 https://doi.org/10.12816/0061676

Criminal Confrontation for the Crime of Electronic Blackmail in accordance with Jordanian Law: "A Comparative Study"

Ismail Mohammad Sbitan Al-Halalma
Faculty of Law
Middle East University
ialhalalmeh@meu.edu.jo

Received : 05/06/2022 Accepted :12/09/2022

Abstract:

This study aims to find out what electronic blackmail is according to the Jordanian law and why it is hard to prove and stop it. The study also looked at the penalties for this crime and how they compare to other laws that address it. The study began by looking at a problem with the laws in Jordan. The problem was that the laws may not cover everything they need to. To compare this work with Egyptian laws, we need to know if it just needs a general intention to break the law or a specific intention. The study used the analytical approach to read and analyze legal texts and court decisions because it responds to the research's goals. The research reached a lot of conclusions, the most important of which is that the Jordanian government recognized how serious electronic blackmail is, and they made special laws to deal with it and came up with solutions to help prove these crimes and inform the authorities about them. The study also presented a number of recommendations, like: considering hurtful things online a crime, punishing and making accountable anyone who does these things, educating people about their dangers, and creating a method to monitor these actions.

Keywords: Criminal Confrontation, Electronic Blackmail, Jordanian Law.

المواجهة الجزائية لجريمة الابتزاز الإلكتروني وفقًا للتشريع الأردني "دراسة مقارنةً"

إسماعيل محمد سبيتان الحلالمة
كلية الحقوق
جامعة الشرق الأوسط
ialhalalmeh@meu.edu.jo

الاستلام : 2022/06/05 القبول : 2023/09/12

الملخص:

هدفت الدراسة التعرف إلى المواجهة الجزائية لجريمة الابتزاز الالكتروني وفقًا للتشريع الأردني، وذلك من خلال معرفة طبيعة عمل هذا الابتزاز، وبيان صعوبة إثباته والوقاية منه، مع تحديد أركانه، والعقوبات الواردة عليه، وإجراء مقارنة مع بعض القوانين الأخرى التي عالجت هذه المسألة. حيث انطلقت الدراسة من مشكلة بحثية تُفيد بعدم كفاية التشريع الأردني أو شموليته لمعالجة هذا العمل، مقارنة بالتشريع المصري، كما أنّها تتساءل بخصوص الاكتفاء بوجود القصد الجزائي العام، أم يتطلب قصدًا خاصًّا، مع تبيان وجود عقوبات أصيلة أم تبعية. وقد استخدمت الدراسة المنهج التحليلي بوصفه المنهج الأكثر انسجامًا مع طبيعة الدراسة الحاليّة وأهدافها؛ وذلك من خلال قراءة النصوص الشرعية والأحكام القضائية وتحليلها، وقد خرجت الدراسة بالعديد من النتائج أهمها أن المُشرّع الأردني أدرك خطورة هذه الجريمة، وأفرد لها تشريعًا خاصًّا لمعالجتها والتعامل مع خصوصيتها، وأن المُشرّع وضح الحلول الممكنة لمواجهة صعوبة إثبات جريمة الابتزاز الإلكتروني، وإحاطة المؤسسات المعنية بكافة أنشطة هذه العملية، كما خرجت الدراسة بالعديد من التوصيات من أهمها وجوب تجريم كل من مارس هذه الأعمال الإلكترونية سواء أكان بالتشهير، أم بتشويه السمعة، أم بأيّ عمل آخر، علاوة على الملاحقة الأمنية لكل من تُسوّل له نفسه القيام بهذه الأعمال، وإجراء جانب وقائي توعوي يبيّن للعامة خطورة القيام بهذه الأعمال، وضرررورة إنشاء آلية رقابية مختصة.

الكلمات المفتاحية: المواجهة الجزائية، ابتزاز الكتروني، تشريع اردني

المقدمة:

تطورت جريمة الابتزاز الإلكتروني لتصبح من أكثر الجرائم قسوةً، خصوصًا بعدما اتُّخذت وسائل الاتصال الحديثة أداةً للاستغلال، والاعتداء على خصوصية الآخرين وتهديدهم، بما يضعهم في موقف صعب في المجتمع، حيث تسلل المجرم إلى تلك الخصوصية كوسيلة للضغط على الضحية أو تهديدها، لهذا يرتكب المجرم هذه الجريمة بعد الحصول على ما يمكّنه من التسلط على ضحيته.

إذًا الابتزاز هو كل استخدام غير مشروع صادر من مجرم مبتدئ أو متخصص لوسائل الاتصال الحديثة؛ لتهديد الضحية أو ترهيبها بنشر صور أو فيديوهات أو محادثات على منصتَي واتس آب أو فيس بوك أو غير ذلك؛ لتسريب معلومات سرية تخصّ الضحية عبر الوسائل الإلكترونية، تكون مقابل دفع مبالغ مالية، أو استغلال الضحية للقيام بأعمال غير مشروعة لصالح المهدّدين.

وتجدر الإشارة إلى أنّ التطور الحاصل في تكنولوجيا المعلومات نتيجة التقدم العلمي، أنتج مجموعة من الجرائم المستحدثة يطلق عليها – الجرائم الإلكترونية– والتي تتمثل في جرائم الحاسب الآلي الذي يتم استخدامه في المجالات المختلفة، أو جرائم الهاتف النقال، بحيث تعتبر جريمة الابتزاز الإلكتروني من الجرائم التي قد ترتكب عن طريق الحاسب الآلي، وينتشر من خلال هذه الوسائل والآليات الشائعات التي تضرّ بجميع أركان الدولة.

أهداف البحث:

تحاول الدراسة تحقيق بعض الأهداف المهمّة من بين ذلك:

1- التعرف إلى الابتزاز الإلكتروني وبيان صعوبة إثباته وكيفية الوقاية منه.
2- التعرف إلى أركان جريمة الابتزاز الإلكترّوني.
3- تحديد العقوبات الواردة التي تؤدي إلى حماية الضحية من الابتزاز الإلكتروني.
4- معرفة مفهوم جريمة الابتزاز الإلكترّوني باعتبارها صورة من صور الجرائم الإلكتَّرونية المستحدثة.
5- مدى كفاية القوانين الحالية الأردنية والمصرية في مكافحة جريمة الابتزاز الإلكتروني.

أهمية البحث:

1. تسليط الضوء على جريمة الابتزاز الإلكتروني التي تتم عبر

عبر الوسائل الإلكترونية الحديثة.

2- محاولة تحديد وسائل إثبات جريمة الابتزاز الإلكتروني في القانون الأردني والمصري.

3- تحديد الآليات الجزائية لمكافحة جريمة الابتزاز الإلكترّوني.

4- محاولة للحد من التهديد الذي يمارس عبر الوسائل الإلكتروني للأشخاص.

مشكلة البحث:

ثمة اعتبارات عدة تساهم في خلق مشكلة الدراسة، والتي تتصل بالجوانب الرئيسة لمسألة جريمة الابتزاز الإلكتروني، ولكن الإشكالية الرئيسة تتمثل في مدى كفاية كلّ من التشريعَين الأردني والمصري في مواجهة جريمة الابتزاز الإلكتروني؟ وهل تكفي القواعد الواردة في المادة (415) من قانون العقوبات الأردني رقم (16) لسنة (1960)، وفقًا لآخر تعديل بشأن العقوبات البديلة لعام (2022)، والمادة (327) من قانون العقوبات المصري رقم (58) لسنة (1937) وفقًا لآخر تعديل صادر في (20) نوفمبر عام (2021).

أسئلة البحث:

1- هل اعتبرت القوانين الأردنية والمصرية ظاهرة الابتزاز الإلكتروني جريمة؟

2- ما هو الركن المادي لجريمة الابتزاز الإلكتروني؟

3- هل نكتفي بوجود القصد الجزائي العام في جريمة الابتزاز الإلكتروني، أم الأمر يتطلب قصدًا جزائيًا خاصًا؟

4- هل توجد عقوبات أصلية أو تبعية مقررة لهذه الجريمة أم لا؟

5- ما مدى كفاية النصوص ذات العلاقة في مواجهة جريمة الابتزاز الإلكتروني؟

منهج البحث:

سنتناول موضوع الدراسة من خلال المنهج التحليلي، باعتباره المنهج الأكثر انسجامًا مع طبيعة هذا البحث وأهدافه؛ من خلال استقراء النصوص التشريعية والأحكام القضائية الصادرة من محكمة التمييز الأردنية ومحكمة النقض المصرية وتحليلها.

كذلك نطبق المنهج المقارن للوصول إلى نتائج للدراسة لتحديد أركان الجريمة وفقًا للمادة (415) من قانون العقوبات الأردني، وقانون العقوبات المصري، وقانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015)، وقانون جرائم تقنية المعلومات المصري رقم (175) لسنة (2018)، حيث نعرض لأوجه القصور التي شابتها، وطرق معالجتها في الدراسة.

مصطلحات البحث:

1- الابتزاز: هو ما يمارسه المبتزّ على الضحية مستخدمًا أسلوبًا من أساليب الضغط والإكراه تجاه الضحية؛ بهدف التعدي على حياتها الخاصة، والمساس بها عن طريق التشهير فيما يخصها من معلومات، كصورة شخصية، أو وبيانات عائلية.

2- جريمة الابتزاز الإلكتّروني: "هي الحصول على معلومات سرية إلكترونيًّا تتعلق بالمجني عليه لا يرغب وصلوها للآخرين، والتهديد بإفشاء السر، أو نشر المعلومات إن لم تتحقق مطالبه وتُنفذ؛ مما يؤثر على إرادة المجني عليه وعلى نفسيته؛ فيستجيب لرغبات الجاني".

3- مكافحة الجريمة: "تشير إلى الأساليب التي اتخذت للحدّ من الجريمة في المجتمع ومعاملة المجرمين، وكثيرًا ما تركز على استخدام العقوبات الجنائية كوسيلة؛ لردع الناس عن ارتكاب الجرائم بصورة مؤقتة أو دائمة، ويستخدم هذا القانون لمن ارتكبوا جرائم بالفعل، وأيضًا يمنع الجريمة من الانتشار في نطاق دوليّ واسع، ويكون المخوّل للقضاء على الجريمة هي الحكومة والشرطة".

خطة البحث:

للإحاطة بموضوع البحث فقد قُسّم إلى مبحثين رئيسن، يتفرع من كل منهما مطلبين، وذلك وفق الآتي:

المبحث الأول: ماهية جريمة الابتزاز الإلكتروني.

المطلب الأول: مفهوم جريمة الابتزاز الإلكتروني.

المطلب الثاني: أركان جريمة الابتزاز الإلكتروني.

المبحث الثاني: مسلك التشريعات في مواجهة جريمة الابتزاز الإلكتروني.

المطلب الأول: الأسباب الرئيسة للتدخل التشريعي لتوقّي جريمة الابتزاز الإلكتروني.

المطلب الثاني: صعوبات إثبات جريمة الابتزاز الإلكتروني والعقوبات المحددة.

الخاتمة (النّتائج، والتوصيات).

المبحث الأول.

ماهية جريمة الابتزاز الإلكتروني.

تمهيد وتقسيم:

بالرغم من حداثة مصطلح الابتزاز الإلكتروني، إلا أنه كان موجودًا من قبل في القانون الجنائي، فقد نص المشرّع الأردني في المادة (415) من قانون العقوبات الأردني على جريمة الابتزاز بصورتها التقليدية بمسمى جريمة التهديد، على أنه:" 1- كل من هدد شخصًا بفضح أمرٍ أو إفشائه أو الإخبار عنه، عوقب بالحبس من ثلاثة أشهر إلى سنتين، وبالغرامة من خمسين دينارًا إلى مائتي دينار. 2- كل من ابتزّ شخصًا لكي يحمله على جلب منفعة غير مشروعة له أو لغيره، عوقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسين دينارًا ولا تزيد على مائتي دينار. 3- تكون العقوبة الحبس

مدة سنتين وغرامة مقدارها خمسون دينارًا إذا تعلق الأمر المزعوم بحادث مروري، وإن لم ينطوِ على تهديد أو لم يكن من شأنه النيل من قدر هذا الشخص أو من شرفه أو من شرف أحد أقاربه"، وبالمقابل نجد أن المشرِّع المصري قد نص على هذه الجريمة في صورتها التقليدية بموجب المادتين (326) و(327) من قانون العقوبات المصري، على أنه: ""كل من حصل بالتهديد على إعطائه مبلغًا من النقود أو أي شيء آخر يعاقب بالحبس. ويعاقب الشروع في ذلك بالحبس مدة لا تتجاوز سنتين". وفي المادة (327): "كل مَن هدد غيره كتابة بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو السجن المؤبد أو المشدد أو بإفشاء أمور أو نسبة أمور مخدشة بالشرف وكان التهديد مصحوبًا بطلب أو بتكليف بأمر يعاقب بالسجن. ويعاقب بالحبس إذا لم يكن التهديد مصحوبًا بطلب أو بتكليف بأمر. وكل من هدد غيره شفهيًّا بواسطة شخص آخر بمثل ما ذكر، يعاقب بالحبس مدة لا تزيد على سنتين، أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوبًا بتكليف بأمر أم لا. وكل تهديد سواء أكان بالكتابة أم شفهيًّا بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة، يعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنيه".

ولم يرد ذكر مصطلح الابتزاز الإلكتروني صراحة في قانون الجرائم الالكترونية الأردني رقم (27) لسنة (2015م)، ولكن ورد مصطلح التهديد، وبالمقابل لم يستخدم هذا المصطلح صراحة القانون المصري رقم (175) لسنة (2018م)، وإن كان قد عاقب عليه بموجب المادة (25) منه.

لذا، نرى أن التشريعات محل الدراسة استخدمت مصطلح التهديد والابتزاز، ولحداثة هذا المصطلح، فسوف نتناول بالشرح التعريف به في مطلب أول، بعنوان مفهوم جريمة الابتزاز الإلكتروني، ثم نحدد في مطلب ثانٍ، أركان جريمة الابتزاز الإلكتروني، على النحو الآتي:

المطلب الأول.

مفهوم جريمة الابتزاز الإلكتروني:

نوضح في هذا المطلب، في الفرع الأول، تعريف الابتزاز الإلكتروني، أما في الفرع الثاني، أنواع جرائم الابتزاز الإلكتروني، وعلى النحو الآتي:

الفرع الأول: تعريف الابتزاز الإلكتروني.

أولاً: معنى الابتزاز:

الابتزاز لغة: هي على وزن افتعال مأخوذة من بزّ أي سلب، ومنه قولهم في المثل: من عزّ بزّ، ومعناه من غلب سلب. وابتززت الشيء أي سلبته، وبزّ ثيابه أي انتزعها (Ibn Manzoor, 2005)

وقد عرف جانب من الفقه الابتزاز بأنه:" مساومة المرأة على شرفها وعرضها، وسلب كرامتها على البغاء عن طريق تسجيلات صوتية أو مرئية لعلاقة سابقة والتهديد بفضحها" (Al–Hermel, 2009).

الابتزاز إجرائيًّا: يقصد الباحث في تعريفه للابتزاز إجرائيًّا الحصول على مكاسب مادية أو معنوية من شخص معين، أو من شخصية معنوية بالإكراه عن طريق تهديده بإفشاء سر من أسرار المبتزّ من شأنه أن يلحق الضرر به.

ثانيًا: التهديد:

فالتهديد لغة، تهديد مصدر هدد، وجّه، أي تهديدًا، إنذارًا، وعيدًا، هدد (فعل) هدد يهدد، فهو مهدد، والمفعول مهدد، هدد فلان، تهدده، خوفه وتوعده بالعقوبة (معجم اللغة العربية المعاصر) أما اصطلاحًا، يمكن تعريف التهديد هو كل فعل يقوم به الشخص لإنذار آخر بخطر سيلحقه به أو بماله، أو بشخص الغير أو بمال الغير، ومن شأنه أن يلحق به ضررًا، وقد يكون ذلك بمحرر موقع عليه، أو بصور، أو رموز، أو شعارات (Alshamrani, 2010).

أما فقهًا، فقد ذهب جانب فقهي لتعريف التهديد بأنه: "كل عبارة من شأنها إزعاج المجني عليه ، أو إلقاء الرعب في نفسه، أو إحداث الخوف لديه من خطر يراد إيقاعه بشخصه، أو ماله، أو بشخص الغير أو ماله" (Namor, 2013). وذهب جانب فقهي أخر بأنه: "الوعيد بشرّ يصيب المجني عليه، مهما كانت الوسيلة التي توصل بها الجاني، سواء أكان الشر بالاعتداء على نفسه أم ماله أم عرضه؛ مما يحدث الرعب في نفسه، فكل فعل مادي أو قول يشكل اعتداء على الحرية والأمن للمجني عليه يُعتبر تهديدًا" (Hnash, 2020).

ثالثًا: الابتزاز الإلكتروني:

يعرَّف الابتزاز الإلكتروني لغويًّا: هو الابتزاز الذي يقع بوسيلة آلية إلكترونية. كما يعرف اصطلاحًا بأنه: الابتزاز الذي يؤدي مفعول الابتزاز المادي والجنسي نفسيهما، ويتطلب من المشرِّع عقوبة رادعة تناسب تأثير الابتزاز الإلكتروني الضار (Hamuda, 2009, p. 4). وذهب جانب من الفقه إلى أن تعريف الابتزاز الإلكتروني إجرائيًّا هو: "الحصول على معلومات سرية إلكترونيًّا تتعلق بالمجني عليه لا يرغب وصولها للآخرين، والتهديد بإفشاء السرّ أو نشر المعلومات إن لم تتحقق المطالب وتُنفذ؛ مما يؤثر على إرادة المجني عليه ونفسيته؛ فيستجيب لرغبات الجاني" (Kaabi, 2009)، وذهب جانب فقهي أخر بأنه: "الحصول على توقيع أو القيام بعمل أو الامتناع عن عمل أو الكشف عن سر أو تسليم الأموال أو أي ممتلكات أخرى، ويكون ذلك باستخدام العنف أو التهديد بالعنف أو الإكراه" (Abdul Atti and Manchawi, 2021)

ومن جانبنا نعرِّف الابتزاز الالكتروني بأنه: قيام الجاني بتهديد الضحية؛ من أجل الحصول على مكاسب مادية، وقد تكون معنوية، أو بإفشاء أسرار ومعلومات متعلقة بالمجني عليه، وذلك بتهديده بكشف أسراره أو معلوماته الخاصة. وهذا الابتزاز يمكن أن يتم بطرق تقليدية، كما يمكن أن يتم باستخدام إمكانات ووسائل تكنولوجية حديثة يكون من خلالها ابتزازًا إلكترونيًّا.

الفرع الثاني: تصنيف جرائم الابتزاز الإلكتروني:

بالرغم من أن التكنولوجيا المعلوماتية يسَّرت سبل الحياة، إلا أنها بالمقابل يسرت سبل ارتكاب الجريمة؛ فظهرت مصطلحات جديدة في العلوم الجنائية، كالجريمة الإلكترونية، والمجرم الإلكتروني، والضحية الإلكترونية، والدليل الرقمي، فالأمر طبيعي أن يُستغل الجانب السلبي للتكنولوجيا الحديثة، واستخدامها بوصفها وسيلة لارتكاب بعض الجرائم، أو أن تقع الجرائم على هذه التكنولوجيا (Al–maaiaa, 2021)، مثل الجريمة محل الدراسة.

إذًا الابتزاز الإلكتروني له عدة صور وأنواع ووسائل يستخدمها الجاني في التأثير على المجني عليه والتأثير في إرادته، وهذا مما جعلها من الجرائم المعقدة والمنتشرة داخل المجتمعات؛ لاستهدافها أكثر من ضحية، ويمكن تفصيل القول فيها وفق الآتي:

أولًا: نوع الضحية التي يتم تهديدها:

أ– الحكومات والشركات والمؤسسات:

تتمثل هذه الجرائم التي يستهدف فيها الجناةُ الحكومات والشركات والمؤسسات، عن طريق التجسس الإلكتروني على أنشطتها، واختراق أنظمتها، والحصول على معلومات سرية تتعلق بالمنشأة، والتي يحرص القائمون على تلك الشركات والمؤسسات على عدم ظهورها للآخرين، وإبقائها في إطار ضيق تشمل عددًا من الموظفين التابعين لها.

وقد حرصت الكثير من الدول منذ الأزل على المحافظة على وثائقها الرسمية السرية، خاصة المتعلقة بكيانها، ومخططاتها، وإمكاناتها، ونشاطاتها، وتعداد الجيوش وتسليحها، والمعلومات الاستخباراتية. وجعلت هذه المعلومات بحرزٍ أمنيّ ضد تلاعب الأشخاص والوصول إليها. ومع استخدام التقنيات والاتصالات ونظم المعلومات، أصبحت تلك المعلومات السرية هدفًا لبعض المنظمات الإجرامية؛ للحصول على تلك المعلومات المهمة، وابتزاز الدول بالحصول على مبالغ كبيرة نظير عدم نشر تلك المعلومات في جميع أنحاء العالم؛ مما يشكل ضغطًا كبيرًا على الدول، ودفع تلك المبالغ لضمان المحافظة على السرية التي تحرص عليها (Al–Atayanan, 2005).

كما أن هناك كثيرًا من الشركات التجارية والمؤسسات لديها من الأسرار والوثائق المتعلقة بنشاطها، والتي قد تؤثر في سير الربح الذي تجنيه الشركة أو المؤسسة، أو قد تسيء لسمعتها داخل السوق؛ مما يجعل تلك المنشآت تحرص على ضمان بقائها داخل نطاق السرية، وحمايتها من الوصول للآخرين للمصلحة، وبذلك تكون هدفًا للجناة للحصول على المال (الكسب المالي)، وهو الأكثر انتشارًا سواء على مستوى الشركات أو على مستوى الأفراد، حيث يقوم الجاني باختراق أنظمة البنوك، أو الحصول على بطاقات الائتمان المصرفية (Alhakem, 2019)

ب– النساء:

تعدُّ النساء أكثر أنواع الابتزاز الإلكتروني انتشارًا، حيث تكون الضحية امرأة والمبتز رجلاً أو امرأة؛ بسبب العلاقة غير الشرعية، والتعارف داخل غرف المحادثات (الشات)، أو التعارف من خلال وسائل التواصل الاجتماعي: (الفيسبوك– تويتر– انستغرام– سناب شات) وغيرها من الوسائل العديدة للتواصل بين أفراد المجتمع، حيث يعمد المبتزّ الطلب من الفتاة أن تصور جسدها، أو تسجيل محادثة بالكاميرا (الكام)، وفي لحظة ضعف وإغراء من الجاني للضحية تنفذ ذلك. حيث استُغلت هذه الطريقة من قبل ضعاف النفوس؛ للإيقاع بالعديد من النساء؛ من أجل الحصول على الكسب المالي، أو الاستغلال الجنسي، أو غير ذلك.

ج– الأطفال:

الطفل هو كل إنسان لم يكمل الثامنة عشرة من العمر، حيث انتشرت ظاهرة الابتزاز الإلكتروني التي تلحق بالطفل بسهولة؛ بسبب التعامل المتزايد من قبل هذه الفئة بوسائل تقنية المعلومات. حيث يقوم المبتزّ بالتعرف إلى الأحداث صغار السن؛ من خلال غرف الدردشة، ووسائل التواصل الاجتماعي، ثم يطلب منه صورًا جنسية مقابل إعطائه مبلغًا من المال، أو إعطائه بطاقات شحن الهواتف، وبعد ذلك يقوم بتسجيل المحادثة، وقد يكون المبتزّ هنا امرأة، حيث تستغل بعض النساء الأحداث صغار السن في التعرف إليهم وتصويرهم، ثم طلب المال في مقابل عدم نشر الصور والفيديوهات عبر الإنترنت أو لأحد أقاربه (Manchawi, 2021).

د– الرجال:

وهو أقل صور الابتزاز الإلكتروني وجودًا داخل المجتمعات، ويوجد بصورة أقل من ابتزاز النساء والأحداث، حيث يعمد بعض الشباب أو بعض النساء إلى إقامة علاقات غير الشرعية مع رجال غالبًا من الميسورين ماديًّا، واستغلال تلك العلاقة في تسجيل عدد من مقاطع الكاميرا، أو تسجيل صوتي عبر وسائل التواصل، أو غرف المحادثات، ثم يستغل ذلك في طلب المال من الضحية مقابل عدم نشر تلك المعلومات عبر الإنترنت، أو لأحد أقاربه، أو أهل بيته، وهنا يبحث المبتزون والمبتزات عن الرجال أصحاب الشركات والميسورين ماديًّا(Abu Bakr, 2015).

ثانيًا: تصنيف جرائم الابتزاز الإلكتروني المرتكز على الهدف:

أ: ابتزاز مادي:

من أهم الأهداف التي ينشدها المبتز هو الحصول على المال، حيث يقوم المبتز بطلب دفع مبالغ مالية أو عينية ذات قيمة من المجني عليه، في مقابل عدم إفشاء الإسرار الموجودة بحوزته ونشرها عبر الشبكة المعلوماتية "الإنترنت"، وقد تصل تلك المبالغ لأرقام فلكية كما يحدث عند ابتزاز الحكومات والشركات الكبرى والمؤسسات ذات الوزن السوقي، ويقع الابتزاز المادي، حيث تضطر تلك الشركات والمؤسسات الدفع للمبتزّ خشية التشهير بها، والمحافظة على سمعتها، وعدم فقدان ثقة العملاء بها، ومن الأمثلة على ذلك، قيام الجاني الذي يعمل مُبرمجًا لدى إحدى الشركات الألمانية، بالاستيلاء على (22) شريطًا تحوي معلومات تخصّ عملاء الشركة، وهدّد ببيعها للشركات المنافسة إذا لم يحصل على مبلغ (200000) دولار، واضطرت الشركة لدفع المبلغ لاسترداد الأشرطة الممغنطة المسروقة .

ومن ذلك أيضًا، الدخول إلى مواقع البنوك، واختراق أجهزتها، وتحويل المبالغ من أرصدة المودعين والبطاقات الائتمانية، والقيام باحتيالات مالية؛ من أجل إجبار تلك البنوك على دفع مبالغ لهم؛ لضمان عدم إساءة سمعتها.

ب– ابتزاز جنسي:

وهي أكثر أنواع الابتزاز شيوعًا، حيث تكون الضحية امرأة أو حدثًا صغيرًا، حيث يتعرف المبتزّ على الضحية عن طريق مواقع التواصل الاجتماعي المختلفة، أو عن طريق غرف المحادثة "الشات"، أو عن طريق المنتديات وغيرها من الوسائل التي يمكن أن تنشأ فيها علاقة بين المبتز والضحية، ثم يبدأ بمحادثتها عبر الكاميرا، وأخذ صور لها بموافقتها، بعد ذلك يطلب تمكينه من فعل الفاحشة وإشباع رغباته الجنسية، أو التهديد بنشر الأسرار التي حصل عليها في حال عدم الامتثال لرغباته؛ فتضطر الضحية للموافقة خشية الفضيحة والعار، وقد يطلب الجاني من المجني عليه ممارسة الفاحشة عدة مرات، وكذلك ممارسة الفاحشة مع غيره ممن تربطه بهم علاقة كأصدقائه مثلً، ويستمر إرغام الفتاة أو الحدث بممارسة ذلك لفترات طويلة حتى بعد زواج الفتاة؛ مما يهدد حياتها الزوجية (Al–Amira, 2012).

فقد قضت محكمة التمييز الأردنية على أن: "المجني عليها قد تعرفت على المتهم (ع) من خلال حساب الأخير (فحل المحرومات) و(س)، وتبين لها أن المتهم استطاع الاستيلاء على حسابها، والحصول على صورها من حسابها، وكانت صورًا محتشمة، وقد هددها أنه سيعمل على تركيب صورة وجهها على أجساد فتيات عاريات إن لم ترسل له صورها وهي عارية، وقد رضخت المجني عليها له وأرسلت له بالفعل صورها وهي عارية، وبعدها طلب منها أن تتحدث معه عبر الكاميرا وهي عارية، وعندما رفضت ذلك هددها أنه سيقوم بنشر صورها وإرسالها لأقاربها ورفضت المجني عليها ذلك، فما كان من المتهم"[*]. وتحليلًا للحكم السابق، يتضح أن الأفعال المرتكبة من قبل المتهم (ع)، قد اقتصرت على الطلب من المجني عليها إرسال صور عارية لها، وقيام المجني عليها البالغة من العمر (17) سنة بالاستجابة، لذلك وجدت المحكمة بأن تلك الأفعال لم تستطل استطالة مادية مباشرة إلى مكان العفة والعورة لدى المجني عليها سواء باللمس المباشر أو المشاهدة العلنية المباشرة لها؛ مما لا تشكل تلك الأفعال جناية هتك العرض كما هو مسند للمتهم (ع) من قبل النيابة العامة، وإنما تشكل بالتطبيق القانوني جنحة الابتزاز لجلب منفعة غير مشروعة خلافًا لأحكام المادة (2/415) من قانون العقوبات، وبدلالة المادة (15) من قانون الجرائم الإلكترونية.

ج– ابتزاز منفعة:

حيث يطلب الجاني من الضحية تنفيذ عدد من الطلبات لتحقيق مصالح شخصية له، كأن يطلب من الضحية القوادة على أحد أقاربها إذا كانت امرأة، أو إقامة سهرات ماجنة، أو تناول المخدرات ونشرها بين صديقاتها، أو ارتكاب سرقات، أو ترويج مخدرات إذا كانت الضحية حدثًا صغير السن، واستغلال الضحايا لتكون وسائل لارتكاب الجرائم؛ مما يشكل تهديدًا لأمن المجتمع واستقراره وزيادة معدلات الجريمة (Al-Mutairi, 2009, p. 29) ، ويأتي هذا النوع في المرتبة الثالثة من حيث الانتشار داخل المجتمع الأردني والمصري.

ومن جانبنا، نرى تتعدد طرق الابتزاز الإلكتروني حسب كل مجرم وتخطيطه لجريمته واحتياجاتها، ووسائله في ذلك قد تكون تقليدية، أو وسائل إلكترونية، بالنظر إلى الضحية، ودوافعِ الجاني لارتكاب جريمة الابتزاز الإلكتروني.

المطلب الثاني.

أركان جريمة الابتزاز الإلكتروني:

الأصل أن كل جريمة تتكون من ركنين: الركن المادي، والركن المعنوي، وإذا تخلف أحدهما اعتبر الفعل غير مجرم، كما تطلب القانون لبعض الجرائم قصدًا خاصًا. فجريمة الابتزاز تعد من جرائم النتيجة التي تتطلب صدور نشاط يكون سببًا في تحقق النتيجة، وليست جريمة شكلية، فاعتداء الجاني على الضحية من خلال تهديدها وابتزازها أمر لازم، لا تقوم الجريمة دونه، إلا إذا كان هو السبب في النتيجة، وهي الحصول على المال، أو أوراق مالية، أو غيرها.

---

[*] حكم محكمة التمييز بصفتها الجزائية الأردنية في الحكم رقم (310) لسنة 2022، بجلسة 2022/4/21، متاح على موقع قرارك الأردن.

وفي جريمة الابتزاز الإلكتروني، تتحقق النتيجة الإجرامية عند قيام الجاني بتهديد المجني عليه بإفشاء سرّ من أسراره، ويتعلق هذا التهديد بأمر غير مشروع، يكون سببًا في زرع الخوف والهلع والتأثير على نفسية المجني عليه وإرادته، الأمر الذي دفعه إلى تنفيذ تهديد المبتز.

ولكن نظرًا للتطور التكنولوجي الذي لحق بجميع جوانب الحياة، ظهرت جريمة الابتزاز الإلكتروني، وترتب على ذلك تغيّر النطاق الذي يمكن أن تقترف فيه الجريمة، وهذا النطاق يعدّ وضعًا سابقًا على ارتكاب الجريمة، يستوجب القانون وجوده من أجل قيام الجريمة، وعليه لا يعد هذا النطاق جزءًا من الجريمة، وبالتالي فهو يعدّ عملًا مشروعًا، بينما الجريمة فعل غير مشروع، ويتمثل هذا النطاق في البيئة الرقمية التي تقع فيه الجريمة، وهذا ما يسمى بالشرط المسبق لجريمة الابتزاز الإلكتروني (Abdul Atti, 2021).

كما يشترط في جريمة الابتزاز من أجل الحصول على المال بالتهديد، أن تتوافر فيها الأركان العامة كما في باقي الجرائم، وهي الركن المادي والركن المعنوي (Abelazeez, 2018)؛ فأما الأول، فيقتضي تحقق العناصر الآتية، وهي: التهديد بإفشاء أو نسبة أمور شائنة، والتهديد من أجل الحصول على مال، أو أوراق مالية، أو على توقيع، أو على تسليم ورقة، في حين يتطلب الثاني العلم والإرادة.

بناءً على ما سبق، نوضح أركان الجريمة، على النحو الآتي:

الفرع الأول: الشرط المسبق لجريمة الابتزاز الإلكتروني:

الشرط المفترض عبارة عن وقائع تسبب ارتكاب الجاني لنشاطه الإجرامي، وهي من خلال ذلك تكون من الوِجهة المنطقيّة مستقلةً عن هذا النشاط، على اعتبار أنها المجال الذي تقع فيه الجريمة. الأمر الذي يمكن معه القول إن استقلال هذه الشروط عن النشاط الإجرامي يجعلها بلا ريب تستقلّ عن رابطة السببية، أيضًا بوصفها حلقة الوصل بين ذلك النشاط والنتيجة الإجرامية المتولدة عنه (Sroor, 1996).

فقد نصت المادة (1/415) من قانون العقوبات على أنه:" كل من هدد شخصًا بفضح أمر، أو إفشائه، أو الإخبار عنه، وكان من شأنه أن ينال من قدْر هذا الشخص، أو من شرفه، أو من قدْر أحد أقاربه، أو شرفه، عوقب بالحبس من ثلاثة أشهر إلى سنتين، وبالغرامة من خمسين دينارًا إلى مائتي دينار".

والسؤال الذي يثار هنا، هل الشرط المفترض يعتبر ركنًا من أركان الجريمة؟ بعض الفقه رفض اعتبار الشرط المفترض ركنًا من أركان الجريمة، معتمدًا على المادة (415) من قانون العقوبات الأردني (Mostafa, 1983)، وبعضه الآخر اعتبره ركنًا في بعض الجرائم الخاصة بدلالة المادة (15) من قانون الجرائم الإلكترونية الأردني التي نصت على أنه: "كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ، باستخدام الشبكة المعلوماتية، أو أي نظام معلومات، أو موقع إلكتروني، أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع" (Mahdi, 2008).

فقد ذهب جانب فقهي (wazeer, 1983) بالقول إنّ الشرط المفترض، هو ذلك الشرط الذي يفترض القانون توافره وقت مباشرة الجاني نشاطه، وبدونه لا يوصف هذا النشاط بأنه جريمة، ويوجب القانون توافر الركن المفترض من أجل وجود الجريمة، أو من أجل اعتبارها من نوع معين (جناية أو جنحة)، ومن أمثلة الشرط المفترض ما يأتي:

1- أن يكون المجني عليه حيًّا في جريمة القتل.
2- أن يكون المال المختلس مملوكًا لغير الجاني في جريمة السرقة.
3- وجود دعوى في جريمة شهادة الزور، وحالة الحمل في جريمة الإجهاض.

ويلاحظ أن الشرط المفترض سابق على وقوعها، ويترتب على ذلك الآتي:

1. إنّ توافره لا يتحقق به البدء في التنفيذ الذي يقوم به الشروع.
2. إنّ مكان وقوع الجريمة يتحدد بمكان وقوع ركنها المادي، أو جزء منه، لا بالمكان الذي يتحقق فيه ركنها المفترض (Hosni, 1989).

مما تقدم، يرى الباحث أن إثبات الركن المفترض يخضع لوسائل الإثبات المقررة في القانون الذي ينتمي العنصر إليه، فصفة المواطن في جريمة الالتحاق بقوات العدو، تثبت وفقًا لقانون الجنسية، في حين أن الأركان العامة للجريمة تخضع في إثباتها للقواعد المقررة للإثبات في المسائل الجزائية.

بتطبيق ما سبق، على جريمة الابتزاز الإلكتروني، نجد أن النطاق الذي يجب أن تقع فيه الجريمة هو البيئة الرقمية، أي يجب أن تقع الجريمة عبر وسيلة من الوسائل الإلكترونية، إذا تقع الجريمة من خلال الشبكة المعلوماتية.

فقد نصت المادة (2) من قانون الجرائم الإلكترونية الأردني رقم (27) لسنة (2015)، على **مصطلح نظام المعلومات بأنه:** مجموعة البرامج والأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيًّا، أو إرسالها أو تسلمها، أو معالجتها، أو تخزينها، أو إدارتها، أو عرضها بالوسائل الإلكترونية. **أما الشبكة المعلوماتية فهي:** ارتباط بين أكثر من نظام معلومات لإتاحة البيانات والمعلومات والحصول عليها، أو هي إحدى وسائل تقنية المعلومات، فقد نصت المادة (1) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة (2018) بأنّ **تقنية المعلومات:** أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًّا أو لاسلكيًّا. **أما شبكة معلوماتية:** فهي مجموعة من الأجهزة أو نظم المعلومات مرتبطة معًا، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة،

وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليه، وبالتالي اذا اقترفت هذه الجريمة خارج نطاق هاتين الوسيلتين، فلا نكون بصدد جريمة الابتزاز الإلكتروني.

مما تقدم تتضح لنا ضرورة أن تقع جريمة الابتزاز الإلكتروني عبر الشبكة المعلوماتية، مثل: الفيس بوك، أو الواتس آب، أو الإنسغرام، أو ماسنجر، أو بواسطة أي وسيلة من وسائل التقنية الحديثة مثل: الهاتف المحمول، أو الحاسب الآلي الشخصي، وإلّا انتفت عنها صفة جريمة الابتزاز الإلكتروني، وإن كان من الممكن أن تشكل جريمة أخرى وهي جريمة التهديد التقليدية المنصوص عليها في قانون العقوبات الأردني والمصري.

الفرع الثاني: الركن المادي لجريمة الابتزاز الإلكتروني:

الركن المادي للجريمة هو مادياتها، أي كل ما يدخل في كيانها، وتكون له طبيعة مادية فتلمسه الحواس(*). وللركن المادي خصوصية، فلا يعرف القانون جرائم بغير ركن مادي، إذ بغير ماديات ملموسة لا ينال المجتمع اضطرابًا، ولا يصيب الحقوق الجديرة بالحماية عدوان (Bilal, 2014).

فقد نصت المادة (4/327) من قانون العقوبات المصري على أنه: "كل تهديد سواء أكان كتابة أم شفهيًّا بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة، يعاقب عليه بالحبس مدة لا تزيد على ستة أشهر، أو بغرامة لا تزيد على مائتي جنيه".

بالإضافة إلى ذلك، فإن قيام الجريمة على ركن مادي، يجعل إقامة الدليل عليها ميسورًا، إذ إنّ إثبات الماديات سهل، فهو يقي الأفراد من احتمال أن تؤاخذهم السلطات العامة دون أن يصدر عنهم سلوك مادي محدد، فتعصف بأمنهم وحرياتهم. ويمثل الركن المادي المظهر الخارجي للجريمة فهو عبارة عن السلوك الإجرامي الخارجي الذي يعاقب عليه القانون سواء أكان فعلاً أم امتناعًا (Al–Amira, 2018).

وفيما يتعلق بجريمة الابتزاز الإلكتروني، إن السلوك الإجرامي في الجريمة يرتبط عمومًا بالمعلومة المخزنة على الحاسوب، أو تلك التي يتم إدخالها، فالجريمة الإلكترونية يتطلب ارتكاب ركنها المادي أن يتوافر القدر اللازم من العلم والإدراك لاستخدام هذه التقنية، فهي تتم عبر شركة الإنترنت، أو باستخدام نظام المعالجة الآلية للمعطيات، مثل المصرفي الذي ينوي سرقة مبالغ مالية من المصرف الذي يعمل فيه باستخدام الإنترنت، ثم الدخول لشبكة المصرف عبر مزودات مجهولة؛ عن طريق الاستعانة ببرامج اختراق توفرها مراكز خاصّة للهاكرز (Mohsen, 2015).

والواقع أن مسألة إمكانية الابتزاز على نظام الحاسب، وإيقاعه في غلط، قد اختلف بشأنها الفقه والتشريع، سواء المصري منه أو المقارن، وبالتالي فإننا نتناول موقف الفقه والتشريعات من هذه المسألة، حيث يمكننا أن نقسّم هذا الموقف إلى اتجاهين هما:

الاتجاه الأول: يرى عدم إمكانية وقوع فعل الابتزاز على الحاسب، وإيقاعه في غلط، وبالتالي لا تتوافر جريمة النصب في حق من ارتكب هذا الفعل، ويبررون رأيهم هذا بالقول بأنه يجب لكي تتوافر هذه الجريمة أن يكون الجاني والمجني عليه أشخاصًا طبيعيين، وبالتالي فهو متصور يقضي بخداع الشخص المكلف بمراقبة البيانات، أو مراجعتها، أو فحصها (Abdelaziz, 2018).

والاتجاه الثاني: يرى إمكانية وقوع فعل الابتزاز على الحاسب، ومن المتصوّر إيقاعه في غلط، وهذا الاتجاه تمثله تشريعات الدول الأنجلوسكسونية، وبعض التشريعات الصادرة في بعض ولايات الولايات المتحدة، وجانب من الفقه الفرنسي (Bilal, 2014).

ويستند هذا الاتجاه على حكم محكمة النقض الفرنسية القاضي بتطبيق عقوبة النصب على شخص دخل بسيارته إلى أماكن انتظار السيارات، فبدلًا من وضع النقود الأصلية المطلوبة في عداد أماكن الانتظار، قام بوضع قطعة معدنية عديمة القيمة فيه، ويترتب على ذلك تشغيل الماكينة وتحريك العقارب، حيث أسست المحكمة حكمها على أن وضع قطعة معدنية عديمة القيمة في العداد، يعدّ من قبيل الطرق الاحتيالية، ويدعم هذا الاتجاه أيضًا جانبًا من الفقه المصري، بأنّ غش العدادات والأجهزة الحسابية نوعٌ من تجسيد الكذب الذي يتحقق به الطرق الاحتيالية (Hosni, 1989, p. 45).

الفرع الثالث: الركن المعنوي لجريمة الابتزاز الإلكتروني:

يحتوى الركن المعنوي (L'élément moral) العناصر النفسية للجريمة، ويعني ذلك أن الجريمة ليست كيانًا ماديًّا خالصًا قوامه الفعل وآثاره، ولكنها كذلك كيان نفسي (Merle & Viru, 1997). ويمثل الركن المعنوي الأصول النفسية لماديات الجريمة، والسيطرة النفسية عليها؛ ذلك أن هذه الماديات لا تعني المُشرّع إلا إذا صدرت عن إنسان يُسأل عنها، ويتحمل العقاب المقرر لها (Almaraghi, 2018).

إنَّ المشرّع الأردني لم يتعرض إلى مفهوم القصد الجنائي، واكتفى بالنص في الجرائم المُعمّدة، دون الحديث عن الجرائم الخطأ التي تقع نتيجة إهمال وتقصير، ومن هنا فإن الركن المعنوي في الجريمة يتكون من العلم والإرادة، حيث إنّ الجريمة قد تقع نتيجة اتجاه الإرادة إلى إحداث النتيجة، وقد تقع نتيجة الأهمال ووعد الابتزاز.

ومن هنا نقول إن الركن المعنوي في الجرائم الالكترونية يتخذ صورة الجريمة العمدية، على اعتبار أن الجاني خطط ودبر لارتكاب جريمته؛ من أجل الحصول على المعلومات، أو لاختراق شبكة الحاسوب، أو

(*) راجع تفصيلًا حكم المحكمة الدستورية العليا المصرية: في القضية رقم (12) لسنة 13 ق دستورية، جلسة 1992/12/3، الجريدة الرسمية، العدد رقم (49)، متاح على موقع المحكمة الدستورية العليا، تاريخ الدخول 2022/5/10، https://www.sccourt.gov.eg/

الاعتداء على أنظمة المعالجة الآلية للمعطيات، سواء بالإدخال أو المحو أو التعديل.

ويتطلّب الركن المعنوي لكل جريمة التحديد الدقيق للمسؤولية الجنائية، من حيث توافر القصد الجنائي في جرائم التهديد بالإفشاء، أو نسبة أمور شائنة، أو التهديد من أجل الحصول على مال، أو أوراق مالية، أو على توقيع، أو على تسليم ورقة، من هنا يستوجب هذا الركن ارتكاب الجاني الفعل المكون للجريمة عن علم بأن الفعل يترتب عليه المساس بالضحية. وتأسيسًا على ما سبق، فإنّ القصد الجنائي في جريمة الابتزاز الالكتروني، يَشترطُ توافر عنصرين هما:

1- **العلم:** ويقصد به علم الجاني بنتيجة النشاط الذي يقوم به، وما يتصل به من وقائع لها علاقة بالجريمة، على أنَّ انتفاء علم الجاني، ينتفي معه القصد الجنائي كما لو حصل على المعلومات بالغلط أو بالصدفة (Izzat, 2010).

2- **الإرادة:** ويقصد به الدافع الأساسي لاتخاذ سلوك إجرامي معين لتحقيق نتيجة محددة، لذلك يجب أن تكون إرادة السلوك والنتيجة متلازمتين في الوقت نفسه، كمن ينوي القيام بابتزاز فتاة كونه يتوفر على معلومات سريّة خاصة بها، بحيث متى علم بها الغير أثّرت على سمعتها، وفي الوقت نفسه يريد تحقيق النتيجة في حصوله على المال كمقابل لكتم السرّ (Abdelaziz, 2018).

فقد قضت محكمة التمييز الأردنية بأنه: "إنَّ قيام المتهم (المميز) بتهديد المشتكية إذا لم تحضر له مبلغ عشرين ألف دينار، سوف يقوم بفضحها ونشر صورها وهي عارية، فإن أفعاله تلك تشكل بالتطبيق القانوني سائر أركان وعناصر جنحة الابتزاز بحدود المادة (2/415) من قانون العقوبات، ودلالة المادة (15) من قانون الجرائم الإلكترونية، كما نجد أن أفعال المتهم المتمثلة بإرسال رسالة تهديد لها عبر الهاتف بأنه سوف يفضحها عند زوجها والعالم إذا لم تعمل ما يريده، تشكل سائر أركان جنحة التهديد وعناصرها طبقًا للمادة (354) من قانون العقوبات.

وبتطبيق القانون على الواقعة الثابتة، وجدت المحكمة أن قيام المتهم بتهديد المشتكية إذا لم تحضر له مبلغ عشرين ألف دينار أنه سوف يقوم بفضحها ونشر صورها وهي عارية، فإنّ هذه الأفعال تشكل كافة أركان جنحة الابتزاز وعناصرها بحدود المادة (2/415) من قانون العقوبات، وبدلالة المادة (15) من قانون الجرائم الإلكترونية"[*].

مما تقدم نرى أنّ جريمة الابتزاز الإلكتروني من الجرائم التي تحتاج إلى معرفة خاصة وعالية بتكنولوجيا المعلومات من أجل تنفيذها، بحيث لا يمكننا أن نتصور إمكانية حصولها بغير قصد، فهي من الجرائم العمدية التي يكتفى فيها بالقصد العام، ولا يشترط أن يكون القصد خاصًا.

المبحث الثاني

مسلك التشريعات في مواجهة جريمة الابتزاز الإلكتروني.

تمهيد وتقسيم:

ساهم التقدم الهائل الذي أضحى واضحًا في المجال التكنولوجي، والزيادة المطّردة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة، من أشخاص طبيعيين، أو هيئات وأشخاص معنوية، وكذلك الاستخدام المتزايد لوسائل التواصل الاجتماعي، كل ذلك ساهم في ظهور فئة جديدة من الإجرام، مرتبطة بالتكنولوجيا، ومنها جرائم الابتزاز الإلكتروني (Al-Shabib, 2020) ، ونظرًا لتزايد نسب ارتكاب هذه الجريمة في الآونة الأخيرة، ونظرًا لأنّ جريمة الابتزاز الإلكتروني لها خصوصية، ووسائل وطرق تنفذ بها، كلّ ذلك أدى إلى انعكاس هذه الخصوصية على مضمون القوانين، حتى تنسجم مع طبيعة الجريمة، ومعطياتها، وآثارها.

في ضوء ذلك، نتناول في المطلب الأول، الأسباب الرئيسة للتدخل التشريعي لتوقي جريمة الابتزاز الإلكتروني، ثم في مطلب ثاني، نوضح صعوبات إثبات جريمة الابتزاز الإلكتروني، على النحو الآتي:

المطلب الأول

الأسباب الرئيسة للتدخل التشريعي لتوقّي جريمة الابتزاز الإلكتروني:

إنَّ الابتزاز الإلكتروني في تزايد دائمًا، ممّا يؤثر على الفرد والمجتمع؛ وذلك بسبب الجهل بسلبيات التعامل مع تقنيات المعلومات والاتصالات، أو بسبب التهور وغياب الوازع الديني والأخلاقي مع كثير من الشباب والرجال والنساء، وعلى حسب نوع الوسيلة التي ارتُكبت بها الجريمة، والغاية أو الهدف من ارتكاب هذه الأفعال غير المشروعة.

الفرع الأول:

الأسباب الرئيسة لتدخل المشرِّع الأردني والمصري في مكافحة الجريمة:

أولًا: تعدّ الجرائم (الابتزاز الإلكتروني) هي إحدى الجرائم الخطيرة على الفرد؛ والتي وجدت مع التقدم التكنولوجي التي شهدتها المجتمعات الإنسانية، حيث لاحت في الأفق تلك الجرائم الحديثة بعد الاستخدام المفرط لتلك التقنيات، والاستخدام السلبي لها، والتغير الواضح في علاقات المجتمعات وسلوكاتها، والاعتماد على التقنية في علاقات

---

[*] انظر حكم محكمة التمييز بصفتها الجزائية في القضية رقم (2:175) لسنة 2020م، بجلسة 2020/9/30، متاح على موقع قرارك الأردني، تاريخ الاطلاع 2022/5/10، https://qarark.com/courts?page

الأفراد، حيث تنشأ تلك العلاقات بين فئات المجتمع، والتي تكون غالبًا مع شخص مجهول للآخر –مجرد لقب فقط– في البداية، ثم تتطور تلك العلاقة وتصبح علاقة أقوى، إما أن تكون علاقة صداقة، أو علاقة حب، أو علاقة تجارة، أو غيرها من العلاقات بين فئات المجتمع (Ahmed, 2015).

ثانيًا: من الآثار السلبية للابتزاز الإلكتروني على الفرد: كونه أسلوبًا من أساليب الضغط والإكراه على المجني عليه، يمارسه الجاني لتحقيق مقاصده الإجرامية، وإلا سينشر المعلومات التي يحتفظ بها على الملأ، فيجد المجني عليه نفسه مرغمًا على التنفيذ، ويصبح مسلوب الحرية والإرادة؛ تفاديًا للتشهير والفضيحة، وهي صورة من الصور القبيحة التي تحملها نفس الجاني، وفيها من الدناءة والوضوح ما تشمئز منه النفوس السليمة، حيث يستغل ثقة شخص استأمنه، ثم يبدأ بالضغط والإكراه وممارسة قوته أمام ضعف الضحية التي لا تجد مخرجًا سوى القبول بتلك الرغبات الدنيئة، وإلا تحمل العواقب الوخيمة التي ستلحق بها، وقد تكون الضحية سببًا في استمرار الابتزاز لخشيتها إبلاغ ذويها، بما تتعرض له خوفًا من تعمق المشكلة، وتعرضها للضرر الجسدي والنفسي منهما (Al–Hermel, 2009, p. 45).

فقد قضت محكمة التمييز الأردنية بأنه: "وفي الشهر الثالث من عام (2021)، فقدت المشتكية هاتفها، وبعد فترة من الوقت ورد المشتكية من حساب يدعى (ن.ف) طلب صداقة، وأصبح هناك تواصل بين المشتكية وذلك الحساب، وفـــي ضوء ذلك أخبرت المشتكية صاحبة حساب (ن. ف) عن طريق الرسائل عن فقدان هاتفها، حيث وعدت صاحبة الحساب في ضوء علاقتها استطاعتها بإحضار الهاتف، وعلى أثرها قامت المشتكية بإعطاء الحساب (ن. ف) الرقم التسلسلي والرقم السري لهاتفها، وبعدها أصبحت المشتكية تتواصل مع حساب يدعى (خ. ت)، وأصبح ذلك الحساب يهدد المشتكية بالصور الموجودة على هاتفها؛ كونه أصبح يرسل لها صورها، وطلب منها أن تقوم بإجراء مكالمة فيديو معه، وأن تقوم بتصوير نفسها وهي عارية، حيث قامت المشتكية بتصوير نفسها عارية وإرسالها لذلك الحساب، حيث قام صاحب ذلك الحساب بتهديدها وابتزازها وأن تقوم بتحويل نقود له، وبالفعل ونظرًا للتهديد قامت المشتكية بوضع محارم بدل النقود، وإرسالها للمكان المطلوب من قبل صاحب الحساب، وبعدها قامت بشطب حسابها، بعدها قام المتهم بإعداد صفحة فيسبوك عليها صورة المشتكية وقام من خلالها بإرسال صورة المشتكية وهي عارية إلى شقيق المشتكية (ط)، وبعدها تواصل المتهم مع شقيق المشتكية، وطلب منه مبلغ ألفـي دينار لعدم قيامه بإرسال أي صورة لشقيقته، حيث قام شقيقها بالتواصل مع الجرائم الإلكترونية، وتم عمل كمين له، وتم إلقاء القبض على المتهم، وتم إرسال رسائل من هاتف شقيق المشتكية إلى صاحب حساب (خ. ت) نفسه، حيث وردت الرسالة على تلفون هاتف المتهم، وبعد فتحه تبين وجود كامل صور المشتكية على هاتف المتهم، وعلى هذا الأساس تم ضبط المتهم وجرت الملاحقة"[*].

وبتحليل هذه الحكم، يتضح أنَّ ما قام به المتهم من إجبار المشتكية من خلال ابتزازها بتلك الصور من أجل أخذ مبالغ مالية، فإن أفعاله تشكل جنحة الابتزاز وفقًا لأحكام المادة (2/415) عقوبات، وكذلك قيام المتهم بإنشاء موقع إلكتروني مدعيًا فيه أنه يعود للمشتكية دون معرفة المشتكية أو علمها، فإن أفعاله تشكل جنحة مخالفة أحكام المادة (3/ج) من قانون الجرائم الإلكترونية.

ثالثًا: الآثار المادية لجريمة الابتزاز الإلكتروني، حيث يعتبر الابتزاز الإلكتروني وسيلة للكسب المادي من المجني عليه، والحصول على مبالغ كبيرة مقابل الاحتفاظ بما لديه من أسرار، خاصة وعندما تكون الضحية إحدى الشركات الكبرى في الدولة، أو المؤسسات ذات القيمة المالية العالية، أو يكون المجني عليه من الميسورين ماديًا؛ مما يجعل الجاني مسيطرًا سيطرة معنوية على المجني عليه، ومؤثِّرًا على إرادته ونفسيته، فيدفع المبالغ الكبيرة والأموال الطائلة؛ حفاظًا على السمعة، وخوفًا من التشهير.

رابعًا: الآثار على سمعة الضحية، حيث يستطيع الجاني إشباع رغباته الجنسية، عندما تكون الضحية امرأة، أو حدثًا صغيرًا، فيفعل الفاحشة بالضحية رغمًا عن إرادتها؛ تحقيقًا لرغباته وإشباعًا لنزواته، وقد يصل الأمر إلى أبعد من ذلك، فيسيطر الجاني على الضحية ويتحكم بها معنويًا؛ مما يؤدي إلى ارتكاب المجني عليه جرائم أخرى بطلب من الجاني، فتكون الضحية وسيلة الجاني في ارتكاب الجرائم التي يريد كالسرقة، والإجهاض، والقوادة، والقتل، وترويج المخدرات... إلخ، وينفذ الضحية ما يمليه عليه الجاني مهما كانت خطورته وصعوبته؛ ليكسب رضاه، ويضمن عدم افتضاح أمره.

الفرع الثاني:

صعوبات مواجهة جريمة الابتزاز الإلكتروني:

إن جرائم الابتزاز الإلكتروني لها العديد من الآثار الخطيرة على المجتمع، ويُمكن بيانها وفق الآتي:

1– جرائم صعبة الاثبات والوصول إليها:

تتميز جريمة الابتزاز الإلكتروني بأنها لا تترك أثاراً مادية عند القيام بها (فلا وجود لجثة أو بقع دم)، وبالتالي من الصعب اكتشافها، فكل ما يحدث فيها هي مجرد تحرك وانتقال لذبذبات ونبضات إلكترونية من خلال استخدام النظم المعلوماتية، وشبكات الاتصال (Baghdadi, 2018).

---

[*] حكم محكمة التمييز بصفتها الجزائية الأردنية رقم (1323) لسنة 2022، بجلسة 2022/7/17، متاح على موقع قرارك الأردني.

كما أن أدلة الادانة فيها في الغالب غير كافية، ويرجع ذلك بما أوضحناه سابقًا، إلى عدم وجود آثار مادية ملموسة، فيتم نقل المعلومات عن طريق النبضات المغناطيسية، كما أنّ الجاني يستطيع تدمير دليل الإدانة في وقت وجيز، يضاف إلى ذلك نقص الخبرة العلمية للشرطة القضائية ورجال القضاء، وعدم كفاية القوانين الإجرائية القائمة (Abdelmotaleb, 2006).

وهذا يرجع –بطبيعة الحال– إلى أنها تختلف عن الجرائم التقليدية لأنها تتم في بيئة افتراضية، ولا تترك أي آثار خارجية، كما يملك الجاني القدرة على محو آثار جريمته؛ مما يصعب الأمر على سلطات التحري في كشف الجريمة، وتقديم المتهم إلى العدالة، كما يصعّب من اكتشافها أنها لا تحتاج إلى وجود المتهم في مكان الجريمة، حيث يمكن أن ترتكب وتنفذ في دولة بعيدة عن مكان إقامة المتهم (Izzat, 2010). وما يصعّب من اكتشافها أن المجني عليه في جريمة الابتزاز يؤدّي دورًا سلبيًّا في الكشف عنها، فهو يمتنع في الغالب عن التبليغ عنها لسببين: الأول صعوبة تحديد هوية المجرم الإلكتروني، وثانيًا التحديثات التقنية لاستخلاص الدليل الإلكتروني، حيث نجد أنّ بعض المجني عليهم يمتنعون عن إبلاغ السلطات المختصة خشية على السمعة والمنصب، وعدم اهتزاز الثقة مع المتعامل معها، خاصة إذا كانت شركات كبرى، مع أن هذه الجرائم قد يترتب عليها خسائر مادية كبيرة لهذه الشركات.

2– طبيعة جريمة الابتزاز الإلكتروني جريمة عابرة للحدود:

مع انتشار شبكة الاتصالات العالمية والإنترنت، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر، حيث لا يعترف المجتمع المعلوماتي بالحدود الجغرافية، فالشبكات تخترق الزمان والمكان، خاصة عندما ظهرت شبكات المعلومات الدولية؛ أي الإنترنت، حيث إن القائم على النظام المعلوماتي في أي دولة يمكنه أن يحول مبلغًا من المال لأي مكان في العالم، مضيفًا له صفرًا أو بعض أصفار لحسابه الخاص، بل يستطيع الشخص أن يعرف كلمة السر لأي شبكة في العالم، ويتصل بها، ويغير ما بها من معلومات. ولأنّ المشرّع الأردني يعلم بهذه الخاصيّة، ولأجل مكافحة الجرائم الإلكترونية، قام المشرّع العُماني بالتصديق على نصوص الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، حيث جاءت المادة الأولى ونصت على: "تهدف الاتفاقية إلى تعزيز التعاون العربي لمنع ومكافحة الجرائم المنظمة عبر الحدود الوطنية"(*).

كما قام المشرّع الأردني أيضًا بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي تنص في مادتها الأولى على: "تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظًا على أمن الدول العربية ومصالحها، وسلامة مجتمعاتها وأفرادها"(**).

حيث من المفترض أن تكون هذه الاتفاقيات إضافة جديدة في مجال مكافحة الجرائم الإلكترونية في الأردن ومصر، وتحقق الغرض منها في منع الجريمة الإلكترونية ومكافحتها بكل أشكالها وصورها، ومن ضمنها جريمة الابتزاز الإلكتروني.

3– جرائم الابتزاز عبارة عن جرائم هادئة ولا تحتاج إلى العنف:

تمتاز الجرائم الإلكترونية بأنها جرائم ناعمة لا تتطلب عنفًا، وهي في ذلك تختلف عن الجرائم التقليدية التي تتطلب أحيانًا استخدام العنف، كما في جرائم القتل والضرب، بل تتطلب مواصفات خاصة كالذكاء، وامتلاك الوسائل المناسبة، وقدرة على التعامل مع شبكة الإنترنت، حيث إن الدخول غير المشروع للحاسوب، أو القرصنة والسطو الإلكتروني على الأرصدة وبيانات بطاقات الائتمان، لا يتطلب أي عنف سواء أكان ماديًّا أم معنويًّا، ولا يبذل فيه الجاني أي جهد عضلي، فهي جرائم هادئة بطبيعتها (Al–Maaiaa, 2021).

وقد قضت محكمة النقض المصرية بأنه: "لما كانت جناية التهديد المنصوص عليها في الفقرة الأولى من المادة (٣٢٧) من قانون العقوبات، تتوافر إذا وقع التهديد كتابة بارتكاب جريمة ضد النفس أو المال، وكان التهديد مصحوبًا بطلب، أو تكليف بأمر، وكان الحكم قد أورد بأسبابه قيام الطاعن بتهديد المجني عليهما عبر مواقع التواصل الاجتماعي، وتمكّن من خداعهما، وتحصل منهما على صور ومقاطع مرئية في أوضاع مخلة بالحياء وهددهما بنشرها، وإذ كان مصطلح الكتابة قد ورد في المادة (٣٢٧) سالفة الذكر على سبيل البيان في صيغة عامة، لتشمل كافة وسائل الكتابة المختلفة سواء كانت بالطرق التقليدية أو بإحدى الوسائل الإلكترونية الحديثة ، فإذا أثبت الحكم على الطاعن إرساله عبارات التهديد عن طريق الوسائط الإلكترونية الحديثة –وهي لوحة المفاتيح– بقصد إيقاع الخوف في نفس المجني عليهما لحملهما على أداء ما هو مطلوب، فإنه يكون قد استظهر أركان جريمة

(*) انظر: الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، على الموقع الالكتروني التالي، تاريخ الاطلاع 2022/5/11:
http://haqqi.info/ar/haqqi/legislation/arab-convention-against-transnational-organized-crime.

(**) انظر: الاتفاقية العربية لمكافحة جرائم تقية المعلومات، متاح على الموقع الإلكتروني الآتي، تاريخ الاطلاع 2022/5/11:
http://haqqi.info/ar/haqqi/legislation/arab-convention-cyber%E2%80%8B%E2%80%8Bcrimes

التهديد كما هي معرفة به في القانون، ويضحى منع الطاعن في هذا الشأن على غير أساس"[*].

ومن جانبنا نرى الابتزاز صورة من صور التهديد، حيث يتطلب فيه الحصول على مقابل من الضحية، وقد يكون هذا المقابل منفعة مادية أو معنوية، كالمبالغ المالية أو العلاقات الجنسية وغيرها، التي تؤثر على الفرد والمجتمع، وقد يكون بهدف الانتقام من الضحية كرد فعل عن فعل صدر منها.

المطلب الثاني.

صعوبات إثبات جريمة الابتزاز الإلكتروني والعقوبات المحددة:

ترتكب جريمة الابتزاز الإلكتروني في مسرح غير قابل للتحديد الجغرافي، إلا أنه يضم أكبر تجمع إنساني يتميز بارتباط وتشابك معقد، وتتمثل أهم خصائصه في خلق آليات خاصة لفرض العقوبات على من ارتكب تهديدًا، أو ابتز أحد الأشخاص عبر الشبكة المعلوماتية (Al–Ajami, 2014)، ولكن ما هي الوسائل والآليات التي وضعها القانون الأردني والمصري في مكافحة جريمة الابتزاز الإلكتروني، وهذا ما سنوضحه وفق النحو الآتي:

الفرع الأول:

تحديد المسؤولية الجزائية عن جريمة الابتزاز الإلكتروني:

ذهب جانب فقهي بأن المسؤولية الجزائية هي الالتزام بتحمل الجزاء المقرر للجريمة قانونًا، ويتطلب للمسؤولية الجزائية ركنين: الركن المادي وهو وقوع الجريمة، والأصل أن المسؤول جزائيًا هو الشخص الطبيعي؛ لأن أساسها هو الإرادة التي لا تتوافر إلا للشخص الطبيعي، وبالتالي إذا كان مَن اقترف الجريمة شخصًا طبيعيًا، فلا ملاءمة في تطبيق العقوبة المقررة قانونًا (Manchawi, 2021).

أما بالنسبة لمسؤولية الشخص المعنوي في جريمة الابتزاز الإلكتروني، فقد نصت المادة (35) من قانون جرائم تقنية المعلومات المصري رقم (175) لسنة (2018) على أنه: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنية، ولا تزيد عن مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مسؤول عن الإدارة الفعلية لأي شخص اعتباري، إذا تعرض الموقع، أو الحساب الخاص، أو البريد الإلكتروني، أو النظام المعلوماتي المخصص للكيان الذى يديره، لأي جريمة من الجرائم المنصوص عليها في هذا القانون، ولم يبلغ بذلك الجهات المختصة وقت علمه بالجريمة".

وقضت محكمة التمييز الأردنية بأنه: "طلب المتهم من المجني عليها (د) أن تقوم بإرسال صورها وهي عارية الصدر له، وكانت وقتها بعمر يتجاوز الثامنة عشرة، وكان ذلك بموافقتها ورغبتها، حيث كانت على علاقة غرامية معه وفق ما ورد بشهادتها، حيث ذكرت بشهادتها (علمًا بأنني كنت ارتبط مع المتهم بعلاقة غرامية، وكنت قد أرسلت له صورًا وأنا عارية الصدر، وكان عمري وقتها (25) سنة .. بعد أن تعمقت علاقتي مع المتهم كان يحضر المتهم إلى باب المنزل، ويأخذ مني مصاري، وأنا كنت أعطيه من باب المساعدة وبرضاي، المتهم حضر إلى منزلي مرتين في النهار، وشرب القهوة أثناء وجود زوجي في العمل، في إحدى المرات دخل المتهم وجلست معه في الصالون داخل منزلي مدة ربع ساعة، وبعدها غادر وكان عمري (24) سنة، أنا كنت أقبل المتهم وهو يقبلني ونحضن بعضنا وتربطني به علاقة).

وعملًا بأحكام المادتين (1/52 و1/426) من قانون العقوبات، بإسقاط دعوى الحق العام عن المتهم (م.ح.م.س) بالنسبة لجنحة تهديد شخص بفضح أمره وإفشائه بشكل ينال من قدر هذا الشخص وفقًا لأحكام المادة (1/415) من قانون العقوبات، وبدلالة المادة (15) من قانون الجرائم الإلكترونية، وجنحة ابتزاز شخص لكي يحمله على جلب منفعة غير مشروعة له وفقًا لأحكام المادة (2/415) من قانون العقوبات، وبدلالة المادة (15) من قانون الجرائم الإلكترونية، وذلك لإسقاط المشتكية رانية والمشتكية دعاء حقهما الشخصي عن المتهم"[*].

ممَّا تقدم، نرى أنَّ المسؤولية الجزائية التي تقع على المبتزّ أو المهدد سواء أكان شخصًا طبيعيًّا أم شخصًا معنويًّا، وقيام المبتزّ بطرق احتيالية الحصول على البيانات والمعلومات الإلكترونية الخاصة بالضحية، تقترن بوجوب توفير الحماية القانونية للضحايا من الابتزاز الإلكتروني.

الفرع الثاني:

معالجة الصعوبات التي تواجه السلطات المختصة في الإثبات:

تتنوع الصعوبات التي تواجه السلطات في الإثبات باستخدام الدليل الرقمي، وذلك بسبب العديد من الأسباب، وهي:

1- **سهولة محو الدليل:** حيث إنّ الجناة بعد ارتكابهم للجريمة يكون منهم الحريص، سيما وأن المجرم الإلكتروني، في جريمة الابتزاز،

---

[*] انظر: حكم محكمة النقض المصرية في الطعن رقم 22620 لسنة 88 قضائية، الدوائر الجنائية، جلسة 2020/7/9، متاح على موقع محكمة النقض المصرية، تاريخ الاطلاع 2022/5/11، https://www.cc.gov.eg/judgment_single?id=111399002&ja=277482

[*] انظر: حكم محكمة التمييز بصفتها الجزائية في القضية رقم (393) لسنة2021، بجلسة 2021/3/30، متاح على موقع قرارك الأردني، https://qarark.com/courts?page

بعد قيامه بتهديد المجني عليه، يقوم بمحو آثار جريمته؛ مما يجعل الوصول للدليل عسيرًا، وفي بعض الأحيان يكون مستحيلًا.

2- **معوّقات لها علاقة بكشف هوية الجاني من خلال الدليل الرقمي:** تختلف جريمة الابتزاز الإلكتروني عن جريمة الابتزاز التقليدية، في أن الأولى تحدث في عالم افتراضي تحكمه الرموز والبيانات، يخلو من العنف والآثار المادية كجريمة الابتزاز التقليدية؛ مما يصعب معه التوصل لدليل مادي كبصمة الإصبع، أو نقطة دم؛ مما يجعل الوصول إلى الجاني معترضًا بالعقبات (Al–Qahtani, 2014).

3- **عرقلة الوصول إلى الدليل:** ففي بعض الحالات يضع الجاني عقبات فنية وتقنية لمنع كشف جريمته واكتشاف أدلتها، وذلك كأنظمة التشفير؛ بقصد حجب المعلومات عن التداول العام، ومنع الوصول إلى مصدر الإرسال.

4- **نقص خبرة بعض العاملين في جهات التحقيق:** فمن ضمن الصعوبات التي تواجه عملية الحصول على الأدلة الرقمية في جريمة الابتزاز الإلكتروني، نقص الخبرة لدى بعض العاملين من رجال الضبط الجنائي، وأعضاء هيئات التحقيق، وذلك فيما يتعلق بأجهزة الحاسوب وملحقاتها، ولغة الحاسوب، ومهارات تتعلق باستجواب مجرم ذكي كالمجرم الإلكتروني في جريمة الابتزاز الإلكتروني (Abdelaziz, 2018).

مما تقدم يتضح لنا ضرورة الاهتمام بتدريب العنصر البشري وتأهيله، كالمحققين والجهات المعاونة؛ وذلك لمواكبة التقدم السريع في مسائل الجريمة الرقمية بشكل عام، والابتزاز الإلكتروني بوجه خاص.

5- **الإحجام عن الإبلاغ من المجني عليه:** فقد يرجع إلى خوف المجني عليه من الإبلاغ كي لا يفتضح أمره، فهذه الجريمة ارتكبت في الأساس بسبب خوف المجني عليه من أن تتكشف أسراره، وبالتالي فإن هذا الإحجام يساعد على اختفاء الدليل الرقمي الذي يدل على الجاني؛ مما يجعل هذا السبب عقبة خطيرة تقف في طريق الإثبات عن طريق الدليل الإلكتروني(*).

6- **عدم وجود آلية تشريعية موحدة:** فيوجد اختلاف بين التشريعات، في تجريم أفعال الابتزاز الإلكتروني مختلفة في دولة عن أخرى، مما يجعل ملاحقة الجاني تمر بعقبات وعراقيل، فما تراه دولة مباح تراه أخرى مجرم، وعلى ذلك نرى أن الحاجة ماسة إلى وضع تشريعات جزائية دولية موحدة، أكثر مرونة حتى تواكب سرعة التقدم في الإجرام الرقمي.

بعد سرد هذه الصعوبات التي تواجه إثبات جريمة الابتزاز الإلكتروني، فيكف يتم معالجة هذه الصعوبات؟ قد نرى أنه لإثبات هذه الجريمة وسهولة التعرف على المجرم المرتكب الجريمة، يجب اتخاذ بعض الإجراءات القانونية والتقنية، ومن بينها ما نصت عليها المادة (13) قانون الجرائم الالكترونية الأردني رقم (27) لسنة 2015م، التي نصت على أنه:

"أ– مع مراعاة الشروط والأحكام المقررة في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمه إلى المدعي العام المختص.

ب– مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل المستخدمة لارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

ج– للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل والمواد وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة الفاعل".

الفرع الثالث:

تشديد العقوبات المترتبة على جريمة الابتزاز الإلكتروني

تعدُّ العقوبات من أهم الآثار التي تترتب على تجريم السلوك المعتدي، لذا نظم المشرّع كل فعلٍ أو تركٍ خالفَ نصوصه الموضوعة، وجعل مقابل هذا الفعل أو الترك عقوبة للمجرمين، وهذه العقوبة تأتي لضمان تحقيق الردع الخاص للمجرم، ولتحقيق الردع العام للمجتمع ككل، فللعقوبة وجهان: علاجي ووقائي، وتختلف القوانين المجرّمة في كل دولة، وذلك باختلاف كل سياسة جزائية يتخذها المشرّع ما بين التخفيف أو التشديد في العقوبات (Mohammed, 2020).

(*) انظر: انظر حكم محكمة النقض المصرية في لطعن المقيد برقم 22830 لسنة 88 قضائية، بجلسة 2022/1/24م.
https://www.parlmany.com/News/2

وقد أكد المشرِّعان الأردني والمصري على قناعتهم الشديدة بالاهتمام بالمجتمع بأغلب فئاته، وتخوفه من جريمة الابتزاز الإلكتروني؛ لذا نجده قد جرم هذا السلوك بكل صوره وتعدّياته، ووضع لهذه التعديات عقوبات لتتناسب مع الجريمة التي اقترفها الجاني، ونعرض فيما يأتي العقوبات في القانون الأردني، وكذلك في القانون المصري:

أولًا: العقوبة الأصلية لجريمة الابتزاز الإلكتروني:

إن الصياغة التشريعية لنصوص التجريم والعقاب ليست مجرد إفراغ للنصوص في قوالب شكلية، وإنما هي أولًا وقبل كل شيء فكر قانوني يرد النصوص لضوابطه القانونية، التزامًا بالأصول المنطقية، ومن ثم يدخل فيها التثبت من اتفاق نصوص التشريع المقترح مع مواد النظام الأساسي والقوانين السارية، فضلًا عن إجراء التعديلات التي يقتضيها التجانس بين القوانين التي تشكل النظام القانوني بالدولة، والتناسق والترابط بين نصوص التشريع الواحد، وهو ما نأمل به في نصوص القوانين الجزائية (Al-Safu, 2015).

حيث تباين موقف التشريعات محلّ الدراسة بشأن العقوبة الجزائية المقررة لجريمة الابتزاز الإلكتروني، حيث نص المشرّع الأردني في المادة (11) من قانون الجرائم الإلكترونية رقم (27) لسنة (2015)، بأنه: "يعاقب كل من قام قصدًا بإرسال، أو إعادة إرسال، أو نشر بيانات، أو معلومات عن طريق الشبكة المعلوماتية، أو الموقع الإلكتروني، أو أي نظام معلومات تنطوي على ذمّ، أو قدح، أو تحقير أي شخص بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن (100) مائة دينار، ولا تزيد على (2000) ألفي دينار".

أما المشرِّع المصري فقد سلك مسلكًا قريبًا من موقف المشرّع الأردني، فقد نص في المادة (25) من قانون جرائم تقنية المعلومات المصري رقم (175) لسنة (2018م) بأن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه، ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري، أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام، أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية، أو بإحدى وسائل تقنية المعلومات معلومات، أو أخبارًا، أو صورًا، وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة".

ونرى من سياق المادة السابقة، أن سلطة القاضي تقديرية في أن يجمع بين عقوبتي الحبس والغرامة أو يختار إحداهما، وشدد العقوبة إلى الحبس إذا كانت الجريمة اقترفت لربطها بمحتوى منافٍ للآداب العامة، حيث نصت المادة (26) من قانون جرائم تقنية المعلومات المصري رقم (175) لسنة (2018م)على أنه: "يعاقب بالحبس مدة لا تقل عن سنتين، ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه، ولا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين كل من تعمد استعمال برنامج معلوماتي، أو تقنية معلوماتية في معالجة معطيات شخصية للغير، لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه"، كما عاقب بالسجن المشدد إذا نتج عن الجريمة إضرارٌ بالنظام العام، أو بسلامة المجتمع وأمنه، أو الإضرار بالأمن القومي للبلاد، حيث نصت المادة (34) من قانون جرائم تقنية المعلومات المصري رقم (175) لسنة (2018م) بأنه: "إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون، بغرض الإخلال بالنظام العا،م أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد، أو بمركزها الاقتصادي، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور، أو القوانين، أو اللوائح، أو الإضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدّد".

كما أنه يوجد اختلاف واضح بين التشريعات محل الدراسة من حيث معاملتها العقابية لهذه الجريمة، فمثلًا إذا تم اكتشاف الجريمة من قبل السلطات المختصة وقبل التصرف فيها، ولكن الفاعل الأصلي أو الشريك أدلى بمعلومات كانت السبب في القبض على باقي الجناة، أو ضبط الأموال محل الجريمة، ساعدت على كشف الحقيقة، أو ساعدت على القبض على مرتكبي جريمة أخرى مماثلة لها في النوع والخطورة، فيجوز للقاضي إعفاؤه من العقوبة كاملة وفقًا للقانون الأردني، أما في القانون المصري فيجوز للقاضي في هذه الحالة إعفاؤه من العقوبة كليًا، أو تخفيف هذه العقوبة.

ثانيًا: العقوبة التبعية لجريمة الابتزاز الإلكتروني:

نشير في البداية إلى ما ذهب إليه بعض الفقه (Abdul Atti, 2021) بالقول إن العقوبة التبعية هي العقوبة التي تتبع العقوبة الأصلية للجريمة المحكوم بها ضد المتهم بقوة القانون، دون الحاجة للنص عليها في الحكم، وعليه فتطبق العقوبة التبعية سواء تضمنها الحكم أو لم يتضمنها، ولذلك نلاحظ أن النصوص القانونية المتعلقة بالعقوبة التبعية لجريمة الابتزاز الإلكتروني، قد استخدمت مصطلح يدل على وجوبية تطبيق هذه العقوبات المنصوص عليها في التشريعات محل الدراسة.

فقد نصت المادة (15) من قانون الجرائم الالكترونية الأردني رقم (27) لسنة (2015م) على أنّ: "كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية، أو أي نظام معلومات، أو موقع إلكتروني، أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع".

كما نصت المادة (38) من قانون جرائم تقنية المعلومات المصري رقم (175) لسنة (2018م) على أنه: "مع عدم الإخلال بحقوق الغير

حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون، أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة، مما لا يجوز حيازتها قانونًا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهّل أو ساهم في ارتكابها. وفى الحالات التي يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الاعتباري المدان بأي جريمة منصوص عليها في هذا القانون، لم يحصل على الترخيص، فيحكم فضلًا عن العقوبات المقررة بالغلق".

مما تقدم، يتضح بأن القاضي عند الحكم في جريمة من الجرائم المنصوص عليها في هذا القانون، أن يحكم بإحدى العقوبات التبعية المنصوص عليها في هذا القانون صراحة، وإذا لم يتضمن الحكم أيًا من هذه العقوبات، وجب على الجهات المختصة تطبيق هذه العقوبات، وبذلك وضع التشريعان عقوبة تبعية لجريمة الابتزاز الإلكتروني، تتمثل في **المصادرة والغلق**، سواء مصادرة جميع الأجهزة والأدوات والبرامج وغيرها من الأشياء التي استعملت في ارتكاب الجريمة، وكذلك الأموال المتحصلة منها، وأيضًا غلق الموقع الإلكتروني والمحل الرقمي الذي ارتكبت فيه الجريمة أو الشروع فيها.

الخاتمة:

لقد أدت التطورات الإلكترونية إلى تطور أشكال جديدة من الجريمة الإلكترونية، وهي جريمة غير تقليدية، تتميز بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية؛ وذلك نتيجة ارتباطها بالحاسب الآلي عبر وسائل حديثة ومتطورة، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عددًا من السمات والخصوصية، التي انعكست بدورها على مرتكب هذه الجريمة، الذي أصبح يعرف بالمجرم الإلكتروني لتميّزه أيضًا عن المجرم التقليدي.

لذلك كان موضوع الدراسة المواجهة الجزائية لجريمة الابتزاز الإلكتروني وفقًا للتشريع الأردني "دراسةً مقارنةً بالتشريع المصري"، حيث أصبحت جرائم الابتزاز التي تتم عبر الوسائل الإلكترونية، من الجرائم التي أصبحت تثار في المجتمع الأردني والمصري، خاصة مع تعدد أنواع الاتصال، وسهولة التواصل بين الأشخاص، وبالرغم من ذلك، فكثيرًا ما يتم ربط جرائم الابتزاز بنظام الجرائم الإلكترونية، فتحكم بنصوصها، ولكن قد حددت نص المادة (415) من قانون العقوبات الأردني، وبدلالة نص المادة (15) من قانون الجرائم الإلكترونية أركان جريمة الابتزاز الإلكتروني، وتوافقه مع المادة (327) من قانون العقوبات المصري، بسند من المادة (25) من قانون جرائم تقنية المعلومات المصري، فأيّ صنف من تصنيفات جرائم الابتزاز أو التهديد، يخرج من النص الجنائي، فيترك للقاضي حتى يتم إثباته بالوسائل التقليدية والحديثة.

إذاً أدرك المشرّع الجزائي الأردني مدى خطورة جريمة الابتزاز الإلكتروني، التي انتشرت بعد التقدم العلمي الهائل في وسائل التكنولوجيا الحديثة، فأصدر قانون الجرائم الالكترونية رقم (27) لسنة (2015م)، كما أصدر المشرّع المصري قانون جرائم تقنية المعلومات رقم (175) لسنة (2018م)، لوضع ضوابط قانونية وتقنية لحماية الضحايا؛ بسبب التهديد والابتزاز غير المبرر من المجرمين الإلكترونيين.

النتائج:

1. أدرك المشرّع الجزائي الأردني مدى خطورة جريمة الابتزاز الإلكتروني قديمًا وفق نص المادة (415) من قانون العقوبات الأردني، والمادة (327) من قانون العقوبات المصري، وحديثًا بدلالة المادة (15) من قانون الجرائم الإلكترونية رقم (27) لسنة (2015م)، والمادة (25) من قانون جرائم تقنية المعلومات رقم (175) لسنة (2018م).
2. قبول الدليل الإلكتروني في مجال الإثبات أمام محكمة التمييز الأردنية، ومحكمة النقض المصرية، وذلك لما يمثله من قيمة ثبوتية في مجال جرائم الابتزاز (التهديد) عبر الوسائل الإلكترونية.
3. يشترط لوقوع جريمة الابتزاز الإلكتروني أن يكون بطلب أمر رغمًا عن إرادة المجني عليه، وذلك كأن يطلب منه مالًا ليس من حقه، أو يطلب منه علاقة جنسية، أو أي شيء مباح أو غير مباح.
4. تبين قدرة النصوص التقليدية في التشريع الأردني والمصري عند مواجهة جريمة الابتزاز الإلكتروني، كذلك أعطت التشريعات الحديثة حماية أعلى، وفاعلية أكبر لحماية الضحايا من الابتزاز.
5. كما ظهر لنا جليًّا بأن على الجهات الرقابية المنوط بها مراقبة تقنية المعلومات، متابعة كل ما هو حديث في التقنيات الحديثة، ووضع الحلول الممكنة لمواجهة صعوبات إثبات جريمة الابتزاز الإلكتروني؛ بهدف إحاطة المؤسسات المنوط بها مكافحة الجريمة بجميع هذه الأنشطة.

التوصيات:

1. توصي الدراسة المشرّع الأردني بتجريم ممارسات تشكل جرائم إلكترونية لم يُنصّ عليها في قانون الجرائم الإلكترونية ومنها: الملاحقة الإلكترونية، والتشهير، والمضايقة، وتشويه السمعة سواء أكان عبر الوسائل التقليدية أم الحديثة.
2. يجب عدم الاكتفاء بما ورد في نص المادة (327) من قانون العقوبات المصري، والمادة (15) من قانون الجرائم الإلكترونية والأردني في مكافحة جريمة الابتزاز الإلكتروني.
3. تجب الملاحقة الأمنية المشددة لكل من تسول له نفسه ارتكاب أفعال مجرمة، عبر استخدام وسائل التقنية الحديثة في الملاحقة والتحقيق والإثبات؛ حتى يتحقق الأمن والأمان للمجتمع.

4.دعوة المشرِّع الأردني والمصري إلى التشديد من العقوبة في حالة ثبوت ارتكاب جريمة الابتزاز الإلكتروني، وجعلها من الجنايات، وليس من الجنح البسيطة، وإحالة مرتكبيها على محاكم الجنايات المختصة.

5.ضرورة إنشاء آلية رقابية مستقلة تتمتع بسلطات محددة تتصل بالأخبار والمعلومات المنشورة عبر الوسائل الإلكترونية، وتمنح الحق في فرض عقوبات فيما يخص تجاوز حدود المصداقية، ونشر الشائعات، بما لا يتعارض مع العقوبات المقررة على الجرائم المرتكبة بواسطة الوسائل الإلكترونية، والتي نص عليها قانون العقوبات المصري والأردني.

انسجامًا مع السياسة الجزائية في تشديد العقاب على جريمة الابتزاز الإلكتروني، فلا بدّ من المعاقبة على الشروع بهذه الجريمة، مثل عقوبة الجريمة التامة نفسها.

References:

- Abdelaziz, Dr. Dalia (2018): "Criminal Liability for the Crime of Cyber Extortion", research published in the Journal of the Generation of in-depth Legal Research, No. 25.
- Abdelmotaleb, Dr. Mamdouh Abdel Hamid (2006): Digital Criminal Investigation and Investigation of Computer and Internet Crimes, Law Books House, Cairo.
- Abdul Atti, Dr. Mohammed Saeed, Manchawi, D. Mohamed Ahmed (2021): "The Role of Criminal Law in Protecting Children from Electronic Extortion, Comparative Study", Journal of Jurisprudence and Legal Research, Faculty of Sharia Law, Al-Azhar University, Dakahlia, Egypt, No. 36.
- Abu Bakr, Omar Mohammed (2015): Crimes arising from the use of the Internet, substantive judgments and procedural aspects, Arab Renaissance House, Cairo.
- Ahmed, Dr. Tariq Afifi Tariq (2015): Cybercrime "Mobile Crimes", National Center for Legal Issuances, Cairo.
- Al-Ajami, Abdullah Dagash (2014): "Practical and legal problems of cybercrime, comparative study", master's thesis, Faculty of Law, Middle East University, Jordan.
- Al-Amira, Mohammed Saleh (2012): "Prohibiting the extortion of women in an applied root study", research submitted for completion of a master's degree in criminal justice, Nayef Arab University of Security Sciences, Saudi Arabia.
- Al-Atayanan, Turki Mohammed (2005): "Computer Crime, Psychoanalytic Study", paper presented at the 4th Society and Security Symposium, Contemporary Criminal Phenomena, King Fahd Security College, Riyadh, Saudi Arabia.
- Alhakem, Dr. Mazen Samir (2019): "Electronic extortion of concept, characteristics and ways of confrontation", working paper, Iraqi Ministry of Interior, Documentary Books House, Baghdad, vol II.
- Al-Hermel, Ibrahim Suleiman (2009): "Crimes of extortion of girls and ways to detect and investigate them", working paper presented to the scientific recipient on information crimes organized by the Investigative and Prosecutorial Authority and the Nayef Arab University of Security Sciences from 23-25/10/1430 AH.
- Al-Maaiaa, Thamer Youssef Salem (2021): "Procedural aspects of libel and insult crimes committed through websites", doctoral thesis, Faculty of Law, Ain Shams University, Egypt.
- Al-Mutairi, Tariq Abd al-Razak (1430H): "Provisions for the offence of extortion established in the Saudi system for combating cybercrime", supplementary research for a master's degree at Imam Mohammed bin Saud Islamic University.
- Al-Qahtani, Abdullah bin Hussein Al-Hajraf (2014), "Development of Criminal Investigation Skills in the Face of Cybercrime", Master's Thesis, Faculty of Police Sciences, Naif Arab University of Mini Sciences, Riyadh.
- Al-Safu, Dr. Nufal Abdullah Ali (2015): "Legal Drafting Methods of Criminal Texts, "Comparative Study"", Shari'a and Law Journal, Faculty of Law, University of the United Arab Emirates, No. 62.
- Al-Shabib, Yasser (2020): Article entitled "Information safety", warning against falling into the trap of electronic blackmail, available on the following website, date 10/5/2022, https://alroya.om/p/171532
- Alshamrani, Dr. M. Hamad Saleh Ali (2010): "The phenomenon of extortion in Saudi society from the point of view of criminal control workers", Master's thesis, Faculty of Security Sciences, Nayef University of Security Sciences, Saudi Arabia.
- Arab Convention against Transnational Organized Crime, on the following website:
- Baghdadi, Adham Basem Nimr (2018): Means of Research and Investigation on Cybercrime, Master's Thesis, Faculty of Law, National University of Success, Palestine.
- Bilal, Dr. Ahmed Awad (2014): Principals of Egyptian Penal Code, Section I, Arab Renaissance House, Cairo, Egypt.

- Mehdi, Dr. Abdel Rauf (2008): Explanation of the General Rules of the Penal Code, Part I, Giza Bar Association Edition, Egypt.
- Mohammed, Dr. Assad Abdul Hamid Ibrahim (2020): "The Role of Criminal Policy in Combating the Crime of Cyber Extortion in Saudi Arabia in Islamic Law and Order, "Comparative Study"", Al-Qazzan Scientific Journal, Center for Research and Studies of Red Sea Basin States, No. 5.
- Mohsen, Sinai Abdullah (2015): "Legislative confrontation with computer-related crimes in the light of international and national legislation", regional symposium on "Internet-related crimes", United Nations Programme for the Promotion of the Rule of Law in some Arab States, Kingdom of Morocco.
- Mustafa, Dr. Mahmoud Mohamed (1983): Explanation of the Penal Code/General Section, I1, Arab Renaissance House, Cairo.
- Namor, Mohammed Said (2013): Explanation of Penal Code, Special Section, Offences against Persons, Part I, p. 5, Dar AL-thakafah (Culture House) Press, Amman.
- Noura Abdullah Mohammed Al-Mutlaq (2019): "Extortion of Girls and its Provisions in Islamic Jurisprudence", Imam Mohammed Bin Saud Islamic University, Riyadh.
- Sirur, Dr. Ahmed Fathi (1996): Mediator in the Penal Code/General Section, I6, Arab Renaissance House, Cairo.
- The Arab Convention on Combating Information Prevention Offences, available on the following website, date of 11/5/2022 's access:
- Wazier, Dr. Abdeladim Morsi (1983): Presumed Conditions in Crime, Galilee Printing House, Egypt.
- Zainab Mahmoud Hussein (2021): "Criminal Confrontation of Blackmail", Journal of the Faculty of Law for Legal and Political Sciences, University of Kirkuk, Iraq, MJ10, A37, P568-597
- Contemporary Arabic lexicon, https://www.almaany.com/ar/dict/ar-ar/
- Egyptian Information Technology Crimes Act No. 175 of 2018, published in the Official Gazette, No. 32 bis/c, 14 August 2018.
- Egyptian Penal Code No. 58 of 1937, in accordance with the latest amendment issued on November 20, 2021.
- El Maraghi, Dr. Ahmed Abdella (2018): Mediator in the Commentary on the Penal Code, "Section on Offences against the Public Interest", p. 1, d. N '
- Hamuda, Dr. Ali Mahmoud Ali (2009): "Evidence and assessment of cybercrime", paper presented to the World Conference on Legal and Security Aspects - Dubai Police Academy, Center for Research and Studies No.: 2003 Date 26 April expiry date 28 April 2009 Dubai - United Arab Emirates.
- Hansh, Sarah Mohammed (2020): "Penal Responsibility for Cyber Threat, Comparative Study", Master's Thesis, Faculty of Law, Middle East University, Jordan.
- Hosni, Dr. Mahmoud Najib (1989): Explanation of Penal Code, General Section, T6, Arab Renaissance House, Cairo, 1989.

  http://haqqi.info/ar/haqqi/legislation/arab-convention-against-transnational-organized-crime

  http://haqqi.info/ar/haqqi/legislation/arab-convention-cyber-%E2%80%8B%E2%80%8Bcrimes
- Ibn Manzoor (2005): *Lisan al-Arab*, Part V.
- Izzat, Fathi Mohamed Anwar (2010): Electronic Evidence in Criminal Matters, I2, Arab Renaissance House, Egypt.
- Jordanian Electronic Crimes Act No. 27 of 2015, published in the Official Gazette No. 5343 of 6 January 2015.
- Jordanian Penal Code No. 16 of 1960, in accordance with the latest amendment on alternative penalties for 2022.
- Jordan's Code of Criminal Procedure No. (9) of 1961, promulgated in the Official Gazette No. 1539 of 16 March 1961, on page 311.
- Jordan's Communications Act No. 13 of 1995, promulgated in Official Gazette No. 4072 of 1/10/1995, p. 2939, in accordance with the latest amendments of 2022.
- Kaabi, d. Mohammed Obaid (2009): "Crimes arising from the illicit use of the Internet" I 2, Arab Renaissance house, Cairo.