السياسة الجنائية الوقائية في مكافحة جريمة الابتزاز الإلكتروني في التشريع العراقي

أ.د .محمد علي حاجي ده آبادي
استاذ مشارك، قسم القانون الجنائي،جامعة قم،محافظة قم،ايران
Dr-hajidehabadi@yahoo.com

م.م .علي حسين أحمد الباوي
طالب دكتوراه ،قانون جنائي، كلية الحقوق ،جامعة قم،محافظة قم،الجمهورية الاسلامية ايران
ali.hussein@uomustansiriyah.edu.iq

الكلمات المفتاحية: السياسة الجنائية الوقائية، الابتزاز الإلكتروني، الجريمة الإلكترونية، التشريع العراقي، الأدلة الرقمية، العدالة الجنائية.

كيفية اقتباس البحث
آبادي، محمد علي حاجي ده ، علي حسين أحمد الباوي ، السياسة الجنائية الوقائية في مكافحة جريمة الابتزاز الإلكتروني في التشريع العراقي،مجلة مركز بابل للدراسات الانسانية، تشرين الثاني ٢٠٢٦، المجلد:١٦ ،العدد:١١ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نَسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Preventive Criminal Policy in Combating the Crime of Cyber-Extortion under Iraqi Legislation

Prof.Dr.Mohammad Ali Haji Deh Abadi
Associate Professor, Department of Criminal Law, University of Qom, Qom, Iran
Asst.Lecturer. Ali Hussein Ahmed
Ph.D. Student, Criminal Law, Faculty of Law, University of Qom, Qom, Islamic Republic of Iran

Keywords : Preventive Criminal Policy, Cyber Extortion, Cybercrime, Iraqi Legislation, Digital Evidence, Criminal Justice.

How To Cite This Article
Abadi, Mohammad Ali Haji Deh, Ali Hussein Ahmed, Preventive Criminal Policy in Combating the Crime of Cyber-Extortion under Iraqi Legislation,Journal Of Babylon Center For Humanities Studies, November 2026,Volume:16,Issue 11.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Abstract

The rapid advancement of digital technologies has created a new criminal landscape that transcends the boundaries of traditional criminalization. Among the emerging cybercrimes, cyber extortion has become one of the most serious threats to personal security, privacy, and social stability due to its ease of commission, cross-border nature, and the complexity of its detection and prosecution. In this context, the effectiveness of criminal policy can no longer be measured solely by its ability to impose criminal sanctions after an offence has occurred; rather, it should be assessed by its capacity to establish a preventive legal framework capable of reducing criminal opportunities through integrated legislative, institutional, and technological mechanisms. Against this

background, this study examines the preventive criminal policy adopted by the Iraqi legal system as an appropriate framework for addressing cyber extortion by evaluating the responsiveness of Iraqi criminal legislation to the challenges posed by the digital environment and assessing its effectiveness in preventing this evolving form of cybercrime. The study adopts an analytical legal approach based on an examination of the relevant Iraqi legislative provisions, supported by an analysis of contemporary jurisprudential opinions and judicial trends, with the aim of evaluating the adequacy of the existing legal framework in addressing the legal and technical characteristics of cyber extortion. The analysis demonstrates that, although the general provisions of the Iraqi Penal Code provide a limited legal basis for prosecuting certain forms of cyber extortion, they do not constitute a comprehensive legislative response capable of addressing the distinctive nature of cybercrime. This legislative gap is further exacerbated by the absence of a specialized cybercrime law, inadequate regulation of digital evidence, and the limited effectiveness of preventive measures based on institutional coordination, digital awareness, and international cooperation.

The study concludes that strengthening the effectiveness of Iraq's preventive criminal policy requires a shift from a reactive punitive model to a proactive legislative approach that emphasizes prevention, legal modernization, enhanced protection of digital evidence, specialized investigative capacities, and broader national and international cooperation. Such reforms would establish a more adaptive legal framework capable of effectively reducing cyber extortion and enhancing the overall efficiency of the criminal justice system in responding to the challenges of the digital age.

الملخص

ان التحول الرقمي المتسارع قد فرض واقعا إجراميا جديدا تجاوز الحدود التقليدية للتجريم وأصبحت جريمة الابتزاز الإلكتروني من أكثر الجرائم قدرة على تهديد الأمن الشخصي والاجتماعي والاقتصادي بفعل سهولة ارتكابها وسرعة انتشارها وتعقيد وسائل إثباتها وفي هذا السياق لم يعد نجاح السياسة الجنائية يقاس بقدرتها على توقيع العقوبة فحسب وإنما بمدى قدرتها على بناء منظومة وقائية تستبق الجريمة وتحد من فرص وقوعها عبر أدوات تشريعية ومؤسساتية وتقنية متكاملة ومن هذا المنطلق تتناول هذه الدراسة السياسة الجنائية الوقائية في التشريع العراقي بوصفها الإطار القانوني الأكثر ملاءمة لمواجهة جرائم الابتزاز الإلكتروني، من خلال

تحليل مدى استجابة المنظومة التشريعية العراقية للتحولات التي فرضتها البيئة الرقمية وقياس قدرتها على تحقيق الوقاية الجنائية في مواجهة أنماط إجرامية تتسم بالتطور المستمر والتخفي العابر للحدود.

ويقوم البحث على تحليل النصوص القانونية النافذة، ومناقشة الاتجاهات الفقهية والقضائية ذات الصلة للكشف عن مدى كفاية البنية التشريعية العراقية في استيعاب الخصائص القانونية والتقنية لجريمة الابتزاز الإلكتروني ومدى انسجامها مع متطلبات السياسة الجنائية الوقائية الحديثة ويبين التحليل أن الاعتماد على النصوص العامة في قانون العقوبات رغم أهميته في توفير حماية جزئية لا يحقق استجابة تشريعية متكاملة تتناسب مع الطبيعة المتغيرة للجرائم الإلكترونية في ظل استمرار غياب تنظيم تشريعي متخصص يعالج الجوانب الموضوعية والإجرائية المرتبطة بالدليل الرقمي وأساليب التحري والتحقيق الإلكتروني فضلاً عن محدودية التدابير الوقائية القائمة على التوعية والتنسيق المؤسسي والتعاون الدولي.

وتؤكد الدراسة أن تعزيز فاعلية السياسة الجنائية الوقائية يقتضي الانتقال من مفهوم المواجهة العقابية اللاحقة إلى نموذج تشريعي استباقي يقوم على تحديث البنية القانونية وإقرار تنظيم خاص بالجرائم الإلكترونية وتعزيز الحماية القانونية للدليل الرقمي ورفع كفاءة الجهات المختصة في مجال التحقيق الرقمي وتوسيع برامج الوقاية المجتمعية بما يحقق استجابة قانونية أكثر مرونة وقدرة على الحد من جريمة الابتزاز الإلكتروني في البيئة الرقمية ويعزز فعالية العدالة الجنائية في مواجهة هذا النمط المتطور من الإجرام.

المقدمة

تفرض جريمة الابتزاز الإلكتروني إعادة النظر في الأسلوب الذي تتبعه السياسة الجنائية في مواجهة الجرائم المستحدثة لأن التدخل بعد وقوع الضرر لا يحقق دائما الحماية المطلوبة ولا سيما عندما يتعلق الأمر بمحتوى رقمي يمكن نسخه ونشره خلال مدة قصيرة فقد تتمكن الجهات المختصة من تحديد الجاني ومعاقبته من دون أن تتمكن من إزالة الآثار التي خلفتها الجريمة أو منع استمرارها ولهذا لم يعد نجاح السياسة الجنائية مرتبطا بحجم العقوبة فقط وإنما بمدى قدرتها على التدخل المبكر ومنع الخطر قبل تحوله إلى ضرر يصعب تداركه.

ولا تقوم جريمة الابتزاز الإلكتروني على التهديد المجرد وحده بل على استغلال حالة القلق التي يعيشها المجني عليه نتيجة اعتقاده أن الجاني يملك محتوى يمكن أن يضر بخصوصيته أو سمعته أو مركزه الاجتماعي فقد يكون المحتوى حقيقيا أو معدلا أو مصطنعا ومع ذلك يبقى قادرا على التأثير في إرادة الضحية متى ظهر بصورة قابلة للتصديق ويستفيد الجاني من سهولة حفظ المواد الرقمية ونسخها وإعادة تداولها فيجعل منها وسيلة ضغط متجددة تمكنه من تكرار مطالبه حتى بعد استجابة المجني عليه.

وتكشف الطبيعة المستمرة لهذه الجريمة أن الوقاية منها لا يمكن أن تعتمد على إجراء واحد أو جهة واحدة وإنما تحتاج إلى سياسة جنائية تتوزع أدواتها على المراحل التي تمر بها الواقعة فتبدأ بتقليل فرص الحصول غير المشروع على البيانات ثم تنتقل إلى اكتشاف التهديد في وقت مبكر وتوفير طرق آمنة للإبلاغ عنه وتنتهي بحفظ الأدلة ووقف انتشار المحتوى وحماية المجني عليه من استمرار الضغط وبذلك تصبح الوقاية جزءا من المواجهة الجنائية وليست مجرد تدبير يسبق التجريم والعقاب

ولا يصح أن تقتصر الوقاية على مطالبة الأفراد بالحذر في استعمال الوسائل الرقمية لأن هذا الاتجاه قد يؤدي إلى تحميل المجني عليه مسؤولية الجريمة بدلا من توفير الحماية له وإنما ينبغي أن تتولى الدولة ومؤسساتها والمنصات الرقمية جانبا أساسيا من هذه المسؤولية من خلال تطوير النصوص القانونية والإجراءات الفنية وتدريب الجهات المختصة وضمان سرعة الاستجابة للشكاوى مع المحافظة على سرية بيانات الضحايا ومع أهمية التدخل الوقائي فإنه يجب أن يبقى في حدود القانون لأن مواجهة الابتزاز الإلكتروني لا تسوغ التوسع غير المنضبط في المراقبة أو جمع البيانات ولهذا تقوم السياسة الجنائية المتوازنة على تحقيق الحماية من دون التضحية بالحقوق والحريات وعلى تسريع الإجراءات من دون إهدار ضماناتها ومن هذا المنطلق يتناول البحث السياسة الجنائية الوقائية في مواجهة الابتزاز الإلكتروني لبيان مدى قدرتها على منع الجريمة والحد من آثارها والكشف عن مواطن القصور فيها وصولا إلى بناء مواجهة قانونية تسبق الضرر بدلا من أن تكتفي بملاحقته بعد وقوعه.

أولا / موضوع البحث

ينصب موضوع البحث على تحليل السياسة الجنائية الوقائية في مواجهة جريمة الابتزاز الإلكتروني في التشريع العراقي ويبحث في مدى ملاءمة النصوص العقابية النافذة وبخاصة

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 11
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

أحكام التهديد في المواد (430–432) وبعض النصوص الأخرى بحسب عناصر الواقعة لتوفير حماية ذات بعد وقائي كما يتناول دور الإبلاغ المبكر وحفظ الدليل الرقمي وتخصيص المؤسسات التوعوية والتعاون العابر للحدود ويقتصر نطاق البحث على المواجهة الجنائية الوقائية ولا يتناول المسؤولية المدنية أو التنظيم التقني للمنصات إلا بالقدر المتصل مباشرة بموضوع الدراسة.

ثانياً :أهمية البحث

تنبع الأهمية العلمية للبحث من محاولة تأصيل الصلة بين السياسة الجنائية الوقائية وخصوصية الابتزاز الإلكتروني بدلا من حصر الدراسة في الوصف العقابي للجريمة وتظهر أهميته القانونية في اختبار مدى كفاية النصوص العراقية النافذة في استيعاب السلوك الرقمي دون التوسع في التفسير على حساب مبدأ الشرعية أما أهميته العملية فتتمثل في تحديد نقاط التدخل التي يمكن أن تمنع استمرار الجريمة أو تقلل آثارها ولا سيما الإبلاغ المبكر وحفظ الدليل وسرعة الإحالة والتنسيق مع المؤسسات كما تكتسب الدراسة أهمية مجتمعية بسبب ما يثيره الابتزاز من خوف وذعر قد يدفعان المجني عليه إلى التأخر في الإبلاغ.

ثالثا/ مشكلة البحث

تتمثل مشكلة البحث في وجود فجوة بين الطبيعة المتسارعة والمتغيرة للابتزاز الإلكتروني وبين اعتماد المواجهة في جانب مهم منها على نصوص عامة صيغت قبل شيوع البيئة الرقمية الحديثة ولا يعني ذلك انعدام الأساس القانوني للملاحقة بل يثير إشكالا أدق يتعلق بمدى قدرة النصوص النافذة والاليات المؤسسية على تحقيق وظيفة وقائية تتجاوز العقاب اللاحق إلى منع استمرار الضرر وحفظ الدليل والاستجابة المبكرة وعليه تتمحور المشكلة حول السؤال الرئيس الآتي إلى أي مدى تحقق السياسة الجنائية العراقية النافذة وقاية فعالة من جريمة الابتزاز الإلكتروني وما أوجه القصور التشريعي والإجرائي والمؤسسي التي تحد من هذه الفاعلية؟

رابعاً :أسئلة البحث

يتفرع عن السؤال الرئيس الأسئلة الآتية

(1) ما المقصود بالسياسة الجنائية الوقائية، وما حدود تمييزها عن السياسة العقابية؟

(2) ما العناصر القانونية والخصائص الإجرامية التي تميز الابتزاز الإلكتروني؟

(3) كيف تكيف النصوص العراقية النافذة صور الابتزاز الإلكتروني، وما حدود تطبيق المواد 430–432والمادة 452 ؟

(4) ما التحديات التي تواجه الإبلاغ وحفظ الدليل والاستجابة المؤسسية؟

(5) ما التدابير التشريعية والإجرائية والتقنية اللازمة لتعزيز الوقاية؟

خامساً :فرضية البحث

يقوم البحث على فرضية مؤداها أن التشريع العراقي النافذ يوفر أساسا جزئيا لملاحقة عدد من صور الابتزاز الإلكتروني من خلال النصوص العامة إلا أن تشتت التكييف وغياب تنظيم متخصص لبعض متطلبات الاستجابة الرقمية العاجلة يحدان من بناء سياسة وقائية متكاملة ومن ثم فإن رفع الفاعلية يتطلب تكامل الإصلاح التشريعي مع الإجراءات الفنية والمؤسساتية والتوعوية.

سادسا / أهداف البحث

يهدف البحث إلى تأصيل مفهوم السياسة الجنائية الوقائية وبيان تمييزها عن السياسة العقابية وتحديد العناصر القانونية والخصائص الإجرامية للابتزاز الإلكتروني تحليل الأساس القانوني العراقي القابل للتطبيق مع ضبط العلاقة بين المواد (430–432) والمادة (452) بحسب عناصر الواقعة وتقييم دور الإبلاغ وحفظ الدليل والتخصص والتنسيق المؤسسي والكشف عن أوجه القصور واقتراح مسارات تشريعية وإجرائية وتقنية قابلة للتطبيق.

سابعا :أصالة البحث وإضافته العلمية

تتمثل أصالة البحث في انتقاله من دراسة الابتزاز الإلكتروني بوصفه سلوكا إجراميا يستوجب التكييف والعقاب إلى تقييم قدرة السياسة الجنائية العراقية على منع الجريمة أو وقف امتداد ضررها في البيئة الرقمية وتبرز إضافته العلمية في الربط بين تعدد التكييف القانوني لصور الابتزاز الإلكتروني في النصوص النافذة وبين فاعلية الوقاية إذ يفترض البحث أن اضطراب التكييف لا ينعكس على الوصف القانوني والعقوبة وحدهما بل قد يؤثر كذلك في توحيد إجراءات

الاستجابة وتصنيف البلاغات وبناء البيانات الإحصائية وتوجيه التدريب وموارد المؤسسات كما يقترح البحث قياس فاعلية السياسة الوقائية بمؤشرات عملية من بينها زمن الاستجابة للبلاغ وسرعة حفظ الدليل الرقمي ومدى وقف استمرار الضرر بدلا من الاقتصار على عدد الدعاوى أو الأحكام الصادرة.

ثامناً :حدود الدراسة

تتحدد الحدود الموضوعية للدراسة بتحليل السياسة الجنائية الوقائية في مواجهة جريمة الابتزاز الإلكتروني في التشريع العراقي، ولذلك لا تمتد إلى دراسة الجرائم المعلوماتية بجميع صورها أو المسؤولية المدنية الناشئة عنها إلا بالقدر الذي يخدم تفسير التدابير الوقائية محل البحث .كما تقتصر دراسة النصوص على القواعد العراقية النافذة والاتجاهات القضائية المنشورة ذات الصلة، ولا تعامل مشروعات القوانين غير النافذة بوصفها مصدراً للتجريم أو الإجراء .أما الإشارة إلى الحسابات الوهمية والتزييف العميق والذكاء الاصطناعي فترد بوصفها تطورات في وسيلة ارتكاب الابتزاز أو صناعة مادة الضغط وتتمثل الحدود المكانية في العراق في حين تمتد الحدود الزمنية إلى التشريعات والاتجاهات القضائية والمصادر المتاحة حتى سنة.2026

تاسعاً :منهج البحث

اعتمد البحث على المنهج التحليلي في تفسير النصوص القانونية العراقية النافذة وربطها بالاتجاهات القضائية المنشورة ذات الصلة، ولا سيما في مسألة التكييف بين أحكام التهديد وحمل المجني عليه على تسليم المال بطريق التهديد .كما استخدم المنهج الوصفي لبيان الخصائص التقنية والإجرامية للابتزاز الإلكتروني وآثاره في الوقاية والإثبات .ولم يعتمد البحث منهجاً مقارناً مستقلاً؛ لأن نطاقه ينصب على التشريع العراقي كما لم يعامل أي مشروع قانون غير نافذ بوصفه قانوناً واجب التطبيق.

عاشراً/ خطة البحث

اقتضت طبيعة البحث تقسيمه إلى مبحثين خصص المبحث الأول للإطار المفاهيمي للسياسة الجنائية الوقائية وجريمة الابتزاز الإلكتروني من خلال مطلبين يتناول أولهما ماهية السياسة الوقائية، ويبحث ثانيهما مفهوم الابتزاز الإلكتروني وأركانه وصوره وخصائصه أما المبحث الثاني فخصص لتطبيقات السياسة الوقائية في التشريع العراقي من خلال مبحثين إذ يعرض في مطلبه

الأول الآليات التشريعية والمؤسسية ثم يقيم في مطلبه الثاني أوجه القصور والتحديات ويقترح سبل التطوير.

المبحث الأول :الإطار المفاهيمي للسياسة الجنائية الوقائية وجريمة الابتزاز الإلكتروني

تمثل الوقاية أحد أبعاد السياسة الجنائية الحديثة وهي لا تلغي العقاب وإنما تعيد ترتيب أدوات المواجهة بحيث لا تنتظر الدولة تحقق الضرر في كل حالة وتزداد أهمية هذا الاتجاه في الجرائم الرقمية لأن سرعة الانتشار وقابلية البيانات للنسخ تجعل إعادة الحال إلى ما كانت عليه أمرا بالغ الصعوبة وعليه يتناول هذا المبحث ماهية السياسة الجنائية الوقائية ثم ماهية الابتزاز الإلكتروني.

المطلب الأول :ماهية السياسة الجنائية الوقائية

تقوم السياسة الجنائية على الاختيارات التي تعتمدها الدولة في مواجهة الظاهرة الإجرامية وإذا كانت السياسة العقابية ترتكز تقليديا على التجريم والجزاء فإن السياسة الوقائية تتجه إلى تقليل احتمالات وقوع الجريمة أو الحد من آثارها وتكرارها ولا تنحصر الوقاية في عمل الشرطة بل تشمل جودة التشريع وتصميم الإجراءات وحماية البيانات، والتوعية والتنسيق المؤسسي، وبناء القدرات التقنية.

الفرع الأول :تعريف السياسة الجنائية الوقائية وتمييزها عن السياسة العقابية

يجد هذا الاتجاه سنده في الأدبيات الحديثة للسياسة الجنائية التي تنظر إلى الوقاية باعتبارها جزءاً من إدارة الظاهرة الإجرامية قبل تحقق الفعل أو تكراره من خلال تهيئة الظروف التي تقلل فرص الجريمة ومعالجة عواملها وقد أكدت دراسة غول حول دور السياسة الجنائية في مكافحة الظاهرة الإجرامية أن الوقاية تمثل أحد السبل الأساسية للحيلولة دون وقوع الفعل الإجرامي[١] ، وكذلك أهمية التدابير السابقة على وقوع الاعتداء في حماية المصالح محل الحماية الجنائية . وبذلك لا يستند المفهوم الذي يتبناه البحث إلى الاعتبارات التقنية للابتزاز الإلكتروني وحدها بل إلى أساس فقهي حديث يوسع وظيفة السياسة الجنائية من مجرد الجزاء إلى الوقاية وإدارة الخطر[٢].

ويستند هذا التصور إلى التأصيل الفقهي الحديث للسياسة الجنائية إذ تعد الوقاية من الجريمة أحد موضوعاتها الأساسية إلى جانب التجريم والعقاب وتقوم على توقي الجريمة واتخاذ التدابير

اللازمة لمنع المجرم المحتمل من ارتكابها أو الحد من العودة إليها كما يرتبط نجاح السياسة الجنائية بقدرتها على تقييم فاعلية المؤسسات والقواعد المخصصة لمكافحة الجريمة وهو ما يبرر اعتماد البحث معيار الفاعلية الوقائية عند تحليل مواجهة الابتزاز الإلكتروني(٣).

السياسة الجنائية الوقائية هي مجموعة التدابير القانونية والمؤسسية والاجتماعية والتقنية التي تعتمدها الدولة والمجتمع بقصد تقليل فرص ارتكاب الجريمة والكشف المبكر عن مخاطرها والحد من آثارها وتكرارها ويكشف هذا وبذلك تقوم السياسة الجنائية الوقائية الاستباق، وتعدد الأدوات، والارتباط بتقييم المخاطر(٤).

فالاستباق يعني أن التدخل لا يبدأ بعد اكتمال الجريمة فقط وقد يتمثل في تجريم سلوك تمهيدي محدد إذا اقتضت الضرورة ومبدأ الشرعية ذلك أو في وضع التزامات تنظيمية لحماية البيانات أو في تيسير قنوات الإبلاغ أما تعدد الأدوات فيعني أن القانون الجنائي ليس الأداة الوحيدة إذ تتكامل معه التدابير الإدارية والتقنية والتعليمية وأما تقييم المخاطر فيقتضي توجيه الموارد نحو البيئات والفئات الأكثر تعرضاً دون تحويل الوقاية إلى مراقبة عامة تمس الحقوق والحريات

وتختلف السياسة الوقائية عن السياسة العقابية من حيث التوقيت والغاية والأداة فالعقابية تتدخل أساسا بعد تحقق الجريمة لإسناد المسؤولية وفرض الجزاء وتحقيق الردع بينما تتجه الوقائية إلى تقليل الفرصة الإجرامية قبل تحقق الضرر أو منع امتداده ومع ذلك فالعلاقة بينهما تكاملية لأن وضوح التجريم وسرعة إنفاذ القانون يؤديان وظيفة ردعية وقائية كما أن الوقاية الناجحة تقلل العبء على أجهزة العدالة (٥).

وفي مجال الابتزاز الإلكتروني يظهر التكامل بوضوح فالعقوبة ضرورية لمواجهة الجاني لكن حماية الحسابات والبيانات والتوعية بعدم الاستجابة للمبتز وسرعة حفظ الدليل وتمكين الضحية من الإبلاغ الآمن كلها تدابير قد تمنع الجريمة أو توقف استمرارها ونرى أن معيار نجاح السياسة الجنائية هنا لا ينبغي أن يقتصر على عدد الأحكام الصادرة بل يجب أن يشمل سرعة الاستجابة ونسبة وقف نشر المحتوى وقدرة الضحايا على الوصول إلى الحماية.

الفرع الثاني :أهداف السياسة الجنائية الوقائية وأهميتها

تهدف السياسة الوقائية إلى التحكم في معدلات الجريمة عبر تقليل الفرص التي تسمح بارتكابها وهي لا تفترض إمكان القضاء الكامل على الجريمة بل تسعى إلى إدارة المخاطر ضمن حدود

تحمي المجتمع وتحترم الحقوق كما تهدف إلى التدخل في البيئة المنتجة للجريمة وتعزيز الثقافة القانونية والرقمي وحماية الفئات الأكثر عرضة وتقليل الضرر ودعم كفاءة مؤسسات العدالة[٦].

وتتميز الوقاية في البيئة الرقمية بمرونتها فوسائل الجناة تتغير أسرع من دورات التشريع ولذلك ينبغي أن تصاغ القواعد على نحو يحدد السلوك المحظور والنتيجة الإجرامية بدقة مع ترك التفاصيل التقنية المتغيرة للمعايير والإجراءات الفنية ومن غير الملائم ربط الحماية باسم تطبيق أو منصة بعينها لأن الوسيلة قد تزول بينما يبقى النمط الإجرامي[٧].

وفي الابتزاز الإلكتروني تتحدد أهداف الوقاية في حماية البيانات من الوصول غير المشروع ورفع حذر المستخدمين والكشف المبكر عن محاولات الاستدراج وتشجيع الإبلاغ وحفظ الأدلة ومنع إعادة نشر المحتوى وتنسيق الاستجابة بين القضاء والجهات التحقيقية والمؤسسات التقنية وتبرز أهمية الوقاية لأن الضرر الرقمي قابل للتضاعف فنسخة واحدة من محتوى خاص قد تتحول إلى عدد غير محدود من النسخ.

ويجب التاكيد على التوعية العامة رغم أهميتها فلا يجوز أن تتحول إلى تحميل الضحية مسؤولية الجريمة فالخطأ في إعدادات الخصوصية أو الثقة بشخص آخر لا يبرر التهديد أو الابتزاز وتبقى المسؤولية الجنائية مرتبطة بسلوك الجاني بينما تستخدم التوعية لتقليل المخاطر وتمكين الأفراد من التصرف الصحيح عند التعرض للتهديد.

المطلب الثاني :ماهية جريمة الابتزاز الإلكتروني

الابتزاز الإلكتروني ليس مجرد تهديد تقليدي أرسل عبر هاتف فالوسيلة الرقمية تغير نطاق الخطر وقوة الإكراه وطبيعة الدليل والاختصاص المكاني لذلك يلزم تحليل الجريمة من حيث مفهومها وأركانها وصورها وخصائصه مع تجنب الخلط بين الابتزاز وبين كل إساءة أو تشهير يقع عبر الإنترنت.

الفرع الأول :تعريف الابتزاز الإلكتروني وأركانه القانونية

هو استخدام وسيلة رقمية في تهديد شخص بكشف أو نشر أو استعمال بيانات أو صور أو تسجيلات أو معلومات تمسه أو تمس من يهمه أمره بقصد حمله على تقديم مال أو منفعة أو

القيام بفعل أو الامتناع عنه ويستوعب المواد الحقيقية والمعدلة أو المصطنعة متى كانت صالحة في ظروف الواقعة لإحداث الضغط المقصود[٨]

ويقوم الركن المادي على سلوك التهديد .ولا يشترط أن ينفذ الجاني ما توعد به، لأن جوهر الاعتداء يتمثل في الضغط على إرادة المجني عليه متى بلغ التهديد درجة الجدية وفق ظروف الواقعة وقد يقع التهديد برسالة مكتوبة أو تسجيل صوتي أو صورة أو حساب وهمي أو نشر جزئي للمحتوى لإثبات القدرة على النشر الكامل[٩] .

أما محل التهديد فقد يكون صورة خاصة أو محادثة أو معلومة مالية أو مهنية أو عائلية، وقد يكون محتوى مصنوعاً بالتزييف العميق .ولا ينبغي أن تتوقف الحماية على كون المادة صحيحة؛ لأن قوة الإكراه قد تنشأ من قابلية الجمهور لتصديقها ومن كلفة نفيها[١٠]

ويتمثل القصد الجنائي في علم الجاني بطبيعة التهديد واتجاه إرادته إلى استعماله للضغط على المجني عليه وإذا اشترط النص المطبق غرضا معينا أو طلبا مصاحبا للتهديد وجب إثباته ويستفاد القصد من مضمون الرسائل وتسلسل الاتصال وطبيعة الطلب ومحاولات إخفاء الهوية أو تكرار الضغط[١١].

ولا تعد الوسيلة الإلكترونية ركناً مستقلا بالمعنى التقليدي في جميع صور التكييف لكنها عنصر يضفي الخصوصية على الجريمة فهي توسع مسرح الجريمة وتزيد سرعة الضرر وتخلق أدلة رقمية تحتاج إلى حفظ فني ومن ثم فإن التكييف يجب أن يراعي مبدأ الشرعية دون تجاهل الواقع التقني.

الفرع الثاني :صور الابتزاز الإلكتروني وخصائصه الإجرامية

تتعدد صور الابتزاز الإلكتروني بحسب الغرض فالابتزاز المالي يهدف إلى الحصول على مبالغ أو تحويلات أو أصول ذات قيمة[١٢] وقد يبدأ باستدراج الضحية للحصول على مادة خاصة ثم المطالبة بالمال وهناك الابتزاز ذو الطابع الجنسي أو المعنوي حيث يستخدم المحتوى الخاص لإجبار الضحية على إرسال مواد إضافية أو الاستمرار في علاقة قسرية أو تنفيذ طلب شخصي كما قد يقع الابتزاز الوظيفي حين يهدد شخص موظفا أو مسؤولا بنشر بيانات لحمله على اتخاذ قرار أو تسريب معلومة أو التغاضي عن مخالفة[١٣].

وقد يتخذ الابتزاز صورة مرتبطة بالمحتوى المصطنع فتقنيات معالجة الصورة والصوت قادرة على إنتاج مادة تبدو حقيقية ويستغل الجاني صعوبة التحقق السريع منها وهنا لا يكون الخطر في سرقة سر قائم فقط بل في صناعة مادة ضاغطة وهذا التطور يكشف قصور التصورات التي تربط الابتزاز حصراً بحيازة الجاني لمعلومة صحيحة عن الضحية(١٤).

ومن خصائص الجريمة اتساع مسرح الجريمة فقد يوجد الجاني والضحية والخادم التقني في دول مختلفة بما يثير مسائل الاختصاص والتعاون الدولي كما تتميز بسهولة التخفي النسبي باستخدام حسابات مستعارة وأرقام أو خدمات متعددة وإن كان التخفي الرقمي ليس مطلقاً متى توافرت القدرات الفنية والإجراءات القانونية المناسبة(١٥).

وتتصف الجريمة كذلك بقابلية الضرر للتضاعف والديمومة فالنشر قد يتم إلى عدد كبير خلال وقت قصير وإزالة المحتوى من موقع لا تعني زوال نسخه كما أن الجريمة تميل إلى الاستمرار والاستنزاف لأن رضوخ الضحية لأول طلب قد يشجع الجاني على تكرار المطالب(١٦).

أما الدليل الرقمي فيتميز بقابليته للتغيير أو الحذف، لكنه في الوقت نفسه قد يحمل بيانات وصفية وآثار اتصال ذات قيمة إثباتية .لذلك فإن المشكلة ليست في هشاشته وحدها، بل في الحاجة إلى جمعه وحفظه وتوثيق سلامته وفق إجراءات تضمن مشروعيته وحجيته(١٧).

حيث أن هذه الخصائص تبرر سياسة وقائية متخصصة لكنها لا تبرر التوسع غير المنضبط في التجريم أو المراقبة فخصوصية الجريمة الرقمية تستوجب دقة أكبر في التشريع والإجراءات ولايوجد استثناء من مبادئ الشرعية والخصوصية والمحاكمة العادلة.

المبحث الثاني :تطبيقات السياسة الجنائية الوقائية في مكافحة الابتزاز الإلكتروني في التشريع العراقي

تتجسد السياسة الوقائية في العراق من خلال النصوص الجنائية النافذة وقواعد الإجراءات وعمل الجهات المختصة والتوعية والحماية التقنية غير أن تعدد هذه الأدوات لا يعني بالضرورة وجود سياسة متكاملة إذ تقاس الفاعلية بوضوح الاختصاصات وسرعة تبادل المعلومات وتوافر الخبرة وقدرة الضحية على الوصول إلى حماية عملية لذلك يتناول هذا المبحث الآليات التشريعية والمؤسسية ثم يقيم فاعليتها ويقترح سبل تطويرها.

المطلب الأول :الآليات التشريعية والمؤسسية للوقاية

يمثل التشريع أساس الحماية الجنائية لأنه يحدد السلوك المحظور والسلطات الإجرائية والضمانات لكن الوقاية من الابتزاز الإلكتروني تحتاج أيضا إلى مؤسسات قادرة على استقبال البلاغ وحفظ الدليل والتعامل مع المنصات والجهات النظيرة خارج العراق ويتطلب ذلك قراءة النصوص النافذة ضمن حدودها وعدم نسبة أحكام إلى قوانين أو مشروعات غير نافذة.

الفرع الأول :السياسة الوقائية في قانون العقوبات العراقي لمواجهة الابتزاز الإلكتروني

لا يتضمن قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل تنظيما مستقلا شاملا لجريمة الابتزاز الإلكتروني بهذا الوصف ولذلك يجري البحث عن التكييف في النصوص العامة بحسب وقائع كل حالة وتبرز أحكام التهديد في المواد 432–430 بوصفها من أهم الأسس القانونية متى تحقق التهديد بالصورة التي يجرمها القانون ويجب التمييز بين صور التهديد واختلاف جسامتها وشروطها وعدم استعمال لفظ الابتزاز كبديل عن تحديد النص المنطبق[١٨]

وتظهر أهمية المادة 438 في نطاق حماية بعض جوانب الحياة الخاصة والأسرار بحسب شروطها عندما يرتبط السلوك بإفشاء أو استعمال معلومات خاصة إلا أن الابتزاز قد يقع دون نشر فعلي وقد تكون المادة محل التهديد مصطنعة ولذلك لا تكفي نصوص الخصوصية وحدها لتغطية جميع الصور[١٩]

كما تكتسب القواعد العامة للشروع في المادتين 30 و 31أهمية حين يبدأ الجاني بتنفيذ جريمة مقصودة ولا تتم لأسباب لا دخل لإرادته فيها، متى انطبقت شروط الشروع على الجريمة محل التكييف ويمكن أن تؤدي أحكام المصادرة ومنها المادة 101 في حدودها القانونية وظيفة وقائية بمنع بقاء بعض الأدوات أو الأشياء المتحصلة من الجريمة في التداول مع مراعاة حقوق الغير حسن النية وطبيعة الأشياء الرقمية[٢٠].

إن الاعتماد على النصوص العامة يحقق قدراً من الحماية ويمنع القول بوجود فراغ مطلق، لكنه يثير صعوبات منها أولا تشتت التكييف بين التهديد والخصوصية وجرائم أخرى تبعاً للوقائع وثانيها أن النصوص صيغت في بيئة سابقة على المنصات الرقمية والتزييف العميق وانتشار المحتوى الفوري .وثالثها أن السياسة الوقائية تحتاج إلى قواعد تتجاوز العقوبة لتشمل حفظ البيانات والاستجابة العاجلة وحماية الضحية[٢١].

حيث أن الحل ليس في تفسير النصوص العقابية تفسيرا موسعا يضر بمبدأ الشرعية بل في تدخل تشريعي دقيق يعرف السلوك الإجرامي من خلال عناصره الجوهرية ويشدد الحماية عند استهداف القاصر أو تكرار الابتزاز أو استخدام محتوى جنسي أو انتحال تقني متقدم مع إبقاء التناسب بين الجريمة والعقوبة وفي نطاق تطبيق النصوص العامة يثير موقف القضاء العراقي من تعدد التكييف القانوني للابتزاز الإلكتروني ملاحظة خاصة[٢٢]

كذلك تكشف التطبيقات القضائية والكتابات القضائية العراقية المنشورة أن وصف الابتزاز الإلكتروني لا يقود بذاته إلى مادة عقابية واحدة وإنما يتحدد النص المنطبق وفق عناصر الواقعة وطبيعة التهديد والطلب المصاحب له فإذا اقترن التهديد بطلب أو تكليف بأمر أو الامتناع عن فعل برزت المادة (430/1) من قانون العقوبات متى تحققت شروطها وهو الاتجاه الذي أكده القرار التمييزي رقم/1841) هيئة الأحداث (2024/في .15/10/2024)[٢٣] ،أما التهديد غير المقترن بطلب فيخضع بحسب جسامته وصورته لأحكام المادتين (431) و .(432)وفي الحالات التي يستعمل فيها التهديد لحمل المجني عليه على تسليم نقود أو أشياء يثار تطبيق المادة (452) متى اكتملت عناصرها القانونية دون اعتبارها نص عاما لكل ابتزاز ذي دافع مالي[٢٤].

حيث أن تعدد التكييف لا يمثل إشكالا عقابيا أو فنيا محضا بل يمتد أثره إلى السياسة الجنائية الوقائية فاختلاف تسجيل الوقائع وتصنيفها بين جرائم التهديد وجرائم اغتصاب وجرائم الأموال أو غيرها قد يصعب تكوين صورة إحصائية موحدة عن حجم الابتزاز الإلكتروني وأنماطه وهو ما ينعكس على توجيه الموارد والتدريب وتحديد الفئات والوسائل الأكثر تعرضا للخطر لذلك لا تستهدف الدعوة إلى تنظيم تشريعي أدق مجرد توحيد العقوبة وإنما تسعى أيضا إلى بناء تعريف تشغيلي واضح يسمح بتوحيد تصنيف البلاغات وإجراءات الاستجابة وجمع البيانات، مع بقاء سلطة القضاء في التكييف القانوني للواقعة وفق عناصرها.

الفرع الثاني :دور المؤسسات المختصة والتدابير التقنية والتوعوية

تبدأ الوقاية المؤسسية من سهولة الإبلاغ فالضحية التي تخشى الفضيحة أو لا تعرف الجهة المختصة قد تتأخر في تقديم الشكوى وهو ما يمنح الجاني وقتا لمضاعفة الضغط أو نشر المحتوى لذلك ينبغي أن تكون قنوات الإبلاغ واضحة وسرية وقادرة على توجيه الضحية فورا إلى خطوات حفظ الدليل وعدم الاستجابة للمبتز[٢٥] ، وتضطلع الجهات التحقيقية والأمنية المختصة بجرائم المعلوماتية بدور أساسي في تتبع الحسابات والأجهزة والاتصالات ضمن الأطر القانونية وتزداد الفاعلية عندما تتوافر وحدات فنية قادرة على استخراج البيانات وتوثيقها وربطها بمحاضر التحقيق والمحافظة على سلسلة الحيازة فالأداة التقنية لا تنتج دليلا صالحا بذاتها بل يجب أن يثبت مصدر البيانات وسلامتها وطريقة الحصول عليها[٢٦].

ويؤدي القضاء والادعاء العام دورا في ضمان مشروعية الإجراءات وسرعة اتخاذ القرارات التي تمنع استمرار الضرر كل ضمن اختصاصه القانوني وفي الجرائم العابرة للحدود تبرز أهمية قنوات التعاون القضائي والدولي للحصول على بيانات أو حفظها قبل زوالها[٢٧].

أما التوعية فهي جزء من الوقاية الأولية وينبغي أن تركز على حماية الحسابات والمصادقة متعددة العوامل وعدم مشاركة رموز الدخول والحذر من الاستدراج وحفظ لقطات ورسائل التهديد والإبلاغ المبكر ويجب أن تصاغ الرسائل التوعوية بلغة لا تجرم الضحية اجتماعيا ولا تدفعها إلى إخفاء الواقعة[٢٨].

كما أن المؤسسات التعليمية والجامعات ووسائل الإعلام تستطيع نشر ثقافة قانونية رقمية ونرى إدراج برامج قصيرة دورية تستند إلى سيناريوهات واقعية ماذا يفعل الشخص عند تلقي أول تهديد؟ وما الأدلة التي يجب ان يحفظها؟ ما الذي لا ينبغي حذفه؟ وكيف يتجنب تحويل الأموال أو إرسال محتوى إضافي؟ إن تحويل التوعية من شعارات عامة إلى تعليم سلوكي قابل للتطبيق يرفع قيمتها الوقائية.

المطلب الثاني :تقييم فاعلية السياسة الوقائية وسبل تطويرها

تكشف دراسة الواقع التشريعي والمؤسسي أن العراق يمتلك قواعد عامة وأجهزة قادرة على التدخل إلا أن طبيعة الابتزاز الإلكتروني تتطلب مستوى أعلى من التخصص والتنسيق ويجب أن ينطلق

التقييم من الفجوة بين سرعة الجريمة وسرعة الاستجابة وبين الطبيعة العابرة للحدود وحدود الاختصاص الوطني وبين تطور وسائل التزييف ودقة النصوص التقليدية.

الفرع الأول :أوجه القصور والتحديات التشريعية والتقنية والمؤسسية

يتمثل التحدي التشريعي الأول في غياب تنظيم جنائي متكامل يحدد الابتزاز الإلكتروني بوضوح ويعالج صوره الحديثة ضمن قانون نافذ شامل ويؤدي الاعتماد على النصوص العامة إلى اختلاف التكييف بحسب تفاصيل الواقعة ولا يعني ذلك انعدام الحماية لكنه يقلل من اليقين القانوني ويضع عبئا أكبر على التحقيق والقضاء[٢٩].

والتحدي الثاني هو أزمة المفاهيم فمصطلحات مثل البيانات والحساب والمحتوى الرقمي والمحتوى المصطنع، ومزود الخدمة والحفظ العاجل للبيانات تحتاج إلى تعريفات منضبطة وينبغي ألا تكون التعريفات ضيقة إلى حد تقادمها سريعا ولا فضفاضة إلى حد المساس بمبدأ الشرعية[٣٠].

أما التحدي الثالث فيتعلق بالطابع العابر للحدود للجريمة فقد يبدأ الاتصال من خارج العراق أو تمر البيانات عبر بنية تقنية أجنبية وهذا يجعل الوصول إلى بعض المعلومات مرتبطاً بالتعاون الدولي وإجراءات قانونية قد تكون أبطأ من دورة حياة الدليل الرقمي[٣١].

ويبرز تحدي الدليل الرقمي في سرعة الحذف والتعديل وتعدد الأجهزة والحسابات والحاجة إلى خبرة فنية كما قد يقع الخلط بين مجرد لقطة شاشة وبين الدليل الكامل القابل للتحقق ولذلك تحتاج السياسة الوقائية إلى بروتوكولات مؤسسية واضحة للحفظ والتوثيق مع احترام الضمانات الإجرائية[٣٢].

ومن التحديات المؤسسية تفاوت القدرات التقنية ونقص التدريب المتخصص والحاجة إلى تنسيق أسرع بين جهات تلقي البلاغ والتحقيق والخبرة الفنية والاتصال الدولي [٣٣]، وقد يؤدي تعدد الجهات دون مسار موحد للقضية إلى تأخير الاستجابة.

كما يمثل الخوف الاجتماعي من الإبلاغ تحديا مستقلا فالضحية قد تعتقد أن تقديم الشكوى سيؤدي إلى انتشار المحتوى أو لومها ويستفيد المبتز من هذا الخوف ومن ثم فإن سرية التعامل وحماية البيانات الشخصية والتواصل المهني مع الضحية ليست مسائل إنسانية فحسب بل أدوات وقائية تقوض مصدر قوة الجاني وقد نواجه تحديا حديثا يتمثل في التزييف العميق فإمكان إنتاج

صور أو أصوات مصطنعة يقلل من كفاية التصور التقليدي القائم على سرقة محتوى خاص وقد يصبح الجاني قادرا على صناعة مادة الابتزاز من عامة الصور لذلك يجب أن تركز الحماية على فعل التهديد والإكراه والاستعمال الضار للمحتوى لا على مصدر المادة وحده.

الفرع الثاني : سبل تعزيز وتطوير السياسة الجنائية الوقائية

ان الوقاية من الجريمة الركيزة الأساسية التي تقوم عليها السياسة الجنائية الحديثة إذ تهدف إلى منع وقوع الجريمة من خلال معالجة أسبابها والحد من العوامل المؤدية إليها، بدلاً من الاقتصار على توقيع العقوبة بعد ارتكابها ومع التطورات الاجتماعية والتكنولوجية وظهور أنماط إجرامية مستحدثة برزت الحاجة إلى إعادة النظر في أدوات السياسة الجنائية الوقائية والعمل على تطويرها بما يواكب هذه التحديات حيث يتطلب التطوير عدة عوامل اهمها :

١- تدخلا تشريعيا متخصصا يجرم الابتزاز الإلكتروني بصياغة دقيقة ويحدد صوره المشددة ويعالج استعمال المحتوى المصطنع ويحمي القاصرين والفئات الأكثر تعرضا وينبغي أن ينسجم النص مع مبدأ الشرعية والتناسب وأن يميز بين التهديد والابتزاز والتشهير والوصول غير المشروع إلى البيانات[٣٤].

٢- يحتاج العراق إلى إطار متكامل لحماية البيانات الشخصية يحدد أسس جمع البيانات ومعالجتها وحفظها والإفصاح عنها ويقرر التزامات أمنية وإجرائية مناسبة فكلما تقلصت فرص التسرب والوصول غير المشروع انخفضت المواد التي يمكن توظيفها في الابتزاز[٣٥].

٣- ينبغي تطوير قواعد وإجراءات الدليل الرقمي ولا سيما الحفظ العاجل والتوثيق، وسلسلة الحيازة والاستعانة بالخبرة والتعامل مع البيانات الموجودة خارج الإقليم ويجب أن تقترن السرعة برقابة قانونية تحمي الخصوصية وحقوق المتهم[٣٦].

٤- يجب إنشاء أو تعزيز مسار وطني موحد للاستجابة لبلاغات الابتزاز الإلكتروني، يربط تلقي البلاغ بالتوجيه الفوري وحفظ الأدلة والإحالة إلى الجهة المختصة ولا يشترط أن يكون ذلك بإنشاء جهاز جديد إذا أمكن تحقيقه من خلال تكامل الجهات القائمة ونظام إحالة إلكتروني واضح[٣٧].

٥- يتعين الاستثمار في التدريب المستمر للقضاة وأعضاء الادعاء العام والمحققين والخبراء في موضوعات الأدلة الرقمية والتزييف العميق وتتبع الأصول الرقمية وأساليب الهندسة الاجتماعية فالتخصص البشري لا يقل أهمية عن شراء الأدوات التقنية[٣٨].

٦- يجب بناء شراكات وقائية مع شركات الاتصالات والمنصات ومقدمي الخدمات ضمن القانون .ويتركز التعاون في حفظ البيانات بناءً على الطلبات القانونية، والاستجابة للمحتوى المخالف، وتوفير قنوات اتصال مؤسسية، ونشر التحذيرات .ولا ينبغي نقل وظيفة التجريم أو القضاء إلى الشركات الخاصة[٣٩].

٧- ينبغي اعتماد استراتيجية توعية مستمرة تقاس نتائجها .فعدد المنشورات ليس مؤشراً كافيا والأهم هو قياس معرفة الجمهور بخطوات التصرف عند التعرض للابتزاز، ومدى الثقة بقنوات الإبلاغ، وزمن تقديم البلاغ منذ أول تهديد[٤٠].

٨- يقتضي الطابع العابر للحدود تفعيل التعاون القضائي والأمني الدولي وتبادل الخبرات . ويجب تطوير نقاط اتصال متخصصة قادرة على التعامل السريع مع طلبات حفظ البيانات والمساعدة القانونية، مع احترام السيادة والضمانات القانونية[٤١].

من خلال ماتقدم يتضح إلى أن السياسة الوقائية الفعالة ليست نصا واحدا ولا حملة مؤقتة بل منظومة قابلة للقياس والمراجعة وينبغي نشر تقارير دورية ببيانات مجمعة لا تكشف هوية الضحايا تتضمن أنماط الابتزاز ووسائل الاتصال وزمن الاستجابة ونتائج التدخل لتوجيه السياسة على أساس الأدلة.

الخاتمة

أن جريمة الابتزاز الإلكتروني تكشف بوضوح حدود السياسة الجنائية التي تكتفي برد الفعل العقابي بعد وقوع الجريمة إذ إن سرعة تداول المحتوى الرقمي وقابليته للنسخ والإخفاء وما يصاحب الابتزاز من ضغط نفسي وخوف اجتماعي، قد تسمح باستمرار الضرر قبل اكتمال إجراءات الملاحقة ومن ثم فإن المواجهة الفعالة تقتضي بناء سياسة جنائية وقائية تجمع بين وضوح التجريم وسرعة الإبلاغ والاستجابة وحفظ الدليل الرقمي والتخصص المؤسسي، والتوعية

العملية وقد أظهر تحليل التشريع العراقي والاتجاهات القضائية المنشورة أن النصوص النافذة توفر أساسا قانونيا لمواجهة عدد من صور الابتزاز الإلكتروني ولا سيما أحكام التهديد في المواد (430–432)من قانون العقوبات مع إمكان تطبيق المادة (452) متى تحققت عناصر حمل المجني عليه على تسليم المال بطريق التهديد غير أن تعدد التكييفات وغياب تنظيم متخصص لبعض متطلبات الاستجابة الرقمية العاجلة يحدان من تكوين سياسة وقائية متكاملة وبناءً على أسئلة البحث وفرضية الدراسة توصل الباحث إلى النتائج والتوصيات الآتية:

أولا/ النتائج

١- بشأن السؤال المتعلق بمفهوم السياسة الجنائية الوقائية وتمييزها عن السياسة العقابية نجد أن السياسة الوقائية لا تمثل بديلا عن التجريم والعقاب وإنما هي سياسة تكاملية تستهدف تقليل فرص وقوع الجريمة والكشف المبكر عنها والحد من استمرار آثارها في حين تتركز السياسة العقابية أساسا على إسناد المسؤولية وفرض الجزاء بعد تحقق الجريمة.

٢- وبشأن العناصر القانونية والخصائص الإجرامية للابتزاز الإلكتروني، تبين أن جوهر الجريمة يتمثل في توظيف التهديد الرقمي للضغط على إرادة المجني عليه وحمله على تقديم مال أو منفعة أو القيام بفعل أو الامتناع عنه وأن الوسيلة الرقمية تضفي على الجريمة خصائص مميزة أهمها سرعة الانتشار وقابلية المحتوى للنسخ والتخفي النسبي والطابع العابر للحدود وصعوبة وقف الضرر بعد النشر.

٣- وفيما يتعلق بالتكييف القانوني في التشريع العراقي، يبدو أن قانون العقوبات رقم (111) لسنة 1969 المعدل لا ينظم الابتزاز الإلكتروني تنظيما مستقلا بهذا الوصف وأن المواد(430–432)تمثل أساسا مهما لتكييف صور التهديد بحسب اقترانه بطلب وطبيعة الواقعة في حين لا تطبق المادة (452) على كل ابتزاز مالي بصورة تلقائية بل متى تحققت عناصر حمل المجني عليه على تسليم النقود أو الأشياء بطريق التهديد.

٤- أن الاعتماد على النصوص العامة يحقق حماية جزئية لكنه يؤدي إلى تشتت التكييف القانوني ويزيد العبء على سلطات التحقيق والقضاء في تحديد النص المنطبق ولا يجوز معالجة هذا القصور بالتوسع في تفسير النصوص العقابية على نحو يتعارض مع مبدأ الشرعية.

٥- وبشأن تحديات الإبلاغ وحفظ الدليل والاستجابة المؤسسية تبين أن خوف المجني عليه من الوصمة أو انتشار المحتوى قد يؤدي إلى التأخر في الإبلاغ وهو ما يمنح الجاني فرصة لمواصلة الضغط أو تنفيذ التهديد كما أن قابلية الدليل الرقمي للحذف أو التغيير وتعدد الأجهزة والحسابات تفرض ضرورة الحفظ العاجل والتوثيق الفني وسلامة سلسلة الحيازة.

٦-أن فاعلية المؤسسات لا تقاس بتعدد الجهات المختصة بل بوضوح مسار البلاغ وسرعة الإحالة والتنسيق بين جهات التحقيق والخبرة الفنية والقضاء والجهات المعنية بالتعاون الدولي.

٧- يوفر التشريع العراقي النافذ أساسا قانونيا جزئيا لملاحقة صور متعددة من الابتزاز الإلكتروني إلا أن تشتت التكييف وغياب تنظيم متخصص لبعض متطلبات الاستجابة الرقمية العاجلة وحفظ الدليل يحدان من بناء سياسة جنائية وقائية متكاملة.

ثانيا/ التوصيات

١- ان يقوم المشرع العراقي بوضع تنظيم تشريعي دقيق لجريمة الابتزاز الإلكتروني يحدد عناصرها وصورها والظروف المشددة المرتبطة بالقاصرين وتكرار السلوك واستعمال المحتوى ذي الطبيعة الجنسية أو المحتوى المصطنع مع مراعاة مبدأي الشرعية والتناسب.

٢- ضبط العلاقة التشريعية بين جريمة التهديد وصور الابتزاز المالي بما يقلل اضطراب التكييف مع الإبقاء على تطبيق المادة (452) في حدود عناصرها القانونية وعدم تحويلها إلى نص عام لكل صورة من صور الابتزاز الإلكتروني.

٣- تطوير قواعد إجرائية واضحة للحفظ العاجل للبيانات الرقمية وجمع الدليل وتوثيقه وسلسلة حيازته بما يضمن سلامة الدليل ومشروعية الحصول عليه ويحمي في الوقت نفسه الخصوصية وحقوق المتهم.

٤- اعتماد مسار وطني واضح وسريع وسري لتلقي بلاغات الابتزاز الإلكتروني يزود المجني عليه منذ أول اتصال بتعليمات عملية لحفظ الرسائل والروابط وبيانات الحساب وعدم حذف الأدلة أو الاستجابة للمبتز.

Journal Of Babylon Center For Humanities Studies 2026 Volume :16 Issue : 11
(ISSN): 2227-2895 (Print) (E-ISSN):2313-0059 (Online)

٥- تعزيز التخصص الفني والقانوني لدى المحققين والقضاة وأعضاء الادعاء العام والخبراء من خلال برامج تدريب دورية في الأدلة الرقمية والتزييف العميق والهندسة الاجتماعية وتتبع الحسابات والبيانات وفق الأطر القانونية.

٦- إنشاء آلية تنسيق بين المؤسسات و نظام إلاحالة إلكتروني موحد يربط جهة تلقي البلاغ بالجهة التحقيقية والخبرة الفنية والسلطة القضائية مع تحديد مسؤوليات كل جهة ومؤشرات زمنية للاستجابة.

٧- تنظيم التعاون القانوني مع مزودي خدمات الاتصالات والمنصات الرقمية في مجال حفظ البيانات والاستجابة للطلبات القانونية مع عدم نقل سلطة التجريم أو الفصل في المسؤولية الجنائية إلى الجهات الخاصة.

٨- اعتماد برامج توعية قائمة على سيناريوهات عملية توضح للمواطن ما يجب فعله عند تلقي أول تهديد مع تجنب خطاب لوم الضحية وقياس أثر التوعية من خلال مستوى المعرفة بقنوات الإبلاغ وزمن تقديم البلاغ.

٩- تعزيز التعاون القضائي والأمني الدولي وتطوير نقاط اتصال متخصصة لطلبات حفظ البيانات والمساعدة القانونية في الجرائم العابرة للحدود بما ينسجم مع القانون والضمانات الإجرائية.

١٠- اعتماد مؤشرات دورية لقياس فاعلية السياسة الوقائية من بينها زمن الاستجابة للبلاغ وسرعة حفظ الدليل ونسبة وقف استمرار الضرر مع نشر بيانات إحصائية مجهولة الهوية تساعد في تطوير السياسة الجنائية على أساس الأدلة.

(١) علي حمزة عسل الخفاجي، وغسان عبد السادة حسن، مفهوم السياسة الجنائية الوقائية في قانون العمل، مجلة المنصور، المجلد ٣٩، العدد ١، ٢٠٢٣، ص ٣-٤.

(٢) أحمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة، ١٩٧٢، ص١٣؛ سليم أحمد المصمودي، الاتجاهات الحديثة للوقاية من الجريمة: كيف تتجدد المقاربات الكلاسيكية في العصر الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، المجلد ٤، العدد ٢، ٢٠٢٢، ص ١٦٨-١٦٩.

(٣) محمد بن المدني بوساق، اتجاهات السياسة الجنائية المعاصرة والشريعة الإسلامية، ط١، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٢، ص ٢١؛شريفة سوماتي، «التجريم الوقائي في السياسة الجزائية المعاصرة»، مجلة صوت القانون، المجلد ٦، العدد ٢، ٢٠١٩، ص ٦٧٤-٦٧٦.

(٤) عبد الرحمن صدقي، السياسة الجنائية في العالم المعاصر، دار المعارف، القاهرة، ١٩٨٦، ص ١٥.

(٥) رمسيس بهنام، علم الوقاية والتقويم: الأسلوب الأمثل لمكافحة الإجرام، منشأة المعارف، الإسكندرية، ١٩٨٦، ص٦٩.

(٦) فائزة يونس الباشا، السياسة الجنائية في جرائم المخدرات، ط٣، دار النهضة العربية، القاهرة، ٢٠٠١، ص ٨.

(٧) منذر كامل عبد اللطيف، السياسة الجنائية في قانون العقوبات العراقي، ط٢، مطبعة الاديب البغدادية، بغداد ١٩٧٩، ص٧؛أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، ط١، مكتبة القانون والاقتصاد، الرياض، ٢٠١٥، ص ٨٤.

(٨) جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، ط١، مكتبة السنهوري، بغداد، ٢٠١٢، ص ٣٠.

(٩) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص ٧٤.

(١٠) عبد الرحمن بن عبد الله المسند، جريمة الابتزاز، ط١، مطبوعات الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر، الرياض، ٢٠١٨، ص ١٥.

(١١) فرج القصير، القانون الجنائي العام، مركز النشر الجامعي، تونس، ٢٠٠٦، ص ٨٤-٨٥.

(١٢) أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥، ص ١٠٢.

(١٣) مصطفى خالد الرواشدة، القواعد القانونية الناظمة لأكثر الجرائم الإلكترونية شيوعاً في المجتمع الأردني: جرائم التهديد والذم والقدح والتحقير والابتزاز، مركز الكتاب الأكاديمي، عمّان، ص ٥١.

(١٤) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ١١٥.

(١٥) فتوح الشاذلي، شرح قانون العقوبات . ـ القسم الخاص، دار المطبوعات الجامعية ، الاسكندرية، ٢٠١٠، ص١١٤٣.

(١٦) عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة: دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨، ص ١٦.

(١٧) غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، ٢٠١٠، ص ١١.

(١٨) فخري عبد الرزاق صلبي الحديثي، شرح قانون العقوبات القسم الخاص، مطبعة الزمان، بغداد، ١٩٩٦، ص ٢٤٤؛ أحمد أمين، شرح قانون العقوبات القسم الخاص، مطبعة دار النهضة، القاهرة، ١٩٣٢، ص ٧١٠.

(١٩) ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي: دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٨٣، ص ٢٢٥؛ وحسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة: الحق في الخصوصية، دار النهضة العربية، القاهرة، ١٩٧٨، ص ٢٣٢–٢٣٣.

(٢٠) علي حسين خلف وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، ١٩٨٢، ص ١٧٤؛ وفخري عبد الرزاق صلبي الحديثي، شرح قانون العقوبات: القسم العام، مطبعة الزمان، بغداد، ١٩٩٢، ص ٢٥٤–٢٥٥.

(٢١) أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، ط١، مكتبة القانون والاقتصاد، الرياض، ٢٠١٥، ص ٨٤؛ وعمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤، ص ٢١٩.

(٢٢) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص ٣٧١؛ وجمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، ط١، مكتبة السنهوري، بغداد، ٢٠١٢، ص ٣٠

(٢٣) قرار محكمة التمييز الاتحادية، الهيئة الجزائية، رقم (١٨٤١/الهيئة الجزائية/٢٠٢٤)، المؤرخ في ٢٠٢٤/١٠/١٥.

(٢٤) قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل،المواد ٤٥٢،٤٣٢،٤٣١.

(٢٥) ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٢٠٠٨، ص ١٠–١١؛ وخالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ١١٥.

(٢٦) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ٢٠٠٥، ص ١–٣؛ وخالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ٢٢٠–٢٢٤.

(٢٧) مر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤، ص ٢١٩؛ وغنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، ٢٠١٠، ص ١١.

(٢٨) خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، ٢٠٠٨، ص ١٥٧–١٦٤؛ وأيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، ط١، مكتبة القانون والاقتصاد، الرياض، ٢٠١٥، ص ٨٤.

(٢٩) سليم أحمد المصمودي، الاتجاهات الحديثة للوقاية من الجريمة: كيف تتجدد المقاربات الكلاسيكية في العصر الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، المجلد ٤، العدد ٢، ٢٠٢٢، ص١٦٩.

(٣٠) خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ٢٢٠-٢٢٤

(٣١) صفاء كاظم غازي الجياشي، جريمة قرصنة البريد الاكتروني-دراسة مقارنة، رسالة ماجستير غير منشورة ،كلية القانون، جامعة بابل، ٢٠١٦، ص٦.

(٣٢) بد الفتاح بيومي حجازي، الجريمة في عصر العولمة: دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨، ص ١٦.

(٣٣) حسام أحمد كيلاني،الدليل الرقمي ومعوقات إثبات الجريمة الإلكترونية، مجلة البحوث الفقهية والقانونية، العدد ٤٧، ٢٠٢٤، ص ٧٩٨-٨٠٥.

(٣٤) جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، ط١، مكتبة السنهوري، بغداد، ٢٠١٢، ص ٣٠.

(٣٥) ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي: دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٨٣، ص ٢٢٥.

(٣٦) حسام أحمد كيلاني،الدليل الرقمي ومعوقات إثبات الجريمة الإلكترونية، مجلة البحوث الفقهية والقانونية، العدد ٤٧، ٢٠٢٤، ص ٧٩٨-٨٠٥.

(٣٧) ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٢٠٠٨، ص ١٠-١١.

(٣٨) خالد ممدوح إبراهيم،فن التحقيق الجنائي في الجرائم الإلكترونية،ط١،دار النهضة العربية،القاهرة،٢٠٠٩،ص١١٥.

(٣٩) سامي جاد عبد الرحمن واصل، التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة القانون والتكنولوجيا، المجلد ٣، العدد ١، ٢٠٢٣، ص ٣٠-٣٥.

(٤٠) سليم أحمد المصمودي، الاتجاهات الحديثة للوقاية من الجريمة: كيف تتجدد المقاربات الكلاسيكية في العصر الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، المجلد ٤، العدد ٢، ٢٠٢٢، ص ١٦٨-١٧١.

(٤١) جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، ص٣٠.

قائمة المصادر

اولا /الكتب

- أحمد أمين، شرح قانون العقوبات: القسم الخاص، مطبعة دار النهضة، القاهرة، ١٩٣٢.
- أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٥.
- أحمد فتحي سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة، ١٩٧٢.
- أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، ط١، مكتبة القانون والاقتصاد، الرياض، ٢٠١٥.
- جمال إبراهيم الحيدري، الجرائم الإلكترونية وسبل معالجتها، ط١، مكتبة السنهوري، بغداد، ٢٠١٢.
- حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة: الحق في الخصوصية، دار النهضة العربية، القاهرة، ١٩٧٨.
- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية، ٢٠٠٨.
- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، ط١، دار النهضة العربية، القاهرة، ٢٠٠٩.
- رمسيس بهنام، علم الوقاية والتقويم: الأسلوب الأمثل لمكافحة الإجرام، منشأة المعارف، الإسكندرية، ١٩٨٦.
- عبد الرحمن بن عبد الله المسند، جريمة الابتزاز، ط١، مطبوعات الرئاسة العامة لهيئة الأمر بالمعروف والنهي عن المنكر، الرياض، ٢٠١٨.
- عبد الرحمن صدقي، السياسة الجنائية في العالم المعاصر، دار المعارف، القاهرة، ١٩٨٦.
- عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة: دراسة في الظاهرة الإجرامية المعلوماتية مع التطبيق على القانون الإماراتي، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨.
- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، ٢٠٠٥.
- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦.
- علي حسين خلف وسلطان عبد القادر الشاوي، المبادئ العامة في قانون العقوبات، المكتبة القانونية، بغداد، ١٩٨٢.

•عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت: الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، ٢٠٠٤.
•غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والإنترنت، دار الفكر والقانون، المنصورة، ٢٠١٠.
•فائزة يونس الباشا، السياسة الجنائية في جرائم المخدرات، ط٣، دار النهضة العربية، القاهرة، ٢٠٠١.
•فتوح الشاذلي، شرح قانون العقوبات: القسم الخاص، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٠.
•فرج القصير، القانون الجنائي العام، مركز النشر الجامعي، تونس، ٢٠٠٦.
•فخري عبد الرزاق صلبي الحديثي، شرح قانون العقوبات: القسم الخاص، مطبعة الزمان، بغداد، ١٩٩٦.
•فخري عبد الرزاق صلبي الحديثي، شرح قانون العقوبات: القسم العام، مطبعة الزمان، بغداد، ١٩٩٢.
•محمد بن المدني بوساق، اتجاهات السياسة الجنائية المعاصرة والشريعة الإسلامية، ط١، مركز الدراسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٢.
•ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٨٣.
•منذر كامل عبد اللطيف، السياسة الجنائية في قانون العقوبات العراقي، ط٢، مطبعة الأديب البغدادية، بغداد، ١٩٧٩.
•مصطفى خالد الرواشدة، القواعد القانونية الناظمة لأكثر الجرائم الإلكترونية شيوعاً في المجتمع الأردني: جرائم التهديد والذم والقدح والتحقير والابتزاز، مركز الكتاب الأكاديمي، عمّان، دون سنة نشر.
•ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، ٢٠٠٨.

ثانياً: البحوث والمقالات

•حسام أحمد كيلاني، الدليل الرقمي ومعوقات إثبات الجريمة الإلكترونية، مجلة البحوث الفقهية والقانونية، العدد ٤٧، ٢٠٢٤.

•سامي جاد عبد الرحمن واصل، التعاون الدولي في مكافحة الجرائم الإلكترونية، مجلة القانون والتكنولوجيا، المجلد ٣، العدد ١، ٢٠٢٣.
•سليم أحمد المصمودي، الاتجاهات الحديثة للوقاية من الجريمة كيف تتجدد المقاربات الكلاسيكية في العصر الرقمي، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، المجلد ٤، العدد ٢، ٢٠٢٢.
•شريفة سوماتي، «التجريم الوقائي في السياسة الجزائية المعاصرة»، مجلة صوت القانون، المجلد ٦، العدد ٢، ٢٠١٩.
•علي حمزة عسل الخفاجي وغسان عبد السادة حسن، مفهوم السياسة الجنائية الوقائية في قانون العمل، مجلة المنصور، المجلد ٣٩، العدد ١، ٢٠٢٣.

ثالثاً: الرسائل الجامعية

•صفاء كاظم غازي الجياشي، جريمة قرصنة البريد الإلكتروني دراسة مقارنة، رسالة ماجستير غير منشورة، كلية القانون، جامعة بابل، ٢٠١٦.

رابعاً: القوانين

•قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

خامساً: القرارات القضائية

•قرار محكمة التمييز الاتحادية، الهيئة الجزائية، رقم (١٨٤١/الهيئة الجزائية/٢٠٢٤)، المؤرخ في ٢٠٢٤/١٠/١٥

List of Sources

I. Books

•Ahmed Amin, *Explanation of the Penal Code: Special Part*, Dar Al-Nahda Press, Cairo, 1932.
•Ahmed Khalifa Al-Malt, *Information Crimes*, Dar Al-Fikr Al-Jami'i, Alexandria, 2005.
•Ahmed Fathi Sorour, *Principles of Criminal Policy*, Dar Al-Nahda Al-Arabiya, Cairo, 1972.
•Ayman Abdullah Fikri, *Information Crimes: A Comparative Study of Arab and Foreign Legislation*, 1st ed., Law and Economics Library, Riyadh, 2015.
•Jamal Ibrahim Al-Haidari, *Cybercrimes and Methods of Addressing Them*, 1st ed., Al-Sanhouri Library, Baghdad, 2012.
•Hossam El-Din Kamel Al-Ahwani, *The Right to Respect for Private Life: The Right to Privacy*, Dar Al-Nahda Al-Arabiya, Cairo, 1978.
•Khaled Mamdouh Ibrahim, *Cybercrime Security*, University House (Al-Dar Al-Jami'iya), Alexandria, 2008.
•Khaled Mamdouh Ibrahim, *The Art of Criminal Investigation in Cybercrimes*, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, 2009.

•Ramses Behnam, *The Science of Prevention and Rehabilitation: The Optimal Method for Combating Crime*, Munsha'at Al-Ma'arif, Alexandria, 1986.
•Abdul Rahman bin Abdullah Al-Musnad, *The Crime of Extortion*, 1st ed., Publications of the General Presidency for the Promotion of Virtue and the Prevention of Vice, Riyadh, 2018.
•Abdul Rahman Sidqi, *Criminal Policy in the Contemporary World*, Dar Al-Ma'arif, Cairo, 1986.
•Abdel Fattah Bayoumi Hijazi, *Crime in the Era of Globalization: A Study of the Phenomenon of Information Crime with Application to UAE Law*, 1st ed., Dar Al-Fikr Al-Jami'i, Alexandria, 2008. • Abd al-Fattah Bayoumi Hijazi, *Criminal Evidence and Forgery in Computer and Internet Crimes*, Dar Al-Kutub Al-Qanuniyya, Egypt, 2005.
•Abd al-Fattah Bayoumi Hijazi, *Combating Computer and Internet Crimes under the Arab Model Law*, 1st ed., Dar Al-Fikr Al-Jami'i, Alexandria, 2006.
•Ali Hussein Khalaf and Sultan Abd al-Qadir al-Shawi, *General Principles of Penal Law*, Al-Maktaba Al-Qanuniyya, Baghdad, 1982.
•Omar Muhammad Abu Bakr bin Yunus, *Crimes Arising from Internet Use: Substantive Provisions and Procedural Aspects*, Dar Al-Nahda Al-Arabiya, Cairo, 2004.
•Ghannam Muhammad Ghannam, *The Role of Penal Law in Combating Computer and Internet Crimes*, Dar Al-Fikr wa Al-Qanun, Mansoura, 2010.
•Faiza Yunus al-Basha, *Criminal Policy Regarding Drug Crimes*, 3rd ed., Dar Al-Nahda Al-Arabiya, Cairo, 2001.
•Futuh al-Shadhli, *Commentary on Penal Law: Special Part*, Dar Al-Matbu'at Al-Jami'iyya, Alexandria, 2010.
•Faraj al-Qusayr, *General Criminal Law*, University Publishing Center, Tunisia, 2006.
•Fakhri Abd al-Razzaq Salbi al-Hadithi, *Commentary on Penal Law: Special Part*, Al-Zaman Press, Baghdad, 1996.
•Fakhri Abd al-Razzaq Salbi al-Hadithi, *Commentary on Penal Law: General Part*, Al-Zaman Press, Baghdad, 1992.
•Muhammad bin al-Madani Bousaq, *Contemporary Criminal Policy Trends and Islamic Sharia*, 1st ed., Center for Studies and Research, Naif Arab Academy for Security Sciences, Riyadh, 2002.
•Mamdouh Khalil Bahr, *Protection of Privacy in Criminal Law: A Comparative Study*, Dar Al-Nahda Al-Arabiya, Cairo, 1983. • Munthir Kamil Abd al-Latif, *Criminal Policy in the Iraqi Penal Code*, 2nd ed., Al-Adeeb Al-Baghdadiya Press, Baghdad, 1979.
•Mustafa Khalid Al-Rawashdeh, *Legal Rules Governing the Most Common Cybercrimes in Jordanian Society: Crimes of Threat, Defamation, Slander, Contempt, and Extortion*, Academic Book Center, Amman, n.d.
•Nasser bin Muhammad Al-Buqami, *Combating Cybercrimes and Their Applications in the Gulf Cooperation Council (GCC) States*, The Emirates Center for Strategic Studies and Research, Abu Dhabi, 2008.
Secondly: Research Papers and Articles
•Hossam Ahmed Kilani, "Digital Evidence and Obstacles to Proving Cybercrime," *Journal of Jurisprudential and Legal Research*, Issue 47, 2024.

•Sami Jad Abd al-Rahman Wasil, "International Cooperation in Combating Cybercrime," *Journal of Law and Technology*, Vol. 3, Issue 1, 2023.
•Salim Ahmed Al-Masmoudi, "Modern Trends in Crime Prevention: How Classical Approaches Are Renewed in the Digital Age," *Arab Journal of Forensic Sciences and Forensic Medicine*, Naif Arab University for Security Sciences, Vol. 4, Issue 2, 2022.
•Sharifa Soumati, "Preventive Criminalization in Contemporary Penal Policy," *Voice of Law Journal*, Vol. 6, Issue 2, 2019.
•Ali Hamza Asal Al-Khafaji and Ghassan Abd al-Sadah Hassan, "The Concept of Preventive Criminal Policy in Labor Law," *Al-Mansour Journal*, Vol. 39, Issue 1, 2023. Third: Academic Theses
•Safaa Kadhim Ghazi Al-Jiyashi, *The Crime of Email Hacking: A Comparative Study*, unpublished Master's thesis, College of Law, University of Babylon, 2016.
Fourth: Laws
•Iraqi Penal Code No. (111) of 1969, as amended.
Fifth: Judicial Decisions
•Decision of the Federal Court of Cassation, Criminal Panel, No. (1841/Criminal Panel/2024), dated October 15, 2024.