HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

عنوان البحث

الإطار القانوني لمكافحة الابتزاز الإلكتروني في العراق ولبنان: دراسة مقارنة

عبد القادر سعد حاتم الحبيب[1]

[1] الجامعة الاسلامية في لبنان – كلية الحقوق – قسم القانون العام

البريد الالكتروني: abdulqader.saad.93@gmail.com

HNSJ, 2025, 6(1); https://doi.org/10.53796/hnsj61/43

المعرف العلمي العربي للأبحاث: arsri.org/10000/61/43

تاريخ الاستقبال: 2024/12/07م تاريخ القبول: 2024/12/15م تاريخ النشر: 2025/01/01م

المستخلص

تهدف هذه الدراسة إلى تحليل القوانين العراقية واللبنانية المتعلقة بجريمة الابتزاز الإلكتروني، ومقارنة فعاليتها في مواجهة هذه الظاهرة المتزايدة. كما تسعى إلى تحديد نقاط القوة والضعف في كل من النظامين القانونيين، وتقديم مقترحات لتحسين الإطار التشريعي بما يضمن توفير حماية أكبر للضحايا، وتعزيز قدرة الجهات المعنية على مواجهة هذه التحديات. اعتمدت هذه الدراسة على المنهج التحليلي المقارن. توصلت الدراسة الى عدة نتائج اهمها أن التشريعات في العراق ولبنان تحتوي على مواد قانونية تهدف إلى مكافحة الابتزاز الإلكتروني، إلا أن هناك حاجة ملحة لتحديث هذه القوانين لتواكب التطورات الرقمية الحديثة وتعزز فعاليتها في الحد من هذه الجرائم المتزايدة.

الكلمات المفتاحية: القانون، الابتزاز الالكتروني، العراق، لبنان.

RESEARCH TITLE

The Legal Framework for Combating Cyber Extortion in Iraq and Lebanon: A Comparative Study

Abstract

This study aims to analyze the Iraqi and Lebanese laws related to the crime of cyber-extortion, and compare their effectiveness in confronting this growing phenomenon. It also seeks to identify the strengths and weaknesses of each of the two legal systems, and to provide proposals to improve the legislative framework to ensure greater protection for victims, and enhance the ability of the relevant authorities to confront these challenges. This study relied on the comparative analytical approach. The study reached several results, the most important of which is that the legislation in Iraq and Lebanon contains legal articles aimed at combating cyber-extortion, but there is an urgent need to update these laws to keep pace with modern digital developments and enhance their effectiveness in reducing these increasing crimes.

Key Words: Law, cyber extortion, Iraq, Lebanon.

المقدمة

ظهرت العديد من الجرائم الإلكترونية التي تشكل تهديدًا للأفراد والمجتمعات مع التقدم السريع في التكنولوجيا وانتشار وسائل الاتصال الرقمية، ، ومن أبرزها جريمة الابتزاز الإلكتروني. يُعرف الابتزاز الإلكتروني بأنه تهديد يتعرض له شخص أو مؤسسة بنشر معلومات حساسة، سواء كانت صحيحة أو مزيفة، بهدف تحقيق مكاسب مالية أو معنوية، أو لإجبار الضحية على القيام بأفعال معينة تحت ضغط الخوف والقلق النفسي.

نظرًا للتأثيرات السلبية لهذه الجريمة على الضحايا من النواحي النفسية والاجتماعية والاقتصادية، عملت الدول على تطوير تشريعات قانونية لمكافحتها والحد من انتشارها. ومع ذلك، لا تزال هناك تساؤلات حول مدى كفاية هذه القوانين وفعاليتها في تحقيق الردع العام والخاص، وحماية الأفراد من الاستغلال الرقمي.

أهمية الدراسة وأهدافها

تهدف هذه الدراسة إلى تحليل القوانين العراقية واللبنانية المتعلقة بجريمة الابتزاز الإلكتروني، ومقارنة فعاليتها في مواجهة هذه الظاهرة المتزايدة. كما تسعى إلى تحديد نقاط القوة والضعف في كل من النظامين القانونيين، وتقديم مقترحات لتحسين الإطار التشريعي بما يضمن توفير حماية أكبر للضحايا، وتعزيز قدرة الجهات المعنية على مواجهة هذه التحديات. [١]

المنهجية

تعتمد هذه الدراسة على المنهج التحليلي المقارن، حيث يتم استعراض وتحليل النصوص القانونية العراقية واللبنانية المتعلقة بالجرائم الإلكترونية، مع التركيز على الأحكام الخاصة بجريمة الابتزاز الإلكتروني. كما سيتم تقييم مدى انسجام هذه التشريعات مع المعايير الدولية، وبيان أوجه التشابه والاختلاف بين النظامين القانونيين.

الإطار القانوني للابتزاز الإلكتروني في العراق ولبنان

في العراق، يُعتبر الابتزاز الإلكتروني جزءًا من الجرائم الإلكترونية التي يعاقب عليها القانون. وقد تم إصدار تشريعات تهدف إلى تنظيم الجرائم السيبرانية، مثل قانون مكافحة الجرائم الإلكترونية الذي يتناول العقوبات المرتبطة بالابتزاز عبر الإنترنت. في المقابل، قام لبنان بتعديل بعض القوانين الجنائية لتشمل الجرائم الإلكترونية، إلا أن هناك نقاشًا مستمرًا حول كفاية هذه القوانين لمواكبة التطورات التقنية السريعة. [٢]

مقارنة بين التشريعات العراقية واللبنانية

• التعريف والتجريم : يحدد القانون العراقي الابتزاز الإلكتروني بشكل واضح ويحدد العقوبات بشكل دقيق، بينما يتعامل القانون اللبناني مع هذه الجريمة من خلال القوانين العامة المتعلقة بالجرائم الإلكترونية دون وجود نصوص محددة تعالجها بدقة.

• العقوبات : تختلف العقوبات بين النظامين، حيث ينص القانون العراقي على عقوبات أكثر تشددًا، تشمل فترات حبس طويلة وغرامات مالية كبيرة، بينما قد تكون العقوبات في القانون اللبناني أقل صرامة في بعض الحالات. [٣]

• آليات الملاحقة القضائية : في العراق، هناك جهود لتعزيز التعاون بين الجهات الأمنية والقضائية لمكافحة الابتزاز الإلكتروني، بينما تواجه لبنان تحديات تتعلق بسرعة الإجراءات القانونية ومدى توفر الموارد التقنية اللازمة للتحقيق في هذه الجرائم.

الفصل الأول :مفهوم الابتزاز الإلكتروني وأركانه القانونية

في العصر الرقمي الحالي، أصبحت التكنولوجيا عنصرًا لا يتجزأ من حياتنا اليومية، حيث يعتمد الأفراد والمؤسسات على الوسائل الرقمية في شتى الأنشطة، سواء في العمل أو التواصل أو إدارة المعلومات الشخصية والمالية. ومع هذا التقدم، ظهرت تحديات جديدة، من بينها الجرائم الإلكترونية التي تهدد الأمن الرقمي والخصوصية. ويُعتبر الابتزاز الإلكتروني من أخطر هذه الجرائم، نظرًا لما يترتب عليه من آثار نفسية واجتماعية واقتصادية على الأفراد والمجتمعات.

الابتزاز الإلكتروني يُعتبر من الجرائم الحديثة التي تستغل الوسائل التكنولوجية لتهديد الأفراد أو المؤسسات، سواء من خلال نشر معلومات حساسة، أو التلاعب بالبيانات الشخصية، أو حتى اختراق الحسابات الإلكترونية، بهدف تحقيق مكاسب غير قانونية. يمكن أن يتخذ الابتزاز الإلكتروني أشكالًا متنوعة، مثل الابتزاز المالي الذي يسعى لإجبار الضحية على دفع مبالغ مالية، أو الابتزاز العاطفي الذي يعتمد على استغلال المشاعر والعلاقات الشخصية، أو الابتزاز السياسي الذي يُستخدم للضغط على شخصيات سياسية أو عامة لتحقيق مصالح معينة. ومع تطور هذا النوع من الجرائم بشكل مستمر بالتوازي مع تقدم التكنولوجيا، أصبح من الضروري وجود قوانين وتشريعات واضحة تُجرّم هذه الأفعال وتوفر الحماية للأفراد والمؤسسات من خطر الوقوع ضحايا لها. (٦)

تعريف الابتزاز الإلكتروني

الابتزاز الإلكتروني هو أسلوب من أساليب التهديد أو التلاعب النفسي الذي يتم عبر الوسائل الرقمية. يتضمن هذا النوع من الابتزاز تهديد الضحية بنشر معلومات خاصة أو حساسة، أو إلحاق ضرر إلكتروني بها، سواء من خلال سرقة بياناتها الشخصية، أو القرصنة، أو التهديد بنشر محتوى مسيء أو محرج. الهدف من هذه التهديدات هو إجبار الضحية على الاستجابة لمطالب معينة، والتي قد تتضمن دفع مبالغ مالية، أو تقديم معلومات إضافية للجاني، أو حتى القيام بأفعال معينة تخدم مصلحة الجاني.

تستند هذه الجريمة بشكل كبير إلى استغلال الثغرات في الأمان الإلكتروني وقلة وعي الأفراد والمؤسسات بمخاطر الإنترنت. يستخدم المجرمون أساليب مثل التصيد الإلكتروني، والقرصنة، واختراق الحسابات الشخصية، بالإضافة إلى التلاعب العاطفي لاستدراج الضحايا وجعلهم في موقف ضعيف يسهل من خلاله ابتزازهم. وقد تشمل الضحايا أفرادًا عاديين، أو شخصيات عامة، أو حتى مؤسسات قد تُستهدف لسرقة بيانات حساسة أو تهديدها بالتشهير. (٧)

أنواع الابتزاز الإلكتروني

يمكن تصنيف الابتزاز الإلكتروني إلى عدة فئات بناءً على طبيعة الجريمة والأهداف التي يسعى المبتز لتحقيقها. من بين هذه الفئات، يبرز الابتزاز المالي كأكثر الأنواع شيوعًا، حيث يتم تهديد الضحية بنشر معلومات حساسة أو سرية ما لم يتم دفع مبلغ مالي للمبتز. يعتمد المجرمون في هذا النوع على وسائل متنوعة، مثل اختراق الحسابات المصرفية، أو الوصول إلى معلومات شخصية يمكن استخدامها للضغط على الضحية، أو حتى إرسال رسائل احتيالية تحتوي على برامج خبيثة تسهل عليهم تنفيذ مخططاتهم.

يوجد أيضًا الابتزاز العاطفي، الذي يعتمد على استغلال المشاعر والعلاقات الشخصية لإجبار الضحية على تقديم تنازلات أو تلبية مطالب معينة. غالبًا ما يستهدف هذا النوع من الابتزاز الأفراد الذين يشاركون معلومات شخصية أو صورًا خاصة عبر الإنترنت، حيث يستغل الجاني هذه المعلومات لتهديد الضحية وإجبارها على الاستجابة لمطالبه. يمكن أن يؤدي

الابتزاز العاطفي إلى عواقب نفسية خطيرة، حيث يشعر الضحية بالخوف والعجز، مما يؤثر سلبًا على حياتها الشخصية والاجتماعية. (٨)

أما الابتزاز السياسي، فهو نوع آخر من الابتزاز الإلكتروني يُستخدم كوسيلة ضغط ضد شخصيات سياسية أو عامة، من خلال تهديدهم بنشر معلومات قد تضر بسمعتهم أو بمسيرتهم المهنية. يُعتبر هذا النوع من الابتزاز خطيرًا لأنه قد يُستخدم لتحقيق أهداف غير مشروعة تتعلق بالتأثير على القرارات السياسية أو الاقتصادية.

بالإضافة إلى ذلك، يُعتبر الابتزاز المعلوماتي من الظواهر التي تستهدف الشركات والمؤسسات، حيث يتم تهديدها بسرقة بياناتها أو تعطيل أنظمتها الإلكترونية إذا لم تستجب لمطالب المبتزين. يُعد هذا النوع من الابتزاز من أبرز التحديات التي تواجه الشركات في العصر الرقمي، إذ يمكن أن يؤدي إلى خسائر مالية كبيرة أو الإضرار بسمعة المؤسسة في حال تسرب معلومات حساسة. (٩)

الأركان القانونية لجريمة الابتزاز الإلكتروني

تُعتبر جريمة الابتزاز الإلكتروني من الجرائم التي تتطلب توافر مجموعة من الأركان لتصنيفها قانونيًا كجريمة تستحق العقوبة. ومن أهم هذه الأركان هو الركن المادي، الذي يتمثل في الفعل الإجرامي نفسه، أي استخدام وسائل رقمية أو إلكترونية لتهديد الضحية أو التلاعب بها. ويشمل ذلك إرسال رسائل تهديد عبر البريد الإلكتروني، أو استخدام وسائل التواصل الاجتماعي لنشر معلومات مضللة، أو اختراق الحسابات الرقمية وسرقة البيانات الشخصية.

أما الركن المعنوي، فهو يتعلق بالقصد الجنائي، أي النية التي يحملها الجاني أثناء ارتكاب الجريمة. ولكي تُعتبر الجريمة مكتملة من الناحية القانونية، يجب أن يكون الجاني على دراية بأن أفعاله غير مشروعة، وأن يكون لديه قصد واضح في تحقيق مكاسب غير مشروعة على حساب الضحية. وفي كثير من القوانين، يتم تشديد العقوبة إذا ثبت أن الجاني كان لديه نية مسبقة في ارتكاب الجريمة، أو إذا كان الابتزاز قد أدى إلى أضرار جسيمة للضحية. (١٠)

الركن الثالث هو الركن الشرعي، والذي يرتبط بالنصوص القانونية التي تُجرّم الابتزاز الإلكتروني، حيث يجب أن يكون هناك قانون واضح يحدد أن هذا النوع من الأفعال يُعتبر جريمة يعاقب عليها القانون. وفي العديد من الدول، تمت إضافة مواد قانونية جديدة لمكافحة الجرائم الإلكترونية، تتضمن نصوصًا صريحة تجرّم الابتزاز الإلكتروني، وتحدد العقوبات المناسبة له وفقًا لخطورة الجريمة. وتختلف العقوبات من بلد إلى آخر، فبعض الدول تفرض عقوبات مشددة قد تصل إلى السجن لعدة سنوات، بينما تكتفي دول أخرى بفرض غرامات مالية أو عقوبات أخف.

الابتزاز الإلكتروني هو جريمة تتطور مع تقدم التكنولوجيا، مما يجعل من الضروري مكافحة هذه الظاهرة لحماية أمن الأفراد والمؤسسات. نظرًا لتنوع أساليب الابتزاز، من المهم أن يكون لدى المستخدمين وعي كافٍ بطرق الحماية من هذه الجريمة، مثل تجنب مشاركة المعلومات الشخصية على الإنترنت، واستخدام كلمات مرور قوية، وتحديث برامج الحماية بشكل دوري. بالإضافة إلى ذلك، فإن تطوير القوانين والتشريعات لمواكبة التحديات الرقمية يعد أمرًا أساسيًا لضمان تحقيق العدالة، ومعاقبة الجناة، وحماية الضحايا من الاستغلال الرقمي. (١١)

الفصل الثاني :التشريعات العراقية واللبنانية حول الابتزاز الإلكتروني

مع تزايد الجرائم الإلكترونية وارتفاع حالات الابتزاز الإلكتروني، قامت العديد من الدول بوضع أطر قانونية وتشريعية لمكافحة هذه الظاهرة والتقليل من آثارها السلبية على الأفراد والمجتمعات. يُعتبر كل من العراق ولبنان من الدول التي اعتمدت تشريعات لمواجهة الابتزاز الإلكتروني، إلا أن هناك اختلافات جوهرية في شمولية وفعالية هذه القوانين في التصدي لهذه الجريمة المتطورة. تهدف هذه الدراسة إلى تحليل التشريعات العراقية واللبنانية المتعلقة بالابتزاز الإلكتروني، وتحديد نقاط القوة والضعف في كل منها، في ظل التطورات التكنولوجية السريعة التي أوجدت بيئة جديدة تتيح لمجرمي الإنترنت تنفيذ تهديداتهم بطرق أكثر تعقيدًا. (١٣)

التشريعات العراقية المتعلقة بالابتزاز الإلكتروني

في العراق، يُعد الابتزاز الإلكتروني جريمة يعاقب عليها القانون بموجب عدة نصوص قانونية تهدف إلى حماية الأفراد من التهديد والاستغلال عبر الوسائل الرقمية. ويعد قانون العقوبات العراقي رقم 111 لسنة 1969 أحد القوانين الأساسية التي تتناول الابتزاز بشكل عام، إذ يحتوي على مواد تجرّم التهديد والابتزاز، سواء تم ذلك بالوسائل التقليدية أو الرقمية. ورغم أن القانون لم يكن مصممًا في الأصل لمواجهة الجرائم الإلكترونية الحديثة، فقد تم اللجوء إلى بعض مواده لتجريم الأفعال المرتبطة بالابتزاز عبر الإنترنت.

علاوة على ذلك، تم تقديم مشروع قانون لمكافحة الجرائم الإلكترونية يهدف إلى معالجة الثغرات الموجودة في التشريعات الحالية، من خلال إدراج نصوص واضحة تتعلق بالابتزاز الإلكتروني والعقوبات المقررة على مرتكبيه. وفقًا لهذا المشروع، يُعتبر الابتزاز الإلكتروني جريمة تستدعي فرض عقوبات صارمة، تشمل السجن والغرامات المالية، بهدف تحقيق الردع العام وحماية المجتمع من مخاطر الجرائم السيبرانية. كما يتضمن المشروع تدابير لحماية الضحايا، مثل توفير آليات للإبلاغ عن حالات الابتزاز الإلكتروني، وتعزيز التعاون بين الجهات الأمنية والقضائية لضمان ملاحقة المجرمين بسرعة وكفاءة. (٦)

بالإضافة إلى القوانين الجنائية، يعمل العراق على تعزيز الأمن السيبراني من خلال وضع استراتيجيات وطنية لمكافحة الجرائم الإلكترونية. تتضمن هذه الاستراتيجيات تحسين البنية التحتية الرقمية وتوفير التدريب الضروري للجهات المعنية في التحقيق بقضايا الابتزاز الإلكتروني. ورغم هذه الجهود، لا تزال هناك تحديات تتعلق بسرعة الإجراءات القانونية، وفعالية تنفيذ العقوبات، ومدى استعداد المؤسسات الأمنية والقضائية للتعامل مع هذه الجرائم المعقدة.

التشريعات اللبنانية المتعلقة بالابتزاز الإلكتروني

في لبنان، يتم تنظيم قضايا الابتزاز الإلكتروني من خلال قانون العقوبات اللبناني، الذي يتضمن مواد تجرّم التهديد والابتزاز، بالإضافة إلى بعض القوانين الحديثة التي تتناول الجرائم الإلكترونية بشكل عام. ورغم أن قانون العقوبات لم يُصمم خصيصًا لمواجهة الجرائم السيبرانية، فقد تم تعديله لإضافة مواد تجرّم الاستغلال الإلكتروني للبيانات الشخصية، إلى جانب قوانين أخرى تهدف إلى حماية الأفراد من الابتزاز والتشهير عبر الإنترنت.

يواجه النظام القانوني اللبناني تحديات تتعلق بسرعة تحديث القوانين لتواكب التطورات التكنولوجية السريعة، حيث تعتمد التشريعات الحالية بشكل أساسي على القوانين التقليدية التي تم تعديلها لتشمل الجرائم الإلكترونية، دون وجود قانون شامل يغطي جميع جوانب الابتزاز الإلكتروني. ومع ذلك، تحتوي بعض النصوص القانونية اللبنانية على عقوبات مشددة في حالات الابتزاز التي تؤدي إلى أضرار جسيمة، خاصة إذا كان الضحية قاصرًا أو تعرض لضرر نفسي كبير. [٣]

من جهة أخرى، تسعى السلطات اللبنانية إلى تعزيز التعاون مع المنظمات الدولية والإقليمية لمكافحة الجرائم الإلكترونية، من خلال تبادل المعلومات والخبرات، وتعزيز الأمن السيبراني عبر تدريب الكوادر الأمنية والقضائية على أساليب التحقيق في هذه الجرائم. ومع ذلك، لا تزال هناك تحديات تواجه تطبيق القوانين، خاصة في ظل التطورات المستمرة في تقنيات الجرائم السيبرانية، وظهور أساليب جديدة يستخدمها المبتزون لتنفيذ تهديداتهم دون ترك أثر رقمي واضح.

المقارنة بين التشريعات العراقية واللبنانية المتعلقة بالابتزاز الإلكتروني

توجد بعض الاختلافات بين التشريعات العراقية واللبنانية فيما يتعلق بالابتزاز الإلكتروني. يتميز القانون العراقي بصرامة أكبر في بعض الجوانب، خاصة فيما يتعلق بالعقوبات المفروضة على مرتكبي الجرائم الإلكترونية. على سبيل المثال، ينص القانون العراقي على عقوبات تشمل السجن لفترات طويلة وغرامات مالية مرتفعة في حالات الابتزاز الإلكتروني، بينما يعتمد القانون اللبناني غالبًا على عقوبات أقل شدة، إلا في حال حدوث ضرر جسيم للضحية.

كما يسعى العراق إلى إنشاء إطار قانوني أكثر شمولية لمكافحة الجرائم الإلكترونية من خلال قانون مكافحة الجرائم الإلكترونية المقترح، الذي يتضمن نصوصًا واضحة تتعلق بالابتزاز الإلكتروني. في المقابل، يعتمد لبنان حتى الآن على تعديلات في قوانينه التقليدية لمعالجة هذه الجريمة. وهذا يشير إلى أن النظام القانوني العراقي أكثر مرونة في التعامل مع التطورات التكنولوجية مقارنة بالنظام القانوني اللبناني، الذي يحتاج إلى تحديثات أوسع لمواكبة التحديات الرقمية الحديثة.[١]

إضافةً إلى ذلك، تختلف آليات تنفيذ القوانين بين لبنان والعراق، حيث يواجه لبنان تحديات تتعلق بسرعة الإجراءات القانونية ومدى توفر الموارد التقنية اللازمة للتحقيق في الجرائم الإلكترونية. في المقابل، يسعى العراق إلى تعزيز التعاون بين الجهات الأمنية والقضائية لتسريع عمليات الملاحقة والمحاسبة في قضايا الابتزاز الإلكتروني. ومع ذلك، لا يزال كلا النظامين القانونيين بحاجة إلى تحسينات إضافية لضمان حماية فعالة للمواطنين، خاصةً مع تزايد حالات الابتزاز الإلكتروني وتعقيد أساليب الجرائم السيبرانية.

يُعتبر الابتزاز الإلكتروني من الجرائم الخطيرة التي تهدد الأفراد والمجتمعات في العصر الرقمي، مما يستدعي تشريعات صارمة لمكافحته والحد من انتشاره. وقد أظهرت الدراسة وجود تفاوت بين التشريعات العراقية واللبنانية في التعامل مع هذه الجريمة، حيث يتميز القانون العراقي بصرامة أكبر في بعض الجوانب، بينما يعتمد القانون اللبناني على نصوص عامة قد تحتاج إلى تحديث لتتوافق مع التطورات التكنولوجية. ورغم الجهود التي تبذلها السلطات في كلا البلدين لمكافحة الابتزاز الإلكتروني، إلا أن هناك تحديات مستمرة تتعلق بتطبيق القوانين.

لتحقيق حماية أكثر فعالية، يُستحسن تحديث القوانين اللبنانية لتتضمن نصوصًا واضحة تتعلق بالابتزاز الإلكتروني، مع تشديد العقوبات في الحالات التي تؤدي إلى أضرار نفسية أو مالية كبيرة. كما يُنصح بتعزيز التعاون بين العراق ولبنان في مجال مكافحة الجرائم الإلكترونية، من خلال تبادل الخبرات، والتعاون في التحقيقات الدولية، وتطوير استراتيجيات وطنية للأمن السيبراني. بالإضافة إلى ذلك، من الضروري نشر الوعي حول مخاطر الابتزاز الإلكتروني، وتعزيز برامج الحماية الرقمية، وتشجيع الأفراد والمؤسسات على اتخاذ تدابير وقائية لحماية أنفسهم من الوقوع ضحايا لهذه الجريمة المتزايدة. [٢]

الفصل الثالث :التحديات القانونية وسبل التطوير

يعتبر الابتزاز الإلكتروني من أخطر الجرائم السيبرانية التي تهدد الأفراد والمؤسسات على حد سواء، حيث يستغل المبتزون التطورات التكنولوجية الحديثة لتنفيذ جرائمهم بطرق يصعب تتبعها. وعلى الرغم من الجهود القانونية المبذولة لمكافحة هذه الظاهرة، إلا أن هناك العديد من التحديات التي تعيق تحقيق الحماية الكاملة للضحايا وتطبيق العقوبات الرادعة على الجناة. ومن أبرز هذه التحديات ضعف بعض القوانين في معالجة الجوانب المختلفة للابتزاز الإلكتروني، وصعوبة تعقب المجرمين في الجرائم العابرة للحدود، بالإضافة إلى نقص الوعي القانوني لدى الضحايا، مما يسهم في تفاقم المشكلة [٤]

تسعى الدول إلى تحديث تشريعاتها لمواكبة التغيرات السريعة في مجال الجريمة الإلكترونية. أصبح من الضروري وجود قوانين واضحة وشاملة تجرّم الابتزاز الإلكتروني بجميع أشكاله، بالإضافة إلى وضع آليات قانونية تعزز من قدرة الأجهزة الأمنية والقضائية على ملاحقة الجناة وتقديمهم للعدالة. في هذا الإطار، يمكن أن يسهم تعزيز التعاون الدولي بين الدول وتبادل المعلومات حول مرتكبي الجرائم الإلكترونية في تقليل هذه الظاهرة، خاصة أن العديد من حالات الابتزاز الإلكتروني تتم عبر شبكات تمتد عبر دول متعددة، مما يجعل عملية الملاحقة القانونية أكثر تعقيدًا. [٦]

التحديات القانونية في مكافحة الابتزاز الإلكتروني

يواجه المشرعون وأجهزة إنفاذ القانون تحديات متعددة في مكافحة الابتزاز الإلكتروني، تتعلق بتطور الأساليب الإجرامية، وضعف القوانين في بعض الدول، وصعوبة تتبع الجناة بسبب الطبيعة العابرة للحدود لهذه الجرائم. على الرغم من أن العديد من الدول قد أدرجت قوانين خاصة بالجرائم الإلكترونية، إلا أن هناك فجوات تشريعية لا تزال تعيق قدرة الجهات المعنية على التصدي للابتزاز الإلكتروني بفعالية. (٨)

أحد أبرز التحديات القانونية هو ضعف التشريعات وعدم شموليتها، حيث تعتمد بعض الدول على قوانين عامة تتعلق بالجرائم التقليدية دون تخصيص مواد قانونية تفصيلية للابتزاز الإلكتروني. هذا يؤدي إلى تفسيرات غير دقيقة للقوانين، مما يتيح للجناة العثور على ثغرات قانونية تمكنهم من التهرب من العقوبات. بالإضافة إلى ذلك، قد تكون العقوبات في بعض الأنظمة القانونية غير كافية لتحقيق الردع المطلوب، حيث تقتصر في بعض الحالات على غرامات مالية أو أحكام مخففة، مما يجعل الابتزاز الإلكتروني جريمة مربحة للمجرمين مقارنة بالمخاطر القانونية التي قد يواجهونها.

تُعتبر صعوبة تعقب مرتكبي الجرائم الإلكترونية من أبرز التحديات التي تواجه أجهزة إنفاذ القانون، حيث يعتمد المجرمون على تقنيات التشفير وإخفاء الهوية الرقمية، مما يصعّب عملية تحديد مواقعهم أو إثبات تورطهم في الجرائم. بالإضافة إلى ذلك، تُنفذ العديد من عمليات الابتزاز الإلكتروني عبر منصات تقع خارج نطاق اختصاص الدول المتضررة، مما يستدعي ضرورة التعاون الدولي لملاحقة الجناة وتقديمهم للعدالة. إلا أن هذا التعاون قد يكون معقدًا نتيجة لاختلاف القوانين بين الدول، فضلاً عن التحديات القانونية المتعلقة بسيادة الدول وحقوق الأفراد في الخصوصية الرقمية. (٣)

كما يُشكل نقص الوعي القانوني لدى الضحايا تحديًا آخر يعرقل جهود مكافحة الابتزاز الإلكتروني، حيث يتردد العديد من الضحايا في الإبلاغ عن هذه الجرائم خوفًا من الفضيحة أو من عدم حصولهم على الحماية القانونية اللازمة. ويجهل البعض وجود قوانين تحميهم، مما يؤدي إلى استمرار هذه الجرائم وتفاقمها. لذلك، تلعب التوعية القانونية دورًا حيويًا في الحد من هذه الظاهرة، حيث تساعد الأفراد على فهم حقوقهم والإجراءات التي يمكن اتخاذها في حال تعرضهم للابتزاز الإلكتروني.

سبل تطوير التشريعات لحماية الأفراد من الابتزاز الإلكتروني

لمواجهة التحديات القانونية المرتبطة بالابتزاز الإلكتروني، من الضروري اعتماد استراتيجيات تشريعية وأمنية متطورة تهدف إلى تحسين القوانين الحالية وتعزيز فعاليتها في التصدي لهذه الجرائم. الخطوة الأولى في هذا السياق هي تحديث التشريعات لتكون أكثر وضوحًا وشمولًا، بحيث تغطي جميع أشكال الابتزاز الإلكتروني، سواء كان ماليًا أو عاطفيًا أو سياسيًا أو معلوماتيًا. يجب أن تتضمن القوانين تعريفًا دقيقًا للابتزاز الإلكتروني، وتحديد العقوبات المقررة على مرتكبيه، مع ضرورة تشديد العقوبات في الحالات التي يكون فيها الضحية قاصرًا أو تتسبب الجريمة في أضرار نفسية خطيرة.

علاوة على ذلك، يُعتبر تعزيز التعاون الدولي أمرًا بالغ الأهمية، حيث يتطلب التصدي للابتزاز الإلكتروني جهودًا مشتركة بين الدول، نظرًا لأن الجرائم الإلكترونية غالبًا ما تُنفذ عبر شبكات عالمية معقدة. من الضروري وضع اتفاقيات دولية تتيح تبادل المعلومات حول الجرائم الإلكترونية بشكل أسرع، وتسهيل إجراءات تسليم المجرمين بين الدول، بالإضافة إلى توحيد بعض القوانين المتعلقة بالجرائم الإلكترونية لضمان عدم وجود ثغرات قانونية يمكن أن يستغلها المجرمون للتهرب من العقاب. (١١)

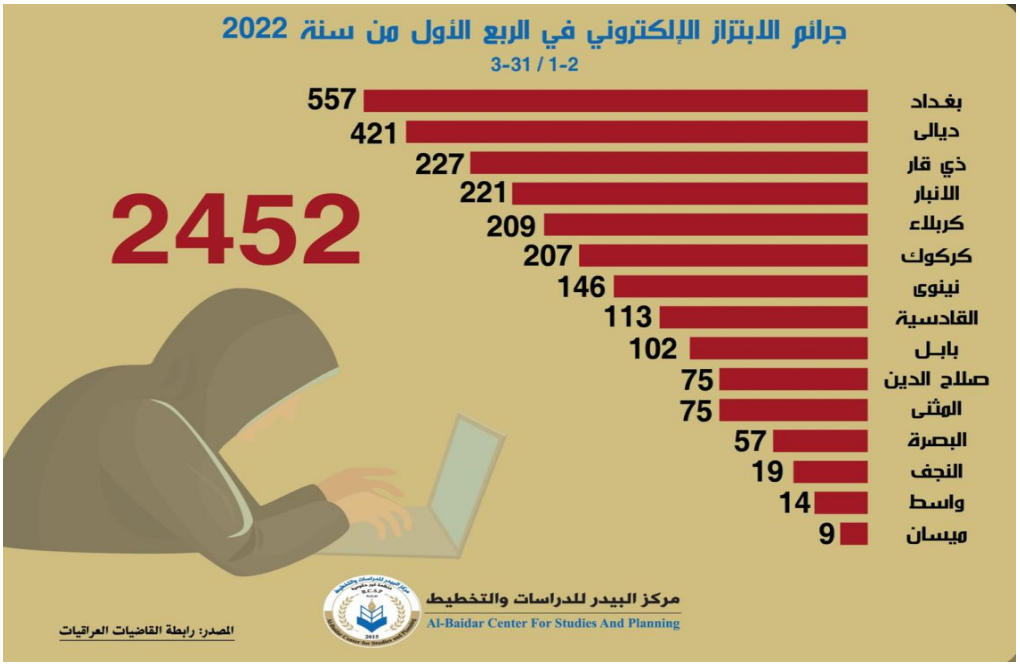
تحسين الأدوات التقنية والقانونية المستخدمة في التحقيقات الإلكترونية يعد عنصرًا أساسيًا في تطوير التشريعات. يجب أن تُمنح الجهات المعنية الصلاحيات اللازمة لاستخدام تقنيات متطورة في تعقب الجرائم الإلكترونية، مثل تحليل البيانات الرقمية، وتحديد مصادر التهديدات، وفك تشفير الرسائل المشبوهة. وفي الوقت نفسه، ينبغي أن يتم ذلك مع مراعاة حقوق الأفراد في الخصوصية الرقمية، مما يتطلب تحقيق توازن دقيق بين الأمن الرقمي وحقوق المستخدمين.

بالإضافة إلى ذلك، يُعتبر نشر الوعي القانوني بين المواطنين من أهم الإجراءات الوقائية لمكافحة الابتزاز الإلكتروني. من خلال حملات التوعية، يمكن تثقيف الأفراد حول كيفية حماية بياناتهم الشخصية على الإنترنت، وأهمية استخدام كلمات مرور قوية، وتجنب مشاركة المعلومات الحساسة مع أشخاص غير موثوقين. كما ينبغي تعزيز الثقة بين المواطنين والأجهزة الأمنية، ليشعر الضحايا بالأمان عند الإبلاغ عن حالات الابتزاز، دون خوف من العواقب الاجتماعية أو القانونية.

يجب أيضًا إنشاء منصات رقمية آمنة تتيح الإبلاغ عن الجرائم الإلكترونية، بحيث يتمكن الضحايا من تقديم شكاواهم بسهولة مع ضمان سرية معلوماتهم بالكامل. يمكن أن تتضمن هذه المنصات خدمات الدعم النفسي والقانوني، مما يساعد الضحايا على التعامل مع حالات الابتزاز بشكل صحيح، ويقلل من فرص تعرضهم لمزيد من الضغوط النفسية. (١٥)

وفي هذا السياق، من الضروري توفير تدريب مستمر للقضاة والمحامين ورجال الأمن حول أحدث تقنيات الجرائم الإلكترونية وطرق التحقيق فيها، مما يضمن تعزيز مهاراتهم وقدرتهم على التعامل مع القضايا الرقمية بفعالية. فبدون وجود كوادر قانونية وأمنية مدربة بشكل جيد، ستظل القوانين عاجزة عن مواجهة هذه الجرائم المتطورة.

تتطلب مكافحة الابتزاز الإلكتروني استراتيجية شاملة تجمع بين الجوانب القانونية والأمنية. يتضمن ذلك تحديث القوانين، وتعزيز التعاون الدولي، وتوفير أدوات تحقيق متطورة، فضلاً عن نشر الوعي القانوني بين المواطنين. على الرغم من الجهود المبذولة في العديد من الدول، لا تزال هناك تحديات تحتاج إلى حلول أكثر فعالية، خاصة فيما يتعلق بتوحيد التشريعات المتعلقة بالجرائم الإلكترونية، وتحسين آليات تعقب المجرمين، وتقديم الدعم اللازم للضحايا. من خلال اتخاذ هذه التدابير، يمكن تقليل انتشار الابتزاز الإلكتروني وحماية الأفراد من التهديدات الرقمية التي أصبحت جزءًا لا يتجزأ من حياتنا اليومية في العصر الحديث.



التوصيات

1. تحديث القوانين العراقية واللبنانية لتشمل تعريفًا أكثر تفصيلًا للابتزاز الإلكتروني، مع تصنيف أنواعه المختلفة مثل الابتزاز المالي، العاطفي، السياسي، والمعلوماتي، وضمان تغطية جميع أشكال التهديد الإلكتروني ضمن النصوص القانونية بوضوح.

2. تعزيز التعاون القانوني بين العراق ولبنان والدول الأخرى من خلال توقيع اتفاقيات تبادل المعلومات وتنسيق الجهود بين الجهات الأمنية والقضائية لمكافحة الجرائم الإلكترونية العابرة للحدود، مما يسهم في تعقب الجناة والحد من استغلال الفجوات القانونية بين الدول.

3. إطلاق حملات توعوية شاملة عبر وسائل الإعلام التقليدية والرقمية لتعريف المواطنين بحقوقهم القانونية، وإرشادهم حول كيفية حماية بياناتهم الشخصية، وآليات الإبلاغ عن الابتزاز الإلكتروني، مع التركيز على الفئات الأكثر عرضة لهذه الجريمة مثل المراهقين والفئات غير المتمكنة رقميًا.

4. إنشاء وحدات متخصصة داخل الجهات الأمنية والقضائية تتولى حصريًا متابعة قضايا الابتزاز الإلكتروني، بحيث يتم تزويدها بأحدث التقنيات والموارد البشرية المدربة، لضمان سرعة التحقيق والكشف عن المبتزين واتخاذ الإجراءات القانونية اللازمة بكفاءة أكبر.

5. تشديد العقوبات على مرتكبي جرائم الابتزاز الإلكتروني من خلال فرض عقوبات رادعة تشمل الغرامات المالية الكبيرة والسجن لفترات تتناسب مع خطورة الجريمة، مع مراعاة الظروف المشددة مثل استهداف القاصرين أو الابتزاز الجماعي أو استغلال البيانات الحساسة للمؤسسات الحكومية والخاصة.

6. تعزيز الأمن السيبراني على المستوى الوطني من خلال تطوير البنية التحتية الرقمية للحماية من الهجمات الإلكترونية، وفرض معايير صارمة على المؤسسات المالية والحكومية لضمان عدم تسرب المعلومات الحساسة التي قد يتم استخدامها في عمليات الابتزاز الإلكتروني.

7. إدراج مواد دراسية حول الأمن الرقمي في المناهج التعليمية لتعزيز وعي الطلاب بأهمية الحماية الإلكترونية، وتعليمهم كيفية التعامل مع الابتزاز الإلكتروني والتصيد الاحتيالي، مما يساعد في بناء جيل أكثر وعيًا وقدرة على التعامل مع المخاطر الرقمية.

8. إنشاء منصات رقمية رسمية مخصصة لاستقبال شكاوى الابتزاز الإلكتروني بحيث تتيح للمواطنين الإبلاغ عن الجرائم بسرية تامة، مع توفير الدعم القانوني والنفسي للضحايا لضمان عدم تعرضهم لمزيد من الضغط أو الإيذاء.

9. إلزام شركات التواصل الاجتماعي والمنصات الرقمية بالتعاون مع السلطات القانونية للكشف عن الحسابات المتورطة في الابتزاز الإلكتروني، ومنح الجهات الأمنية صلاحيات محددة للوصول إلى بيانات المستخدمين المشتبه بهم وفقًا لإجراءات قانونية واضحة ومتوافقة مع معايير حماية الخصوصية.

10. تطوير برامج تدريبية للقضاة والمحامين ورجال الأمن حول أحدث تقنيات الجرائم الإلكترونية وأساليب التحقيق الرقمية، لضمان امتلاكهم المعرفة والخبرة اللازمة للتعامل مع القضايا المتعلقة بالابتزاز الإلكتروني بكفاءة وفعالية.

11. تعزيز التعاون مع المنظمات الدولية المتخصصة في مكافحة الجرائم السيبرانية مثل الإنتربول والمنظمات الأمنية الإقليمية، لضمان الاستفادة من الخبرات العالمية في تعقب الجناة وتطوير استراتيجيات أكثر فعالية في مكافحة الابتزاز الإلكتروني.

12. إجراء دراسات وأبحاث مستمرة حول تطور الابتزاز الإلكتروني وأساليبه الحديثة بحيث يتم تحديث التشريعات والاستراتيجيات الأمنية باستمرار وفقًا لأحدث التحديات والتهديدات السيبرانية

الخاتمة

يُعتبر الابتزاز الإلكتروني من أخطر الجرائم الناتجة عن التطور السريع في التكنولوجيا، حيث يستغل المجرمون الفضاء الرقمي ووسائل الاتصال الحديثة لتهديد الأفراد والمؤسسات وابتزازهم بطرق متعددة. لا تقتصر آثار هذه الجريمة على الأضرار المالية فحسب، بل تمتد لتشمل الأضرار النفسية والاجتماعية، مما يجعل من الضروري مواجهتها لضمان بيئة إلكترونية آمنة للمجتمع.

أظهرت هذه الدراسة أن التشريعات في العراق ولبنان تحتوي على مواد قانونية تهدف إلى مكافحة الابتزاز الإلكتروني، إلا أن هناك حاجة ملحة لتحديث هذه القوانين لتواكب التطورات الرقمية الحديثة وتعزز فعاليتها في الحد من هذه الجرائم المتزايدة.

من خلال التحليل المقارن للتشريعات العراقية واللبنانية، يتضح أن كلا البلدين يسعيان إلى معالجة ظاهرة الابتزاز الإلكتروني، لكن بطرق تختلف من حيث تشديد العقوبات وآليات التنفيذ. ورغم أن القوانين الحالية توفر إطارًا قانونيًا لمواجهة هذه الجريمة، إلا أن هناك ثغرات قانونية تحتاج إلى معالجة لضمان عدم استغلالها من قبل المجرمين. إن التطور المستمر في تقنيات الابتزاز الإلكتروني يتطلب استجابة قانونية مرنة وديناميكية.

إن تنفيذ التوصيات الواردة في هذه الدراسة سيساهم في تعزيز الحماية القانونية للأفراد والمؤسسات، من خلال تحديث القوانين لتشمل جميع أشكال الابتزاز الإلكتروني، وتعزيز التعاون الدولي في ملاحقة المجرمين، وزيادة الوعي القانوني لدى المواطنين بشأن حقوقهم وسبل التعامل مع هذه الجرائم. كما أن إنشاء وحدات أمنية متخصصة، وتطبيق عقوبات مشددة، وتطوير منصات إلكترونية للإبلاغ عن الجرائم السيبرانية، تُعتبر خطوات ضرورية لضمان استجابة فعالة للتحديات الرقمية المتزايدة.

بناءً على ما سبق، يتوجب على الجهات التشريعية والأمنية والقضائية في العراق ولبنان اتخاذ إجراءات ملموسة لتعزيز مكافحة الابتزاز الإلكتروني، من خلال تشريعات أكثر شمولاً، وتعاون دولي فعال، واستراتيجيات أمنية حديثة. فالتكنولوجيا تتطور بسرعة، ومعها تتطور أساليب الجريمة، مما يستدعي أن تظل القوانين والأجهزة المعنية جاهزة للتعامل مع التهديدات الجديدة. إن بناء بيئة إلكترونية آمنة يتطلب جهودًا متكاملة من الحكومات والمجتمع لضمان حماية الأفراد من الابتزاز الإلكتروني، وترسيخ مفهوم الأمن الرقمي كجزء أساسي من الحياة المعاصرة.

المصادر

1. Interpol. (2023). Interpol report on cybercrime trends. https://www.interpol.int

2. United Nations Office on Drugs and Crime (UNODC). (2022). Cybercrime report. https://www.unodc.org

3. Lebanese Ministry of Justice. (2021). Cybercrime legislation. Beirut, Lebanon.

4. MIT Technology Review. (2022). Deepfake and AI-based cyber threats. https://www.technologyreview.com

5. Lebanese Cybercrime Unit. (2022). Annual report on cybercrime. Beirut, Lebanon.

6. Iraq's Ministry of Interior. (2023). Cybersecurity report. Baghdad, Iraq.

7. Journal of Cybersecurity. (2021). Ransomware attacks on financial institutions. Oxford University Press.

8. Harvard Law Review. (2022). Cyber espionage and political blackmail. Harvard University Press.

9. World Economic Forum. (2023). Cyber threats report. https://www.weforum.org

10. Oxford University Press. (2022). Cybersecurity and financial crime. Oxford, UK.

11. Journal of Digital Crime. (2022). Psychological impact of cyber extortion. https://www.digitalcrimejournal.org

12. Interpol. (2023). Interpol report on dark web and cybercrime. https://www.interpol.int