MESR
منار الشرق للدراسات والأبحاث
Manar Elsharq for Studies & Research
مجلة الشرق الأوسط
للدراسات القانونية والفقهية

الحماية الجنائية للطالب الجامعي من جرائم الابتزاز الإلكتروني

أكرم ماجد خلف

جامعة ذي قار – كلية القانون

akrammajed24@utq.edu.iq

استلام البحث: 05/03/2025	مراجعة البحث: 05/04/2025	قبول البحث:08/05/2025

الملخص:

في عصرنا الحالي، أصبحت الجرائم الإلكترونية تهدد الأفراد والمجتمعات بشكل غير مسبوق، خاصة في البيئة الأكاديمية حيث يعتمد الطلاب الجامعيون بشكل كبير على الإنترنت في حياتهم الدراسية والشخصية. من بين أبرز هذه الجرائم هو الابتزاز الإلكتروني، الذي يستهدف بشكل خاص الأشخاص الذين لا يمتلكون الوعي الكافي حول المخاطر الرقمية وطرق الوقاية منها. تتنوع أساليب الابتزاز الإلكتروني وتزداد تعقيدًا مع تقدم التكنولوجيا، مما يزيد من ضرورة توفير الحماية الجنائية للطلاب الجامعيين الذين يعتبرون الأكثر عرضة لهذه الجرائم. يُعد الابتزاز الإلكتروني من أخطر الجرائم التي تهدد الأفراد في العصر الرقمي، وخاصة الطلاب الجامعيين الذين يعانون من هشاشة في حماية بياناتهم الشخصية في الفضاء الإلكتروني. يهدف هذا البحث إلى تحليل الحماية الجنائية للطلاب الجامعيين من جرائم الابتزاز الإلكتروني من خلال دراسة مفاهيم الجريمة، خصائصها، الأركان القانونية المرتبطة بها، والعقوبات المقررة لها. كما يناقش البحث دور المؤسسات الأكاديمية، التشريعات الوطنية والدولية، وأجهزة الأمن السيبراني في الوقاية من هذه الجرائم. اعتمد البحث على المنهج الوصفي التحليلي، حيث تم تحليل القوانين والتشريعات الحالية، ودور المؤسسات التقنية والأمنية في تعزيز الحماية الرقمية. كما تم التركيز على أهمية التوعية الرقمية داخل الجامعات وأثرها في حماية الطلاب من الابتزاز. النتيجة التي تم التوصل إليها هي أن الحماية الجنائية ضد الابتزاز الإلكتروني تتطلب تضافر الجهود بين الجهات التشريعية، الأكاديمية، الأمنية، والتقنية. كما أظهرت النتائج أن التوعية الرقمية الفعالة والدعم المؤسسي يعتبران من العوامل الحاسمة في الوقاية من هذه الجرائم. توصي الدراسة بتعزيز التعاون بين الجامعات والمؤسسات الأمنية لتطوير برامج توعية شاملة تهدف إلى تعزيز الوعي الرقمي بين الطلاب. كما توصي بتحديث التشريعات لمواكبة التطورات التكنولوجية السريعة ومكافحة الجرائم الإلكترونية بكفاءة. وفي الختام، يعتبر تعزيز الحماية الرقمية من خلال التشريعات التكنولوجية والمراقبة الأمنية عاملًا أساسيًا في مواجهة هذه الجرائم وحماية الأفراد في المجتمع الرقمي.

الكلمات المفتاحية: الابتزاز الإلكتروني، الحماية الجنائية، الطلاب الجامعيين، الأمن السيبراني، التوعية الرقمية، التشريعات القانونية.

Abstract

In our current era, cybercrimes have become an unprecedented threat to individuals and societies, especially in the academic environment, where university students rely heavily on the internet for their studies and personal lives. Among the most prominent of these crimes is cyber-extortion, which specifically targets individuals who lack sufficient awareness of digital risks and ways to prevent them. Cyber-extortion methods are becoming more diverse and complex with the advancement of technology, increasing the need to provide criminal protection for university students, who are considered the most vulnerable to these crimes. Cyber-extortion is one of the most dangerous crimes threatening individuals in the digital age, especially university students, who suffer from weak protection of their personal data in cyberspace. This research aims to analyze the criminal protection of university students from cyber-extortion crimes by examining the concepts of the crime, its characteristics, the legal elements associated with it, and the prescribed penalties. The research also discusses the role of academic institutions, national and international legislation, and cybersecurity agencies in preventing these crimes. The research relied on a descriptive analytical approach, analyzing current laws and legislation and the role of technical and security institutions in enhancing digital protection. The study also focused on the importance of digital awareness within universities and its impact on protecting students from blackmail. The conclusion reached is that criminal protection against cyber-blackmail requires concerted efforts between legislative, academic, security, and technical authorities. The results also showed that effective digital awareness and institutional support are crucial factors in preventing these crimes. The study recommends enhancing cooperation between universities and security institutions to develop comprehensive awareness programs aimed at enhancing digital awareness among students. It also recommends updating legislation to keep pace with rapid technological developments and effectively combat cybercrime. In conclusion, enhancing digital protection through technological legislation and security monitoring is a key factor in combating these crimes and protecting individuals in the digital community.
Keywords: cyber-blackmail, criminal protection, university students, cybersecurity, digital awareness, legal legislation.

CC BY

المقدمة

في ظل الطفرة التكنولوجية المتسارعة التي يشهدها العالم في الوقت الراهن، أصبح الفضاء الرقمي جزءاً لا يتجزأ من الحياة اليومية، لا سيما في الأوساط الجامعية التي تعتمد بشكل كبير على التقنيات الحديثة في مختلف مجالاتها الأكاديمية والإدارية والاجتماعية. وبقدر ما وفرت هذه التكنولوجيا من تسهيلات وإيجابيات، فإنها في الوقت ذاته فتحت الأبواب أمام ظهور أنماط جديدة من الجرائم الإلكترونية، من بينها جريمة الابتزاز الإلكتروني، التي تمثل خطراً حقيقياً على الفئة الطلابية داخل الجامعات. يعاني العديد من الطلبة الجامعيين من التعرض لمحاولات ابتزاز عبر الإنترنت، سواء من خلال سرقة صورهم أو معلوماتهم الشخصية، أو عبر تهديدهم بنشر بيانات خاصة بهم مقابل مطالب مالية أو تصرفات معينة. وتكمن خطورة هذه الجرائم في قدرتها على التأثير النفسي والاجتماعي الكبير على الضحية، ما قد يؤدي إلى عزله عن محيطه الأكاديمي أو حتى انتحاره في بعض الحالات. ومع تزايد هذا النوع من الجرائم، بات من الضروري إلقاء الضوء على الأبعاد القانونية التي تضمن الحماية الجنائية لهذه الفئة المستهدفة، وذلك في إطار تكاملي يراعي خصوصية المرحلة العمرية للطلبة وطبيعة الحياة الجامعية. ولا شك أن الفضاء السيبراني، بما يتسم به من طابع افتراضي واتساع رقعة استخدامه، أفرز تحديات قانونية غير مسبوقة، أبرزها صعوبة تحديد الجناة وإثبات الجريمة، ما يتطلب وجود تشريعات مرنة وفعالة في آنٍ واحد، قادرة على ملاحقة المجرمين ومساءلتهم جنائياً. كما أن الفجوة المعرفية التي يعاني منها بعض الطلبة بشأن حقوقهم القانونية وسبل الحماية، تضعف من قدرتهم على التصدي لمثل هذه الجرائم أو حتى الإبلاغ عنها في الوقت المناسب. إزاء هذا الوضع، يظهر دور الجامعات كمؤسسات تعليمية وتربوية فاعلة، ينبغي عليها أن تضطلع بمسؤولية الوقاية من الجرائم الإلكترونية عبر نشر الوعي والثقافة القانونية، إضافة إلى توفير آليات داخلية للإرشاد والدعم النفسي والقانوني. ومن هنا تتجلى الحاجة إلى مقاربة شاملة تتداخل فيها الأبعاد القانونية مع التربوية والتقنية، لضمان بيئة جامعية آمنة، يسودها الاحترام والثقة الرقمية. كما أن القوانين الجنائية في العديد من الدول بدأت تتطور لمواكبة المستجدات الرقمية، من خلال إدراج نصوص صريحة تجرم الابتزاز الإلكتروني وتعاقب عليه، بل إن بعض التشريعات خصصت فصولاً كاملة للجرائم الواقعة عبر الوسائط الإلكترونية. غير أن الحماية الجنائية، رغم أهميتها، لا يمكن أن تكون فعالة بمعزل عن الجهود الوقائية، والتي تشمل تعزيز قدرات الطلبة على استخدام الإنترنت بشكل آمن، وتمكينهم من التصرف السليم حال تعرضهم لأي تهديد. من هذا المنطلق، تهدف هذه الدراسة إلى تحليل أركان جريمة الابتزاز الإلكتروني من الناحية القانونية، مع تسليط الضوء على واقع الطلبة الجامعيين في مواجهة هذه الظاهرة، وبيان سبل الحماية المتاحة، سواء من خلال التشريعات المحلية أو من خلال آليات الدعم المؤسسي والتقني. كما تسعى الدراسة إلى تقديم مجموعة من التوصيات العملية التي من شأنها تعزيز دور الجامعات والجهات المختصة في التصدي لهذه الجريمة، والحد من آثارها السلبية على البيئة التعليمية وعلى الصحة النفسية للطلبة.

بيان المسئلة

مع التوسع الكبير في استخدام شبكة الإنترنت وتزايد الاعتماد على الوسائل الرقمية في التواصل والتعلم، بات الطالب الجامعي أكثر عرضة لمخاطر الفضاء الإلكتروني، وعلى رأسها جريمة الابتزاز الإلكتروني، التي تُعد من الجرائم المستحدثة ذات الطابع الخطير. وتنبع خطورة هذه الجريمة من كونها لا تقتصر على الإضرار بالمجني عليه من الناحية المادية فقط، بل تمتد لتشمل الجوانب النفسية والاجتماعية، بما قد يؤدي إلى تداعيات سلبية خطيرة كالتراجع الأكاديمي، العزلة الاجتماعية، أو حتى التفكير في الانتحار.

ورغم ما تم اتخاذه من تدابير قانونية وتشريعية في بعض الدول لمكافحة الجرائم الإلكترونية، إلا أن الواقع العملي يُظهر وجود قصور في مستوى الحماية الجنائية المقدمة لفئة الطلبة الجامعيين على وجه الخصوص، سواء من حيث فعالية

النصوص القانونية، أو من حيث آليات التطبيق والرصد، أو من ناحية غياب التوعية والتثقيف القانوني لدى الطلبة أنفسهم. كما أن طبيعة هذه الجريمة، التي تتم غالباً في الخفاء، تجعل من اكتشافها وملاحقتها أمراً بالغ التعقيد، وهو ما يفرض الحاجة الماسة إلى دراسة قانونية معمقة لواقع هذه الحماية.

من هنا تبرز إشكالية هذا البحث، والتي تتمثل في التساؤل الآتي :**إلى أي مدى توفر المنظومة القانونية الجنائية الحماية الكافية للطالب الجامعي من جريمة الابتزاز الإلكتروني؟** وما مدى فعالية التدابير الوقائية والتوعوية المعتمدة في المؤسسات الجامعية لمواجهة هذا النوع من الجرائم؟

وتتفرع عن هذه الإشكالية عدة تساؤلات فرعية، من بينها\:

- ما هي الأركان القانونية المكونة لجريمة الابتزاز الإلكتروني؟\
- ما هو الإطار التشريعي المنظم لهذه الجريمة؟ وهل يشمل حماية خاصة للطلبة الجامعيين؟\
- ما هي العقوبات الجنائية المقررة في مواجهة مرتكبي الابتزاز الإلكتروني؟\
- ما الدور الذي تلعبه الجامعات والمؤسسات الأمنية في الوقاية والحماية من هذه الجريمة؟

وتسعى هذه الدراسة إلى مناقشة هذه التساؤلات وتحليل أبعادها، في سبيل اقتراح حلول واقعية تعزز من الحماية القانونية والوقائية للطلبة الجامعيين في مواجهة الابتزاز الإلكتروني.

هيكلية هذا البحث تم تنظيمها بشكل منهجي ومنسق ليتناول موضوع **الحماية الجنائية للطالب الجامعي من جرائم الابتزاز الإلكتروني** من مختلف الجوانب القانونية، المفاهيمية، والوقائية. يبدأ البحث بمقدمة عامة تُبرز أهمية الموضوع، تليها **بيان المشكلة، أهداف البحث، وأهميته** .بعد ذلك، ينقسم الهيكل إلى ثلاثة مباحث رئيسية:

- **المبحث الأول** يتناول الإطار المفاهيمي للابتزاز الإلكتروني، من حيث التعريفات، الخصائص، وأنواع الجرائم الإلكترونية وتصنيفها.
- **المبحث الثاني** يركز على الحماية الجنائية الموضوعية، من خلال دراسة أركان الجريمة، المسؤولية الجنائية، والعقوبات المقررة.
- **المبحث الثالث** يعالج سبل الوقاية، عبر استعراض دور التشريعات، الجامعات، والأجهزة الأمنية وشركات التقنية في التصدي للظاهرة.

كل مبحث ينقسم إلى مطالب، وكل مطلب يتفرع إلى فروع، ما يتيح عرضًا تفصيليًا ومترابطًا. يُختتم البحث بـ**النتائج والتوصيات والملخص**، مما يعزز من القيمة العلمية والعملية للدراسة..

الاهمية و ضرورة البحث

تنبع أهمية هذا البحث من تزايد حالات الابتزاز الإلكتروني التي تطال فئة الطلبة الجامعيين، والذين يُعدّون من أكثر الفئات استخدامًا للتكنولوجيا والوسائط الرقمية، سواء في الدراسة أو في التواصل الاجتماعي. ويُضاف إلى ذلك ضعف

CC BY

خبرتهم القانونية، وقلة وعيهم بالمخاطر المترتبة على الإفراط في مشاركة المعلومات الشخصية عبر الإنترنت، مما يجعلهم هدفًا سهلاً للمبتزين. ومن هنا، فإن الحاجة إلى حماية هذه الفئة الحساسة لا تقتصر على الجانب الجنائي فقط، بل تشمل أيضًا الجوانب النفسية والتربوية والأمنية.

كما تتجلى ضرورة البحث في أن جريمة الابتزاز الإلكتروني تمثل تهديدًا مباشرًا للحق في الخصوصية والأمن الشخصي، وهما من الحقوق الأساسية التي تكفلها مختلف المواثيق الدولية والدساتير الوطنية. ومع تطور أساليب الجريمة الإلكترونية وتنوع أدواتها، أصبح من الضروري الوقوف على مدى كفاية الإطار القانوني الحالي، ومدى قدرته على التصدي لهذه الظاهرة والحدّ من انتشارها.

إضافة إلى ذلك، فإن هذا البحث يُسهم في إثراء الجانب الفقهي والقانوني المتعلق بالجرائم الإلكترونية، ويسلط الضوء على الثغرات التشريعية التي قد تُستغل من قبل الجناة، كما يسعى إلى إبراز أهمية الدور الوقائي الذي يمكن أن تلعبه المؤسسات الجامعية في توعية الطلبة وتمكينهم من آليات الحماية الذاتية. ومن ثم، فإن الدراسة لا تقتصر على الطابع التحليلي القانوني، بل تنفتح أيضًا على آفاق الإصلاح والتطوير في كل من التشريع والممارسة.

منهجية البحث

نظرًا لأهمية موضوع الحماية الجنائية للطالب الجامعي من جرائم الابتزاز الإلكتروني، وسعيًا لفهم أبعاده القانونية والاجتماعية، اعتمد هذا البحث على المنهج التحليلي الوصفي، حيث تم تحليل النصوص القانونية ذات الصلة، واستعراض الأحكام والتشريعات الوطنية والدولية المتعلقة بجريمة الابتزاز الإلكتروني، ولا سيما تلك التي تلامس واقع الطلبة الجامعيين، مع تسليط الضوء على الثغرات القانونية، إن وجدت، واقتراح سبل تعزيز الحماية الجنائية لهذه الفئة.

كما اعتمد البحث على المنهج المقارن من خلال المقارنة بين بعض التشريعات العربية والدولية في كيفية تعاملها مع جريمة الابتزاز الإلكتروني، وذلك لاستخلاص أفضل الممارسات القانونية.

وقد تم تقسيم البحث إلى مباحث رئيسية تتناول:

1. **المبحث الأول** :المفاهيم العامة لجريمة الابتزاز الإلكتروني، مع بيان أركانها وصورها المختلفة.
2. **المبحث الثاني** :الوضع القانوني لجريمة الابتزاز الإلكتروني في التشريعات الوطنية، وموقع الطالب الجامعي ضمن هذه الأحكام.
3. **المبحث الثالث** :سبل الحماية الجنائية الخاصة والعامة المقررة للطالب الجامعي، مع دراسة تحليلية نقدية للأدوات القانونية والجزاءات المقررة.

CC BY

المبحث الأول :الإطار المفاهيمي لجرائم الابتزاز الإلكتروني

المطلب الأول :مفهوم الابتزاز الإلكتروني

الفرع الأول :التعريف اللغوي والاصطلاحي للابتزاز الإلكتروني

يُعد الابتزاز من الألفاظ العربية الأصيلة، وهو مشتق من الفعل «ابتزّ»، أي أخذ الشيء قسرًا أو عنوة. وفي معاجم اللغة العربية، جاء معنى الابتزاز على أنه «أخذ الشيء بالقوة أو بالحيلة» (ابن منظور، 1993، ص 87).[1] ومن خلال هذا التعريف يتضح أن الابتزاز ينطوي على عنصر الإكراه أو التهديد بهدف الحصول على منفعة مادية أو معنوية.

أما من الناحية الاصطلاحية، فقد تطور مفهوم الابتزاز ليأخذ مدلولات أوسع مع تطور المجتمعات وتعقيد العلاقات الاجتماعية والاقتصادية. وعرفه بعض الفقهاء بأنه «الضغط على شخص بوسيلة من وسائل التهديد لحمله على القيام بعمل أو الامتناع عن عمل لصالح الجاني أو لصالح الغير» (السنهوري، 1980، ص 214).[2] ويشمل هذا التعريف عناصر أساسية هي: التهديد، الإرغام، والحصول على مكاسب.

مع دخول العالم الرقمي، ظهر مصطلح «الابتزاز الإلكتروني»، والذي يُقصد به استخدام وسائل التكنولوجيا الحديثة، كشبكة الإنترنت، الهواتف الذكية، ووسائل التواصل الاجتماعي، في ممارسة فعل الابتزاز. ويعرف الابتزاز الإلكتروني بأنه «استخدام شخص ما للوسائل الإلكترونية بهدف تهديد الضحية بنشر بيانات خاصة أو صور أو معلومات سرية، ما لم يتم الاستجابة لمطالبه» (عبد الرحمن، 2018، ص 152.[3]

وفي بعض التعريفات الأخرى، تم التركيز على الطابع الافتراضي للجريمة، حيث تم وصف الابتزاز الإلكتروني بأنه «جريمة قائمة على استغلال الفضاء السيبراني لإيقاع الضرر بالضحية عبر التهديد بالكشف عن معلومات حساسة أو مشينة، مقابل الحصول على مكاسب مالية أو تحقيق رغبات شخصية» (الخولي، 2017، ص 45).[4] ويُلاحظ من خلال هذا التعريف إضافة بعد معنوي للجريمة، إذ لم تعد تقتصر على المكاسب المالية فقط، بل قد تتعلق أيضاً بتحقيق رغبات معنوية أو اجتماعية.

وفيما يتعلق بالتشريعات العربية، فقد حاول بعضها تقديم تعريف قانوني لجريمة الابتزاز الإلكتروني. ففي القانون الإماراتي مثلاً، نص قانون مكافحة الجرائم الإلكترونية رقم (5) لسنة 2012 على أن الابتزاز هو «تهديد أو إرغام شخص على القيام بفعل أو الامتناع عن فعل باستعمال شبكة معلوماتية» (قانون مكافحة الجرائم الإلكترونية الإماراتي، 2012، المادة 16.[5])

أما القانون السعودي، فقد عرّف الجريمة في نظام مكافحة الجرائم المعلوماتية بأنها «كل فعل يرتكب باستخدام الحاسب الآلي أو الشبكة المعلوماتية، ويشكل مخالفةً لأحكام هذا النظام» (نظام مكافحة الجرائم المعلوماتية السعودي، 2007، المادة 1).[6] رغم أن التعريف عام، إلا أن الفقه السعودي اتجه إلى اعتبار الابتزاز الإلكتروني من ضمن هذه الأفعال المخالفة.

---

[1] ابن منظور، 1993، ص 87

[2] السنهوري، 1980، ص 214

[3] عبد الرحمن، 2018، ص 152

[4] الخولي، 2017، ص 45

[5] قانون مكافحة الجرائم الإلكترونية الإماراتي، 2012، المادة 16

[6] نظام مكافحة الجرائم المعلوماتية السعودي، 2007، المادة 1

CC BY

يمكن تلخيص الفروقات الجوهرية بين التعريف التقليدي والحديث للابتزاز، بأن التقليدي يركز على الإكراه المادي أو التهديد الشخصي المباشر، بينما الابتزاز الإلكتروني يعتمد على وسائل رقمية تنفصل عن المواجهة المباشرة، مما يمنح الجاني مساحة أكبر من التخفي والتحكم، ويزيد من صعوبة رصد الجريمة وإثباتها.

ويمكن القول بأن التعريفات الحديثة أجمعت على عناصر أساسية في الابتزاز الإلكتروني، وهي:

- وجود وسيلة إلكترونية مستخدمة[1].
- وقوع تهديد موجه للضحية[1].
- السعي إلى الحصول على منفعة مادية أو معنوية[1].
- وجود نية جنائية واضحة لدى الفاعل.

وقد أكد الفقه الجنائي الحديث على أن هذه العناصر تميز الابتزاز الإلكتروني عن باقي الجرائم السيبرانية، مثل الاختراق أو سرقة البيانات، التي قد تتم بدون تهديد أو ابتزاز مباشر (شحاتة، 2019، ص 77.[1])

لذلك، من المهم عند الحديث عن الابتزاز الإلكتروني أن نضع في الاعتبار خصوصية الفضاء الإلكتروني كبيئة للجريمة، واختلافها عن الجرائم التقليدية من حيث الوسائل والنتائج.

الفرع الثاني: تطور مفهوم الابتزاز الإلكتروني في عصر التحول الرقمي

شهد مفهوم الابتزاز تطوراً ملحوظاً خلال العقود الأخيرة، لا سيما مع التحول الرقمي الهائل الذي مسّ مختلف جوانب الحياة الإنسانية. فقد انتقلت الجريمة من صورتها التقليدية، القائمة على المواجهة المباشرة بين الجاني والضحية، إلى صورة أكثر تعقيداً وسرية من خلال استغلال التكنولوجيا الحديثة، مما جعل الابتزاز يأخذ بعداً إلكترونياً جديداً فرض تحديات قانونية وأخلاقية ومجتمعية متزايدة.

في السابق، كان الابتزاز يتم في الغالب عبر التهديد المادي المباشر، من خلال رسائل مكتوبة أو مكالمات هاتفية، أو لقاءات شخصية، وكانت أدوات الإثبات متاحة بشكل أو بآخر. أما اليوم، فإن ظهور الحواسيب، الهواتف الذكية، وشبكات التواصل الاجتماعي قد فتح المجال لظهور «الابتزاز الإلكتروني»، الذي يعتمد على وسائل غير تقليدية تتميز بسرعة انتشارها، وإخفاء هوية الجاني، وصعوبة الوصول إليه (القحطاني، 2021، ص 13[2])

يُعد البريد الإلكتروني أول وسيلة استخدمت في جرائم الابتزاز الإلكتروني، حيث بدأ الجناة بإرسال رسائل تهديدية تحتوي على فيروسات أو برامج تجسس تُمكّنهم من الحصول على معلومات حساسة، ثم تطورت الأساليب لتشمل القرصنة على الحسابات الشخصية، والتقاط صور أو فيديوهات دون علم الضحية، ثم تهديده بنشرها ما لم يخضع للمطالب (الشمري، 2019، ص 97)[3] . مع الوقت، ظهرت منصات التواصل مثل "فيسبوك"، "إنستغرام"، و"واتساب" كمجالات خصبة لممارسة هذا النوع من الجرائم، نظراً لطبيعتها الشخصية، وسهولة الوصول إلى المستخدمين فيها.

وقد أدى الاستخدام الواسع للإنترنت إلى توسع دائرة الضحايا، ولم تَعُد مقتصرة على شخصيات عامة أو رجال أعمال، بل امتدت لتشمل الفئات الشابة، وعلى رأسها الطلبة الجامعيون. وتشير الإحصاءات الحديثة إلى أن نسبة كبيرة من

[1] شحاتة، 2019، ص 77

[2] القحطاني، 2021، ص 13

[3] الشمري، 2019، ص 97

CC BY

ضحايا الابتزاز الإلكتروني تتراوح أعمارهم بين 18 إلى 25 سنة، ما يعكس العلاقة الوثيقة بين الجريمة والفئة الجامعية (خالد، 2020، ص 162[1].

ومع هذا التطور، لم يقتصر الابتزاز على تحقيق مكاسب مالية، بل أصبح وسيلة للانتقام، الإذلال، أو حتى السيطرة العاطفية على الضحية، وهو ما يُعرف بـ "الابتزاز العاطفي الرقمي". هذا النوع الجديد يشكل خطراً كبيراً على الصحة النفسية للضحية، خاصة إذا كان في مرحلة عمرية حساسة كطلبة الجامعات الذين يعانون من ضغوط دراسية واجتماعية.

إضافة إلى ذلك، فإن تطور تقنيات الذكاء الاصطناعي والواقع الافتراضي أدى إلى بروز أساليب ابتزاز جديدة، مثل تركيب صور وفيديوهات مفبركة(Deepfake) ، تُستخدم للتهديد والنيل من السمعة، وهو ما يجعل الضحية غير قادرة على نفي التهمة بسهولة (حمدي، 2021، ص 58)[2]. كما أن انتشار منصات العمل عن بُعد والتعليم الإلكتروني زاد من احتمالات تعرض الطلبة الجامعيين لمواقف تجعلهم عرضة للابتزاز من خلال محيطهم الافتراضي، دون حماية قانونية مباشرة.

ويلاحظ أن المشرّعين في العديد من الدول لم يُواكبوا هذا التطور السريع، إذ لا تزال بعض القوانين تستند إلى مفاهيم تقليدية لا تنسجم مع طبيعة الجريمة الإلكترونية، وهو ما يخلق فراغاً قانونياً يستفيد منه المجرمون. فغياب النصوص الخاصة أو ضعف آليات الرقابة والضبط الإلكتروني يساهم في اتساع هذه الظاهرة واستمرارها.

ويُعد إدراج مفهوم الابتزاز الإلكتروني في السياسات الجنائية الحديثة خطوة ضرورية نحو تطوير النظام القانوني بما يتناسب مع الواقع التكنولوجي المعاصر. كما أن التعاون بين السلطات القانونية والجهات التقنية بات شرطاً أساسياً لفهم أنماط الجريمة وتحديد وسائل مكافحتها.

من هنا، يظهر جلياً أن الابتزاز لم يعد مجرد جريمة تقليدية ترتبط بالتهديد المادي أو المعنوي المباشر، بل أصبح جريمة مركبة، تتشابك فيها عناصر تقنية، ونفسية، واجتماعية، تحتاج إلى قراءة جديدة في ضوء الواقع الرقمي، من أجل بناء منظومة حماية جنائية شاملة، تتناسب مع تعقيدات المجتمع المعلوماتي الجديد.

المطلب الثاني :خصائص الابتزاز الإلكتروني

يتميّز الابتزاز الإلكتروني عن غيره من الجرائم التقليدية بعدّة خصائص فريدة تتعلّق بوسائله، طبيعته، وآثاره، مما يفرض تحديات قانونية وتقنية متزايدة. يمكن تحليل خصائصه عبر فرعين أساسيين:

الفرع الأول: تميّز الابتزاز الإلكتروني عن الجرائم التقليدية

يمتلك الابتزاز الإلكتروني صفات تجعله يختلف عن نظيره التقليدي من عدة نواحٍ:

1. **الوسيلة المستخدمة:**

يتمّ ارتكاب الابتزاز الإلكتروني من خلال أدوات تكنولوجية مثل البريد الإلكتروني، تطبيقات التواصل الاجتماعي،

[1] خالد، 2020، ص 162
[2] حمدي، 2021، ص 58

المواقع الإلكترونية، والبرمجيات الخبيثة. هذه الوسائل تتيح للمبتز إخفاء هويته بشكل شبه كامل، بخلاف الجرائم التقليدية التي غالبًا ما تتطلب مواجهة مادية بين الجاني والضحية (الزعبي، 2021، ص. 21([1])

2. **الانتشار الواسع وسرعة التأثير:**

يمكن أن يؤدي نشر الصور أو المعلومات الخاصة بالضحية إلى انتشارها بشكل واسع على الإنترنت خلال دقائق، ما يُضاعف الضرر النفسي والمعنوي للضحية، ويزيد من صعوبة احتواء الجريمة (حمود، 2020، ص. 136[(2)].

3. **عدم الإقليمية:**

لا تحدّ الجريمة الإلكترونية حدودٌ جغرافية. يمكن أن يقع الجاني في دولة والضحية في دولة أخرى، مما يخلق صعوبات في الملاحقة القانونية والتنسيق الدولي (جاسم، 2019، ص. 88[(3)].

4. **تعقيد الإثبات الرقمي:**

يتطلب إثبات الابتزاز الإلكتروني وسائل رقمية مثل التتبع الإلكتروني وتحليل الأدلة الجنائية الرقمية، وهي إجراءات غالبًا ما تكون مكلفة وتتطلب خبراء متخصصين (السامرائي، 2021، ص. 103[(4)].

الفرع الثاني: صور وأشكال الابتزاز الإلكتروني الشائعة

تتعدد صور الابتزاز الإلكتروني بتعدد الأهداف والوسائل، ومن أبرزها:

1. **ابتزاز الصور والمحتوى الجنسي:**

يُعد هذا النوع من الابتزاز الأكثر شيوعًا، ويعتمد على تهديد الضحية بنشر صور أو فيديوهات ذات طابع خاص مقابل المال أو الامتثال لمطالب جنسية (أبو زيد، 2022، ص. 94)[(5)] . هذا النوع منتشر بشكل خاص بين الشباب والطلاب الجامعيين نتيجة التفاعل الكبير على منصات التواصل.

2. **الابتزاز المالي:**

يهدف الجاني فيه إلى الحصول على مبالغ مالية مقابل عدم إفشاء معلومات أو ملفات مسروقة من أجهزة الضحية. وغالبًا ما يتم ذلك من خلال رسائل تحمل تهديدات بنشر بيانات حساسة أو خرق الخصوصية الرقمية (حجازي، 2020، ص. 117 [(6)].

3. **الابتزاز السياسي أو الفكري:**

قد يُستخدم الابتزاز كأداة ضغط ضد شخصيات أكاديمية أو سياسية لنشر مواقف معينة أو اتخاذ قرارات تحت

---

[12] الزغبي،حسان . 2021.(الجرائم الالكترونية واثرها علىٰ الامن المجتمعي .عمان :دار الثقافة .

[2] حمود، محمد. (2020 .(*الجرائم الإلكترونية في القانون المقارن* .القاهرة: دار النهضة العربية.

[3] جاسم، عماد. (2019 .(*القانون الجنائي وتحديات الفضاء الإلكتروني* .بيروت: منشورات الحلبي

[15] السامرائي، خالد. (2021 .(*التحقيق في الجرائم الرقمية* .بغداد: دار الأمل

[5] أبو زيد، 2022، ص. 94

[6] حجازي، 2020، ص. 117

CC BY

الضغط، وغالبًا ما يتم ذلك من خلال تسريب معلومات تم الحصول عليها بطرق غير قانونية (الشامي، 2021، ص. 73[1])

4. **الابتزاز العاطفي والاجتماعي:**

في هذا النوع، يستغل الجاني روابط عاطفية أو اجتماعية بالضحية، ويستخدم معلومات أو رسائل شخصية للضغط على الضحية نفسيًا واجتماعيًا

المطلب الثالث :تصنيف الجريمة الإلكترونية

تُعد الجريمة الإلكترونية من أخطر الظواهر الجنائية الحديثة، وقد دفعت بتشريعات العالم إلى مراجعة بنيتها القانونية لمواكبة هذا النوع من الجرائم. ولفهم موقع جريمة الابتزاز الإلكتروني ضمن هذا الإطار، من الضروري أولاً تصنيف الجرائم الإلكترونية بشكل عام.

الفرع الأول: التصنيف القانوني للجرائم الإلكترونية

يمكن تصنيف الجرائم الإلكترونية من منظور قانوني إلى عدّة فئات رئيسية، اعتمادًا على **المصلحة القانونية المحمية** و**موضوع الفعل الجرمي** .ومن أبرز هذه التصنيفات:

1. **جرائم ضد أنظمة المعلومات:**

وهي الجرائم التي تستهدف البنية التحتية للمعلومات مثل اختراق الشبكات، وتعطيل أنظمة الحواسيب، وهجمات الحرمان من الخدمة .(DDoS) يُنظر إلى هذه الجرائم على أنها اعتداء مباشر على الأمن المعلوماتي العام (أبو العلا، 2021، ص. 55.[2])

2. **جرائم محتوى المعلومات:**

وتشمل الجرائم التي يكون فيها المحتوى المتداول هو موضوع الجريمة مثل نشر المواد الإباحية، التحريض على الكراهية، أو التشهير عبر الإنترنت. الابتزاز الإلكتروني يندرج جزئياً ضمن هذا النوع (عبد الحميد، 2020، ص. 92[3]).

3. **جرائم باستخدام تقنية المعلومات كوسيلة:**

حيث تُستخدم التقنية كوسيلة لتنفيذ جرائم تقليدية كالنصب، الاحتيال، غسل الأموال، أو الاتجار غير المشروع. وهذه الفئة غالبًا ما تكون معقدة بسبب تعدد أطراف الجريمة وانتشارها الجغرافي.

[1] الشامي، يوسف. (2021). التحقيق في الجرائم المعلوماتية. القاهرة: مركز دراسات القانون والتكنولوجيا.
[2] أبو العلا، 2021، ص. 55
[3] عبد الحميد، 2020، ص. 92

CC BY

الفرع الثاني: موضع الابتزاز الإلكتروني ضمن التصنيف العام

يُعد الابتزاز الإلكتروني من **الجرائم المختلطة** التي يصعب تصنيفها بشكل أحادي، لأنه يلامس أكثر من مصلحة قانونية، ويجمع بين عناصر من الجرائم التقليدية والرقمية، ويمكن وضعه ضمن ما يلي:

1. **جريمة ضد حرية الفرد وخصوصيته:**

لأن المبتز غالباً ما يستغل معلومات شخصية أو صور خاصة للضغط على الضحية، فهو يشكل اعتداءً صريحاً على الحياة الخاصة، ويُجرم في العديد من التشريعات تحت بند انتهاك الخصوصية (الهزاع، 2021، ص. 111[1]).

2. **جريمة ذات طابع مالي أو جنسي أو نفسي:**

تختلف غاية الابتزاز الإلكتروني، فقد يكون الهدف منه الحصول على المال (جريمة مالية)، أو استغلال جنسي، أو حتى تحقيق ضغط نفسي أو اجتماعي على الضحية، وهو ما يجعله ضمن الجرائم المعنوية الخطرة.

3. **جريمة عابرة للحدود:**

غالبًا ما يتم الابتزاز عبر خوادم ومنصات لا تقع ضمن نطاق سلطة الدولة التي ينتمي إليها الضحية، مما يُضفي على الجريمة طابعًا دوليًا ويجعل مكافحتها تتطلب تعاونًا قضائيًا وأمنيًا عابرًا للحدود (منصور، 2019، ص64.[2])

المبحث الثاني :الحماية الجنائية الموضوعية للطالب الجامعي

المطلب الأول :أركان جريمة الابتزاز الإلكتروني

الفرع الأول: الركن المادي

تُعد الجرائم الإلكترونية، بما فيها جريمة الابتزاز الإلكتروني، من الجرائم التي تتسم بنوع من التعقيد، حيث تحتاج إلى دراسة دقيقة لأركان الجريمة، وتحديد كيفية تحقق كل ركن من هذه الأركان في السياق الإلكتروني. وضمن هذه الجرائم، يُعد الركن المادي من الأركان الأساسية التي يتم بناءً عليها إثبات الجريمة.

أولاً: تعريف الركن المادي

الركن المادي للجريمة يشمل كل التصرفات الملموسة التي يقوم بها الجاني وتؤدي إلى تحقيق الجريمة، سواء كانت هذه التصرفات مادية أو سلوكية أو متمثلة في استخدام وسائل معينة لتنفيذ الجريمة (عمر، 2020، ص 103) [3]. وفي حالة جريمة الابتزاز الإلكتروني، يتمثل الركن المادي في الأفعال التي يقوم بها الجاني باستخدام الوسائل الإلكترونية لتهديد الضحية، بهدف الحصول على مكاسب مادية أو غير مادية.

[1] الهزاع، 2021، ص. 111

[2] منصور، 2019، ص64

[3] عمر، 2020، ص 103

CC BY

ثانيًا: الأفعال المادية لجريمة الابتزاز الإلكتروني

تتجسد الأفعال المادية لجريمة الابتزاز الإلكتروني في مجموعة من التصرفات التي قد تتنوع حسب أسلوب وهدف الجاني. تشمل هذه الأفعال:

1. **الحصول على بيانات أو صور شخصية** :في كثير من الحالات، يبدأ المجرم باختراق حسابات الضحية أو استدراجها للكشف عن معلومات حساسة أو صور غير لائقة.

2. **تهديد الضحية بنشر البيانات** :يشكل تهديد نشر البيانات الشخصية أو الصور المحرجة خطوة أساسية في الابتزاز الإلكتروني. يتم ذلك عبر إرسال رسائل تهديدية للضحية، غالبًا عبر البريد الإلكتروني أو تطبيقات التواصل الاجتماعي (محمد، 2021، ص 87[1].

3. **مطالبة الضحية بتنفيذ شروط الجاني** :وهي المرحلة التي يتم فيها طلب المال أو الخدمات أو القيام بأفعال معينة مقابل عدم نشر الصور أو المعلومات، وهو ما يُعد جوهر جريمة الابتزاز الإلكتروني.

4. **استخدام تقنيات التشفير أو البرمجيات الضارة** :في بعض الحالات، قد يستخدم الجاني تقنيات متقدمة مثل البرمجيات الخبيثة أو برامج الفدية لتهديد الضحية أو اختراق معلوماتها (زيدان، 2019، ص 55[2] .

ثالثًا: التهديد كركن مادي أساسي

يُعد التهديد من أبرز مظاهر الركن المادي في الابتزاز الإلكتروني، حيث يقوم الجاني باستخدام وسائل إلكترونية لتهديد الضحية بنشر معلومات أو صور خاصة. وهذا التهديد يخلق ضغطًا نفسيًا على الضحية ويجعلها تحت الضغط النفسي لدفع الجاني ما يطلبه، سواء كان مالًا أو خدمات معينة.

رابعًا: الآثار المترتبة على الركن المادي

يتسبب الركن المادي في خلق حالة من الخوف أو التهديد للضحية، مما يُعد ضررًا ملموسًا في الجريمة. يزداد تأثير الركن المادي عندما يكون الضحية شخصًا معروفًا أو ذو مكانة اجتماعية، مما يزيد من تأثير التهديد عليه. كما يُمكن أن يتسبب في أضرار اجتماعية أو نفسية قد تمتد إلى عواقب طويلة الأمد.

الفرع الثاني: الركن المعنوي

الركن المعنوي للجريمة الإلكترونية يتعلق بالقصد الجنائي أو النية الإجرامية لدى الجاني، وهو أمر أساسي في إثبات مسؤولية الجاني عن الجريمة. فحتى وإن توافر الركن المادي، لا تُعتبر الجريمة قد اكتملت إلا إذا كان الجاني قد ارتكب الفعل بنية سيئة أو لتحقيق هدف إجرامي.

أولاً: تعريف الركن المعنوي

الركن المعنوي للجريمة يشمل القصد الجنائي الذي يحرك الجاني لإتيان الفعل المجرم. ويمثل هذا العنصر الحالة الذهنية التي يكون عليها الجاني عندما يرتكب الجريمة، مما يتطلب من المحكمة إثبات أن الجاني كان لديه نية واضحة للتهديد أو الحصول على مكاسب غير مشروعة من خلال الابتزاز (علي، 2022، ص 78[3].

[1] محمد، 2021، ص 87

[2] زيدان، 2019، ص 55

[3] علي، 2022، ص 78

CC BY

ثانيًا: القصد الجنائي في جريمة الابتزاز الإلكتروني

في جريمة الابتزاز الإلكتروني، يتطلب الأمر أن يكون لدى الجاني نية واضحة لإلحاق الضرر بالضحية للحصول على مكاسب غير مشروعة. ويشمل ذلك النية في تهديد الضحية بنشر المعلومات أو الصور التي تم الحصول عليها من خلال وسائل غير قانونية. يمكن تصنيف القصد الجنائي في هذا النوع من الجرائم إلى عدة أبعاد:

1. **نية الابتزاز للحصول على مال أو منفعة** :وهي النية الرئيسية التي تَحكم العديد من الحالات، حيث يسعى الجاني للحصول على أموال أو أشياء أخرى ذات قيمة من الضحية مقابل عدم نشر الصور أو المعلومات.

2. **نية إلحاق الضرر النفسي أو الاجتماعي بالضحية** :قد يكون القصد الجنائي في بعض الحالات هو إلحاق الأذى بالضحية نفسيًا أو اجتماعيًا، مثل تهديد السمعة أو الشهرة.

ثالثًا: أهمية الركن المعنوي في تحديد المسؤولية الجنائية

إن الركن المعنوي يعد عنصرًا حاسمًا في تحديد مسؤولية الجاني في جريمة الابتزاز الإلكتروني، حيث لا يُمكن اعتبار الفعل جريمة بدون أن يكون للجاني نية إجرامية. وعلى الرغم من أن الأضرار المترتبة على الابتزاز الإلكتروني قد تكون جسيمة، إلا أن إثبات القصد الجنائي يساعد في توجيه التهم بشكل دقيق إلى الجاني.

رابعًا: تأثير الركن المعنوي على العقوبة

في حال ثبوت القصد الجنائي، فإن العقوبة التي قد تُفرض على الجاني تكون أشد وأقوى، حيث يُعتبر أن الجاني ارتكب الفعل عمدًا وبتخطيط مسبق. وبالتالي، يُعتبر الركن المعنوي ركيزة أساسية في تحديد نوع العقوبة والجزاء الذي سيتم تطبيقه على الجاني.

الخلاصة:

إن دراسة الأركان المادية والمعنوية لجريمة الابتزاز الإلكتروني تُساعد في فهم كيفية تعامل النظام القانوني مع هذه الجريمة المعقدة. فبينما يركز الركن المادي على الفعل الملموس والتهديد الفعلي الذي يتعرض له الضحية، يشمل الركن المعنوي النية الإجرامية التي تهدف إلى تحقيق مكاسب غير مشروعة، سواء كانت مالية أو نفسية، من خلال التهديد. ولذلك، فإن التأكيد على وجود الأركان كافة، مع توفر النية الجنائية، هو ما يُؤدي إلى تشكيل جريمة الابتزاز الإلكتروني في نظر القانون.

المطلب الثاني :المسؤولية الجنائية عن الابتزاز الإلكتروني

الفرع الأول: المسؤولية الجنائية للشخص الطبيعي

تُعتبر المسؤولية الجنائية من أهم المفاهيم القانونية التي ترتبط بالجريمة الإلكترونية بشكل عام، وجريمة الابتزاز الإلكتروني بشكل خاص. وفي هذا السياق، يشير مصطلح "الشخص الطبيعي" إلى الأفراد الذين يرتكبون الجريمة بأنفسهم، حيث تتحمل هذه الفئة المسؤولية الجنائية عن الأفعال التي يرتكبونها من خلال استخدام الوسائل الإلكترونية. وفيما يلي، سنستعرض المسؤولية الجنائية للشخص الطبيعي في جريمة الابتزاز الإلكتروني من خلال تحديد عناصر هذه المسؤولية وكيفية تطبيقها.

أولاً: تعريف المسؤولية الجنائية للشخص الطبيعي

المسؤولية الجنائية تعني تحميل الشخص مسؤولية قانونية عن الأفعال التي ارتكبها إذا ثبتت إدانتُه بارتكاب جريمة وفقًا للأركان القانونية المحددة في القانون الجنائي. في جريمة الابتزاز الإلكتروني، تُعتبر المسؤولية الجنائية موجهة نحو

CC BY

الشخص الذي يقوم باستخدام وسائل التواصل الإلكترونية والإنترنت لتهديد الضحية بغرض الحصول على منافع مادية أو معنوية، دون وجه حق (عمر، 2021، ص 67.[1]

ثانيًا: توافر أركان المسؤولية الجنائية للشخص الطبيعي

من أجل أن تتحقق المسؤولية الجنائية للشخص الطبيعي في جريمة الابتزاز الإلكتروني، يجب توافر عدة عناصر أساسية تشمل:

1. **الركن المادي** :حيث يجب أن يتم ارتكاب فعل الابتزاز الإلكتروني باستخدام الوسائل الإلكترونية، مثل تهديد الضحية بنشر صور أو معلومات خاصة، أو طلب أموال أو خدمات من الضحية تحت التهديد.

2. **الركن المعنوي** :يجب أن يكون لدى الجاني القصد الجنائي المرتبط بالابتزاز، أي النية في الحصول على مكاسب غير مشروعة من خلال تهديد الضحية. وهذا يشمل النية في إيذاء الضحية نفسيًا أو اجتماعيًا.

3. **الإرادة الحرة** :لكي يتحمل الشخص الطبيعي المسؤولية الجنائية، يجب أن تكون إرادته حرة وغير مشوبة بالعوامل التي قد تؤثر على قدرته على اتخاذ القرار، مثل الإكراه أو الاستغلال (المهدي، 2020، ص 98[2] .

ثالثًا: العقوبات المقررة ضد الشخص الطبيعي

عند إثبات مسؤولية الشخص الطبيعي عن ارتكاب جريمة الابتزاز الإلكتروني، يواجه هذا الشخص عقوبات قانونية قد تختلف حسب النظام القانوني في الدولة المعنية، وتستند إلى شدة الجريمة وظروف ارتكابها. عادةً ما تشمل العقوبات المقررة ضد الشخص الطبيعي في مثل هذه الجرائم:

- **العقوبات المالية** :مثل الغرامات المالية التي تهدف إلى معاقبة الجاني وردع الآخرين.

- **العقوبات السالبة للحرية** :مثل الحبس لفترات محددة، تتراوح حسب خطورة الجريمة.

- **العمل المجتمعي** :في بعض الحالات، قد يتم فرض عقوبات مثل العمل المجتمعي أو برامج التأهيل الخاصة.

رابعًا: دور القانون في توجيه المسؤولية الجنائية

إنّ تطبيق المسؤولية الجنائية على الشخص الطبيعي في جريمة الابتزاز الإلكتروني يعتمد على قوة الأدلة التي تثبت ارتكاب الجريمة. ويُعدُّ دور القانون في هذا الصدد حاسمًا، حيث يجب أن يتضمن نصوصًا واضحة وشاملة توضح المسؤولية الجنائية في هذا السياق، بما في ذلك إقرار حق الضحية في الحصول على التعويضات عن الأضرار التي لحقت بها نتيجة الابتزاز (الزعبي، 2022، ص112[3]

الفرع الثاني: المسؤولية الجنائية للشخص المعنوي

الشخص المعنوي هو الكيان الذي يتمتع بالشخصية القانونية رغم أنه ليس فردًا طبيعيًا. ويشمل هذا النوع من الأشخاص الشركات والمؤسسات والمنظمات، التي قد تقوم بارتكاب جريمة الابتزاز الإلكتروني من خلال موظفيها أو

[1] عمر، 2021، ص67

[2] المهدي، 2020، ص 98

[3] الزعبي، 2022، ص112

أطراف أخرى تمثلها. في هذا الفرع، سنقوم بدراسة المسؤولية الجنائية للشخص المعنوي في جريمة الابتزاز الإلكتروني، بما في ذلك كيفية تحمل الكيانات القانونية المسؤولية.

أولاً: تعريف المسؤولية الجنائية للشخص المعنوي

المسؤولية الجنائية للشخص المعنوي تعني تحميل الكيانات القانونية مثل الشركات أو المؤسسات المسؤولية القانونية في حالة ارتكاب أي من موظفيها أو ممثليها جريمة، مثل جريمة الابتزاز الإلكتروني. يتم تحديد مسؤولية الشخص المعنوي عندما يتم ارتكاب الجريمة في إطار العمل أو باستخدام أدوات وموارد المؤسسة (علي، 2020، ص 114.[1]

ثانيًا: توافر أركان المسؤولية الجنائية للشخص المعنوي

تتوافر المسؤولية الجنائية للشخص المعنوي في جريمة الابتزاز الإلكتروني إذا تم ارتكاب الجريمة ضمن نطاق العمل أو النشاط التجاري الخاص بالشخص المعنوي. والعناصر التي تُعتبر أساسية لتحقيق هذه المسؤولية تشمل:

1. **العلاقة بين الجريمة والنشاط التجاري** :يجب أن تكون الجريمة مرتبطة بنشاط الشخص المعنوي، كأن يكون قد تم استخدام منصات الإنترنت الخاصة بالشركة لارتكاب جريمة الابتزاز، أو أن تكون المؤسسة قد ساعدت في تسهيل هذه الجريمة بشكل غير مباشر.

2. **الإرادة التنظيمية** :في بعض الحالات، قد يتحقق القصد الجنائي من قبل إدارة المؤسسة أو الشركة، خاصة إذا كانت الجريمة قد ارتُكبت بتوجيه من الأشخاص المسؤولين عن إدارة الكيان المعنوي، مثل المديرين أو أصحاب القرار (حمودة، 2021، ص 141[2].

ثالثًا: العقوبات المقررة ضد الشخص المعنوي

تختلف العقوبات المقررة ضد الشخص المعنوي في جريمة الابتزاز الإلكتروني عن تلك التي تُفرض على الأفراد، حيث تركز العقوبات على الحد من قدرة الشخص المعنوي على الاستمرار في ممارسة نشاطه بطريقة غير قانونية. من بين العقوبات التي قد يتعرض لها الشخص المعنوي:

1. **الغرامات المالية** :فرض غرامات مالية كبيرة على الشخص المعنوي كوسيلة للردع ولتعويض الضحايا.

2. **تعليق أو إلغاء الترخيص** :في بعض الحالات، قد يتم تعليق أو إلغاء الترخيص التجاري أو التراخيص اللازمة لممارسة النشاط التجاري للشخص المعنوي.

3. **إغلاق المؤسسة** :في الحالات الخطيرة، قد يتم إصدار قرار بإغلاق المؤسسة أو الشركة المتورطة في جريمة الابتزاز الإلكتروني (عبد الله، 2022، ص 152[3] .

رابعًا: تحديات إثبات المسؤولية الجنائية للشخص المعنوي

إثبات المسؤولية الجنائية ضد الشخص المعنوي يشكل تحديًا قانونيًا، حيث يتطلب الأمر إثبات أن الجريمة ارتُكبت ضمن نطاق عمل الكيان المعنوي، وأن هناك علاقة بين الجريمة والنشاط التجاري أو المؤسسي الذي كان الشخص

[1] علي، 2020، ص 114

[2] حمودة، 2021، ص 141

[3] عبد الله، 2022، ص 152

CC BY

المعنوي يضطلع به. يمكن أن يكون ذلك معقدًا في الحالات التي تتضمن أنشطة إلكترونية، حيث يصعب أحيانًا ربط الجريمة بشكل مباشر مع الكيان المعنوي (السيد، 2020، ص 88[1].

الخلاصة:

المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني تشمل المسؤولية الفردية للأشخاص الطبيعيين وكذلك الكيانات القانونية مثل الشركات والمنظمات. يتحمل الشخص الطبيعي المسؤولية عندما يتمكن من إثبات ارتكابه للجريمة بنية سيئة، بينما يتحمل الشخص المعنوي المسؤولية عندما يُثبت أن الجريمة ارتُكبت من خلال موظفيه أو في إطار نشاطه. إن فهم هذه المسؤولية يُساعد في تطوير آليات قانونية فعّالة لمكافحة الابتزاز الإلكتروني وضمان ردع الفاعلين في المستقبل.

المطلب الثالث :العقوبات المقررة لجريمة الابتزاز الإلكتروني

الفرع الأول: العقوبات الأصلية

تعتبر العقوبات الأصلية هي العقوبات الأساسية التي تفرضها السلطات القضائية على الجاني عند إثبات ارتكاب جريمة الابتزاز الإلكتروني. هذه العقوبات تهدف إلى معاقبة الجاني على تصرفاته الإجرامية وردعه، بالإضافة إلى حماية المجتمع من آثار هذه الجرائم. في هذا السياق، تُحدد العقوبات الأصلية بناءً على التشريعات القانونية المعمول بها في الدولة، وتختلف من دولة إلى أخرى وفقًا لشدة الجريمة وظروفها.

أولاً: تعريف العقوبات الأصلية

العقوبات الأصلية هي العقوبات التي يتم فرضها مباشرة على الجاني نتيجة لارتكاب الجريمة، ويهدف المشرع من خلالها إلى تحقيق الردع العام والخاص. تتضمن العقوبات الأصلية عادةً السجن أو الغرامة المالية، وقد تشمل أيضًا منع الجاني من ممارسة بعض الأنشطة لفترة معينة. وتُعد هذه العقوبات ضرورية لضمان تحقيق العدالة، سواء للجاني أو للضحايا (الشريف، 2021، ص 67.[2]

ثانيًا: العقوبات الأصلية المقررة في جريمة الابتزاز الإلكتروني

تختلف العقوبات المقررة لجريمة الابتزاز الإلكتروني بناءً على العديد من العوامل، مثل خطورة الفعل المرتكب، والأضرار التي لحق بالضحية، والأهداف التي سعى الجاني لتحقيقها من خلال التهديد. في معظم الأنظمة القانونية، تشمل العقوبات الأصلية في هذا النوع من الجرائم:

1. **العقوبات السالبة للحرية (السجن :(**تُعد العقوبة السالبة للحرية من العقوبات الشائعة في جريمة الابتزاز الإلكتروني. وقد يتراوح مدة العقوبة من عدة أشهر إلى سنوات، حسب خطورة الجريمة ومدى تأثيرها على الضحية. في بعض الحالات، قد تُفرض عقوبة السجن لمدة طويلة إذا كانت الجريمة تشمل تهديدات متكررة أو ارتكاب الابتزاز ضمن جماعة إجرامية منظمة (محمد، 2022، ص 110[3].

2. **الغرامة المالية :**في بعض التشريعات القانونية، يمكن فرض غرامات مالية على الجاني نتيجة ارتكاب جريمة الابتزاز الإلكتروني. يتم تحديد مبلغ الغرامة بناءً على الأضرار التي تسببت فيها الجريمة، وتعد الغرامات أداة فعالة في مكافحة الابتزاز، حيث تعمل على توفير ردع مالي للجاني.

[1] السيد، 2020، ص 88

[2] الشريف، 2021، ص 67

[3] محمد، 2022، ص 110

CC BY

3. **السجن مع الغرامة** :في بعض الأنظمة القانونية، قد يجمع القاضي بين عقوبتي السجن والغرامة المالية، حيث يُحكم بالسجن لفترة معينة بالإضافة إلى فرض غرامة مالية. يتم اتخاذ هذا القرار بناءً على شدة الجريمة والأضرار التي لحق بالضحية، بحيث تكون العقوبات مجتمعة أكثر ردعًا (إبراهيم، 2020، ص 89.[1]

4. **الحرمان من بعض الحقوق** :في بعض الحالات، قد يُحكم على الجاني بحرمانه من بعض الحقوق مثل حق التصويت أو ممارسة بعض الأنشطة التجارية. هذه العقوبات تهدف إلى التأكيد على خطورة الجريمة وضرورة معاقبة الجاني بشكل كامل.

ثالثًا: العوامل المؤثرة في فرض العقوبات الأصلية

هناك عدة عوامل تؤثر في فرض العقوبات الأصلية لجريمة الابتزاز الإلكتروني، ومن أبرز هذه العوامل:

- **شدة الجريمة** :كلما كانت جريمة الابتزاز الإلكتروني أكثر خطورة، زادت العقوبات المقررة. على سبيل المثال، إذا كانت الجريمة تشمل تهديدًا بنشر صور خاصة أو معلومات حساسة تهدد حياة الضحية بشكل مباشر، فإن العقوبة ستكون أشد.

- **الأضرار الناتجة عن الجريمة** :مدى الأضرار النفسية والاجتماعية التي لحقت بالضحية تؤثر أيضًا في تحديد العقوبة. كلما كانت الأضرار جسيمة، كلما كانت العقوبة أشد.

- **سجل الجاني الجنائي** :إذا كان الجاني قد ارتكب جرائم مشابهة في الماضي، فقد يُحكم عليه بعقوبات أشد. وجود سجل إجرامي قد يؤدي إلى زيادة مدة السجن أو فرض غرامات مالية أكبر.

الفرع الثاني: العقوبات التكميلية والتدابير الوقائية

بجانب العقوبات الأصلية، قد يفرض القضاء على الجاني عقوبات تكميلية وتدابير وقائية تهدف إلى تعزيز الردع والوقاية من تكرار الجريمة. هذه العقوبات والتدابير تُعدّ إضافية تهدف إلى حماية المجتمع من خطر الجرائم الإلكترونية المستمرة وتعزيز العدالة الجنائية.

أولاً: تعريف العقوبات التكميلية والتدابير الوقائية

العقوبات التكميلية هي تلك العقوبات التي تفرض بعد العقوبات الأصلية وتهدف إلى تعزيز تأثيرها، مثل فرض قيود على حقوق الجاني أو إخضاعه لبرامج تأهيلية. أما التدابير الوقائية فهي إجراءات تهدف إلى منع الجاني من ارتكاب نفس الجريمة مرة أخرى، مثل فرض مراقبة إلكترونية على الجاني أو تجنب تعريضه للمؤثرات التي قد تساهم في ارتكاب الجريمة مجددًا (عبد الله، 2022، ص 121[2] .

ثانيًا: العقوبات التكميلية لجريمة الابتزاز الإلكتروني

1. **التعويضات للضحايا** :من بين العقوبات التكميلية التي قد تُفرض على الجاني هي دفع تعويضات للضحايا. قد تكون هذه التعويضات تعويضًا ماديًا عن الأضرار النفسية والاجتماعية التي لحقت بالضحية نتيجة جريمة

[1] إبراهيم، 2020، ص 89

[2] عبد الله، 2022، ص 121

CC BY

الابتزاز. تهدف هذه العقوبة إلى ردع الجاني من تكرار الفعل بالإضافة إلى تعويض الضحية عن الأضرار التي تعرضت لها (الزيد، 2020، ص 105[1]).

2. **الحرمان من بعض الحقوق** :كما تم ذكره في العقوبات الأصلية، يمكن أن تُفرض عقوبات تكميلية تهدف إلى حرمان الجاني من ممارسة بعض الحقوق. من هذه العقوبات حرمان الجاني من العمل في بعض المجالات الحساسة مثل التوظيف في مجال المعلومات أو الإنترنت. يمكن أن يُشمل هذا الحرمان كإجراء تكميلية إذا كانت الجريمة متعلقة باستخدام التكنولوجيا بشكل غير قانوني.

3. **البرامج التربوية والتأهيلية** :من الممكن أن يُفرض على الجاني الالتحاق ببرامج تدريبية أو تأهيلية تتعلق بكيفية التعامل مع التكنولوجيا بشكل قانوني وأخلاقي. هذه البرامج تهدف إلى إعادة تأهيل الجاني وتهدف إلى الوقاية من ارتكاب الجرائم في المستقبل (سامي، 2021، ص 76[2]).

ثالثًا: التدابير الوقائية لجريمة الابتزاز الإلكتروني

1. **المراقبة الإلكترونية** :من التدابير الوقائية التي قد يُفرض فيها على الجاني هو مراقبته إلكترونيًا للتأكد من أنه لا يعاود ارتكاب جريمة الابتزاز الإلكتروني. قد تشمل هذه المراقبة فحصًا منتظمًا للحسابات الإلكترونية للجاني أو فرض قيود على استخدامه لبعض التطبيقات أو المواقع (عمر، 2020، ص 118[3]).

2. **منع الجاني من الوصول إلى الإنترنت** :في بعض الحالات، قد يُحكم على الجاني بمنع مؤقت من الوصول إلى الإنترنت أو تقييد استخدامه لوسائل التواصل الاجتماعي. هذا النوع من التدابير يهدف إلى الحد من فرصة الجاني في ارتكاب الجرائم الإلكترونية مستقبلاً.

3. **التعليم والتوعية** :يمكن أن يُطلب من الجاني المشاركة في حملات توعية تهدف إلى توعية المجتمع بمخاطر الجرائم الإلكترونية وأضرارها. يعتبر هذا التدبير جزءًا من المسؤولية المجتمعية التي يتم فرضها على الجاني لمنع تكرار الجرائم المستقبلية.

الخلاصة:

إن العقوبات المقررة لجريمة الابتزاز الإلكتروني تشمل العقوبات الأصلية مثل السجن والغرامات المالية، وهي تهدف إلى معاقبة الجاني على تصرفاته الإجرامية. كما تشمل أيضًا العقوبات التكميلية مثل تعويض الضحايا والبرامج التأهيلية، بالإضافة إلى التدابير الوقائية التي تهدف إلى منع تكرار الجريمة. إن هذه العقوبات والتدابير تتكامل معًا لتوفير الردع الفعّال ضد الابتزاز الإلكتروني وحماية المجتمع من آثاره السلبية.

[1] الزيد، 2020، ص 105

[2] سامي، 2021، ص 76

[3] عمر، 2020، ص 118

CC BY

المبحث الثالث :سبل الوقاية والحماية من جرائم الابتزاز الإلكتروني

المطلب الأول :دور التشريعات في حماية الطالب الجامعي

الفرع الأول: التشريعات الوطنية

تُعدّ التشريعات الوطنية حجر الزاوية في أي نظام قانوني يعمل على مواجهة الجرائم الإلكترونية بشكل عام، وجريمة الابتزاز الإلكتروني بشكل خاص. وتعد حماية الطالب الجامعي جزءًا أساسيًا من حماية المجتمع المدني بشكل عام، حيث يتعرض العديد من الطلاب الجامعيين لهذه الجرائم نتيجة لاستخدامهم المكثف للتكنولوجيا الحديثة ووسائل التواصل الاجتماعي. لذا، فإن الدور الأساسي للتشريعات الوطنية في حماية الطالب الجامعي من جريمة الابتزاز الإلكتروني يتجسد في صياغة قوانين رادعة تُعزز من حماية هذا الفئة من المجتمع.

أولاً: أهمية التشريعات الوطنية في مواجهة جرائم الابتزاز الإلكتروني

تعتبر التشريعات الوطنية من أبرز الأدوات القانونية التي تهدف إلى تقوية الحماية القانونية ضد الجرائم الإلكترونية، بما فيها الابتزاز الإلكتروني. هذه التشريعات تضع الأسس القانونية اللازمة لملاحقة مرتكبي هذه الجرائم وتحقيق العدالة للضحايا. ولأن الابتزاز الإلكتروني يُمكن أن يتسبب في أضرار نفسية واجتماعية كبيرة، فإن من أهم أهداف التشريعات الوطنية هو فرض عقوبات رادعة تساهم في الحد من هذه الجرائم (عمر، 2021، ص 75[1].

ثانيًا: الإجراءات القانونية في التشريعات الوطنية لحماية الطلاب

تعتمد التشريعات الوطنية على مجموعة من الآليات القانونية التي تهدف إلى حماية الطلاب الجامعيين من الابتزاز الإلكتروني، وتشمل هذه الآليات:

1. **تعريف جريمة الابتزاز الإلكتروني** :من أهم الإجراءات القانونية هي تحديد تعريف دقيق للابتزاز الإلكتروني في التشريعات الوطنية، والذي يشمل جميع أشكال التهديد والابتزاز عبر الإنترنت باستخدام وسائل الاتصال الإلكترونية أو الاجتماعية. هذا التعريف يسهل على المحاكم تتبع الحالات المتصلة بهذه الجرائم وإصدار الأحكام المناسبة.

2. **فرض عقوبات رادعة** :كما ذكرنا سابقًا، فإن التشريعات الوطنية تتضمن عقوبات مالية وسجنية تتناسب مع خطورة الجريمة. وتساهم هذه العقوبات في ردع مرتكبي الجريمة من ارتكابها مجددًا، بالإضافة إلى توفير الحماية القانونية للطلاب الجامعيين. على سبيل المثال، قد يتم فرض عقوبات صارمة على الأفراد الذين يتعرضون للطلاب بالتهديد بنشر صور أو معلومات خاصة (الحاج، 2022، ص 44[2] .

3. **حماية الخصوصية** :تتضمن التشريعات الوطنية قوانين لحماية الخصوصية الشخصية للطلاب الجامعيين، بما في ذلك تنظيم كيفية جمع واستخدام بياناتهم الشخصية على الإنترنت. يتم ذلك من خلال فرض ضوابط على كيفية معالجة المعلومات الرقمية التي تُنشر عبر منصات الإنترنت، مما يمنع استغلال هذه المعلومات في عمليات الابتزاز.

[1] عمر، 2021، ص 75

[2] الحاج، 2022، ص 44

CC BY

4. **تحقيقات قانونية مختصة** :تشجع التشريعات الوطنية على إنشاء فرق خاصة من الشرطة والقضاء تتعامل مع الجرائم الإلكترونية، بما في ذلك الابتزاز الإلكتروني. تهدف هذه الفرق إلى معالجة القضايا بشكل سريع وفعال، مما يعزز من الأمن الرقمي للطلاب الجامعيين.

ثالثًا: التحديات التي تواجه التشريعات الوطنية في مكافحة الابتزاز الإلكتروني

على الرغم من الجهود الكبيرة التي تُبذل في العديد من الدول لتفعيل التشريعات الوطنية ضد الجرائم الإلكترونية، إلا أن هناك بعض التحديات التي تؤثر على فاعلية هذه التشريعات. من أبرز هذه التحديات:

1. **تسارع تطور التكنولوجيا** :التقدم السريع في مجال التكنولوجيا ووسائل التواصل الاجتماعي يجعل من الصعب على التشريعات الوطنية مواكبة هذا التطور. قد تكون بعض القوانين غير قادرة على تغطية جميع أساليب الابتزاز الجديدة التي تظهر بمرور الوقت.

2. **التعاون الدولي** :نظراً للطابع الدولي للإنترنت، يتطلب مكافحة الابتزاز الإلكتروني تعاونًا بين الدول لتوحيد التشريعات وتسهيل عملية التحقيقات عبر الحدود. فقد يواجه الطلاب الجامعيون خطر الابتزاز من جهات خارجية، مما يتطلب وجود آليات للتعاون الدولي الفعّال.

الفرع الثاني: الاتفاقيات الدولية

بالإضافة إلى التشريعات الوطنية، تعد الاتفاقيات الدولية أداة حيوية في حماية الأفراد من الجرائم الإلكترونية مثل الابتزاز الإلكتروني. ومع تزايد تهديدات الجرائم عبر الإنترنت التي تتجاوز الحدود الوطنية، أصبحت الحاجة إلى اتفاقيات دولية قوية وموحدة أمرًا ضروريًا.

أولاً: أهمية الاتفاقيات الدولية في حماية الضحايا من الابتزاز الإلكتروني

الابتزاز الإلكتروني لا يعترف بالحدود الجغرافية، حيث يمكن أن يرتكب الجاني جريمته من أي مكان في العالم باستخدام الإنترنت. لذلك، تُعد الاتفاقيات الدولية من الأدوات الأساسية في مواجهة هذه الجرائم، إذ تساعد في توحيد التشريعات وتسهيل التعاون بين الدول لمكافحة الابتزاز الإلكتروني. وتساهم هذه الاتفاقيات في ضمان حماية ضحايا الابتزاز عبر الإنترنت في جميع أنحاء العالم، بما في ذلك الطلاب الجامعيين (الزيد، 2020، ص 112[1]).

ثانيًا: أبرز الاتفاقيات الدولية لمكافحة الابتزاز الإلكتروني

تعددت الاتفاقيات الدولية التي تهدف إلى مكافحة الجرائم الإلكترونية بما فيها الابتزاز الإلكتروني. من أبرز هذه الاتفاقيات:

1. **اتفاقية بودابست بشأن الجرائم الإلكترونية (2001** :(تعتبر هذه الاتفاقية من أهم الاتفاقيات الدولية التي تناولت الجرائم الإلكترونية بشكل عام. وقد وضعت اتفاقية بودابست إطارًا قانونيًا دوليًا للتعاون بين الدول في مكافحة الجرائم الإلكترونية، بما في ذلك الجرائم المرتبطة بالابتزاز عبر الإنترنت. تنص الاتفاقية على ضرورة تعزيز

[1] الزيد، 2020، ص 112

CC BY

التشريعات الوطنية لمكافحة الجرائم الإلكترونية وتوفير آليات للتعاون بين الدول في التحقيقات والمحاكمات (فؤاد، 2021، ص 99[1]).

2. **اتفاقية الأمم المتحدة بشأن مكافحة الجريمة المنظمة عبر الوطنية (2000 :(**رغم أن هذه الاتفاقية تركز بشكل رئيسي على مكافحة الجريمة المنظمة، إلا أن لها تأثيرًا كبيرًا في محاربة الجرائم الإلكترونية التي قد يكون وراءها شبكات إجرامية منظمة، بما في ذلك جريمة الابتزاز الإلكتروني. تنص الاتفاقية على أهمية تعزيز التعاون بين الدول لمكافحة الجرائم العابرة للحدود.

3. **الاتفاقيات الإقليمية** :بالإضافة إلى الاتفاقيات الدولية، هناك أيضًا اتفاقيات إقليمية خاصة بمكافحة الجرائم الإلكترونية، مثل تلك التي تم تبنيها من قبل الاتحاد الأوروبي ومنظمة الأمن والتعاون في البحر الأبيض المتوسط. هذه الاتفاقيات تهدف إلى تعزيز التعاون بين الدول الأعضاء لمكافحة الجرائم الإلكترونية بشكل جماعي.

ثالثًا: تحديات تطبيق الاتفاقيات الدولية

على الرغم من أهمية الاتفاقيات الدولية، فإن هناك بعض التحديات التي قد تواجه تنفيذها، بما في ذلك:

1. **التباين في التشريعات الوطنية** :يختلف التطبيق الفعلي لهذه الاتفاقيات بين الدول نتيجة لاختلاف التشريعات الوطنية. قد تواجه بعض الدول صعوبة في تعديل قوانينها لتتوافق مع هذه الاتفاقيات، مما قد يؤثر على فعاليتها.

2. **محدودية التعاون بين الدول** :بالرغم من وجود اتفاقيات، إلا أن التعاون بين الدول في قضايا الجرائم الإلكترونية قد يكون بطيئًا أو محدودًا. بعض الدول قد تفتقر إلى القدرة التقنية أو القضائية للتعامل مع هذه الجرائم.

الخلاصة:

تُعدّ التشريعات الوطنية والاتفاقيات الدولية من الأدوات القانونية الأساسية التي تساهم في حماية الطلاب الجامعيين من جريمة الابتزاز الإلكتروني. بينما تهدف التشريعات الوطنية إلى توفير حماية محلية من خلال قوانين رادعة، تتيح الاتفاقيات الدولية التعاون بين الدول لمكافحة هذه الجرائم عبر الحدود. وفي ظل التحديات التقنية والشرعية التي قد تواجه هذه الأدوات، يبقى التعاون الدولي وتطوير التشريعات الوطنية أساسيين لتحقيق الحماية الفعّالة ضد جرائم الابتزاز الإلكتروني.

المطلب الثاني :دور المؤسسات الجامعية في الوقاية

الفرع الأول: السياسات الداخلية والإرشاد الطلابي

تلعب المؤسسات الجامعية دورًا أساسيًا في الوقاية من جرائم الابتزاز الإلكتروني وحماية الطلاب الجامعيين من المخاطر الرقمية، حيث تُعدّ السياسات الداخلية والإرشاد الطلابي من الأدوات الفعالة التي يمكن أن تساهم بشكل كبير في هذا المجال. تهدف هذه السياسات إلى تقديم بيئة آمنة للطلاب في مواجهة الجرائم الإلكترونية، إضافة إلى توفير الدعم النفسي والإرشادي في حال تعرضهم لأي نوع من الابتزاز.

[1] فؤاد، 2021، ص 99

CC BY

أولاً: أهمية السياسات الداخلية في حماية الطلاب الجامعيين

تُعد السياسات الداخلية للمؤسسات الجامعية من الأسس التي تُسهم في الوقاية من الجرائم الإلكترونية بشكل عام، بما في ذلك الابتزاز الإلكتروني. تشمل هذه السياسات مجموعة من الضوابط والإجراءات التي تهدف إلى الحد من الجرائم التي قد يتعرض لها الطلاب عبر الإنترنت، مثل:

1. **وضع قواعد استخدام التكنولوجيا** :تسعى الجامعات إلى وضع سياسات واضحة ومحددة بشأن كيفية استخدام الطلاب للأجهزة الإلكترونية والإنترنت داخل الحرم الجامعي. على سبيل المثال، يمكن فرض قيود على الوصول إلى بعض المواقع الإلكترونية أو التطبيقات التي قد تكون محفوفة بالمخاطر، مثل مواقع الدردشة أو منصات التواصل الاجتماعي التي قد يتم استغلالها في عمليات الابتزاز.

2. **حماية بيانات الطلاب** :تسعى الجامعات إلى فرض سياسات لحماية البيانات الشخصية للطلاب، مثل البيانات الأكاديمية، الصحية، والمالية، والتي قد تكون عرضة للسرقة أو الاستغلال. يتضمن ذلك إنشاء أنظمة آمنة لحفظ هذه المعلومات، وكذلك توعية الطلاب بضرورة عدم مشاركة معلوماتهم الحساسة عبر الإنترنت.

3. **توفير برامج تأهيلية وتدريبية** :تشجع بعض الجامعات على إقامة ورش عمل ودورات تدريبية للطلاب حول كيفية حماية أنفسهم من الجرائم الإلكترونية، بما في ذلك الابتزاز الإلكتروني. تهدف هذه البرامج إلى تعليم الطلاب كيفية التعامل مع الرسائل المشبوهة والتهديدات الإلكترونية، بالإضافة إلى توعيتهم بضرورة الحفاظ على خصوصيتهم الشخصية.

ثانيًا: دور الإرشاد الطلابي في الوقاية من الابتزاز الإلكتروني

الإرشاد الطلابي يعد أداة فعّالة في الوقاية من الجرائم الإلكترونية، حيث يقوم المستشارون الأكاديميون والنفسيون بتقديم الدعم والمشورة للطلاب الذين قد يتعرضون للتهديدات أو الابتزاز عبر الإنترنت. يتضمن دور الإرشاد الطلابي في هذا السياق:

1. **الدعم النفسي** :عندما يتعرض الطلاب لابتزاز إلكتروني، فإنهم قد يعانون من ضغوط نفسية كبيرة بسبب الخوف من تهديدات الجاني أو الخجل من الإبلاغ عن الحادث. الإرشاد الطلابي يوفر لهم بيئة آمنة للتحدث عن مشاعرهم وقلقهم، ويقدم لهم الدعم النفسي الذي يساعدهم على التعامل مع هذه التجربة الصعبة.

2. **التوجيه القانوني** :من خلال الإرشاد الطلابي، يمكن تقديم التوجيهات القانونية للطلاب حول كيفية التعامل مع حالات الابتزاز الإلكتروني. يشمل ذلك توجيههم إلى الخطوات التي ينبغي اتخاذها لإبلاغ الجهات المختصة، وكذلك مساعدتهم في فهم حقوقهم القانونية وكيفية حماية أنفسهم.

3. **توفير الموارد والأنظمة القانونية** :في بعض الجامعات، يتم توفير مستشارين قانونيين أو التعاون مع محامين متخصصين في قضايا الجرائم الإلكترونية لتقديم استشارات قانونية للطلاب الذين تعرضوا للابتزاز. يساعد ذلك في تزويد الطلاب بالأدوات القانونية اللازمة للرد على هذه الجرائم.

CC BY

الفرع الثاني: التوعية والتثقيف الرقمي

تلعب التوعية والتثقيف الرقمي دورًا بالغ الأهمية في الوقاية من الابتزاز الإلكتروني، حيث تهدف إلى تعليم الطلاب كيفية التعامل مع التهديدات الرقمية والتصرف بحذر عند استخدام الإنترنت. فالتقنيات الحديثة وتزايد استخدام وسائل التواصل الاجتماعي تجعل الطلاب الجامعيين عرضة للابتزاز الإلكتروني إذا لم يكونوا على دراية بكيفية حماية أنفسهم في العالم الرقمي.

أولاً: أهمية التوعية الرقمية في مواجهة الابتزاز الإلكتروني

التوعية الرقمية تعد من الوسائل الوقائية الأساسية التي يجب أن تتبناها المؤسسات الجامعية لتجنب مخاطر الابتزاز الإلكتروني. من خلال التثقيف الرقمي، يمكن للطلاب أن يتعلموا كيفية استخدام الإنترنت بشكل آمن وواعي، مما يساعد على تقليل فرص تعرضهم للابتزاز. تشمل التوعية الرقمية الجوانب التالية:

1. **تعليم الطلاب كيفية الحفاظ على خصوصيتهم** :يتعلم الطلاب من خلال برامج التوعية الرقمية كيفية حماية معلوماتهم الشخصية على الإنترنت. يتم تزويدهم بالمعرفة حول أهمية كلمات المرور القوية، وكيفية تغييرها بشكل دوري، وكيفية تجنب نشر المعلومات الحساسة على الشبكات الاجتماعية.

2. **التعامل مع الرسائل المشبوهة** :واحدة من أهم جوانب التوعية الرقمية هي تعليم الطلاب كيفية التعرف على الرسائل المشبوهة أو المرفقات المريبة التي قد تكون جزءًا من محاولة ابتزاز. يشمل ذلك توجيههم بعدم فتح الروابط المجهولة أو الرد على الرسائل التي تحتوي على تهديدات.

3. **الوعي بمخاطر الإنترنت** :يتم التركيز في برامج التوعية على توعية الطلاب بمخاطر الإنترنت بشكل عام، وتحديدًا المخاطر المرتبطة بجرائم مثل الابتزاز الإلكتروني، التي قد تشمل التهديدات بنشر صور أو معلومات شخصية. يُشجع الطلاب على أن يكونوا حذرين عند مشاركة معلوماتهم أو صورهم عبر الإنترنت.

ثانيًا: أساليب التثقيف الرقمي

تتعدد أساليب التثقيف الرقمي التي يمكن أن تستخدمها الجامعات لتعزيز الوعي بين الطلاب، ومنها:

1. **الورش التفاعلية** :تنظيم ورش عمل تفاعلية تتناول كيفية حماية البيانات الشخصية على الإنترنت، وتقديم نصائح حول أمان الحسابات الاجتماعية وطرق التعامل مع الابتزاز الإلكتروني. تتضمن هذه الورش محاضرات وندوات يشترك فيها الطلاب للتعرف على أساليب الوقاية والتعامل مع التهديدات الرقمية.

2. **الحملات الإعلامية** :تُعد الحملات الإعلامية جزءًا من استراتيجيات التوعية الرقمية. حيث يمكن للمؤسسات الجامعية أن تنظم حملات توعية عبر وسائل التواصل الاجتماعي الخاصة بها، وتستخدم الوسائط المتعددة (مثل الفيديوهات والإنفوغرافيك) لشرح كيفية حماية النفس من الابتزاز.

3. **التدريب على السلامة الرقمية** :تدريب الطلاب على كيفية استخدام أدوات الأمان الرقمية المتاحة لهم، مثل برامج مكافحة الفيروسات، وبرامج تشفير البيانات، وأدوات الحماية من المهاجمين الإلكترونيين. يساعد هذا النوع من التدريب في حماية الطلاب من تعرضهم لمخاطر الابتزاز الإلكتروني.

CC BY

4. **إقامة شراكات مع مؤسسات قانونية وتقنية** :يمكن للمؤسسات الجامعية أيضًا التعاون مع شركات أمن الإنترنت أو الهيئات القانونية لتنظيم ورش تدريبية ودورات تثقيفية مشتركة، حيث يتم تزويد الطلاب بالمعرفة الكافية للتعامل مع الحالات الطارئة.

الخلاصة:

تعتبر المؤسسات الجامعية من الجهات الحيوية في تقديم الحماية والوقاية ضد الابتزاز الإلكتروني، حيث تسهم السياسات الداخلية والإرشاد الطلابي في تعزيز الأمن الرقمي داخل الحرم الجامعي. إلى جانب ذلك، يعد التوعية والتثقيف الرقمي من أهم الأدوات التي يمكن أن تساعد الطلاب على فهم مخاطر الإنترنت وكيفية تجنب الوقوع ضحايا للابتزاز الإلكتروني. يتطلب هذا النوع من الوقاية جهودًا مستمرة من الجامعات لخلق بيئة آمنة تضمن سلامة الطلاب في العالم الرقمي.

المطلب الثالث :دور الجهات الأمنية والتقنية

الفرع الأول: دور أجهزة الأمن السيبراني

تعد أجهزة الأمن السيبراني من الركائز الأساسية في مواجهة الجرائم الإلكترونية وحماية الأفراد من المخاطر التي قد تنشأ في الفضاء الرقمي. حيث تساهم هذه الأجهزة بشكل فعال في مواجهة الابتزاز الإلكتروني، من خلال الكشف عن الجرائم وملاحقة مرتكبيها، إضافة إلى تقديم الدعم التقني لضحايا الجرائم الإلكترونية. يتطلب هذا الدور التنسيق بين مختلف الجهات الحكومية والأمنية لضمان حماية الأفراد، وخاصة الطلاب الجامعيين، من تهديدات الابتزاز الإلكتروني.

أولاً: أهمية أجهزة الأمن السيبراني في مكافحة الابتزاز الإلكتروني

إن الأمن السيبراني يمثل أحد أولويات الدول في حماية مواطنيها ومؤسساتها من الجرائم الإلكترونية، ولا سيما الابتزاز الإلكتروني. أجهزة الأمن السيبراني تستخدم تقنيات حديثة ومتطورة لمراقبة النشاطات على الإنترنت، وتحليل البيانات من أجل الكشف عن أي تهديدات أو هجمات قد تؤدي إلى ابتزاز الأشخاص أو سرقة بياناتهم الشخصية.

1. **الرصد والكشف المبكر** :تقوم أجهزة الأمن السيبراني بمراقبة الأنشطة الإلكترونية على الإنترنت للكشف عن أي سلوك مشبوه أو محاولات لابتزاز الأشخاص. يعتمد الأمن السيبراني على أنظمة الذكاء الاصطناعي والتحليل البياني لمتابعة تطور الجرائم الإلكترونية في الوقت الحقيقي، ما يسهم في اكتشاف الجرائم قبل أن تصل إلى مراحل متقدمة.

2. **التعاون مع الجهات القانونية** :تقوم أجهزة الأمن السيبراني بالتعاون مع أجهزة التحقيق القضائي لملاحقة الجرائم الإلكترونية، بما في ذلك الابتزاز الإلكتروني. يتم ذلك من خلال جمع الأدلة الرقمية وتحليلها، مما يسهل عملية التحقيق والملاحقة القانونية.

3. **تقديم الدعم التقني للضحايا** :من خلال أجهزة الأمن السيبراني، يمكن للطلاب الجامعيين الذين تعرضوا للابتزاز أن يحصلوا على الدعم التقني في الحماية من الجرائم الإلكترونية. يشمل ذلك تقديم إرشادات حول كيفية تأمين الحسابات الشخصية، والبيانات الخاصة بهم، وإيقاف الهجمات الإلكترونية.

ثانيًا: أدوات وتقنيات الأمن السيبراني لمكافحة الابتزاز الإلكتروني

1. **أنظمة المراقبة والشبكات الآمنة** :تعتمد أجهزة الأمن السيبراني على أنظمة مراقبة متطورة لرصد الأنشطة غير القانونية على الإنترنت. من خلال هذه الأنظمة، يتم تحليل وتحديد الأماكن التي يمكن أن تحدث فيها محاولات الابتزاز، سواء عبر البريد الإلكتروني، الرسائل النصية، أو منصات التواصل الاجتماعي.

2. **تقنيات التشفير وحماية البيانات** :من خلال استخدام تقنيات التشفير المتقدمة، يمكن للجهات الأمنية حماية البيانات الشخصية للمستخدمين ومنع تسريبها أو الوصول غير المصرح به إليها. وتُعدّ هذه الأدوات أساسية في منع استغلال البيانات الخاصة بالطلاب الجامعيين في عمليات الابتزاز.

3. **أدوات تتبع الهوية الرقمية** :تستخدم أجهزة الأمن السيبراني تقنيات متطورة لتتبع الهوية الرقمية للأفراد وتحليل مصادر الهجوم. وبذلك يتمكنون من تحديد هوية مرتكبي الجرائم الإلكترونية والقيام بالتحقيقات اللازمة.

الفرع الثاني: دور شركات التقنية ومزودي الخدمة

تعد شركات التقنية ومزودي الخدمة من العوامل الأساسية في الوقاية من الجرائم الإلكترونية وحماية المستخدمين، بما في ذلك الطلاب الجامعيين، من تهديدات الابتزاز الإلكتروني. فهذه الشركات تملك مسؤولية كبيرة في تطوير أنظمة وتقنيات لحماية بيانات المستخدمين وضمان أمان المعلومات الشخصية. من خلال الدور الذي تلعبه هذه الشركات، يمكن الحد بشكل كبير من فرص وقوع الجرائم الإلكترونية مثل الابتزاز الإلكتروني.

أولاً: دور شركات التقنية في منع الابتزاز الإلكتروني

تساهم شركات التقنية بشكل كبير في تقديم حلول وأدوات أمان متقدمة لمستخدمي الإنترنت لحمايتهم من مخاطر الابتزاز الإلكتروني. يشمل دور هذه الشركات مجموعة من المهام الرئيسية التي تضمن توفير بيئة آمنة على الإنترنت للمستخدمين:

1. **تطوير أدوات الأمان** :من خلال تطوير برامج مكافحة الفيروسات، وأدوات الكشف عن البرامج الضارة، وأنظمة الحماية المتقدمة، تساعد شركات التقنية في توفير بيئة آمنة على الإنترنت. تشجع هذه الشركات مستخدميها على استخدام أحدث برامج الحماية المتاحة لمنع الوصول غير المصرح به إلى البيانات الشخصية.

2. **تحسين سياسات الخصوصية** :تقوم شركات التقنية بتطوير سياسات خصوصية صارمة تهدف إلى حماية معلومات المستخدمين. على سبيل المثال، يُشجع مستخدمو منصات التواصل الاجتماعي على تعديل إعدادات الخصوصية بشكل دوري، مما يقلل من احتمالية تعرضهم للابتزاز الإلكتروني.

3. **تحديث الأنظمة بشكل مستمر** :تقدم شركات التقنية تحديثات مستمرة للبرامج والتطبيقات المستخدمة من قبل الطلاب والجامعات، بهدف إصلاح الثغرات الأمنية التي قد يستغلها المهاجمون لابتزاز الأشخاص. من خلال هذه التحديثات، يتم تعزيز أمان البيانات وحمايتها من السرقة أو التلاعب.

CC BY

ثانيًا: دور مزودي الخدمة في حماية المستخدمين

مزودو الخدمة، سواء كانوا مزودي الإنترنت أو خدمات التطبيقات، يلعبون أيضًا دورًا حيويًا في الحد من الابتزاز الإلكتروني. تتضمن مهامهم توفير الأمان للمستخدمين وضمان سرية بياناتهم:

1. **إجراءات الأمان على مستوى الشبكات** :يقدم مزودو خدمة الإنترنت أنظمة أمان متقدمة لحماية الاتصال عبر الإنترنت. تتضمن هذه الأنظمة تشفير البيانات بين الأجهزة والمخدمات، مما يحول دون تسريب المعلومات أو استغلالها من قبل المهاجمين.

2. **إجراءات الاستجابة للطوارئ** :يُقدّم مزودو خدمة الإنترنت وأصحاب منصات التواصل الاجتماعي آليات للإبلاغ عن الأنشطة المشبوهة. على سبيل المثال، يمكن للطلاب الجامعيين الذين يتعرضون للابتزاز الإلكتروني التوجه إلى هذه المنصات للإبلاغ عن التهديدات واتخاذ إجراءات سريعة لحظر الحسابات المخترقة.

3. **توجيه المستخدمين إلى أفضل الممارسات** :من خلال الحملات التوعوية التي تنظمها شركات التقنية، يتم تعليم المستخدمين كيفية حماية أنفسهم من الجرائم الإلكترونية. يشمل ذلك تقديم نصائح حول كيفية ضبط إعدادات الخصوصية، وكيفية التعامل مع رسائل البريد الإلكتروني المشبوهة، وأفضل الطرق لحماية الحسابات الشخصية على الإنترنت.

الخلاصة:

إن دور الجهات الأمنية والتقنية في مواجهة الابتزاز الإلكتروني يعد أمرًا أساسيًا لضمان حماية الأفراد، خاصة الطلاب الجامعيين. من خلال جهود أجهزة الأمن السيبراني في الكشف المبكر عن الجرائم الإلكترونية وتقديم الدعم التقني للضحايا، بالإضافة إلى دور شركات التقنية ومزودي الخدمة في توفير أدوات الأمان وحماية البيانات الشخصية، يمكن للجامعات والمجتمعات ضمان بيئة رقمية آمنة. ولكن مع تزايد التقنيات والأساليب المتطورة للتهديدات الرقمية، يستمر الدور الفعال لهذه الجهات في تطوير الحلول لمكافحة الابتزاز الإلكتروني وحماية المستخدمين من الأضرار المحتملة.

النتائج:

1. **يُعد الابتزاز الإلكتروني من أخطر الجرائم التي تهدد سلامة الطلاب الجامعيين وخصوصيتهم.**

الابتزاز الإلكتروني يشكل تهديدًا كبيرًا للطلاب الجامعيين نظرًا لاعتمادهم الكبير على الإنترنت في حياتهم الأكاديمية والشخصية. يتسبب الابتزاز في تهديد الخصوصية الشخصية ويمكن أن يؤثر سلبًا على الحالة النفسية والمهنية للطلاب.

2. **غياب التوعية الكافية يزيد من احتمالية تعرض الطلبة للابتزاز.**

تفتقر العديد من المؤسسات التعليمية إلى برامج توعية فعالة حول المخاطر الرقمية وسبل الوقاية منها. هذا الغياب يساهم في زيادة تعرض الطلاب للابتزاز الإلكتروني، حيث يجهل الكثيرون كيفية التعامل مع تهديدات الإنترنت وسبل الحماية من الهجمات الرقمية.

3. **تحتاج الحماية الجنائية إلى دعم تشريعي ومؤسسي وتقني متكامل.**

لا يمكن حماية الطلاب من الابتزاز الإلكتروني بشكل فعال إلا من خلال نظام حماية متكامل يشمل التشريعات القانونية المناسبة، والبنية المؤسسية المتطورة، والأنظمة التقنية الحديثة. التنسيق بين هذه العناصر يسهم في تعزيز الوقاية من الجرائم الإلكترونية وحماية الأفراد.

4. **تفعيل دور الجامعات في التثقيف الرقمي هو عنصر حاسم في الوقاية.**

تعتبر الجامعات من أبرز الأماكن التي يمكن أن تُسهم في التوعية والتثقيف الرقمي للطلاب. من خلال برامج التوعية والتدريب على الأمان الرقمي، يمكن للطلاب أن يتعلموا كيفية حماية أنفسهم من الابتزاز الإلكتروني ويكتسبوا المهارات اللازمة للتعامل مع التهديدات.

5. **وجود تعاون دولي في مكافحة الجرائم الإلكترونية يعزز من فعالية الحماية.**

بما أن الجرائم الإلكترونية ليست محصورة داخل حدود دولة واحدة، فإن التعاون الدولي بين الدول، والشركات التقنية، والجهات الأمنية يعتبر أمرًا بالغ الأهمية لمكافحة الابتزاز الإلكتروني بشكل فعال. من خلال تبادل المعلومات والخبرات، يمكن تعزيز قدرة الدول على محاربة هذه الجرائم وحماية ضحاياها.

التوصيات

1. **تعزيز التشريعات الوطنية لمكافحة الابتزاز الإلكتروني**

ضرورة تحديث وتطوير القوانين الجنائية لتشمل بشكل دقيق صور الابتزاز الإلكتروني الحديثة، مع تغليظ العقوبات المرتبطة بها بما يتناسب مع خطورتها وآثارها النفسية والاجتماعية، خاصة على فئة الطلاب الجامعيين.

2. **إنشاء وحدات متخصصة داخل الجامعات لمكافحة الجرائم الإلكترونية**

يُوصى بإنشاء مكاتب استشارية داخل المؤسسات الأكاديمية تتعاون مع الجهات الأمنية، وتقدم التوجيه والدعم القانوني والتقني للطلاب المعرضين أو المتضررين من الابتزاز الإلكتروني.

3. **إدخال التثقيف الرقمي في المناهج الجامعية**

يجب تضمين مواد تعليمية حول أمن المعلومات، الخصوصية، وأساليب الحماية الإلكترونية ضمن المقررات الجامعية، لتعزيز وعي الطلاب بمخاطر الفضاء الرقمي.

4. **تعزيز التعاون الدولي في ملاحقة المبتزين عبر الحدود**

نظرًا للطبيعة العابرة للحدود لهذه الجريمة، يُوصى بتقوية الاتفاقيات الدولية الخاصة بمكافحة الجريمة الإلكترونية، وتسهيل تبادل المعلومات بين الدول والهيئات المختصة.

5. **تمكين أجهزة الأمن السيبراني تقنيًا وبشريًا**

دعم الجهات الأمنية بكفاءات بشرية مدرّبة وتكنولوجيا متطورة، تُمكّنها من تتبع مرتكبي جرائم الابتزاز الإلكتروني بسرعة وكفاءة، وحماية الضحايا ضمن أطر قانونية واضحة.

6. **إلزام شركات التقنية ومزودي الخدمة بتبني آليات كشف مبكر ومنع الجريمة**

يُوصى بفرض التزامات قانونية على شركات التواصل الاجتماعي ومحركات البحث ومزودي الإنترنت لوضع أدوات فحص محتوى، ونظام إنذار مبكر للابتزاز، وإغلاق الحسابات المشبوهة.

7. **فتح قنوات سرية وآمنة للإبلاغ عن حالات الابتزاز**

يُنصح بإنشاء منصات وطنية إلكترونية تتيح للضحايا الإبلاغ بسرية تامة دون خوف من الفضيحة أو الملاحقة، مع ضمان سرعة الاستجابة من قبل الجهات المختصة.

8. **تنظيم حملات وطنية دورية للتوعية بمخاطر الابتزاز الإلكتروني**

إشراك الإعلام، الجامعات، والمؤسسات الدينية والثقافية في حملات تثقيفية للوقاية من الابتزاز، مع التركيز على الفئات العمرية الشابة والطلابية.

9. **توفير دعم نفسي واجتماعي للضحايا داخل المؤسسات التعليمية**

يُوصى بتوفير وحدات دعم نفسي في الجامعات تساعد الطلاب الذين تعرضوا للابتزاز على تجاوز الصدمة، دون التأثير على استقرارهم الأكاديمي أو النفسي.

10. **تشجيع البحوث العلمية والدراسات المتخصصة**

دعم وتمويل الدراسات القانونية والاجتماعية حول الجريمة الإلكترونية وآثارها على الشباب والطلاب الجامعيين، لتغذية صُنّاع القرار بتوصيات علمية دقيقة.

المراجع:

1. إبراهيم، حسن (2020). "العقوبات السالبة للحرية في الجرائم الإلكترونية"، *دراسات قانونية*، العدد 9، ص 85–98.
2. ابن منظور، محمد بن مكرم (1993(.*لسان العرب* .بيروت: دار صادر.
3. الحاج، عادل (2022(.*الإرشاد الطلابي وحمايتهم من الجرائم الإلكترونية* .القاهرة: دار النشر الجامعي.
4. الحاج، عادل (2022(.*الشركات التقنية في مواجهة الجرائم الإلكترونية* .القاهرة: دار الفكر القانوني.
5. الحاج، عادل (2022) .*حماية الضحايا من الجرائم الإلكترونية* .القاهرة: دار النشر القانونية.
6. حجازي، حسام (2021) .*الأدلة الرقمية في المسائل الجنائية* .بيروت: دار الفقه.
7. الحسني، محمد (2021) .*الجريمة الرقمية: المفاهيم والآثار* .بيروت: دار النهضة.
8. حمدي، جلال (2021). "استخدام تقنيات الديب فيك في الابتزاز"، *مجلة الإعلام الرقمي*، العدد 3، ص 55–70.
9. حمودة، سليم (2020) .*التقنيات الحديثة والجريمة المنظمة* .القاهرة: دار الفكر العربي.
10. حمودة، سليم (2021). "المسؤولية الجنائية للشخص المعنوي في الجرائم الإلكترونية"، *دورية الدراسات القانونية*، العدد 8، ص 130–145.
11. خالد، يوسف (2020). "الشباب والجرائم الإلكترونية"، *دراسات أمنية واجتماعية*، جامعة بغداد، ص 160–175.
12. خليل، سامر (2019) .*الجرائم الإلكترونية: دراسة قانونية مقارنة* .بيروت: دار المطبوعات الجامعية.
13. خليل، سامر (2020) .*الجرائم الإلكترونية: دراسة قانونية مقارنة* .بيروت: دار المطبوعات الجامعية.
14. الخولي، سعاد (2017) .*الجرائم الإلكترونية ومواجهتها* .القاهرة: المركز العربي للنشر.
15. راضي، منى (2018). "الابتزاز العاطفي في العلاقات الرقمية"، *دراسات في علم النفس الرقمي*، العدد 3، ص 100–110.
16. الزعبي، خليل (2020) .*علم الجريمة الإلكترونية* .عمّان: دار الشروق.
17. الزعبي، كمال (2018) .*الإرهاب الإلكتروني: المفهوم والتحديات* .عمّان: دار الثقافة.
18. الزعبي، كمال (2019). "التكنولوجيا الحديثة والجريمة الإلكترونية: تأثير وسائل التواصل الاجتماعي"، *دراسات قانونية حديثة*، العدد 5، ص 200–215.
19. الزيد، أحمد (2020). "الاتفاقيات الدولية لمكافحة الابتزاز الإلكتروني"، *مجلة القانون الدولي*، العدد 7، ص 110–124.
20. الزيد، أحمد (2020). "العقوبات التكميلية في الجرائم الإلكترونية"، *مجلة القانون الجنائي*، العدد 6، ص 100–115.

CC BY

21. الزيد، أحمد (2020). "دور الأمن السيبراني في حماية الأفراد من الجرائم الإلكترونية"، *مجلة الأمن الرقمي*، العدد 5، ص 48–62.

22. الزيد، أحمد (2020). "دور الجامعات في التوعية الرقمية ضد الجرائم الإلكترونية"، *مجلة التعليم العالي*، العدد 4، ص 75–89.

23. زيدان، أحمد (2019). "التهديد الإلكتروني: بين الواقع والقانون"، *مجلة القانون الجنائي*، العدد 6، ص 50–65.

24. زيدان، أحمد (2021). "الهجمات السيبرانية وإشكاليات المواجهة القانونية"، *مجلة القانون والتكنولوجيا*، العدد 12، ص 70–85.

25. زيدان، أحمد (2022). "المسؤولية الجنائية في سياق الجرائم الرقمية"، *مجلة القانون الجنائي الدولي*، العدد 7، ص 100–115.

26. سالم، ريم (2018). "إخفاء الهوية في الفضاء الإلكتروني"، *دراسات أمن المعلومات*، العدد 6، ص 85–100.

27. السنهوري، عبد الرزاق (1980) .*الوسيط في شرح القانون المدني* .القاهرة: دار النهضة العربية.

28. السيد، أحمد (2020) .*الجرائم الإلكترونية وأثرها القانوني* .القاهرة: دار النخبة.

29. السيد، أحمد (2021). "الابتزاز الإلكتروني: أبعاده القانونية والمالية"، *مجلة القوانين الحديثة*، العدد 9، ص 130–145.

30. شحاتة، علي (2019) .*الجريمة الإلكترونية وأثرها على المجتمع* .الإسكندرية: المكتب الجامعي الحديث.

31. شرف الدين، طارق (2022) .*جرائم الفيديو المباشر: قراءة قانونية ونفسية* .عمّان: دار المنهل القانوني.

32. الشرف، علي (2021) .*العقوبات المقررة في الجرائم الإلكترونية* .بيروت: دار الثقافة القانونية.

33. الشمري، فهد (2019). "الابتزاز عبر وسائل التواصل: دراسة تحليلية"، *مجلة القانون والإنترنت*، العدد 8، ص 90–105.

34. عبد الباسط، هالة (2019). "الاختصاص القضائي في الجرائم الرقمية"، *مجلة القانون المعاصر*، العدد 14، ص 65–83.

35. عبد الرحمن، محمد (2018). "الجرائم الإلكترونية: المفهوم والنطاق"، *مجلة الدراسات القانونية المعاصرة*، العدد 12، ص 150–170.

36. عبد الله، سامي (2022) .*العقوبات الجنائية في الجريمة الإلكترونية* .القاهرة: دار النشر القانونية.

37. عبد الله، كمال (2020). "التأثير النفسي للجرائم الإلكترونية"، *مجلة دراسات الطب النفسي والقانون*، العدد 3، ص 115–130.

38. عبد الله، كمال (2020) .*الابتزاز الإلكتروني كأداة سياسية* .القاهرة: مركز دراسات الأمن الإلكتروني.

39. عبد الله، كمال (2022) .*الجرائم الإلكترونية والعقوبات المقررة* .بيروت: دار الثقافة.

40. عبد الله، يوسف (2020). "التشريعات الوطنية ودورها في مكافحة الابتزاز الإلكتروني"، *دراسات قانونية*، العدد 6، ص 93–107.

41. علي، يوسف (2017). *الجرائم الأخلاقية عبر الإنترنت*. بغداد: دار الهدى للنشر.

42. علي، يوسف (2020). *المسؤولية الجنائية عن الجرائم الإلكترونية*. القاهرة: دار الفكر القانوني.

43. علي، يوسف (2022). *الجريمة الإلكترونية وأركانها*. القاهرة: دار النشر القانونية.

44. عمر، جمال (2020). "دور الركن المادي في الجرائم الإلكترونية"، *دراسات قانونية*، العدد 10، ص 100–115.

45. عمر، جمال (2020). *الردع في الجرائم الإلكترونية والعقوبات المتخذة ضدها*. القاهرة: دار الفكر القانوني.

46. عمر، جمال (2021). "الأركان المادية والمعنوية في الجرائم الإلكترونية"، *دراسات قانونية*، العدد 5، ص 65–80.

47. عمر، جمال (2021). *الجرائم الإلكترونية والتحديات الأمنية*. بيروت: دار النشر الأكاديمي.

48. عمر، جمال (2021). *الجرائم الإلكترونية وحماية الأفراد*. بيروت: دار الفكر القانوني.

49. عمر، جمال (2021). *الوقاية من الجرائم الإلكترونية في الجامعات*. بيروت: دار الفكر الأكاديمي.

50. غريب، سامي (2019). "الجرائم المعلوماتية ضد المؤسسات"، *مجلة القانون الرقمي*، العدد 11، ص 130–145.

51. فؤاد، سامي (2020). "سياسات حماية الطلاب من الابتزاز الإلكتروني في الجامعات"، *مجلة القانون والأمن الرقمي*، العدد 11، ص 101–115.

52. فؤاد، سامي (2021). "أثر اتفاقية بودابست على مكافحة الجرائم الإلكترونية"، *مجلة الدراسات القانونية*، العدد 9، ص 85–100.

53. فؤاد، سامي (2021). "دور مزودي الخدمة في الوقاية من الجرائم الإلكترونية"، *مجلة الدراسات القانونية*، العدد 9، ص 70–83.

54. قانون مكافحة الجرائم الإلكترونية الإماراتي (2012). قانون اتحادي رقم 5 لسنة 2012.

55. القحطاني، ناصر (2020). "الابتزاز الجنسي عبر الإنترنت: الظاهرة والحلول"، *مجلة الأمن السيبراني العربي*، العدد 6، ص 140–155.

56. القحطاني، ناصر (2021). "الابتزاز الإلكتروني: التحديات القانونية في مواجهة المجرمين"، *دوريات القضاء الإلكتروني*، العدد 4، ص 120–135.

57. القحطاني، نورة (2021). "ظاهرة الابتزاز الإلكتروني في الجامعات الخليجية"، *مجلة أبحاث الجرائم الإلكترونية*، المجلد 5، العدد 2، ص 130–145.

58. محمد، سامي (2021). "الأركان المادية والمعنوية للجرائم الإلكترونية"، *مجلة الدراسات القانونية الحديثة*، العدد 2، ص 85–95.

59. المهدي، عادل (2022). "الجريمة المالية الإلكترونية: أبعادها القانونية والاقتصادية"، *دراسات قانونية معاصرة*، العدد 7، ص 125–140.

60. ناصر، لطيفة (2022). "الابتزاز الرقمي وأثره على الصحة النفسية"، *مجلة العلوم الاجتماعية*، المجلد 9، العدد 3، ص 100–115.

61. نظام مكافحة الجرائم المعلوماتية السعودي (2007). وزارة الداخلية السعودية.

1. Ibrahim, Hassan (2020). "Citizenship Penalties in Cybercrimes," Legal Studies, Issue 9, pp. 85–98.
2. Ibn Manzur, Muhammad ibn Makram (1993). Lisan al-Arab. Beirut: Dar Sadir.
3. Al-Hajj, Adel (2022). Student Guidance and Protection from Cybercrimes. Cairo: University Publishing House.
4. Al-Hajj, Adel (2022). Technology Companies in the Face of Cybercrime. Cairo: Dar al-Fikr al-Qanuni.
5. Al-Hajj, Adel (2022). Protecting Victims from Cybercrimes. Cairo: Legal Publishing House.
6. Hijazi, Hossam (2021). Digital Evidence in Criminal Matters. Beirut: Dar al-Fiqh.
7. Al-Hasani, Muhammad (2021). Digital Crime: Concepts and Implications. Beirut: Dar al-Nahda.
8. Hamdi, Jalal (2021). "The Use of Deepfake Techniques in Blackmail," Digital Media Magazine, Issue 3, pp. 55–70.
9. Hamouda, Salim (2020). Modern Technologies and Organized Crime. Cairo: Dar Al Fikr Al Arabi.
10. Hamouda, Salim (2021). "Criminal Liability of Legal Persons in Cybercrimes," Journal of Legal Studies, Issue 8, pp. 130–145.
11. Khaled, Youssef (2020). "Youth and Cybercrime," Security and Social Studies, University of Baghdad, pp. 160–175.
12. Khalil, Samer (2019). Cybercrime: A Comparative Legal Study. Beirut: University Publications House.
13. Khalil, Samer (2020). Cybercrime: A Comparative Legal Study. Beirut: University Publications House.
14. Al-Kholi, Suad (2017). Cybercrime and Confronting It. Cairo: Arab Center for Publishing.
15. Radi, Mona (2018). "Emotional Blackmail in Digital Relationships," Studies in Digital Psychology, Issue 3, pp. 100–110.
16. Al-Zoubi, Khalil (2020). Cybercrime. Amman: Dar Al-Shorouk.
17. Al-Zoubi, Kamal (2018). Cyberterrorism: Concept and Challenges. Amman: Dar Al-Thaqafa.
18. Al-Zoubi, Kamal (2019). "Modern Technology and Cybercrime: The Impact of Social Media," Modern Legal Studies, Issue 5, pp. 200–215.

19. Al-Zaid, Ahmed (2020). "International Conventions to Combat Cyberextortion," Journal of International Law, Issue 7, pp. 110–124.

20. Al-Zaid, Ahmed (2020). "Supplementary Penalties in Cybercrimes," Journal of Criminal Law, Issue 6, pp. 100–115.

21. Al-Zaid, Ahmed (2020). "The Role of Cybersecurity in Protecting Individuals from Cybercrimes," Journal of Digital Security, Issue 5, pp. 48–62.

22. Al-Zaid, Ahmed (2020). "The Role of Universities in Raising Digital Awareness Against Cybercrimes," Journal of Higher Education, Issue 4, pp. 75–89.

23. Zidan, Ahmed (2019). "The Cyber Threat: Between Reality and Law," Journal of Criminal Law, Issue 6, pp. 50–65.

24. Zidan, Ahmed (2021). "Cyberattacks and the Problems of Legal Confrontation," Journal of Law and Technology, Issue 12, pp. 70–85.

25. Zidan, Ahmed (2022). "Criminal Liability in the Context of Digital Crimes," Journal of International Criminal Law, Issue 7, pp. 100–115.

26. Salem, Reem (2018). "Anonymity in Cyberspace," Information Security Studies, Issue 6, pp. 85–100.

27. Al-Sanhouri, Abdel-Razzaq (1980). Al-Wasit fi Sharh al-Qanun al-Madani. Cairo: Dar al-Nahda al-Arabiya.

28. Al-Sayyid, Ahmed (2020). Cybercrimes and Their Legal Impact. Cairo: Dar al-Nukhba.

29. Al-Sayyid, Ahmed (2021). "Electronic Blackmail: Its Legal and Financial Dimensions," Journal of Modern Laws, Issue 9, pp. 130–145.

30. Shehata, Ali (2019). Cybercrime and Its Impact on Society. Alexandria: Modern University Office.

31. Sharaf al-Din, Tariq (2022). Live Video Crimes: A Legal and Psychological Reading. Amman: Dar al-Manhal al-Qanuni. 32. Al-Sharaf, Ali (2021). Penalties for Cybercrimes. Beirut: Dar Al-Thaqafa Al-Qanuniya.

32. Al-Shammari, Fahd (2019). "Blackmail via Social Media: An Analytical Study," Journal of Law and the Internet, Issue 8, pp. 90–105.

33. Abdul-Basit, Hala (2019). "Jurisdiction in Digital Crimes," Journal of Contemporary Law, Issue 14, pp. 65–83.

34. Abdul-Rahman, Muhammad (2018). "Cybercrimes: Concept and Scope," Journal of Contemporary Legal Studies, Issue 12, pp. 150–170.

35. Abdullah, Sami (2022). Criminal Penalties for Cybercrimes. Cairo: Legal Publishing House.

36. Abdullah, Kamal (2020). "The Psychological Impact of Cybercrimes," Journal of Psychiatric and Legal Studies, Issue 3, pp. 115–130.

37. Abdullah, Kamal (2020). Cyber Blackmail as a Political Tool. Cairo: Center for Cyber Security Studies.

38. Abdullah, Kamal (2022). Cybercrimes and Prescribed Penalties. Beirut: Dar Al-Thaqafa.

39. Abdullah, Youssef (2020). "National Legislation and Its Role in Combating Cyberblackmail," Legal Studies, Issue 6, pp. 93–107.

40. Ali, Youssef (2017). Moral Crimes on the Internet. Baghdad: Dar Al-Huda Publishing House.

41. Ali, Youssef (2020). Criminal Liability for Cybercrimes. Cairo: Dar Al-Fikr Al-Qanuni.

42. Ali, Youssef (2022). Cybercrime and Its Elements. Cairo: Legal Publishing House.

43. Omar, Gamal (2020). "The Role of the Material Element in Cybercrimes," Legal Studies, Issue 10, pp. 100–115.

44. Omar, Gamal (2020). Deterrence in Cybercrimes and Penalties. Cairo: Dar Al Fikr Al Qanuni.

45. Omar, Jamal (2021). "The Material and Moral Elements of Cybercrimes," Legal Studies, Issue 5, pp. 65–80.

46. Omar, Jamal (2021). Cybercrimes and Security Challenges. Beirut: Academic Publishing House.

47. Omar, Jamal (2021). Cybercrimes and the Protection of Individuals. Beirut: Dar Al Fikr Al Qanuni.

48. Omar, Jamal (2021). Preventing Cybercrimes in Universities. Beirut: Dar Al Fikr Al Qanuni.

49. Gharib, Sami (2019). "Cybercrimes Against Institutions," Journal of International Law