جمهوريـــة العـــراق
وزارة التعليم العالي والبحث العلمي
جامعة المستقبل
كلية القانون

المواجهـــة الجنائيـــة للجرائـــم المعلوماتيـــة

بحث مقدم الى مجلس جامعة المستقبل - كلية القانون وهو جزء من متطلبات نيل شهادة البكالوريوس في قسم القانون

اعداد الطالبة

سارة رياح حسن موسى

إشراف

م.م محمد حمزة عيدان

1446 هـ

2025م

قُلْ إِنَّمَا حَرَّمَ رَبِّيَ الْفَوَاحِشَ مَا ظَهَرَ مِنْهَا وَمَا بَطَنَ وَالْإِثْمَ وَ
الْبَغْيَ بِغَيْرِ الْحَقِّ وَأَن تُشْرِكُوا بِاللَّهِ مَا لَمْ يُنَزِّلْ بِهِ سُلْطَانًا
وَأَن تَقُولُوا عَلَى اللَّهِ مَا لَا تَعْلَمُونَ .

صدق الله العلي العظيم

سورة ﴿الأعراف- 33﴾

الاهداء

أهدي بحثي هذا الى :

- إلى . . . خاتم الأنبياء والمرسلين . . . معلمنا وقدوتنا محمد المصطفى (صلى الله عليه واله) . إلى . . . شهداء العراق الذين قدموا الغالي والنفيس وضحوا بأنفسهم من اجل تربة عراقنا الحبيب.
- ايقونة الحنان ، الى القلب النابض بالحب والصدر الدافئ التي أرضعتني الوفاء والصبر على الملمات والعطاء الدائم . أمي وهل قبلها او بعدها حب
- حزام الظهر والسند الدائم أخوتي عوني على الملمات والشدائد
- جميع أهلي وكل وأصدقائي، إليهم جميعاً

الباحثة

شكر وامتنان

من لا يشكر الناس . . . لا يشكر الله تتقدم بالشكر أولاً وأخيراً لله سبحانه وتعالى الذي وفقنا في انجاز هذا البحث الى الاستاذ الفاضل والمربي الكبير الذي رافق مشوار بحثنا الى من كان قلبه على قلبنا الى الاستاذ (م . م محمد حمزة عيدان) وأتوجه بالشكر والعرفان الى كلية القانون التي احتضنتني و طيلة السنين الماضية عرفانا .

فشكراً لكم جميعاً

الباحثة

المستخلص

الجرائم المعلوماتية تعد من التحديات الكبرى التي تواجه الأنظمة القانونية في العصر الحالي، وذلك بسبب الاعتماد المتزايد على التكنولوجيا في كافة المجالات الحياتية. هذه الجرائم تشمل مجموعة من الأنشطة غير القانونية التي تتم عبر الوسائل الإلكترونية مثل القرصنة الإلكترونية، التجسس على البيانات، الاحتيال المالي عبر الإنترنت، والتشهير الإلكتروني. مع تطور هذه الجرائم وتنوعها، أصبح من الضروري أن تكون هناك استراتيجيات قانونية وتقنية فعالة لمواجهتها.

من أبرز جوانب المواجهة الجنائية لهذه الجرائم هو الأطر القانونية التي تنظم مكافحة الجرائم المعلوماتية. حيث تحتاج الدول إلى سن قوانين متخصصة لحماية الأفراد والمؤسسات من التهديدات الرقمية. في هذا السياق، هناك العديد من القوانين الوطنية والدولية التي تم تبنيها لمكافحة هذه الجرائم، مثل قانون مكافحة الجرائم الإلكترونية الذي يعمل على تعريف وتحديد أنواع الجرائم الموجهة ضد الأنظمة المعلوماتية. كما تسهم الاتفاقيات الدولية، مثل اتفاقية بودابست، في تنسيق الجهود بين الدول لمكافحة الجرائم المعلوماتية عبر الحدود.

التقنيات الحديثة تلعب دورًا محوريًا في مواجهة الجرائم الإلكترونية. التحقيق الجنائي الرقمي أصبح ضرورة للكشف عن الأدلة التي يمكن أن تساعد في إدانة مرتكبي الجرائم الإلكترونية. يشمل ذلك تحليل الأجهزة الرقمية مثل الحواسيب والهواتف الذكية وكذلك تتبع الأنشطة المشبوهة عبر الشبكة. كما أن الاستجابة السريعة للحوادث الإلكترونية تساهم بشكل كبير في تقليل الأضرار الناتجة عن الهجمات الإلكترونية، حيث تركز على منع أو تقليل تأثير الهجمات في الوقت الفعلي.

على الرغم من هذه الجهود، فإن هناك العديد من التحديات التي تواجه مواجهة الجرائم المعلوماتية. من أبرز هذه التحديات الخصوصية، حيث يجب موازنة حقوق الأفراد في الخصوصية مع الحاجة إلى التحقيقات الجنائية. إضافة إلى ذلك، فإن الجرائم الإلكترونية غالبًا ما تتجاوز الحدود الوطنية، مما يجعل التعاون بين الدول أمرًا معقدًا. كما أن سرعة تطور

التكنولوجيا تجعل من الصعب على الأنظمة القانونية والجنائية متابعة التغيرات المستمرة في أساليب الجريمة الرقمية.

تلعب المؤسسات الحكومية دورًا رئيسيًا في مواجهة هذه الجرائم من خلال التنسيق بين أجهزة الشرطة الإلكترونية والمحاكم والهيئات المعنية بحماية البيانات. تتطلب مكافحة الجرائم الإلكترونية تعاونًا بين جميع الأطراف، بما في ذلك القطاع الخاص، حيث أن العديد من الهجمات تستهدف الشركات والمؤسسات الخاصة.

قائمة المحتويات

المقدمة

تعتبر الجرائم المعلوماتية من أبرز القضايا التي تهم الأفراد والمجتمعات في العصر الحديث، مع انتشار استخدام التكنولوجيا والتواصل عبر الإنترنت بشكل غير مسبوق. مع تزايد الاعتماد على الأنظمة الرقمية في شتى مجالات الحياة، أصبح من الضروري مواجهة التهديدات التي تهدد الخصوصية والأمن الرقمي. لقد برزت أنواع جديدة من الجرائم التي تتم عبر الفضاء الإلكتروني، مثل القرصنة، الاحتيال، والاعتداء على البيانات الشخصية، مما يستدعي تطوير أساليب قانونية وتقنية فعالة لمكافحة هذه الجرائم وحماية الأفراد والمؤسسات.

أولاً: – موضوع البحث

يدور هذا البحث حول المواجهة الجنائية للجرائم المعلوماتية، حيث يركز على استعراض التشريعات القانونية المتعلقة بهذه الجرائم، ودور المؤسسات القانونية والتقنية في التحقيق وملاحقة الجناة. كما يتناول تطور الجرائم الإلكترونية وأساليب المكافحة المتبعة من قبل السلطات، بالإضافة إلى استعراض التحديات التي تواجه المواجهة الجنائية في هذا المجال.

ثانياً :– أهمية البحث

تتزايد أهمية هذا البحث في ظل تفشي الجرائم الإلكترونية وتأثيرها الكبير على الأفراد والمجتمعات، سواء على مستوى الأمان الشخصي أو الأمن الوطني. كما يسلط الضوء على ضرورة تطوير الأطر القانونية والتقنية لمواكبة تطور الجرائم الرقمية، ويوفر دراسة معمقة حول كيفية تحقيق التوازن بين حماية الخصوصية ومكافحة الجريمة الإلكترونية. يساهم البحث في تقديم رؤية شاملة لكيفية مواجهة الجرائم المعلوماتية وتعزيز فعالية الأنظمة القانونية في هذا المجال.

ثالثاً :– مشكلة البحث

تتمثل مشكلة البحث ، في تزايد الجرائم المعلوماتية التي تهدد الأفراد والمجتمعات بشكل مستمر، في الوقت الذي يواجه فيه النظام القانوني تحديات كبيرة في مواكبة هذا النوع من الجرائم المعقدة

والمتطورة. تكمن المشكلة في صعوبة تحديد نطاق الجريمة الإلكترونية، صعوبة التحقيق فيها عبر الحدود الدولية، بالإضافة إلى التحديات المتعلقة بحماية الخصوصية وحقوق الأفراد في العصر الرقمي. وكذلك من الاشكاليات الاخرى هو نقص التنسيق بين الأنظمة القانونية المختلفة في مواجهة هذه الجرائم.

رابعاً :- منهجية البحث

اعتمد هذا البحث على منهجية تحليلية وصفية، حيث تم دراسة الأدبيات القانونية والتقارير والموارد الرقمية المتعلقة بالجرائم المعلوماتية. وقد تم جمع البيانات من خلال مراجعة التشريعات المحلية والدولية المتعلقة بالجرائم الإلكترونية، بالإضافة إلى تحليل آليات التحقيق والتقنيات المستخدمة في مواجهة هذه الجرائم. كما تم دراسة التجارب المختلفة للدول في التعامل مع الجرائم المعلوماتية لفهم أفضل للسياسات الفعالة في هذا المجال.

خامساً :- هيكلية البحث

يتكون البحث من ثلاثة مطالب رئيسية تبدأ بالمطلب الأول ، مفهوم الجرائم المعلوماتية ونتناول في الفرع الاول منه تعريف الجرائم المعلوماتية ، أما الفرع الثاني نتناول التمييز بين الجرائم المعلوماتية والجرائم التقليدية . اما المطلب الثاني ، اركان الجريمة المعلوماتية ونتناول في الفرع الأول منه الركن المادي للجريمة المعلوماتية اما الفرع الثاني ، الركن المعنوي للجريمة المعلوماتية . اما المطلب الثالث سوف نبحث في المواجهة الجنائية للجرائم المعلوماتية نتناول في الفرع الأول منه المواجهة الجنائية على مستوى التشريع الوطني اما الفرع الثاني: المواجهة الجنائية على مستوى التعاون الدولي .

المطلب الأول

مفهوم الجرائم المعلوماتية

الجرائم المعلوماتية تشير إلى الأفعال غير القانونية التي تُرتكب باستخدام التكنولوجيا الرقمية أو الإنترنت. تشمل هذه الجرائم مجموعة من الأنشطة مثل القرصنة، الاحتيال الإلكتروني، انتهاك الخصوصية، توزيع البرمجيات الضارة، والتلاعب بالبيانات. تمثل هذه الجرائم تهديدات للأفراد والشركات، حيث يمكن أن تؤدي إلى فقدان المعلومات الحساسة، الأضرار المالية، وتآكل الثقة في الأنظمة الرقمية. تتطلب مكافحة الجرائم المعلوماتية تعاوناً بين الحكومات والشركات والمستخدمين لتعزيز الأمان الرقمي. [1]

سوف نقسم هذا المطلب الى فرعين ، يتناول الفرع الاول تعريف الجرائم المعلوماتية والفرع الثاني يتناول التمييز بين الجرائم المعلوماتية والجرائم التقليدية وكالاتي :

الفرع الأول

تعريف الجرائم المعلوماتية

الجرائم المعلوماتية هي نوع من الجرائم التي ترتكب باستخدام تقنيات المعلومات الحديثة، مثل أجهزة الكمبيوتر، الإنترنت، والشبكات الرقمية. هذه الجرائم غالبًا ما تستهدف البيانات الرقمية، الأنظمة الإلكترونية، أو الأفراد عبر الإنترنت. وقد تطورت مع تطور التكنولوجيا وأصبحت تهديدًا كبيرًا في العصر الرقمي.[2] وان أنواع الجرائم المعلوماتية هي :

أنواع الجرائم المعلوماتية:

القرصنة (الهاكرز) والاختراق:

- القرصنة تعني محاولة الوصول غير المصرح به إلى الأنظمة أو الشبكات الرقمية.
- قد يقوم الهاكرز باختراق أنظمة الحواسيب أو مواقع الإنترنت بهدف سرقة البيانات أو تغييرها أو حتى إتلافها.[3]

([1]) أحمد أبو الروس، التحقيق الجنائي والتعرف فيه والادلة الجنائية، مرجع سابق، ص ١٥. أحمد المهدي، اشرف شافعي التحقيق الجنائي الابتدائي وضمانات المتهم وحمايتها، دار الكتب القانونية، المحلة، مصر، ٢٠٠٥م.

([2]) احمد سعد محمد الحسيني الجوانب الاجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية رسالة دكتوراه، كلية الحقوق جامعة عين شمس، ٢٠١٢م.

([3]) الاستاذه بوعناد فاطمة زهرة مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية ، الجزائر ، العدد الأول، ٢٠١٣م.

- على سبيل المثال، اختراق الأنظمة البنكية لسرقة أموال أو بيانات العملاء.

والتصيد الإلكتروني:(Phishing)

- هو استخدام أساليب خادعة عبر الإنترنت للحصول على معلومات حساسة مثل كلمات المرور، أرقام بطاقات الائتمان، أو تفاصيل الحسابات البنكية.[1]
- يتم ذلك عادةً عبر إرسال رسائل بريد إلكتروني أو روابط مزيفة تشبه المواقع الحقيقية للبنك أو الشركات الكبرى. والبرمجيات الخبيثة:(Malware) [2]
- هي برامج ضارة يتم تحميلها على الأجهزة بهدف تدمير البيانات أو سرقتها أو التحكم بالجهاز عن بُعد.
- تشمل الفيروسات، الديدان، وبرامج التجسس، التي قد تقوم بتسريب بيانات المستخدمين، أو تعطيل الجهاز بشكل كامل.

والاحتيال الإلكتروني:

- يتضمن الخداع عبر الإنترنت لتحقيق مكاسب غير مشروعة. قد يتضمن ذلك إنشاء مواقع ويب مزيفة لبيع منتجات أو خدمات غير موجودة، أو الاحتيال في المعاملات التجارية عبر الإنترنت. [3]
- قد يطلب المحتالون معلومات حساسة من المستخدمين على أنها عرض خاص أو عروض مزيفة.

والتشهير الإلكتروني:

- هو نشر محتوى ضار عبر الإنترنت بهدف الإضرار بسمعة شخص أو جهة.
- قد يتضمن نشر أخبار كاذبة، أو تحريف الحقائق حول شخص ما في مواقع التواصل الاجتماعي أو المنتديات. [1]

([1]) (1) انيس حسيب المحلاوي الخبرة القضائية في الجرائم المعلوماتية والرقمية دار الفكر الجامعي الاسكندرية ، ٢٠١٦م.

(2) حسين بن سعيد بن سيف الغافري السياسة الجنائية في مواجهة جرائم الانترنت دراسة مقارنة ، رسالة دكتوراه كلية الحقوق جامعة عين شمس، القاهره ٢٠٠٧م.

([3]) خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن، ٢٠١١م.

والقرصنة الرقمية للمحتوى:

- يشمل ذلك سرقة المحتوى الرقمي المحمي مثل الأفلام، الموسيقى، أو البرمجيات، ونشرها أو توزيعها دون إذن من مالك الحقوق. [2]

وسرقة الهوية الإلكترونية:

- يقوم المجرم بسرقة معلومات شخصية عن فرد ما، مثل رقم الهوية أو رقم الضمان الاجتماعي، ثم استخدامها لأغراض غير قانونية، مثل فتح حسابات بنكية أو بطاقات ائتمان باسم الضحية. [3]

والتسلل عبر شبكات التواصل الاجتماعي:

قد يتضمن ذلك استخدام حسابات مزيفة على مواقع مثل فيسبوك أو تويتر لاستغلال الآخرين، إما لأغراض شخصية أو إجرامية.

تشير الجرائم المعلوماتية في الوطن العربي إلى الأفعال غير القانونية التي تُرتكب باستخدام التكنولوجيا الرقمية والإنترنت، وتشمل مجموعة واسعة من الأنشطة مثل القرصنة، الاحتيال الإلكتروني، انتهاك الخصوصية، وتوزيع البرمجيات الضارة.[4]

وفي العراق، تعتبر الجرائم المعلوماتية قضية متزايدة الأهمية، حيث شهدت البلاد زيادة في استخدام الإنترنت والتكنولوجيا. وقد أدى ذلك إلى ظهور تحديات جديدة تتعلق بالأمان السيبراني. الحكومة العراقية أصدرت قوانين لمكافحة هذه الجرائم، مثل قانون مكافحة جرائم المعلوماتية، الذي يهدف إلى حماية المعلومات الشخصية وفرض عقوبات على مرتكبي هذه الجرائم.[5]

تتطلب مكافحة الجرائم المعلوماتية في العراق تعاوناً بين الجهات الحكومية والقطاع الخاص والمجتمع المدني لتعزيز الوعي والتثقيف حول المخاطر المرتبطة بالتكنولوجيا، بالإضافة إلى تطوير البنية التحتية الأمنية.

([1]) د. إبراهيم حامد طنطاوي، التحقيق الجنائي من الناحيتين النظرية والعلمية، ط1، دار النهضة العربية ، القاهرة، سنة ١٩٩٩م.

([2]) د. أحمد عاصم عجيله الحماية الجنائية للمحررات الإلكترونية، دراسة مقارنة دار النهضة العربية، القاهرة ٢٠١٤م.

([3]) (3) د. أحمد عبد اللاه المراعي الجريمة الإلكترونية ودور القانون الجنائي في الحد منها – دراسة تحليلية تأصيلية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٧م.

([4]) د. أحمد فتحي سرور، الوسيط في قانون العقوبات، دار النهضة العربية، الطبعة السادسة، ٢٠١٥م.

(5) د. برهم محمد ظاهر، تنظيم التحقيق الابتدائي في الجرائم، دار وائل للنشر ، عمان، ط1، ٢٠١٣م.

الفرع الثاني

التمييز بين الجرائم المعلوماتية والجرائم التقليدية

الجرائم المعلوماتية والجرائم التقليدية هما نوعان من الجرائم التي تختلف في العديد من الجوانب، بالرغم من أن الهدف النهائي لكلا النوعين قد يكون هو الإضرار بالآخرين أو تحقيق مكاسب غير مشروعة. الجرائم المعلوماتية، كما يوحي اسمها، تتعلق باستخدام الوسائل التقنية مثل الإنترنت وأجهزة الكمبيوتر، بينما الجرائم التقليدية تتعلق بالأفعال الإجرامية التي تحدث في العالم المادي، مثل السرقة أو الاعتداء. [1]

وان الجرائم المعلوماتية هي الجرائم التي يتم ارتكابها باستخدام وسائل التكنولوجيا الحديثة، مثل الحواسيب، الإنترنت، والهواتف الذكية، بهدف التسلل إلى الأنظمة الرقمية أو التسبب في ضرر للبيانات والمعلومات. تعتمد هذه الجرائم على المعرفة التقنية للأدوات الرقمية، وقد تستهدف الأفراد أو المؤسسات. من أمثلة الجرائم المعلوماتية :الاختراق أو القرصنة الإلكترونية، الاحتيال الإلكتروني مثل التصيد(Phishing) ، البرمجيات الخبيثة مثل الفيروسات، التشهير عبر الإنترنت، السرقة الرقمية، وسرقة الهوية الإلكترونية.

في الجرائم المعلوماتية، يمكن للمجرم أن يكون بعيدًا جغرافيًا عن الضحية، مما يجعل اكتشافه أكثر صعوبة. على سبيل المثال، يمكن للقراصنة اختراق الأنظمة المالية عن بعد، وسرقة أموال أو بيانات حساسة دون أن يكونوا في نفس البلد أو المدينة. ويعتمد المجرمون في هذه الجرائم على استغلال الثغرات في الأنظمة أو على خيانة الأمان الشخصي للمستخدمين. [2]

أما الجرائم التقليدية هي الجرائم التي تحدث في العالم المادي وتتضمن الأفعال التي يتم ارتكابها باستخدام أدوات مادية أو عبر التفاعل المباشر مع الضحية. هذه الجرائم تشمل أنواعًا عديدة من الأفعال الإجرامية مثل السرقة، الاعتداء الجسدي، القتل، التحرش، الاحتيال التقليدي، التشهير العلني، والعديد من الجرائم الأخرى التي تتطلب عادة تواجد الجاني في نفس المكان أو الموقع الذي يحدث فيه الجريمة.

---

(1) د. جميل عبد الباقي الصغير، ادلة الاثبات الجنائي والتكنولوجيا الحديثة واجهزة الرادار ، الحاسبات الآليه البصمة الوراثية ، دراسة مقارنه، دار النهضة العربية، القاهرة، سنة ٢٠٠١م.

(2) د. حسن المرصفاوي، المرصفاوي في المحقق الجنائي، منشأة دار المعارف بالإسكندرية ١٩٧٧م.

الجرائم التقليدية تعتمد على العنف المادي أو التهديد بالضرر المباشر، وغالبًا ما يتم التعرف عليها بسرعة بناءً على الأدلة المادية أو الشهادات. على سبيل المثال، في حالة السرقة التقليدية، يمكن للشرطة العثور على المجرم بناءً على الأدلة مثل بصمات الأصابع أو تسجيلات كاميرات المراقبة. وبالمثل، في حال وقوع جريمة اعتداء، تكون الأدلة الجسدية مثل الجروح أو الكدمات واضحة. [1]

وقد تلتقي الجرائم المعلوماتية مع الجرائم التقليدية ، وتختلف عنها في بعض اوجه الاختلاف ، الامر الذي يؤدي الى الخلط بينهما ، وعليه سوف نتكلم في الفقرة الاولى عن اوجه التشابه ، وفي الفقرة الثانية عنم اوجه الاختلاف وكما يلي :-

أولاً :- أوجه الشبه

1. كلا النوعين من الجرائم ينطويان على أفعال غير قانونية تستهدف الأفراد أو المجتمع.
2. يمكن أن تؤدي كلا الجرائم إلى أضرار مالية أو نفسية للأفراد.
3. تتطلب كلا الجرائم تدخل السلطات القانونية لتحقيق العدالة.
4. يمكن أن تكون الدوافع وراء كلا النوعين متشابهة، مثل الجشع أو الانتقام. [2]

ثانياً :- أوجه الاختلاف

1. وسيلة التنفيذ :الجرائم المعلوماتية تُرتكب عبر التكنولوجيا الرقمية، بينما الجرائم التقليدية تُرتكب من خلال الأفعال المباشرة.
2. التأثير المكاني :الجرائم المعلوماتية يمكن أن تؤثر على الأفراد عبر المسافات الكبيرة، بينما الجرائم التقليدية غالباً ما تكون مرتبطة بمكان محدد.
3. أنماط الجريمة :الجرائم المعلوماتية تتسم بالتطور المستمر مع التقدم التكنولوجي، بينما الجرائم التقليدية تعتمد على أنماط سلوكية ثابتة. [3]

---

(1) د. حسن جوخدار ، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية – دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨م.

(2) د. حسين بن سعيد الغافري التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٩م.

(3) د. خالد محمد عجاج القاضي علي دايج جريان اصول التحقيق الجنائي، دار التعليم الجامعي، الاسكندرية، ٢٠١٨م.

4. الأدلة :في الجرائم المعلوماتية، الأدلة غالباً ما تكون رقمية (مثل سجلات الكمبيوتر)، بينما في الجرائم التقليدية، الأدلة قد تشمل شهادات، بقايا مادية، أو مشاهدات مباشرة .

المطلب الثاني

اركان الجريمة المعلوماتية

أركان الجريمة المعلوماتية هي العناصر الأساسية التي يجب توافرها لكي تُعتبر جريمة معلوماتية مكتملة. مثل باقي الجرائم، تتطلب الجريمة المعلوماتية وجود أركان معينة لكي تُعتبر جريمة قائمة. وتشمل الأركان الرئيسية للجريمة المعلوماتية على ركنين الاول ركن الجريمة المعلوماتية المادي ويشير إلى العناصر الفعلية التي تتكون منها الجريمة، ويتضمن السلوك الإجرامي مثل اختراق الأنظمة وتوزيع البرمجيات الضارة والاحتيال الإلكتروني. كما يشمل الوسائل المستخدمة مثل الحواسيب والبرمجيات، والنتائج التي تترتب على الجريمة مثل فقدان البيانات أو الأضرار المالية أو انتهاك الخصوصية. [1]

أما الركن الثاني فهو الركن المعنوي ويتعلق بالنوايا والدوافع وراء ارتكاب الجريمة. يجب أن يكون لدى الجاني نية واضحة لارتكاب الجريمة، سواء كانت بهدف الربح أو الانتقام أو إلحاق الضرر. ويتضمن أيضًا الوعي بالمخاطر، حيث يجب أن يكون الجاني مدركًا لطبيعة أفعاله ونتائجها المحتملة، بالإضافة إلى الدافع الذي يمكن أن يكون متعلقًا بالمال أو السلطة أو الأيديولوجيات.[2]

ومن اجل توضيح ذلك سوف يقسك المطلب الى فرعين الفرع الاول يتكلم عن الركن المادي للجريمة المعلوماتية وفي الثاني سوف نتكلم عن الركن المعنوي للجريمة المعلوماتية وكما يلي:

الفرع الأول

الركن المادي

الركن المادي للجريمة المعلوماتية هو العنصر الذي يحدد الفعل الفعلي الذي يتم ارتكابه باستخدام الوسائل التكنولوجية أو الرقمية، وهو يترجم الجريمة إلى عمل ملموس، أي ما يفعله

---

(1) د. خالد ممدوح ابراهيم فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي الاسكندرية، الطبعة الأولى، ٢٠١٨م.

(2) د. ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالانترنت – دراسة تطبيقية مقارنة مركز الدراسات العربية للنشر والتوزيع، الجيزة، ٢٠١٧م.

الجاني لتحقيق الهدف الإجرامي. يعتبر هذا الركن أساسيًا لأن الفعل المادي هو الذي يوضح وجود الجريمة من الناحية العملية. دون هذا الفعل، لا يمكن تحديد ما إذا كانت الجريمة قد ارتُكبت أم لا.[1] وان الركن المادي للجريمة المعلوماتية يتضمن عدة عناصر، ومنها:

أولاً :- الفعل الإجرامي (التصرف المادي):

- الفعل الإجرامي في الجرائم المعلوماتية هو التصرف الذي يقوم به الجاني باستخدام تقنيات المعلومات والأنظمة الرقمية بشكل غير قانوني. قد يكون هذا الفعل في شكل الاختراق، التصدي لبيانات محمية، الاحتيال الإلكتروني، أو نشر الفيروسات.[2]

ومن أبرز الأمثلة على الفعل الإجرامي:

- الاختراق :الدخول غير المصرح به إلى أنظمة الكمبيوتر أو الشبكات بهدف سرقة أو تعديل البيانات.
- نقل الفيروسات :نشر برامج ضارة بهدف تدمير أو سرقة البيانات.
- التصيد الإلكتروني :(Phishing) إرسال رسائل بريد إلكتروني مزيفة للحصول على معلومات حساسة مثل كلمات المرور أو أرقام الحسابات البنكية.

والفعل الإجرامي في الجريمة المعلوماتية غالبًا ما يتم عن بُعد باستخدام الإنترنت أو الشبكات الإلكترونية، مما يجعل من الصعب تعقبه أو تحديده بسهولة.

ثانياً:- النتيجة (الضرر الناتج):

في الجرائم المعلوماتية، غالبًا ما تكون النتيجة غير مادية، مثل تدمير البيانات أو التأثير على الأنظمة الإلكترونية. قد تكون هذه النتيجة على شكل:

- تدمير البيانات :مثل الحذف غير القانوني للملفات أو تعطيل أنظمة الكمبيوتر.
- تعديل البيانات :مثل التلاعب بالمعلومات الرقمية بهدف تغيير محتوى البيانات.
- التعطيل :مثل تعطيل الأنظمة أو الخدمات الإلكترونية، وهو ما يحدث في الهجمات من نوع هجوم رفض الخدمة.(DDoS)

---

(1) د. سلطان الشاوي أصول التحقيق الإجرامي، المكتبة القانونية للتوزيع، بغداد، ١٩٧٢م.

(2) د. عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائل الالكترونية دراسة قانونية، مقارنة ، الطبعة الثالثة دار الثقافة للنشر والتوزيع، عمان، سنة ٢٠١٩م.

- سرقة البيانات :مثل سرقة البيانات الشخصية أو المعلومات المالية من الأنظمة الإلكترونية.

على سبيل المثال، في حالة اختراق نظام مالي، النتيجة المترتبة قد تكون سرقة الأموال أو تسريب البيانات الحساسة مثل أرقام الحسابات البنكية. [1]

ثالثاً :- الوسيلة المستخدمة:

في الجرائم المعلوماتية، الوسيلة المستخدمة هي التكنولوجيا الرقمية مثل الحواسيب، الإنترنت، الهواتف الذكية، الشبكات، البرمجيات، أو أي نوع من الأجهزة التقنية الحديثة التي تسمح بالتفاعل مع الأنظمة الرقمية. هذه الوسائل هي أدوات الجريمة التي يتم من خلالها ارتكاب الفعل الإجرامي.

- الإنترنت :يعد الإنترنت من أهم الوسائل التي تُستخدم لارتكاب الجرائم المعلوماتية. من خلاله يمكن تنفيذ القرصنة الإلكترونية أو نشر البرمجيات الخبيثة أو القيام بأنشطة احتيالية.
- الأنظمة الرقمية :مثل الحواسيب أو الشبكات التي تحتوي على معلومات حساسة يمكن الوصول إليها غير قانونيًا.
- البرمجيات :يتم استخدامها كوسيلة لتنفيذ الفعل الإجرامي مثل الفيروسات والديدان والبرمجيات الخبيثة. [2]

على سبيل المثال، في الهجوم الإلكتروني، يستخدم المهاجم برامج خبيثة للوصول إلى النظام وتدمير البيانات أو سرقتها.

رابعاً :- عدم التراخيص أو الدخول غير المشروع:

في أغلب الجرائم المعلوماتية، يتطلب الركن المادي أن يكون الفعل قد تم بدون إذن أو تصريح قانوني .بمعنى أن الجاني يجب أن يدخل الأنظمة أو الشبكات الإلكترونية أو يعبث بالبيانات دون أن يحصل على ترخيص قانوني من صاحب النظام أو الجهة المالكة للمعلومات.

- الاختراق :(Hacking) الدخول غير المصرح به إلى نظام كمبيوتر.
- الاحتيال الإلكتروني :جمع أو استخدام معلومات شخصية أو مالية من دون إذن.

([1]) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر الانترنت، ٢٠٠٩ بلا دار نشر.

([2]) د. علي جبار الحسناوي ، جرائم الحاسوب والانترنت دار اليازوري للنشر والتوزيع، عمان ٢٠٠٩م.

- البرمجيات الخبيثة :استخدام البرمجيات الضارة للوصول إلى الأنظمة بشكل غير قانوني.[1]

خامساً :- الفعل الجرمي المستمر:

من السمات المهمة في الجرائم المعلوماتية أن الفعل الإجرامي قد يكون مستمرًا أو متعدد الأفعال .مثلًا، في جريمة القرصنة الإلكترونية، قد يستمر الجاني في الوصول إلى الأنظمة أو تحميل البيانات لأيام أو حتى أسابيع دون اكتشافه. [2]

- على سبيل المثال، في الهجمات من نوع البرمجيات الخبيثة، قد يستمر تأثير الفيروس على الأنظمة أو الأجهزة بعد فترة طويلة من نشره.

سادساً :- استخدام الأدوات التقنية (مثل برامج التجسس والفيروسات:)

في العديد من الجرائم المعلوماتية، يتم استخدام أدوات تقنية متقدمة كوسيلة لارتكاب الجريمة. يمكن استخدام البرمجيات الخبيثة مثل الفيروسات، الديدان، أو برامج التجسس لأغراض غير قانونية. يتم نشر هذه الأدوات عبر الإنترنت أو البريد الإلكتروني أو حتى من خلال الوسائط المحمولة، مثل الأقراص الصلبة. [3]

على سبيل المثال، فيروسات الكمبيوتر قد تتسبب في تعطيل النظام أو تسريب البيانات إلى أطراف ثالثة، وبالتالي يُعتبر ذلك الفعل المادي جزءًا من الجريمة المعلوماتية. [4]

([1]) د. عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، منشورات الحلبي الحقوقية، لبنان، ٢٠١٥م

([2]) د. عمر الفاروق الحسيني، أصول علم الإجرام وعلم العقاب، دار النهضة العربية القاهره ، ٢٠٠٢م.

([3]) د. محمد انور عاشور، المبادئ الاساسية في التحقيق الجنائي العملي عالم الكتب، القاهره ١٩٨٧م.

(4) د. فايز الضفيري، المعالم الأساسية لقضية العدالة في مرحلة الاستدلالات والتحقيق الإجرائي"، مجلس النشر العلمي، جامعة الكويت، ٢٠٠١م.

الفرع الثاني

الركن المعنوي

الركن المعنوي للجريمة المعلوماتية هو عنصر أساسي في تكوين الجريمة، حيث يعبر عن نية الجاني أو قصده عند ارتكاب الفعل الإجرامي. يختلف الركن المعنوي عن الركن المادي في أنه يتعلق بالحالة النفسية للجاني، أي ما إذا كان قد ارتكب الفعل عن عمد ووعي أو كان ذلك عن غير قصد. ويعد الركن المعنوي عاملًا محوريًا في تحديد مسؤولية الجاني ومدى تعرضه للعقاب. وان الركن المعنوي للجريمة المعلوماتية من وجهة نظر المشرع العراقي يتضمن عدة عناصر رئيسية تركز على النية والإرادة: [1]

أولاً:- العلم :يشير إلى وعي الجاني بطبيعة الأفعال التي يقوم بها، حيث يجب أن يكون مدركاً أنه يرتكب فعلاً غير قانوني. يتطلب ذلك أن يكون الجاني على دراية بالعواقب القانونية لفعلته.

ثانياً :- الإرادة :تعكس رغبة الجاني في تنفيذ الفعل الإجرامي. يجب أن تكون لدى الجاني نية واضحة لارتكاب الجريمة، وهذا يتضمن اختياراً مقصوداً لتنفيذ السلوك المجرم.

ثالثاً :- سوء النية :في بعض الحالات، يمكن أن يكون سوء النية عاملاً مهماً في تحديد طبيعة الجريمة. إذا كان الجاني يتصرف بطريقة تضر بالآخرين أو تنتهك حقوقهم، فهذا يعزز من طابع الجريمة.

رابعاً :- الدافع :قد تتضمن الإرادة دوافع مختلفة، سواء كانت مالية أو انتقامية أو مرتبطة بالسلطة. المشرع يأخذ بعين الاعتبار الدوافع التي تحرك الجاني، حيث يمكن أن تؤثر على العقوبات المفروضة.

وبشكل عام، يُعتبر الركن المعنوي من العناصر الأساسية لتحديد الجريمة المعلوماتية في القانون العراقي، حيث يُساعد في تقييم مدى مسؤولية الجاني وتحديد العقوبات المناسبة.[2]

---

(1) د. فرج عيد يونس حسن، التخصص القضائي إحدى الدعائم الأساسية لتحقيق العدالة الناجزة"، دار الجامعة الجديدة، الإسكندرية، ٢٠١٧م.

(2) د. مأمون محمد سلامة الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار النهضة العربية، القاهرة، ٢٠٠٨م.

أن أهمية الركن المعنوي في الجريمة المعلوماتية:

الركن المعنوي يعتبر أساس المسؤولية القانونية في الجرائم المعلوماتية. معرفة القصد الجنائي للجاني يمكن أن تؤثر في عقوبته وفي تحديد مدى خطورة الجريمة التي ارتكبها.[1] على سبيل المثال النية الإجرامية المباشرة قد تؤدي إلى عقوبات أشد مقارنةً بحالة القصد غير المباشر أو الإهمال. و يمكن للمحاكم أن تأخذ بعين الاعتبار القصد أو الإهمال لتحديد درجة الجريمة ومدى خطورتها على الضحية أو المجتمع. [2]

([1]) د. مجيد خضر السبعاوي، والاستاذ مولان قادر أحمد الضرورة الإجرائية في مرحلة التحقيق الابتدائي – دراسة تحليلية مقارنة ، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٧م.

(2) د. محمد الأمين البشري، الاساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية"، محاضرة مقدمة في الحلقة العلمية – تحليل الجرائم المستحدثة والسلوك المنعقدة في الفترة من ١٩-١٧ / ٢٠١١ بمقر جامعة نايف العربية للعلوم الإجرامي الأمنية.

المطلب الثالث

المواجهة الجنائية للجرائم المعلوماتية

المواجهة الجنائية للجرائم المعلوماتية تشير إلى الجهود المبذولة لمكافحة الجرائم التي ترتكب باستخدام التكنولوجيا الحديثة والإنترنت. تشمل هذه المواجهة تطوير التشريعات والقوانين التي تنظم الفضاء الإلكتروني وتحدد العقوبات المناسبة للجرائم المعلوماتية.[1]

تتضمن أيضاً تحسين القدرات الأمنية من خلال تدريب الفرق المختصة في مجال التحقيقات الإلكترونية وتعزيز التعاون بين الجهات المحلية والدولية لمكافحة هذه الأنشطة الإجرامية.

علاوة على ذلك، تركز المواجهة على رفع الوعي العام حول مخاطر الجرائم المعلوماتية وسبل الحماية اللازمة، بالإضافة إلى استخدام التكنولوجيا المتقدمة في الكشف عن هذه الجرائم.

بشكل عام، تسعى المواجهة الجنائية إلى خلق بيئة أكثر أماناً في الفضاء الرقمي، مما يساهم في حماية الأفراد والمؤسسات من التهديدات المعلوماتية. [2]

وسوف نوضح المواجهة الجنائية تباعاً في الفرع الاول المواجهة الجنائية على مستوى التشريع الوطني أما الفرع الثاني نوضح المواجهة الجنائية على مستوى التعاون الدولي وكما يلي . [3]

الفرع الأول

المواجهة الجنائية على مستوى التشريع الوطني

المواجهة الجنائية للجرائم المعلوماتية على مستوى التشريع الوطني تتعلق بالقوانين والإجراءات التي تتبناها كل دولة لمكافحة الجرائم التي ترتكب عبر الإنترنت أو باستخدام التكنولوجيا الحديثة. نظراً للطبيعة الخاصة للجرائم المعلوماتية التي تشمل مجموعة واسعة من الأفعال مثل القرصنة الإلكترونية، الاحتيال الإلكتروني، التهديدات الرقمية، وانتهاك الخصوصية، أصبح من الضروري أن يتوافر تشريع خاص لهذه الجرائم يتناسب مع تطور الوسائل التكنولوجية.

([1]) د. محمد الأمين البشري، التحقيق الجنائي المتكامل"، أكاديمية نايف العربية للعلوم الأمنية مركز الدراسات والبحوث، الرياض، ١٩٩٨م.

(2) د. محمد الأمين البشري، التحقيق الجنائي المتكامل"، أكاديمية نايف العربية للعلوم الأمنية مركز الدراسات والبحوث، الرياض، ١٩٩٨م.

([3]) د. محمد سعيد نمور أصول الإجراءات الجزائية، شرح لقانون أصول المحاكمات الجزائية"، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، ٢٠١١م.

وفي هذا السياق، تتمثل المواجهة الجنائية على مستوى التشريع الوطني في وضع القوانين التي تحدد الأفعال غير المشروعة، العقوبات المقررة، والإجراءات التي يجب اتباعها لمكافحة هذه الجرائم وتوفير الحماية القانونية للأفراد والمجتمعات. [1]

وان أهمية التشريعات الوطنية في مواجهة الجرائم المعلوماتية:

أولاً :- الحماية القانونية :من خلال قوانين الجرائم المعلوماتية، يمكن حماية الأفراد والشركات من الاختراقات الإلكترونية، الاحتيال الإلكتروني، والتلاعب بالمعلومات. [2]

ثانياً :- ضبط وتنظيم :القوانين الوطنية تساعد في ضبط الأنشطة الإلكترونية المجهولة وتحديد المسؤوليات القانونية لمن يرتكب هذه الأنشطة.

ثالثاً :- التعاون الدولي :قد تتطلب الجرائم المعلوماتية تعاونًا بين الدول في حال كانت الجريمة قد ارتكبت عبر الحدود. ولذلك، تكون التشريعات الوطنية ضرورية لضمان التعاون بين الدول لمكافحة هذه الجرائم عبر آليات قانونية دولية. [3]

وأبرز التشريعات الوطنية لمكافحة الجرائم المعلوماتية:

اولاً :- قانون الجرائم المعلوماتية في بعض الدول العربية:

1. السعودية :يعتمد نظام مكافحة الجرائم المعلوماتية في السعودية الذي أقر عام 2007 على تحديد الجرائم الإلكترونية بشكل شامل، مثل القرصنة، الاحتيال الإلكتروني، التشهير عبر الإنترنت، والدخول غير المشروع إلى الأنظمة .ويشمل هذا القانون فرض غرامات وعقوبات سجن تتفاوت حسب نوع الجريمة. بالإضافة إلى ذلك، يعاقب النظام على الأعمال التي تؤدي إلى تدمير البيانات أو انتقال الفيروسات. [4]

---

(1) د. مصطفي محمد موسي، التحقيق الجنائي في الجرائم الإلكترونية" ، الطبعة الأولى، مطابع الشرطه ، القاهره ، ٢٠٠٩م.

(2) د. هلالي عبد اللاه احمد ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١ ، الطبعة الأولى، دار النهضة العربية ، القاهرة، ٢٠٠٣م.

(3) فاروق الكيلاني، محاضرات في قانون أصول المحاكمات الجزائية الاردني والمقارن، ج ٢ ، ط ٢، دار المروج، بيروت ، ١٩٩٥م.

(4) د. محمد عمر مصطفى النتيجة وعناصر الجريمة، مجلة العلوم القانونية والاقتصادية، العدد ٢ لسنة ١٩٦٥ ، كلية الحقوق، جامعة عين شمس.

2. مصر :في مصر، تم إقرار قانون مكافحة الجرائم الإلكترونية في عام 2018، الذي يتعامل مع الجرائم التي يتم ارتكابها عبر الإنترنت مثل التحايل الإلكتروني، القرصنة، التهديدات الرقمية، وانتهاك الخصوصية .يُعاقب مرتكبو الجرائم الإلكترونية بعقوبات مشددة تشمل السجن و الغرامات المالية.
3. الإمارات :يتضمن القانون الاتحادي رقم 5 لعام 2012 لمكافحة الجرائم الإلكترونية في الإمارات، حيث يعاقب على جميع الجرائم المتعلقة بالتكنولوجيا الرقمية، مثل الاحتيال الإلكتروني و التهديد عبر الإنترنت و الدخول غير المشروع إلى البيانات الشخصية . يشمل هذا القانون العديد من الإجراءات المساعدة لضمان حماية الخصوصية وحماية المستخدمين.
4. الأردن :يعترف قانون مكافحة الجرائم الإلكترونية في الأردن بالأضرار التي تلحق بالأفراد نتيجة الجرائم المعلوماتية، ويحدد العقوبات مثل السجن والغرامات المالية للأفعال مثل التشهير عبر الإنترنت أو انتهاك حقوق الملكية الفكرية عبر الشبكة.

ثانياً :- المعايير الدولية والموافقة على الاتفاقيات: [1]

1. اتفاقية بودابست :هي اتفاقية دولية اعتمدتها مجلس أوروبا عام 2001 لتوحيد التشريعات المتعلقة بالجرائم المعلوماتية بين الدول الأعضاء وغير الأعضاء. تسعى هذه الاتفاقية إلى ضمان التعاون الدولي في مكافحة الجرائم المعلوماتية، مثل الاختراق الإلكتروني و الاحتيال الإلكتروني، بالإضافة إلى تحديد الأسس القانونية للتعاون بين الدول.
2. الاتحاد الأوروبي :من خلال تشريعات مثل اللائحة العامة لحماية البيانات(GDPR) ، توفر الاتحاد الأوروبي إطارًا تنظيميًا لحماية الخصوصية الرقمية، وفرض عقوبات صارمة ضد من ينتهك البيانات الشخصية للأفراد. كما يتم تطبيق قوانين حماية البيانات في حال حدوث اختراقات أو تسريبات للبيانات.

أما التحديات التي تواجه التشريع الوطني لمكافحة الجرائم المعلوماتية

(1) محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية رسالة ماجستير في العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٤م.

تواجه التشريعات الوطنية لمكافحة الجرائم المعلوماتية عدة تحديات، منها بطء التكيف مع التطورات التكنولوجية السريعة، مما يجعل القوانين قديمة وغير فعالة. هناك أيضاً صعوبة في تحديد نطاق الجريمة المعلوماتية بسبب طبيعتها المعقدة وعابرة الحدود. بالإضافة إلى ذلك، قد تواجه الدول نقصاً في الخبرات الفنية والموارد اللازمة لتطبيق القوانين بشكل فعال. التحديات الثقافية والاجتماعية قد تعيق نشر الوعي حول الجرائم المعلوماتية وأهمية مواجهتها. كما يمكن أن تؤثر الاعتبارات السياسية والاقتصادية على إرادة الدول في تبني قوانين فعالة.[1] هذه العوامل تتطلب تعاوناً وثيقاً بين الجهات المعنية لتطوير أطر قانونية قوية وفعالة وكما يلي :

1. التطور السريع للتكنولوجيا:

التكنولوجيا تتطور بسرعة كبيرة، مما يجعل من الصعب على التشريعات مواكبة هذه التغيرات . فكلما ظهرت تقنيات جديدة، يزداد احتمال استخدامها لأغراض غير قانونية، ويصبح من الصعب وضع قوانين تحددها أو تتعامل معها بشكل شامل.[2]

- على سبيل المثال، مع ازدياد استخدام الذكاء الصناعي، قد تظهر أنواع جديدة من الجرائم المعلوماتية، مثل استخدام الذكاء الصناعي في الهجمات السيبرانية أو التلاعب بالبيانات.

2. التعاون بين الدول:

بما أن الجرائم المعلوماتية تتم غالبًا عبر الإنترنت وتؤثر على العديد من البلدان في آن واحد، يصبح التعاون الدولي أمرًا أساسيًا. إلا أن كل دولة لديها تشريعات وقوانين مختلفة، مما يعقد عملية التنسيق بين الدول لمكافحة الجرائم عبر الحدود.

- على سبيل المثال، يمكن أن يحدث اختراق بيانات في دولة ويُستخدم ذلك ضد أفراد في دول أخرى .وبالتالي، تصبح القضية أكثر تعقيدًا بسبب الاختلافات القانونية بين الدول.

3. صعوبة إثبات الجريمة:

([1]) محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها – دراسة مقارنة"، رسالة دكتوراه كلية الحقوق، جامعة المنصورة، ٢٠٠٥م.

([2]) د. محمد عبد الله إبراهيم: المواجهة الأمنية لجرائم شبكة المعلومات الدولية"، اكاديمية الشرطة القاهرة، ٢٠١٦م.

بما أن الجريمة المعلوماتية غالبًا ما تتم عن بُعد وباستخدام أدوات تقنية متقدمة، فإن إثبات الجريمة قد يكون معقدًا للغاية. تتطلب القوانين المتبعة في هذه الحالات تقنيات متخصصة لتحليل الأدلة الرقمية وتحديد الجاني، وهذه التقنيات غالبًا ما تكون مكلفة ومعقدة.

4. الخصوصية وحماية البيانات:

تمثل الخصوصية الرقمية قضية أخرى هامة في التشريعات الوطنية لمكافحة الجرائم المعلوماتية. يجب أن تضمن الدول في تشريعاتها حماية البيانات الشخصية وعدم التعرض لانتهاك الخصوصية أثناء التحقيقات الخاصة بالجرائم المعلوماتية. [1]

(1) محمد علي محمد عبيد المحواث الحمودي ، دور مأمور الضبط القضائي في مواجهة جرائم المعلومات، رسالة ماجستير ، كلية الحقوق جامعة القاهره، ٢٠٠٩م.

الفرع الثاني

المواجهة الجنائية على مستوى التعاون الدولي

نظرًا للطبيعة العابرة للحدود للجرائم المعلوماتية، فإن التعاون الدولي يُعد أمرًا حاسمًا في مكافحة هذه الجرائم. ففي ظل العولمة والإنترنت الذي لا يعترف بالحدود، قد تُرتكب الجرائم المعلوماتية في دولة وتؤثر في أشخاص أو كيانات في دول أخرى. لذلك، فإن التعاون بين الدول في إطار التشريعات و الإجراءات القانونية يصبح أمرًا ضروريًا لمكافحة الجرائم الإلكترونية بفعالية.[1]

ومن الآليات والاتفاقيات الدولية في مكافحة الجرائم المعلوماتية:

أولاً :- اتفاقية بودابست (2001)

تعد اتفاقية بودابست (أو اتفاقية مجلس أوروبا بشأن الجرائم الإلكترونية (واحدة من أهم وأول الاتفاقيات الدولية التي تهدف إلى مكافحة الجرائم المعلوماتية .تم اعتماد هذه الاتفاقية عام 2001 تحت إشراف مجلس أوروبا، وهي أول معاهدة دولية تتناول مكافحة الجرائم المعلوماتية عبر الإنترنت بشكل شامل. تشمل الاتفاقية:

1. تعريف الجرائم الإلكترونية :مثل القرصنة، الاحتيال الإلكتروني، و الاعتداء على البيانات.
2. التحقيقات العابرة للحدود :تعزيز التعاون بين الدول في مجال جمع الأدلة وال تحقيقات في الجرائم الرقمية.
3. تسليم المجرمين :تسهيل تسليم المجرمين بين الدول للقيام بالملاحقة القضائية.

تنص الاتفاقية على ضرورة وضع تشريعات وطنية تستهدف مكافحة الجرائم الرقمية وتعزيز التعاون بين الدول الأعضاء.[2]

حاليًا، 44دولة و الاتحاد الأوروبي من بين الدول التي صادقت على الاتفاقية، مما يعكس رغبتهم في توحيد الجهود لمكافحة الجرائم المعلوماتية.

ثانياً :- البرنامج الدولي للأمن السيبراني:(UNCITRAL)

([1]) د. هلالي عبد اللاه احمد ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١ ، الطبعة الأولى، دار النهضة العربية ، القاهرة، ٢٠٠٣م.

([2]) د. مصطفي محمد موسى، الجهاز" الإلكتروني لمكافحة الجريمة، دار الكتب القانونية، المحلة الكبرى، مصر ٢٠٠٦م.

تهدف الأمم المتحدة من خلال هذا البرنامج إلى تعزيز القدرة القضائية لمكافحة الجرائم الإلكترونية على مستوى العالم. يتعاون البرنامج مع الدول النامية لتطوير إجراءات مكافحة الجرائم الإلكترونية بما يتناسب مع احتياجاتها الخاصة. [1]

بالإضافة إلى ذلك، تقدم اللجنة الأمم المتحدة للقانون التجاري الدولي (UNCITRAL) توصيات ومساعدات في تطوير التشريعات الوطنية المتعلقة بالأمن السيبراني.

ثالثاً:- المجموعة العالمية للأمن السيبراني:(GAC)

هي منظمة دولية تضم شركات تكنولوجيا و دولًا تهدف إلى تعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية .تركز هذه المجموعة على تزويد الدول بالأدوات اللازمة لمواجهة التهديدات السيبرانية.

رابعاً:- الشرطة الجنائية الدولية (الإنتربول)

تسهم الإنتربول في التنسيق بين الشرطة الوطنية في مختلف الدول لمكافحة الجرائم الإلكترونية. تنظم الإنتربول بشكل دوري مؤتمرات تدريبية و ورش عمل، وتعزز التعاون الدولي عبر تقديم الاستشارات القانونية و الموارد التقنية، لتمكين الدول من ملاحقة الجرائم الإلكترونية بفعالية.

كما أن الإنتربول يعمل على جمع البيانات والمعلومات المتعلقة بالأنشطة الإجرامية عبر الإنترنت، مما يسهل التعاون بين الدول في ملاحقة الجناة.

5. الاتحاد الأوروبي:

من خلال مبادرات مثل اللائحة العامة لحماية البيانات(GDPR) ، يعمل الاتحاد الأوروبي على توحيد الجهود لمكافحة الجرائم الرقمية وحماية البيانات الشخصية في الدول الأعضاء.

- توجيهات الاتحاد الأوروبي :يسعى الاتحاد إلى تنظيم ومواءمة التشريعات الأمنية السيبرانية بين الدول الأعضاء، مما يسهل التعاون في التحقيقات عبر الحدود.

6. اتفاقية مكافحة الجريمة المنظمة عبر الوطنية:(UNTOC)

على الرغم من أن هذه الاتفاقية تركز بشكل أساسي على الجريمة المنظمة، فإنها تحتوي على مواد تتعلق بـ الجرائم الإلكترونية مثل القرصنة الإلكترونية و الاحتيال الرقمي .يُعَزّز التعاون الدولي في ملاحقة الجريمة المنظمة عبر الإنترنت من خلال هذه الاتفاقية، حيث تضمن إجراءات قانونية موحدة. [2]

([1]) فاروق الكيلاني، محاضرات في قانون أصول المحاكمات الجزائية الاردني والمقارن، ج ٢ ، ط ٢، دار المروج، بيروت ، ١٩٩٥م.

(2) مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وأثباتها في فلسطين – دراسة مقارنة"، بحث منشور مجلة علوم الشريعة والقانون الجامعة الأردنية، المجلد ٤٥ ، عدد ٤ ، ملحق ٢، ٢٠١٨م.

الخاتمة :

في ختام بحثنا حول المواجهة الجنائية للجرائم المعلوماتية، يتضح أن هذا الموضوع يتطلب اهتماماً خاصاً من جميع الأطراف المعنية. إن تطوير التشريعات لمواكبة التغيرات التكنولوجية السريعة يعد أمراً ضرورياً لضمان حماية فعالة للحقوق والمصالح. كما أن التعاون الدولي يلعب دوراً مهماً في مكافحة هذه الجرائم، إذ أن طبيعتها العابرة للحدود تستدعي تنسيق الجهود بين الدول.

علاوة على ذلك، يمكن أن تُستخدم التكنولوجيا كأداة فعالة في الكشف والتحقيق في الجرائم المعلوماتية، مما يتطلب استثماراً في تطوير أدوات جديدة. من المهم أيضاً تعزيز الوعي العام حول مخاطر هذه الجرائم وسبل الحماية اللازمة، فضلاً عن ضرورة تدريب وتأهيل الكوادر البشرية في الأجهزة الأمنية والقضائية لمواجهة هذه التحديات بشكل فعال.

في النهاية، فإن المواجهة الجنائية للجرائم المعلوماتية تمثل مسألة حيوية تحتاج إلى استجابة شاملة ومتكاملة لضمان سلامة المجتمع وحماية حقوق الأفراد في عصر التكنولوجيا الحديثة.

أولاً :- الاستنتاجات

1. الجرائم المعلوماتية تمثل تهديدًا عالميًا :تزايدت الجرائم المعلوماتية بشكل ملحوظ في العصر الرقمي، وهي تشكل تهديدًا على الأفراد، المؤسسات، والدول. هذه الجرائم لا تقتصر على الأضرار المالية فقط، بل تمتد لتشمل التهديدات للخصوصية، السمعة، وأمن الأنظمة الرقمية.
2. أهمية التشريعات الوطنية في مكافحة الجرائم الإلكترونية :إن التشريعات الوطنية المتعلقة بالجرائم المعلوماتية تشكل الأساس في حماية الأفراد والمجتمع من الهجمات الرقمية. فوجود قوانين واضحة وصارمة يساعد في محاكمة الجناة و ردع الجرائم، وبالتالي تعزيز الأمن السيبراني على المستوى المحلي.
3. التعاون الدولي ضرورة لمكافحة الجرائم العابرة للحدود :بالنظر إلى أن الجرائم المعلوماتية تتم في بيئة عابرة للحدود، فإن التعاون بين الدول يصبح ضرورة قصوى لملاحقة مرتكبي الجرائم وحماية المجتمعات. الاتفاقيات الدولية مثل اتفاقية بودابست والهيئات مثل الإنتربول تشكل إطارًا حيويًا لتنسيق الجهود الدولية في مكافحة الجرائم الإلكترونية.

ثانياً:- التوصيات

1. تطوير التشريعات الوطنية :يجب على الدول العمل على تحديث وتطوير التشريعات المتعلقة بالجرائم المعلوماتية بما يتماشى مع التطورات التكنولوجية الحديثة. وينبغي تضمين قوانين تحكم الجرائم الرقمية بشكل شامل، مع تحديد العقوبات المناسبة لردع المجرمين الإلكترونيين.
2. تعزيز التعاون الدولي :من الضروري أن تقوم الدول بتعزيز التعاون الدولي في مكافحة الجرائم المعلوماتية من خلال الانضمام إلى الاتفاقيات الدولية مثل اتفاقية بودابست وتفعيل دور المنظمات الدولية مثل الإنتربول .ويجب العمل على تطوير آليات تشريعية موحدة لمكافحة الجرائم العابرة للحدود.
3. توفير التدريب المتخصص للكوادر الأمنية والقضائية :يجب على الدول توفير تدريب متخصص للشرطة والقضاء والعاملين في المجال الأمني حول أحدث أساليب التحقيق في الجرائم الرقمية وتقنيات التحليل الرقمي .كما يجب دعم هذه الكوادر بالأدوات والموارد اللازمة لمواكبة التطورات في أساليب الجريمة الإلكترونية.
4. زيادة الوعي المجتمعي بالأمن السيبراني :يجب على الحكومات والمنظمات غير الحكومية تطوير برامج توعية تستهدف المجتمع بخصوص الأمن السيبراني وأهمية حماية البيانات الشخصية. ويجب أن تشمل هذه البرامج كافة الفئات العمرية والمهنية، وذلك من خلال حملات إعلامية وورش عمل وتدريب حول السلوك الآمن عبر الإنترنت.

المصادر

اولاً :- الكتب القانونية

1. د. إبراهيم حامد طنطاوي، التحقيق الجنائي من الناحيتين النظرية والعلمية، ط1، دار النهضة العربية ، القاهرة، سنة ١٩٩٩م.
2. د. سلطان الشاوي أصول التحقيق الإجرامي، المكتبة القانونية للتوزيع، بغداد، ١٩٧٢م.
3. د. محمد انور عاشور، المبادئ الاساسية في التحقيق الجنائي العملي عالم الكتب، القاهره ١٩٨٧م.
4. د. مصطفي محمد موسى، الجهاز" الإلكتروني لمكافحة الجريمة، دار الكتب القانونية، المحلة الكبرى، مصر ٢٠٠٦م.
5. د. مصطفي محمد موسي، التحقيق الجنائي في الجرائم الإلكترونية" ، الطبعة الأولى، مطابع الشرطه ، القاهره ، ٢٠٠٩م.
6. د. هلالي عبد اللاه احمد ، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١ ، الطبعة الأولى، دار النهضة العربية ، القاهرة، ٢٠٠٣م.
7. انيس حسيب المحلاوي الخبرة القضائية في الجرائم المعلوماتية والرقمية دار الفكر الجامعي الاسكندرية ، ٢٠١٦م.
8. أحمد أبو الروس، التحقيق الجنائي والتعرف فيه والادلة الجنائية، مرجع سابق، ص ١٥. أحمد المهدي، اشرف شافعي التحقيق الجنائي الابتدائي وضمانات المتهم وحمايتها، دار الكتب القانونية، المحلة، مصر، ٢٠٠٥م.
9.
10. خالد عباد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، الأردن، ٢٠١١م.
11. د. أحمد عاصم عجيله الحماية الجنائية للمحررات الإلكترونية، دراسة مقارنة دار النهضة العربية، القاهرة ٢٠١٤م.

12. د. أحمد عبد اللاه المراعي الجريمة الإلكترونية ودور القانون الجنائي في الحد منها – دراسة تحليلية تأصيلية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٧م.
13. د. أحمد فتحي سرور، الوسيط في قانون العقوبات، دار النهضة العربية، الطبعة السادسة، ٢٠١٥م.
14. د. برهم محمد ظاهر، تنظيم التحقيق الابتدائي في الجرائم، دار وائل للنشر ، عمان، ط1، ٢٠١٣م.
15. د. جميل عبد الباقي الصغير، ادلة الاثبات الجنائي والتكنولوجيا الحديثة واجهزة الرادار ، الحاسبات الآليه البصمة الوراثية ، دراسة مقارنه، دار النهضة العربية، القاهرة، سنة ٢٠٠١م.
16. د. حسن المرصفاوي، المرصفاوي في المحقق الجنائي، منشأة دار المعارف بالإسكندرية ١٩٧٧م.
17. د. حسن جوخدار ، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية – دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨م.
18. د. حسين بن سعيد الغافري التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٩م.
19. د. خالد محمد عجاج القاضي علي دايج جريان اصول التحقيق الجنائي، دار التعليم الجامعي، الاسكندرية، ٢٠١٨م.
20. د. خالد ممدوح ابراهيم فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي الاسكندرية، الطبعة الأولى، ٢٠١٨م.
21. د. ربيع محمود الصغير، القصد الجنائي في الجرائم المتعلقة بالانترنت – دراسة تطبيقية مقارنة مركز الدراسات العربية للنشر والتوزيع، الجيزة، ٢٠١٧م.
22. د. عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائل الالكترونية دراسة قانونية، مقارنة ، الطبعة الثالثة دار الثقافة للنشر والتوزيع، عمان، سنة ٢٠١٩م.
23. د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر الانترنت، ٢٠٠٩ بلا دار نشر.

24. د. علي جبار الحسناوي ، جرائم الحاسوب والانترنت دار اليازوري للنشر والتوزيع، عمان ٢٠٠٩م.
25. د. عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، منشورات الحلبي الحقوقية، لبنان، ٢٠١٥م
26. د. عمر الفاروق الحسيني، أصول علم الإجرام وعلم العقاب، دار النهضة العربية القاهره ، ٢٠٠٢م.
27. د. عمر محمد سالم الوجيز في شرح قانون الاجراءات الجنائية، الجزء الأول، مركز جامعة القاهرة للتعليم المفتوح، ٢٠٠٧م.
28. د. فايز الضفيري، المعالم الأساسية لقضية العدالة في مرحلة الاستدلالات والتحقيق الإجرائي"، مجلس النشر العلمي، جامعة الكويت، ٢٠٠١م.
29. د. فرج عيد يونس حسن، التخصص القضائي إحدى الدعائم الأساسية لتحقيق العدالة الناجزة"، دار الجامعة الجديدة، الإسكندرية، ٢٠١٧م.
30. د. مأمون محمد سلامة الإجراءات الجنائية في التشريع المصري، الجزء الأول، دار النهضة العربية، القاهرة، ٢٠٠٨م.
31. د. مجيد خضر السبعاوي، والاستاذ مولان قادر أحمد الضرورة الإجرائية في مرحلة التحقيق الابتدائي – دراسة تحليلية مقارنة ، المركز القومي للإصدارات القانونية، القاهرة، ٢٠١٧م.
32. د. محمد الأمين البشري، الاساليب الحديثة للتعامل مع الجرائم المستحدثة من طرف أجهزة العدالة الجنائية"، محاضرة مقدمة في الحلقة العلمية – تحليل الجرائم المستحدثة والسلوك المنعقدة في الفترة من ١٩-١٧ / ٢٠١١ بمقر جامعة نايف العربية للعلوم الإجرامي الأمنية.
33. د. محمد الأمين البشري، التحقيق الجنائي المتكامل"، أكاديمية نايف العربية للعلوم الأمنية مركز الدراسات والبحوث، الرياض، ١٩٩٨م.
34. د. محمد سعيد نمور أصول الإجراءات الجزائية، شرح لقانون أصول المحاكمات الجزائية"، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، ٢٠١١م.

35. د. محمد صبحي نجم الوجيز في قانون أصول المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٢م.
36. د. محمد عبد الله إبراهيم: المواجهة الأمنية لجرائم شبكة المعلومات الدولية"، اكاديمية الشرطة القاهرة، ٢٠١٦م.
37. د. محمد عمر مصطفى النتيجة وعناصر الجريمة، مجلة العلوم القانونية والاقتصادية، العدد ٢ لسنة ١٩٦٥ ، كلية الحقوق، جامعة عين شمس.
38. د. محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي" ، دراسة مقارنة، دار الجامعة الجديدة، الاسكندرية ، ٢٠١٨م
39. فاروق الكيلاني، محاضرات في قانون أصول المحاكمات الجزائية الاردني والمقارن، ج ٢ ، ط ٢، دار المروج، بيروت ، ١٩٩٥م.
40. محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها – دراسة مقارنة"، رسالة دكتوراه كلية الحقوق، جامعة المنصورة، ٢٠٠٥م.
41. محمد علي محمد عبيد المحواث الحمودي ، دور مأمور الضبط القضائي في مواجهة جرائم المعلومات، رسالة ماجستير ، كلية الحقوق جامعة القاهره، ٢٠٠٩م.
42. مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وأثباتها في فلسطين – دراسة مقارنة"، بحث منشور مجلة علوم الشريعة والقانون الجامعة الأردنية، المجلد ٤٥ ، عدد ٤ ، ملحق ٢، ٢٠١٨م.

ثانياً :- الرسائل والاطاريح

1. احمد سعد محمد الحسيني الجوانب الاجرائية للجرائم الناشئة عن استخدام الشبكات الالكترونية رسالة دكتوراه، كلية الحقوق جامعة عين شمس، ٢٠١٢م.
2. حسين بن سعيد بن سيف الغافري السياسة الجنائية في مواجهة جرائم الانترنت دراسة مقارنة ، رسالة دكتوراه كلية الحقوق جامعة عين شمس، القاهره ٢٠٠٧م.
3. محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت، دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية رسالة ماجستير في العلوم الشرطية، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٤م.

رابعاً :- المجلات

1. الاستاذه بوعناد فاطمة زهرة مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانونية ، الجزائر ، العدد الأول، ٢٠١٣م.