دور السياسات الرقمية الجامعية في التصدي لجرائم الابتزاز الإلكتروني بين الطلبة: دراسة تحليلية لأحدث لوائح الجامعات في الشرق الأوسط.

أ.د. فاطمة رحيم الموسوي

F.iq777@yahoo.com

م.م. نرجس عودة رشك

Narcissusodaa@uomisan.edu.iq

ملخص :

في السنوات الأخيرة، خطت الجامعات العراقية خطواتٍ سريعة نحو الرقمنة من خلال تطبيق أنظمة إدارة التعلم الإلكتروني والاتصالات عبر منصات رقمية متنوعة. وقد أثار هذا بالتالي العديد من التحديات الأمنية التي يمكن أن تُشكل تهديدًا لخصوصية وسلامة الطلاب، والتي تشمل بشكل رئيسي جرائم الابتزاز الإلكتروني. وتشمل هذه الجرائم عددًا كبيرًا من الطلاب المستهدفين بشكل رئيسي عبر وسائل التواصل الاجتماعي والبريد الإلكتروني الجامعي والمنصات الإلكترونية التي تستخدمها المؤسسات التعليمية. تهدف هذه الورقة إلى دراسة السياسات الرقمية المطبقة في الجامعات العراقية، بالإضافة إلى دورها في الحد من هذه الظاهرة. وستجري عملية تفتيش بناءً على الوثائق الرسمية واللوائح المنشورة على مواقع الجامعات الإلكترونية، مثل مواقع جامعة ميسان ، وجامعة المستنصرية، وجامعة البصرة، وغيرها من الجامعات الخاصة والعامة. كما تتبع عملية فحص مدى تضمين مفاهيم السلامة الرقمية والخصوصية وطرق الإبلاغ والتدابير العقابية المرتبطة بالابتزاز الإلكتروني في هذه السياسات. تحاول الدراسة إظهار مدى وضوح وتكامل سياسات الجامعات في مكافحة هذا النوع من الجرائم الرقمية، خاصةً في ظل غياب قانون عام على مستوى الوزارة أو الحكومة. كما تهدف إلى تسليط الضوء على المشاكل التي تعيق نجاح هذه السياسات، مثل ضعف الوعي الرقمي لدى الطلاب أو عدم وجود وحدات أمن سيبراني في الحرم الجامعي. تُظهر النتائج الأولية قصورًا كبيرًا في وضع وتحديث السياسات الرقمية في معظم الجامعات العراقية، حيث تفتقر العديد من القواعد إلى أجزاء واضحة تتعلق بالابتزاز الإلكتروني أو سبل منعه. كما أن بعض السياسات تكتفي بذكر "الانضباط الجامعي" بشكل عام، ولا تتعلق مباشرةً بالجرائم الرقمية الجديدة. بناءً على هذه النتائج، توصي الدراسة، من بين أمور أخرى، بأن تُطلق وزارة التعليم العالي والبحث العلمي إطارًا سياسيًا موحدًا للأمن السيبراني في الجامعات، يتضمن قنوات إبلاغ واضحة، وحماية قانونية للضحايا، وإجراءات صارمة ضد المبتزين. كما يشدد البحث على

أهمية تحديث المناهج الرقمية وتضمين مفاهيم الوعي السيبراني ضمن برامج التثقيف الطلابي، كخطوة وقائية على المدى البعيد.

الكلمات المفتاحية : الابتزاز الإلكتروني،السياسات الرقمية،الأمن السيبراني الجامعي، الجامعات العراقية،الخصوصية الرقمية،التحول الرقمي في التعليم، الجرائم الإلكترونية ضد الطلبة

١.١مقدمة

شهدت السنوات الأخيرة تحوّلًا جذريًا وشاملًا في البنية التحتية للجامعات في منطقة الشرق الأوسط، ولا سيما في العراق، وذلك نتيجة للتطورات المتسارعة في مجال الرقمنة وتبني الجامعات لأنظمة التعلم الإلكتروني، إلى جانب اعتمادها المتزايد على وسائل التواصل الحديثة والمنصات الرقمية الرسمية للتفاعل الأكاديمي والإداري على حد سواء. وقد أدّى هذا التوجه إلى خلق بيئة تعليمية أكثر انفتاحًا ومرونة، حيث أصبح بإمكان الطلبة وأعضاء هيئة التدريس الوصول إلى مصادر المعرفة والخدمات الجامعية من أي مكان وفي أي وقت، مما ساهم في تعزيز جودة التعليم وتوسيع نطاق المشاركة الأكاديمية. غير أن هذه التحولات الرقمية، وعلى الرغم من فوائدها الكبيرة، قد أفرزت تحديات جديدة ومعقدة، لا سيما في مجال الأمن السيبراني وحماية الخصوصية الرقمية. ومن بين أبرز هذه التحديات ظاهرة الابتزاز الإلكتروني، التي أصبحت تشكّل تهديدًا متزايدًا لسلامة الطلبة النفسية والاجتماعية، حيث تُمارس غالبًا من خلال وسائل التواصل الاجتماعي أو البريد الإلكتروني أو حتى عبر المنصات الرسمية التي توفرها الجامعات، مستغلّة الثغرات الأمنية أو قلة الوعي الرقمي لدى الطلبة. وتفرض هذه الظاهرة على الجامعات ضرورة تطوير سياسات رقمية واضحة وشاملة تهدف إلى التصدي لهذه الجرائم، وضمان بيئة تعليمية آمنة ومستقرة تحمي الطلبة من المخاطر الإلكترونية المتنامية

وفي هذا السياق، بات من الضروري أن تضطلع الجامعات بدور محوري في تبني استراتيجيات وقائية واستباقية، تهدف إلى مواجهة جرائم الابتزاز الإلكتروني بكل أشكالها، سواء تلك التي تستهدف الأفراد بشكل مباشر أو تلك التي تُستخدم كوسيلة لإضعاف الثقة بالمؤسسات الأكاديمية. ويشمل ذلك صياغة لوائح وقوانين رقمية داخلية تُراعي الخصوصية الثقافية والاجتماعية للمجتمع الجامعي في الشرق الأوسط، وتضمن في الوقت نفسه التماشي مع المعايير الدولية للأمن السيبراني. كما يتعيّن على الجامعات العمل على تعزيز الوعي الرقمي بين الطلبة والهيئات التدريسية من خلال تنظيم ورش تدريبية ودورات توعوية متخصصة، تُعرّفهم بكيفية التعامل مع التهديدات الإلكترونية، وتُنمّي مهاراتهم في التفاعل الآمن عبر الفضاء الرقمي. ولا يقلّ أهمية عن ذلك ضرورة توفير قنوات واضحة وسرّية للإبلاغ عن حالات الابتزاز أو الانتهاك الرقمي، بما يضمن التعامل مع هذه القضايا بحساسية وسرعة وفعالية، ويحافظ في الوقت ذاته على كرامة الضحية وخصوصيتها. إنّ بناء بيئة جامعية رقمية آمنة لا يُعدّ

ترفًا أو خيارًا، بل هو شرط أساسي لضمان استمرارية العملية التعليمية وتحقيق العدالة الرقمية لجميع المنتسبين إلى المؤسسة الجامعية.

1.2 مشكلة الدراسة

مع تزايد الاعتماد على المنصات الرقمية من قبل الطلبة في المؤسسات التعليمية، سواء لأغراض دراسية أو تواصلية أو إدارية، برزت على السطح ظاهرة مقلقة تتعلق بالابتزاز الإلكتروني، والتي أصبحت تتخذ أشكالًا متعددة ومتطورة، من بينها التهديد بنشر صور أو مقاطع فيديو أو رسائل ذات طابع شخصي أو حساس، أو استخدام المعلومات الشخصية التي يتم الحصول عليها عبر اختراق الحسابات أو التنصت على المراسلات، كوسيلة للضغط النفسي أو تحقيق مكاسب غير مشروعة. وتؤدي هذه الممارسات إلى آثار سلبية جسيمة على الضحايا، لا تقتصر فقط على تدهور حالتهم النفسية والشعور بالخوف والقلق والعزلة الاجتماعية، بل تمتد لتشمل انخفاض مستوى التحصيل العلمي، وتراجع المشاركة الأكاديمية، بل وفي بعض الحالات الانقطاع عن الدراسة أو التحول إلى العزلة الرقمية. ورغم خطورة هذه الظاهرة المتفاقمة، إلا أن معظم الجامعات في منطقة الشرق الأوسط، وخصوصًا في الدول التي تمر بتحولات رقمية متسارعة كالعراق، لا تزال تفتقر إلى سياسات رقمية واضحة، شاملة، ومحدثة تعالج هذا النوع من الجرائم الإلكترونية بشكل مباشر. وفي كثير من الأحيان، تتعامل الإدارات الجامعية مع حالات الابتزاز بأسلوب فردي أو ارتجالي، مما يؤدي إلى نتائج محدودة وغير كافية، ويُسهم في تفاقم المشكلة بدلاً من احتوائها. كما يُلاحظ غياب إطار تنظيمي موحّد أو تشريعات مركزية صادرة عن وزارات التعليم العالي أو الجهات الرقابية المعنية، ما يخلق فجوة قانونية وتنظيمية تعيق الاستجابة الفاعلة والمنسقة لهذه الظاهرة. وفي ظل هذا الواقع، تبدو الحاجة ماسّة إلى تطوير منظومات حماية رقمية متكاملة، تُبنى على التعاون بين الجهات الجامعية، والمؤسسات الحكومية، وخبراء الأمن السيبراني، ومؤسسات المجتمع المدني، لضمان بيئة أكاديمية رقمية آمنة وعادلة

١.٣ أهمية الدراسة

تكمن الأهمية العلمية والعملية لهذا البحث في تسليطه الضوء على ثغرة قانونية وإدارية حساسة ومهملة إلى حد كبير في البيئة التعليمية المعاصرة، ألا وهي ضعف أو غياب السياسات الرقمية الواضحة لمكافحة جرائم الابتزاز الإلكتروني داخل الجامعات. ففي ظل الوتيرة المتسارعة للتحول الرقمي، واعتماد الجامعات بشكل شبه كلي على المنصات الإلكترونية في تقديم خدماتها الأكاديمية والإدارية، أصبحت الحاجة إلى تنظيم هذا الفضاء الرقمي مسألة لا تحتمل التأجيل، خاصة مع تصاعد حالات الابتزاز الإلكتروني التي باتت تهدد أمن الطلبة وسلامتهم النفسية، وتؤثر بشكل مباشر في جودة العملية التعليمية واستقرارها. ومن هنا، تنبع أهمية هذا البحث في كونه يسعى إلى دراسة وتحليل السياسات الرقمية الحالية المعتمدة في عدد من الجامعات في الشرق الأوسط، مع التركيز على مدى

فعاليتها وشموليتها واستجابتها للمتغيرات الرقمية المعاصرة. كما يهدف البحث إلى الكشف عن مواطن الضعف في هذه السياسات، وتقديم توصيات قائمة على أسس تحليلية وعلمية قابلة للتطبيق، تُسهم في بناء منظومة رقمية أكثر أمنًا وفاعلية. ولا تقتصر أهمية الدراسة على الجانب الأكاديمي فقط، بل تتعداها إلى البُعد المجتمعي، إذ تسهم نتائجها في تعزيز ثقة الطلبة وأولياء الأمور بالمؤسسات التعليمية، وتدعم توجه الجامعات نحو التحول الرقمي الآمن، القائم على أسس الحوكمة الرقمية الرشيدة. كما تمثل هذه الدراسة مرجعًا مهمًا لصنّاع القرار في وزارات التعليم العالي، وصنّاع السياسات، ومطوري اللوائح الجامعية، لتبنّي سياسات رقمية أكثر استباقية وعدالة، تستوعب تحديات العصر الرقمي ومتطلباته المتسارعة.

1.4 أهداف الدراسة

٢ تحليل اللوائح الرقمية الحالية في عدد من الجامعات العراقية والعربية.
٣ تقييم مدى شمول هذه السياسات لمفاهيم الأمان الرقمي، والخصوصية، وآليات الإبلاغ عن الابتزاز.
٤ الكشف عن أوجه القصور والفراغات القانونية والتنظيمية في السياسات الرقمية الجامعية.
٥ اقتراح توصيات عملية لتحسين أداء السياسات الرقمية في مكافحة الابتزاز الإلكتروني.

١.٥ منهجية الدراسة

تعتمد هذه الدراسة في إطارها المنهجي على مزيج من التحليل الوثائقي والتحليل النوعي، بوصفهما أداتين مناسبتين لفهم السياقات التنظيمية والسياساتية المعقدة المرتبطة بإدارة الفضاء الرقمي داخل المؤسسات الجامعية. ويُقصد بالتحليل الوثائقي هنا مراجعة دقيقة ومنهجية للسياسات واللوائح الرسمية المتعلقة باستخدام المنصات الرقمية، والأمن السيبراني، وحماية خصوصية الطلبة، والتي تم نشرها على المواقع الإلكترونية لعدد من الجامعات المختارة ضمن العينة البحثية. وتشمل العينة كلًّا من جامعة ميسان، والجامعة المستنصرية، وجامعة البصرة، فضلًا عن جامعات حكومية وخاصة أخرى، تم اختيارها بناءً على معايير التنوّع الجغرافي، وتفاوت حجم المؤسسة، ونوعية الخدمات الرقمية المتوفرة لديها. ويهدف هذا التنوّع إلى بناء صورة شاملة وواقعية عن واقع السياسات الرقمية الجامعية في العراق والمنطقة. أما من الناحية التحليلية، فتقوم الدراسة بإجراء تحليل محتوى دقيق لتلك الوثائق، من أجل الكشف عن مدى تضمينها لعناصر الأمان الرقمي الأساسية، مثل آليات حماية البيانات، والتعامل مع الشكاوى الرقمية، وخطط الاستجابة لحالات الابتزاز الإلكتروني، والبروتوكولات الخاصة بالإبلاغ والدعم النفسي والقانوني. ويُستخدم هذا التحليل كأساس للمقارنة مع الممارسات الدولية الفضلى المعتمدة في عدد من الجامعات العالمية الرائدة التي وضعت نماذج متقدمة في مجال الحوكمة الرقمية الجامعية، وذلك بهدف تحديد الفجوات والثغرات، وكذلك النقاط

المضيئة التي يمكن البناء عليها. وبذلك، تُسهم هذه المنهجية في تقديم تحليل نقدي قائم على الأدلة، يدعم استنتاجات البحث وتوصياته العملية الرامية إلى تطوير السياسات الرقمية داخل الجامعات في المنطقة.

6.1حدود الدراسة

تُركّز هذه الدراسة بشكل رئيسي على تحليل السياسات الرقمية المعتمدة في الجامعات العراقية، نظرًا لما تشهده هذه المؤسسات من تحوّلات متسارعة في مجال التحول الرقمي، وما تواجهه من تحديات متزايدة تتعلق بالأمن السيبراني وجرائم الابتزاز الإلكتروني بين الطلبة. وتركز الدراسة على رصد وتحليل مضمون الوثائق الرسمية المتاحة على المواقع الإلكترونية لتلك الجامعات، بما في ذلك اللوائح التنظيمية، السياسات الداخلية، والتوجيهات العامة المتعلقة بالاستخدام الرقمي، دون التطرق إلى العمل الميداني أو إجراء مقابلات واستطلاعات رأي، وهو ما يحدد نطاق الدراسة ويجعل نتائجها مرهونة بما هو منشور ومتوفّر إلكترونيًا فقط. كما تتوسّع الدراسة في إطلالتها التحليلية لتشمل عينة محدودة من السياسات الرقمية المعتمدة في جامعات عربية مختارة في الشرق الأوسط، بهدف توفير سياق مقارن يساعد على إبراز أوجه القصور أو التميّز في الحالة العراقية، ويمهّد لتقديم توصيات مستندة إلى نماذج ناجحة قابلة للتكييف مع السياق المحلي.

الفصل الثاني: الإطار النظري

٢.١ مفهوم السياسات الرقمية الجامعية

تشير السياسات الرقمية الجامعية إلى مجموعة القوانين والإرشادات التنظيمية التي تضعها المؤسسات التعليمية بهدف تنظيم استخدام التكنولوجيا الرقمية داخل البيئة الجامعية. وتتضمن هذه السياسات مجموعة متنوعة من البنود التي تغطي نطاقًا واسعًا من الأنشطة والممارسات الرقمية، مثل ضوابط استخدام البريد الإلكتروني الجامعي، والسلوكيات المسموح بها عند استخدام منصات التعلم الإلكتروني، إضافة إلى قواعد حماية الخصوصية الرقمية للطلبة وأعضاء هيئة التدريس، ومعايير التعامل مع البيانات الشخصية، وآليات رصد ومواجهة السلوكيات الرقمية الضارة أو المسيئة، كحالات التنمّر الإلكتروني، أو التحرش، أو الابتزاز، أو انتهاك الخصوصية عبر الوسائط الرقمية (Kift, 2017). وتُعد هذه السياسات بمثابة إطار تشريعي وإداري مرجعي يهدف إلى تحقيق التوازن بين الاستفادة من الفرص التعليمية التي توفرها التكنولوجيا الحديثة، وبين الحد من المخاطر المصاحبة لاستخدامها، من خلال ضبط العلاقة بين المستخدمين والمنصات الرقمية المختلفة داخل المؤسسة الجامعية.

وتهدف هذه السياسات، في جوهرها، إلى حماية الطلبة والعاملين من أي تهديدات رقمية محتملة، وضمان وجود بيئة تعليمية رقمية آمنة وعادلة وشاملة، تُعزّز من فاعلية العملية التعليمية، وتُكرّس مبادئ النزاهة الأكاديمية، وتحترم

حقوق الأفراد الرقمية. كما تسهم في توعية جميع أفراد المجتمع الجامعي بمسؤولياتهم الرقمية، وتعزّز من قدرتهم على التفاعل الآمن والمسؤول داخل الفضاءات الإلكترونية الجامعية. وفي ظل تزايد الاعتماد على التكنولوجيا في التعليم العالي، أصبحت هذه السياسات ضرورة ملحّة، وليست مجرد خيار تنظيمي، مما يفرض على الجامعات تطويرها باستمرار لمواكبة التحديات والمستجدات الرقمية المتلاحقة.

٢.٢ الابتزاز الإلكتروني: المفهوم والأبعاد

الابتزاز الإلكتروني هو شكل متطور وخطير من أشكال الجرائم الإلكترونية، يُمارَس فيه الضغط على الضحية من خلال التهديد بنشر أو استغلال معلومات أو محتويات خاصة أو حساسة – مثل الصور الشخصية، المحادثات الخاصة، أو البيانات السرية – بهدف إجبارها على تقديم تنازلات معينة، سواء كانت مادية أو معنوية أو عاطفية (Ogilvie, 2020). ويُعد هذا النوع من الابتزاز واحدًا من أكثر الجرائم الرقمية انتشارًا وتعقيدًا في العصر الحديث، نظرًا لما توفره التكنولوجيا من أدوات سريعة وفعالة لتبادل المعلومات، مع ما يصاحب ذلك من إمكانات عالية للإخفاء والتمويه والتلاعب بالهوية.

ويتخذ الابتزاز الإلكتروني أشكالًا متعددة، قد تبدأ بابتزاز عاطفي يستغل مشاعر الضحية أو علاقتها بالمبتز، وقد يتطور ليشمل مطالب مالية مباشرة تحت التهديد، أو حتى ابتزاز شخصي يهدف إلى تحقير السمعة، أو إجبار الضحية على تنفيذ سلوكيات لا ترغب بها. وغالبًا ما تتم هذه الممارسات عبر وسائط التواصل الاجتماعي مثل فيسبوك، إنستغرام، وتلغرام، أو من خلال البريد الإلكتروني، أو حتى عبر تطبيقات التراسل الخاصة، مستغلّة الثغرات الأمنية في حسابات المستخدمين أو ضعف الوعي الرقمي لدى الأفراد. وتكمن خطورة الابتزاز الإلكتروني في آثاره النفسية والاجتماعية العميقة، حيث يؤدي إلى شعور الضحية بالخوف، والقلق، والعار، ما قد يدفعها للعزلة أو التردد في طلب المساعدة، بل وفي بعض الحالات قد يؤدي إلى نتائج كارثية على الصعيد النفسي والسلوكي. وفي السياق الجامعي، تصبح هذه الظاهرة أكثر حساسية وتعقيدًا، خصوصًا عندما يتم استهداف طلبة صغار السن أو أفراد لا يمتلكون الخبرة الكافية في التعامل مع التهديدات الرقمية، الأمر الذي يبرز الحاجة الماسة إلى تدخل مؤسسات التعليم العالي من خلال تبني سياسات واضحة للتوعية، والحماية، والإبلاغ، ضمن إطار قانوني وأخلاقي فعّال يضمن التصدي لهذه الجريمة بشكل ممنهج ومستدام.

٢.٣. البيئة الجامعية الرقمية والتحديات السيبرانية

مع التوسع المستمر في الاعتماد على الفضاء الرقمي داخل الجامعات، سواء في مجالات التعليم، والإدارة، والتواصل، والخدمات الطلابية، أصبحت هذه المؤسسات عرضة لمجموعة متزايدة من التهديدات والمخاطر السيبرانية، خاصة في ظل غياب أو ضعف الاستراتيجيات الأمنية الفعالة والمتكاملة التي تراعي طبيعة البيئة

التعليمية وخصوصياتها (Alshamrani et al., 2021). ومع أن التحول الرقمي قد سهّل الوصول إلى الموارد الأكاديمية ورفع من كفاءة الأداء الإداري والتربوي، إلا أنه في الوقت نفسه كشف عن هشاشة العديد من الأنظمة والبنى التحتية الإلكترونية التي لم تُصمم في الأصل للتعامل مع التهديدات السيبرانية المتقدمة أو مع الجرائم الرقمية المستحدثة. وتبرز من بين التحديات الأبرز التي تواجهها الجامعات ضعف البنية التحتية السيبرانية، التي تشمل غياب أنظمة الحماية المتقدمة، وعدم وجود برمجيات فعّالة لرصد التهديدات والهجمات الرقمية، فضلاً عن الاعتماد على منصات رقمية قد لا توفر مستويات أمان كافية لحماية بيانات الطلبة والعاملين. كما يشكّل انخفاض مستوى الوعي الرقمي لدى شريحة كبيرة من الطلبة – وأحيانًا بين أعضاء الهيئة التدريسية – عاملًا مساهمًا في زيادة الثغرات الأمنية، حيث يؤدي ذلك إلى ممارسات غير آمنة، مثل مشاركة كلمات المرور، أو النقر على روابط مشبوهة، أو استخدام شبكات غير موثوقة.

ولا يقلّ أهمية عن ذلك غياب الوحدات أو الفرق المتخصصة داخل الحرم الجامعي، والتي يمكن أن تتولى مسؤولية إدارة الأمن السيبراني، والاستجابة السريعة للحوادث الرقمية، وتقديم الدعم الفني والقانوني والنفسي في حال وقوع هجمات رقمية أو حالات ابتزاز. فغياب هذه الهياكل المؤسسية يجعل من الصعب على الجامعات وضع آليات واضحة للتعامل مع الانتهاكات الرقمية، ما يترك الطلبة عرضة للتهديدات دون حماية مؤسسية كافية. وعليه، فإن الحاجة إلى تطوير استراتيجيات أمنية رقمية متكاملة وشاملة، تُبنى على أسس علمية وتُنفذ ضمن إطار تنظيمي مستدام، لم تعد ترفًا بل ضرورة ملحّة لضمان استمرارية العملية التعليمية، وحماية مجتمع الجامعة من المخاطر الرقمية.

م٢.٥ نظريات داعمة للبحث

٢.٥.١ نظرية الحوكمة المؤسسية (Institutional Governance Theory)

تُشير هذه النظرية إلى أن فعالية المؤسسات، لا سيما في البيئات التنظيمية المعقدة، ترتبط ارتباطًا وثيقًا بمدى وضوح وتكامل السياسات الداخلية التي تحكم أداءها (Peters, 2010). وتُعد هذه النظرية من الأدوات النظرية الجوهرية في فهم كيفية عمل المؤسسات وتفاعلها مع المتغيرات الخارجية، وخصوصًا في السياقات الرقمية المتسارعة التي تتطلب بنى تنظيمية مرنة وواضحة المعالم. ويؤكد Peters أن السياسات الفعالة ليست مجرد وثائق إدارية، بل هي انعكاس للهوية المؤسسية والرؤية المستقبلية، إذ تُمثّل الإطار الذي من خلاله تُترجم الأهداف إلى إجراءات، وتُبنى العلاقات بين الفاعلين، ويُدار التغيير بكفاءة. وفي البيئة الجامعية الرقمية، تزداد أهمية هذا الطرح النظري، حيث تواجه المؤسسات التعليمية تحديات متزايدة تتعلق بالتكنولوجيا، مثل الأمن السيبراني، الخصوصية، والابتزاز الإلكتروني. وهنا تصبح فعالية الجامعة مرهونة بمدى قدرتها على تطوير سياسات رقمية متكاملة وواضحة تُراعي خصوصية الفضاء الرقمي، وتضع معايير تنظيمية تحكم سلوكيات الطلبة والعاملين، وتحدّد طرق التدخل عند

حدوث خروقات رقمية. فالسياسات الغامضة أو المتفرقة تؤدي إلى تشتت المسؤوليات، وضعف التنسيق المؤسسي، وتخلق فراغًا تنظيميًا يمكن أن يُستغل من قبل المبتزين أو المتجاوزين. كما أن وضوح السياسات وتكاملها يعزز من ثقافة الامتثال الرقمي داخل المؤسسة، ويُسهِم في بناء الثقة بين أفرادها، حيث يعرف كل فرد ما له وما عليه، وما هي الإجراءات المتبعة لحماية حقوقه الرقمية. وعليه، فإن النظرية تبرُز كإطار مفاهيمي مناسب لتحليل واقع السياسات الرقمية في الجامعات، وتقييم مدى اتساقها الداخلي، واستجابتها للمخاطر المتولّدة عن الاستخدام المتزايد للتكنولوجيا في البيئة التعليمية.

٢.٥.٢ نظرية الحماية الدافعية (Protection Motivation Theory – PMT)

تُفسر نظرية الدافع للحماية (Protection Motivation Theory) التي طرحها Rogers عام ١٩٨٣ كيف يتفاعل الأفراد مع التهديدات، لا سيما في البيئات التي تتطلب وعيًا واستجابة فورية، مثل الفضاء الرقمي. وتركز هذه النظرية على العوامل النفسية والمعرفية التي تدفع الفرد إلى اتخاذ قرارات وقائية عند مواجهة خطر معين، سواء كان ذلك الخطر صحيًا، اجتماعيًا، أو رقميًا. وفقًا لـ Rogers، فإن الاستجابة الوقائية الفعالة لا تحدث تلقائيًا، بل تتطلب توافر عنصرين رئيسيين: الوعي الكافي بحجم التهديد، والإيمان بفعالية السلوك أو الاستراتيجية المقترحة للحماية منه.

وفي السياق الرقمي، تكتسب هذه النظرية أهمية خاصة في تفسير سلوك الطلبة داخل الجامعات عند تعرّضهم لتهديدات إلكترونية مثل الابتزاز أو اختراق الخصوصية. فالفرد لن يُقدِم على حماية نفسه من المخاطر الرقمية ما لم يكن مدركًا بشكل واضح لوجود التهديد، ومدى خطورته، واحتمالية وقوعه. كما أنه بحاجة إلى الشعور بوجود أدوات فعالة يمكن اللجوء إليها لتفادي هذا الخطر أو التعامل معه، مثل السياسات المؤسسية، وقنوات الإبلاغ، والدعم الفني أو القانوني. من هنا، تبرز أهمية وجود سياسات رقمية واضحة وشاملة داخل المؤسسات الجامعية، لأنها لا تُسهم فقط في خلق بيئة آمنة، بل تشكّل في حد ذاتها عنصرًا محفّزًا لسلوك الحماية، كما توضح النظرية. وتقترح النظرية كذلك أن الحماية لا تتحقق من خلال الوعي الفردي فقط، بل من خلال البنية التنظيمية التي تُعزز هذا الوعي وتدعمه بسياسات وإجراءات عملية. فكلما كانت السياسات الجامعية أكثر وضوحًا واتساقًا، زادت قدرة الأفراد على إدراك فاعليتها، وبالتالي، ازداد دافعهم لاتّباعها. في المقابل، غياب السياسات أو غموضها يُضعف من دافع الحماية، ويجعل الأفراد أكثر عُرضة للاستسلام أو التجاهل عند مواجهة التهديد. لذلك، يمكن اعتبار نظرية Rogers أداة تحليلية فعالة لفهم العلاقة بين الوعي بالتهديدات الرقمية وبين فعالية السياسات في تحفيز السلوك الوقائي لدى الطلبة والعاملين في الجامعة.).

٢.٥.٣ نظرية الأمان الرقمي (Digital Security Theory)

تُعد نظرية الاقتصاد الأمني (Security Economics Theory) التي قدّمها Anderson & Moore عام ٢٠٠٦ من النظريات الرائدة في تفسير كيفية بناء سياسات رقمية فعالة تُوازن بين تكلفة الحماية الرقمية والفوائد المترتبة على تطبيقها، مع التركيز بشكل خاص على حماية الخصوصية والبيانات الحساسة في المؤسسات، بما في ذلك المؤسسات التعليمية. وتنطلق هذه النظرية من مبدأ أن القرارات المتعلقة بالأمن السيبراني – مثل تصميم السياسات، وتحديد آليات الحماية، وتوزيع المسؤوليات – لا تتم بمعزل عن الاعتبارات الاقتصادية، بل هي خاضعة لتحليل التكلفة والعائد، سواء على مستوى الأفراد أو المؤسسات. وتؤكد النظرية أن السياسات الرقمية الناجحة هي تلك التي تُصمم بطريقة تضمن تحقيق أقصى درجات الحماية الممكنة مقابل أقل التكاليف، سواء كانت مادية أو بشرية أو تقنية. ففي بيئة مثل الجامعة، حيث تتنوع مستويات الوعي الرقمي وتتفاوت الموارد التقنية، يصبح من الضروري أن تكون السياسات الرقمية مرنة، وقابلة للتطبيق، وذات مردود فعلي على حماية خصوصية المستخدمين، لا سيما الطلبة الذين يُعدّون الفئة الأكثر عرضة للاستغلال الرقمي. وتشمل هذه الحماية: الحفاظ على سرية المعلومات الأكاديمية، وتأمين حسابات البريد الجامعي، وضمان حماية منصات التعلم الإلكتروني من الاختراق أو التالدقي ومن منظور هذه النظرية، فإن أحد أبرز التحديات في المؤسسات التعليمية هو غياب التقييم الاقتصادي الدقيق للقرارات الأمنية، حيث قد يُنظر إلى الأمن الرقمي على أنه عبء مالي أو إداري، وليس استثمارًا استراتيجيًا في استدامة العملية التعليمية. لكن Anderson & Moore يشددان على أن الفشل في حماية البيانات الحساسة قد يكلّف المؤسسات خسائر كبيرة، سواء من حيث السمعة أو الثقة العامة أو حتى الأثر القانوني. وعليه، فإن تصميم السياسات الرقمية لا ينبغي أن يكون عشوائيًا أو تقنيًا بحتًا، بل يجب أن يستند إلى تحليل اقتصادي يُراعي حجم المخاطر، ودرجة التعرض لها، وقيمة الأصول الرقمية المراد حمايتها. في السياق الجامعي، تدعو هذه النظرية إلى تبنّي نماذج حوكمة رقمية تضع حماية الخصوصية والأمن السيبراني ضمن أولويات التخطيط المؤسسي، وأن تُخصص الموارد البشرية والتقنية والمالية الكافية لتطوير سياسات رقمية محكمة. كما تشجع على دمج أصحاب المصلحة – من إداريين، وأكاديميين، وطلبة – في صياغة السياسات، لضمان ملاءمتها للسياق الواقعي، ورفع مستوى الالتزام بها. ومن خلال هذا المنظور، يمكن تقييم مدى نضج السياسات الرقمية في الجامعات، ليس فقط من حيث وجودها الشكلي، بل من حيث فعاليتها الاقتصادية والوظيفية.

٢.٦. دور السياسات الرقمية في الوقاية من الجرائم السيبرانية

تشير العديد من الدراسات الحديثة إلى أن وجود سياسات رقمية واضحة وشاملة داخل المؤسسات التعليمية يسهم بدرجة كبيرة في الحد من تعرض الطلبة لحوادث الابتزاز الإلكتروني، ويقلل من آثارها النفسية والاجتماعية والأكاديمية على الضحايا (Yousef & Aziz, 2020). وتؤكد هذه الدراسات أن فعالية السياسات لا تكمن فقط في وجودها الشكلي، بل في مدى تطبيقها العملي، واستجابتها للحاجات الواقعية لمجتمع الطلبة. إذ أن السياسات غير

المفصّلة، أو غير المفعّلة، لا تؤدي دورًا وقائيًا حقيقيًا، بل قد تعزز الشعور بعدم الأمان في الفضاء الرقمي الجامعي. ومن هذا المنطلق، حدد الباحثون أربعة عناصر مركزية تشكل جوهر السياسة الرقمية الفعالة في التصدي للابتزاز الإلكتروني:

١. توعية الطلبة:

تعد حملات التوعية الرقمية من أبرز الركائز التي تقوم عليها أي سياسة ناجحة، إذ أن رفع مستوى الوعي بين الطلبة حول طبيعة الابتزاز الإلكتروني، وأساليبه، ووسائل الوقاية منه، يُعتبر خط الدفاع الأول. تشمل هذه التوعية ورش العمل، الدورات التدريبية، الحملات الإلكترونية التفاعلية، ونشر المواد الإرشادية عبر منصات الجامعة الرسمية. كما ينبغي أن تستهدف هذه الحملات الفئات الأكثر عرضة، مثل الطلبة الجدد أو المستخدمين ذوي المهارات الرقمية المحدودة، لتزويدهم بالمعرفة والأدوات اللازمة لحماية أنفسهم.

٢. وضوح العقوبات:

تلعب العقوبات دورًا حاسمًا في ردع مرتكبي الابتزاز الرقمي، لكن تأثيرها الفعلي مرهون بمدى وضوحها وقابليتها للتنفيذ. يجب أن تتضمن السياسات الجامعية تعريفًا دقيقًا لسلوك الابتزاز الإلكتروني، مع تحديد العقوبات الإدارية والقانونية المترتبة عليه، سواء تعلق الأمر بطرد أكاديمي، أو إنذار رسمي، أو إحالة إلى الجهات القضائية المختصة. كما ينبغي تضمين هذه المعلومات في الأدلة الطلابية أو السياسات المنشورة، لضمان علم جميع الأطراف بها مسبقًا.

٣. تسهيل آليات الإبلاغ:

في الكثير من الحالات، يتردد الضحايا في التبليغ عن حوادث الابتزاز بسبب التعقيد الإجرائي، أو الخوف من الفضيحة، أو عدم وضوح القنوات المناسبة. لذلك، تُعد سهولة الإبلاغ من أهم مؤشرات السياسة الرقمية الناجحة. ويمكن تحقيق ذلك من خلال توفير منصات إلكترونية آمنة وسرية للإبلاغ، وتخصيص فرق مؤهلة للتعامل مع الشكاوى الرقمية بسرعة وكفاءة، وضمان سرية بيانات الضحية أثناء التحقيق.

٤. الحماية القانونية للضحايا:

لا يقتصر دور السياسة على المعاقبة، بل يجب أن تشمل أيضًا توفير الحماية للضحايا، سواء من خلال الدعم القانوني، أو المساندة النفسية، أو الحماية من أي انتقام محتمل. وتُعتبر هذه النقطة حاسمة في بناء ثقة الطلبة

بالمنظومة الرقمية، وتشجيعهم على اتخاذ خطوات استباقية في حال تعرضهم لأي تهديد. ينبغي أيضًا أن تتعاون الجامعات مع الجهات الأمنية والقضائية المختصة لتأمين حماية شاملة للطلبة المتضررين، وربطهم بالخدمات القانونية المناسبة عند الحاجة. إن توافر هذه العناصر مجتمعة، وتكاملها ضمن سياسة واحدة، يجعل من الممكن بناء بيئة رقمية جامعية آمنة، تُراعي خصوصية الطلبة، وتُحصّنهم ضد التهديدات الرقمية المتزايدة. كما أن هذه السياسات لا تقتصر فوائدها على الجانب الأمني فحسب، بل تعزز أيضًا من جودة الحياة الطلابية، وتسهم في بناء ثقافة رقمية قائمة على الوعي، والمسؤولية، والاحترام المتبادل.

3: المنهجية ((Methodology :

تهدف منهجية البحث الذي اتبعته الدراسة لتحقيق أهدافها، والإجابة عن أسئلتها البحثية. كما توضح الأدوات والإجراءات المستخدمة لجمع وتحليل البيانات الخاصة بالسياسات الرقمية الجامعية في الشرق الأوسط، وكيفية التعامل مع قضايا الابتزاز الإلكتروني في بيئات التعليم العالي. وتستهدف الدراسة بشكل خاص السياسات الرقمية في الجامعات العراقية، مع إجراء مقارنة مع بعض الجامعات العربية الأخرى. وتعتمد المنهجية على التحليل الوثائقي النوعي، وهو الأسلوب الأكثر ملاءمة للموضوع الذي يتطلب فحص الوثائق والسياسات الرسمية المنشورة من قبل الجامعات حول الاستخدام الآمن للتكنولوجيا وحماية الطلاب من الابتزاز الإلكتروني .

٣.٢٠ تصميم البحث

تم اعتماد تصميم البحث الوصفي التحليلي لهذا البحث، حيث يهدف إلى تقديم تفسير دقيق للسياسات الرقمية الجامعية المتبعة في الجامعات المعنية، وتحليل مدى فعاليتها في التصدي لجرائم الابتزاز الإلكتروني بين الطلاب. كما يهدف التصميم إلى تقديم مقارنة تحليلية بين السياسات الرقمية في الجامعات المختارة من خلال مراجعة الوثائق القانونية والتنظيمية المتاحة على المواقع الإلكترونية الرسمية. ويُعد هذا النوع من التصميم ملائمًا بشكل خاص نظرًا لأنه يسمح بجمع وتحليل بيانات مكتوبة، سواء كانت قوانين أو لوائح أو إرشادات جامعية.

٣.٣٠ منهج البحث

تتبنى هذه الدراسة المنهج التحليلي الوثائقي، حيث تم مراجعة وتحليل مجموعة من الوثائق الرسمية المنشورة على الإنترنت والتي تتعلق بالسياسات الرقمية في الجامعات العراقية وبعض الجامعات العربية الأخرى. يعتمد البحث على جمع البيانات من خلال المراجعة النقدية للمحتوى، حيث يتم تحليل النصوص الوثائقية لتحديد عناصر الأمن السيبراني المضمنة، وكذلك الكشف عن الثغرات المحتملة التي قد تؤدي إلى استغلال الطلاب أو تعرضهم لمخاطر الابتزاز الرقمي. ويرتكز منهج البحث على مفهوم "تحليل المحتوى" الذي يهدف إلى فحص وتحليل النصوص بهدف استخراج أنماط وعناصر معينة تتعلق بالأمن الرقمي وحماية الخصوصية.

٣.٤٠ مجتمع الدراسة وعينته

يشمل مجتمع الدراسة الجامعات العراقية الحكومية والخاصة، حيث تم اختيار عينة من الجامعات ذات السياسات الرقمية المتاحة علنًا على الإنترنت. تم اختيار هذه الجامعات بناءً على معايير مثل: **التوافر الإلكتروني للسياسات، حجم الجامعة، وتعدد البرامج الأكاديمية.** وتعد هذه الجامعات الأكثر تمثيلًا للواقع الجامعي في العراق.

تشمل العينة المختارة من الجامعات:

- **جامعة ميسان**
- **الجامعة المستنصرية**
- **جامعة البصرة**
- **جامعة بغداد**
- **جامعة الكوفة**
- **جامعة دهوك**
- **جامعة الزيتونة الأردنية** (كمثال للجامعات في المنطقة العربية)
- **جامعة الشارقة الإماراتية** (كمثال آخر للجامعات في الخليج العربي)
- **الجامعة اللبنانية** (كمثال للجامعات في لبنان)

وقد تم اختيار هذه الجامعات بناءً على توفر وثائق سياسات واضحة على مواقعها الإلكترونية المتعلقة بالأمن الرقمي وحماية البيانات. علاوة على ذلك، تم تحليل السياسات الرقمية المعلنة في هذه الجامعات مقارنة بالمعايير العالمية في مجال الأمن السيبراني وحماية البيانات.

٣.٥ أدوات جمع البيانات

تم الاعتماد على **جمع البيانات الثانوية** في هذه الدراسة، حيث تم جمع البيانات من خلال **مراجعة الوثائق الرسمية** المتاحة على المواقع الإلكترونية للجامعات المختارة. وتتضمن هذه الوثائق:

- **السياسات الرسمية لاستخدام البريد الإلكتروني الجامعي**
- **إرشادات الاستخدام الآمن للإنترنت**
- **لوائح حماية الخصوصية**
- **إجراءات التعامل مع الحوادث الرقمية مثل الابتزاز الإلكتروني**
- **تعليمات حول التبليغ عن السلوكيات الرقمية الضارة**
- **أدلة حول حقوق الطلاب في حال تعرضهم لابتزاز إلكتروني**

٣.٦ أداة التحليل

تم تطبيق **تحليل المحتوى** كأداة رئيسية لتحليل الوثائق، حيث تم استخلاص العناصر التالية:

١. **التعريفات الواضحة للابتزاز الإلكتروني:** حيث يتم البحث عن ما إذا كانت السياسات تحدد بوضوح الابتزاز الإلكتروني وأشكاله المختلفة.
٢. **آليات الحماية:** تحليل مدى توافر آليات الحماية التي توفرها السياسات، مثل الحماية القانونية والدعم النفسي للضحايا.
٣. **آليات الإبلاغ:** يتم دراسة مدى وضوح وسهولة آليات الإبلاغ عن الحوادث الرقمية.
٤. **العقوبات المفروضة على الجناة:** يتم تحليل الشروط الواردة بشأن العقوبات التي يتم فرضها على المتهمين في جرائم الابتزاز الإلكتروني.
٥. **التوعية الرقمية:** يتم تقييم مدى وجود برامج توعية وحملات إعلامية موجهة للطلاب حول الابتزاز الإلكتروني والمخاطر الرقمية الأخرى.
٦. **التعاون مع الجهات الخارجية:** البحث عن أية إشارات لتعاون الجامعات مع مؤسسات أخرى مثل الشرطة أو المحاكم لمعالجة قضايا الابتزاز الإلكتروني.

٣.٧ حدود البحث

- **حدود جغرافية:** تركز الدراسة على الجامعات في العراق، مع مقارنة سياسات بعض الجامعات العربية الأخرى مثل الأردن والإمارات ولبنان.
- **حدود زمنية:** تم الاعتماد على السياسات المنشورة خلال السنوات الأخيرة (٢٠٢٠-٢٠٢٤).
- **حدود منهجية:** تقتصر الدراسة على تحليل السياسات الرقمية المنشورة على الإنترنت فقط، ولا تشمل دراسات ميدانية مثل المقابلات أو الاستطلاعات.
- **حدود موضوعية:** تركز الدراسة بشكل رئيسي على تحليل سياسات الحماية من الابتزاز الإلكتروني ولا تشمل جميع جوانب الأمن الرقمي في الجامعات، مثل حماية البيانات الشخصية أو الأمن في الشبكات الجامعية.

٣.٨ الموثوقية والصدق

من أجل ضمان **الموثوقية والصدق** في جمع وتحليل البيانات، تم الالتزام بأسس المنهج العلمي في مراجعة الوثائق، واختيار الجامعات التي تتمتع بمصداقية في نشر سياساتها عبر الإنترنت. كما تم إجراء التحليل وفقًا لمعايير دقيقة تضمن تحليل العناصر المتشابهة في السياسات الجامعية، وتطبيق مقارنة موضوعية مع الممارسات العالمية المثلى. تمت الاستعانة بمصادر أكاديمية ودراسات سابقة لدعم التحليل وتحديد المعايير المناسبة للمقارنة.

٣.٩ تحليل النتائج Results Analysis

٣.٩.١ أداة التحليل وتحديد المؤشرات

تم تحديد **خمسة مؤشرات أساسية** تم استخدامها لتحليل كل وثيقة سياسة رقمية:

تم ترميز الاستجابات بـ:

- (١): متوفر بشكل واضح
- (٠): غير متوفر أو غير مذكور

جدول (١) المؤشرات الرئيسية لتحليل كل وثيقة سياسة رقمية

الوصف	المؤشر	الرمز
هل ورد تعريف دقيق في الوثيقة	وجود تعريف واضح	M1
هل تم توضيح وسائل إلابلاغ (نموذج، بريد، منصة)	آليات إلابلاغ	M2
هل تتضمن الوثيقة حملات او إرشادات توعوية	التوعية الرقمية	M3
هل هناك تفصيل للعقوبات المترتبة على المبتز؟	العقوبات	M4
هل يتم الإشارة للحماية القانونية للضحية ؟	الحماية القانونية للضحايا	M5

تشير نتائج الجدول إلى أن الوثائق المدروسة تتفاوت في مدى شموليتها ووضوحها فيما يتعلق بمواجهة جرائم الابتزاز الإلكتروني في الجامعات· فقد أظهرت المؤشرات أن بعض الوثائق تتضمن تعريفاً دقيقاً وواضحاً للابتزاز الإلكتروني (M1)، بينما تفتقر أخرى إلى ذلك، ما قد يؤثر في فهم الطلبة لطبيعة الجريمة· أما آليات الإبلاغ (M2)، فتراوحت بين الإشارة إلى وسائل محددة كالنماذج والبريد والمنصات الإلكترونية، وبين غياب أي توضيح، مما قد يحد من فعالية التبليغ· وبالنسبة للتوعية الرقمية (M3)، فإن عدداً محدوداً من الوثائق أدرج حملات أو إرشادات، مما يبرز الحاجة إلى جهود مؤسساتية أكبر في هذا المجال· فيما يتعلق بالعقوبات (M4)، فقد كانت بعض الوثائق دقيقة في تفصيل العقوبات، وهو عنصر رادع مهم، بينما اكتفت أخرى بالإشارة العامة· وأخيراً، برز تفاوت واضح في تضمين الحماية القانونية للضحايا (M5)، حيث لم تشر بعض اللوائح بشكل مباشر إلى حقوق الضحية، مما يسلّط الضوء على ضرورة تطوير الأطر القانونية لضمان بيئة جامعية آمنة.

3.9.2· نتائج تحليل الجامعات العراقية

تم تحليل السياسات الرقمية لـ **٦ جامعات عراقية**. الجدول التالي يوضح مدى توفر المؤشرات:

جدول (٢) السياسات الرقمية للجامعات العراقية

الجامعة	M1	M2	M3	M4	M5	المجموع
جامعة بغداد	١	١	٠	١	٠	٣
جامعة البصرة	٠	٠	٠	١	٠	١
جامعة المستنصرية	٠	١	1	٠	٠	٢
جامعة ميسان	٠	٠	٠	٠	٠	٠
جامعة الكوفة	١	١	١	١	١	٥
جامعة دهوك	١	٠	٠	١	٠	٢

تشير نتائج الجدول إلى تفاوت كبير في مدى شمول السياسات الرقمية للجامعات العراقية للعناصر الخمسة المرتبطة بالتصدي لجرائم الابتزاز الإلكتروني. فقد تصدرت جامعة الكوفة التقييم بتحقيقها الحد الأقصى من المؤشرات (٥ من ٥)، مما يدل على وجود سياسة رقمية شاملة وواضحة تشمل التعريف، الإبلاغ، التوعية، العقوبات، والحماية القانونية. في المقابل، أظهرت جامعة ميسان غيابًا تامًا لأي من هذه العناصر، ما يعكس ضعفًا واضحًا في بنيتها التنظيمية الرقمية. كما سجلت جامعة بغداد نتيجة متوسطة (٣ من ٥) بينما تراوحت نتائج الجامعات الأخرى بين ١ و٢، وهو ما يُبرز وجود فجوة واضحة في وعي وأولوية الجامعات لمخاطر الابتزاز الإلكتروني، ويؤكد الحاجة إلى تطوير سياسات أكثر تكاملًا وتحديثًا لمواكبة التحديات الرقمية في البيئة التعليمية

٣.١٠ تحليل إحصائي وصفي

تعكس نتائج الجدول خللاً واضحًا في تركيبة السياسات الرقمية المعتمدة في الجامعات العراقية فيما يتعلق بالابتزاز الإلكتروني، حيث لم تتجاوز نسبة الجامعات التي تتضمن تعريفًا دقيقًا لهذه الجريمة ٥٠% فقط، مما يشير إلى غياب رؤية موحدة أو وعي قانوني واضح بمفهوم الابتزاز الإلكتروني في البيئة الجامعية. ويؤدي هذا الغياب إلى ضعف في الإجراءات الوقائية والتوعوية، ويترك الطلبة عرضة للاستغلال الرقمي دون وجود إطار مفاهيمي يحميهم أو يُفهمهم حقوقهم. وفيما يتعلق بآليات الإبلاغ (M2)، أظهرت النتائج نسبة مشابهة (٥٠%) من الجامعات التي توفر وسيلة واضحة للإبلاغ عن الابتزاز، وهو مؤشر يُظهر ضعف البنية المؤسسية للتعامل مع هذه الحالات. فغياب منظومات الإبلاغ الفعالة يحدّ من قدرة الضحايا على اتخاذ خطوات سريعة وآمنة لحماية أنفسهم، ما يُسهم في تفاقم الأثر النفسي والاجتماعي الناتج عن الجريمة.

أما عنصر التوعية الرقمية (M3)، فقد سُجّل في جامعتين فقط من أصل ست، بنسبة ٣٣%، وهو ما يعكس غيابًا شبه تام للمبادرات الوقائية والتثقيفية. هذا القصور في الجانب التوعوي يعزز الفجوة بين تطور التهديدات الرقمية وسلوك الطلبة، حيث إن التوعية تُعدّ خط الدفاع الأول في مواجهة الابتزاز الإلكتروني. رغم ذلك، فإن أغلب الجامعات (٦٧%) ذكرت العقوبات المترتبة على مرتكبي الابتزاز، ما يدل على تركيز السياسات على البُعد العقابي دون إيلاء الاهتمام الكافي للجوانب الوقائية والداعمة للضحايا. ويُلاحظ أن الحماية القانونية للضحايا (M5) تكاد تكون غائبة، إذ لم تُذكر سوى في جامعة واحدة فقط، بنسبة ١٧%، وهو ما يشير إلى ضعف الإطار القانوني والحقوقي الموجه لحماية الضحية، ما قد يُضعف ثقة الطلبة في التبليغ ويزيد من معاناتهم النفسية والاجتماعية.

٣.١٠.١ مقارنة مع الجامعات العربية الأخرى

تمت مقارنة النتائج مع **٣ جامعات عربية:**

الجامعة	M1	M2	M3	M4	M5	المجموع
جامعة الشارقة (الإمارات)	١	١	١	١	١	٥
جامعة الزيتونة (الأردن)	١	١	١	٠	١	٤
الجامعة اللبنانية	٠	١	١	١	٠	٣

تحليل مقارن

تكشف المقارنة بين الجامعات العراقية والعربية عن فجوة ملحوظة في مدى شمول السياسات الرقمية، خصوصًا فيما يتعلق بعنصري التوعية الرقمية والحماية القانونية للضحايا. ففي حين يظهر ضعف واضح في هذه الجوانب داخل الجامعات العراقية، تتميز الجامعات العربية – مثل جامعة الشارقة والجامعة الأردنية – بتضمين برامج توعية واضحة ضمن سياساتها، ما يشير إلى اهتمام أكبر بالجانب الوقائي والمعرفي في التعامل مع التهديدات الإلكترونية.
واحدة من أبرز النقاط اللافتة في النتائج هي أن الحماية القانونية للضحايا ((M5، والتي ظهرت بنسبة منخفضة جدًا في الجامعات العراقية (جامعة واحدة فقط من أصل ست)، كانت حاضرة في معظم الجامعات العربية، مما يدل على وعي قانوني متقدم لدى المؤسسات التعليمية العربية بضرورة توفير أطر داعمة للضحايا بدلًا من الاقتصار على العقوبات فقط. هذه السياسات تُسهم في تعزيز ثقة الطلبة وتشجيعهم على الإبلاغ دون خوف من العواقب أو الوصمة الاجتماعية.

جامعة الشارقة تصدرت نتائج الجدول بحصولها على أعلى درجة شمولية (٥ من ٥)، وهو مؤشر قوي على اعتمادها سياسات رقمية ناضجة ومتكاملة تستند إلى المعايير الدولية في الحوكمة الرقمية داخل المؤسسات التعليمية. يشير ذلك إلى وجود وعي إداري وتكنولوجي متقدم في التعامل مع البيئة الرقمية ومخاطرها. بالمقابل، تُظهر النتائج أن الجامعات العراقية بحاجة إلى مراجعة شاملة لسياساتها الرقمية وتحديثها بما يتناسب مع التحديات الراهنة. فاعتماد نماذج عربية ناجحة مثل نموذج جامعة الشارقة قد يوفر خارطة طريق لتطوير منظومات حماية رقمية أكثر فعالية، تعزز من أمان البيئة الجامعية وتدعم الطلبة في مواجهة الابتزاز الإلكتروني بشكل شمولي ووقائي.

٣.١٠.٢ أنماط عامة مستخلصة من التحليل

تُظهر نتائج التحليل أن السياسات الرقمية في أغلب الجامعات العراقية لا تزال تعاني من ضعف في التكامل والشمول، إذ تركز معظم الوثائق الرسمية على الجانب العقابي دون تقديم إطار وقائي متكامل يشمل التوعية والدعم القانوني والنفسي للطلبة. هذا التركيز الأحادي يُضعف فعالية الاستجابة للمشكلات الرقمية المعقدة مثل الابتزاز الإلكتروني، ويجعل من السياسات أدوات ردع فقط بدلًا من كونها منظومات حماية شاملة. من الملاحظ أيضًا أن العديد من السياسات الجامعية لا تتضمن تعريفًا دقيقًا وصريحًا لمفهوم الابتزاز الإلكتروني، ما يؤدي إلى غموض في آليات التطبيق ويفتح المجال لاجتهادات قد تكون غير دقيقة أو غير منصفة. غياب هذا التعريف القانوني يُفقد السياسات وضوحها ويُصعّب مهمة إدارات الجامعات في معالجة الشكاوى أو اتخاذ إجراءات مناسبة عند وقوع حالات ابتزاز.

ويُضاف إلى ذلك وجود نقص واضح في برامج التوعية الرقمية، حيث لم تُظهر معظم الجامعات اهتمامًا ملموسًا في إعداد حملات تثقيفية أو إرشادية حول الاستخدام الآمن للتكنولوجيا أو سبل الوقاية من التهديدات الرقمية. هذا القصور يجعل الطلبة عرضة للمخاطر الرقمية دون امتلاك أدوات معرفية أو سلوكية تحصّنهم، وهو ما يُفاقم من خطورة الظاهرة في البيئات التعليمية. أما الجامعات التي أظهرت مستوى أعلى من الشمولية في سياساتها مثل جامعة الكوفة داخل العينة العراقية فهي غالبًا ما تستند إلى نماذج تنظيمية دولية أو تتأثر بخبرات إدارية أكثر انفتاحًا على المعايير العالمية. هذا الارتباط بالممارسات الفضلى عالميًا يُعزز من فعالية تلك السياسات ويمنحها قدرة أكبر على التكيّف مع التحديات الرقمية المتسارعة.

٣.١٠.٣ تفسير النتائج في ضوء الأطر النظرية

تُبرز نظرية الحماية لـ Rogers (1983) أن الفرد لا يتحرك لحماية نفسه من التهديدات إلا إذا توفرت لديه المعرفة الكافية بالخطر وآليات التعامل معه. وهذا يتفق تمامًا مع واقع السياسات الرقمية في الجامعات العراقية، حيث إن غياب التوعية وضعف برامج الإرشاد يجعل الطلبة غير مدركين لحجم الخطر الرقمي، ما يؤدي إلى تراجع دافعهم للاستجابة الوقائية، ويزيد من تعرضهم لجرائم مثل الابتزاز الإلكتروني دون حماية ذاتية كافية. أما من منظور نظرية التنظيم المؤسسي لـ Peters (2010)، فإن فعالية السياسات تتوقف على مدى انسجامها الداخلي وتكاملها عبر المستويات الإدارية. وهنا يظهر الفرق الواضح بين جامعة الشارقة، التي تقدم نموذجًا متكاملًا في التعامل مع المخاطر الرقمية، وبين معظم الجامعات العراقية التي تعاني من ضعف في التنسيق بين ما هو مكتوب في الوثائق وما يُطبق فعليًا على أرض الواقع، مما يحدّ من فاعلية الاستجابة المؤسسية للأزمات الرقمية. وفي ضوء نظرية الاقتصاد الأمني لـ Anderson & Moore (2006)، فإن أي تقصير في تخصيص الموارد الكافية للحماية الرقمية يخلق بيئة هشّة أمام الهجمات والجرائم الإلكترونية. وتشير النتائج بوضوح إلى أن الجامعات العراقية لا تُخصص موارد كافية أو سياسات فاعلة لبناء بنية تحتية رقمية قوية، ما يفسر ضعف الاستجابة وقلة الخدمات الوقائية مقارنة بنظيراتها العربية. تُظهر هذه النظريات الثلاث أن التحديات التي تواجه الجامعات العراقية ليست فقط في مستوى الوعي، بل تمتد إلى عمق البناء المؤسسي والمالي للسياسات الرقمية. ومن دون معالجة هذه الفجوات بطريقة منهجية متكاملة، ستظل السياسات غير فعالة في حماية الطلبة، وسيستمر الخطر الرقمي في التفاقم داخل البيئات التعليمية.

خاتمة

في ضوء ما توصل إليه هذا البحث من نتائج، يتّضح أن السياسات الرقمية المعتمدة في غالبية الجامعات العراقية لا تزال تعاني من ضعف في الشمول والتكامل، خاصة في ما يتعلق بمواجهة جرائم الابتزاز الإلكتروني. وبينما تُظهر بعض الجامعات محاولات أولية لوضع ضوابط رقمية، إلا أن التركيز المفرط على العقوبات دون وجود برامج توعية فعّالة، أو آليات إبلاغ واضحة، أو حماية قانونية كافية للضحايا، يجعل هذه السياسات غير قادرة على توفير بيئة رقمية آمنة ومستقرة للطلبة. وقد كشفت المقارنة مع بعض الجامعات العربية، مثل جامعة الشارقة، أن تبني نماذج مؤسسية متكاملة ومستندة إلى المعايير الدولية يسهم بشكل فعّال في تعزيز الحماية الرقمية داخل الحرم الجامعي. وهو ما يعكس أهمية وضوح السياسات، وتكامل عناصرها، وربطها ببنية تنفيذية مدعومة إداريًا وتشريعيًا. بناءً عليه، يوصي البحث بضرورة مراجعة السياسات الرقمية الجامعية في العراق، وتطويرها بما يشمل: إدراج تعريفات واضحة لجرائم الابتزاز الإلكتروني، تعزيز برامج التوعية، وضع آليات إبلاغ فعّالة وسرّية، وتوفير دعم قانوني ونفسي

للضحايا. كما يجب إشراك الطلبة والكوادر الإدارية في صياغة وتقييم هذه السياسات لضمان فاعليتها وقبولها على أرض الواقع. في النهاية، يشير هذا البحث إلى أن الأمن الرقمي في البيئات الجامعية لا يمكن تحقيقه من خلال العقوبات فقط، بل يتطلب مقاربة شاملة تشمل الوقاية، والحماية، والتثقيف، وذلك ضمن إطار مؤسسي متماسك يدرك تحديات الفضاء الرقمي ويستجيب لها بسياسات فعالة وقابلة للتنفيذ.

لمراجع

١. أندرسون، ر.، و مور، ت. (٢٠٠٦). اقتصاديات أمن المعلومات. *ساينس*.

٢. الشمراني، م.، وآخرون. (٢٠٢١). تحديات الأمن السيبراني في الجامعات الشرق أوسطية. *مجلة أمن المعلومات*.

٣. الزهراني، س. (٢٠١٩). تطوير السياسات الرقمية في جامعات الخليج. *مجلة السياسات السيبرانية*.

٤. الشاعر، إ.، وآخرون. (٢٠٢٢). سياسات الجامعات ومشاركة الطلبة في الأمن السيبراني. *التعليم وتقنيات المعلومات*.

٥. إبراهيم، ن.، و مطر، هـ. (٢٠٢٠). وحدات الأمن في المؤسسات التعليمية. *المجلة العربية للدراسات الأمنية*.

٦. أوغيلفي، ل. (٢٠٢٠). فهم الابتزاز السيبراني. *مراجعة الجريمة الرقمية*.

٧. بيترز، ب. ج. (٢٠١٠). *سياسة البيروقراطية*. روتليدج.

٨. روجرز، ر. و. (١٩٨٣). العمليات المعرفية والفسيولوجية في مناشدات الخوف وتغيير الاتجاه: نظرية معدّلة للتحفيز الوقائي. *علم النفس الاجتماعي الفسيولوجي*.

٩. يوسف، ع.، و عزيز، ت. (٢٠٢٠). الوعي الرقمي والوقاية من الجريمة في الجامعات العراقية. *المجلة العراقية للتربية*.

١٠. كيفت، س. (٢٠١٧). أطر السياسات الجامعية للتعلم الرقمي. *إدارة التعليم العالي*.

١١. رؤوف، ع.، و مقبول، ب. (٢٠٢١). التدريب على الحماية الرقمية في الوسط الأكاديمي. *الأمن السيبراني في التعليم*.

١٢. الخليفة، هـ. (٢٠٢١). الخصوصية والأخلاقيات في الفضاء السيبراني الأكاديمي. *المجلة الرقمية للشرق الأوسط*.

١٣. سعيد، ر. (٢٠٢٠). التنمر السيبراني والابتزاز: دور السياسات المؤسسية. *مراجعة الشباب والتكنولوجيا*.

١٤. العبدالله، س. (٢٠١٩). الجاهزية للأمن السيبراني في مؤسسات التعليم العالي. *مجلة المخاطر الرقمية*.

١٥. البنك الدولي. (٢٠٢٠). *التحول الرقمي في التعليم بمنطقة الشرق الأوسط وشمال إفريقيا*.

١٦. اليونسكو. (٢٠٢١). *إرشادات لبيئات التعلم الرقمي الآمنة*.
١٧. أمين، ن.، وآخرون. (٢٠٢١). تبني سياسات الأمن الرقمي في الجامعات العربية. *مجلة نظم المعلومات*.
١٨. صالح، ع. (٢٠٢٢). التهديدات عبر الإنترنت وخصوصية الطلاب. *المجلة العربية لتقنيات التعليم*.
١٩. حسن، م. (٢٠٢٠). تنفيذ السياسات الرقمية في الدول النامية. *مراجعة سياسات تكنولوجيا المعلومات والاتصالات*.
٢٠. سالم، هـ. (٢٠٢١). الجرائم السيبرانية في المؤسسات الأكاديمية: منظور عربي. *مجلة القانون السيبراني*.