو أجهزة مختلفة أو وسائل لإخفاء مصدر الاتصال، مما قد يؤدي إلى صعوبة الربط بين الفعل الرقمي والشخص الذي يقف وراءه ومن هنا لا يكفي إثبات وجود رسالة تهديد أو حساب إلكتروني، وإنما يجب، عند المنازعة، إقامة الدليل على نسبة السلوك إلى المتهم، بالاستناد إلى مجموع الأدلة الفنية والموضوعية المتاحة، وليس إلى مجرد وجود اسم أو صورة على الحساب الإلكتروني.

الفرع الثالث

الركن المعنوي والقصد الجنائي

لا تكتمل المسؤولية الجنائية في الجرائم العمدية بمجرد تحقق السلوك المادي، وإنما يجب أن يتوافر لدى الجاني القصد الجنائي الذي يتكون، في صورته العامة، من العلم والإرادة[22].ويتمثل العلم في إدراك الجاني لطبيعة السلوك الذي يأتيه والظروف والعناصر التي يتطلبها النموذج القانوني للجريمة، بينما تتمثل الإرادة في اتجاه إرادته إلى ارتكاب السلوك المجرّم.وفي الجريمة الإلكترونية، لا يكفي إثبات أن رسالة أو صورة أو محتوى رقمياً صدر من جهاز أو حساب معين، وإنما ينبغي، بحسب ظروف الواقعة، إثبات صلة المتهم بالفعل وعلمه بطبيعته واتجاه إرادته إلى ارتكابه .وتتضح أهمية القصد الجنائي في الابتزاز الإلكتروني بصورة أكبر؛ إذ ينبغي أن يكون الجاني عالماً بمضمون التهديد وبطبيعة الوسيلة التي يستخدمها، وأن تتجه إرادته إلى استعمال التهديد للضغط على المجني عليه وحمله على الاستجابة لمطلبه أما إذا ثبت أن الفعل وقع نتيجة خطأ مادي أو تقني لا تتوافر معه إرادة ارتكاب السلوك المجرّم، فإن ذلك قد يؤثر في قيام القصد الجنائي، بحسب ظروف الواقعة والنص القانوني المنطبق وعليه، فإن الطابع الإلكتروني للجريمة لا يؤدي إلى إنشاء صورة مستقلة من القصد الجنائي، وإنما يفرض وسائل خاصة لإثبات العلم والإرادة، وهو ما يجعل الدليل الرقمي والقرائن الفنية ذات أهمية كبيرة في هذا المجال.

الفرع الرابع

متطلبات النموذج القانوني للجريمة الإلكترونية

بعد بيان الأركان العامة للجريمة، تبرز الحاجة إلى تحديد العناصر التي يفرضها النموذج القانوني للجريمة الإلكترونية بحسب طبيعة الفعل والنص المجرّم[23] ولا يصح اعتبار البيئة الرقمية ركناً رابعاً عاماً لكل جريمة إلكترونية؛ لأن الجرائم تختلف في عناصرها، وقد تكون التقنية وسيلة لارتكاب الجريمة دون أن تكون محلاً للاعتداء، كما قد تكون البيانات أو النظام المعلوماتي محل الاعتداء بصورة مباشرة[24] ويقصد بمتطلبات النموذج

القانوني، في نطاق هذه الدراسة، العناصر الخاصة التي يتطلبها النص العقابي لتحديد محل الحماية أو الوسيلة أو الظرف الذي يرتبط به السلوك الإجرامي فقد يكون النظام المعلوماتي أو البيانات الإلكترونية محل الاعتداء في بعض الجرائم، وقد تكون الوسيلة الإلكترونية مجرد أداة لتنفيذ جريمة أخرى. ولذلك تختلف هذه المتطلبات بحسب طبيعة الجريمة والنص الواجب التطبيق وفي جريمة الابتزاز الإلكتروني، يظهر هذا الأمر بصورة واضحة؛ إذ لا يشترط أن يكون النظام المعلوماتي ذاته محل الاعتداء، وإنما قد تكون البيانات أو الصور أو المحادثات الخاصة هي محل الاستغلال، بينما تكون الوسيلة الإلكترونية أداة لإيصال التهديد أو ممارسة الضغط على المجني عليه وبذلك نصل إلى نتيجة مهمة في البناء القانوني للدراسة، وهي أن الأركان العامة للجريمة شيء، ومتطلبات النموذج القانوني للجريمة الإلكترونية شيء آخر؛ فلا ينبغي إدخال البيئة الرقمية بوصفها ركناً رابعاً عاماً، وإنما يجب تحديد العنصر الخاص الذي يتطلبه النص في كل جريمة على حدة وهذه النتيجة ستكون أساساً لتحليل جريمة الابتزاز الإلكتروني في المبحث الثاني، إذ سنبحث هناك متطلبات نموذجها القانوني، ثم ركنها المادي والمعنوي، وبعد ذلك ننتقل إلى التكييف التشريعي والقضائي وإشكالات الإثبات الرقمي.

المبحث الثاني

جريمة الابتزاز الإلكتروني وتكييفها القانوني وإثباتها

تمثل جريمة الابتزاز الإلكتروني التطبيق الأبرز الذي يمكن من خلاله اختبار مدى ملاءمة القواعد العامة للجريمة ومتطلبات نموذجها القانوني للأفعال المرتكبة في البيئة الرقمية. ولا تقتصر خصوصية هذه الجريمة على استعمال وسيلة إلكترونية في تنفيذها، وإنما تمتد إلى طبيعة محل الاستغلال، وطريقة توجيه التهديد، وإمكان إخفاء هوية الفاعل، فضلاً عن الصعوبات التي تثار عند إثبات نسبة المحتوى الرقمي إلى مرتكبه وتقوم فكرة الابتزاز الإلكتروني، في صورتها الأساسية، على استغلال الجاني لمعلومات أو صور أو تسجيلات أو مراسلات أو بيانات تتصل بالمجني عليه، ثم استخدام هذه المادة أو التهديد باستخدامها لحمله على القيام بفعل أو الامتناع عنه أو تقديم منفعة للجاني. وقد تختلف صور السلوك باختلاف الوسيلة المستخدمة وطبيعة الطلب والبيانات المستغلة، إلا أن القاسم المشترك بينها يتمثل في توجيه ضغط غير مشروع إلى إرادة المجني عليه ويقتضي تحليل هذه الجريمة عدم التعامل معها باعتبارها جريمة منفصلة عن النظرية العامة للجريمة، وإنما باعتبارها نموذجاً تطبيقياً تتجسد فيه الأركان العامة، إلى جانب العناصر الخاصة التي يحددها النص العقابي الواجب التطبيق.

ولذلك ينقسم هذا المبحث إلى مطلبين؛ يتناول الأول البناء القانوني لجريمة الابتزاز الإلكتروني، بينما يتناول الثاني التكييف القانوني والمواجهة التشريعية والقضائية وإشكالات الإثبات الرقمي.

المطلب الأول

البناء القانوني لجريمة الابتزاز الإلكتروني

تتطلب دراسة الابتزاز الإلكتروني تحديد العناصر التي يقوم عليها نموذجها القانوني، ثم بيان كيفية تحقق الركن المادي والركن المعنوي في البيئة الرقمية. ويستوجب ذلك عدم الخلط بين الوسيلة الإلكترونية التي قد تستخدم في ارتكاب الجريمة وبين العناصر التي يتطلبها النص العقابي لقيامها.

وعليه، يتناول هذا المطلب متطلبات النموذج القانوني لجريمة الابتزاز الإلكتروني، ثم الركن المادي، وأخيراً الركن المعنوي.

الفرع الأول

متطلبات النموذج القانوني لجريمة الابتزاز الإلكتروني

يفترض الابتزاز الإلكتروني وجود محل أو مادة يستغلها الجاني في ممارسة الضغط على المجني عليه، وقد تتمثل هذه المادة في صورة أو تسجيل أو محادثة أو وثيقة أو بيانات شخصية أو غير ذلك من المحتويات الرقمية التي يحرص المجني عليه على عدم نشرها أو إتاحتها للغير[25].

ولا يشترط بالضرورة أن يحصل الجاني على هذه المادة عن طريق اختراق نظام معلوماتي؛ فقد تصل إليه من خلال علاقة سابقة مع المجني عليه، أو نتيجة إرسالها إليه طوعاً، أو عن طريق الخداع، أو نتيجة اختراق حساب أو جهاز، أو من خلال حصوله عليها من شخص آخر ومن ثم فإن طريقة الحصول على المادة الرقمية ليست في ذاتها عنصراً لازماً في جميع صور الابتزاز الإلكتروني، وإنما العبرة بالسلوك الذي يأتيه الجاني بعد حصوله عليها، وبمدى انطباق عناصر النص العقابي على ذلك السلوك وتظهر خصوصية النموذج القانوني للابتزاز الإلكتروني في أن المادة المستغلة قد تكون ذات طبيعة شخصية أو خاصة، وأن قيمة التهديد بالنسبة إلى المجني عليه تنشأ من الخوف من نشرها أو إتاحتها للغير[26] ولذلك فإن البيانات والصور والمحادثات لا تمثل مجرد وسيلة تقنية، وإنما قد تكون محل الاستغلال الذي يقوم عليه الضغط الواقع على المجني عليه وفي هذا الإطار، يجب التمييز بين البيئة الرقمية بوصفها إطاراً لارتكاب الفعل وبين المادة أو المحتوى الذي ينصب عليه الاستغلال. فالابتزاز قد يرتكب عبر تطبيقات التواصل الاجتماعي أو البريد الإلكتروني أو غيرها من الوسائل، إلا أن استعمال هذه الوسائل لا يعني أنها تمثل ركناً مستقلاً للجريمة كما أن طبيعة المحتوى المستغل تختلف من واقعة إلى أخرى؛ فقد يكون صورة شخصية، أو مقطعاً مرئياً، أو تسجيلاً صوتياً، أو محادثة خاصة، أو معلومات مالية، أو وثائق شخصية[27]. وبالتالي لا ينبغي حصر الابتزاز الإلكتروني في نوع واحد من البيانات، ما دام السلوك يحقق العناصر التي يتطلبها النص العقابي.

ومن ناحية أخرى، قد يكون حصول الجاني على المادة الرقمية مشروعاً في بدايته، ثم يتحول السلوك إلى غير مشروع عند استعمالها للتهديد أو الضغط أو الحصول على منفعة. ولذلك فإن مشروعية حيازة المادة في مرحلة سابقة لا تعني بالضرورة مشروعية استعمالها لاحقاً وبذلك يمكن القول إن متطلبات النموذج القانوني للابتزاز الإلكتروني تتمثل، بحسب النص الذي يجري التكييف بموجبه، في وجود مادة أو مصلحة محل استغلال، وسلوك تهديد أو ضغط غير مشروع، وغاية أو طلب يرتبط بهذا التهديد متى كان النص يشترطه، إلى جانب توافر الأركان العامة للجريمة[28] وهذه العناصر هي التي ينبغي أن تكون محل البحث عند تكييف الواقعة، وليس مجرد وصفها بأنها «ابتزاز إلكتروني»؛ لأن التسمية وحدها لا تكفي لقيام المسؤولية الجنائية ما لم تتوافر العناصر القانونية للجريمة.

الفرع الثاني

الركن المادي لجريمة الابتزاز الإلكتروني

يتجسد الركن المادي في جريمة الابتزاز الإلكتروني في السلوك الخارجي الذي يصدر عن الجاني، وما يرتبط به من نتيجة أو أثر قانوني بحسب طبيعة النص المنطبق. وتظهر الخصوصية هنا في أن السلوك يتم بواسطة وسيلة رقمية، وأن الدليل على وقوعه يكون غالباً محفوظاً في صورة إلكترونية.

ويمكن تناول الركن المادي من خلال العناصر الآتية:

أولاً: السلوك الإجرامي

يتمثل السلوك الإجرامي في الابتزاز الإلكتروني في توجيه تهديد أو ضغط إلى المجني عليه باستخدام وسيلة إلكترونية، بحيث يكون من شأن هذا التهديد التأثير في إرادته وحمله على الاستجابة لمطلب الجاني [29]وقد يتحقق ذلك عن طريق إرسال رسالة نصية، أو تسجيل صوتي، أو صورة، أو مقطع مرئي، أو إنشاء حساب إلكتروني واستخدامه في توجيه التهديد، أو نشر جزء من المحتوى بهدف الضغط على المجني عليه وحمله على تنفيذ الطلب[30]ولا تتوقف صفة السلوك الإجرامي على نوع التطبيق المستخدم؛ فقد يقع الفعل من خلال تطبيقات المراسلة أو منصات التواصل الاجتماعي أو البريد الإلكتروني أو غيرها من الوسائل الرقمية. فالوسيلة لا تغير في ذاتها من طبيعة السلوك، وإنما تضيف إليه خصوصية تقنية تؤثر في طريقة ارتكابه وإثباته كما قد يتخذ الابتزاز صورة تهديد بالنشر مستقبلاً، دون أن يكون الجاني قد نشر المحتوى فعلاً. وهنا ينبغي التمييز بين التهديد بالنشر وبين النشر الفعلي؛ فلكل منهما وصفه القانوني بحسب النصوص التي يمكن تطبيقها على الواقعة.

ولا يشترط كذلك أن يكون التهديد مصحوباً بعبارات صريحة في جميع الأحوال، فقد يستفاد من مضمون الرسالة أو الصور أو السياق العام للمراسلات أن المقصود هو الضغط على المجني عليه. إلا أن تقدير ذلك يبقى مسألة موضوعية تخضع لظروف كل واقعة وأدلتها.

ثانياً: النتيجة الإجرامية

تتحدد النتيجة الإجرامية وفقاً للنص العقابي الذي يجري تطبيقه. فإذا كان النص يتطلب تحقق أثر معين، وجب إثباته، أما إذا كانت الجريمة تامة بمجرد تحقق السلوك المجرّم، فلا يشترط تحقق الغاية التي كان الجاني يسعى إليها وفي جرائم التهديد والابتزاز، قد يظهر الأثر في إخافة المجني عليه أو الضغط على إرادته أو حمله على اتخاذ موقف لم يكن ليتخذه لولا التهديد ولا يلزم أن يستجيب المجني عليه فعلاً لطلب الجاني حتى يكون السلوك مجرّماً متى كان النص يجعل الجريمة قائمة بمجرد تحقق السلوك والظروف التي يتطلبها. ومن ثم فإن فشل الجاني في الحصول على المال أو المنفعة لا يعني بالضرورة انتفاء الجريمة، وإنما يتوقف الأمر على التكييف القانوني الدقيق للواقعة.

ثالثاً: العلاقة بين السلوك والنتيجة

متى كانت النتيجة عنصراً لازماً للجريمة، ينبغي إثبات العلاقة بينها وبين السلوك الصادر عن الجاني.

وتتخذ هذه العلاقة أهمية خاصة في الابتزاز الإلكتروني؛ لأن إثبات أن حالة الضغط أو الخوف نشأت عن الرسالة أو التهديد الصادر عن المتهم يتطلب أحياناً تحليل سلسلة المراسلات والاتصالات والظروف المحيطة بالواقعة كما أن تحديد مصدر الرسالة لا يكفي وحده لإثبات هوية الجاني؛ فقد يكون الحساب مستخدماً من أكثر من شخص، أو يكون قد تعرض للاختراق، أو يكون اسم المستخدم غير مطابق للهوية الحقيقية. ولهذا يجب أن تقوم نسبة الفعل إلى المتهم على مجموعة من الأدلة والقرائن الفنية والقانونية المتساندة.

الفرع الثالث

الركن المعنوي لجريمة الابتزاز الإلكتروني

تعد جريمة الابتزاز، في صورها التي تقوم على التهديد والضغط، من الجرائم العمدية التي يتطلب قيامها توافر القصد الجنائي. ويتحقق القصد، في صورته العامة، بعلم الجاني بعناصر السلوك واتجاه إرادته إلى ارتكابه [31].

أولاً: العلم

يجب أن يكون الجاني عالماً بطبيعة السلوك الذي يأتيه، وأن يدرك أنه يستخدم المادة أو المحتوى الرقمي في ممارسة ضغط غير مشروع على المجني عليه [32].

كما يجب أن يكون عالماً، بحسب ظروف الواقعة، بطبيعة المادة التي يستخدمها في التهديد وبصلة هذه المادة بالمجني عليه، وأن يكون مدركاً أن سلوكه من شأنه التأثير في إرادة المجني عليه.

ولا يشترط أن يكون الجاني ملماً بالتفصيلات القانونية للنص العقابي؛ إذ إن الجهل بالقانون لا يعد، في الأصل، عذراً لنفي المسؤولية، وإنما محل البحث هو علمه بالوقائع والعناصر المادية التي يتكون منها السلوك المجرّم.

ثانياً: الإرادة

لا يكفي مجرد العلم، وإنما يجب أن تتجه إرادة الجاني إلى ارتكاب السلوك المادي، أي إرسال التهديد أو استخدام المحتوى الرقمي بقصد الضغط على المجني عليه.

وتظهر الإرادة من ظروف الواقعة، مثل تكرار الرسائل، أو تحديد الطلب، أو ربط عدم الاستجابة بالنشر، أو إعطاء المجني عليه مهلة لتنفيذ المطلوب، أو استخدام عبارات تكشف بوضوح عن الغاية من السلوك وتزداد أهمية هذه القرائن في البيئة الرقمية؛ لأن الجاني قد يستخدم حساباً وهمياً أو اسماً مستعاراً، مما يجعل إثبات الصلة النفسية بين الشخص والفعل مرتبطاً بمجموعة من الأدلة الفنية والموضوعية.

ثالثاً: الغاية من الابتزاز

قد تتخذ غاية الجاني صورة طلب المال، أو الحصول على منفعة، أو إجبار المجني عليه على القيام بفعل معين، أو الامتناع عن فعل، أو الاستمرار في علاقة أو تواصل لا يرغب فيه غير أن تحديد الغاية لا ينبغي أن يؤدي إلى حصر الابتزاز الإلكتروني في المطالب المالية فقط؛ إذ يمكن أن تكون الغاية ذات طبيعة غير مالية، بحسب النموذج القانوني الذي يجري تطبيقه ومن ثم فإن معيار التكييف يجب أن ينصرف إلى طبيعة التهديد والسلوك والطلب والغاية التي يكشف عنها الفعل، وليس إلى كون الطلب مالياً أو غير مالي فقط.

المطلب الثاني

التكييف القانوني والمواجهة التشريعية والقضائية للابتزاز الإلكتروني

إن تحديد الأركان ومتطلبات النموذج القانوني لجريمة الابتزاز الإلكتروني يقود إلى المسألة الأكثر أهمية من الناحية العملية، وهي تحديد النص القانوني الذي يمكن تطبيقه على الواقعة في ظل التشريع العراقي وتزداد أهمية هذه المسألة بسبب عدم وجود تنظيم تشريعي عراقي خاص ومستقل يجمع صور الجرائم الإلكترونية ويحدد أحكامها بصورة تفصيلية. ولذلك يثور التساؤل حول مدى إمكانية تطبيق النصوص العامة في قانون العقوبات على الابتزاز المرتكب بواسطة الوسائل الإلكترونية، وحدود هذا التطبيق في ضوء مبدأ الشرعية الجنائية كما تقتضي الدراسة الوقوف على بعض النماذج التشريعية المقارنة، ثم بحث الموقف القضائي وإشكالات الإثبات الرقمي التي تفرضها طبيعة هذه الجريمة.

الفرع الأول

التكييف القانوني للابتزاز الإلكتروني في التشريع العراقي والمقارن

أولاً: التكييف في التشريع العراقيفي ظل عدم وجود قانون خاص ومستقل ينظم جريمة الابتزاز الإلكتروني في العراق، يثور اتجاه عملي إلى تطبيق النصوص العامة التي تتوافر عناصرها في الواقعة، ومن أبرزها النصوص

المتعلقة بالتهديد، وقد تمتد المسألة إلى نصوص أخرى بحسب طبيعة السلوك والغاية منه [33]ومن أبرز النصوص التي يمكن أن تثار في هذا السياق المادة (430) من قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، متى توافرت عناصر التهديد التي يتطلبها النص[34] وتظهر أهمية هذه المادة في الحالات التي يستخدم فيها الجاني وسيلة إلكترونية لإيصال تهديد إلى المجني عليه بقصد حمله على القيام بفعل أو الامتناع عنه أو تحقيق غرض معين ولا يعني استخدام الهاتف أو تطبيق إلكتروني أو منصة تواصل اجتماعي أن الواقعة تخرج تلقائياً عن نطاق النص التقليدي؛ إذ ينبغي النظر إلى العناصر التي جرمها النص ومقارنتها بالسلوك الواقعي[35]فإذا كان النص يجرّم التهديد في ذاته، وكان التهديد قد تحقق فعلاً، فإن الوسيلة الإلكترونية قد تكون مجرد طريقة لتنفيذ السلوك. أما إذا كان تطبيق النص يتطلب عناصر لا تتوافر في الواقعة الرقمية، فلا يجوز تجاوز النص لمجرد الرغبة في العقاب، لأن مبدأ الشرعية يحول دون القياس في التجريم أما المادة (456) من قانون العقوبات العراقي فإن إثارتها تكون بحسب ظروف الواقعة، ولا ينبغي اعتبارها نصاً عاماً للابتزاز الإلكتروني إذ يتطلب تطبيقها توافر عناصر جريمة الاحتيال التي يحددها النص، ومنها الوسيلة الاحتيالية والنتيجة التي يرتب عليها القانون المسؤولية[36] وعليه لا يصح القول إن كل ابتزاز إلكتروني يشكل بالضرورة جريمة احتيال، كما لا يصح القول إن كل ابتزاز إلكتروني يخضع للمادة (430) دون فحص عناصر الواقعة؛ وإنما يكون التكييف الصحيح نتيجة لمقارنة الوقائع الثابتة بالعناصر القانونية لكل نص وهذا يبين أن المشكلة التشريعية لا تتمثل فقط في غياب تسمية مستقلة لجريمة الابتزاز الإلكتروني، وإنما في الحاجة إلى تحديد صور السلوك الرقمي وعناصرها بصورة واضحة، بما يضمن حماية المجني عليه دون الإخلال بمبدأ الشرعية.

ثانياً: التكييف في التشريع المصري

اتجه المشرع المصري إلى تنظيم عدد من الجرائم المرتبطة باستخدام تقنية المعلومات في قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018، بما يوفر إطاراً تشريعياً خاصاً للتعامل مع بعض الاعتداءات الواقعة على الخصوصية والمحتوى الرقمي[37] وتبرز أهمية هذا التنظيم بالنسبة إلى موضوع الدراسة في أنه لا يترك التعامل مع الجرائم المرتبطة بالبيئة الرقمية للقواعد التقليدية وحدها، وإنما يتضمن نصوصاً تراعي خصوصية استخدام تقنية المعلومات في ارتكاب الفعل وتتصل المادتان (25) و(26) من القانون المذكور بحماية بعض الجوانب المرتبطة بالخصوصية والبيانات والمحتوى الرقمي، الأمر الذي يجعل التشريع المصري نموذجاً للمقارنة عند دراسة مدى الحاجة إلى نصوص خاصة في التشريع العراقي[38]ولا تعني المقارنة نقل الأحكام المصرية إلى البيئة العراقية بصورة حرفية، وإنما الاستفادة من الاتجاه التشريعي الذي يقوم على تحديد الأفعال الرقمية المجرمة بصورة أكثر وضوحاً، وربط التجريم بخصوصية الوسيلة والمحتوى عند الحاجة.

ثالثاً: التكييف في التشريع السعودي

تبنى المنظم السعودي تنظيماً خاصاً للجرائم المعلوماتية من خلال نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/17) لعام 1428هـ، الذي تضمن نصوصاً تعالج مجموعة من الأفعال المرتكبة باستخدام

الحاسب الآلي والشبكات المعلوماتية[39] وتكمن أهمية النموذج السعودي بالنسبة إلى الدراسة في إدخاله بعض الأفعال المرتبطة بالتهديد والابتزاز ضمن نطاق التجريم المعلوماتي[40] ، وهو ما يوضح اتجاه التشريع الخاص إلى تحديد السلوك الإلكتروني بصورة مباشرة بدلاً من الاكتفاء بتطبيق النصوص التقليدية ومن ثم تكشف المقارنة بين النماذج العراقية والمصرية والسعودية عن اختلاف في أسلوب المعالجة؛ فبينما يعتمد التطبيق العراقي، عند غياب النص الخاص، على التكييف وفق القواعد العامة بحسب ظروف الواقعة، اتجهت التشريعات المقارنة إلى وضع تنظيمات خاصة تستوعب طبيعة الجرائم المرتكبة باستخدام التقنية[41].

الفرع الثاني

الموقف القضائي وإشكالات الإثبات الرقمي

لا تكتمل دراسة الابتزاز الإلكتروني بمجرد تحديد النص العقابي الممكن تطبيقه، لأن الجانب العملي من هذه الجرائم يرتبط بصورة وثيقة بإمكان إثبات الواقعة ونسبتها إلى مرتكبها فالرسالة الإلكترونية أو الحساب الرقمي أو الصورة أو التسجيل قد يكون دليلاً مهماً في الدعوى، إلا أن قيمته الإثباتية لا تنشأ من وجوده المجرد، وإنما من إمكان التحقق من سلامته ومصدره ونسبته إلى الشخص المتهم.

أولاً: الموقف القضائي

تواجه المحاكم العراقية قضايا تتعلق بالتهديد والابتزاز المرتكب بواسطة وسائل الاتصال الحديثة، الأمر الذي أدى إلى ظهور تطبيقات قضائية تتعامل مع الرسائل والحسابات والمحتويات الرقمية بوصفها وسائل يمكن أن تكون محلاً للفحص والاستدلال وفي هذا السياق، تبرز أهمية التكييف القضائي للواقعة؛ إذ يتعين على المحكمة تحديد النص العقابي المنطبق بعد التحقق من عناصر السلوك، وعدم الاكتفاء بوصف الواقعة بأنها «ابتزاز إلكتروني«كما يجب التحقق من نسبة الحساب أو الرقم أو الجهاز إلى المتهم، لأن مجرد وجود حساب باسم معين لا يكفي، في ذاته، لإثبات أن الشخص المعني هو من ارتكب الفعل، ما لم تؤيده أدلة أخرى.

ثانياً: خصوصية الدليل الرقمي

يتميز الدليل الرقمي بخصائص تختلف عن كثير من الأدلة التقليدية؛ فهو قابل للنسخ والنقل والتعديل والحذف، وقد توجد البيانات الأصلية في جهاز، بينما تظهر نسخة منها في جهاز آخر أو خادم أو منصة إلكترونية.

وتثير هذه الخصائص عدة إشكالات، أهمها:

1 .سهولة التعديل والحذف:

يمكن حذف الرسائل أو تعديل محتواها أو تغيير الحساب المستخدم، مما يفرض ضرورة المحافظة على الدليل منذ لحظة ضبطه وفحصه.

2 .صعوبة تحديد هوية المستخدم:

قد يستخدم الشخص حساباً باسم مستعار أو رقماً غير مسجل باسمه، كما يمكن استخدام أجهزة أو حسابات مملوكة لأشخاص آخرين.

3 .تعدد مصادر البيانات:

قد تكون البيانات موزعة بين الهاتف والحاسب والخادم والمنصة الإلكترونية، مما يجعل جمع الأدلة مرتبطاً أحياناً بجهات متعددة.

4 .الحاجة إلى الخبرة الفنية:

قد يتعذر على المحكمة، دون مساعدة فنية متخصصة، التحقق من سلامة البيانات أو طريقة استخراجها أو نسبتها إلى الجهاز أو الحساب محل البحث.

ولهذا فإن قيمة الدليل الرقمي تتطلب إجراءات فنية وقانونية تضمن المحافظة على سلامته منذ جمعه وحتى تقديمه إلى المحكمة.

ثالثاً: نسبة الفعل الرقمي إلى مرتكبه

تعد مسألة نسبة الفعل إلى الجاني من أهم إشكالات الإثبات في الابتزاز الإلكتروني. فإثبات أن رسالة تهديد أرسلت من حساب معين لا يعني بالضرورة أن صاحب الحساب هو الشخص الذي كتبها وأرسلها ومن هنا ينبغي أن تستند نسبة الفعل إلى مجموعة من القرائن، مثل بيانات الجهاز، وأرقام الاتصال، وسجل الدخول، والبيانات الفنية المتاحة، ومحتوى المراسلات، فضلاً عن أي اعترافات أو أدلة أخرى تتصل بالواقعة ولا ينبغي التعامل مع عنوان إلكتروني أو اسم مستخدم واحد باعتباره دليلاً حاسماً في جميع الأحوال، لأن البيئة الرقمية تسمح باستخدام حسابات مشتركة أو منتحلة أو مخترقة وبذلك يصبح الدليل الرقمي جزءاً من منظومة إثبات متكاملة، وليس دليلاً منفرداً بمعزل عن بقية الأدلة.

رابعاً: أثر إشكالات الإثبات في المواجهة التشريعية

تكشف الصعوبات السابقة أن مواجهة الابتزاز الإلكتروني لا تتطلب فقط إنشاء نص عقابي خاص، وإنما تحتاج كذلك إلى تنظيم متكامل لجمع الدليل الرقمي وضبطه وفحصه والمحافظة على سلامته.

كما ينبغي أن يحدد التنظيم التشريعي الجهات المختصة بإجراء الفحص الفني، والضوابط التي تحكم الحصول على البيانات، وضمانات الأشخاص محل الإجراءات، وكيفية تقديم الدليل الرقمي أمام المحكمة ومن ثم فإن المعالجة التشريعية المتكاملة ينبغي ألا تقتصر على تحديد العقوبة، بل يجب أن تشمل التجريم، والتكييف، وإجراءات البحث والتحري، وضبط الأدلة الرقمية، والاستعانة بالخبرة الفنية، وضمان سلامة الدليل وحجيته وهذا يمثل أحد أهم أوجه الاختلاف بين التعامل مع الجريمة الإلكترونية وبين الجرائم التقليدية، ويؤكد أن التطور التقني يفرض تطويراً متوازياً في قواعد التجريم والإثبات والإجراءات.

الخاتمة

بعد أن تناول البحث الأركان العامة للجريمة الإلكترونية، وحدد موقع متطلبات النموذج القانوني ضمن البناء القانوني للجريمة، ثم طبق ذلك على جريمة الابتزاز الإلكتروني، وانتهى إلى بحث التكييف القانوني لهذه الجريمة وإشكالات إثباتها في البيئة الرقمية، يمكن استخلاص مجموعة من النتائج التي تجيب عن الإشكالية الرئيسة للبحث، وما يتفرع عنها من تساؤلات.

أولاً: الاستنتاجات

1 .خلص البحث إلى أن مصطلح الجريمة الإلكترونية هو المصطلح الأوسع في نطاق هذه الدراسة، ويقصد به الأفعال غير المشروعة التي ترتكب باستخدام تقنية المعلومات أو تستهدف البيانات أو الأنظمة أو المحتوى الرقمي، بينما يمثل الابتزاز الإلكتروني صورة تطبيقية محددة من صور السلوك الإجرامي الذي يستغل الوسائل الرقمية للضغط على المجني عليه وتهديده، ومن ثم لا يصح استعمال المصطلحين على أنهما مترادفان.

2 .تبين أن اختلاف المصطلحات بين الجريمة الإلكترونية والجريمة المعلوماتية والجريمة السيبرانية لا يؤدي بالضرورة إلى اختلاف جوهري في جميع الاستخدامات الفقهية، إلا أن توحيد المصطلح داخل البحث يظل ضرورياً لمنع الالتباس وتحديد نطاق الدراسة. ولذلك اعتمد البحث مصطلح الجريمة الإلكترونية باعتباره المصطلح الرئيس، واستعمل مصطلح الابتزاز الإلكتروني للدلالة على النموذج التطبيقي محل الدراسة.

3 .أظهرت الدراسة أن البيئة الرقمية لا تمثل ركناً رابعاً مستقلاً من أركان الجريمة، وإنما ترتبط في بعض النماذج بمتطلبات النموذج القانوني للجريمة، سواء تعلق الأمر بمحل السلوك أو بالوسيلة التي ارتكب بها الفعل. وبذلك لا ينبغي الخلط بين البيئة التي تقع فيها الجريمة وبين الركن الشرعي والمادي والمعنوي.

4 .تبين أن غياب النص الخاص بالجرائم الإلكترونية في العراق لا يعني انعدام إمكانية مساءلة مرتكب بعض الأفعال الرقمية، متى أمكن إخضاع الواقعة لنص عقابي قائم دون توسع أو قياس في التجريم. غير أن هذا الحل يظل محدوداً بحدود النص القائم ومدى استيعابه للعناصر الفعلية للجريمة الرقمية.

5 .أظهر البحث أن المادة (430) من قانون العقوبات العراقي يمكن أن تكون محلاً للتطبيق في بعض صور التهديد المرتكب إلكترونياً متى توافرت عناصرها، إلا أن ذلك لا يعني اعتبارها نصاً خاصاً بالابتزاز الإلكتروني، وإنما يمثل تكييفاً للواقعة وفق النص التقليدي الذي تتوافر عناصره فيها.

6 .كما تبين أن الاستناد إلى المادة (456) من قانون العقوبات العراقي لا يكون صحيحاً لمجرد وجود طلب مالي في واقعة الابتزاز، وإنما يتطلب تحقق عناصر الاحتيال التي يقوم عليها النص. ولذلك ينبغي أن يسبق التكييف تحديد دقيق لطبيعة السلوك والأداة المستخدمة والنتيجة التي ترتبت عليه.

7 .أثبتت المقارنة التشريعية أن وجود نصوص خاصة بالجرائم المرتبطة بتقنية المعلومات يوفر وضوحاً أكبر في تحديد السلوك المجرّم وحدود المسؤولية الجنائية، ويقلل من الحاجة إلى تحميل النصوص التقليدية وقائع لم تكن البيئة التقنية القائمة عند تشريعها معروفة على صورتها الحالية.

8 .توصل البحث إلى أن خصوصية الابتزاز الإلكتروني لا تكمن في مجرد استخدام الهاتف أو شبكة الإنترنت، وإنما في اجتماع التهديد أو الضغط غير المشروع مع استغلال محتوى أو بيانات رقمية أو معلومات من شأنها التأثير في إرادة المجني عليه.

9 .تبين أن حصول الجاني على المادة الرقمية محل الابتزاز ليس بالضرورة عن طريق الاختراق؛ فقد يحصل عليها من خلال علاقة سابقة أو إرسال طوعي أو خداع أو نقل من شخص آخر، الأمر الذي يستوجب عدم حصر مفهوم الابتزاز الإلكتروني في حالات اختراق الحسابات والأجهزة.

10 .كشفت الدراسة أن أهم إشكالات الابتزاز الإلكتروني عملياً تتمثل في إثبات نسبة الفعل إلى مرتكبه؛ إذ إن إثبات صدور الرسالة من حساب أو رقم معين لا يكفي دائماً لإثبات أن المتهم هو الشخص الذي أنشأ الرسالة وأرسلها، ما لم تتساند معه أدلة وقرائن فنية أخرى.

11 .أظهرت الدراسة أن الدليل الرقمي يتمتع بخصوصية تختلف عن الأدلة التقليدية بسبب قابليته للنسخ والتعديل والحذف والنقل، الأمر الذي يجعل سلامة إجراءات جمعه وحفظه وفحصه عنصراً مهماً في تقدير قيمته الإثباتية.

12 .انتهى البحث إلى أن مواجهة الابتزاز الإلكتروني لا تتحقق بالعقوبة وحدها، وإنما تحتاج إلى منظومة متكاملة تجمع بين وضوح التجريم، ودقة التكييف، وتنظيم إجراءات الحصول على الدليل الرقمي، والاستعانة بالخبرة الفنية، وضمان سلامة الأدلة المقدمة إلى القضاء.

ثانياً: المقترحات

في ضوء النتائج المتقدمة، يقترح البحث ما يأتي:

1 .أن يتضمن التشريع العراقي الخاص بالجرائم الإلكترونية تعريفاً تشريعياً واضحاً يميز بين الجريمة الإلكترونية بوصفها مفهوماً عاماً وبين صورها الخاصة، ومنها الابتزاز الإلكتروني، منعاً لتعدد التكييفات الناتجة عن اختلاف المصطلحات.

2 .أن يعالج التشريع العراقي الابتزاز الإلكتروني باعتباره نموذجاً مستقلاً من النماذج الإجرامية، مع تحديد عناصره بصورة دقيقة، ولا سيما طبيعة التهديد والمحتوى المستغل والطلب أو الغاية التي يسعى الجاني إلى تحقيقها.

3 .أن يتجنب النص التشريعي حصر الابتزاز الإلكتروني في المطالب المالية؛ لأن التطور العملي للظاهرة يظهر صوراً يكون فيها الهدف إجبار المجني عليه على فعل أو الامتناع عن فعل أو الاستمرار في علاقة أو تقديم منفعة غير مالية.

4 .أن يراعي التشريع الجديد الفصل بين التجريم الموضوعي وقواعد الإثبات والإجراءات الرقمية، بحيث لا يكتفى بإضافة عقوبات جديدة، وإنما توضع قواعد واضحة للتعامل مع الأدلة الرقمية منذ لحظة الحصول عليها وحتى عرضها أمام المحكمة.

5 .أن ينظم المشرع العراقي إجراءات حفظ الدليل الرقمي بطريقة تمنع العبث بمحتواه، وأن يحدد المسؤولية الفنية عن استخراجه وحفظه، بما يسمح للمحكمة بالتحقق من سلامة الدليل ومصدره وتسلسل حيازته.

6 .أن يُعتمد في العمل القضائي والفني على أكثر من مؤشر لإثبات نسبة الحساب أو الرسالة إلى المتهم، وعدم الاكتفاء باسم الحساب أو رقم الهاتف وحده متى كانت ظروف الواقعة تسمح باحتمال استعمال الحساب من شخص آخر.

7 .إنشاء آلية فنية موحدة لتوثيق الأدلة الرقمية المتعلقة بالابتزاز الإلكتروني، تتضمن حفظ النسخة الأصلية للبيانات وتسجيل إجراءات استخراجها وفحصها، بما يقلل من المنازعات المتعلقة بسلامة الدليل أمام القضاء.

8 .تعزيز التنسيق المؤسسي بين الجهات القضائية والفنية المختصة بالجرائم الإلكترونية، بحيث لا يكون التعامل مع الدليل الرقمي مقتصراً على الجانب الأمني، وإنما يرتبط منذ البداية بالمتطلبات القانونية اللازمة لقبوله وتقييمه قضائياً.

9 .أن يوجه التطوير التشريعي نحو معالجة مشكلة الاختلاف بين سرعة تطور الوسائل الرقمية وبطء النصوص القانونية، وذلك من خلال صياغة النصوص بطريقة تستوعب الوسائل التقنية المستحدثة دون الحاجة إلى تعديل القانون عند ظهور كل تطبيق أو وسيلة جديدة.

10. أن يركز أي تنظيم مستقبلي للجرائم الإلكترونية على تحقيق التوازن بين حماية الأفراد من الابتزاز والاعتداءات الرقمية وبين ضمانات المتهم، ولا سيما في إجراءات الوصول إلى الأجهزة والحسابات والبيانات الخاصة.

-الهوامش :

[1] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت: دراسة في القانون الجنائي المقارن، دار المطبوعات الجامعية، الإسكندرية، 2003.
[2] محمد حماده مرهج الهيتي، جرائم الحاسوب والأبعاد الفنية والقانونية للمواجهة، ط1، دار المناهج للنشر والتوزيع، عمّان، 2005
[3] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2002.
[4] عبد الفتاح مراد، شرح جرائم الكمبيوتر والإنترنت والوسائل الفنية والقانونية لمواجهتها، دار الكتب والوثائق المصرية، الإسكندرية، 2005
[5] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، ولا سيما المادة (430)
[6] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، 2002، ص 17
[7] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت: دراسة في القانون الجنائي المقارن، دار المطبوعات الجامعية، الإسكندرية، 2003، ص 25
[8] محمد حمادة مرهج الهيتي، جرائم الحاسوب والأبعاد الفنية والقانونية للمواجهة، ط1، دار المناهج للنشر والتوزيع، عمّان، 2005، ص 31
[9]محمد حمادة مرهج الهيتي، جرائم الحاسوب والأبعاد الفنية والقانونية للمواجهة، ط1، دار المناهج للنشر والتوزيع، عمّان، 2005
[10] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2003، ص155
[11] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، 2004، ص بيانات الكتاب والناشر والسنة مؤكدة ببليوغرافية.
[12] مشروع قانون مكافحة الجرائم الإلكترونية العراقي لسنة 2011.
[13] مشروع قانون الجرائم المعلوماتية العراقي لسنة 2019
[14] مشروع قانون مكافحة الجرائم الإلكترونية العراقي لسنة 2021
[15] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل
[16] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، المادة (28)، والمادة (29).
[17] علي حسين خلف، وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، ص 138 وما بعدها
[18] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2002.
[19] علي حسين خلف، وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات،العاتك لصناعة ص 138-147.
[20] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، المادة (29)، مع مراعاة النص الخاص الواجب التطبيق على الواقعة
[21] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، المادة (1/29).
[22] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، المواد (33–35).
[23]عماد عبد الله، «التكييف القانوني للجريمة»، مجلس القضاء الأعلى العراقي، 2022/7/26.
[24] محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2003، ص 147–155.
[25] طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي، ص 54–59.

[26] ممدوح رشيد مشرف الرشيد، «الحماية الجنائية للمجني عليه من الابتزاز»، المجلة العربية للدراسات الأمنية، مجلد 33، العدد 70، الرياض، 2017، ص 199.

[27]ممدوح رشيد مشرف الرشيد، «الحماية الجنائية للمجني عليه من الابتزاز»، المجلة العربية للدراسات الأمنية، مجلد 33، العدد 70، الرياض، 2017، ص 199

[28] طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي، ص 54–59.

[29] طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي، ص 96–103.

[30] حسين عباس حميد، «جريمة الابتزاز الإلكتروني»، مجلة القانون للدراسات والبحوث القانونية، المجلد 23، العدد 22، جامعة ذي قار، كلية القانون، 2021، ص 583–606.

[31] طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة كركوك، 2022، ص 103–104.

[32] طارق نامق محمد رضا، المسؤولية الجنائية عن الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي، ص 104 وما بعدها.

[33] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، ولا سيما المواد (430–432) الخاصة بجريمة التهديد.

[34] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، المادة (1/430).

[35] ينظر: قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، المادة (1/430)؛ ومبدأ الشرعية الجنائية المقرر في المادة (1) من القانون ذاته.

[36] قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، المادة (456).

[37] قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.

[38] قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018، المادتان (25) و(26).

[39] نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ الموافق 2007/3/26م.

[40] نظام مكافحة جرائم المعلوماتية السعودي، المادة (2/3).

[41] ينظر: قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل، المواد (430–432)؛ قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018؛ نظام مكافحة جرائم المعلوماتية السعودي، ولا سيما المادة (3).

المراجع

أولاً: الكتب والمؤلفات

1 .حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2002.

2 .مراد، عبد الفتاح، شرح جرائم الكمبيوتر والإنترنت والوسائل الفنية والقانونية لمواجهتها، دار الكتب والوثائق المصرية، الإسكندرية، 2005.

3 .الهيتي، محمد حماده مرهج، جرائم الحاسوب والأبعاد الفنية والقانونية للمواجهة، ط1، دار المناهج للنشر والتوزيع، عمّان، 2005.

4 .الرومي، محمد أمين، جرائم الكمبيوتر والإنترنت: دراسة في القانون الجنائي المقارن، دار المطبوعات الجامعية، الإسكندرية، 2003.

5 .عبد القادر، نهلا، الجرائم المعلوماتية: دراسة في ضوء السياسة الجنائية الحديثة، ط1، دار الثقافة للنشر والتوزيع، عمّان، 2010.

6. د. ماهر عبد الشويش، الأدلة الرقمية وحجيتها في الإثبات الجنائي، مجلة العلوم القانونية - جامعة بغداد، المجلد 35، العدد 2، 2020، ص 47.

ثانياً: التشريعات العراقية

1 .قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل.

2 .قانون أصول المحاكمات الجزائية العراقي رقم (23) لسنة 1971 المعدل.

3 .دستور جمهورية العراق لسنة 2005.

4 .مشروع قانون مكافحة الجرائم الإلكترونية العراقي لسنة 2011.

5 .مشروع قانون الجرائم المعلوماتية العراقي لسنة 2019.

6 .مشروع قانون مكافحة الجرائم الإلكترونية العراقي لسنة 2021.

7 .المسودة الحديثة لمشروع قانون الجرائم المعلوماتية في العراق، بحسب النسخة المعتمدة في الدراسة.

ثالثاً: التشريعات العربية المقارنة

1 .قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.

2 .نظام مكافحة الجرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم (م/17) لسنة 1428هـ.

رابعاً: التقارير والدراسات

1 .مجلس النواب العراقي، دائرة البحوث والدراسات، نحو استراتيجية وطنية لتشريع قانون جرائم المعلوماتية في العراق، المجلد الرابع، 2021.

2 .الدراسات والتقارير المتعلقة بالتشريعات العراقية الخاصة بمكافحة الجرائم المعلوماتية ومشروعات القوانين ذات الصلة.

خامساً: التطبيقات والقرارات القضائية

1 .قرارات وتطبيقات المحاكم العراقية المتعلقة بجرائم التهديد والابتزاز المرتكبة باستخدام الوسائل الإلكترونية.

2. قرار محكمة تحقيق الكرخ المختصة بقضايا الجرائم الإلكترونية، القرار رقم (1284/ت/2022)، في 2022/5/14، غير منشور.

References

First: Books and Legal Studies

1. Abdel Fattah Bayoumi Hijazi, Criminal Evidence and Forgery in Computer and Internet Crimes, Dar Al-Kutub Al-Qanuniyya, El-Mahalla El-Kubra, Egypt, 2002.

2. Abdel Fattah Murad, Explanation of Computer and Internet Crimes and the Technical and Legal Means of Combating Them, Dar Al-Kutub wa Al-Wathaiq Al-Misriyya, Alexandria, 2005.

3. Muhammad Hamada Murhij Al-Hiti, Computer Crimes and the Technical and Legal Dimensions of Combating Them, 1st ed., Dar Al-Manahij for Publishing and Distribution, Amman, 2005.

4. Muhammad Amin Al-Rumi, Computer and Internet Crimes: A Study in Comparative Criminal Law, Dar Al-Matboo'at Al-Jami'iyya, Alexandria, 2003.

5. Nahla Abdel Qader, Informatics Crimes: A Study in Light of Modern Criminal Policy, 1st ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, 2010.

Second: Iraqi Legislation

1. 6. Iraqi Penal Code No. (111) of 1969, as amended.
2. 7. Iraqi Code of Criminal Procedure No. (23) of 1971, as amended.
3. 8. Constitution of the Republic of Iraq of 2005.
4. 9. Iraqi Draft Law on Combating Cybercrimes of 2011.
5. 10. Iraqi Draft Informatics Crimes Law of 2019.
6. 11. Iraqi Draft Law on Combating Cybercrimes of 2021.
7. 12. The Recent Draft Iraqi Cybercrime Law.

Third: Comparative Legislation

1. . Egyptian Anti-Information Technology Crimes Law No. (175) of 2018.
2. Saudi Anti-Cybercrime Law, issued by Royal Decree No. (M/17) of 1428 AH.

Fourth: Reports and Research

1. Iraqi Council of Representatives, Research and Studies Directorate, Towards a National Strategy for Enacting an Informatics Crimes Law in Iraq, Vol. 4, 2021.

Fifth: Judicial Decisions

1. Decision of Al-Karkh Investigation Court Specializing in Cybercrime Cases, Decision No. (1284/T/2022), dated 14 May 2022, unpublished.