



جرائم تكنولوجيا المعلومات والآثار الناجمة عنها

CRIMES OF TECHNOLOGY AND THE RESULTING EFFECTS

الباحث/حمد محمد الدوسري

كلية القانون جامعة لوسيل، قطر، QATAR, ALDOSARIHM@GMAIL.COM

تاريخ القبول: 2025/09/08

تاريخ الاستلام: 2025/05/21

ملخص:

تناول هذه الدراسة الجرائم المعلوماتية باعتبارها مظهرًا معاصرًا لانحراف السلوك الإجرامي في ظل التحولات الرقمية المتسارعة، فتعنى أولاً باستجلاء المفهوم القانوني لهذه الجرائم في ضوء الفقه والتشريعات الحديثة، وتحديد خصائصها المميزة التي تفرّقها عن الأفعال الإجرامية التقليدية، من حيث الطبيعة غير المادية للجريمة، وتعقيد أدواتها، واتساع نطاقها العابر للحدود، ويُعد هذا التحديد النظري مدخلاً جوهرياً لفهم الإشكاليات القانونية والعملية المرتبطة بمكافحة هذا النمط من الجرائم.

وفي سياق متصل، تبحث الدراسة في التداعيات المترتبة على ارتكاب الجرائم المعلوماتية، سواء على المستويات الفردية أو المؤسسية أو السيادية، لما تُحدثه من آثار تمس الأمن العام والثقة في الفضاء الرقمي، كما تستعرض السياسات الأمنية والوقائية التي تنتهجها الدول للحد من انتشار هذه الظاهرة، مع التركيز على دور التشريعات الوطنية، وتكامل الأطر التقنية والقانونية، وضرورة تبني استراتيجيات مرنة تستجيب للطبيعة الديناميكية لهذه الجرائم، بما يعزز الحماية القانونية ويضمن الأمن المعلوماتي في البيئة الرقمية المعاصرة.

الكلمات المفتاحية: الجرائم المعلوماتية، الجريمة الإلكترونية، الأمن السيبراني، التشريعات الرقمية، الجرائم المستحدثة، السياسات الوقائية، الفضاء الرقمي، الأدلة الرقمية، الحماية القانونية.

Abstract:

This study examines cybercrimes as a contemporary manifestation of deviant criminal behavior in light of accelerating digital transformations. It first explores the legal concept of these crimes in light of modern jurisprudence and legislation, and identifies their distinctive characteristics that distinguish them from traditional criminal acts. These characteristics include the non-material nature of the crime, the complexity of its tools, and its transnational scope. This theoretical definition is an essential entry point for understanding the legal and practical issues associated with combating this type of crime.

In a related context, the study examines the repercussions of cybercrimes, whether at the individual, institutional, or sovereign levels, given their impact on public security and confidence in the digital space. It also reviews the security and preventive policies adopted by countries to limit the spread of this phenomenon, focusing on the role of national legislation, the integration of technical and legal frameworks, and the necessity of adopting flexible strategies that respond to the dynamic nature of these crimes, thereby enhancing legal protection and ensuring information security in the contemporary digital environment.

Keywords: cybercrime, cybercrime, cybersecurity, digital legislation, emerging crimes, preventive policies, cyberspace, digital evidence, legal protection.

* المؤلف المرسل

مقدمة:

مع التطور السريع في التكنولوجيا والانتشار الواسع لاستخدام الإنترنت في مختلف مجالات الحياة، أصبحت الجرائم الإلكترونية التي تستهدف الأنظمة التقنية، بما في ذلك الشبكات والمواقع الإلكترونية، تشكل تهديدًا متزايدًا في العصر الرقمي، وتشمل هذه الجرائم الاختراقات الإلكترونية، والاحتيال الإلكتروني، وانتهاك حقوق الملكية الفكرية، والتجسس الإلكتروني، وعمليات التهديد والابتزاز الإلكتروني، مما يعرض الأفراد والمؤسسات لمخاطر عديدة.

وللتصدي لهذه التحديات، وضعت دولة قطر قوانين صارمة تهدف إلى مكافحة هذه الجرائم وحماية المعلومات والأنظمة الرقمية، حيث تنظم التشريعات القطرية مختلف الجوانب القانونية المتعلقة بالأمن الإلكتروني، وتفرض عقوبات مشددة على المخالفين، ويعد الاختراق للأنظمة الإلكترونية من أخطر هذه الجرائم، إذ يؤدي إلى تعريض البيانات الحساسة للخطر، مما يستلزم اتخاذ إجراءات قانونية رادعة ضد المتورطين، كما تتضمن القوانين القطرية عقوبات ضد الاحتيال الإلكتروني، الذي يمثل انتهاكًا لثقة المستخدمين وأمانهم الرقمي، ويعد تطبيق هذه القوانين بصرامة من العوامل الأساسية التي تساعد في الحد من الجرائم السيبرانية وتعزيز الاستقرار والأمان في البيئة الرقمية الوطنية.

كما عززت دولة قطر جهودها في مجال مكافحة الجرائم الإلكترونية من خلال تطوير تشريعات حديثة تهدف إلى حماية البيانات والأنظمة الرقمية، ومن أبرز هذه القوانين قانون مكافحة الجرائم الإلكترونية، الذي صدر بموجب القانون رقم 14 لسنة 2014، ويحدد هذا القانون بوضوح مختلف الجرائم المرتبطة بالتكنولوجيا الرقمية، ويشمل العقوبات المفروضة على المخالفين، ويغطي نطاقًا واسعًا من الجرائم، بما في ذلك الاختراق غير المشروع، والاحتيال عبر الإنترنت، وانتهاك حقوق التأليف والنشر، والتجسس الإلكتروني، والتهديدات السيبرانية، وتعد هذه التشريعات خطوة مهمة نحو تعزيز الأمن الرقمي، وضمان بيئة إلكترونية آمنة لجميع المستخدمين.

إشكالية البحث: تتبلور إشكالية البحث حول مدى ملائمة القانون القطري لمكافحة الجرائم الإلكترونية، التي تستهدف الأنظمة التقنية والشبكات والمواقع الإلكترونية، وي طرح البحث تساؤلًا جوهريًا حول مدى كفاءة القوانين الحالية في التعامل مع التهديدات الرقمية المتزايدة، مما يستدعي تحليلًا دقيقًا للتشريعات القائمة ومدى ملاءمتها للتطورات المستمرة في عالم الجرائم الإلكترونية، كما يسعى البحث إلى استكشاف الثغرات القانونية المحتملة التي قد تؤثر على قدرة النظام القانوني في دولة قطر على فرض عقوبات رادعة وحماية البنية التحتية الرقمية بشكل شامل⁽¹⁾، ومن خلال هذا التحليل يهدف البحث إلى تقييم الحاجة إلى تعديلات أو تحسينات الإطار القانوني، لضمان فعالية التصدي لمختلف أنواع الجرائم السيبرانية، وتعزيز الأمن

الإلكتروني، وفي هذا السياق يتمثل التساؤل الأساسي الذي يسعى البحث إلى الإجابة عليه هو: إلى أي مدى تتيح القوانين القطرية الحالية تطبيقاً فعالاً لتجريم الجرائم الإلكترونية التي تستهدف أنظمة المعلومات التقنية والشبكات والمواقع الإلكترونية؟

أسئلة البحث: يتناول هذا البحث مجموعة من التساؤلات الجوهرية التي ترتبط بالقانون القطري ودوره في مكافحة الجرائم الإلكترونية وحماية الأنظمة التقنية، ومن أبرز هذه الأسئلة:

- ما الدور الذي تلعبه التشريعات الوطنية والدولية في التصدي للجرائم الإلكترونية وتعزيز الأمن السيبراني؟

- ما هي الأساليب والتقنيات الأكثر فعالية في حماية أنظمة المعلومات من التهديدات الإلكترونية؟

- كيف يساهم التدريب والتوعية السيبرانية في تعزيز مستوى الأمان الرقمي وتقليل المخاطر الإلكترونية؟

- ما الطرق المتاحة لقياس كفاءة الإجراءات الأمنية الحالية، وكيف يمكن تحديد نقاط الضعف ومعالجتها لتحسين

مستوى الحماية؟

أهمية البحث: تكمن أهمية البحث في ظل التقدم التكنولوجي المتسارع والاعتماد المتزايد على النظم الرقمية في مختلف مجالات الحياة، حيث تعد الجرائم الإلكترونية تهديداً خطيراً يهدد استقرار وأمن البنية التحتية الرقمية، والمواقع الإلكترونية، والشبكات المعلوماتية، وتشكل هذه الجرائم تحدياً كبيراً للحكومات والمؤسسات، نظراً لما تسببه من خسائر مالية ضخمة، وانتهاكات للخصوصية، وتعطيل للخدمات الحيوية، مثل القطاعات المصرفية، والاتصالات، والطاقة، والخدمات الحكومية الإلكترونية.

ومن هنا يأتي دور هذا البحث في تسليط الضوء على هذه التهديدات وتحليل تأثيرها على المجتمع والاقتصاد، مع التركيز على كيفية مكافحتها بفعالية، لذا فإن هذا البحث لا يقتصر فقط على استعراض المخاطر، بل يتعمق في دراسة القوانين القطرية الحالية، ومدى فعاليتها في مواجهة الجرائم الإلكترونية، حيث يهدف إلى تحليل التشريعات المعمول بها، وتحديد ما إذا كانت قادرة على توفير الحماية الكافية للبيانات والأنظمة الرقمية، كما يسعى إلى استكشاف الفجوات القانونية التي قد تحتاج إلى تعديلات أو تطوير لضمان التصدي الفعال للهجمات الإلكترونية، وبالتالي، يساهم هذا البحث في تحسين المنظومة القانونية، واقتراح سياسات أمنية أكثر صرامة لمواجهة التحديات المستمرة في مجال الأمن السيبراني.

كما يلقي البحث الضوء على أهمية التوعية والتدريب في تعزيز الأمن السيبراني، فمع تطور أساليب الهجمات الإلكترونية، أصبح من الضروري رفع مستوى الوعي لدى الأفراد والمؤسسات حول كيفية حماية بياناتهم ومعلوماتهم الشخصية،

ويهدف البحث إلى تقديم توصيات حول أفضل الممارسات والتقنيات الحديثة التي يمكن اعتمادها للحد من الجرائم الإلكترونية، مثل تعزيز أنظمة الحماية، وتطوير استراتيجيات الأمن السيبراني، واستخدام الذكاء الاصطناعي في كشف التهديدات السيبرانية، كما يستعرض البحث دور التعاون الدولي في مكافحة هذه الجرائم، حيث أصبحت الجريمة الإلكترونية عابرة للحدود، مما يستلزم تنسيقاً قانونياً وأمنياً بين الدول لتعزيز الجهود العالمية في التصدي لهذه التهديدات، فإن هذا البحث لا يقتصر على دراسة الإطار القانوني فقط، بل يمتد ليشمل الجوانب التقنية، والأمنية، والتوعوية، مما يجعله ذا قيمة كبيرة في دعم الجهود المبذولة لحماية الفضاء الإلكتروني، وتحقيق بيئة رقمية أكثر أماناً واستقراراً، كما يساهم في وضع استراتيجيات فعالة لتعزيز الأمن السيبراني، وحماية الأفراد والمؤسسات من المخاطر المتزايدة في العالم الرقمي الحديث.

أهداف البحث:

- استكشاف مدى تأثير الجرائم الإلكترونية على أنظمة المعلومات التقنية والشبكات والمواقع الرقمية، مع دراسة انعكاساتها على البيئة الرقمية، وذلك في إطار القوانين القطرية المعنية بمكافحة هذا النوع من الجرائم.
- تصنيف وتحليل مختلف أنواع الجرائم الإلكترونية التي تستهدف البنية التحتية الرقمية، مع تقديم رؤية واضحة حول طبيعة هذه الجرائم استناداً إلى التشريعات القطرية المعمول بها، مما يساهم في تحديد أفضل السبل لمواجهتها والحد من مخاطرها.
- مراجعة ودراسة القوانين والسياسات المحلية والدولية المتعلقة بمكافحة الجرائم الإلكترونية، وتقييم مدى فاعليتها، مع التركيز على آليات تنفيذها ودور الجهات المعنية في تعزيز تطبيقها بشكل فعال.
- اقتراح حلول واستراتيجيات متطورة لتعزيز حماية أنظمة المعلومات والشبكات من الهجمات الإلكترونية، بما يتماشى مع الأطر القانونية القطرية والتوجهات الأمنية المعتمدة لضمان بيئة رقمية أكثر أماناً.

- تعزيز مستوى الوعي حول مخاطر الجرائم الإلكترونية لدى الأفراد والمؤسسات، من خلال نشر ثقافة الأمن السيبراني، وتوضيح الإجراءات الوقائية وأفضل الممارسات التي تحمي المستخدمين من التهديدات الرقمية، وذلك وفق القوانين والإرشادات الأمنية المعتمدة.

منهجية البحث: استخدم الباحث المنهج التأصيلي التحليلي لدراسة تأثيرات الجريمة الإلكترونية على الأفراد والمؤسسات، ومدى انعكاساتها السلبية، والآثار المترتبة عليها.

خطة البحث:

-المقدمة

-ملخص باللغة العربية.

-مخلص باللغة الإنجليزية.

-المبحث الأول: مفهوم الجرائم المعلوماتية.

-المطلب الأول: أنواع الجرائم المعلوماتية.

-الفرع الأول: جريمة القرصنة الإلكترونية.

-الفرع الثاني: جريمة الاحتيال الإلكتروني.

-الفرع الثالث: جريمة التجسس الإلكتروني.

-الفرع الرابع: جريمة التعدي على حقوق النشر.

-المطلب الثاني: سمات الجرائم المعلوماتية.

-الفرع الأول: الجهود الوطنية للحد من الجرائم الإلكترونية.

-الفرع الثاني: العقوبات المقررة وفقاً للقانون.

-الفرع الثالث: التشريعات الوطنية والدولية.

-المبحث الثاني: الآثار الناجمة عن الجرائم المعلوماتية.

-المطلب الأول: مدى انعكاس الجريمة المعلوماتية.

-الفرع الأول: البرمجيات الخبيثة والفيروسات.

-الفرع الثاني: سرقة البيانات الشخصية.

-الفرع الثالث: الآثار السلبية على الأفراد والمؤسسات.

-المطلب الثاني: السياسات الأمنية والوقائية للحد من الجريمة.

-الفرع الأول: تعزيز أمن المعلومات.

-الفرع الثاني: أهمية الوعي السيبراني.

-الفرع الثالث: السياسات التوعوية والتعليمية.

-الخاتمة:

-النتائج:

-الاقتراحات:

-المراجع:

المبحث الأول: مفهوم الجرائم المعلوماتية

مع التطور السريع في التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية، أصبحت الجرائم الإلكترونية واحدة من أخطر التحديات التي تواجه الأفراد والمؤسسات والحكومات على مستوى العالم، إذ تتنوع هذه الجرائم بين عمليات الاختراق، والاحتيال الإلكتروني، وسرقة البيانات، والتجسس الإلكتروني، مما يجعل من الضروري دراسة أبعادها وتأثيراتها على أمن المعلومات والاقتصاد والمجتمع بشكل عام، ويعد الفضاء الإلكتروني بيئة متجددة تتطلب إجراءات أمنية متطورة لمواجهة التهديدات المستمرة التي تتطور بمرور الوقت، مما يستلزم وجود تشريعات صارمة وآليات رقابة دقيقة لضبط الأنشطة الإلكترونية غير القانونية⁽²⁾.

وقد أعبرت دولة قطر عن مبادراتها لمكافحة الجرائم الإلكترونية في ظل التحول الرقمي الذي تشهده الدولة بمختلف القطاعات، حيث تم وضع قوانين وسياسات تهدف للحد من هذه الجرائم وحماية أنظمة المعلومات والشبكات الرقمية من التهديدات المتزايدة، وتعد التشريعات القطرية المتعلقة بمكافحة الجرائم الإلكترونية جزءاً أساسياً من الجهود المبذولة لتعزيز الأمن السيبراني، إذ تهدف إلى توفير بيئة إلكترونية آمنة تضمن سرية المعلومات وسلامة الأنظمة الرقمية، ومن خلال دراسة الإطار العام للجرائم الإلكترونية، يصبح من الممكن فهم طبيعة هذه الجرائم وأساليب ارتكابها، مما يساهم في تطوير حلول فعالة واستراتيجيات لمواجهتها⁽³⁾.

إذ يعتبر التحدي الأكبر الذي تفرضه الجرائم الإلكترونية هو طبيعتها المتغيرة، حيث يبتكر المهاجمون أساليب جديدة لاختراق الأنظمة واستغلال الثغرات الأمنية، مما يجعل التصدي لها أمراً يتطلب تحديثاً مستمراً للقوانين والتشريعات، إلى جانب الاستثمار في التكنولوجيا الحديثة لحماية البيانات والمعلومات، كما أن رفع الوعي حول مخاطر الجرائم الإلكترونية يلعب دوراً حيوياً في الحد من انتشارها، وذلك من خلال تثقيف الأفراد والمؤسسات حول أهمية اتخاذ التدابير الاحترازية واستخدام تقنيات الحماية المتقدمة، مما يعزز الأمن الرقمي ويساهم في خلق بيئة إلكترونية أكثر أماناً، وسوف نتناول تعريف الجرائم المعلوماتية (بالمطلب الأول) وسماتها (بالمطلب الثاني).

المطلب الأول: أنواع الجرائم المعلوماتية: تعرف الجرائم الإلكترونية بأنها الأفعال غير القانونية التي تُرتكب عبر استخدام الحاسوب أو الإنترنت، حيث تعتمد هذه الجرائم بشكل أساسي على التكنولوجيا الحديثة ووسائل الاتصال الرقمية، مما يميزها عن الجرائم التقليدية من حيث الأساليب، والأدوات المستخدمة في تنفيذها، فهي لا تتطلب وجوداً مادياً للمجرم في موقع الجريمة، بل يمكن تنفيذها عن بُعد عبر الشبكات الإلكترونية، فعلى سبيل المثال، يستطيع المخترقون الوصول بشكل غير مشروع إلى الأنظمة الرقمية، وتنفيذ أعمال ضارة بسهولة من خلال الفضاء الإلكتروني، مما يجعل مكافحتها تحدياً يتطلب حلولاً تقنية

وتشريعية متطورة.⁽⁴⁾

الفرع الأول: جريمة القرصنة الإلكترونية: يعد الاختراق الإلكتروني أحد أخطر الجرائم السيبرانية، حيث يتمثل في الدخول غير المشروع إلى أنظمة الحواسيب أو الشبكات أو الأجهزة الإلكترونية بهدف الوصول إلى بيانات حساسة وتعطيل النظام، أو تنفيذ أنشطة ضارة أخرى، ويشكل هذا النوع من الجرائم تهديدًا كبيرًا على أمن المعلومات والبيانات، إذ يمكن للمخترقين استغلال الثغرات الأمنية للوصول إلى معلومات سرية، سواء كانت شخصية أو مالية، مما يؤدي إلى انتهاك الخصوصية والتسبب في خسائر كبيرة للأفراد والشركات على حد سواء.

وتتنوع أساليب الاختراق ما بين استخدام البرمجيات الخبيثة مثل الفيروسات، وبرامج التجسس، وبرامج الفدية، إلى الهجمات المتطورة التي تعتمد على استغلال الثغرات الأمنية في الأنظمة والشبكات، كما يمكن للمهاجمين تنفيذ عمليات اجتياح منهجة لاختراق الأنظمة المستهدفة، مما قد يؤدي إلى شل الخدمات وتعطيل الأنشطة التشغيلية للمؤسسات، الأمر الذي يتسبب في خسائر مالية كبيرة وتأثير سلبي على سير الأعمال، ولا تقتصر الهجمات الإلكترونية على الأفراد فقط، بل تمتد أيضًا إلى الشركات الكبرى والمؤسسات الحكومية.

ما يجعل من الضروري اتخاذ تدابير أمنية مشددة لحماية الأنظمة من الاختراقات، ويتضمن ذلك استخدام تقنيات الحماية المتقدمة مثل أنظمة كشف التسلل، وبرامج الحماية من الفيروسات، وتحديث البرمجيات بشكل دوري لسد الثغرات الأمنية، فالوعي الأمني والتدابير الوقائية يمثلان خط الدفاع الأول ضد هذه التهديدات السيبرانية المتزايدة.⁽⁵⁾

الفرع الثاني: جريمة الاحتيال الإلكتروني: يعد الاحتيال الإلكتروني أحد أكثر أساليب الجرائم السيبرانية شيوعًا، حيث يعتمد على استخدام طرق خادعة لإقناع الأفراد بالكشف عن معلومات حساسة مثل: كلمات المرور، أو بيانات الحسابات المصرفية، وتكمن خطورة هذا النوع من الجرائم في قدرته على استغلال الثقة، إذ يقوم المهاجمون بانتحال صفة جهات موثوقة مثل البنوك أو المؤسسات المالية أو الوكالات الحكومية، مستهدفين الضحايا برسائل إلكترونية تبدو حقيقية، لكنها تهدف إلى الاحتيال عليهم، وتعتمد أساليب الاحتيال الإلكتروني على الخداع البصري والتلاعب النفسي، حيث يتم إرسال رسائل بريد إلكتروني أو رسائل نصية مزيفة تدّعي وجود مشكلة أمنية في الحساب أو تعرض المستخدم لعملية احتيالية، ويتم توجيهه إلى النقر على رابط مشبوه يؤدي إلى موقع إلكتروني مزيف مصمم ليبدو مطابقًا للموقع الرسمي للجهة المزعومة.

وعند إدخال البيانات الشخصية أو معلومات الحسابات، يتمكن المهاجمون من سرقتها واستخدامها لعمليات مالية غير مشروعة، أو حتى لانتحال هوية الضحية، ونظرًا للتطور المستمر في أساليب الاحتيال الإلكتروني، من الضروري أن يكون الأفراد والمؤسسات أكثر وعيًا وحذرًا، فعدم النقر على الروابط المشبوهة، والتحقق من هوية المرسل، وعدم مشاركة المعلومات

الشخصية عبر البريد الإلكتروني أو الرسائل النصية، كلها إجراءات ضرورية للحماية من الوقوع ضحية لهذه الجرائم، كما أن استخدام تقنيات الحماية مثل التحقق الثنائي وتحديث كلمات المرور بانتظام يساعد في تعزيز الأمان الرقمي وتقليل مخاطر الاحتيال الإلكتروني.⁽⁶⁾

الفرع الثالث: جريمة التجسس الإلكتروني: يعد التجسس الإلكتروني أحد أخطر أشكال الجرائم السيبرانية، حيث يعتمد على استخدام برمجيات خبيثة مصممة لجمع البيانات دون علم أو إذن المستخدم، ويعمل هذا النوع من الهجمات على اختراق الأجهزة الإلكترونية وسرقة المعلومات الشخصية والحساسة، مما يجعله تهديداً كبيراً للأفراد والمؤسسات على حد سواء، تُزرع برامج التجسس على أجهزة الكمبيوتر أو الهواتف الذكية بطرق خفية، إما من خلال تحميل ملفات ملوثة، أو فتح روابط مشبوهة، أو حتى عبر عمليات تصيد إلكتروني متطورة، وبمجرد إصابة الجهاز.

تبدأ هذه البرامج في تسجيل أنشطة المستخدم مثل نقرات لوحة المفاتيح، وسجل التصفح، ومعلومات تسجيل الدخول، بالإضافة إلى سرقة البيانات المالية مثل أرقام الحسابات وكلمات المرور، يمكن أن تُستخدم المعلومات المسروقة بطرق ضارة مثل الاحتيال المالي، أو انتحال الهوية، أو حتى في عمليات ابتزاز إلكتروني، كما أن التجسس الإلكتروني لا يقتصر على الأفراد فقط، بل يمكن أن يستهدف الشركات والمؤسسات، مما قد يؤدي إلى تسريب بيانات حساسة، أو تدمير سمعة الشركات في حال اختراق أنظمتها الأمنية، للحد من مخاطر التجسس الإلكتروني لابد من اتباع تدابير الحماية مثل: تثبيت برامج مكافحة الفيروسات القوية، وتحديث أنظمة التشغيل والتطبيقات بانتظام، بالإضافة إلى تجنب فتح الملفات أو الروابط المجهولة المصدر، كما أن تعزيز الوعي الأمني حول مخاطر التجسس الإلكتروني يعد من الخطوات الأساسية لحماية البيانات والحفاظ على الخصوصية في البيئة الرقمية المتطورة.⁽⁷⁾

الفرع الرابع: جريمة التعدي على حقوق النشر: يعد التعدي على حقوق النشر من الجرائم الإلكترونية التي تنتهك حقوق الملكية الفكرية، حيث يتمثل في استغلال أو إعادة نشر المحتوى المحمي بحقوق النشر دون إذن مسبق من صاحبه، وهذا يشمل مختلف أنواع الأعمال الإبداعية مثل الكتب والمقالات والموسيقى والأفلام والبرمجيات والتصميمات الفنية وغيرها من المواد المحمية قانوناً.

ويحدث هذا الانتهاك غالباً عبر الإنترنت، حيث يتم توزيع المحتوى المحمي بطرق غير مشروعة عبر المواقع الإلكترونية، أو منصات التواصل الاجتماعي، أو تطبيقات مشاركة الملفات، مما يؤدي إلى خسائر مالية ضخمة لأصحاب الحقوق، ويؤثر سلباً على الابتكار والإبداع، إذ إن عدم احترام حقوق النشر يقلل من الدافع للإنتاج الإبداعي نتيجة عدم حصول المبدعين على حقوقهم القانونية والمالية، ولمواجهة هذه الظاهرة، تفرض العديد من الدول، بما في ذلك دولة قطر، قوانين صارمة تحمي حقوق

النشر، حيث تشمل العقوبات غرامات مالية كبيرة، وحظر المواقع المخالفة، وحتى المساءلة القانونية للأفراد المتورطين في نشر أو تحميل المحتوى المحمي دون ترخيص، كما تلعب الجهات الرقابية ومزودو خدمات الإنترنت دورًا رئيسيًا في الحد من هذه المخالفات من خلال إزالة المحتوى غير القانوني وتعزيز الوعي حول أهمية احترام حقوق الملكية الفكرية، ولتجنب الوقوع في مخالفة قانونية يجب على الأفراد والشركات الحرص على الحصول على التراخيص المناسبة عند استخدام المحتوى المحمي بحقوق النشر، بالإضافة إلى دعم المنصات القانونية التي توفر المحتوى الإبداعي بطرق مشروعة، مما يساهم في حماية حقوق المبدعين وضمان استمرارية الإنتاج الفني والتقني بشكل قانوني وأخلاقي⁽⁸⁾.

المطلب الثاني: سمات الجرائم المعلوماتية: تتميز الجرائم الإلكترونية بخصائص فريدة تجعلها مختلفة تمامًا عن الجرائم التقليدية من حيث: الأساليب المستخدمة وطرق التنفيذ والتحديات القانونية المرتبطة بها، فعلى عكس الجرائم التقليدية التي يكون دافعها الأساسي غالبًا تحقيق مكاسب مالية مباشرة أو الانتقام، فإن مرتكب الجريمة الإلكترونية غالبًا ما يكون شخصًا متكيفًا اجتماعيًا، ويمتلك مستوى عالٍ من المعرفة التقنية، وقد يكون دافعه الرئيسي هو اختبار قدرته على اختراق الأنظمة، والتلاعب بها أكثر من كونه يسعى لتحقيق منفعة مادية مباشرة، ومع ذلك فإن بعض الجرائم الإلكترونية يكون هدفها الربح غير المشروع مثل الاحتيال المالي، وسرقة البيانات المصرفية، وأحد التحديات الكبرى المرتبطة بالجرائم الإلكترونية هو صعوبة تعقب مرتكبيها وإثباتها قانونًا.

حيث تتم هذه الجرائم في الفضاء الرقمي ولا تترك وراءها آثارًا مادية واضحة مثل الجرائم التقليدية، فلا توجد بصمات أو شهود عيان أو أدلة مادية يمكن جمعها بسهولة، مما يجعل التحقيقات الجنائية في هذا النوع من الجرائم معقدة للغاية، أيضًا فإن المجرمين الإلكترونيين يستخدمون تقنيات متقدمة مثل التشفير وإخفاء الهوية لتجنب التعقب، مما يزيد من صعوبة الوصول إليهم وإثبات تورطهم في الجريمة⁽⁹⁾.

كما تتميز الجرائم الإلكترونية بطابعها العابر للحدود، حيث يمكن أن تُرتكب في دولة ما وتستهدف أفرادًا أو مؤسسات في دولة أخرى باستخدام خوادم موزعة في مناطق مختلفة حول العالم، وهذا البعد الدولي يعقد عملية الملاحقة القانونية، إذ تتطلب مكافحة هذه الجرائم تنسيقًا دوليًا بين الجهات القانونية، وأجهزة الأمن السيبراني في مختلف الدول، كما تطرح هذه الطبيعة العابرة للحدود تحديات قانونية تتعلق بتحديد الجهة المختصة بالتحقيق والمقاضاة، بالإضافة إلى اختلاف القوانين والتشريعات بين الدول في التعامل مع هذا النوع من الجرائم.

وقد أدركت الجهات المختصة بدولة قطر خطورة الجرائم الإلكترونية وتأثيرها على الأفراد والمؤسسات، ووضعت تشريعات جنائية صارمة، تهدف إلى مكافحة الجريمة والحد من انتشارها، ومن أبرزها قانون رقم 14 لسنة 2014 بشأن

مكافحة الجرائم الإلكترونية، الذي يحدد العقوبات المفروضة على مختلف أنواع الجرائم الرقمية مثل: الاختراق غير المشروع، وانتهاك الخصوصية، والاحتيال الإلكتروني، ونشر المحتوى غير القانوني، وسرقة الهوية الرقمية، كما أنشأت الدولة هيئات متخصصة في الأمن السيبراني تعمل على تطوير استراتيجيات لحماية البنية التحتية الرقمية، وتعزيز الوعي المجتمعي بمخاطر الجرائم الإلكترونية⁽¹⁰⁾.

كما تلعب المؤسسات والشركات دورًا حيويًا في التصدي لهذه التهديدات من خلال تبني أحدث تقنيات الحماية مثل: أنظمة التشفير، وبرمجيات الحماية من الفيروسات، والجدران النارية، إلى جانب تعزيز سياسات الأمن السيبراني داخل المؤسسات، وتدريب الموظفين على كيفية التعامل مع التهديدات الرقمية، كما أن التوعية العامة تلعب دورًا أساسيًا في الوقاية من هذه الجرائم، إذ يساعد تثقيف المستخدمين حول أساليب الاحتيال الإلكتروني والممارسات الآمنة عبر الإنترنت على تقليل فرص الوقوع ضحايا للهجمات الإلكترونية، لذا تعد مكافحة الجرائم الإلكترونية مسؤولية مشتركة تتطلب تضافر الجهود بين الأفراد والمؤسسات والحكومات، ومن خلال تحديث القوانين، وتعزيز التقنيات الأمنية، والتعاون الدولي، ليتم الحد من هذه الجرائم وتقليل تأثيرها على المجتمع، مما يساهم في بناء بيئة رقمية أكثر أمانًا واستقرارًا⁽¹¹⁾.

الفرع الأول: الجهود الوطنية للحد من الجرائم الإلكترونية:

اعتمد التشريع القطري، أداة قانونية صارمة في مكافحة الجرائم الإلكترونية التي تستهدف نظم المعلومات التقنية، حيث يوفر إطارًا شاملاً لحماية البيانات الرقمية، وتعزيز الأمن السيبراني في الدولة، ويتضمن هذا القانون مجموعة من المواد التي تفرض عقوبات صارمة على الجرائم الإلكترونية المختلفة، مثل: الاختراق للأنظمة والشبكات، والاحتيال الإلكتروني، والتزوير الرقمي، وانتهاك حقوق الملكية الفكرية، مما يساهم في ردع المتسللين والمحتالين ومنعهم من ممارسة أنشطتهم غير القانونية،

كما يهدف هذا القانون إلى تعزيز ثقة الأفراد والمؤسسات في البيئة الرقمية، من خلال وضع ضوابط واضحة تحكم التعامل مع البيانات والمعلومات المخزنة إلكترونياً، ويساهم في حماية الأصول الرقمية من التلاعب والاستغلال غير القانوني.

كما يوفر للجهات المختصة الأدوات القانونية اللازمة لملاحقة مرتكبي الجرائم الإلكترونية، مما يضمن تحقيق العدالة ومعاقبة المخالفين، إضافة إلى ذلك، يساهم القانون في نشر الوعي بأهمية تبني الممارسات الأمنية الصحيحة، ويشجع المؤسسات والأفراد على اتخاذ التدابير الوقائية لحماية أنظمتهم الرقمية من التهديدات السيبرانية⁽¹²⁾.

وباستقراء نصوص المواد الواردة بصدر القانون سالف الذكر، نجد أن المشرع القطري قد تصدى للجرائم الإلكترونية بشكل عام، إذ نص بالمادة رقم 2 على عقوبات الدخول غير المشروع إلى الأنظمة والشبكات الإلكترونية الخاصة للدولة بالحبس والغرامة، بينما تتناول المادة رقم 3 الدخول غير المصرح به إلى كافة المواقع والأنظمة الإلكترونية، وتنص على عقوبات لمن يستمر

في التواجد داخلها بعد الاختراق، أما في المادة رقم 10 فتتركز على جريمة التزوير الإلكتروني، وتفرض عقوبات رادعة على من يقوم بتزييف المستندات الرسمية أو غير الرسمية بوسائل رقمية.

كما أن المادة رقم 13 تتعلق بحماية حقوق الملكية الفكرية عبر الإنترنت، حيث تعاقب كل من يعتدي على هذه الحقوق من خلال الوسائل الإلكترونية، ورغم فعالية هذا القانون في مكافحة الجرائم الإلكترونية، إلا أن تطبيقه يتطلب كوادراً متخصصة تمتلك مهارات تقنية متقدمة قادرة على التعامل مع الأدلة الرقمية، مما يشكل تحدياً للجهات المعنية بإنفاذ القانون، ولا يقتصر دور القانون على المعاقبة فقط، بل يتطلب أيضاً تعزيز التعاون بين المؤسسات القانونية والتقنية، والأجهزة الأمنية لمواجهة التهديدات السيبرانية المتزايدة وحماية المنظومة الرقمية.⁽¹³⁾

الفرع الثاني: العقوبات المقررة وفقاً للقانون: رسم القانون مجموعة من العقوبات الرادعة لمن يرتكب جريمة إلكترونية تهدد أمن المعلومات والخصوصية في الدولة، حيث شدد على ضرورة التصدي لهذه الجرائم بصرامة لضمان سلامة الفضاء الرقمي وحماية الأفراد والمؤسسات، وفقاً للمادتين الثانية والثالثة من القانون.

يُعاقب كل من قام بالدخول إلى موقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية دون الحصول على إذن مسبق، أو تجاوز حدود الصلاحيات الممنوحة له، بالسجن لمدة تصل إلى ثلاث سنوات، وغرامة مالية تصل إلى 500,000 ريال قطري، وإذا ترتب على هذا الاختراق الحصول على معلومات تمس الأمن الداخلي أو الخارجي للدولة، يتم تشديد العقوبة لتصل إلى الضعف⁽¹⁴⁾.

أما المادة الرابعة فقد نصت على معاقبة كل من تعمد التنصت على بيانات متداولة عبر الشبكة المعلوماتية أو وسائل التواصل الاجتماعي بالسجن لمدة تصل إلى سنتين، أو بغرامة مالية لا تتجاوز 100,000 ريال قطري، أو بالعقوبتين معاً، وذلك لحماية سرية البيانات والمراسلات، كما حددت المادة الخامسة العقوبات لمن يدير موقعاً إلكترونياً لصالح الجماعات الإرهابية، أو يساهم في تسهيل تواصلهم أو الترويج لأفكارهم، حيث يُعاقب بالسجن لمدة تصل إلى ثلاث سنوات، مع فرض غرامة مالية لا تتجاوز 500,000 ريال قطري.

وفيما يتعلق بجرائم استغلال الأطفال بالمواد الإباحية، فقد نصت المادة السابعة على معاقبة كل من قام بإنتاج محتوى إباحي يتعلق بالأطفال باستخدام الوسائل التقنية بالسجن لمدة تصل إلى خمس سنوات، أو بغرامة تصل إلى 500,000 ريال قطري، أو بالعقوبتين معاً، كما يُعاقب كل من حصل على مادة إباحية تخص طفلاً بالسجن لمدة عام، أو بغرامة تصل إلى 250,000 ريال قطري، أو بكليتا العقوبتين، وقد حدد القانون سن الطفولة بأنه كل شخص لم يتجاوز الثامنة عشر عاماً⁽¹⁵⁾.

أما المادة الثامنة فقد شددت العقوبات على من يقوم بنشر أخبار أو صور أو تسجيلات صوتية تمس الحياة الخاصة للأفراد

أو العائلات، حتى وإن كانت هذه المعلومات صحيحة، حيث يُعاقب بالسجن لمدة تصل إلى ثلاث سنوات، أو بغرامة تصل إلى 100,000 ريال قطري، أو بكلتا العقوبتين معاً، وفيما يخص الابتزاز الإلكتروني، أوضحت المادة التاسعة أن كل من يستغل الإنترنت أو وسائل الاتصال الأخرى لابتزاز شخص ما، أو تهديده بغرض إجباره على دفع أموال أو القيام بأفعال غير مشروعة، يُعاقب بالسجن لمدة تصل إلى ثلاث سنوات، أو بغرامة تصل إلى 100,000 ريال قطري، أو بكلتا العقوبتين، ومن هذا المنطلق تبرز جهود دولة قطر والتزامها التام، بحماية المجتمع من مخاطر الجرائم الإلكترونية، وضمان بيئة إلكترونية آمنة تحترم الخصوصية والأمن المعلوماتي⁽¹⁶⁾.

الفرع الثالث: التشريعات الوطنية والدولية: تُعد التشريعات الوطنية والدولية من الأدوات الأساسية لمكافحة الجرائم الإلكترونية، حيث تهدف إلى وضع إطار قانوني واضح يُحدد الأنشطة غير المشروعة عبر الإنترنت ويقر العقوبات المناسبة على مرتكبيها، فالهدف الأساسي من هذه القوانين هو حماية الأفراد والمؤسسات من الهجمات الإلكترونية وضمان أمن البيانات والمعلومات الحساسة، وتتفاوت هذه التشريعات بين القوانين التي تعتمد على الدول لحماية مواطنيها، والاتفاقيات الدولية التي تسعى إلى تنسيق الجهود العالمية لمكافحة هذا النوع من الجرائم.

وعلى المستوى الوطني تُصدر الحكومات قوانين محلية تُجرّم مجموعة واسعة من الجرائم الإلكترونية مثل عمليات الاختراق غير المشروع، والاحتيال الرقمي، والتجسس الإلكتروني، وسرقة البيانات، وانتهاك حقوق الملكية الفكرية، كما تتضمن هذه القوانين إجراءات قانونية صارمة تفرض عقوبات رادعة على المجرمين، إلى جانب آليات لحماية الضحايا، وضمان استرداد حقوقهم، كما تعتمد الدول استراتيجيات لتعزيز الأمن السيبراني تشمل تطوير البنية التحتية التكنولوجية وتوفير التدريب المستمر للجهات المختصة في إنفاذ القانون لمواكبة التطورات السريعة في مجال الجريمة الرقمية⁽¹⁷⁾.

وعلى الصعيد الدولي فهناك مجموعة من الاتفاقيات والمعاهدات التي تهدف إلى توحيد الجهود العالمية في التصدي للجرائم الإلكترونية، حيث تسهل هذه الاتفاقيات التعاون القانوني بين الدول، وتتيح تبادل المعلومات بين الهيئات الأمنية، مما يعزز من قدرة الدول على ملاحقة المجرمين حتى وإن كانوا خارج نطاق سلطاتها القضائية، كما تشمل هذه المعاهدات تطوير معايير موحدة للتعامل مع التهديدات السيبرانية، وتحقيق مستوى أعلى من الحماية للأفراد والشركات على مستوى العالم، لذا أصبح من الممكن الحد من مخاطر الجرائم الإلكترونية وتعزيز بيئة رقمية أكثر أماناً، كما أن التحدي الأكبر يكمن في التحديث المستمر لهذه القوانين لمواكبة التغيرات السريعة في التقنيات وأساليب الهجمات الإلكترونية، مما يستدعي تعاوناً مستمراً بين الحكومات، والمؤسسات، والجهات الفاعلة في مجال الأمن السيبراني لضمان فعالية هذه القوانين وقدرتها على مواجهة التهديدات المستجدة⁽¹⁸⁾.

لذلك تم سن مجموعة من القوانين واللوائح الهادفة إلى مكافحة الجرائم الإلكترونية وحماية البيانات، حيث وُضع إطار قانوني متكامل يهدف إلى الحد من الأنشطة غير المشروعة عبر الإنترنت وضمان بيئة رقمية آمنة، ومن بين أبرز هذه القوانين، قانون مكافحة الجرائم الإلكترونية، والذي يحدد بدقة الجرائم التي تُرتكب في الفضاء السيبراني، مثل عمليات القرصنة الإلكترونية، والاحتيال الرقمي، وانتهاك الخصوصية، كما يتضمن هذا القانون إجراءات صارمة لتعزيز الحماية الإلكترونية، بما في ذلك تدابير للحد من الاختراقات وتأمين الأنظمة الرقمية ضد أي تهديدات محتملة، بالإضافة إلى فرض عقوبات رادعة على مرتكبي هذه الجرائم لضمان تحقيق الردع العام⁽¹⁹⁾.

وفيما يتعلق بالمستوى الدولي نجد أن العديد من الدول تطبق قوانين مماثلة لمكافحة الجرائم الإلكترونية، فعلى سبيل المثال، في الولايات المتحدة، يُعتبر قانون مكافحة الاحتيال وإساءة استخدام الحواسيب، أحد أهم التشريعات التي تهدف إلى التصدي للهجمات السيبرانية، حيث يُجرّم القانون أي محاولة لاختراق الأنظمة الإلكترونية بطرق غير قانونية أو استخدامها في أنشطة تخريبية، ويشمل ذلك فرض عقوبات مشددة تتراوح بين الغرامات المالية والسجن، وذلك لضمان التعامل بحزم مع أي تهديدات رقمية قد تؤثر على الأفراد أو المؤسسات، كما تساهم هذه القوانين في تعزيز الأمن السيبراني على المستوى المحلي والدولي، حيث تضع إطاراً قانونياً واضحاً لملاحقة الجرائم الرقمية ومعاقبة مرتكبيها.

كما أنها تعزز الثقة في استخدام التكنولوجيا من خلال حماية الأفراد والمؤسسات من أي استغلال غير مشروع، ومع التطور السريع في مجال التقنية، أصبح تحديث هذه التشريعات أمراً ضرورياً لمواكبة الأساليب الحديثة التي يستخدمها المجرمون، مما يجعل التعاون بين الحكومات والمؤسسات الأمنية والتكنولوجية أمراً حيوياً لضمان بيئة إلكترونية أكثر أماناً⁽²⁰⁾.

وتلعب الاتفاقيات والمعاهدات الدولية دوراً أساسياً في تعزيز التعاون بين الدول لمكافحة الجرائم الإلكترونية التي تتجاوز الحدود الجغرافية، إذ تهدف هذه الاتفاقيات إلى وضع أطر قانونية موحدة تساعد في التصدي للتهديدات السيبرانية، وتعزز الأمن الرقمي على نطاق عالمي، ومن بين أبرز هذه الاتفاقيات، تأتي اتفاقية مجلس أوروبا لجرائم الحاسوب، التي تُعرف أيضاً باسم اتفاقية بودابست، وهي تُعد من أوائل الاتفاقيات الدولية، التي وضعت معايير واضحة لتجريم السلوكيات غير المشروعة في الفضاء الإلكتروني.

كما تسعى إلى توحيد القوانين والإجراءات الجنائية بين الدول الأعضاء لمكافحة الاختراقات الإلكترونية، والاحتيال الرقمي، وسرقة البيانات الحساسة، مما يسهل التعاون القضائي في تعقب الجناة وتقديمهم للعدالة، كما تمثل اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود مبادرة عالمية تهدف إلى التصدي للأنشطة الإجرامية التي تُرتكب عبر الإنترنت، حيث تركز هذه الاتفاقية على مكافحة الجرائم السيبرانية التي تُستخدم كوسيلة لدعم أنشطة غير مشروعة، مثل الاتجار بالبشر، وغسل الأموال، وتمويل الإرهاب، وتعتمد الاتفاقية على تعزيز التعاون بين الدول الأعضاء، وتسهيل تبادل المعلومات، وتطوير آليات

قانونية تُمكن الأجهزة الأمنية من ملاحقة مرتكبي هذه الجرائم في أي مكان بالعالم.

ومن خلال هذه الاتفاقيات وغيرها يتم توفير بيئة قانونية تساعد الحكومات على اتخاذ إجراءات صارمة ضد المجرمين، كما أنها تعزز التنسيق بين مختلف الجهات المعنية لمواجهة التطورات السريعة في أساليب الجرائم الإلكترونية، ومع تزايد التهديدات الرقمية، إذ أصبح الالتزام بهذه المعاهدات أمرًا ضروريًا لضمان حماية الأفراد والمؤسسات، وتعزيز أمن الفضاء الإلكتروني على مستوى العالم⁽²¹⁾.

كما تمثل هذه التشريعات دورًا محوريًا في توحيد الأطر القانونية على مستوى العالم، مما يساهم في تعزيز الحماية الرقمية للأفراد والمؤسسات، وتعد القوانين الأوروبية من أبرز الأمثلة على ذلك، حيث يحرص الاتحاد الأوروبي على تطوير تشريعات صارمة لحماية البيانات الشخصية، وضمان الخصوصية في البيئة الرقمية، ومن أبرز هذه التشريعات اللائحة العامة لحماية البيانات (GDPR)، التي تضع معايير واضحة لكيفية جمع البيانات الشخصية، ومعالجتها، وتخزينها، ونقلها.

وتهدف هذه القوانين إلى تعزيز حقوق المستخدمين، وإلزام الشركات والمؤسسات باتباع إجراءات صارمة تضمن أمان المعلومات، مع فرض عقوبات مشددة على الجهات التي تخالف هذه اللوائح، إذ يمكن ربط هذه التشريعات بالجهود التي تبذلها دولة قطر في مكافحة الجرائم الإلكترونية، حيث تعمل الدولة على تعزيز التعاون مع المنظمات الإقليمية والدولية من خلال تبادل المعلومات والخبرات في هذا المجال.

كما أن المشاركة في الاتفاقيات لمكافحة جرائم الإنترنت تساهم في دعم الجهود القطرية لمواجهة التحديات المتزايدة المرتبطة بالهجمات السيبرانية، ويساعد هذا التعاون في تحسين الأطر القانونية المحلية، وتبني أفضل الممارسات العالمية التي تعزز الأمن السيبراني في البلاد، كما تستفيد الدولة من التشريعات عبر دراسة التجارب الناجحة في الدول المتقدمة في مجال الحماية الرقمية، مما يتيح تطوير قوانين وطنية متوافقة مع المعايير العالمية، كما تساهم المشاركة في المؤتمرات والمنتديات المعنية بالأمن السيبراني في تبادل الأفكار والتقنيات الحديثة لمكافحة الجرائم الإلكترونية، ويساهم هذا التفاعل في بناء شراكات قوية وتعزيز القدرات المحلية لمواجهة التهديدات الرقمية، مما يعكس التزام الدولة بتحديث أنظمتها القانونية لمواكبة التطورات السريعة في المجال الرقمي، وتعزيز الأمن المعلوماتي على المستويين الوطني والدولي⁽²²⁾.

المبحث الثاني: الآثار الناجمة عن الجرائم المعلوماتية

مع التطور السريع في التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية في مختلف مجالات الحياة، أصبحت الجرائم الإلكترونية واحدة من أخطر التهديدات التي تواجه الأفراد والمؤسسات والدول، حيث يعتمد المجرمون على تقنيات حديثة لاختراق الشبكات، وسرقة البيانات، والتلاعب بالمعلومات، مما يجعل أمن المعلومات عرضة للخطر.

وتشمل هذه الجرائم أشكالاً متعددة مثل القرصنة، والاحتيال الإلكتروني، والهجمات السيبرانية على البنية التحتية الرقمية، والتجسس الإلكتروني، والتعدي على الخصوصية، مما يؤدي إلى خسائر مالية كبيرة للأفراد والحكومات والشركات، وتنعكس هذه الجرائم بشكل مباشر على أمن المعلومات، حيث تؤثر على سرية البيانات وسلامتها وتوافرها،

فقد يؤدي اختراق قاعدة بيانات شركة ما إلى تسريب معلومات حساسة تخص العملاء، مما يؤثر على سمعة المؤسسة ويضعها أمام تحديات قانونية كبيرة، كما يمكن أن تتسبب الهجمات الإلكترونية في تعطيل أنظمة حكومية أو مؤسسية، مما يؤثر على تقديم الخدمات الحيوية، ويهدد الاستقرار الاقتصادي والأمني، لذا أصبح من الضروري تطوير استراتيجيات فعالة لمكافحة هذه التهديدات وتعزيز الحماية السيبرانية من خلال سن قوانين صارمة، وتطبيق تقنيات متقدمة للكشف عن الجرائم الإلكترونية ومنعها، بالإضافة إلى توعية الأفراد والمؤسسات بأهمية اتباع ممارسات أمنية تحمي بياناتهم من التهديدات المتزايدة في العالم الرقمي وسوف نتناول مدى انعكاس الجريمة المعلوماتية بالمطلب الأول والسياسات الأمنية والوقائية للحد من الجريمة بالمطلب الثاني⁽²³⁾.

المطلب الأول: مدى انعكاس الجريمة المعلوماتية: لقد حققت الجريمة المعلوماتية انعكاسات خطيرة على مختلف المستويات، لا سيما من حيث الآثار السلبية التي تلحق بالأفراد والمؤسسات نتيجة الاختراقات الأمنية المتكررة، وتعد البرمجيات الخبيثة والفيروسات من أبرز الأدوات المستخدمة في تنفيذ هذه الجرائم، لما تسببه من تعطيل للأنظمة وسرقة للمعلومات، كما تُعد سرقة البيانات الشخصية من أخطر أشكال هذه الجرائم، لما يترتب عليها من انتهاك للخصوصية وابتزاز إلكتروني وأضرار مالية ونفسية، مما يستوجب تدخلاً تشريعياً وتقنياً عاجلاً للحد من تفاقم آثارها.

الفرع الأول: البرمجيات الخبيثة والفيروسات: تعد الفيروسات والبرمجيات الخبيثة من أخطر التهديدات التي تواجه الأنظمة الإلكترونية، حيث يمكنها التسلل إلى أجهزة الكمبيوتر والشبكات بطرق غير مشروعة والتسبب في أضرار جسيمة، وتؤثر هذه البرامج الضارة على استمرارية الأعمال وإنتاجية المؤسسات، وقد تؤدي إلى فقدان البيانات وتعطيل العمليات التشغيلية، مما ينعكس سلباً على الأداء العام ويهدد سلامة وأمن المعلومات، والفيروسات هي برامج ضارة مصممة للانتشار والتكاثر داخل

الأنظمة الإلكترونية، بينما تستهدف البرمجيات الخبيثة إلحاق الضرر بالمستخدمين والأنظمة من خلال سرقة المعلومات أو تدميرها، غالبًا ما يعتمد المخترقون على استغلال الثغرات الأمنية في البرمجيات أو التطبيقات أو الأجهزة للدخول إلى الأنظمة وتنفيذ أنشطتهم غير المشروعة، ومن خلال ذلك، يمكن لهذه البرمجيات تعطيل الأنظمة، إتلاف الملفات، سرقة البيانات الحساسة مثل المعلومات المالية أو الشخصية، والتحكم في الأجهزة عن بُعد، مما يعرض الأفراد والمؤسسات لخسائر كبيرة، سواء على المستوى المالي أو الأمني، وللمحد من هذه المخاطر يجب على المستخدمين والمؤسسات اتخاذ تدابير وقائية فعالة، مثل تحديث البرمجيات والأنظمة بشكل دوري، واستخدام برامج مكافحة الفيروسات، وتطبيق سياسات أمنية صارمة، بالإضافة إلى النسخ الاحتياطي للبيانات وتوعية الموظفين حول كيفية اكتشاف التهديدات الإلكترونية والتعامل معها بفعالية، يساعد ذلك في الحد من فرص نجاح الهجمات السيبرانية، وتقليل الخسائر المحتملة الناتجة عنها⁽²⁴⁾.

الفرع الثاني: سرقة البيانات الشخصية: تُعد سرقة البيانات الشخصية من أخطر التهديدات التي تواجه أمن المعلومات والخصوصية في العصر الرقمي، حيث يستهدف المجرمين أنظمة الحواسيب والشبكات لاخترافها بطرق غير مشروعة، مما يتيح لهم الوصول إلى بيانات حساسة وسرية.

ومن بين أكثر المخاطر شيوعًا، سرقة المعلومات الشخصية للعملاء، بما في ذلك بيانات الدفع الإلكتروني، ومعلومات الحسابات المصرفية، وبيانات الائتمان، وهو ما يؤدي إلى انتهاك الخصوصية، والتسبب في خسائر مالية جسيمة، وفقد ثقة العملاء بالمؤسسات التي تعرضت للهجمات، ويعتمد القراصنة على استغلال الثغرات الأمنية في الأنظمة الرقمية للوصول إلى الشبكات الداخلية وسرقة البيانات، وقد يتم ذلك من خلال تقنيات متطورة مثل هجمات التصيد الاحتيالي، أو استغلال نقاط الضعف في البرمجيات، أو زرع برمجيات خبيثة داخل الأنظمة، وبمجرد نجاحهم في اختراق النظام، يصبح بإمكانهم استخدام البيانات المسروقة لأغراض غير قانونية، مثل الاحتيال المالي، أو بيعها في الأسواق السوداء الرقمية، ما يعرض الضحايا لمخاطر متعددة تتراوح بين الاستغلال المالي وسرقة الهوية الرقمية، ولخطورة هذا النوع من الجرائم فقد تبني المشرع القطري بالمادة الثانية والثالثة من القانون جريمة الدخول غير المشروع إلى الأنظمة الإلكترونية.

مما يؤكد التزام الدولة بحماية المعلومات الرقمية وضمان أمنها، وبفضل هذه التشريعات الصارمة، تلعب دولة قطر دورًا حيويًا في تعزيز الأمن السيبراني من خلال وضع إطار قانوني متين يردع الجرائم الإلكترونية، كما تسعى السلطات المختصة إلى تطوير آليات مستمرة لمراقبة الجرائم الرقمية، وتعزيز قدرات إنفاذ القانون لملاحقة المجرمين، بالإضافة إلى تشجيع المؤسسات على اعتماد أفضل ممارسات الحماية السيبرانية، مثل تشفير البيانات، وتحديث الأنظمة الأمنية، والتوعية بمخاطر الهجمات الإلكترونية، مما يساهم في بناء بيئة إلكترونية آمنة تحمي الأفراد والمؤسسات من التهديدات الرقمية المتزايدة⁽²⁵⁾.

الفرع الثالث: الآثار السلبية على الأفراد والمؤسسات: تعد الهجمات الإلكترونية تهديداً كبيراً على الأفراد والمؤسسات، حيث لا تقتصر أضرارها على اختراق البيانات وسرقة المعلومات فحسب، بل تمتد لتشمل خسائر مالية فادحة وتأثيرات سلبية على السمعة والمصداقية، عند تعرض أي مؤسسة لهجوم إلكتروني، فإنها تتحمل تكاليف باهظة لاستعادة بياناتها وإصلاح الأضرار التي لحقت بأنظمتها.

ويتطلب ذلك استثماراً كبيراً في استعادة الخوادم والملفات المتضررة، إلى جانب الإنفاق على تحسين البنية الأمنية لمنع حدوث هجمات مستقبلية، كما أن تعطيل العمليات التشغيلية أثناء التعامل مع الاختراق، يؤدي إلى خسائر مالية إضافية، نتيجة توقف الإنتاجية، وتعطل الخدمات لفترة قد تطول بحسب حجم الهجوم ومدى تأثيره، كما تؤثر الهجمات الإلكترونية بشكل مباشر على سمعة الشركات والمؤسسات، عندما يفقد العملاء والشركاء الثقة في قدرة الشركة على حماية بياناتهم، فإن ذلك يؤدي إلى تراجع مستوى التعامل معها، مما يؤثر على ولاء العملاء ويقلل من فرص جذب مستثمرين جدد.

كما أن تسرب المعلومات الحساسة قد يتسبب في أضرار قانونية وإجراءات قضائية قد تزيد من تعقيد الأوضاع وتكبد المؤسسة المزيد من الخسائر، لذا فإن الحفاظ على الأمن السيبراني لا يعد مجرد خيار، بل هو ضرورة لضمان استمرارية الأعمال وحماية السمعة المؤسسية من أي انتكاسات تؤثر على نجاحها في السوق⁽²⁶⁾.

المطلب الثاني: السياسات الأمنية والوقائية للحد من الجريمة: تُعد السياسات الأمنية والوقائية من الأدوات الفاعلة في مكافحة الجريمة بمختلف أشكالها، وخاصة الجريمة المعلوماتية التي باتت تشكل تحدياً متزايداً على المستويين الوطني والدولي، ويتركز دور هذه السياسات في تعزيز أمن المعلومات عبر تبني تقنيات متطورة، ووضع ضوابط فعالة لحماية الأنظمة الرقمية من التهديدات السيبرانية، كما يُعتبر الوعي السيبراني حجر الزاوية في الوقاية، إذ يُمكن الأفراد والمؤسسات من التعرف على المخاطر المحتملة واتخاذ إجراءات الحيلة اللازمة، ولا يخفى الدور الحيوي للسياسات التوعوية والتعليمية، التي تسعى إلى نشر ثقافة أمنية شاملة عبر حملات توعية ومناهج تعليمية مخصصة، لتعزيز القدرات الوقائية على المدى الطويل، ومن خلال هذه المحاور المتكاملة، يمكن تحقيق بيئة أمنية مستدامة قادرة على الحد من الجريمة بكفاءة وفاعلية.

الفرع الأول: تعزيز أمن المعلومات: لحماية الأنظمة الرقمية من التهديدات الإلكترونية، لابد من تبني استراتيجيات فعالة تضمن الوقاية من الهجمات وتعزيز الأمن السيبراني، ويتطلب ذلك اعتماد مجموعة من الممارسات التي تساهم في تقليل المخاطر، مثل تحديث الأنظمة والبرمجيات بشكل مستمر لضمان عدم وجود ثغرات أمنية يمكن استغلالها، كما أن استخدام وسائل الحماية المتقدمة، كبرامج مكافحة الفيروسات والجدران النارية، يساعد في التصدي لأي محاولات اختراق غير مشروعة، ومن الضروري توعية المستخدمين بأفضل الممارسات الأمنية، مثل تجنب الروابط المشبوهة، وعدم مشاركة المعلومات الحساسة مع جهات غير موثوقة.

ونلاحظ أن قانون مكافحة الجرائم الإلكترونية القطري نص على عقوبات صارمة بحق الأفراد الذين يحاولون اختراق الأنظمة أو سرقة البيانات، مما يعكس التزام الدولة بحماية أمنها الرقمي، كما يمنع القانون أي انتهاك للخصوصية أو إفشاء معلومات حساسة دون تصريح، وذلك لضمان سرية البيانات ومنع إساءة استخدامها، فرض القانون ضوابط صارمة على مزودي الخدمات الإلكترونية لضمان التزامهم بمعايير الأمن الرقمي، حيث يتعرض المخالفون لغرامات مالية أو عقوبات قانونية، كما يمنح القانون الجهات المختصة الحق في مصادرة أي أجهزة أو برامج تُستخدم في الجرائم الإلكترونية، مما يشكل رادعاً لمنع ارتكاب هذه الأفعال غير القانونية، وبفضل هذه الإجراءات والتشريعات، تتمتع دولة قطر بإطار قانوني قوي يساعد في مواجهة التحديات السيبرانية، ويحمي الأفراد والمؤسسات من المخاطر التي تهدد أمن المعلومات⁽²⁷⁾.

الفرع الثاني: أهمية الوعي السيبراني: مع التوسع المستمر في استخدام التكنولوجيا وتزايد الهجمات الإلكترونية، أصبح تعزيز الوعي السيبراني وتدريب الأفراد والمؤسسات على أساليب الحماية من الجرائم الإلكترونية أمراً ضرورياً لضمان الأمن الرقمي، حيث يساهم التدريب المستمر في تمكين الأفراد من فهم طبيعة التهديدات الإلكترونية المختلفة، مثل محاولات الاختراق وهجمات التصيد الاحتيالي، ويمنحهم القدرة على التصرف بوعي عند التعامل مع البيانات الحساسة، فالمعرفة الجيدة بالمخاطر السيبرانية تساعد في الحد من فرص تعرض المعلومات للاختراق، وتحافظ على استقرار وأمان الأنظمة الرقمية المستخدمة في مختلف القطاعات، لذا فإن توفير برامج تدريبية متخصصة في مجال الأمن السيبراني يرفع مستوى الجاهزية لدى المؤسسات لمواجهة أي تهديدات محتملة، حيث يؤدي ذلك إلى تعزيز القدرة على اكتشاف الهجمات الإلكترونية مبكراً واتخاذ التدابير اللازمة للحد من آثارها.

كما أن توعية الموظفين بالممارسات الأمنية الصحيحة، مثل استخدام كلمات مرور قوية وعدم مشاركة المعلومات السرية عبر الإنترنت، يساهم في تقليل احتمالية تعرض الشركات لعمليات الاحتيال أو سرقة البيانات، مما يعزز من قدرتها على الاستمرار في العمل دون مخاطر تهدد استقرارها، فإن الاستثمار في تطوير المهارات السيبرانية لا يقتصر على الحماية فقط، بل

يسهم في تعزيز الابتكار في مجال الأمن الرقمي، حيث يفتح المجال أمام تطوير حلول وتقنيات جديدة لمواجهة التحديات المتزايدة في الفضاء الإلكتروني، وهذا بدوره يعزز من مكانة الدولة في مجال التكنولوجيا الحديثة، ويدعم بناء اقتصاد رقمي قوي وآمن، كما أن نشر الوعي السيبراني على نطاق واسع يزيد من ثقة المستخدمين في البيئة الرقمية، مما يشجع على تبني التكنولوجيا بشكل أكثر أماناً ويعزز التحول الرقمي في مختلف القطاعات الحكومية والخاصة⁽²⁸⁾.

الفرع الثالث: السياسات التوعوية والتعليمية: تُعد السياسات التوعوية والتعليمية ركيزة أساسية في منظومة مكافحة الجريمة المعلوماتية، إذ تركز على بناء وعي مجتمعي شامل حول مخاطر الفضاء الإلكتروني وسبل الوقاية الفعالة، من هذا المنطلق تُعتمد حملات توعية موجهة بدقة لكل من الأفراد والمؤسسات، تتناول أهم الممارسات الأمنية الرقمية، مثل حماية البيانات الشخصية، واستخدام كلمات مرور قوية، والامتناع عن التعامل مع الروابط المشبوهة، مما يسهم في تقليل فرص استهداف الفاعلين الإجراميين⁽²⁹⁾.

كما يكتسب إدماج مفاهيم الأمن السيبراني في المناهج التعليمية أهمية بالغة، حيث يبدأ تعليم الطلبة منذ المراحل المبكرة بفهم أساسيات الأمن الرقمي، والتعرف على التهديدات الإلكترونية، وبناء ثقافة احترام الخصوصية والسلامة الرقمية، مما يؤسس لجيل واعٍ قادر على التعامل مع التكنولوجيا بمسؤولية وحذر⁽³⁰⁾.

علاوة على ذلك، يلعب الإعلام دوراً محورياً في نشر الثقافة الوقائية من الجرائم الإلكترونية عبر مختلف الوسائل المرئية والمسموعة والمكتوبة، من خلال تقديم برامج توعوية، ومقالات، وتقارير إخبارية، فضلاً عن استخدام وسائل التواصل الاجتماعي للوصول إلى أوسع شريحة ممكنة من الجمهور. ويعزز الإعلام كذلك من الدور المجتمعي في التحذير من الأساليب الاحتيالية والتقنيات الخبيثة، مما يساهم في بناء مناخ أمني أكثر تماسكاً واستجابة للتحديات الرقمية المتزايدة⁽³¹⁾.

الخلاصة:

مع تزايد الاعتماد على التكنولوجيا والاتصال الرقمي، أصبحت الجرائم الإلكترونية تشكل تهديدًا متناميًا يؤثر على الأفراد والمؤسسات والدول، فالتطور السريع في مجال التقنية لم يأت دون تحديات، حيث استغل مجرمو الإنترنت الثغرات الأمنية لاستهداف نظم المعلومات والشبكات والمواقع الإلكترونية بطرق متعددة، مما أدى إلى تصاعد الحاجة إلى استراتيجيات فعالة لحماية البيانات وتعزيز الأمن السيبراني.

وللتصدي لهذه الظاهرة، لا بد من تبني نهج متكامل يجمع بين التشريعات الصارمة والتعاون الدولي والتوعية المجتمعية، فسن القوانين التي تجرم هذه الأفعال وتفرض عقوبات رادعة يعد خطوة أساسية لضمان الحد من هذه الجرائم، كما أن تعزيز التعاون بين الدول والمؤسسات الأمنية يساهم في تعقب مرتكبي الجرائم الإلكترونية، والتصدي لها على نطاق واسع.

فإن التوعية الأمنية والتدريب المستمر يلعبان دورًا محوريًا في الوقاية من التهديدات السيبرانية، فكل فرد يتحمل مسؤولية حماية بياناته من الاختراق وسوء الاستخدام، لذا يجب على المؤسسات والأفراد تبني إجراءات أمنية متقدمة، مثل تحديث الأنظمة بانتظام، واستخدام برامج الحماية، وتعزيز الوعي بالمخاطر المحتملة، لذا فإن ضمان بيئة إلكترونية آمنة يتطلب التزامًا جماعيًا بالتقنيات الحديثة، والتدابير القانونية، والتعاون الدولي، مما يضمن فضاءً رقميًا أكثر أمانًا وثقة للجميع.

النتائج:

- كشف البحث عن تعدد وتنوع صور الجرائم الإلكترونية وتعقيداتها، وهو ما يستلزم فهماً عميقاً لطبيعة التهديدات التي تستهدف الأنظمة الرقمية، وضرورة الاستعداد لمواجهةها باستخدام وسائل تقنية متطورة.
- خلص البحث إلى أهمية سن تشريعات وطنية فعالة في دولة قطر لمكافحة هذه الجرائم، مع التأكيد على ضرورة مراجعتها وتحديثها بشكل مستمر بما يواكب التطورات التكنولوجية المتسارعة.
- سلط البحث الضوء على الدور الجوهري الذي تؤديه الاتفاقيات الدولية في تحقيق العدالة، من خلال تسهيل التعاون القضائي بين الدول وتعزيز الثقة المتبادلة، وهو ما يساهم في بناء علاقات قوية ومستدامة في مجالي الأمن والعدالة.
- بيّن البحث إسهام الاتفاقيات الدولية في دعم القدرات الوطنية للدولة، عبر توفير برامج تدريبية متقدمة، وتبني أحدث الوسائل التقنية، بما يعزز من بناء منظومة أمنية متكاملة وفعالة في مواجهة التهديدات السيبرانية.

الاقتراحات

- تعزيز التعاون الدولي بين الدول والمنظمات العالمية، حيث يُعد التنسيق المشترك وتبادل المعلومات أداة أساسية في مواجهة الجرائم الإلكترونية التي تتجاوز الحدود، فالتعاون الفعال يتيح تبادل الخبرات والموارد لتطوير حلول أكثر كفاءة للتعامل مع هذه التهديدات.

- ضرورة تكثيف برامج التدريب والتوعية بين الجهات الأمنية، والمؤسسات الحكومية، والشركات، والأفراد، مما يعزز قدرة المجتمع على التصدي لها بشكل استباقي.

- لا بد من تطوير التشريعات الوطنية بشكل مستمر لتتماشى مع التطورات التقنية الحديثة.

- تحسين آليات الإنابة القضائية يساهم في تعقب الجناة، وتقديمهم للعدالة، ويحدّ من انتشار الجرائم الإلكترونية.

قائمة المراجع:

أولاً: كتب

- 1- د. عبد الله النوايسة، جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، 2017.
- 2- د. يوسف الشيخ، د. محمود أحمد، سعيد سالم، زايد حمد، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات، سلطنة عمان، الأمانة العامة لدول مجلس التعاون، 2016.

ثانياً: بحوث ورسائل علمية:

- 1- سامي جاد عبد الرحمن، التعاون الدولي في مكافحة الجرائم المنظمة، مجلة العلوم القانونية والاقتصادية، المجلد 60، العدد 1، يناير/2018.
- 2- نسرين سلامة، الجرائم الإلكترونية وأثرها على المجتمع، مجلة القاهرة للخدمة الاجتماعية، العدد 39، 2023.
- 3- عمر محمود حمدان، وأحمد محمد عبد الرحيم اللوزي، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، عمان، 2023.
- 4- حرز محمد، جرائم الأنترنت وتحديات الأمن السيبراني، دراسة في متغيرات الجريمة ومقارباتها العلاجية، مجلة المفكر، المجلد 18، العدد 1، 2023.
- 5- د. كمال الدين مصطفى، محل جرائم العدوان على حقوق الملكية الفكرية الإلكترونية وصورها، مجلة الدراسات القانونية والاقتصادية، 2024.
- 6- مائنو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، المجلد 4، العدد 1، 2022/7.
- 7- حياة جاحض، الدليل الإلكتروني في الجرائم المعلوماتية، مجلة الباحث للدراسات القانونية والقضائية، العدد 52، 2023.
- 8- ياكور الطاهر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، المجلد 4، العدد 4، ديسمبر/2022.

- 9- فاضل عائشة، المسؤولية الجزائية في الجرائم الإلكترونية، مجلة الحقوق والحريات، المجلد 11، العدد 1، 2023.
- 10- ليفة ميلود، أحكام الإلتلاف الفيروسي للبرامج والبيانات الإلكترونية، مجلة البحوث والدراسات، المجلد 13، العدد 2، 2016.
- 11- أكرام سليمان، الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن، جامعة قطر، كلية القانون، رسالة ماجستير، 2021.
- 12- عبد الرحيم وهيب، بن سعيد أمين، عبد الرحيم، نادية، الجرائم الإلكترونية من خلال مؤشرات عالمية وآثارها على المؤسسات، مجلة دراسات العدد الاقتصادي، المجلد 10، العدد 1، 2019.
- 13- أ. د. دليلا خينش، د. سعاد خينش، التعدي على الخصوصية وتحديات الأمن المعلوماتي، مجلة رقمنة للدراسات الإعلامية و الاتصالات، المجلد 3، العدد 1، مارس/2023.

ثالثاً: تشريعات:

14- قانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية.

رابعاً: مراجع أجنبية

- 15- H.R.4718 - Computer Fraud and Abuse Act of 1986 .
- 16- Wang, J., & Lu, Y. (2020). Cybersecurity awareness and education: A comprehensive review of the literature. Computers & Security .
- 17- Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking, .

الموامش:

- 1 سامي جاد عبد الرحمن، التعاون الدولي في مكافحة الجرائم المنظمة، مجلة العلوم القانونية والاقتصادية، المجلد 60، العدد 1، يناير/2018، ص 198.
- 2 نسرين سلامة، الجرائم الإلكترونية وأثرها على المجتمع، مجلة القاهرة للخدمة الاجتماعية، العدد 39، 2023، ص 404.
- 3 قانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية.
- 4 نسرين سلامة، الجرائم الإلكترونية وأثرها على المجتمع، مجلة القاهرة للخدمة الاجتماعية، مرجع سابق، ص 405.
- 5 د. عبدالاله النوايسة، جرائم تكنولوجيا المعلومات شرح الاحكام الموضوعية في قانون الجرائم الإلكترونية، 2017، ص 230.
- 6 عمر محمود حمدان، وأحمد محمد عبد الرحيم اللوزي، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، عمان، 2023، ص 88.
- 7 حرز محمد، جرائم الانترنت وتحديات الأمن السيبراني، دراسة في متغيرات الجريمة ومقارباتها العلاجية، مجلة المفكر، المجلد 18، العدد 1، 2023، ص 73.
- 8 د. كمال الدين مصطفى، محل جرائم العدوان على حقوق الملكية الفكرية الإلكترونية وصورها، مجلة الدراسات القانونية والاقتصادية، 2024، ص 1477.
- 9 مانيو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مجلة القانون والتنمية، المجلد 4، العدد 1، 2022/7، ص 27.
- 10 مانيو جيلالي، عروس كوثر، الجريمة السيبرانية في صورها المستحدثة، مرجع سابق، ص 31.

- 11 عمر محمود حمدان، وأحمد محمد عبد الرحيم اللوزي، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية، مرجع سابق، ص 91.
- 12 حياة جاحض، الدليل الإلكتروني في الجرائم المعلوماتية، مجلة الباحث للدراسات القانونية والقضائية، العدد 52، 2023، ص 57.
- 13 نصوص المواد رقم 2، 3، 10، 13، من قانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري.
- 14 نصوص المواد رقم 2، 3، مرجع سابق.
- 15 نصوص المواد رقم 4، 5، 7، مرجع سابق.
- 16 نصوص المواد رقم 8، 9، مرجع سابق.
- 17 ياكور الطاهر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مجلة الصدى للدراسات القانونية والسياسية، المجلد 4، العدد 4، ديسمبر/2022، ص 15.
- 18 ياكور الطاهر، مكافحة الجرائم الإلكترونية بين التشريعات الوطنية والاتفاقيات الدولية، مرجع سابق، ص 17، 18.
- 19 د. يوسف الشيخ، د. محمود أحمد، سعيد سالم، زايد حمد، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مجمع البحوث والدراسات، سلطنة عمان، الأمانة العامة لدول مجلس التعاون، 2016، ص 23.
- 20 H.R.4718 - Computer Fraud and Abuse Act of 1986.
- 21 حياة جاحض، الدليل الإلكتروني في الجرائم المعلوماتية، مرجع سابق، ص 68.
- 22 نسرین سلامة، الجرائم الإلكترونية وأثرها على المجتمع، مجلة القاهرة للخدمة الاجتماعية، مرجع سابق، ص 410.
- 23 فاضل عائشة، المسؤولية الجزائية في الجرائم الإلكترونية، مجلة الحقوق والحريات، المجلد 11، العدد 1، 2023، ص 617.
- 24 ليفة ميلود، أحكام الإتلاف الفيروسي للبرامج والبيانات الإلكترونية، مجلة البحوث والدراسات، المجلد 13، العدد 2، 2016، ص 66، 67.
- 25 أكرام سليمان، الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن، جامعة قطر، كلية القانون، رسالة ماجستير، 2021، ص 65، 66.
- 26 عبدالرحيم وهيب، بن سعيد أمين، عبدالرحيم، نادية، الجرائم الإلكترونية من خلال مؤشرات علمية وآثارها على المؤسسات، مجلة دراسات العدد الاقتصادي، المجلد 10، العدد 1، 2019، ص 42.
- 27 أ.د. دليلة خينش، د. سعاد خينش، التعدي على الخصوصية وتحديات الأمن المعلوماتي، مجلة رقمنة للدراسات الإعلامية و الاتصالات، المجلد 3، العدد 1، مارس/2023، ص 54.
- 28 د. يوسف الشيخ، د. محمود أحمد، سعيد سالم، زايد حمد، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، مرجع سابق، ص 86، 87.
- 29 Wang, J., & Lu, Y. (2020). Cybersecurity awareness and education: A comprehensive review of the literature. Computers & Security, P10.
- 30 Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking, P75.
- 31 Hadnagy, C. (2018), P95.