بحث بعنوان:
"الجرائم المعلوماتية أركانها وآلية مكافحتها"
دراسة تحليلية مقارنة

إعداد:

الدكتور لورنس سعيد الحوامدة

Dr. lourane said alhawamdeh

أستاذ مساعد

جامعة طيبة – كلية الحقوق

المملكة العربية السعودية

Email:looooww@yahoo.com

٢٠١٦/٢٠١٧م

❖ تعريف المجلة

مجلة الميزان للدراسات الإسلامية والقانونية، مجلة علمية عالمية محكمة، تصدر عن عمادة البحث العلمي في جامعة العلوم الإسلامية العالمية.

مقر المجلة: جامعة العلوم الإسلامية العالمية.

تصدر المجلة ثلاثة أعداد سنويا.

❖ – أهداف المجلة

١. الإسهام في نشر المعرفة العلمية الأصيلة وتقدمها في مجال الدراسات الإسلامية والقانونية.
٢. الإسهام في المحافظة على هوية الأمة العربية والإسلامية وقيمها وترسيخها والاعتزاز بها.
٣. الإسهام في البناء الحضاري الإنساني ونشر الدعوة الإسلامية القائمة على الوسطية والاعتدال.
٤. المعالجة العلمية لقضايا العصر ومشكلاته.
٥. نشر البحوث المتخصصة في علوم الشريعة (العقيدة و الفكر، التفسير، الحديث، أصول الفقه، الفقه) وفي علوم القانون (الدستوري، المدني، الجنائي، الإداري، الدولي، أصول المحاكمات).

❖ هيئة تحرير مجلة الميزان للدراسات الإسلامية والقانونية للعام الجامعي ٢٠١٥/٢٠١٦

١- أ.د محمود علي السرطاوي رئيساً للتحرير

٢- أ.د نواف كنعان عضواً

٣- أ.د هاني طعيمات عضواً

٤- أ.د أحمد البشايرة عضواً

٥- أ.د محمد الجندي عضواً

٦- د. محمد بني سلامة عضواً

المحرر اللغوي للغة العربية د.احمد الخريشة

المحرر اللغوي للغة الإنجليزية د.ليلى عابدين

امانة سر المجلة امل الغانم

❖ الهيئة الاستشارية

(مرتبة هجائيا)

أ.د. أحمد هليل	قاضي القضاة
أ.د. أحمد الخمليشي	دار الحديث الحسنية / المملكة المغربية
أ.د. جاسم علي سالم الشامسي	جامعة الإمارات العربية المتحدة
أ.د. سالم بويحي	جامعة الزيتونة
أ.د. عبد السلام العبادي	وزير الأوقاف الأسبق

أ.د. محمد يوسف علوان جامعة الشرق الأوسط

أ.د. محمد نعيم ياسين الجامعة الأردنية

أ.د. نظام المجالي جامعة مؤتة

❖ طريقة التوثيق

١- الآيات القرآنية: تنسخ الآية الكريمة بخط المصحف العثماني ويوضع بعد نهاية الآية رقم الآية واسم السورة بين قوسين. مثال [٤٦: آل عمران].

٢- الأحاديث النبوية الشريفة: توثق بالرجوع إلى كتب الحديث الأصلية وذلك ببيان الكتاب والباب ورقم الحديث إن أمكن. مثال: عن عائشة قالت: قال رسول الله صلى الله عليه وسلم: "أحب الأعمال إلى الله تعالى أدومها وإن قل ". مسلم، صحيح مسلم، كتاب صلاة المسافرين وقصرها، باب فضيلة العمل الدائم من قيام الليل وغيره، حديث رقم (٢١٨).

٣- الكتب: توثق الاقتباسات النصية أو المأخوذة بتصرف مشارا إليها بأرقام متسلسلة في نهاية البحث على النحو الآتي:

اسم المؤلف كاملا وتاريخ وفاته هجريا وميلاديا بين قوسين متبوعا بفاصلة، ثم اسم الكتاب (مطبوعا بخط غامق Bold) متبوعا بفاصلة، ثم اسم المحقق أو المترجم -إن وجد- متبوعا بفاصلة، ثم مكان النشر متبوعا بفاصلة، ثم اسم الناشر متبوعا بفاصلة، ثم تاريخ النشر مع بيان الطبعة بين قوسين، ثم رقم الجزء إن وجد متبوعا بفاصلة، ثم رقم الصفحة.

مثال: محمد بن عبد الكريم الشهرستاني (توفي ٥٤٨هـ/ ١١٥٣م)، الملل والنحل، تحقيق: أمير علي مهنا وعلي حسن فاعور، بيروت، دار المعرفة، ١٩٩٨م (ط٧)، ج١، ص١١٨. وإذا ذُكر هذا الكتاب مرة أخرى يُوثّق مختصرا : الشهرستاني، الملل والنحل، ج١، ص٣٤١.

ولا ترفق قائمة بالمصادر والمراجع في نهاية البحث.

٤- النصوص القانونية والأحكام القضائية:

- توثيق النصوص القانونية بذكر النص من مصدره. مثال: المادة (٥) من قانون أصول المحاكمات المدنية رقم (٢٤) لسنة ١٩٨٨.

- توثيق الأحكام القضائية بذكر الحكم من مصدره. مثال: عدل عليا، حكم رقم (١٢٠)، مجلة نقابة المحامين، العدد (١) لعام ١٩٨٩، ص١٦١.

٥-الدوريات العلمية: يتم التوثيق على النحو الآتي:

اسم صاحب البحث كاملا متبوعا بفاصلة، ثم عنوان البحث متبوعا بفاصلة، ثم اسم الدورية (مطبوعا بخط غامق Bold) ومكان صدورها متبوعا بفاصلة، ثم رقم المجلد ورقم العدد متبوعا بفاصلة، ثم تاريخ العدد متبوعا بفاصلة، ثم رقم الصفحة. مثال: عزمي طه السيد أحمد، المقصدان العلمي والأخلاقي لمعاني أسماء الله الحسنى عند الغزالي، مجلة المنارة للبحوث والدراسات، جامعة آل البيت، المجلد (١٠)، العدد ١، ١٩٩٤م، ص٤٥.

٦-النقل من الصحف:

أ- الخبر: يشتمل على اسم الصحيفة، والعدد، والتاريخ، ومكان الصدور.

مثال: الدستور، ع٩٢٥٣، ١٣ حزيران، ١٩٩٣م، عمان.

ب- غير الخبر: يشتمل على اسم الكاتب متبوعا بفاصلة، ثم عنوان المقالة (مطبوعا بخط غامق Bold) متبوعا بفاصلة، اسم الصحيفة والعدد متبوعا بفاصلة، والتاريخ متبوعا بفاصلة، ومكان الصدور.

مثال: محمود درويش، أحد عشر كوكباً، الدستور، عمان، ٣١ آذار ١٩٩٣م، ع١٩٦٥.

٧-المخطوطات: يتم التوثيق على النحو الآتي:

اسم المؤلف كاملا متبوعا بفاصلة، ثم عنوان المخطوط كاملا (مطبوعا بخط غامق Bold) متبوعا بفاصلة، ثم رقم المخطوط متبوعا بفاصلة، ثم مكان المخطوط، ثم رقم الصفحة (أو الورقة) مع بيان الوجه أو الظهر المأخوذ منه الاقتباس باستخدام الرمزين (و) و(ظ) على التوالي.

مثال: ابن حجر العسقلاني (توفي ٨٥٢هـ/ ١٤٤٩م)، ذيل الدرر الكامنة، مخطوط رقم ٦٤٩، المكتبة التيمورية، ورقة ٥٤ (وجه).

❖ شروط النشر

١-يشترط في المخطوط المقدم للنشر في المجلة أن لا يكون قد نُشر أو قُدّم للنشر في مجلة أخرى، وعلى الباحث أن يقدم إقرارا خطيا بذلك عند تقديم المخطوط للنشر.

٢-تخضع جميع المخطوطات المقدّمة للنشر في المجلة للتحكيم العلمي الدقيق حسب الأصول المتّبعة مع الحفاظ على سِرّية التحكيم.

٣-تشمل معايير التقويم كلاً من: الأصالة العلمية للمخطوط، ومدى إضافته للمعرفة، وإمكانية تطبيقه، ومنهجيته، وأسلوبه، ونتائجه، ومدى مراعاة الأمانة العلمية، وسلامة اللغة، وسلاسة أسلوب العرض.

٤-للمجلة أن تطلب إجراء تعديلات على المخطوط قبل إجازته للنشر، كما أن لها الحق في إدخال قدر من "التحرير" على المخطوطات المُجازة.

٥- تحتفظ المجلة بالحق في عدم نشر أي مخطوط دون إبداء الأسباب، ويُعدّ قرارها نهائيا.

٦-أن يوافق الباحث على نقل حقوق النشر إلى المجلة، وفي حالة رغبة المجلة إعادة نشر البحث أو جزء منه يجب حصول المجلة على موافقة الباحث.

٧- يلتزم الباحث بدفع النفقات المترتبة عن إجراءات التقويم إذا رغب الباحث بإيقافها.

٨- يلتزم الباحث بدفع النفقات المترتبة على إجراءات التقييم في حال طلبه البحث وعدم إتمام إجراءات التقييم.

٩-الآراء التي ترد في الأبحاث المنشورة في المجلة تعبر عن آراء الباحثين أنفسهم ولا تعكس بالضرورة سياسة جامعة العلوم الإسلامية العالمية أو هيئة تحرير المجلة.

الجرائم المعلوماتية "أركانها وآلية مكافحتها" – دراسة تحليلية مقارنة

Dr.louranc Said Alhawamdeh

ملخص

تُعدُّ الجرائم المعلوماتية من الجرائم المستحدثة في العصر الحالي؛ لذلك سارعت الدول إلى إيجاد قوانين خاصة لمكافحة هذا النوع من الجرائم، كما عُقِدَت بعض الاتفاقيات الدولية في الإطار الإقليمي كاتفاقية بودابست والصادرة عن المجلس الأوربي بتاريخ ٢٣ نوفمبر سنة ٢٠٠١م، حيث أنَّ هذه الاتفاقية تختص بتنظيم كل ما يتعلق بالجرائم المعلوماتية في الإطار الأوربي. أما على المستوى الدولي، فإن الجهود ما زالت دون المستوى المطلوب من حيث عقد الاتفاقيات الدولية أو القضائية ذات العلاقة بالجرائم المعلوماتية، سيما وأنَّ الجريمة المعلوماتية من الجرائم التي تحتاج إلى تظافر الجهود من أجل مكافحتها وضبط تمدُّدها، حيث تمتاز هذه الجرائم بأنَّها جرائم عابرة للحدود ويصعب إثباتها؛ لذلك تناولت الدراسة مبحثين تحدَّث الأول: عن ماهية الجرائم المعلوماتية من حيث مفهومها، وخصائصها. أما المبحث الثاني: فقد تناول الأركان العامة للجريمة المعلوماتية (الركن المادي، والركن المعنوي)، وآلية مكافحة الجرائم المعلوماتية على المستوى الوطني والدولي.

Abstract

The IT crimes of innovative crimes in the current era, so quick to states to create special laws to combat this type of crime, also held in some international conventions in the regional context, such as the Convention Budapest issued by the European Council on 23 November, 2001, as this agreement is concerned with the organization of All about the crimes of informatics in the European framework, while at the international level, efforts are still below the required terms of contract related crimes informatics especially international or judicial agreements and that the crime of crimes that need to be concerted efforts to control and adjust its expansion where the advantage of this level offenses as transient crimes to the limits and difficult to prove, so the study examined two sections first occur: what the IT crimes in terms of its concept, and their characteristics, and the second topic addressed the General Staff of the crime Informatics (material element, the mental element), and the mechanism for combating IT crimes at domestic and international level.

المقدمة :

تُعدُّ جرائم المعلوماتية من الجرائم المستحدثة، والتي بدأت بالظهور في الوقت الحالي سيما في ظل انتشار هذا النوع من الجرائم بعد ازدياد مستخدمي شبكات التواصل الاجتماعي بطرق غير مشروعة، حيث أصبحت هذه الجرائم تُشكل هاجساً يومياً لكثير من البلدان باعتبارها من الجرائم المنظمة العابرة للحدود، مما دفع الدول إلى التفكير الجاد في معالجة هذا النوع من الجرائم من خلال إيجاد تشريعات وطنية تُجرّم الأفعال غير المشروعة عبر تلك الشبكات والتي تُعدُّ جريمة، حيث سارعت بعض الدول كالأردن، والإمارات، والسعودية، والبحرين وغيرها من الدول في الإطار العربي إلى إيجاد تشريع خاص لمكافحة الجرائم المعلوماتية أُطلق على هذا التشريع ما يسمى "قانون مكافحة الجرائم المعلوماتية"، والتي تنبهت لأهمية هذه الجرائم وضرورة وضع التشريعات اللازمة لمكافحتها.

ولكون جرائم المعلوماتية جرائم خطيرة، فإنَّ التعاون الدولي بين الدول لم يصل إلى المستوى المطلوب من حيث "عقد الاتفاقيات الثنائية، والدولية" ذات الصلة بهذا النوع من الجرائم، أو وجود جهة دولية تكون عبارة عن هيئة أو مركز دولي لتنسيق الجهود الدولية في مكافحة هذا النوع من الجرائم، ونحن نجد أنَّ التعاون الدولي أصبح ضرورة ملحَّة في ظلِّ انتشار هذه الجرائم، ويجب أنْ يكون هذا التعاون في جميع المجالات ذات الصلة بالجريمة ومنها المجال (القضائي، الأمني، وتبادل المعلومات، عقد المؤتمرات الدولية).

لذلك فإن الدراسة ستناقش مبحثين سيتناول **الأول:** ماهية الجرائم المعلوماتية من حيث المفهوم الفقهي والقانوني للجرائم المعلوماتية، وهل توصلت الدول إلى مفهوم جامع مانع للجرائم المعلوماتية ومتفق عليه؟. كما سيتم مناقشة خصائص ومميزات الجرائم المعلوماتية، حيث يُعدُّ من أهم مميزات هذه الجرائم أنَّها ذات طابع دولي وعابرة للحدود، ويصعب اكتشافها وإثباتها. أما المبحث الثاني من الدراسة: سيتناول الأركان العامة للجرائم المعلوماتية (الركن المادي، الركن المعنوي)، وسيخصَّص المحور الأخير من المبحث الثاني لدراسة آلية مكافحة الجرائم المعلوماتية على المستوى الوطني، والدولي، وهل هنالك آليات واضحة لمكافحة هذه الجرائم؟ وهل التعاون بين الدول في مجال مكافحة الجرائم المعلوماتية حقَّق النجاح؟ أم ما **زال** دون المستوى المطلوب؟ كل هذه الأسئلة وغيرها ستكون مجالاً للنقاش والبحث في الدراسة.

إشكالية الدراسة:

تتلخص مشكلة الدراسة في بيان معالجة الدول ومكافحتها لجريمة المعلوماتية من خلال وضع التشريع الناظم لها، والذي يحدِّد العقوبات الرادعة لمرتكبي هذه الجرائم العابرة للحدود، كما

سيتم تناول هذه التشريعات والتركيز على السلبيات والإيجابيات في مضمون كل تشريع يعالج هذه الجريمة، وبالنتيجة بيان الآثار المترتبة لكلّ تشريع خاص بالجريمة المعلوماتية على مكافحة الجريمة وضبط تمدُّدها على المستوى الوطني للدولة التي يطبِّق بها التشريع، كما ستناقش الدراسة مسألة مدى بذلّ الدول الجهود في وضع آليات محدَّدة وواضحة لمكافحة جرائم المعلوماتية على المستوى الوطني والدولي، وهل هنالك محاكم متخصِّصة على المستوى الوطني تُعنى بالنظر في هذا النوع من الجرائم؟ وهل اتَّفقت الدول على صياغة تعريف يُعدُّ جامعاً مانعاً للجرائم المعلوماتية؟ وهل هنالك مركز دولي يُعنى بشكل أساسي بمكافحة جرائم المعلوماتية؟ هذه الأسئلة وغيرها ستكون محور النقاش والبحث في هذه الدراسة والتي تتناول جريمة من الجرائم المستحدثة في الوقت الحالي.

منهجية الدراسة:

تقوم الدراسة على اعتماد المنهج المقارن والتحليلي للنصوص القانونيَّة التي تعالج الجريمة المعلوماتية، من خلال تناول أكثر من نظام قانوني نصَّ على الجرائم المعلوماتية بالتجريم، ومقارنة تلك الأنظمة للوقوف على مدى فعالية تلك الأنظمة في مكافحة الجريمة المعلوماتية، وبيان السلبيات والإيجابيات في هذه الأنظمة، كما سيتم استخدام التحليل للنصوص القانونية وذلك من أجل التعليق عليها، وتفسير بعض المصطلحات الغامضة في النصوص إنْ وُجِدَتْ، وستتناول هذه الدراسة الأنظمة القانونية في مجال الجرائم المعلوماتية في كلٍّ من: (الأردن، الإمارات، البحرين، المملكة العربية السعودية).

أهمية البحث:

مما لا شكَّ فيه أنَّ الجرائم المعلوماتية تُعدُّ من أحدث الجرائم وأهمها في هذا الوقت، وهي تحتاج إلى وضع إطار قانوني للجريمة المعلوماتية عبر الشبكات التكنولوجية، يضمن عدم تمدُّد هذا النوع من الجرائم ومكافحتها، في الوقت الذي لا يكون فيه دائماً وضع التشريعات يكفي لمكافحة هذا النوع من الجرائم، كما سيتم التركيز على الثغرات الموجودة في التشريعات الخاصة بالجريمة المعلوماتية لوضع الحلول المناسبة والملائمة لحلها بشكل منهجي وعلمي مع ضرورة بيان الإيجابيات المترتبة على إيجاد تشريعات وطنية واتفاقيات دولية في مجال مكافحة هذا النوع من الجرائم، كما تكمن أهمية الدراسة في البحث في أركان الجريمة المعلوماتية (الركن المادي

والمعنوي للجريمة) باعتبارها جريمة مستحدثة، والتركيز على وضع الحلول العلمية والإجرائية لمكافحة هذه الجريمة على المستوى الوطني والدولي.

فرضيات الدراسة :

١- هل يوجد تعريف جامع مانع للجرائم المعلوماتية متفق عليه على المستوى الفقهي والتشريعي؟

٢- ما هي آلية مكافحة الجرائم المعلوماتية على المستوى الوطني والدولي؟

٣- هل نجح التعاون الدولي في مجال مكافحة الجرائم المعلوماتية بين الدول؟ أم ما زالَ دون المستوى المطلوب.

٤- هل يوجد مركز دولي مقرّه الأمم المتحدة لمكافحة الجرائم المعلوماتية؟

٥- هل يوجد اتفاقية عربية لمكافحة الجرائم المعلوماتية؟

٦- هل يوجد محاكم متخصّصة للنظر في قضايا الجرائم المعلوماتية؟

٧- هل نصّت قوانين مكافحة الجرائم المعلوماتية على حماية المُبلِّغ عن هذه الجرائم؟

الدراسات السابقة:

أشارت الدراسة إلى مجموعة من المراجع والأبحاث القانونية المتخصّصة السابقة في مجال الجرائم المعلوماتية وهي كالآتي:

١- د. هدى حامد قشقوش، جرائم الكمبيوتر والإنترنت والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدَّم إلى **المؤتمر السادس للجمعية المصرية للقانون الجنائي** والمنعقد في الفترة من (٢٥-٢٨) أكتوبر سنة ١٩٩٣م.

٢- د. هدى حامد قشقوش، **جرائم الحاسب الآلي في التشريع المقارن**، بدون طبعة، القاهرة: دار النهضة العربية، سنة ١٩٩٢م.

٣- د. هشام محمد فريد رستم، **الجرائم المعلوماتية "أصول التحقيق الجنائي الفني"**، بحث مقدَّم لمؤتمر **"القانون والكمبيوتر والإنترنت"**، كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة، في الفترة من ١-٣/٥/٢٠٠٠م، المجلد الثاني، ط٣.

٤- محمد حماد مرهج الهيتي، **التكنولوجيا الحديثة والقانون الجنائي**، ط١، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠٠٤م.

٥- محمد أمين الشوابكة، **جرائم الحاسوب والإنترنت**، ط١، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠٠٤م.

٦- د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، ط٤، القاهرة: دار النهضة العربية، سنة ٢٠٠٤م.

٧- د. جميل عبد الباقي الصغير، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**، بدون طبعة، القاهرة: دار النهضة العربية، سنة ١٩٩٨م.

مصطلحات الدراسة:

تتكوَّن الدراسة من المصطلحات التالية:

١. **الجريمة:** هي القيام بعمل أو الامتناع عن عمل غير مشروع صادر من **إرادة** جنائية، حيث يقرِّر القانون لهذا العمل أو الفعل غير المشروع عقوبة جزائية.
٢. **الجريمة المعلوماتية:** أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية.
٣. **النظام المعلوماتي:** مجموعة برامج وأدوات معدَّة لمعالجة البيانات وإدارتها.
٤. **البيانات:** المعلومات أو الأوامر أو الرسائل أو الأصوات أو الصور التي تُعدّ أو التي سبق إعدادها لاستخدامها في الحاسب الآلي، ولكلّ ما يمكن تخزينه معالجته ونقله وإنشاؤه بواسطة الحاسب الآلي[١].
٥. **الشبكة:** ارتباط بين أكثر من نظام معلوماتي لإتاحة البيانات والمعلومات والحصول عليها.
٦. **الموقع:** حيِّز لإتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدَّد[٢].

خطة الدراسة:

تتكوَّن خطة الدراسة للبحث من المباحث الآتية:

- المبحث الأول: ماهية الجريمة المعلوماتية.
  - المطلب الأول: تعريف الجريمة المعلوماتية.
  - المطلب الثاني: خصائص الجرائم المعلوماتية.
- المبحث الثاني: أركان الجريمة المعلوماتية.
  - المطلب الأول: الركن المادي للجريمة.
  - المطلب الثاني: الركن المعنوي للجريمة.
  - المطلب الثالث: آلية مكافحة الجريمة المعلوماتية.

المبحث الأول:
ماهية الجرائم المعلوماتية

تمهيد وتقسيم:

تُعدُّ الجرائم المعلوماتية من الجرائم المستحدثة والتي ظهرت في عصرنا الحديث؛ والسبب يعود إلى ارتباط هذه الجرائم بوسائل التقنيات الحديثة من أجهزة كمبيوتر وشبكات الإنترنت والمواقع الإلكترونية، ويُعدُّ الإنترنت من أكبر شبكات الكمبيوتر ذات الارتباط الوثيق بالجرائم المعلوماتية وكلمة إنترنت (Internet) في اللغة مشتق من اللغة الإنجليزية (Internet Network) أي شبكة التشبيك ويعني أنها شبكة تربط مجموعة من أجهزة الكمبيوتر المتصلة ببعضها البعض وتستطيع تبادل المعلومات فيما بينها[٣]. أما عن مفهوم الجرائم المعلوماتية فإنه لا يوجد إلى الوقت الحالي تعريف جامع مانع لهذا النوع من الجرائم، وقد اختلف الفقه القانوني في تعريفها. أما التشريعات فنجد بعض التشريعات عَرَّفت الجرائم المعلوماتية بطريقة غير مباشرة وبعضها لم يتعرَّض لتعريف الجرائم المعلوماتية فمهمة المُشرِّع هي تجريم الأفعال ووضع الجزاء المناسب لها. أما تعريف المصطلحات القانونية وشرح النصوص هي من عمل الفقه والقضاء.

لذلك فإن هذا المبحث سيتناول بالدراسة مطلبين هما:

- المطلب الأول: تعريف الجريمة المعلوماتية.
- المطلب الثاني: خصائص الجريمة المعلوماتية.

المطلب الأول:
تعريف الجريمة المعلوماتية

أولاً: المفهوم الفقهي للجريمة المعلوماتية:

لم يُجمع الفقه على وضع تعريف جامع مانع للجريمة المعلوماتية، بل اختلف الفقه في تعريف هذا النوع من الجرائم، "وبتحليل مصطلح معلوماتية informatice يتضح أنه عبارة عن موضوع ومجموعة من العمليات الآلية التي يخضع لها هذا الموضوع، فموضوع المعلوماتية يتمثَّل في البيانات والمعلومات. أما مجموعة العمليات الآلية التي يخضع لها هذا الموضوع فتتمثَّل في عمليات الجمع والتحليل والمعالجة والصياغة والنقل والتداول وغيرها، والتي تتم من خلال الحاسبات أو ما يقوم مقامها من النظم المطوَّرة"[٤]، وقد عَرَّف جانب من الفقه الجريمة

المعلوماتية بأنَّها كلّ فعلٍ غير مشروع يؤدي فيه جهاز الحاسوب دوراً مهماً لإتمام السلوك غير المشروع على أنْ يكون هذا الأداء أو الدور مؤثِّر ومؤدِّي إلى ارتكاب الجريمة [٥].

وقام اتجاه ثاني من الفقه بتعريف الجريمة المعلوماتية بأنَّها: "كلّ أشكال السلوك أو الفعل غير المشروع والذي يُرتكب بواسطة جهاز الحاسوب" [٦].

كما عرَّفها اتجاه ثالث من الفقه أيضاً بأنَّها الاعتداء الواقع على البيانات أو المعلومات أو المعالجة الآلية للبيانات في جهاز الحاسوب بطريقة غير مشروعة. فجرائم المعلوماتية فيها جميع أوجه الاعتداء الإلكترونية الموجَّهة للمعلوماتية، مثل: سرقة البيانات المعلوماتية، وجرائم الملكية الفكرية... وغيرها من الأساليب غير المشروعة الإلكترونية الموجَّهة لقواعد البيانات والمعلومات[٧].

واتجاه رابع من الفقه يرى أنَّ الجريمة المعلوماتية تُعرَّف بحسب وسيلة ارتكاب الجريمة، وهي بذلك تشمل كلّ أشكال السلوك أو الأفعال التي تضرُّ بالمجتمع، والتي تُرتكب باستخدام الحاسب الآلي والإنترنت[٨].

أما الاتجاه الخامس فقد جاء عكس الاتجاه الرابع في تعريف الجريمة المعلوماتية، حيث عرَّفها من جانب موضوع الجريمة وليس وسيلة ارتكابها، حيث عُرِّفت بأنَّها مجرَّد نشاط موجَّه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحوَّل عن طريقه[٩].

لكن السؤال الذي يطرح نفسه هو: هل جرائم الكمبيوتر أشمل من مصطلح جرائم المعلوماتية أما لا؟

يرى جانب من الفقه أنَّ استخدام مصطلح جرائم الكمبيوتر أعمُّ وأشمل من استخدام مصطلح جرائم المعلوماتية؛ لأنَّ جرائم الكمبيوتر تشمل كافة الجرائم التي تقع على الحاسبات بشكل عام أو بواسطة الحاسوب، والذي يستخدم فيها الحاسوب كأداة لارتكاب الجريمة، حيث يشمل ذلك الاعتداء على المعلومات الموجودة في الحاسوب[١٠].

ويتفق الباحث مع هذا الرأي من حيث شمولية مصطلح جرائم الكمبيوتر عن مصطلح جرائم المعلوماتية، حيث أنَّ جرائم المعلوماتية تشمل من حيث المفهوم الاعتداء على المعلومات والبرامج داخل جهاز الكمبيوتر، بينما مصطلح جرائم الكمبيوتر أعمُّ وأشمل من حيث المفهوم والمضمون، فهي جرائم تُرتكَب على جهاز الحاسوب وبواسطة الحاسوب كأداة ويشمل الاعتداء على الحاسوب الاعتداء على المعلومات والبرامج من حيث المضمون.

كما أنني لا أتفق مع الاتجاه الفقهي الرابع والخامس واللذين عرَّفا الجريمة المعلوماتية من حيث الموضوع والوسيلة، فالبعض أخذ بالاتجاه الذي يدعو إلى تعريف الجريمة المعلوماتية بحسب وسيلة ارتكابها، والبعض الآخر عرَّف الجريمة المعلوماتية بحسب موضوعها، ويرى

الباحث أنَّ الجريمة المعلوماتية تشمل الوسيلة والموضوع محل الجريمة، وكلاهما وجهان لعملة واحدة، ومن الصعوبة الفصل بين وسيلة ارتكاب الجريمة ومحلها.

ونحن نجد أنَّ تعريف الجريمة المعلوماتية هي كل فعل غير مشروع يستهدف تغيير البيانات أو المعلومات من حيث الحذف والإضافة أو المعالجة أو السرقة أو تحوير المعلومات أو تعديلها لغايات غير مشروعة بواسطة الحاسوب أو أي وسيلة تكنلوجية. مع ملاحظة أنَّ مسمى جرائم الكمبيوتر أو الجرائم الإلكترونية من حيث المنهج هي أشمل من جرائم المعلوماتية؛ لأنَّ كل البيانات والمعلومات التي يتم تغييرها أو التلاعب فيها تتم بواسطة جهاز الحاسوب وعن طريقه، فالمعلومات محل الجريمة هي جزء من أجهزة الحاسوب مع الإشارة إلى أنَّ مسمى الجرائم المعلوماتية لا يُعدُّ أقل أهمية من مسمى الجرائم الإلكترونية، فالمعلومات وجهاز الحاسوب هما الأساس في قيام هذا النوع من الجرائم.

ثانياً: المفهوم القانوني للجريمة المعلوماتية:

تُعدُّ الجريمة المعلوماتية من الجرائم المستحدثة في العصر الحالي ولأهمية هذا النوع من الجرائم سارعت الدول إلى إيجاد قانون خاص يعالج المشاكل الناتجة عن الأفعال غير المشروعة، عبر استخدام أجهزة الحاسوب أو أي وسيلة من وسائل تقنية المعلومات؛ لذلك نجد أنَّ بعض التشريعات اهتمت بتعريف الجريمة المعلوماتية في المواد الأولى من القانون الذي يعالج هذا النوع من الجرائم.

ويرى الباحث أنَّ قيام المُشرِّع بتعريف المصطلحات القانونية، أو تحديد مفهومها، أو شرحها يُعدُّ تجاوزاً على عمل الفقه والقضاء، والذي يتولى بدوره شرح النصوص القانونية والتعليق عليها وتحديد مفهومها. أما فيما يتعلق ببعض الجرائم المستحدثة، ومنها: الجرائم المعلوماتية، والتي تتشكَّل، كظاهرة خطيرة على المجتمعات والدول، ويتفق الباحث مع قيام المُشرِّع بتوضيح أو تعريف بعض المصطلحات القانونية ذات العلاقة بالجريمة محل الدراسة.

وفي الكويت عَرَّف المُشرِّع الكويتي الجريمة المعلوماتية في المادة (١) من قانون مكافحة جرائم تقنية المعلومات رقم (٦٣) لسنة ٢٠١٥م، حيث نصَّت المادة "في تطبيق أحكام هذا القانون يقصد بالمصطلحات التالية المعنى الموضح قرين لكل منها:

- الجريمة المعلوماتية: كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون."

أما نظام مكافحة الجرائم المعلوماتية السعودي فقد عرَّف الجريمة المعلوماتية بأنها: "أي فعل يُرتكب متضمّناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[١١].

أما في مملكة البحرين فإنَّ المُشرِّع البحريني في قانون جرائم تقنية المعلومات رقم (٦٠) لسنة ٢٠١٤م لم يُعرِّف الجرائم المعلوماتية في المادة الأولى منه، إنما اكتفى المُشرِّع البحريني بتعريف بعض المصطلحات، كذلك فعل المُشرِّع الأردني في قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥م، والمُشرِّع الإماراتي في قانون مكافحة تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢م.

ويمكن القول أنَّ المُشرِّعَين الكويتي والسعودي تقدَّما على التشريعات الأخرى عندما عرَّفا الجريمة المعلوماتية، حيث أنَّ تعريف الجريمة المعلوماتية نقطة ارتكاز مهمة للتشريع محل البحث لما للجريمة المعلوماتية من أهمية، كونها من الجرائم المستحدثة في العصر الحالي والتي تتطلَّب بيان مفهومها وتعريفها في صلب النصوص.

المطلب الثاني:
خصائص الجرائم المعلوماتية

تتميَّز الجرائم المعلوماتية بعدّة خصائص تُميِّزها عن غيرها من الجرائم غير المستحدثة التقليدية نظراً لحداثة هذه الجريمة في العصر الحالي، وللوسائل المستخدمة في ارتكابها وطريقة ارتكابها. ومن هذه الخصائص التي تتميَّز بها الجريمة المعلوماتية الآتي:

أولاً: الجرائم المعلوماتية جريمة عابرة للحدود:

تُعدُّ الجرائم المعلوماتية من الجرائم غير المقيدة والمرتبطة بمنطقة جغرافية معيَّنة، فمن المتصوَّر أنْ ترتكب الجريمة في أي وقتٍ دون الالتزام والتقيُّد بدولة ما أو منطقة ما أو بقرب المسافات أو تباعدها، ويتم ارتكاب الجرائم المعلوماتية بواسطة الحواسيب وعن طريق الشبكة المعلوماتية[١٢].

لكن السؤال الذي يطرح نفسه هو: هل لتباعد المسافات بين الفعل غير المشروع الذي يرتكبه المجرم المعلوماتي والنتيجة الجرمية لهذا الفعل أثر في اكتشاف الجريمة أم لا؟

يرى اتجاه من الفقه صعوبة اكتشاف الجريمة المعلوماتية من حيث عدم وجود الفاعل، أي: المجرم المعلوماتي، نظراً لارتكاب جريمته عن بُعد، ومن ثم تباعد المسافات بين الفعل الذي

يرتكب من خلال جهاز الحاسوب وبين النتيجة الجرمية، وبالتالي فإنَّ الجريمة المعلوماتية لا تقف عند حدود دولة معينة، بل تمتدُّ إلى حدود الدول الأخرى، مما يصعب بالنتيجة اكتشافها والوصول إلى الحقيقة[١٣].

ونلاحظ بأنَّ اختراق الجريمة المعلوماتية حدود الدول وبالتالي صعوبة اكتشافها يحتاج من الدول العمل على تظافر الجهود في مجال وضع تشريعات وطنية لمعالجة هذا النوع من الجرائم، ومن ثم العمل على المستوى الدولي عبر الأمم المتحدة؛ لإنشاء مركز دولي لمكافحة الجرائم المعلوماتية يكون مقرَّه الأمم المتحدة، بحيث يقوم المركز بوضع القواعد الأساسية للاتفاقيات الدولية في مجال مكافحة الجرائم المعلوماتية، وعقد المؤتمرات الدولية ذات الصلة بالجريمة؛ لوضع الحلول للمشاكل التي تترتَّب على مثل هذا النوع من الجرائم الحديثة في العصر الحالي.

لكن السؤال الذي يطرح نفسه هو: إذا تجاوزت الجريمة المعلوماتية حدود دولة ما، فأي الدول يحقُّ لها تحريك دعوى الحق العام بحقِّ المتهم؟ وكيف يتم تحديد الاختصاص القضائي؟

من المتعارف **أنَّ** قوانين الإجراءات الجنائية حدَّدت الاختصاص القضائي للجرائم بمكان وقوع الجريمة أو مكان إلقاء القبض على المشتكى عليه أو موطنه، حيث نصَّت المادة **(١/٥)** من قانون أصول المحاكمات الجزائية الأردني رقم (٩) لسنة ١٩٦١م وتعديلاته على تحديد الاختصاص القضائي كما يأتي: "تقام دعوى الحق العام على المشتكى عليه أمام المرجع القضائي المختص التابع له مكان وقوع الجريمة أو موطن المشتكى عليه أو مكان إلقاء القبض عليه... الخ".

ونحن نرى أنَّ المُشرِّع حدَّد الاختصاص القضائي للجرائم التي تقع داخل حدود الدولة، ولم يعالج مسألة تمدُّد الجريمة خارج حدود الدولة، وقياساً على ذلك فإن الباحث يقترح أنْ تتضافر الجهود الدولية بين الدول؛ لإيجاد اتفاقية دولية في مجال الجرائم المعلوماتية تنصُّ في أحد أجزائها على الاختصاص القضائي، بحيث يحدِّد الاختصاص القضائي في مكان وقوع الجريمة أو مكان إلقاء القبض على المشتكى عليه أو موطنه، حيث أنَّ تحديد الاختصاص القضائي في مثل هذا النوع من الجرائم يؤدي إلى مكافحتها وضبط توسُّعِها، مع الأخذ بعين الاعتبار ضرورة تعديل التشريعات الوطنية في مجال مكافحة الجرائم المعلوماتية بالنص وبشكلٍ صريح على الاختصاص القضائي، ويرى الباحث أنَّ المُشرِّع الأردني أشار إلى تحديد الاختصاص القضائي وبشكلٍ غير مباشر في نصِّ المادة (١٧) من قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥م، والتي نصَّت على أنَّه "تقام دعوى الحق العام والحق الشخصي على المشتكى عليه أمام المحاكم الأردنية إذا ارتُكِبَت أي من الجرائم المنصوص عليها في هذا القانون

باستخدام أنظمة معلومات داخل المملكة، أو ألحقت أضراراً بأي من مصالحها أو بأحد المقيمين فيها أو ترتَّبت آثار الجريمة فيها، كلِّياً أو جزئياً، أو ارتُكِبَت من أحد الأشخاص المقيمين فيها".

وفي الإطار العربي نصَّت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٤م في المادة (٣٠) منها على الآتي: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمدِّ اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلِّياً أو جزئياً أو تحقَّقتْ:

أ- في إقليم دولة طرف.

ب- على متن سفينة علم الدولة الطرف.

ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف.

د- إذا كانت الجريمة تمسُّ أحد المصالح العليا للدولة.

كما أنَّ اتفاقية بودابست الموقَّعة في ٢٣ نوفمبر ٢٠٠١م بخصوص الجرائم المعلوماتية قد أحالت بخصوص الإجراءات الجنائيَّة، ومنها الاختصاص القضائي إلى الدول الموقَّعة على الاتفاقية أو الأطراف فيها، حيث نصَّت المادة (١٤) من الاتفاقية على الآتي: "يجب على كلِّ طرف أنْ يتخذ الإجراءات التشريعية، وأيّة إجراءات أخرى يرى أنَّها ضرورية من أجل إنشاء السلطات والإجراءات المنصوص عليها في هذا القسم بغرض التنقيبات أو الإجراءات الجنائية الخاصة"[١٤].

ثانياً: صعوبة إثبات الجرائم المعلوماتية:

تمتاز الجرائم المعلوماتية بصعوبة إثباتها من حيث عدم إيجاد الدليل الذي يُدين مُرتكب الجريمة بطريقة مُيسَّرة ومنهجية. ويرى اتجاه من الفقه أنَّ الجرائم المعلوماتية يسهل فيها محو الدليل، والتلاعب فيه، خصوصاً مع عدم وجود الدليل المادي للجرائم المعلوماتية (كالدم والشعر، والبصمة، ... الخ)، ويرافق ذلك عدم توفُّر الخبرة الكافية لدى رجال الشرطة في الأمور الفنية والتفصيلية ذات الصلة بالجرائم المعلوماتية[١٥].

ويؤكد اتجاه ثانٍ من الفقه على صعوبة اكتشاف الجرائم المعلوماتية، وإقامة الدليل على مرتكبيها؛ ويعود ذلك لعلاقة هذا النوع من الجرائم بالطابع التقني، والذي يعطي هذه الجرائم ويضفي عليها الكثير من التعقيد والصعوبة في الإثبات، وإقامة الدليل على من يرتكب هذه الجرائم، كما أنَّ سهولة تدمير المعلومات وسرعة التخلُّص منها سمة من سمات هذه الجريمة التي يصعب اكتشافها للأسباب الوارد ذكرها[١٦].

ويرى الباحث ضرورة تكاتف الجهود الدوليّة والوطنيّة للدول في مجال إعداد رجال الشرطة الدولية (الإنتربول)، والشرطة المحلية للدول، إعداداً تقنياً وفنياً في مجال مكافحة الجرائم

المعلوماتية عن طريق تأهيلهم؛ وذلك بإلحاقهم بعمل دورات متخصّصة في موضوع هذا النوع من الجرائم، كما يُفترض أيضاً إيجاد محاكم متخصّصة يمتاز قُضَاتُها بدرجةٍ عاليةٍ من التأهيل العلمي والتقني في موضوع هذه الجرائم، أو على الأقل وجود هيئات قضائية متفرّغة متخصّصة بالنظر في مثل هذا النوع من الجرائم، بالإضافة إلى تحديد أدلّة الإثبات في قوانين مكافحة الجرائم المعلوماتية بالتنسيق مع الدول والأمم المتحدة في هذا الإطار؛ وذلك لصعوبة إثبات هذا النوع من الجرائم والكشف عن مرتكبيها.

ثالثاً: قلّة الإبلاغ عن الجريمة المعلوماتية:

نظراً لحساسية هذا النوع من الجرائم وما يتعرَّض له المجني عليه كطرف في الجريمة من تشهير فيما لو أبلغ عن الجريمة، فإنَّ الإبلاغ عن هذا النوع من الجرائم قليل مقارنة مع غيرها من الجرائم، حيث أنَّ معظم جرائم الإنترنت والجرائم المعلوماتية يتم اكتشافها مصادفة، وقد يكون هذا الاكتشاف بعد مُدة طويلة من ارتكاب الجريمة، وهذا يدلُّ على أنَّ الجرائم التي لم تكتشف أكثر بكثير من الجرائم التي تم اكتشافها، وبعبارة أخرى فإنَّ الفجوة بين عدد هذه الجرائم الحقيقي وبين ما تم اكتشافه فجوة كبيرة[١٧]. فنقص الخبرة لدى الجهات المختصَّة أدَّى إلى ازدياد عدد الجرائم المعلوماتية بشكلٍ ملحوظ؛ وذلك بسبب عدم قدرة هذه الجهات على التعامل مع هذا النوع من الجرائم المستحدثة بالوسائل الاستدلالية والإجراءات الجنائية التقليدية، وهذا أدَّى إلى عدم بذل الجهود الكافية من قبل رجال الشرطة للكشف عن هذه الجرائم لعدم الخبرة والمعرفة الفنيّة بطبيعتها وأهميتها[١٨].

ويرى الباحث ضرورة تعديل قوانين مكافحة الجرائم المعلوماتية بوجود نصوص تحمي المُبلِّغ عن هذه الجرائم، من حيث سريّة التبليغ وسرية التحقيق والمحاكمة في هذا النوع من الجرائم، كذلك اشتمال النصوص على محفزات لمن يُبلِّغ عن هذه الجرائم كمبلغ مالي مثلاً يُعطى للشخص الذي يُبلِّغ عن هذه الجرائم تشجيعاً للتبليغ عنها وبالنتيجة مكافحتها.

رابعاً: تمتاز الجرائم المعلوماتية بأنَّها جرائم ناعمة:

حيث يتميَّز هذا النوع من الجرائم بعدم بذل أي مجهود عضلي أو جسدي من الجاني بعكس الكثير من الجرائم الأخرى كجرائم (القتل، والخطف الجنائي، والزنى، والاغتصاب... الخ) والتي تحتاج إلى مزيد من الجهد العضلي والجسدي لإتمام الجريمة. أما جرائم المعلوماتية وباعتبارها من الجرائم المستحدثة فإنَّها لا تحتاج إلا إلى القدرة الذهنية

والعضليَّة للجاني مع إلمامه بتقنيات الحاسوب وتكنولوجيا المعلومات، بحيث يمكِّنه ذلك من ارتكاب الجريمة بشكلٍ سريع دون أنْ يترك الجاني أي أثر[١٩].

لكن السؤال الواجب الإجابة عليه هو: هل يتميَّز المجرم المعلوماتي عن غيره من المجرمين في الجرائم الأخرى أم لا؟

نرى أنَّ الجرم المعلوماتي يتميَّز بعدَّة خصائص تميِّزه عن غيره من المجرمين في الجرائم الأخرى، ويمكن تلخيص هذه الخصائص بما يأتي:

أ. تكرار المجرم المعلوماتي الجرائم المعلوماتية: يعود العديد من المجرمين المعلوماتيين إلى تكرار ارتكاب هذا النوع من الجرائم المستحدثة، إما لاهتمامهم بالاطلاع على المعلومات وكشف الأسرار، أو حصولهم على الأرباح المالية جرَّاء ارتكاب هذه الجرائم، أو إضراراً بالغير[٢٠].

ونجد أنَّ تكرار الجرائم المعلوماتية من قبل المجرم المعلوماتي اعتبرته بعض التشريعات الخاصة بمكافحة الجرائم المعلوماتية ظرف مشدِّد، حيث نصَّت المادة (١٦) من قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥م على ما يأتي: "تضاعف العقوبة المنصوص عليها في هذا القانون في حال تكرار أي من الجرائم المنصوص عليها فيه". أما قانون جرائم تقنية المعلومات البحريني رقم (٦٠) لسنة ٢٠١٤م لم يتحدَّث عن عقوبة تكرار الجريمة بالنسبة للجاني، إنما أشار إلى العقوبة على التكرار فيما يخصُّ "شخص اعتباري" بأنْ يتم غلق المقر الذي تمَّت فيه الجريمة أو العقار الذي يمارس فيها نشاطاً يتعلق بالجريمة غلقاً نهائياً أو للمدة التي تقرِّرها المحكمة[٢١]. أما قانون مكافحة جراء تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢م ونظام مكافحة الجرائم المعلوماتية السعودي رقم (م/١٧) تاريخ ١٤٢٨/٣/٨هـ، ونلاحظ خلو هذه التشريعات من الإشارة إلى الظرف المشدِّد في تكرار المجرم المعلوماتي الجريمة المعلوماتية مما يؤدي بالنتيجة إلى عدم مكافحة هذا النوع من الجرائم وضبطها.

ويتمنى الباحث على المُشرِّعَين السعودي والإماراتي ضرورة تعديل قوانين مكافحة الجرائم المعلوماتية بإضافة نص صريح يعاقب المجرم المعلوماتي على تكرار الجريمة حتى يتم بالنتيجة مكافحة هذا النوع من الجرائم وضبطها.

ب. تخصُّص المجرم المعلوماتي في تكنولوجيا الحاسوب: يُعدُّ المجرم المعلوماتي من المجرمين الذين يمتازون بالتخصُّص في تكنولوجيا المعلومات والحاسوب، حيث تمكِّنه قدراته الذهنية والعقليَّة والفنيَّة من التعامل مع أجهزة الحاسوب في ارتكاب الجرائم المعلوماتية بسهولة وسرعة عالية وفي وقتٍ قصير، بعكس المجرمين في الجرائم الأخرى حيث يمتاز بعضهم بعدم الاختصاص والمعرفة في الجرائم التي يرتكبونها[٢٢].

ويرى اتجاه من الفقه أنَّ المجرم المعلوماتي يتميَّز عن غيره من الجناة في الجرائم الأخرى، حيث يتمتع بمهارات وقدرات تمكِّنه من تشغيل الحاسب الآلي وبالنتيجة اختراق نظم الحماية والكودات السرية للبرامج والمعلومات والبيانات من أجل تحقيق النيَّة الإجراميَّة لديه، أو لإظهار تفوقِّه على الآلة أو بدافع اللهو والترف[٢٣].

وبالنتيجة فإنَّ المجرم المعلوماتي يتميَّز بصفات وخصائص تختلف عن مرتكب الجرائم التقليدية، وهذا مرجعه إلى تميُّز شخصية مرتكبي الجرائم المعلوماتية بالتقدُّم في مجال استخدام الحاسب الآلي، بعكس المجرم العادي في الجرائم التقليدية والذي غالباً ما يتميَّز بالقوة العضلية ونادراً ما يتميَّز بعضهم بعنصر الذكاء[٢٤].

ويرى الباحث بأنَّ الجرائم المعلوماتية جرائم تحتاج إلى دقة عالية ومعرفة فنيَّة تخصُّصية ودقيقة، ولهذا فإنَّ المجرم المعلوماتي يجب أنْ يكون على معرفة فنية علمية بجهاز الحاسوب والإنترنت وكيفية التعامل مع البيانات وتخزينها ومعالجتها وحذفها حتى يتمكَّن من إتمام الجريمة، وبناءً على ذلك فإنَّه لا يستطيع أي شخص أنْ يرتكب الجرائم المعلوماتية دون المعرفة التامة بكيفية التعامل مع جهاز الحاسوب والإنترنت والبيانات والمعلومات بشكلٍ منهجي ودقيق.

المبحث الثاني:
أركان الجريمة المعلوماتية

تمهيد وتقسيم:

تُعدُّ أركان الجريمة الأساس والأصل لقيام أي جريمة، والمُشرِّع يفترض لقيام الجريمة توافر أركانها المادي والمعنوي، وبدون هذين الركنين لا تقوم الجريمة.

ويتكوَّن الركن المادي للجريمة من الفعل والنتيجة والعلاقة السببية تربط بين الفعل والنتيجة، فلا جريمة دون فعل غير مشروع أو امتناع عن القيام بفعل غير مشروع.

أما الركن المعنوي للجريمة فيتكوَّن من العلم والإرادة، ويجب أنْ ينصَّب علم الجاني على مضمون الأفعال غير المشروعة، فالعلم والإرادة عملية نفسية تتعلق بنفسية الجاني مرتبطة بماديات الجريمة، لذا فإنَّ هذا المبحث سيناقش ثلاثة مطالب أساسية هي:

- المطلب الأول: الركن المادي للجريمة المعلوماتية.
- المطلب الثاني: الركن المعنوي للجريمة المعلوماتية.
- المطلب الثالث: آلية مكافحة الجرائم المعلوماتية.

المطلب الأول:
الركن المادي للجريمة المعلوماتية

تتكوَّن الجريمة المعلوماتية كغيرها من الجرائم من الركن المادي للجريمة، والذي يفترض وجوده لقيام الجريمة، ويتكوَّن الركن المادي للجريمة المعلوماتية من ثلاثة عناصر نجملها بالآتي:

أولاً: الفعل أو السلوك غير المشروع:

يتطلَّب القيام بالجريمة المعلوماتيَّة وجود جهاز الحاسوب والاتصال بشبكة الإنترنت، وكذلك يفترض معرفة الجاني بإدارة النشاط والمعرفة في استخدام جهاز الحاسوب، كما يفترض قدرة الجاني الذهنية والجسمانية على تجهيز الحاسوب؛ لكي يتحقَّق له حدوث الجريمة، فيقوم بتحميل الحاسب ببرامج اختراق، أو يقوم بإعداد هذه البرامج بنفسه أو يقوم مثلاً بتهيئة صفحات مخلَّة بالآداب وتحميلها على الجهاز المضيف Hosting Server، كما يمكن أنْ يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها[٢٥].

أما من الناحية القانونية فإنَّ السلوك أو الفعل غير المشروع في الجريمة المعلوماتية له عدَّة صور وتختلف هذه الصور للسلوك أو الفعل غير المشروع من تشريع لآخر، ففي التشريع الأردني نصَّ المُشرِّع على الأفعال غير المشروعة في قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥م كما يأتي:

أ. فعل الدخول إلى الشبكة المعلوماتية أو نظام المعلومات دون تصريح رسمي.

ب. الدخول إلى الشبكة المعلوماتية بطريقة غير مشروعة من أجل الإلغاء أو الحذف أو التعديل أو التغيير أو التدمير أو النقل أو النسخ للبيانات أو المعلومات بطريقة غير مشروعة.

ج. فعل الدخول إلى الموقع الإلكتروني من أجل إتلافه أو تعديل محتوياته أو انتحال شخصية مالكه أو تغييره أو إلغائه أو إتلافه.

د. فعل الاعتراض أو التصنُّت أو الشطب على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات.

هـ. كل فعل يتضمَّن الحصول قصداً عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلَّق ببطاقات الائتمان أو البيانات أو المعاملات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية.

و. فعل الإرسال أو النشر عن طريق نظام المعلومات أو الشبكات المعلوماتية بوسائل الإعلام المسموعة أو المقروءة أو المرئية بحيث يتضمَّن الفعل أعمالاً إباحية أو تتعلَّق بالاستغلال الجنسي أو الترويج للدعارة أو ذم أو قدح أو تحقير أي شخص.

ز. فعل الدخول قصداً أو دون تصريح إلى الشبكة المعلوماتية أو المعلومات غير المتاحة للجمهور والتي تمسُّ الأمن الوطني أو السلامة العامَّة أو الاقتصاد الوطني[٢٦].

وباستعراض النصوص لقانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥م نجد أنَّ المُشرِّع الأردني عالج جميع الأفعال الناتجة عن الجرائم الإلكترونية بمنهج شمولي، حيث لم يترك المُشرِّع الأردني فعلاً له علاقة بالجرائم المعلوماتية، إلا وعالجه بالتجريم والعقاب مع ملاحظة عدم النص على بعض الأفعال الموجودة في التشريعات الأخرى، ومنها التشريع الإماراتي الذي نصَّ في قانون جرائم تقنية المعلومات رقم (٥) لسنة ٢٠١٢م على بعض الأفعال غير المشروعة والتي لم يتم التعرُّض إليها بالتشريع الأردني ومنها:

أ. فعل التعديل أو الإتلاف أو الإفشاء أو الحصول بغير تصريح على بيانات أو مستند إلكتروني عن طريق الشبكة المعلوماتية أو أي موقع إلكتروني أو وسيلة تقنية معلومات تتعلق بفحوصات طبية أو تشخيص طبي أو رعاية طبية أو سجلات طبية.

ب. فعل الابتزاز أو التهديد لشخص لحمله على القيام بعمل أو الامتناع عنه باستخدام شبكة المعلومات أو أي وسيلة تقنية معلومات.

ج. فعل إنشاء أو إدارة موقع إلكتروني أو الإشراف عليه أو نشر معلومات على الشبكات المعلوماتية أو أي وسيلة تقنية، وذلك لجماعة إرهابية أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة[٢٧].

مع ملاحظة أنَّ المُشرِّع الأردني جَرَّم فعل إنشاء موقع إلكتروني أو استخدام نظام معلومات بطريقة غير مشروعة ولصالح جماعات إرهابية في المادة (٣/هـ) من قانون منع الإرهاب الأردني رقم (٥٥) لسنة ٢٠٠٦م حيث نصَّت المادة على أنه يُعدُّ من الأعمال الإرهابية ما يلي: "استخدام نظام المعلومات أو الشبكة المعلوماتية أو أي وسيلة نشر أو إعلام أو إنشاء موقع إلكتروني؛ لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل من شأنه تعريض الأردنيين أو ممتلكاتهم لخطر أعمال عدائية أو انتقامية تقع عليهم".

ويرى الباحث أنَّ المُشرِّع الأردني وقع في خطأ عندما وضع هذه المادة وبما تحتوي من أفعال غير مشروعة مجرمة في قانون منع الإرهاب يتم ارتكابها على النظام المعلوماتي أو الشبكة المعلوماتية في هذا القانون، والأصل أنْ يتم وضع هذه المادة في قانون مكافحة الجرائم المعلوماتية الأردني رقم (٢٧) لسنة ٢٠١٥م بدلاً من قانون منع الإرهاب.

أما نظام مكافحة جرائم المعلوماتية السعودي رقم (م/١٧) تاريخ ١٤٢٨/٣/٨هـ فنجد أنه اتَّفق مع المُشرِّعين الأردني والإماراتي في النص على جميع الأفعال غير المشروعة الواردة في كلا القانونين.

ويمكن القول أنَّ وضع صور للأفعال غير المشروعة للجرائم المعلوماتية في قوانين خاصة لمكافحتها يُعدُّ نقطة تحول نحو مكافحة الجرائم المعلوماتية على المستوى الوطني والدولي، كما نحثُّ الدول الأخرى سواءً في الإطار العربي أو الدولي على ضرورة إيجاد تشريع خاص بمكافحة هذا النوع من الجرائم لخطورتها وآثارها الآنية والمستقبلية في حال عدم وجود إطار قانوني لضبطها على المستوى الداخلي للدول.

لكن السؤال الذي يطرح نفسه هو: هل يشكِّل العمل أو الفعل التحضيري في الجرائم المعلوماتية جريمة أم لا؟

ويرى الباحث أنَّ العمل التحضيري وفي معظم الجرائم لا يشكِّل جريمة يعاقب عليها القانون، إلا إذا أُعتبر العمل التحضيري جريمة أو فعل غير مشروع يعاقب عليه القانون كان يقوم شخص بشراء سلاح ناري دون ترخيص ليقتل شخصاً آخر، إلا أنَّه لم يقم بارتكاب جريمة

القتل، فالعمل التحضيري في هذه الجريمة هو شراء السلاح وبدون ترخيص وهذا معاقب عليه حسب قوانين الأسلحة والذخائر النارية في معظم الدول، أما في إطار الجرائم المعلوماتية فإنَّ العمل التحضيري وقياساً على باقي الجرائم لا يشكِّل جريمة، إلا إذا كان في حدِّ ذاته جريمة مستقلة كشراء برامج للدخول إلى المواقع الإلكترونية، أو آلات لفك الشفرات وكلمات المرور، أو برامج بها صور دعارة أو إباحية، كل ذلك يشكِّل أفعالاً غير مشروعة يعاقب عليها القانون.

ويختلف النشاط غير المشروع أو الفعل في الجريمة المعلوماتية باختلاف نوع الجريمة المرتكبة، حيث تتعدَّد أنواع الجرائم المعلوماتية وتختلف أفعالها من جريمة لأخرى، فمثلاً جريمة إتلاف المعلومات أو تحويرها أو تخريبها، فإن الفعل غير المشروع في هذا النوع الجزئي من الجريمة المعلوماتية ينصبُّ على قيام الجاني بتخريب المعلومات أو تحويرها أو إتلافها في جهاز الحاسوب وبسوء نية، وقد عاقبت معظم التشريعات الوطنية على هذا النوع من الجرائم المعلوماتية، وقد يتخذ صور الفعل غير المشروع في الجريمة المعلوماتية تحريف مفتعل للحقيقة أو تغيير للحقيقة للمعلومات داخل النظام المعلوماتي من خلال محو جزء أو عدَّة أجزاء من المعلومات في جهاز الحاسوب، وتسمى هذه الجريمة (التزوير) للمعلومات وهي نوع من أنواع الجرائم المعلوماتية، والتي يتخذ الفعل فيها تحريف للحقيقة في المعلومات في النظام المعلوماتي[٢٨]. ونجد أنَّ بعض التشريعات عاقبت على هذه الأفعال غير المشروعة ومنها التشريع الأردني حيث نصَّت المادة (٦٧) من قانون الاتصالات الأردني رقم (١٣) لسنة ١٩٩٥م وتعديلاته لسنة ٢٠١١م على أنَّه "كل من اعترض أو أعاق أو صوَّر محتويات رسالة بواسطة شبكات الاتصالات، أو شجَّع غيره على القيام بهذا العمل يعاقَب بالحبس مدة لا تقل عن شهر ولا تزيد عن ستة أشهر أو بغرامة لا تزيد عن (٢٠٠) دينار أو بكلتا العقوبتين".

وقد يترتَّب أيضاً على القيام بالنشاط المادي غير المشروع في استخدام تقنية الكمبيوتر بواسطة الإنترنت ارتكاب جريمة القتل وإزهاق روح إنسان بسوء نيَّة، فالطبيب العامل في المستشفى يستطيع أنْ يصل إلى قاعدة البيانات الخاصة بتوزيع الدواء في المستشفى من منزله أو من أي مكان آخر ومن ثم يقوم بتعديل أو تغيير معدل الدواء لأحد المرضى بقصد قتله[٢٩].

ويرى الباحث أنَّ الفعل غير المشروع أو النشاط يُعدُّ عنصر من عناصر الركن المادي للجريمة المعلوماتية، فلا جريمة دون سلوك أو فعل غير مشروع.

ثانياً: النتيجة الجرمية:

تُعَدُّ النتيجة الجرمية أحد أهم عناصر الركن المادي لأي جريمة، حيث تعتبر النتيجة الجرمية الأثر المباشر للسلوك الجرمي غير المشروع، وفي كثير من الأحيان لا يحدّد القانون على وجه التفصيل أوصاف السلوك المحظور، بل يكتفي بذكر النتيجة الجرمية، حيث يحدّد أوصاف السلوك بناءً على طبيعة النتيجة الجرمية[٣٠].

ويرى اتجاه من الفقه أنَّ النتيجة هي التغيير الذي يحدث كأثر للسلوك أو الفعل غير المشروع الذي قام به الجاني، ويطلق على هذا التغيير والذي يحدث في العالم الخارجي المدلول المادي للنتيجة الجرمية. أما المدلول القانوني للنتيجة الجرمية فهو الاعتداء على الحق الذي يحميه القانون، وهو يمثّل التكييف القانوني للنتيجة المادية التي خلّفها الفعل غير المشروع[٣١].

أما الجريمة المعلوماتية فهي كغيرها من الجرائم والتي يفترض وجود النتيجة الجرمية فيها كعنصر من عناصر الركن المادي للجريمة، وتختلف النتيجة الجرمية في الجريمة المعلوماتية حسب نوع الجريمة المرتكبة، حيث أنَّ الجرائم المعلوماتية تتنوع وتتعدَّد؛ لذلك فالنتيجة الجرمية تختلف باختلاف نوع الجريمة المعلوماتية المقترفة.

ففي جريمة تزوير المعلومات أو البيانات وهي من الجرائم المعلوماتية، فإن النتيجة الجرمية فيها تكون في تحريف الحقيقة في البيانات والمعلومات الموجودة في جهاز الحاسوب أو الموقع الإلكتروني، فالنتيجة هي الأثر المادي المترتّب على القيام بالفعل أو النشاط المادي غير المشروع، وهي أيضاً الأثر القانوني الذي يمثّل اعتداء على خصوصيات الناس ومعلوماتهم بتعديلها أو حذفها أو تحريفها بما يخالف القانون، وفي جريمة القتل والتي تتم بواسطة استخدام النظام المعلوماتي وأجهزة الحاسوب والإنترنت، فإنَّ النتيجة الجرمية تتلخَّص في إزهاق روح المجني عليه، كقيام طبيب في مستشفى بالدخول على قاعدة البيانات لدواء معين يُعطى لمريض من أجل التلاعب في هذا الدواء وكميته وقتل المريض بواسطة الدخول على قاعدة البيانات الخاصة بالمستشفى والتلاعب فيها[٣٢].

ويرى الباحث أنَّ الجريمة المعلوماتية هي كغيرها من الجرائم يفترض فيها وجود النتيجة الجرمية كأساس لقيام الركن المادي للجريمة، وبالتالي قيام الجريمة بشكل تام، فالنتيجة الجرمية هي عنصر أساسي لقيام الركن المادي للجريمة والذي يُعدُّ من أهم أركان الجريمة، والذي بدونه لا تقوم الجريمة، لكن الملاحظ أنَّ الجريمة المعلوماتية تتعدَّد وتتنوَّع أفعالها ونتائجها لكثرة أنواع الجرائم المعلوماتية، وبالتالي فإننا في هذا البحث نسلط الضوء فقط على الأركان العامة للجرائم المعلوماتية دون الحديث بالتفصيل عن الأركان الخاصة لكلّ جريمة معلوماتية، مع ملاحظة أنَّ النتيجة الجرمية لها مدلولان: مادي وقانوني، فالمدلول المادي هو: الأثر المادي الملموس، والذي

يترتَّب على قيام الجاني بالنشاط أو الفعل المادي غير المشروع أو امتناعه. أما المدلول القانوني للنتيجة الجرمية فهو: الاعتداء على حق يحميه القانون.

لكن السؤال الذي يجب طرحه هو: لو كانت النتيجة الجرمية المترتِّبة على القيام بالفعل أو الامتناع عنه ليست مادية، بل معنوية كسرقة المعلومات من النظام المعلوماتي أو جهاز الحاسوب أو الموقع الإلكتروني، وهنا هل المعلومات التي سُرقت مال مادي منقول أو معنوي؟ وهل عاقبت التشريعات الخاصة بالجرائم المعلوماتية على هذا النوع من الجرائم؟ وهل النتيجة الجرمية في جريمة سرقة المعلومات لها مدلول مادي أو معنوي؟

تُعدُّ جريمة سرقة المعلومات نوع من أنواع الجرائم المعلوماتية، لذا فإنَّ سرقة المعلومات وما يدور حول المعلومات في مدى اعتبارها شيئاً مادياً أم معنوياً، فإن الفقه اختلف حول ذلك وانقسم إلى عدّة اتجاهات، جانب من الفقه يرى بأنَّ المعلومات والتي تقع عليها السرقة لها مدلول مادي من حيث النتيجة، وقد وضع هذا الرأي باعتبار أنَّ المعلومات المنتقلة عبر الأسلاك وعلى شكل نبضات ورموز تمثِّل شيفرات يمكن حلّها إلى معلومات مُعيَّنة لها أصل ومولِّد صادر عنه وتمكين سرقتها والاستحواذ على البرامج والمعلومات، والتي لها كيان مادي كما وضّحنا سابقاً[٣٣].

ويرى اتجاه ثانٍ من الفقه أنَّه لا يمكن التسليم بفكرة الكيان المادي للمعلومات، بمعنى أنَّه لا يتصوَّر وجود مدلول مادي للنتيجة الجرمية في جريمة سرقة المعلومات، وهنا لا بُدَّ من وضع الأحكام والنصوص القانونية التي تتناسب وطبيعة الجريمة الخاصة[٣٤].

كما يرى اتجاه ثالث من الفقه أنَّ البيانات والمعلومات تخضع لسيطرة من يبتكرها ويستطيع الانتفاع بها، بحيث تصلح للخروج من حيازته والدخول في حيازة شخص آخر، وهي لها مقابل مادي ويتم التصرُّف بها بالبيع والشراء وبالتالي يمكن أنْ يطبَّق على سرقة المعلومات والبيانات الكيان المادي، وبالتالي وجود المدلول المادي للنتيجة الجرمية في هذا النوع من الجرائم[٣٥].

ويتفق الباحث مع الرأي الفقهي الثاني والذي اعتبر أنَّ المعلومات شيء معنوي وليس مادي، فالمعلومة قد تكون لها قيمة مالية، لكنها ليست ملموسة وليس لها كيان مادي، كما اعتبرها بعض اتجاهات الفقه السابقة، وبالتالي فإنَّ جريمة سرقة المعلومات كأحد أنواع الجرائم المعلوماتية تُعدُّ ذات النتيجة المعنوية وليست المادية، حيث أنَّ محل الجريمة "المعلومة" وهي كيان معنوي وليس مادي ملموس، كذلك لا يمكن قياس المعلومة وسرقتها على القوى المحرَّرة كسرقة الكهرباء.

أما عن المدلول القانوني للنتيجة الجرمية والذي يمثِّل الاعتداء على الحق الذي يحميه القانون في جريمة سرقة المعلومات، **فقد قام الباحث بالبحث** في نظام مكافحة الجرائم المعلوماتية السعودي رقم (م/١٧) تاريخ ١٤٢٨/٣/٨هـ، وقانون جرائم تقنية المعلومات البحريني رقم (٦٠)

لسنة ٢٠١٤م، وبالنتيجة فإن الباحث لم يجد نصٌّ يجرِّم بشكلٍ صريح سرقة المعلومات من النظام المعلوماتي أو المواقع الإلكترونية، وهذا نقص وخلل تشريعي أتمنى على المُشرِّع في هذه الدول تعديل النصوص؛ لتجريم فعل سرقة المعلومات لأهميتها في مكافحة الجرائم المعلوماتية، وحتى تكون المعلومة دقيقة وشمولية فقد تناول الباحث أيضاً دراسة نظام هيئة الاتصالات السعودي والصادر بالمرسوم المكاني رقم (م/١٢) تاريخ ١٤٢٢/٣/١٢هجري، وقانون الاتصالات البحريني رقم (٤٨) لسنة ٢٠٠٢م، وقد توصَّل الباحث إلى خلو هذه التشريعات أيضاً من تجريم فعل سرقة المعلومات. أما المُشرِّعين الأردني والإماراتي فقد نصَّ بشكلٍ غير مباشر على تجريم فعل سرقة المعلومات بالتأكيد صراحة على ذلك باستعمال مصطلح "نسخ"، وهذا واضح من نصِّ المادة (١٢/د) من قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥م، حيث نصَّت المادة على الآتي: "إذا كان الدخول المُشار إليه في الفقرة (٢٠) من هذه المادة لإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها... الخ".

أما قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢م، فقد نصَّ في المادة (٢/٢) على الآتي: "تكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة لا تقل عن مائة وخمسين ألف درهم ولا تتجاوز سبعمائة وخمسون ألف درهم أو بإحدى هاتين العقوبتين إذا ترتَّب على أي فعل من الأفعال المنصوص عليها بالفقرة (١) من هذه المادة إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ... الخ".

مع الإشارة إلى أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات استخدمت نفس المصطلح الذي استخدمته التشريعات المذكورة سابقاً للتعبير عن سرقة المعلومات "بالنسخ"، حيث نصَّت المادة (٢/٦) من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والصادرة بتاريخ ٢٠١٤/٢/٧م على الآتي: "تشدَّد العقوبة إذا ترتَّب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال :

أ- محو أو تعديل أو تشوية أو نسخ أو نقل للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية الخ.....".

لذلك فإن التشريع وحده لا يكفي لمكافحة الجرائم المعلوماتية ما لم يكن هنالك وسائل أخرى تُعنى بالدفاع عن الشبكات المعلوماتية قبل سرقتها أو اختراقها وتسمى هذه الوسائل "أمن النظم أو المعلومات" (SYSTEMS SECURIT)، وهي عبارة عن الحماية لكلّ موارد معلومات المنشأة من السرقة من قبل الأطراف غير المخوَّل لهم استخدام النظام[٣٦].

ويستنتج الباحث ضرورة أنْ تستحدث الدول وحدة حكومية تُعنى بأمن المعلومات وسريتها والحفاظ عليها من العبث أو السرقة أو الاختراق من أي جهة كانت.

ويرى الباحث أيضاً أنَّ كلمة أو مصطلح "نسخ" الواردة في النصوص المذكورة أعلاه تعني وبصفة غير مباشرة أخذ مال الغير دون رضاه، وهو المفهوم القانوني والفقهي للسرقة. وفي هذا الإطار فقد يكون للمعلومات والتي تم نسخها قيمة مالية، ولو أنَّها ليس لها كيان مادي، فالمعلومات هي شيء معنوي غير ملموس، وبالتالي فإنَّ جريمة سرقة المعلومات كنوع من أنواع الجرائم المعلوماتية تفتقر إلى النتيجة الجرمية بمدلولها القانوني والمادي، فمن حيث المدلول القانوني للنتيجة الجرمية والذي يمثِّل الاعتداء على الحق الذي يحميه القانون، ويُلاحظ أن هنالك نقص تشريعي بتجريم فعل سرقة المعلومات في كلٍّ من المملكة العربية السعودية والبحرين، من حيث خلو النص الصريح والواضح في التشريعات الخاصة بالجرائم المعلوماتية في كلٍّ من الأردن والإمارات وحتى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بالنصِّ على مصطلح "كل من سرق المعلومات"، وهذا أيضاً خلل بالتشريع يَستدعي تعديل هذه التشريعات لمكافحة هذا النوع من الجرائم المعلوماتية.

ويرى الباحث أنَّ بعض التشريعات في الدول الأوروبية ومنها: فرنسا، وكندا، استجابوا لهذه النقطة بتعديل التشريعات الجزائية لتشمل سرقة المعلومات، فمثلاً نصَّ المُشرِّع الكندي في المادة (٣٢١) من قانون العقوبات الكندي لسنة ١٩٨٥ وتعديلاته على تعريف المحرّرات في جريمة التزوير لتشمل أي شيء مادي يمكن أنْ يتم عليه تسجيل قراءتها أو فهمها، بواسطة أي شخص، أو بواسطة أنظمة الحواسيب، أو بواسطة أي جهاز آخر.

كما حَسَمَ المُشرِّع الفرنسي الجدل في هذه المسألة عندما تناول هذا الموضوع في قانون العقوبات الفرنسي لسنة ١٩٩٤م في المادة (١/٤٤١) والتي توسَّعت في مفهوم المحرّر الذي يقع عليه التزوير ليشمل التزوير الذي يقع على سرقة المعلومات، مثال: الأقراص الممغنطة، والأسطوانات المدمجة، وغيرها من وسائل تخزين المعلومات[٣٧].

ثالثاً: علاقة السببية:

تُعدُّ علاقة السببية عنصر مهم من عناصر الركن المعنوي للجريمة، فهي حلقة وصل بين السلوك الجرمي والنتيجة الجرمية، وذلك بأنْ يُثبت أنَّ هذا السلوك هو سبب تلك النتيجة الجرمية، كذلك فإنَّ علاقة السببية تساهم في تحديد نطاق المسؤولية الجزائية واستبعاد المسؤولية إذا لم ترتبط النتيجة الجرمية بالفعل[٣٨].

أما في نطاق الجرائم المعلوماتية فإنَّ علاقة السببية أساسية لقيام جميع أنواع الجرائم المعلوماتية، فهي عنصر أساسي من عناصر الركن المادي لأي جريمة معلوماتية، وتقوم العلاقة السببية في الجرائم المعلوماتية على البحث في الصلة بين مُرتكب الجريمة والفعل الذي ارتكبه

وبين الآلة، فالعلاقة التقنيَّة بين مُرتكب الجريمة وبين الآلة محل الجريمة المعلوماتية هي الأساس لبيان رابطة السببية في الجرائم المعلوماتية[٣٩].

وبالنتيجة فإنَّ رابطة السببية في الجرائم المعلوماتية أساسية؛ لتحديد نطاق المسؤولية الجزائية في كل الجرائم المعلوماتية العمدية، ويقع عبء إثبات وجود رابط السببية من عدمها على النيابة العامة بما يُقدَّم إليها من أدّلة وبيِّنات واستماع للشهود في مثل هذا النوع من الجرائم المستحدثة، والتي تحتاج للشهود وبعض البيِّنات الخاصة، وهذا يتطلَّب من الدول بذل الجهود لمكافحتها بإيجاد كوادر قضائية ورجال أمن وجهات تحقيق على درجة عالية من الكفاءة والخبرة الدقيقة من أجل فهم ومعرفة التعامل مع هذا النوع من الجرائم[٤٠].

المطلب الثاني:
الركن المعنوي للجريمة المعلوماتية

يُعدُّ الركن المعنوي للجريمة عنصر أساسي لقيام المسؤولية الجزائية، وبدونه لا تقوم الجريمة؛ إذ لا يسأل شخص عن جريمة ما لم تقم علاقة بين مادياتها ونفسية الجاني وسيطرة الإرادة الجرمية للجاني على ماديات الجريمة، وبالتالي تتحدَّد صورة القصد الجرمي للجريمة مقصودة، أم تأخذ صورة الخطأ الذي تكون به الجريمة غير المقصودة[٤١].

فالركن المعنوي للجريمة هو الوجه الباطني النفسي للسلوك الذي قام به الجاني، والنصُّ القانوني هو الذي يحدِّد الوجه الباطني النفسي ونوعه، لكن في بعض الأحيان يتعدى السلوك الإجرامي نفسية صاحبه أو مُرتكب الجريمة؛ لأسباب خارجة عن إرادته ضغطت عليه ودفعته لارتكاب الجريمة، كأنْ يُكره شخص على التوقيع بإمضاء في سند مرور، وفي هذه الحالة فإنَّ الجاني لا يُسأل جزائياً عن السلوك الذي قام به؛ لذلك فإنَّ الركن المعنوي للجريمة يفترض وجود معيارين: المعيار **الأول:** وجود العلاقة النفسية، والمعيار الثاني: هو تقييم القانون لهذه العلاقة وحكمه عليها[٤٢].

وتؤكِّد محكمة التمييز الأردنية وفي العديد من قراراتها على **أنَّ الإرادة** عنصر أساسي من عناصر الركن المعنوي للجريمة، وللمحكمة استظهارها بالاستنتاج والأدلة وكيفية ارتكاب الفعل الجرمي والوسائل المستعملة ومواقع الإصابة وجسامتها[٤٣].

فالقصد الجنائي هو إرادة اتَّجهت على نحوٍ معين وسيطرت على ماديات الجريمة، وهي تعبير عن خطورة الجاني ونتيجة مؤكِّدة على الإدانة له أمام المحكمة متى تبيَّن للمحكمة صدق هذه الإرادة [٤٤].

أما الركن المعنوي للجرائم المعلوماتية فيُعدُّ كغيرهِ من أهم الأركان وبدونه لا تتحقَّق المسؤولية الجزائية للجرائم المعلوماتية؛ لذلك سنبحث في هذا المطلب القصد العام والقصد الخاص للجرائم المعلوماتية، وهل كل الجرائم المعلوماتية يتطلَّب فيها وجود قصد خاص أم لا؟

تُعدُّ الجرائم المعلوماتية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم، والإرادة) لتحديد المسؤولية الجنائية، ولا يمكن تصوُّر وجود قصد خاص بالجريمة دون أنْ يسبقه القصد العام، أما عن وجود القصد الخاص في الجرائم المعلوماتية، فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنيَّة الخاصَّة لدى الجاني من وراء القيام بالفعل غير المشروع أو ارتكاب الجريمة، فكلّ جريمة معلوماتية تختلف عن الأخرى من حيث أركانها وماهيتها، وطبيعتها.

ويرى اتجاه من الفقه أنَّ القضاء الأمريكي لم يستقرّ على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الإنترنت، من حيث مدى تحديد ما إذا كانت تتطلَّب قصداً عاماً أو خاصاً[٤٥].

ويلاحظ الباحث أنَّ القصد الخاص يتوافر في بعض الجرائم المعلوماتية، سيما وأنَّ معظم الجرائم المعلوماتية تقوم بتوافر القصد العام وهو علم الجاني بمضمون الفعل الذي قام أو سيقوم به بأنَّ هذا الفعل غير مشروع، وكذلك ارتباط هذا العلم بالإرادة وهي حالة نفسية مرتبطة بماديات الجريمة، فمثلاً في جريمة سرقة المعلومات وهي من الجرائم المعلوماتية يجب أنْ ينصبُّ علم الجاني على أنَّ فعل سرقة المعلومات من الحاسب الآلي أو البريد الإلكتروني يُعدُّ فعل غير مشروع، ويجب أنْ يرتبط هذا العلم مع الإرادة وهي الحالة النفسية التي تعكس قيام الجاني بالسلوك، ويترافق مع القصد العام الذي ذكرناه سابقاً في جريمة سرقة المعلومات (نيّة التملُّك) للمعلومة التي تمّ سرقتها والتي تعكس (القصد الخاص) في مثل هذا النوع من الجرائم.

وتطبيقاً لذلك قضت محكمة النقض الفرنسية بتوافر نيّة التملُّك الوقتية في سرقة المنفعة للمعلومات من جهاز الحاسوب، وتتحقَّق هذه النيَّة منذُ سلب وحيازة المستندات خلال الوقت اللازم لإعادة نسخها بدون إرادة صاحب المشروع مالكها أو حائزها منها بصفة دائمة أو مؤقتة، وإنما مشاركة الانتفاع بها، وهو الأمر الذي يتطلَّب تدخُّل تشريعي لمواجهتها بنصوص خاصة مثل تجريم المُشرِّع الهولندي[٤٦].

ويرى اتجاه من الفقه أنَّ نيّة التملُّك في جريمة سرقة المعلومات تبدأ بقيام الجاني بالدخول على أدوات الحاسب الآلي من وحدات الإدخال والإخراج والتخزين والمعالجة أو البرامج

والبيانات والمعلومات والنظم المخزنة داخل ملفات الحاسب الآلي أو في ذاكرته، كل هذا من أجل الاستيلاء على المعلومات الموجودة بقصد نيّة التملُّك والإضرار بالمجني عليه[٤٧].

لكن بعض الجرائم المعلوماتية وبحكم طبيعتها لا يشترط لقيامها وقيام الركن المعنوي فيها وجود قصد خاص، ففي جريمة التعدّي على برامج الحاسب الآلي، نجد بأنّها من الجرائم العمدية التي لا تقوم إلا بتوافر القصد الجنائي العام لدى الجاني بعنصريه العلم والإرادة، فالجاني يفترض أنْ يكون عالماً بأنّ النشاط الذي قام به هو نشاط غير مشروع يحمل في طياته اعتداء على برامج حاسوبية مملوكة للغير، ويجب أنْ يرافق ذلك العلم اتجاه الإرادة إلى مباشرة النشاط الإجرامي المتمثّل في فعل التعدّي بالمخالفة للقانون[٤٨].

وفي بعض الجرائم المعلوماتية كجريمة الدخول غير المشروع لمواقع التجارة الإلكترونية عبّرت بعض النصوص القانونية والتي تناولت هذه الجريمة بالعقاب عن ضرورة توفُّر القصد العام المتطلب في هذه الجريمة أو لقيام الركن المعنوي لها، ومنها قانون العقوبات الفرنسي والذي أكّد على ضرورة توفُّر القصد العام في هذا النوع من الجرائم، وكذلك المُشرِّع الدنماركي والبرتغالي والسويسري، كلُّ هذه النصوص عاقبت الفاعل الذي يدخل بطريقة غير مصرَّح له بالدخول إلى النظام على نحوٍ مخالف للقانون، ويتطلَّب القصد العام في هذه الجريمة ضرورة علم الجاني بأنَّ فعله بالدخول إلى المواقع غير المصرَّح له الدخول إليها مخالف وغير مشروع، ويشترط توقُّع الجاني حين يقوم بالفعل النتيجة الإجرامية، ويجب أنْ يتفق مع العلم إرادة الجاني والتي تدفعه للقيام بفعل الدخول إلى المواقع غير المصرَّح له الدخول إليها قانوناً، أما القصد الخاص في هذه الجريمة فإنّه يتلخَّص بنيّة الإضرار والتي تتوافر لدى الجاني عند دخوله إلى المواقع أو نظام الحاسب الآلي غير المرخَّص له الدخول إليها بقصد الإضرار بالغير، ففي النرويج مثلاً شدَّد المُشرِّع النرويجي في قانون العقوبات على هذا النوع من الجرائم متى ارتكب الفاعل فعل الدخول غير المصرَّح به بنيّة حصول الفاعل له أو للغير على ربح غير مشروع أو كان إلحاق ضرر بالغير نتيجة الاطلاع على معلومات يحتوي عليها النظام[٤٩].

ويرى الباحث أنَّ القصد العام والخاص في جرائم المعلوماتية هو أساسي لتحديد المسؤولية الجزائية، والذي يحدِّد وجود قصد خاص في بعض الجرائم المعلوماتية هو طبيعة الجريمة ونيّة الإضرار أو النيّة الخاصة للجاني والتي يمكن استشفافها من مكوّنات كل جريمة على حدا وبشكلٍ مستقل، وبالتالي فإنَّ الجرائم المعلوماتية وكجرائم مستحدثة هي كغيرها من الجرائم التقليدية يشترط وجود الركن المعنوي لقيام الجريمة ولا يتصوَّر قيام أي نوع من أنواع الجرائم المعلوماتية دون وجود الركن المعنوي.

أما عن الإثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة المختصَّة بالنظر في مثل هذا النوع من القضايا، والمحكمة صاحبة

الصلاحية بتقدير وجود سوء النيَّة من عدمها ووزن البينات وتمحيصها بما لها من صلاحية باعتبارها صاحبة القرار النهائي بالفصل في الدعاوى المرفوعة أمامها.

المطلب الثالث:
آلية مكافحة الجرائم المعلوماتية

تُعدُّ الجرائم المعلوماتية من الجرائم المستحدثة في العصر الحالي والتي تحتاج إلى تظافر جهود الدول سواءً على المستوى الداخلي أو الخارجي من أجل وضع الحلول لمعالجة ومكافحة هذا النوع من الجرائم، والتي تمتاز بأنَّها جرائم عابرة للحدود، لذا يقتضي ذلك من الدول التعاون على المستوى الإجرائي الجنائي من حيث السماح بالاتصال المباشر بين أجهزة الشرطة بين الدول المختلفة، وذلك بإنشاء مكاتب متخصِّصة لجمع المعلومات عن مرتكبي الجرائم المتعلِّقة بالإنترنت وتعميمها(٥٠).

لذلك فإن هذا المطلب سيتناول بالدراسة محورين هما:

أولاً: آلية مكافحة الجرائم المعلوماتية على المستوى الوطني.

ثانياً: آلية مكافحة الجرائم المعلوماتية على المستوى الدولي.

أولاً: آلية مكافحة الجرائم المعلوماتية على المستوى الوطني:

تؤثِّر الجرائم المعلوماتية على الدول إذا ما تم مكافحتها؛ لذلك فإن استفحال وانتشار هذا النوع من الجرائم دون ضوابط وإجراءات تحدُّ من انتشارها سيؤثِّر على الدول في ظلِّ توسُّع مستخدمي شبكة الإنترنت وأجهزة الحاسوب والوسائل التكنولوجية.

وفي الإطار العربي ولخطورة الجريمة، فقد سارعت بعض الدول العربية لوضع تشريعات خاصة بمكافحة الجريمة المعلوماتية منها على سبيل المثال المملكة العربية السعودية، والتي أصدرت نظام مكافحة الجرائم المعلوماتية والصادر بالمرسوم الملكي رقم (م/١٧) تاريخ ١٤٢٨/٣/١٨هـ، وكذلك قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥م، وقانون جرائم تقنية المعلومات البحريني رقم (٦٠) لسنة ٢٠١٤م، وقانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٥م وغيرها من القوانين في الإطار العربي، وهذا يدلُّل على خطورة الجريمة بإيجاد تشريعات خاصة لمكافحتها.

أما على المستوى الأمني فقد تنبَّهت هذه الدول أيضاً إلى إيجاد أجهزة أمنية إدارية متخصِّصة للكشف عن الجرائم المعلوماتية، والقيام بدور التوعية الاجتماعية عن مخاطر هذا النوع من الجرائم، ففي الأردن تمَّ إنشاء قسم الجرائم المعلوماتية عام ٢٠٠٨م، ويتبع هذا القسم إلى مديرية الأمن العام الأردني، ثم تطوَّر هذا القسم ليصبح وحدة الجرائم الإلكترونية عام ٢٠١٥م، وفي البحرين تمَّ إنشاء إدارة الجرائم الإلكترونية والتي تختصُّ بمتابعة كل القضايا والجرائم المتعلقة بالمعلوماتية والإنترنت، أما في المملكة العربية السعودية فإنني لم أجد أي جهاز متخصِّص لمكافحة الجرائم المعلوماتية، إنما يتم الإبلاغ عن هذه الجرائم إلى هيئة الاتصالات السعودية أو المراكز الأمنية التابعة لوزارة الداخلية السعودية ليصار إلى اتخاذ الإجراءات القانونية بحق المخالفين، أما في الإمارات العربية المتحدة فلم نجد أيضاً جهاز متخصِّص لمكافحة هذا النوع من الجرائم، وهذا خلل يحتاج من هذه الدول إلى السرعة في إنشاء أجهزة أمنية متخصِّصة لملاحقة ومكافحة هذا النوع من الجرائم.

ويُعدُّ الاهتمام بعنصر التدريب للأجهزة الأمنية التي تضبط وتلاحق هذا النوع من الجرائم من المرتكزات الأساسية، والمقصود بالتدريب في هذه النقطة ليس التدريب التقليدي، بل التدريب الذي يركِّز على إكساب المشاركين خبرة فنية في مجال الجريمة المعلوماتية، وهذه الخبرة الفنية لا تأتي دون تدريب تخصّصي يُراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب، ويذهب بعض الفقهاء إلى ضرورة أنْ يكون لدى المتدرب خبرة لا تقل عن خمس سنوات في المجالات ذات العلاقة بتكنولوجيا المعلومات كإدارة الشبكات والبرمجة وتصميم النظم...الخ[٥١].

وبالنتيجة فإن التدريب أصبح يلعب دوراً هاماً في حياة الإنسان في عصرنا الحالي، حيث زاد الاهتمام بالتدريب بمختلف جوانبه الفنية والتكتيكية، وقد أضحى ضرورة للفرد المتدرِّب وللمنظمة التي ينتسب إليها في آن واحد، سواء أكانت منظمة مدنيَّة أو عسكريَّة أو حكوميَّة أو خاصَّة [٥٢].

ويرى الباحث أنَّ جهود الدول على المستوى الوطني في مجال مكافحة الجرائم المعلوماتية ما زالت دون المستوى المطلوب، سواء من حيث إيجاد محاكم متخصِّصة أو دوائر تحقيق تكون مساندة للقضاء ومتخصِّصة للنظر في هذا النوع من الجرائم، أو من حيث الاهتمام بالجانب التدريبي لكوادر الأمن العام أو القضاة، سيما وأنَّ الجرائم المعلوماتية تُعدُّ من الجرائم التي تحتاج إلى معرفة فنيَّة دقيقة من أجل التعامل مع مرتكبيها، كما أنَّ الجانب التشريعي في مكافحة الجرائم المعلوماتية يعتريه النقص في العديد من المحاور وخاصَّةً فيما يتعلَّق بالإجراءات الجزائيَّة للتعامل مع هذا النوع من الجرائم.

وفي مجال التوعية الاجتماعية من مخاطر الجرائم المعلوماتية، فإنه يقع على عاتق الدول بذل الجهود في تثقيف المواطنين من خطورة هذه الجرائم خصوصاً فئة الشباب وصغار السن فهم من أكثر الفئات في المجتمع ارتكاباً لهذه الجرائم؛ ويعود السبب في ذلك إلى انتشار مشكلتي الفقر والبطالة، كما توفّر هذه الجرائم للشباب الظهور الإعلامي مما يدفعهم كحافز لارتكابها(٥٣).

ويرى الباحث ضرورة قيام الدول وعلى المستوى الوطني ومن خلال الأجهزة الأمنية المختصّة بمكافحة هذه الجرائم بعقد اللقاءات على مستوى المدارس والجامعات، وحثّ دور العبادة والمؤسّسات الدينية من أجل توعية المجتمع بمخاطر هذه الجرائم وأثرها على المجتمع، سيما في ظلّ انتشار هذه الجرائم، كما أنّه لا بُدَّ من عقد الورشات والمؤتمرات الوطنية في مجال مكافحة الجرائم المعلوماتية بهدف تبادل الخبرات والخروج بالتوصيات التي تساهم في حلّ المشكلات الناتجة عن هذه الجرائم.

ثانياً: آلية مكافحة الجرائم المعلوماتية على المستوى الدولي :

تحدثنا سابقاً عن آلية مكافحة الجرائم المعلوماتية على المستوى الوطني، وفي هذا الإطار فإنّه لا بُدَّ من النظر بشكلٍ شمولي لمكافحة هذا النوع من الجرائم، فلا يكفي أنْ نضع حلول لضبط هذه الجرائم على المستوى الوطني، بل لا بُدَّ من إيجاد إطار شمولي يضمن عدم تكرار هذه الجرائم على المستوى الدولي.

أما عن الجهود الدولية في مكافحة الجرائم المعلوماتية، فهي ما زالت دون المستوى المطلوب رغم بعض الجهود التي لا ترقى إلى مستوى التعاون المطلوب، فعلى صعيد التعاون الأمني بين الدول في مجال جرائم المعلوماتية نجد دور الإنتربول الشرطة الدولية (**Organization Interpol International Criminal Police**) في الجرائم المتعلّقة بالإنترنت، فعندما تم توقيف أحد الطلبة في الجمهورية اللبنانية من قبل القضاء اللبناني بتهمة إرسال صورة إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الإنترنت، كان هذا بفضل تلقي النيابة العامة اللبنانية بلاغ أو برقية من الإنتربول (الشرطة الدولية) في ألمانيا حول الواقعة أو القضية والتي يحقّق فيها القضاء اللبناني، وبالنتيجة فإنّ هذه المنظمة تهدف إلى تأكيد التعاون الأمني بين الدول الأطراف في المنظمة وعلى نحوٍ فعّال في مكافحة الجرائم المعلوماتية، من حيث تجميع البيانات والمعلومات المتعلّقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الموجودة في الدول الأطراف في هذه المنظمة (٥٤).

ويرى الباحث أنَّ جهود الشرطة الدولية في هذا المجال ما زالت دون المستوى المطلوب، من حيث أنَّه يتوجَّب عليها حَثّ الدول الأطراف في منظمة الشرطة الدولية التعاون معها في مجال مكافحة جرائم المعلوماتية عن طريق عقد الاتفاقيات الثنائية بما يبرهن التعاون الدولي بين الدول في مجال الجرائم المعلوماتية والمنظمة، ويقترح الباحث إنشاء قسم متخصِّص في الإنتربول (الشرطة الدولية) مهمته متابعة الجرائم والكشف عنها وملاحقة المجرمين وتبليغ الدول ذات العلاقة بالجرائم المعلوماتية بوقوع الجرائم على أراضيها، والتنسيق مع أقسام الجرائم المعلوماتية في الدول من أجل تبادل الخبرات والمعلومات في مثل هذا النوع من الجرائم المستحدثة، أما على المستوى العربي فيقترح الباحث وفي المجال الأمني إنشاء قسم متخصِّص تابع للمكتب العربي للشرطة الجنائية والذي تم إنشاؤه بقرار من مجلس وزراء الداخلية العرب، بحيث يهتم هذا القسم بمتابعة كل ما يتعلق بالجرائم المعلوماتية بالإطار العربي.

أما في مجال التعاون الدولي لمكافحة الجرائم المعلوماتية على وجه العموم، فإنَّه ما **زال** دون المستوى المطلوب لعدم وجود اتفاقية دولية صادرة عن الأمم المتحدة في مكافحة هذا النوع من الجرائم. **أما على المستوى الإقليمي** فهنالك العديد من الاتفاقيات منها مثلاً اتفاقية بودابست لمكافحة الجرائم المعلوماتية والتي صدرت بتاريخ **٢٠٠١/١١/٢٣م**، وهذه الاتفاقية خاصَّة فقط لدول الاتحاد الأوروبي، وفي الإطار العربي صدر عن جامعة الدول العربية اتفاقية حديثة تُعنى بمكافحة الجرائم المعلوماتية سميت "الاتفاقية العربية لمكافحة جرائم المعلومات" حيث وافق على الاتفاقية مجلس وزراء الداخلية العرب بتاريخ ٢٠١٠/١٢/٢١م ودخلت الاتفاقية حيِّز التنفيذ بتاريخ ٢٠١٠/٢/٧م بعد مصادقة الدول الأطراف عليها وتُعدُّ هذه الاتفاقية نقطة تحوُّل في التعاون العربي لمكافحة هذه الجرائم، حيث نصَّت الاتفاقية على التعاون العربي في مكافحة الجرائم المعلوماتية في العديد من المجالات منها (التعاون القضائي، تبادل المعلومات، تبادل الخبرات، الاختصاص القضائي، تسليم المجرمين، المساعدة القضائية) وغيرها من الموضوعات ذات الصلة[٥٥] .

ويرى الباحث ضرورة إنشاء مركز دولي مقرَّه الأمم المتحدة يسمى "المركز الدولي لمكافحة جرائم المعلوماتية"، تساهم به الدول الأعضاء ويكون الهدف منه تنسيق الجهود في مجال مكافحة الجرائم المعلوماتية، وعقد المؤتمرات الدولية ذات العلاقة بالجرائم المعلوماتية وإعداد الاتفاقيات الدولية أيضاً ذات الصلة بالموضوع.

وفي مجال التعاون الدولي من الناحية القضائية في الجرائم المعلوماتية ومكافحتها، نجد بأنَّه لا يرقى أيضاً إلى المستوى المطلوب؛ والسبب في ذلك يعود إلى عدم وجود الاتفاقيات الدولية المنظمة لهذا النوع من الجرائم، رغم وجود بعض الاتفاقيات الدولية في المجال القضائي والتي تساعد في بعض الأحيان في مكافحة الجرائم المعلوماتية. أما في الإطار العربي هنالك

اتفاقية الرياض للتعاون القضائي والصادرة في ١٩٩٣/٤/٦م، وقد وقِّعت الاتفاقية في مدينة الرياض، وتُعدُّ هذه الاتفاقية النواة الأولى للتعاون العربي في المجال القضائي، كذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والصادرة من الأمم المتحدة سنة ٢٠٠٠م، كذلك هنالك الاتفاقية القضائية والقانونية الصادرة عن مجلس التعاون الخليجي في الفترة من ٢١-٢٠٠٣/١٢/٢٢م في الكويت حيث تمَّ اعتماد هذه الاتفاقية من المجلس الأعلى لمجلس التعاون الخليجي في دورته الرابعة.

وبالنتيجة فإنَّ الجهد الدولي يبقى ناقصاً في ظلِّ عدم وجود **اتفاقية دولية** متخصِّصة وتُعنى بـ "الجرائم المعلوماتية"، بحيث تناقش هذه الاتفاقية آلية مكافحة الجرائم المعلوماتية وملاحقة المجرمين، والقبض عليهم، وتبادل المعلومات بين الدول، والاختصاص القضائي، والتحقيق مع المتهمين ومحاكمتهم، وتسليم المجرمين، فالمطلوب أنْ ترى هذه الاتفاقية ذات العلاقة بالجرائم المعلوماتية الضوء سيما وأنَّ هذا النوع من الجرائم يمتاز بالخطورة؛ كونها جرائم عابرة للحدود ويصعب إثباتها ويسهل ارتكابها، وهنالك مشكلة أيضاً في صعوبة تحديد الاختصاص القضائي في مثل هذا النوع من الجرائم.

الخاتمة

ناقشت هذه الدراسة موضوع يُعدُّ من أهم المواضيع القانونية في العصر الحالي والموسوم بـ (الجريمة المعلوماتية "أركانها وآلية مكافحتها – دراسة تحليلية مقارنة")، وقد تناولت الدراسة الجرائم المعلوماتية كجرائم مستحدثة من حيث تعريفها وبيان خصائصها وصفات المجرم المعلوماتي، كما تمَّ الإشارة إلى التشريعات العربية الخاصَّة بالجرائم المعلوماتية في كل من: (الأردن، البحرين، الإمارات، المملكة العربية السعودية)، وقد تمَّ دراسة هذه التشريعات بالتحليل والمقارنة من خلال التركيز على السلبيات والإيجابيات في التشريعات لإثراء الدراسة، وقد انتهت الدراسة بخاتمة توصَّلت إلى مجموعة من النتائج والتوصيات نجملها بالآتي:

أولاً: النتائج:

١. تُعدُّ الجرائم المعلوماتية من الجرائم المستحدثة في العصر الحالي.

٢. تمتاز الجرائم المعلوماتية بأنَّها جرائم عابرة للحدود ويصعب إثباتها، وتحديد الاختصاص القضائي لها.

٣. المجرم المعلوماتي يمتاز بالذكاء والسرعة في ارتكاب الجريمة والتخصُّص والدقة في مسائل تكنولوجيا المعلومات.

٤. الجرائم المعلوماتية هي كغيرها من الجرائم التقليدية، لا تقوم إلا بتوافر الأركان العامة لأي جريمة (الركن المادي، الركن المعنوي).

٥. أغلب الجرائم المعلوماتية تحتاج لتوافر القصد العام والبعض منها يتطلَّب توافر القصد الخاص والذي يُعدُّ عنصراً من عناصر الركن المعنوي للجريمة.

٦. سارعت الدول إلى إيجاد تشريعات خاصة لمكافحة هذا النوع من الجرائم المستحدثة لخطورتها في العصر الحالي.

٧. الجهود الدولية في مجال مكافحة الجرائم المعلوماتية دون المستوى المطلوب من حيث عدم وجود اتفاقية دولية صادرة عن منظمة الأمم المتحدة في مجال مكافحة الجرائم المعلوماتية.

٨. الجهود الوطنية ما زالت دون المستوى المطلوب في تثقيف المجتمع وبيان مخاطر الجرائم المعلوماتية.

٩. صدور الاتفاقية العربية لمكافحة الجرائم المعلوماتية من جامعة الدول العربية، حيث تمّت المصادقة عليها بقرار مجلس وزراء الداخلية العرب بتاريخ ٢٠١٠/١٢/٢١م ودخلت حيّز التنفيذ بتاريخ ٢٠١٤/٢/٧م يُعدُّ نقطة تحوُّل في التعاون العربي لمكافحة هذه الجرائم.

ثانياً: التوصيات:

١. التوصية بتعديل المواد الأولى من قانون الجرائم الإلكتروني الأردني رقم (٢٧) لسنة ٢٠١٥م، وقانون مكافحة جرائم تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٥م، وقانون مكافحة جرائم المعلومات البحريني رقم (٦٠) لسنة ٢٠١٤م من أجل وضع تعريف منهجي وعلمي للجريمة المعلوماتية أسوةً بالمُشرّع السعودي.

٢. التوصية بتعديل نظام مكافحة الجرائم المعلوماتية السعودي وقانون مكافحة الجرائم المعلوماتية الإماراتي بإضافة نصّ يعاقب المجرم المعلوماتي على تكرار الجريمة المعلوماتية أسوةً بالمُشرّع الأردني والبحريني.

٣. التوصية بتعديل التشريعات الخاصة في الجرائم المعلوماتية في كل من: (الأردن، البحرين، السعودية، الإمارات) لإضافة نصّ يجرّم جريمة سرقة المعلومات من المواقع الإلكترونية أو أجهزة الحاسوب أو البريد الإلكتروني أسوة بما فعل المُشرّع الكندي والفرنسي.

٤. التوصية بإنشاء مركز دولي لمكافحة الجرائم المعلوماتية يسمى "المركز الدولي لمكافحة الجرائم المعلوماتية" ويكون مقرّه الأمم المتحد من أجل تنسيق الجهود بين الدول، وإبرام الاتفاقيات الدولية ذات الصلة، وعقد المؤتمرات الدولية لتبادل الخبرات ووضع آليات واضحة تُجمِع عليها الدول من أجل مكافحة الجرائم المعلوماتية، كذلك يتولّى هذا المركز وبالتنسيق مع الدول صياغة تعريف جامع مانع للجرائم المعلوماتية تتفق عليه الدول.

٥. التوصية بإنشاء مركز متخصّص لمكافحة الجرائم المعلوماتية تابع لمكتب الشرطة الجنائية العربية، والذي أنشئ بقرار من مجلس وزراء الداخلية العرب؛ وذلك لتنسيق الجهود في مكافحة الجرائم المعلوماتية في الإطار العربي.

٦. التوصية بالإشارة إلى خطورة الجرائم المعلوماتية في المناهج التعليمية سواء على مستوى الجامعات أو المدارس من أجل بيان مخاطرها وزيادة الوعي الاجتماعي في مثل هذا النوع من الجرائم.

٧. التوصية بإنشاء قسم متخصّص على المستوى الدولي لمكافحة الجرائم المعلوماتية تابع لمنظمة الشرطة الدولية "الإنتربول" من أجل تنسيق الجهود بين الدول، وتبادل الخبرات.

٨. التوصية بإنشاء محاكم متخصّصة للنظر في قضايا الجرائم المعلوماتية، أو إيجاد هيئات قضائية متخصّصة تضم في عضويتها قضاة على درجة عالية من التأهيل الفني والتقني في مجال جرائم تكنولوجيا المعلومات؛ لأهمية هذا النوع من الجرائم على المستوى الوطني للدول.

٩. التوصية بتعديل قوانين مكافحة الجرائم المعلوماتية بإيجاد نصوص تحمي المُبلِّغ عن هذه الجرائم من حيث سرية التبليغ والنصُّ في التشريع على مَنح أي شخص يُخبر عن هذه الجرائم باستحقاقه مكافأة مالية يحدِّد قيمتها المرجع المختص نظراً لخطورتها.

١٠. التوصية باستحداث دوائر تحقيق خاصة بالجرائم المعلوماتية على المستوى الوطني تكون مساندة للقضاء في اتخاذ الإجراءات القانونية لمكافحة هذا النوع من الجرائم.

قائمة حواشي البحث

١- انظر المادة (١) من نظام مكافحة الجرائم المعلوماتية السعودي رقم (م/١٧) تاريخ ١٤٢٨/٣/٨هـ.

٢- انظر المادة (٢) من قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥م.

٣- د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة، القاهرة، دار النهضة العربية، سنة ٢٠٠٩م، (ط٢)، ص٢٠.

٤- د. هلالى عبد اللاه أحمد، المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست، المجلد السادس، العدد الثالث عشر، مجلة الحقوق، جامعة البحرين سنة ٢٠٠٩م، ص٤٦٢.

٥- د. نائلة عادل محمد فريد، **الجرائم المعلوماتية على شبكة الإنترنت**، لبنان، منشورات الحلبي الحقوقية، سنة ٢٠٠٥م، (بدون طبعة)، ص٢٨ وما بعدها.

٦- د. يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، مصر، المركز القومي للإصدارات القانونية، سنة ٢٠١١م، (ط١)، ص١٣.

٧- أمير فرج يوسف، **الجرائم المعلوماتية على شبكة الانترنت**، الإسكندرية، دار المطبوعات الجامعية، سنة ٢٠١٠م، (بدون طبعة)، ص ١٠٤ وما بعدها.

٨- د. عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي**، مصر، دار الكتب العربية، سنة ٢٠٠٧م، (ط١)، ص٢٤.

٩- د. سامي علي حامد عياد، **الجرائم المعلوماتية وإجرام الإنترنت**، مصر، دار الفكر العربي سنة ٢٠٠٧م، (بدون طبعة)، ص٢٧.

١٠- أمير فرج يوسف، مرجع سابق، ص١٠٤ وما بعدها.

١١- انظر المادة (١) من نظام مكافحة الجرائم المعلوماتية السعودي رقم (م/١٧) تاريخ ١٤٢٨/٣/٨هـ.

١٢- د. عادل خميس المعمري، **التفتيش في الجرائم المعلوماتية**، بحث منشور في مجلة الفكر الشرطي، المجلد الثاني والعشرون، العدد ٨٦، ٢٠١٣م، ص٢٥٢.

١٣- د. خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، الإسكندرية، دار الفكر العربي، سنة ٢٠٠٩م، (ط١)، ص٧٧ وما بعدها.

١٤- د. هلالي عبد اللاه أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء اتفاقية بودابست**، القاهرة، دار النهضة العربية، سنة ٢٠٠٦م، (بدون طبعة)، ص١٦٨.

١٥- د. هلال بن محمد بن حارب البورسعيدي، **الحماية القانونية والفنية لقواعد المعلومات المحوسبة**، القاهرة، دار النهضة العربية، سنة ٢٠٠٩م، (بدون طبعة)، ص٣٥ وما بعدها.

١٦- د. أحمد محمود مصطفى، **جرائم الحاسبات الآلية في التشريع المصري**، القاهرة، دار النهضة العربية، سنة ٢٠١٠م، (ط١)، ص١٨.

١٧- د. خالد ممدوح إبراهيم، مرجع سابق، ص٨٦.

١٨- عمر أبو الفتوح عبد العظيم الحمامي، **المجلة الجنائية للمعلومات**، القاهرة، دار النهضة العربية، سنة ٢٠١٠م، (بدون طبعة)، ص ١٣٧.

١٩- محمد حماد مرهج الهيتي، **التكنولوجيا الحديثة والقانون الجنائي**، عمان، دار الثقافة للنشر والتوزيع، سنة ٢٠٠٤م، (ط١)، ص.١٦٦

٢٠- د. عبد الفتاح بيومي حجازي، مرجع سابق، ص٨٣ وما بعدها.

٢١- انظر المادة (٢١) من قانون تقنية المعلومات البحريني رقم ٦٠ لسنة ٢٠١٤م.

٢٢- د. عبد الفتاح بيومي حجازي، مرجع سابق، ص٨٣ وما بعدها.

٢٣- د. هدى حامد قشقوش، **جرائم الاعتداء على الحاسب الآلي في التشريع المقارن**، القاهرة دار النهضة العربية، سنة ١٩٩٢م، (ط١)، ص٢٧.

٢٤- د. خالد ممدوح إبراهيم، مرجع سابق، ص١٣٣.

٢٥- د. خالد ممدوح إبراهيم، مرجع سابق، ص٩٨ وما بعدها.

٢٦- انظر المواد (٣،٤،٥،٦،٧،٩،١٢) من قانون الجرائم الإلكترونية الأردني رقم ٢٧ لسنة ٢٠١٥م.

٢٧- انظر المواد (٧، ١٦، ٢٦) من قانون جرائم تقنية المعلومات الإماراتي رقم ٥ لسنة ٢٠١٢م.

٢٨- نهلا عبد القادر المومني، **الجرائم المعلوماتية**، عمان، دار الثقافة للنشر والتوزيع، سنة ٢٠١٠م، (ط٢)، ص١٣٤ وما بعدها.

٢٩- د. خالد ممدوح إبراهيم، مرجع سابق، ص١٠٤ وما بعدها.

٣٠- د. كامل السعيد، **شرح الأحكام العامة في قانون العقوبات - دراسة مقارنة**، عمان، دار الثقافة للنشر والتوزيع، سنة ٢٠١٢م، (ط٣)، ص ١٨٨.

٣١- د. محمد صبحي نجم، **قانون العقوبات - القسم العام (النظرية العامة للجريمة)**، عمان، دار الثقافة للنشر والتوزيع، سنة ٢٠١٢م، (ط٤)، ص٢١١.

٣٢- د. خالد ممدوح إبراهيم، مرجع سابق، ص١٠٤ وما بعدها.

٣٣- د. هدى حامد قشقوش، **جرائم الكمبيوتر والإنترنت والجرائم الأخرى في مجال تكنولوجيا المعلومات**، بحث مقدم إلى **المؤتمر السادس للجمعية المصرية للقانون الجنائي** والمنعقد في الفترة من (٢٥-٢٨) أكتوبر سنة ١٩٩٣م، ص٦٢، ٦٣.

٣٤- نهلا عبد القادر المومني، مرجع سابق، ص١١٠.

٣٥- محمد أمين الشوابكة، **جرائم الحاسوب والإنترنت**، عمان، دار الثقافة للنشر والتوزيع، سنة ٢٠٠٤م، (ط١)، ص١٤١.

٣٦- د. محمد محمود مكاوي، **الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية**، مصر المكتبة العصرية للنشر والتوزيع، سنة ٢٠١٠م، (ط١)، ص٢٥٠ وما بعدها.

٣٧- نهلا عبد القادر المومني، مرجع سابق، ص ١٥٠ وما بعدها.

٣٨- د. محمد صبحي نجم، مرجع سابق، ص٢١٣.

٣٩- د. خالد ممدوح إبراهيم، مرجع سابق، ص ١٠٤.

٤٠- انظر قرار محكمة النقض المصرية رقم ٢٩٩١ لسنة ٥٤ ق، جلسة ١٩٥٨/١/١٦م والذي أكّد على أنّ إثبات علاقة السببية في المواد الجنائية مسألة موضوعية ينفرد بها قاضي الموضوع ويقدرها ولا يجوز مجادلته في ذلك أمام محكمة النقض، ولا رقابة لمحكمة النقض على محكمة الموضوع في مسألة إثبات علاقة السببية.

٤١- د. نظام توفيق المجالي، **شرح قانون العقوبات (القسم العام)**، عمان، دار الثقافة للنشر والتوزيع، سنة ٢٠٠٦م، (بدون طبعة)، ص ٢٢٥.

٤٢- د. طلال أبو عفيفة، **شرح قانون العقوبات (القسم العام)**، عمان، دار الثقافة للنشر والتوزيع، سنة ٢٠١٢م، (ط١)، ص٣٠٩ وما بعدها.

٤٣- انظر تميز جزاء أردني ٩٣/٣٨٠، سنة ١٩٩٣م، ص٤٠٣، مجلة نقابة المحامين الأردنيين، وقرار رقم ٢٠٠٥/٤١٦ تميز جزاء أردني، مجلة نقابة المحامين الأردنيين، ص١٦٧٠، سنة ٢٠٠٦م.

٤٤- د. محمود نجيب حسني، **النظرية العامة للقصد الجنائي**، القاهرة، دار النهضة العربية سنة ٢٠٠٤م، (٤)، ص.١٦

٤٥- د. خالد ممدوح إبراهيم، مرجع سابق، ص١٠٩ وما بعدها.

٤٦- بلال أمين زين الدين، **جرائم أنظمة المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية**، الإسكندرية، دار الفكر العربي، سنة ٢٠٠٨م، (ط١)، ص١١٧.

٤٧- د. أحمد محمود مصطفى، مرجع سابق، ص١١٧.

٤٨- د. حسين بن سعيد الغافري، **السياسية الجنائية في مواجهة جرائم الإنترنت**، القاهرة، دار النهضة العربية، سنة ٢٠٠٩م، (بدون طبعة)، ص٣٢٨.

٤٩- د. خالد ممدوح إبراهيم، مرجع سابق، ص٢٥٩.

٥٠- د. جميل عبد الباقي الصغير، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**، القاهرة، دار النهضة العربية، (بدون طبعة)، سنة ١٩٩٨م، ص٧٥.

٥١- د. هشام محمد فريد رستم، **الجرائم المعلوماتية "أصول التحقيق الجنائي الفني"، بحث مقدم لمؤتمر "القانون والكمبيوتر والإنترنت"**، كلية الشريعة والقانون - جامعة الإمارات العربية المتحدة في الفترة من ١-٣/٥/٢٠٠٠م، المجلد الثاني، ط٣، ص٤٩٦.

٥٢- د. محمد السيد عرفة، **تدريب رجال العدالة وأثره في تحقيق العدالة، الرياض**، جامعة نايف للعلوم الأمنية، بدون طبعة، سنة ٢٠٠٥م، ص٥.

٥٣- د. ذياب البداينة، ورقة بحثية بعنوان "**الجرائم الإلكترونية - المفهوم والأسباب" مقدمة في الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"** وانعقد خلال الفترة من ٧-٩/١١/١٤٣٥هـ الموافق ٢-٤/٩/٢٠١٤م، ص١٠ وما بعدها.

٥٤- د. حسين بن سعيد الغافري، مرجع سابق، ص٦٣٨ وما بعدها.

٥٥- انظر المواد **(٢٢،٢٣،٢٤،٣٠،٣١،٣٣)** من الاتفاقية العربية لمكافحة الجرائم المعلوماتية لسنة ٢٠١٤م.

قائمة المراجع

- **المراجع القانونية:**

١. د. أحمد محمد مصطفى، **جرائم الحاسب الآلي في التشريع المصري**، ط١، القاهرة: دار النهضة العربية، سنة ٢٠١٠م.

٢. أمير فرج يوسف، **الجرائم المعلوماتية على شبكة الإنترنت**، بدون طبعة، الإسكندرية دار المطبوعات الجامعية، سنة ٢٠١٠م.

٣. بلال أمين زين الدين، **جرائم أنظمة المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية**، ط١، الإسكندرية: دار الفكر العربي، سنة ٢٠٠٨م.

٤. د. جميل عبد الباقي الصغير، **الجوانب الإجرائية للجرائم المتعلقة بالإنترنت**، بدون طبعة، القاهرة: دار النهضة العربية، سنة ١٩٩٨م.

٥. د. حسين سعيد الغافري، **السياسة الجنائية في مواجهة جرائم الإنترنت – دراسة مقارنة**، بدون طبعة، القاهرة: دار النهضة العربية، سنة ٢٠٠٩م.

٦. خالد ممدوح إبراهيم، **الجرائم المعلوماتية**، ط١، الإسكندرية: دار الفكر العربي ٢٠٠٩م.

٧. سامي علي حامد عياد، **الجرائم المعلوماتية وإجرام الإنترنت**، بدون طبعة، مصر: دار الفكر العربي، سنة ٢٠٠٧م.

٨. د. طلال أبو عفيفة، **شرح قانون العقوبات (القسم العام)**، ط١، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠١٢م.

٩. د. عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي** ط١، مصر: دار الكتب العربية، سنة ٢٠٠٧م.

١٠. عمر أبو الفتوح عبد العظيم الحمامي، **المجلة الجنائية للمعلومات**، بدون طبعة، القاهرة: دار النهضة العربية، سنة ٢٠١٠م.

١١. د. كامل السعيد، **شرح الأحكام العامة في قانون العقوبات – دراسة مقارنة**، ط٣، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠١٢م.

١٢. محمد أمين الشوابكة، **جرائم الحاسوب والإنترنت**، ط١، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠٠٤م.

١٣. محمد حماد مرهج الهيتي، **التكنولوجيا الحديثة والقانون الجنائي**، ط١، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠٠٤م.

١٤. د. محمد صبحي نجم، **قانون العقوبات – القسم العام (النظرية العامة للجريمة)**، ط٤، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠١٢م.

١٥. د. محمد محمود مكاوي، **الجوانب الأخلاقية والاجتماعية للجرائم المعلوماتية**، ط١، مصر المكتبة العصرية للنشر والتوزيع، سنة ٢٠١٠م.

١٦. د. محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت دراسة مقارنة**، ط٢، القاهرة، دار النهضة العربية، سنة ٢٠٠٩م.

١٧. د. محمد السيد عرفة، **تدريب رجال العدالة وأثره في تحقيق العدالة**، بدون طبعة، جامعة نايف للعلوم الأمنية، الرياض، سنة ٢٠٠٥م.

١٨. د. محمود نجيب حسني، **النظرية العامة للقصد الجنائي**، ط٤، القاهرة، دار النهضة العربية، سنة ٢٠٠٤م.

١٩. د. نائلة عادل محمد فريد، **جرائم الحاسب الآلي الاقتصادية**، بدون طبعة، لبنان منشورات الحلبي الحقوقية، سنة ٢٠٠٥م.

٢٠. د. نظام توفيق المجالي، **شرح قانون العقوبات (القسم العام)**، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠٠٦م.

٢١. نهلا عبد القادر المومني، **الجرائم المعلوماتية**، ط٢، عمان: دار الثقافة للنشر والتوزيع، سنة ٢٠١٠م.

٢٢. د. هدى حامد قشقوش، **جرائم الحاسب الآلي في التشريع المقارن**، ط١، القاهرة: دار النهضة العربية، سنة ١٩٩٢م.

٢٣. هلال بن محمد بن حارب البورسعيدي، **الحماية القانونية والفنية لقواعد المعلومات المحوسبة**، بدون طبعة، القاهرة: دار النهضة العربية، سنة ٢٠٠٩م.

٢٤. هلالي عبد اللاه أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلومات على ضوء اتفاقية بودابست**، بدون طبعة، القاهرة: دار النهضة العربية، سنة ٢٠٠٦م.

٢٥. د. هلالي عبد اللاه أحمد، **المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست**، المجلد السادس، العدد الثالث عشر، مجلة الحقوق، جامعة البحرين سنة ٢٠٠٩م.

٢٦. د. يوسف حسن يوسف، **الجرائم الدولية للإنترنت**، ط١، مصر: المركز القومي للإصدارات القانونية، سنة ٢٠١١م.

٢٧. د. عادل خميس المعمري، **التفتيش في الجرائم المعلوماتية**، **مجلة الفكر الشرطي**، المجلد الثاني والعشرون، العدد ٨٦، ٢٠١٣م.

٢٨. د. هشام محمد فريد رستم، **الجرائم المعلوماتية "أصول التحقيق الجنائي الفني"**، بحث مقدم لمؤتمر **"القانون والكمبيوتر والإنترنت"**، كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة، في الفترة من ١-٣/٥/٢٠٠٠م، المجلد الثاني، ط٣.

٢٩. د. هدى حامد قشقوش، **جرائم الكمبيوتر والإنترنت والجرائم الأخرى في مجال تكنولوجيا المعلومات**، بحث مقدَّم إلى **المؤتمر السادس للجمعية المصرية للقانون الجنائي** والمنعقد في الفترة من (٢٥-٢٨) أكتوبر سنة ١٩٩٣م.

٣٠. د. ذياب البداينة، ورقة بحثية بعنوان **"الجرائم الإلكترونية – المفهوم والأسباب"** مقدمة في **الملتقى العلمي "الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"** وانعقد خلال الفترة من ٧-٩/١١/١٤٣٥هـ الموافق ٢-٤/٩/٢٠١٤م، عمان، المملكة الأردنية الهاشمية.

- **التشريعات والاتفاقيات الدولية:**

١. قانون الجرائم الإلكترونية الأردني رقم (٢٧) لسنة ٢٠١٥م.
٢. قانون مكافحة تقنية المعلومات الإماراتي رقم (٥) لسنة ٢٠١٢م.
٣. قانون جرائم تقنية المعلومات البحريني رقم (٦٠) لسنة ٢٠١٤م.
٤. قانون أصول المحاكمات الجزائية الأردني رقم (٩) لسنة ١٩٦١م وتعديلاته.
٥. قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (٦٣) لسنة ٢٠١٥م.
٦. قانون منع الإرهاب الأردني رقم (٥٥) لسنة ٢٠٠٦م.
٧. قانون الاتصالات البحريني رقم (٤٨) لسنة ٢٠٠٢م.
٨. قانون الاتصالات الأردني رقم (١٣) لسنة ١٩٩٥م وتعديلاته لسنة ٢٠١١م.
٩. نظام مكافحة الجرائم المعلوماتية السعودي رقم (م/١٧) تاريخ ٨/٣/١٤٢٨هـ.

١٠. نظام هيئة الاتصالات السعودي رقم (م/١٢) تاريخ ١٤٢٢/٣/١٢هـ.
١١. اتفاقية بودابست والصادرة بتاريخ ٢٣ نوفمبر ٢٠٠١م.
١٢. اتفاقية الرياض للتعاون القضائي والصادرة بتاريخ ١٩٩٣/٤/٦م، الرياض.
١٣. الاتفاقية القانونية والقضائية الصادرة عن مجلس التعاون الخليجي في الفترة من ٢١-٢٠٠٣/١٢/٢٢م، الكويت.
١٤. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تاريخ ٢٠١٤/٢/٧م.