

التنظيم القانوني لمكافحة الجرائم المعلوماتية في النظام السعودي: تحليل الأحكام القضائية المتعلقة بالابتزاز الإلكتروني

إعداد الطالبة/
كيان عبدالرحمن الشهري

إشراف/

العام الدراسي:
(٢٠٢٤ - ٢٠٢٥ م)

• المقدمة:

تعد الجرائم المعلوماتية من أبرز القضايا المعاصرة، حيث أن تكنولوجيا المعلومات والاتصالات تلعب دوراً مزدوجاً؛ فهي تعزز من وسائل التواصل وتسهيل الأعمال، لكنها أيضاً تتيح المجال أمام أنشطة إجرامية خطيرة مثل الابتزاز الإلكتروني. يتجلى الابتزاز الإلكتروني في استخدام

التهديد بنشر معلومات حساسة أو صور خاصة بهدف الحصول على أموال أو مكاسب أخرى، مما يؤدي إلى تآكل الثقة وانتهاك الخصوصية.

يُعتبر الابتزاز الإلكتروني من أبرز التهديدات التي تواجه الأفراد والمجتمعات في عصر تكنولوجيا المعلومات المتطورة. فقد شهدت هذه الظاهرة انتشاراً ملحوظاً في ظل التحولات الرقمية السريعة، مما يضع الأمن الاجتماعي والاقتصادي في المملكة العربية السعودية أمام تحديات جسيمة. يستغل ضعاف النفوس الثغرات الموجودة في الأنظمة الرقمية لتهديد الآخرين وتحقيق مكاسب غير قانونية، سواء على الصعيد المالي أو النفسي.

استجابةً لهذا التحدي، أقدمت الحكومة السعودية على إصدار تشريعات صارمة تهدف إلى مكافحة الابتزاز الإلكتروني، مع الاستفادة من التقنيات الحديثة لتطوير حلول فعالة. تعكس هذه الإجراءات الجادة من السلطات السعودية التزامها بخلق بيئة رقمية آمنة ومزدهرة، بما يتماشى مع الرؤية الوطنية الطموحة للمملكة في مجال التحول الرقمي.

لذلك، اتخذت المملكة خطوات حيوية لمواجهة هذه الظاهرة من خلال إصدار نظام مكافحة جرائم المعلوماتية بموجب مرسوم ملكي رقم (م/17) في 1428/3/8 هـ (2007)، والذي تم تعديله في عام 2017. يعتبر هذا النظام إطاراً قانونياً شاملاً لمكافحة الجرائم المعلوماتية وتوفير الحماية اللازمة للأفراد والمجتمع. على الرغم من الجهود المبذولة، إلا أن هناك تحديات قائمة في تنفيذ هذه القوانين، مما يستدعي الحاجة إلى تحليل الأحكام القضائية المتعلقة بهذا المجال لفهم كيفية تطبيق القوانين ومدى فعاليتها في التصدي للابتزاز الإلكتروني.

يهدف هذا البحث إلى دراسة التنظيم القانوني لمكافحة الجرائم المعلوماتية في النظام السعودي، مع التركيز على تحليل الأحكام القضائية ذات الصلة بالابتزاز الإلكتروني. سيتم تناول الموضوع عبر عدة محاور تشمل الإطار النظري للجرائم المعلوماتية، والتشريعات القانونية لمكافحة هذه الجرائم، ودراسة حالات قضائية محددة. من خلال هذا التحليل، يسعى البحث إلى تقديم توصيات تهدف إلى تحسين فعالية التشريعات الحالية وتعزيز سبل الحماية القانونية للأفراد، حيث يمثل هذا البحث خطوة نحو تعزيز الفهم القانوني لمكافحة الجرائم المعلوماتية في المملكة، مما يساهم في حماية المجتمع من مخاطر هذه الجرائم ويساعد في تطوير التشريعات اللازمة لمواجهة التحديات المستقبلية.

● مشكلة البحث:

تعتبر الجرائم المعلوماتية، وبالأخص الابتزاز الإلكتروني، من التحديات المعقدة التي تواجه المجتمعات الحديثة في ظل الثورة الرقمية. في المملكة العربية السعودية، أدت زيادة استخدام التكنولوجيا والإنترنت إلى تفشي ظاهرة الابتزاز الإلكتروني، مما يستدعي اهتماماً قانونياً خاصاً. ومع ذلك، يبقى السؤال المطروح: هل يفي التنظيم القانوني لمكافحة الجرائم المعلوماتية في النظام السعودي بمتطلبات حماية الأفراد والمجتمع من هذه الأنشطة الإجرامية المتزايدة؟

تتجلى إشكالية البحث من خلال عدة محاور رئيسية:

1. تقييم مدى كفاءة نظام مكافحة الجرائم المعلوماتية في مواجهة الابتزاز الإلكتروني وحماية حقوق الضحايا.
2. دراسة تطبيق القوانين في المحاكم ومدى فعاليتها في حماية الضحايا.
3. استكشاف العقبات التي تواجه الجهات المعنية في تنفيذ القوانين ومدى تأثيرها على الحماية المجتمعية.
4. كيفية تكيف التشريعات مع التطورات التكنولوجية السريعة.
5. تعزيز الوعي القانوني بين الأفراد واستراتيجيات الوقاية الممكنة.
6. تحقيق التوازن بين مكافحة الجرائم وحماية خصوصية الأفراد.

بناءً على هذه المحاور، تهدف إشكالية البحث إلى تقديم تحليل شامل للتنظيم القانوني لمكافحة الجرائم المعلوماتية في المملكة، من خلال دراسة الأحكام القضائية المتعلقة بالابتزاز الإلكتروني. يسعى البحث إلى تقديم توصيات تستند إلى النتائج المستخلصة من هذا التحليل لتحسين فعالية التشريعات وتعزيز سبل الحماية.

• أهداف البحث:

يهدف البحث إلى تقديم مساهمة قيمة في فهم وتطوير الإطار القانوني لمكافحة الجرائم المعلوماتية، وتعزيز فعالية الأنظمة القضائية في مواجهة التحديات الناجمة عن الابتزاز الإلكتروني من خلال:

- تقديم فهم شامل للتنظيم القانوني لمكافحة الجرائم المعلوماتية في السعودية.
- تسليط الضوء على القضايا القانونية المحورية المتعلقة بالابتزاز الإلكتروني.
- توضيح مدى فعالية القوانين الحالية والتحديات التي تواجهها.
- الخروج بتوصيات عملية لتحسين التشريعات والآليات التنفيذية.

من خلال هذه الأهداف يسعى البحث إلى المساهمة الفعالة في تعزيز الإطار القانوني لمواجهة الابتزاز الإلكتروني، مما يساهم في حماية المجتمع من المخاطر المتزايدة في الفضاء الرقمي.

• أهمية البحث:

يبرز البحث أهمية أكاديمية كبيرة في توسيع الفهم القانوني للجرائم المعلوماتية، خصوصاً الابتزاز الإلكتروني. يوفر للباحثين والطلاب فرصة دراسة القوانين في السعودية، ويحلل الأحكام القضائية لفهم تطبيق القوانين عملياً. يساهم البحث في تقديم توصيات للهيئات الحكومية لتحسين استراتيجيات مكافحة الجرائم، ويعزز حماية حقوق الأفراد وزيادة الوعي المجتمعي بمخاطر الابتزاز. كما يمثل نقطة انطلاق لدراسات مستقبلية في هذا المجال، مما يعزز الحركة البحثية حول الأمن الرقمي. باختصار، يساهم البحث في تعزيز الفهم القانوني وبناء نظام قانوني أكثر فعالية لمواجهة تحديات الجرائم المعلوماتية.

• تساؤلات البحث:

يقوم هذا البحث بالإجابة على التساؤل الرئيسي التالي:

كيف يمكن تقييم فعالية التنظيم القانوني لمكافحة الجرائم المعلوماتية في النظام السعودي في التصدي لظاهرة الابتزاز الإلكتروني وحماية حقوق الأفراد والمجتمع؟

تساؤلات فرعية:

1. ما مدى كفاءة نظام مكافحة الجرائم المعلوماتية في مواجهة الابتزاز الإلكتروني؟
2. كيف يتم تطبيق القوانين المتعلقة بالجرائم المعلوماتية في المحاكم، وما مدى فعاليتها في حماية الضحايا؟
3. ما هي العقوبات التي تواجه الجهات المعنية في تنفيذ القوانين المتعلقة بالابتزاز الإلكتروني، وكيف تؤثر هذه العقوبات على الحماية المجتمعية؟
4. كيف تتكيف التشريعات القانونية في المملكة مع التطورات التكنولوجية السريعة في مجال الجرائم المعلوماتية؟
5. ما هو دور الوعي القانوني بين الأفراد في مكافحة الابتزاز الإلكتروني، وما هي استراتيجيات الوقاية الممكنة لتعزيز هذا الوعي؟
6. كيف يمكن تحقيق التوازن بين مكافحة الجرائم المعلوماتية وحماية خصوصية الأفراد في ظل القوانين الحالية؟

• فرضيات البحث:

- 1) تعتبر تشريعات المملكة العربية السعودية لمكافحة الجرائم المعلوماتية فعالة في مواجهة الابتزاز الإلكتروني، مما يسهم في حماية حقوق الضحايا.
- 2) تظهر الأحكام القضائية في المملكة العربية السعودية ارتفاعاً في مستوى التنفيذ الفعلي لقوانين مكافحة الابتزاز الإلكتروني وتطبيقها في المحاكم، مما يعكس قدرة النظام القانوني على التعامل مع هذه القضايا.
- 3) تواجه الجهات المعنية في المملكة تحديات تنفيذية تؤثر سلباً على فعالية القوانين المتعلقة بمكافحة الابتزاز الإلكتروني، مما يستوجب تقديم توصيات لتحسين تلك العملية.
- 4) هناك علاقة إيجابية بين التكيف التشريعي مع التطورات التكنولوجية السريعة وزيادة فعالية سياسة مكافحة الجرائم المعلوماتية في المملكة.
- 5) تعزز زيادة الوعي القانوني بين الأفراد استراتيجيات الوقاية وتقلل من مخاطر الابتزاز الإلكتروني في المجتمع السعودي.
- 6) يساهم تحقيق التوازن بين مكافحة الجرائم وحماية خصوصية الأفراد في تعزيز الثقة في النظام القانوني ويؤدي إلى فعالية أكبر في مواجهة الابتزاز الإلكتروني.

• منهج البحث:

يوضح المنهج المقترح كيفية دراسة "التنظيم القانوني لمكافحة الجرائم المعلوماتية في النظام السعودي: تحليل الأحكام القضائية المتعلقة بالابتزاز الإلكتروني". يتم التركيز على توضيح أهداف البحث ومشكلاته والأساليب المستخدمة لتحقيق النتائج المطلوبة.

- الأسلوب التحليلي: سيتم استخدام الأسلوب التحليلي في تحليل الأحكام القضائية والتشريعات المطبقة. سيتضمن ذلك دراسة نصوص القوانين، وتحليل المعايير القانونية، وقراءة قرارات المحاكم.
- المقابلات والاستبيانات: إجراء مقابلات مع خبراء قانونيين ومحامين وقضاة للاستفادة من آرائهم وتجاربهم في هذا المجال. كما يمكن استخدام استبيانات لجمع آراء الأفراد بشأن تجربتهم مع الابتزاز الإلكتروني وتفاعلهم مع القوانين.
- دراسة حالات: سيتم اختيار عدد من الحالات القضائية لدراسة عميقة، لفهم كيفية تطبيق النظام القانوني ومدى فعاليته في التصدي للابتزاز الإلكتروني.
- المراجعة الأدبية: مراجعة الأدبيات الموجودة حول موضوع الجرائم المعلوماتية، بما في ذلك الدراسات السابقة والبحوث القانونية ذات الصلة، لفهم الاتجاهات الحالية والتحديات المستقبلية.

• أدوات البحث:

١- مصادر أولية:

- التشريعات والأنظمة: مثل نظام مكافحة الجرائم المعلوماتية.
- الأحكام القضائية: التي تصدرها المحاكم السعودية بشأن قضايا الابتزاز الإلكتروني.

٢- مصادر ثانوية:

- الكتب والأبحاث والدراسات السابقة: التي تناولت موضوع الجرائم المعلوماتية.
- المقالات القانونية: في المجالات والمواقع الأكاديمية.

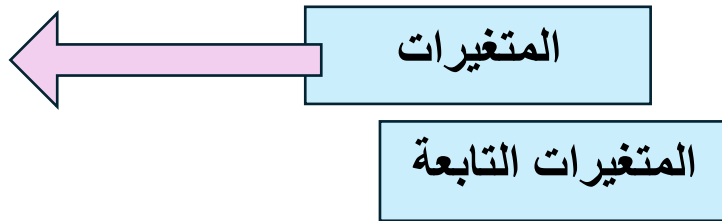
• متغيرات البحث:

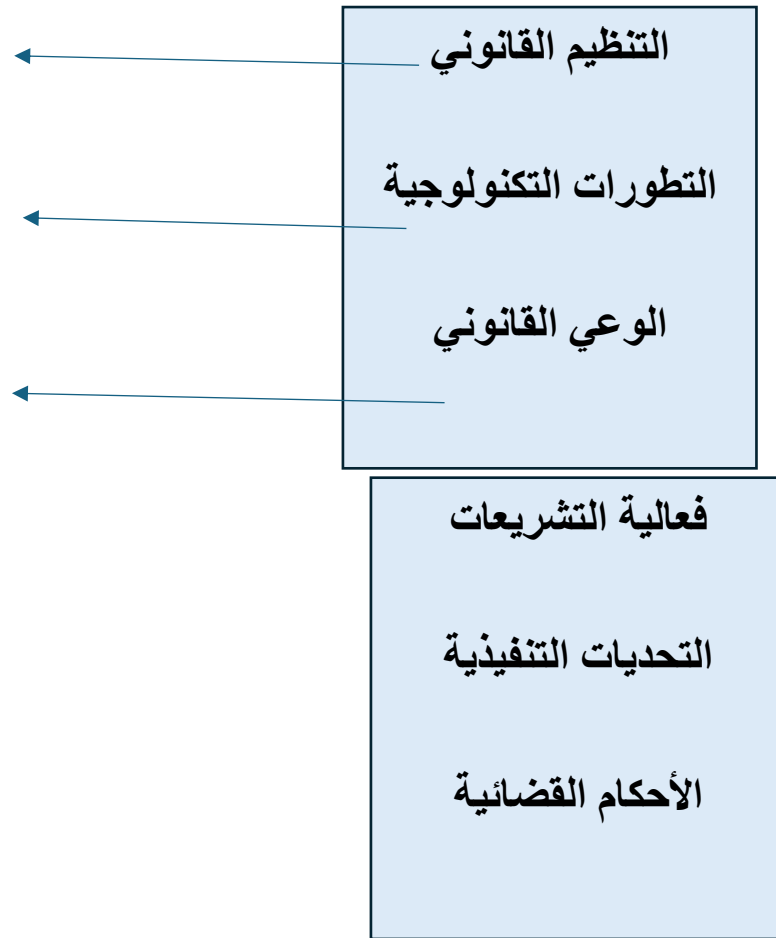
تركز الدراسة على تحليل كيفية تنظيم مكافحة الجرائم المعلوماتية في النظام السعودي، مع التركيز على الابتزاز الإلكتروني كظاهرة متنامية.

- **التنظيم القانوني:** يمثل القاعدة الأساسية التي يُبنى عليها مكافحة الجرائم المعلوماتية، ويشمل تحليل الظروف القانونية الحالية والممارسات المرتبطة بها.
- **التطورات التكنولوجية:** تعتبر عاملاً مؤثراً في كيفية تطور أساليب الابتزاز، مما يتطلب تحديثاً دورياً للتشريعات لمواجهتها.

- الوعي القانوني: يرتبط بمدى قدرة الأفراد على حماية أنفسهم من الجرائم المعلوماتية وفهمهم للقوانين القائمة.

• نموذج البحث:





المصدر: إعداد الباحثه

● حدود البحث:

1. الحدود الزمنية:

- تركز هذه الدراسة على القوانين والأنظمة المعمول بها في المملكة العربية السعودية منذ صدور نظام مكافحة جرائم المعلوماتية في عام 2007، مع الأخذ في الاعتبار التعديلات التي أجريت عليه في عام 2017. ستشمل الدراسة تحليل الأحكام القضائية الصادرة خلال هذه الفترة الزمنية.

2. الحدود الجغرافية:

- تقتصر الدراسة على نطاق المملكة العربية السعودية، حيث سيتم تناول كيفية تعامل النظام القانوني السعودي مع قضايا الابتزاز الإلكتروني والأحكام القضائية المتعلقة بها.

3. الحدود الموضوعية:

- تركز الدراسة على التنظيم القانوني لمكافحة الجرائم المعلوماتية، وبشكل خاص الابتزاز الإلكتروني. ستتناول الدراسة النصوص القانونية، الأحكام القضائية، والعوامل المؤثرة في تطبيق هذه القوانين، دون التطرق إلى أنواع أخرى من الجرائم المعلوماتية.

4. الحدود المنهجية:

- ستعتمد الدراسة على المنهج الوصفي التحليلي المقارن، مما يعني تحليل النصوص القانونية والأحكام القضائية، بالإضافة إلى مقارنة الأنظمة القانونية السعودية مع أنظمة دولية أخرى إذا دعت الحاجة، ولكنها لن تشمل دراسات ميدانية أو تجريبية.

5. الحدود النظرية:

- ستركز الدراسة على الجوانب القانونية والتشريعية المرتبطة بالجرائم المعلوماتية، مع إيلاء اهتمام خاص لدراسة الابتزاز الإلكتروني. لن تتناول الدراسة الجوانب النفسية أو الاجتماعية بشكل مفصل، إلا في إطار تأثيراتها القانونية.
- من خلال هذه الحدود، تهدف الدراسة إلى تقديم تحليل شامل لمشكلة الابتزاز الإلكتروني في السياق القانوني السعودي، مما يساهم في تعزيز الفهم القانوني والبحث في كيفية تطوير التشريعات لمواجهة هذه الظاهرة.

● مصطلحات البحث:

- **الجرائم المعلوماتية:** تشمل الجرائم التي تستخدم فيها تكنولوجيا المعلومات والاتصالات لتحقيق أنشطة إجرامية، مثل القرصنة والابتزاز الإلكتروني.¹
- **الابتزاز الإلكتروني:** هو استخدام التهديد بنشر معلومات حساسة أو صور خاصة للحصول على أموال أو مكاسب أخرى، مما يعد انتهاكاً للخصوصية.²
- **التشريعات القانونية:** القوانين والأنظمة التي تهدف إلى تنظيم الأنشطة الإلكترونية وحماية الأفراد من الجرائم المعلوماتية.³
- **الأحكام القضائية:** القرارات الصادرة عن المحاكم في قضايا الابتزاز الإلكتروني التي تحدد كيفية تطبيق القوانين ومدى فعاليتها.⁴
- **التحديات التنفيذية:** العقبات التي تواجه الجهات المعنية في تطبيق القوانين المتعلقة بالجرائم المعلوماتية.

¹ . نظام مكافحة جرائم المعلوماتية: شرح المادة 3 و6 من النظام.

<https://etqanlawfirm-sa.com/%D9%86%D8%B8%D8%A7%D9%85-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9/>

² قضايا الابتزاز وعقوبتها في القانون السعودي.

<https://naylawfirm.com/%D9%82%D8%B6%D8%A7%D9%8A%D8%A7-%D8%A7%D9%84%D8%A7%D8%A8%D8%AA%D8%B2%D8%A7%D8%B2-%D9%81%D9%8A-%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9/>

³ الهيئة الوطنية للأمن السيبراني. (2024). أنظمة وتشريعات البيانات والأمن السيبراني. <https://nca.gov.sa/ar/>

⁴ أحكام قضايا الابتزاز في القانون السعودي..

<https://alqrnilaw.com/2024/05/04/blackmail-cases>

- التوازن بين الأمن والخصوصية: الجهد المبذول لتحقيق توازن بين حماية الأمن العام ومراعاة حقوق الأفراد وخصوصيتهم.⁵
- الوعي القانوني: معرفة الأفراد بحقوقهم القانونية والإجراءات المتاحة لهم عند تعرضهم لمخاطر مثل الابتزاز الإلكتروني.⁶
- التحول الرقمي: الجهود المبذولة من قبل الحكومة السعودية لتطوير الأنظمة الرقمية وتعزيز الابتكار في مختلف القطاعات.⁷
- استراتيجيات الوقاية: التدابير والإجراءات التي يمكن اتخاذها للحد من مخاطر الجرائم المعلوماتية وزيادة الوعي بين الأفراد.⁸
- المراجع القانونية: المصادر التي تحتوي على النصوص القانونية والتشريعات ذات الصلة بالجرائم المعلوماتية.⁹

• الدراسات السابقة:

○ أولاً: الدراسات العربية:

١- دراسة داليا عبدالعزيز، (2018). المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي: دراسة مقارنة.¹⁰

هدفت الدراسة إلى التعرف على جريمة الابتزاز الإلكتروني في كل من النظام السعودي والقانون الإماراتي، وتقديم تحليل شامل لمكوناتها وأركانها، بالإضافة إلى دراسة الإجراءات القانونية المرتبطة بها.

استخدمت الدراسة المنهج التحليلي المقارن، حيث تمت مقارنة جريمة الابتزاز الإلكتروني في النظامين، وتحليل أركان الجريمة ودوافعها وآثارها، بالإضافة إلى استعراض الإجراءات المتبعة في التحقيق ووسائل الإثبات المستخدمة.

توصلت الدراسة إلى عدد من النتائج، من أهمها أن جريمة الابتزاز الإلكتروني تُعتبر من الصور الحديثة للجريمة الإلكترونية، وأن هناك أوجه قصور في الإجراءات القانونية المعمول بها في كل من النظام السعودي والقانون الإماراتي، مما قد يعوق جهود التحقيق ويعقد من عملية الإثبات،

⁵ . الفرق بين الجرائم المعلوماتية والجرائم الإلكترونية.

<https://jolighm.com/%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9>

⁶ السويدي، ش. م.، & نوفل، د. ز. م. (2023). أسباب الابتزاز الإلكتروني والآثار النفسية والاجتماعية المرتبطة به (دراسة نوعية). مجلة الأدب، 146. <https://doi.org/10.31973/aj.v1i146.4008>

⁷ المجتمع الرقمي. (2024). المنصة الوطنية الموحدة. <https://www.my.gov.sa/aboutksa>

⁸ مداح، أ. ف. (2004). سياسة الوقاية والمنع لحماية الشباب السعودي من الوقوع في الجريمة: دراسة تطبيقية من واقع هيئة الأمر بالمعروف والنهي عن المنكر، (رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية).

https://ncys.ksu.edu.sa/sites/ncys.ksu.edu.sa/files/Crime%2016_5.pdf

⁹ مجموعة الأنظمة السعودية. (2024). "أنظمة المواصلات والاتصالات: نظام مكافحة جرائم المعلوماتية".

¹⁰ عبد العزيز، د. (2018). المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي: دراسة مقارنة. *مجلة جيل الأبحاث القانونية المعمقة*، 25، 27. <https://jilrc.com/archives/9216>

خاصة فيما يتعلق بالدليل الرقمي. كما كشفت الدراسة عن العقوبات المقررة لهذه الجريمة، وبيّنت الفروق بين النظامين في حالات التشديد والإعفاء وعقاب الشروع والمساهمة الجنائية.

أوصت الدراسة بضرورة تعزيز الإطار التشريعي لمكافحة جريمة الابتزاز الإلكتروني في كل من النظام السعودي والقانون الإماراتي، من خلال تحديث القوانين وإجراء تعديلات تشريعية تتماشى مع التطورات التكنولوجية الحديثة، بالإضافة إلى تحسين إجراءات التحقيق والتعامل مع الأدلة الرقمية بشكل أكثر فعالية.

التعقيب على الدراسة:

تعتبر هذه الدراسة مهمة للغاية في ظل تزايد ظاهرة الابتزاز الإلكتروني، حيث تقدم تحليلاً دقيقاً للأبعاد القانونية لهذه الجريمة في سياقين مختلفين. من خلال المقارنة بين النظامين، تسلط الدراسة الضوء على أوجه القصور والنجاح، مما يمكن أن يساهم في تحسين التشريعات والممارسات القانونية في هذا المجال. إن توصيات الدراسة تشكل خطوة نحو تعزيز فعالية مكافحة الابتزاز الإلكتروني، وتؤكد على أهمية التعاون بين الجهات القانونية والتشريعية لتطوير استراتيجيات فعالة لمواجهة هذه الظاهرة المتزايدة.

٢- دراسة الغديان، س. ب. ع.، خطاطبه، ي. ب. م. النعيمي، و عوادم، ع. ع. (2018). صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين.¹¹

هدفت الدراسة إلى الكشف عن أهم صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين.

استخدمت الدراسة المنهج الوصفي التحليلي، حيث تم جمع البيانات من عينة مكونة من (٥٢٣) مستجيباً موزعين إلى ثلاث شرائح، تشمل أعضاء هيئة الأمر بالمعروف والنهي عن المنكر، المستشارين النفسيين، والمعلمين والمعلمات.

توصلت الدراسة إلى أن أكثر صور الجرائم الإلكترونية شيوعاً هي الصور المادية بمتوسط حسابي مرتفع (٣,٩٦)، بينما كانت صور التسلية الأقل شيوعاً بمتوسط حسابي (٣,٠٦). كما أظهرت الدراسة أن الدوافع الجنسية كانت الأكثر ارتفاعاً بمتوسط حسابي (٣,٩٠)، في حين كانت الدوافع المادية أقل بمتوسط حسابي (٣,٢٣). ومن ناحية الآثار النفسية، كانت الإصابة باضطرابات القلق والخوف الأكثر تأثيراً (٣,٩٥)، بينما كانت اضطرابات الإخراج أقل تأثيراً (٢,٧٠). وأيضاً، لم تظهر فروق ذات دلالة إحصائية في صور الجرائم بناءً على فئة المستجيب، بينما وُجدت فروق دالة في الدوافع المادية والانفعالية ودوافع التسلية لصالح المعلمين، وفي الدوافع الجنسية لصالح رجال الهيئة.

¹¹ الغديان، س. ب. ع.، خطاطبه، ي. ب. م. النعيمي، و عوادم، ع. ع. (2018). صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين. *مجلة البحوث الأمنية*، 27(69)، 157-227. <https://search.mandumah.com/Record/878075>

أوصت الدراسة على ضرورة تعزيز الوعي بمخاطر الابتزاز الإلكتروني، وتطوير برامج دعم نفسي للضحايا، وتفعيل التعاون بين المؤسسات التعليمية والجهات ذات الاختصاص لمكافحة هذه الظاهرة.

التعقيب على الدراسة:

تعتبر هذه الدراسة مهمة جداً في سياق تفشي جرائم الابتزاز الإلكتروني وتأثيراتها النفسية على الأفراد، خاصة في المجتمع التعليمي. استخدام العينة المتنوعة من المعلمين ورجال الهيئة والمستشارين النفسيين يعزز من موثوقية النتائج. ومع ذلك، يمكن توسيع نطاق البحث ليشمل فئات اجتماعية أخرى مثل الطلاب وأولياء الأمور، مما قد يساهم في فهم أكثر شمولية لهذه الظاهرة. كما ينبغي أن تتضمن التوصيات استراتيجيات فعالة للتدخل المبكر وتوفير التدريب للعاملين في المجالات النفسية والاجتماعية للتعامل مع حالات الابتزاز الإلكتروني بشكل أكثر فعالية.

٣- دراسة: (Naggi, I. M. A. 2024). بعنوان: التنظيم التشريعي لجريمتي التهديد والابتزاز المعلوماتي - دراسة تحليلية أساسية لقانون الجرائم المعلوماتية السعودي. ¹² "Legislative regulation of both crimes of threat and informational blackmail – Analytical fundamental study of Saudi Informational crimes law"

ها تهدف هذه الدراسة إلى مناقشة واحدة من أهم القضايا الناتجة عن الثورة التكنولوجية المتطورة بسرعة، حيث أصبح الإكراه والابتزاز الإلكتروني من النتائج السلبية لتلك الثورة.

استخدمت الدراسة المنهج التحليلي الأساسي لدراسة الجريمة وعناصرها، وتحليل الأحكام القانونية بهدف الوصول إلى أشكال تنفيذ الجريمة وعناصرها والعقوبات المفروضة على الجاني بشأن هذه الجريمة.

توصلت الدراسة إلى أن جريمة الإكراه والابتزاز تمر بعدة مراحل، وأن هدف الجاني هو تحقيق رغباته، سواء كانت مادية، أو معنوية، أو جنسية. كما تم تقسيم العمل البحثي إلى قسمين، حيث يتناول القسم الأول تعريف جريمة الإكراه وشروطها، وتعريف جريمة الابتزاز الإلكتروني وأنواعها وأهدافها. بينما يتناول القسم الثاني عناصر تحقق الجريمة والعقوبة المحددة لها بموجب القانون.

أوصت الدراسة بضرورة تعزيز الوعي القانوني والاجتماعي حول هذه الجرائم، وتطوير القوانين المتعلقة بالجرائم المعلوماتية لتكون قادرة على مواجهة التحديات المستجدة.

التعقيب على الدراسة:

يمكن اعتبار هذه الدراسة ذات أهمية كبيرة في ظل التغيرات السريعة في التكنولوجيا وتأثيراتها على السلوكيات الإجرامية. تقدم الدراسة تحليلاً شاملاً للمسائل القانونية المتعلقة بالإكراه والابتزاز

¹² Naggi, I. M. A. (2024). Legislative regulation of both crimes of threat and informational blackmail – Analytical fundamental study of Saudi informational crimes law. Journal of Law and Sustainable Development, 12(3), 01-22. <https://doi.org/10.55908/sdgs.v12i3.3447>

المعلوماتي، مما يسهم في تعزيز الفهم القانوني لهذه الجرائم. كما أنها تبرز الحاجة إلى مزيد من الأبحاث والسياسات للتصدي لهذه الظواهر المتزايدة في المجتمع.

٤- دراسة حمدي، غاده م. ع، طوهري م. ص. ع. (2020). الحماية القانونية من جريمة الابتزاز تحت ظل النظام السعودي.¹³

هدفت الدراسة إلى استكشاف الحماية القانونية من جريمة الابتزاز في النظام السعودي، وتحليل كيفية تأثير هذه الحماية على الأفراد والمجتمع.

استخدمت الدراسة المنهج التحليلي والاستقرائي، حيث اعتمد الباحثان على قراءة الأدبيات ذات الصلة، وجمع البيانات من دراسات سابقة، بالإضافة إلى إجراء استبيانات ومقابلات مع أفراد تعرضوا لجريمة الابتزاز.

توصلت الدراسة إلى عدة نتائج، منها:

1. انتشار جريمة الابتزاز، خاصة عبر الإنترنت، مما يتطلب استجابة قانونية فعالة.
 2. عدم وعي الضحايا بالجهات المختصة للتبليغ، حيث أظهرت النتائج أن 88% من المشاركين لا يعرفون كيفية التبليغ عن جريمة الابتزاز.
 3. الحاجة إلى تشديد العقوبات المفروضة على المبتزين وتعديل الأنظمة القانونية ذات الصلة.
- أوصت الدراسة على ضرورة:

1. تشديد العقوبات لتكون رادعة للمبتزين.
 2. تعديل المواد القانونية بما يتناسب مع تغير الإجراءات واحتياجات المجتمع.
 3. توحيد رقم موحد للتبليغ عن جرائم الابتزاز.
 4. تشجيع الضحايا على الإبلاغ عن الجرائم.
 5. توعية المجتمع بكيفية حماية المعلومات الشخصية.
- التعقيب على الدراسة:

تعد هذه الدراسة مهمة وضرورية في ظل تزايد حالات الابتزاز في المجتمع السعودي. تعكس النتائج الحاجة الماسة لتوعية المجتمع وتعزيز الحماية القانونية لضمان سلامة الأفراد وتقليل آثار هذه الجرائم النفسية والاجتماعية.

٥- دراسة: (Elfaouri, O. T. A, 2024). بعنوان: الابتزاز الإلكتروني جريمة وفقاً لقانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023. **Electronic Extortion is a "Crime, According to Jordan's Electronic Crimes Law No. 17 of 2023".**

¹³ حمدي، غاده محمد عبدالله، طوهري، مريم صديق عمر، & عوض الكريم. (2020). الحماية القانونية من جريمة الابتزاز تحت ظل النظام السعودي. المجلة الإلكترونية الشاملة متعددة المعرفة لنشر الأبحاث العلمية و التربوية. <https://www.mecsaj.com>

¹⁴ Elfaouri, O. T. A, 2024. Cyber extortion is a crime under the Jordanian Cybercrime Law No. 17 of 2023. Pakistan Journal of Criminology, 16(3).

هدفت الدراسة إلى تحليل قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023 وكيفية تناول الابتزاز الإلكتروني ضمن هذا التشريع.

استخدمت الدراسة المنهج التحليلي القانوني، حيث استعرضت النصوص القانونية المتعلقة بالابتزاز الإلكتروني وقارنتها بالقوانين السابقة.

توصلت الدراسة إلى أن قانون الجرائم الإلكترونية الجديد يحدد بوضوح الأبعاد القانونية للابتزاز الإلكتروني من خلال المادة 18، مما يعكس التوجه العقابي للمشرع الأردني ويزيل الغموض حول العقوبات.

أوصت الدراسة بتعزيز تطبيق القوانين الجديدة وتوفير التوعية القانونية للمواطنين حول الابتزاز الإلكتروني، إضافة إلى تطوير استراتيجيات فعالة لمكافحة هذه الجريمة.

التعقيب على الدراسة:

تعتبر هذه الدراسة خطوة هامة في فهم كيفية تعامل التشريع الأردني مع ظاهرة الابتزاز الإلكتروني. ومن الضروري أن يتم تطبيق القوانين بشكل فعال لتحقيق الأثر المطلوب في تقليل هذه الظاهرة وحماية الأفراد والمجتمع.

٦- دراسة: (Hussein, S., & Mohammed, S. 2024). بعنوان: تحليل الإطار القانوني وتداعيات المرسوم بقانون اتحادي رقم 34/2021 في مكافحة الابتزاز الإلكتروني في دولة الإمارات العربية المتحدة. ¹⁵ "Analyzing the Legal Framework and Implications of Federal Decree-Law No. 34/2021 in Combatting Cyber Blackmail in the UAE"

تهدف الدراسة إلى تحليل الإطار القانوني لمكافحة الابتزاز الإلكتروني في دولة الإمارات العربية المتحدة، من خلال استعراض العقوبات المحددة في المرسوم بقانون اتحادي رقم 34 لسنة 2021 وتقييم تأثير هذا القانون على مشهد جرائم الابتزاز.

استخدمت الدراسة المنهج الوصفي التحليلي، حيث تم تحليل النصوص القانونية ذات الصلة، ومراجعة الإحصائيات والبيانات حول جرائم الابتزاز قبل وبعد تطبيق القانون.

توصلت الدراسة إلى أن المرسوم بقانون اتحادي رقم 34/2021 يضع إطاراً صارماً للعقوبات ويعزز من مستوى الحماية ضد الابتزاز الإلكتروني. كما أظهرت نتائج الدراسة ارتفاعاً في الوعي العام بمخاطر الجرائم الإلكترونية بعد تطبيق القانون، مما أدى إلى زيادة الإبلاغ عن هذه الجرائم.

https://scholar.google.com/scholar?as_ylo=2023&q=Legal+legislation+on+cyber+extortion&hl=ar&as_sdt=0.5#d=gs_qabs&t=1730421965398&u=%23p%3D5TBm2Xr0TIJ

¹⁵ Hussein, S., & Mohammed, S. (2024). Analysis of the legal framework and Implications of Federal Decree-Law No. 34/2021 on combating cyber extortion In the United Arab Emirates. The 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-6).

<https://colab.ws/articles/10.1109%2Ficcr61006.2024.10533025>

أوصت الدراسة بضرورة تعزيز جهود التوعية الأمنية للمستخدمين والشركات، وتقديم برامج تدريبية متخصصة في الأمن السيبراني. كما اقترحت أن تكون هناك سياسة واضحة للإعفاءات حال تقديم معلومات تستفيد منها التحقيقات المتعلقة بالابتزاز.

التعقيب على الدراسة:

تعتبر هذه الدراسة مهمة في سياق تعزيز الفهم القانوني والإجرائي لمكافحة الابتزاز الإلكتروني في دولة الإمارات. التركيز على إحصائيات الجرائم والتغيرات في السلوكيات بعد تطبيق القانون يسهم في تقديم صورة شاملة حول فعالية التشريع الجديد. ومع ذلك، فإن تعزيز التعاون بين الجهات الحكومية والمجتمع المدني في مجال التوعية والتثقيف يمكن أن يسهم بشكل أكبر في تقليل حالات الابتزاز.

○ ثانياً: الدراسات الأجنبية:

١- دراسة: (Syed Meharanjunisa, 2020)، بعنوان: المنظور العالمي: قانون الإنترنت واللوائح والامتثال.¹⁶ "Global Perspective: Cyberlaw, Regulations and Compliance"

هدفت الدراسة إلى توضيح أهمية الأمن السيبراني وكيفية حماية الشبكات والأنظمة المتصلة بالإنترنت من الهجمات السيبرانية، مع التركيز على الوعي بالقوانين واللوائح المتعلقة بالأمن السيبراني.

استخدمت الدراسة المنهج الوصفي التحليلي، حيث تم تحليل المعلومات المتعلقة بالأمن السيبراني، والجرائم السيبرانية، والإجراءات المتبعة من قبل المؤسسات والحكومات لتعزيز الأخلاقيات السيبرانية.

توصلت الدراسة إلى أن الأمن السيبراني هو عنصر أساسي في حماية المعلومات عبر الإنترنت، وأن هناك تدابير أمان ضرورية يجب اتباعها للحد من الجرائم السيبرانية والنشاطات غير القانونية.

أوصت الدراسة بزيادة الوعي حول الأمن السيبراني وتوفير التدريب اللازم للمستخدمين حول كيفية حماية معلوماتهم الشخصية والتقنية، بالإضافة إلى تعزيز التعاون بين الهيئات الحكومية والقطاع الخاص لتعزيز الأمن السيبراني.

التعقيب على الدراسة:

يمكن أن تعتبر هذه الدراسة خطوة مهمة نحو فهم أفضل لأسس الأمن السيبراني والجرائم الإلكترونية. من المهم أن تشمل المستقبل ممارسات وقائية أكثر فعالية وتحديثاً للتشريعات السارية لضمان أمان المعلومات والحفاظ على الحقوق الرقمية للأفراد. كما يجدر التنويه إلى ضرورة توفير المزيد من الموارد والمعلومات العامة حول الأمن السيبراني للجميع.

¹⁶ Syed Meharanjunisa "Global Perspective: Cyberlaw, Regulations and Compliance" Published in International Journal of Trend in Scientific Research Development and (Ijtsrd), ISSN: 2456-6470, Volume-4, | Issue-5, August 2020, pp.1-4.
www.ijtsrd.com/papers/ijtsrd30777.pdf

٢- دراسة: (Kalu, B. O. (2024). الاختصاص القضائي وتسليم المجرمين والمساعدة القانونية المتبادلة ضد الإرهاب الإلكتروني.¹⁷ Jurisdiction, extradition and "mutual legal assistance against cyber terrorism"

هدفت الدراسة إلى استكشاف مبادئ الاختصاص القضائي وتسليم المجرمين والمساعدة القانونية المتبادلة فيما يتعلق بالإرهاب الإلكتروني، مع التركيز على الحاجة إلى أطر قانونية دولية متماسكة. استخدمت الدراسة المنهج الوصفي التحليلي، حيث قامت بتحليل المبادئ التقليدية للاختصاص القضائي والخارجي والجنسية، بالإضافة إلى دراسة الآليات الناشئة مثل المساعدة القانونية المتبادلة.

توصلت الدراسة إلى أن غموض الاختصاص القضائي يشكل تحديًا كبيرًا في مواجهة الإرهاب الإلكتروني، مما يجعل من الضروري إنشاء اتفاقيات دولية موحدة لتعزيز التعاون القانوني والمساعدة بين الدول.

أوصت الدراسة بضرورة إنشاء اتفاقية متعددة الأطراف للقانون الجنائي لتوفير معايير موحدة للتعامل مع قضايا الإرهاب الإلكتروني، مما يساهم في تعزيز الردع القانوني والتماسك العالمي في مواجهة هذه التهديدات.

التعليق على الدراسة:

تبرز هذه الدراسة أهمية التعاون الدولي في مكافحة الإرهاب الإلكتروني، إذ تساهم في توضيح كيفية معالجة التحديات القانونية المشتركة وتحفز على تعزيز التنسيق بين الدول. من الضروري أن تؤخذ التوصيات المقترحة بعين الاعتبار لتحقيق نتائج فعالة في مواجهة هذه الجريمة العابرة للحدود.

٣- دراسة: (Khan, H. 2024). بعنوان: تجديد قوانين الجرائم الإلكترونية في باكستان: دراسة مشتركة بين المملكة المتحدة وباكستان.¹⁸ Revamping Cybercrime Laws "In Pakistan: A Co and United Kingdom International Journal of

هدفت الدراسة إلى تحليل قوانين الجرائم الإلكترونية في باكستان والمقارنة بينها وبين القوانين المعمول بها في المملكة المتحدة، مع التركيز على أوجه القصور في التشريعات والإجراءات المتعلقة بالأمن السيبراني في باكستان.

استخدمت الدراسة المنهج المقارن، حيث تمت مقارنة القوانين والإجراءات التنفيذية في كل من باكستان والمملكة المتحدة لفهم الفروق والقصور في التشريعات.

¹⁷ Kalu, B. O. (2024). Jurisdiction, extradition and mutual legal assistance against cyber terrorism. Calabar Law Journal, 20(2), 56-95.

<http://calabarlawjournal.com/index.php/CLJ/article/view/15>

¹⁸ Khan, H. (2024). Revamping cybercrime laws In Pakistan: A comparative analysis of Pakistan and United Kingdom. International Journal of Human and Society, 4(1), 1323-1335. https://scholar.google.com/scholar?start=20&q=Legal+legislation+on+cyber+extortion&hl=ar&as_sdt=0.5&as_ylo=2023#d=gs_qabs&t=1730427397731&u=%23p%3Dtg9ZrJzKrcJ

توصلت الدراسة إلى أن باكستان بحاجة إلى تحسين كبير في قوانينها المتعلقة بالجرائم الإلكترونية وآليات إنفاذها، حيث تواجه البلاد العديد من التحديات بما في ذلك الهجمات الإلكترونية المتزايدة وضعف القوانين مقارنة بالنظام الموجود في المملكة المتحدة.

أوصت الدراسة بضرورة تحديث وتدوين قوانين الأمن السيبراني في باكستان، وتطبيق إجراءات تنفيذية فعالة للقضاء على الجرائم الإلكترونية، بالإضافة إلى تحسين التعاون بين الهيئات الحكومية والمجتمع المدني لتعزيز الوعي العام.

التعقيب على الدراسة:

تعتبر هذه الدراسة ذات أهمية كبيرة في مجال الأمن السيبراني، حيث تضيء على الفجوات في التشريعات الحالية وتأثيرها على الأمان الرقمي في باكستان. تشدد على أهمية التحديث السريع للقوانين لتواكب التطورات التكنولوجية، مما يسهم في حماية المستخدمين والبيانات. تقدم الدراسة مجموعة من الاقتراحات البناءة والتي يمكن أن تساعد في تعزيز الأمان السيبراني في باكستان، مما يجعلها مرجعاً مهماً لصانعي القرار والباحثين في هذا المجال.

• هيكل البحث:

تتناول مقدمة البحث مجموعة من العناصر الأساسية التي تساهم في توضيح الإطار العام للدراسة. حيث تبدأ بمشكلة البحث التي تُحدد القضية الرئيسية التي تسعى الباحثة إلى معالجتها، تليها أهداف البحث التي توضح الغايات التي تسعى الباحثة لتحقيقها من خلال دراسته. كما تُبرز أهمية البحث الحاجة إلى هذا النوع من الدراسات وما يمكن أن تضيفه من قيمة معرفية. ويتضمن البحث تساؤلات تبحث عن إجابات محددة، بالإضافة إلى فرضيات تهدف إلى اختبارها خلال الدراسة. يعتمد البحث على منهجية معينة وأدوات بحثية مختارة لجمع البيانات، مع تحديد المتغيرات التي سيتم قياسها. يُقدم نموذج البحث تصوراً عاماً عن الطريقة التي سيتم من خلالها تنظيم المعلومات والبيانات. كما تُحدد حدود البحث نطاق الدراسة وما يشمله أو يستثنيه، في حين تُعرّف مصطلحات البحث الرئيسية لتجنب أي لبس. ومن المهم أيضاً استعراض الدراسات السابقة التي تتعلق بالموضوع، حيث تسلط الضوء على ما تم إنجازه في هذا المجال. وأخيراً، يتضمن هيكل البحث تنظيم الفصول والمحتويات بطريقة تسهل على القارئ فهم المعلومات المقدمة.

المبحث الأول: الإطار النظري لمكافحة الجرائم المعلوماتية

المطلب الأول: مفهوم الجرائم المعلوماتية: تعريف الجرائم المعلوماتية وأنواعها، والتركيز على الابتزاز الإلكتروني.

المطلب الثاني: الإطار القانوني لمكافحة الجرائم المعلوماتية في السعودية

المطلب الثالث: عرض القوانين والأنظمة ذات الصلة، مثل نظام مكافحة الجرائم المعلوماتية.

المطلب الرابع: دراسة الآليات القانونية المطبقة في مواجهة الجرائم المعلوماتية.

المطلب الخامس: دور الهيئات الحكومية: تحليل دور وزارة الداخلية والجهات القضائية والأمنية في مكافحة الابتزاز الإلكتروني.

المبحث الثاني: الأحكام القضائية المتعلقة بالابتزاز الإلكتروني

المطلب الأول: دراسة تحليلية للأحكام القضائية: استعراض وتشخيص أبرز الأحكام الصادرة عن المحاكم في قضايا الابتزاز الإلكتروني.

المطلب الثاني: المعايير القانونية المستخدمة في الحكم: تحليل المعايير التي تعتمد عليها المحاكم في إصدار الأحكام.

المطلب الثالث: تأثير الأحكام القضائية على المتضررين: كيف تؤثر هذه الأحكام على الأشخاص المتضررين وسلوك المجتمع.

المبحث الثالث: التحديات والفرص في مكافحة الجرائم المعلوماتية

المطلب الأول: التحديات القانونية: مناقشة القصور في التشريعات الحالية ومدى كفاءتها في مواجهة الجرائم المعلوماتية.

المطلب الثاني: التحديات الاجتماعية: تحليل العوامل الاجتماعية والثقافية التي تؤثر في ظاهرة الابتزاز الإلكتروني.

المطلب الثالث: الفرص لتحسين النظام القانوني: اقتراح طرق لتطوير التشريعات وتعزيز الجهود الحكومية.

المبحث الرابع: التوصيات

المطلب الأول: توصيات قانونية: تقديم اقتراحات لتحسين ومراجعة القوانين القائمة لمكافحة الجرائم المعلوماتية.

المطلب الثاني: توصيات توعوية: تفعيل برامج توعية المجتمع بخطر الابتزاز الإلكتروني ووسائل الحماية المتاحة.

المطلب الثالث: دور التعاون الدولي: أهمية التعاون مع الدول الأجنبية لمواجهة الجرائم المعلوماتية بشكل فعال.

الخاتمة:

المراجع: قائمة بالمصادر القانونية والأكاديمية والدراسات السابقة التي تم الاعتماد عليها في إعداد البحث.

• المصادر والمراجع:

- (1) نظام مكافحة جرائم المعلوماتية: شرح المادة 3 و6 من النظام. تم الإسترجاع من:
<https://etqanlawfirm-sa.com/%D9%86%D8%B8%D8%A7%D9%85-%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9-%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9/>
- (2) قضايا الابتزاز وعقوبتها في القانون السعودي. تم الإسترجاع من:
<https://naylawfirm.com/%D9%82%D8%B6%D8%A7%D9%8A%D8%A7-%D8%A7%D9%84%D8%A7%D8%A8%D8%AA%D8%B2%D8%A7%D8%B2-%D9%81%D9%8A-%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9/>
- (3) الهيئة الوطنية للأمن السيبراني. (2024). أنظمة وتشريعات البيانات والأمن السيبراني.
[/ https://nca.gov.sa/ar](https://nca.gov.sa/ar)
- (4) أحكام قضايا الابتزاز في القانون السعودي. <https://alqrnilaw.com/2024/05/04/blackmail-cases>
- (5) الفرق بين الجرائم المعلوماتية والجرائم الإلكترونية. تم الإسترجاع من:
<https://jolighm.com/%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9/>
- (6) السويدي، ش. م، & نوفل، د. ز. م. (2023). أسباب الابتزاز الإلكتروني والآثار النفسية والاجتماعية المرتبطة به (دراسة نوعية). مجلة الأدب، 146. <https://doi.org/10.31973/aj.v1i146.4008>
- (7) المجتمع الرقمي. (2024). المنصة الوطنية الموحدة. <https://www.my.gov.sa/aboutksa>
- (8) مداح، أ. ف. (2004). سياسة الوقاية والمنع لحماية الشباب السعودي من الوقوع في الجريمة: دراسة تطبيقية من واقع هيئة الأمر بالمعروف والنهي عن المنكر، (رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العدالة الجنائية).
https://ncys.ksu.edu.sa/sites/ncys.ksu.edu.sa/files/Crime%2016_5.pdf
- (9) مجموعة الأنظمة السعودية. (2024). "أنظمة المواصلات والاتصالات: نظام مكافحة جرائم المعلوماتية".
<https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/>

- 10) عبد العزيز، د. (2018). المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي: دراسة مقارنة. *مجلة جيل الأبحاث القانونية المعمقة*، 25، 27. <https://jilrc.com/archives/9216>
- 11) الغديان، س. ب. ع، خطاطبه، ي. ب. م. النعيمي، و عوادم، ع. ع. (2018). صور جرائم الابتزاز الإلكتروني ودوافعها والآثار النفسية المترتبة عليها من وجهة نظر المعلمين ورجال الهيئة والمستشارين النفسيين. *مجلة البحوث الأمنية*، 27(69)، 157-227.
- 12) حمدي، غاده محمد عبدالله، طوهرى، مريم صديق عمر، & عوض الكريم. (2020). الحماية القانونية من جريمة الابتزاز تحت ظل النظام السعودي. المجلة الالكترونية الشاملة متعددة المعرفة لنشر الابحاث العلمية و التربوية. <https://www.mecsjs.com> <https://search.mandumah.com/Record/878075>
- 13) Naggi, I. M. A. (2024). Legislative regulation of both crimes of threat and Informational blackmail – Analytical fundamental study of Saudi informational crimes law. Journal of Law and Sustainable Development, 12(3), 01-22. <https://doi.org/10.55908/sdgs.v12i3.3447>
- 14) Elfaouri, O. T. A, 2024. Cyber extortion Is a crime under the Jordanian Cybercrime Law No. 17 of 2023. Pakistan Journal of Criminology, 16(3). https://scholar.google.com/scholar?as_ylo=2023&q=Legal+legislation+on+cyber+extortion&hl=ar&as_sdt=0,5#d=gs_qabs&t=1730421965398&u=%23p%3D5TB_Ym2Xr0TIJ
- 15) Hussein, S., & Mohammed, S. (2024). Analysis of the legal framework and Implications of Federal Decree-Law No. 34/2021 on combating cyber extortion In the United Arab Emirates. The 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-6). <https://colab.ws/articles/10.1109%2Ficcr61006.2024.10533025>
- 16) Syed Meharanjunisa "Global Perspective: Cyberlaw, Regulations and Compliance" Published In International Journal of Trend in Scientific Research Development and (Ijtsrd), ISSN: 2456-6470, Volume-4 |, Issue-5, August 2020, pp.1-4. www.ijtsrd.com/papers/ijtsrd30777.pdf
- 17) Kalu, B. O. (2024). Jurisdiction, extradition and mutual legal assistance against cyber terrorism. Calabar Law Journal, 20(2), 56-95. <http://calabarlawjournal.com/Index.php/CLJ/article/view/15>
- 18) Khan, H. (2024). Revamping cybercrime laws In Pakistan: A comparative analysis of Pakistan and United Kingdom. International Journal of Human and Society, 4(1), 1323-1335. https://scholar.google.com/scholar?start=20&q=Legal+legislation+on+cyber+extortion&hl=ar&as_sdt=0,5&as_ylo=2023#d=gs_qabs&t=1730427397731&u=%23p%3Dtgc9ZrJzKrcJ