

# المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني (دراسة مقارنة)

م. خليل يوسف جندي

مدرس القانون الجنائي

جامعة دهوك / كلية القانون والعلوم السياسية / قسم القانون

## المقدمة

يجتاح العالم اليوم ثورة علمية وتقنية هائلة، وذلك بعد دخول الثورة الصناعية في النصف الثاني من القرن العشرين، إذ باتت تلك الثورة تطول كافة مناح الحياة، وامتدت إلى مجال الحاسب الآلي، الذي أدى بظهوره إلى إحداث ثورة علمية هائلة، وأصبح تقدم الدول وتطورها ترتبط تماماً بتقدم تلك الثورة في هذا المجال، ويعد الحاسب الآلي من أبرز التطورات في العصر الحديث، حيث ساعدت تلك الحاسبات الإنسان من خلال مراحل تطورها على حل العديد من المشاكل التي كان يصعب على الإنسان حلها بإمكانياته الذاتية، دون بذل الكثير من الجهد والوقت ودون التأكد في نفس الوقت من صحه ودقة النتائج التي توصل إليها، وقد أدى التطور في استخدام الحاسب الآلي إلى أن صار استخدامه عنصراً فعالاً ورئيسياً لتحقيق تقدم الأمم والشعوب، وكذلك معياراً لقياس مدى تحضر تلك الأمم، ولقد رافق هذا التقدم تزايداً ملحوظاً في الاعتماد على نظم المعلومات الآلية والتقنية القائمة على الحاسب الآلي كوسائل رئيسية لحفظ ومعالجة وتشغيل البيانات داخل معظم المؤسسات الحكومية وغير الحكومية، بل وبين الأفراد في حياتهم اليومية، هذا من ناحية أمّا الجانب الآخر فقد تمثل بتأثر الجريمة

تأثراً واضحاً بمراحل التطور المختلفة التي مر بها المجتمع وتفاعلت مع معطياته بالشكل الذي يساير هذا التطور، حيث نتج عن ذلك ظهور أنماط مستحدثة من صور الإجرام المرتبطة باستخدامات الحاسبات الآلية، أي إن التحول الحضاري والتقدم الذي اجتاح العالم في العصر الحديث، قد أحدث تغييراً ملموساً في نوعية الجرائم والمجرمين، فبعد أن كانت الغلبة للجرائم القائمة على العنف أو القسوة أصبحت الغلبة للجرائم القائمة على المقدرّة الذهنية والذكاء، وتعد شبكة الأنترنت إحدى أهم نتائج هذا التحول الحضاري والتقدم الذي اجتاح العالم في العصر الحديث، فهي عبارة عن عالم ضخم ومتنوع، عالم لا تحده الحدود الجغرافية، عالم خالي من العوائق المادية التي تمنع السفر والتجوال والترحال والأبحار بين أرجاء المعمورة، عالم ساهم في إنتاج وتطوير العديد من السلوكيات الإجرامية ذات الأثر البالغ على حياة الأفراد والمجتمع، ويقول أحد الفقهاء من خلال وصفه لشبكة الأنترنت التي يرتادها الملايين من الناس بأنها " أصبحت الآن مرتعاً للنازيين الجدد الداعين للعنصرية والاضطهاد للعديد من فئات بني البشر، وطريقاً لالتقاء أصحاب الشذوذ الجنسي، ووسيلة للاتصال والتنظيم بين الإرهابيين والقائمين على الجريمة المنظمة وكل من صدر ضده أمراً بألقاء القبض عليه نظير جريمته " ومن كل ما تقدم وانطلاقاً من منهج بحثنا ومن أجل الإحاطة بموضوع دراستنا بشكل دقيق وأكثر تفصيلاً ارتأينا إلى تقسيم هذا البحث على مبحثين، حيث نبحت في المبحث الأول : التعريف بالجريمة المعلوماتية، وفي المبحث الثاني نتناول المعالجة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني .

## المبحث الأول

### التعريف بالجريمة المعلوماتية

عندما انتصف القرن العشرين حدثت طفرة نوعية في مجال العلوم قاطبة، وكان على هرمها ثورة المعلومات التكنولوجية، وكان اختراع الحاسب الآلي الذي كان له تأثير مباشر على الحياة اليومية للإنسان، بحيث لا يخلو مكان من وجوده، فأصبح

موجوداً في كل المجالات لتبادل المعلومات الهامة، والارتباط بين شبكات المعلومات كان له تأثير مهم في تبادل المعلومات، وبات الكبير والصغير يستطيع أن يقرأ ويدون ما يحدث في العالم صباحاً ومساءً وكنا نقول إن العالم أصبح قرية صغيرة<sup>(١)</sup>، وهذا هو عصر الأنترنت أو عصر السماوات المفتوحة أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية، كل هذه الأوصاف والتسميات باتت تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت ومدى تنوع الانجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا اليومية في الآونة الأخيرة<sup>(٢)</sup>، ويبدو بالفعل إن تكنولوجيا المعلومات هي وقود الثورة الصناعية الثالثة، وإن المعلومات في حد ذاتها هي المادة الأساسية (الخام) للإنتاج الذي يعتمد المجتمع على إنتاجها وإيجادها والاستفادة منها<sup>(٣)</sup>، وفي الواقع إن هذا الوجه المشرق لتقنية المعلومات جاء خالياً من الجانب المظلم الذي يتمثل في الإجرام المعلوماتي والذي كان موجوداً ليستغل هذه التقنيات المتطورة لتحقيق مصالح ومآرب متنوعة ومتعددة، ولكل ما سبق ومن أجل تسليط الضوء بشكل أكثر تفصيلاً وتركيزاً سنقوم بتقسيم هذا المبحث على مطلبين، حيث سنتناول في المطلب الأول مفهوم الجريمة المعلوماتية، وفي المطلب الثاني نبحث في خصائص الجريمة المعلوماتية، وعلى النحو التالي:

(١) د. عادل عبدالله خميس المعمري، التفتيش في الجرائم المعلوماتية، بحث منشور، مجلة الفكر الشرطي، المجلد ٢٢، العدد ٨٦، مركز بحوث الشرطة، الإمارات العربية المتحدة، ٢٠١٣، ص ٢٤٧.

(٢) د. هلالى عبد اللاه احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٣، ص ١٢.

(٣) هذا ما اشار اليه العالم الاجتماعي دانيل بل في كتابه مجتمع ما بعد الصناعي مشار اليه في المصدر نفسه، ص ١١.

## المطلب الأول

### مفهوم الجريمة المعلوماتية

إن الجرائم التي نحن بصدد بحثها " جرائم المعلوماتية " لا يوجد مصطلح موحد للدلالة عليها والبعض يطلق عليها جريمة " الغش المعلوماتي " والبعض الآخر يطلق عليها " الجريمة المعلوماتية " والآخر يطلق عليها " ظاهرة الاختلاس المعلوماتي " والآخر يطلق عليها " جناح المعلوماتية "، مما يصعب معه التقرير بإمكان إيجاد تعريف موحد باعتبار إن الظاهرة حديثة نسبياً مما يخشى معه حصرها في نطاق محدد<sup>(١)</sup>، ومفاد ذلك إنه لم يتفق الفقهاء لحد الآن على تعريف جامع مانع للجرائم المعلوماتية، وذلك لأنه من الصعب وضع تعريف محدد لهذه الظاهرة، لكونها تتعلق بتكنولوجيا تتطور باستمرار ولا تقف عند حد<sup>(٢)</sup>، فتنوع واختلاف وسائل ارتكابها، وتجدد أشكالها فضلاً عن اختلاف الزاوية التي ينظر إليها من قبل واضع التعريف<sup>(٣)</sup>، علاوة على ما تتميز به من خصائص، جعل الجريمة المعلوماتية كما قيل عنها بأنها تقاوم التعريف، والدليل على ذلك إن الكتابات التي تناولتها بالتعريف تحفل بحسب تعبير البعض " بملايين الكلمات " التي سطرت في محاولات عديدة لصياغة تعريفها<sup>(٤)</sup>، كما إن المشكلة الرئيسية التي تقف في طريق الباحثين فيما يخص الجريمة المعلوماتية هي عدم وجود مصطلح متفق عليه لهذه الظاهرة، وهذا بالتأكيد ينعكس بدوره على تعريف

(١) عيفي كامل عيفي، جرائم الكمبيوتر، رسالة ماجستير، مقدمة إلى كلية الحقوق، جامعة الإسكندرية، ٢٠٠٣، ص ١٨ .

(2) Timothy J.o'hearn , Crime and Technology : (New rules in a new World) , 1998, Vol.7(2) , Information & Communications Technology Law , p.148 .

(٣) محمود احمد عابينة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠٠٩، ص ١٤ .

(٤) عيفي كامل عيفي، مصدر سابق، ص ١٨ .

الجريمة المعلوماتية، وبالنسبة لاتجاهنا بخصوص المصطلح والتسمية فنحن نميل مع من<sup>(١)</sup> ذهب إلى استعمال مصطلح " الجرائم المعلوماتية "، لكونها من أدق ما يمكن إطلاقه على مثل هذه الجرائم، وذلك على اعتبار انها تشمل الحاسب وسائر المبتكرات والتقنيات الزاهنة والمستقبلية المستخدمة في التعامل مع المعلومات، ويضاف إلى ذلك تجنب أغلبية المشرعين، مسألة إيراد تعريف لها، لكونه مسلك يعاب عليه ويكون عرضة للانتقاد، فالمشرع غير ملزم بإيراد التعاريف، والدليل على خلو ساحته من الانتقاد، هو أن الجرائم المعلوماتية، تعد جرائم مستحدثة ذات بعدين، البعد القانوني والبعد التقني، وهو ما يجعل تعريفها أمراً مستعصياً لدى المشرعين<sup>(٢)</sup>، والتعريفات التي صيغت بصدد الجرائم المعلوماتية عديدة، ومتفاوتة فيما بينها ضيقاً واتساعاً، وبالإمكان تصنيفها بشكل عام مستنديين إلى أربع معايير، سنبحثها في أربعة فروع على النحو التالي :

### الفرع الأول: معيار وسيلة ارتكاب الجريمة

حسب مضمون هذا المعيار، فان تعريف الجرائم المعلوماتية تستند على أداة ارتكاب هذه الجرائم، على اعتبار إن الحاسب الآلي يعد الأداة التي تستخدم في ارتكاب الجرائم المعلوماتية، وخير من يمثل ويؤيد هذا المعيار هو الفقيه الألماني تاديومان (Tiedemann) والذي عرف هذه الجرائم على أنها: " كل أشكال السلوك غير المشروع أو الضار بالمجتمع، والذي يرتكب باستخدام الحاسب"<sup>(٣)</sup>، وعرفها الفقيه الإنكليزي ليزلي بول (Leslie D.Ball) بأنها: " فعل إجرامي يستخدم الحاسب في

(١) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، اسبوط، ١٩٩٤، ص ٣٥ .

(٢) د. عبدالفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنترنت في القانون العربي النموذجي، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٨، ص ١٨ .

(٣) د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١١، ص ١٨ .

ارتكابه كأداة رئيسية<sup>(١)</sup>، وبعبارات يغلب عليها الطابع التقني، يعرف كل من الفقيهين (Richard Totty and Anthony Hard castle) الجرائم المعلوماتية، من خلال تعريفها للجرائم المرتبطة أو المتعلقة بالحاسب على أنها: " تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب، وبعبارة أخرى: " هي تلك الجرائم التي يكون دور الحاسب فيها إيجابياً أكثر من سلبي<sup>(٢)</sup>، كما يعرف الجريمة المعلوماتية على أنها : " كل نشاط إجرامي يؤدي فيه النظام دوراً لإتمامه، أو يقع على النظام نفسه"<sup>(٣)</sup>، وعرفها آخر على أنه : " نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة، كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"<sup>(٤)</sup>، وبحسب التعريفات أعلاه فإنه لإطلاق صفة المعلوماتية على جريمة ما ينبغي أن تتضمن تلك الجريمة استخدام الحاسب الآلي، وهو ذات الاتجاه الذي أعتمد عليه نظام مكافحة جرائم المعلوماتية السعودي بصدد تعريفه للجرائم المعلوماتية حيث نص على أنه: " أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"<sup>(٥)</sup>، وقد تعرض هذا المعيار لانتقادات، مفادها أن تعريف الجريمة المعلوماتية يقوم في الأساس على العمل الرئيسي المكون لها، وليس فقط على

(١) رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، ٢٠١٣، ص ١٩ .

(٢) د. هشام محمد فريد رستم، جريمة الحاسب كصورة من الجرائم الاقتصادية المستحدثة، بحث منشور، مقدم لمؤتمر الأمم المتحدة لمنع الجريمة الذي عقد في ٢٩ أبريل، منشور في مجلة الدراسات القانونية، كلية الحقوق، جامعة اسويط، العدد ١٧، يونيو ١٩٩٥، ص ٣٠ .

(٣) د. شيماء عبدالغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧، ص ١٢ .

(٤) د. عبدالفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ١٧ .

(٥) المادة (١) الفقرة (٨) من نظام مكافحة جرائم المعلوماتية السعودي رقم ١٧ لسنة ٢٠٠٧ .

الأداة المستخدمة فيها<sup>(١)</sup>، علاوة على أن الوسيلة ليست محل اعتبار لدى المشرع الجزائي عند التجريم، لكون أغلب الوسائل متساوية، والتكوين القانوني للجريمة بتوافر أركانها هو محل الاعتبار عند تطبيق نصوص التجريم<sup>(٢)</sup>، فضلاً عن أن الأخذ بهذا المعيار سوف يؤدي وبلا شك إلى توسيع نطاق الجرائم المعلوماتية .

### الفرع الثاني: معيار موضوع الجريمة

استناداً إلى هذا المعيار تعد الجريمة معلوماتية، إذا ما وقعت على الحاسب الآلي أو داخل نظامه، أي بمعنى متى ما كان محل الجريمة هو الحاسب الآلي أو نظامه المعلوماتي، فالجريمة تكون معلوماتية<sup>(٣)</sup>، ومن أمثلة هذه التعريفات ما قال به الفقيه روزنبلات (Rosenblatt) حيث عرف هذه الجرائم بأنها : "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"<sup>(٤)</sup>، وبذات الاتجاه تم تعريف هذه الجرائم بأنها : "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات، والجرائم الإلكترونية مجموعة الجرائم التي تتصل بالمعلوماتية"<sup>(٥)</sup>، بينما عرفها خبراء منظمة التعاون والتنمية الاقتصادية خلال مؤتمر عقد في باريس سنة ١٩٨٣ حول الجرائم المرتبطة بالمعلوماتية على أنها : " كل سلوك غير مشروع أو غير أخلاقي أو

(١) د. سامي جلال فقي حسين، التنقيش في الجرائم المعلوماتية، دار الكتب القانونية، الإسكندرية،

٢٠١١، ص ٢٠.

(٢) محمود احمد عباينة، مصدر سابق، ص ٢٠.

(٣) د. علي حسن الطوالبه، الجرائم الإلكترونية، الطبعة الثانية، مؤسسة فخراوي للدراسات والنشر،

مملكة البحرين، ٢٠٠٩، ص ٤٨.

(٤) د. فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، بحث منشور، مجلة العلوم القانونية

والاقتصادية، كلية الحقوق، جامعة عين شمس، العدد ٢، السنة ٤٤، يوليو ٢٠٠٢، ص ٤٨٦.

(٥) د. هدى حامد قشقوش، جرائم الحاسوب الإلكتروني في التشريع المقارن، دار النهضة العربية،

القاهرة، ١٩٩٢، ص ٢٠.

غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها<sup>(١)</sup>، وهذا المعيار كسابقه قد تعرض للانتقاد، وذلك لكونه يضيق من نطاق الجرائم المعلوماتية ويقتصرها على الجرائم الواقعة على الحاسب الآلي أو داخل نظامه، في الوقت الذي يغفل الجرائم التي تقع بواسطة الحاسب الآلي<sup>(٢)</sup>.

### الفرع الثالث: معيار مدى توافر المهارة بالتقنية المعلوماتية

يستند أصحاب هذا المعيار على لزوم المام الفاعل بتقنية المعلومات وإمكانية استخدام الحاسب الآلي، لكي تعد جريمته من الجرائم المعلوماتية، على اعتبار أن من يفقد هذه المهارة غير قادر على ارتكاب هذه الجرائم<sup>(٣)</sup>، وقد تم تعريف الجريمة المعلوماتية من قبل أنصار هذا المعيار ومنهم الفقيه ديفيد ثومبسون (David Thompson) بأنها: " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً"<sup>(٤)</sup>، وبناءً على ذلك لا بد أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من المعرفة التكنولوجية بالحاسبات لتلاحقه هذه الجريمة قانونياً، كما ان هذا التعريف قد تبنتها وزارة العدل الأمريكية في مجال تعريفها للجرائم المعلوماتية في تقريرها الصادر سنة ١٩٨٩<sup>(٥)</sup>، ويعرفها الفقيه ستين سكيولبيرك

(١) محمد عبدالله أبو بكر سلامة، جرائم الكمبيوتر والأنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦، ص ٧٣ .

(٢) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٥، ص ٢٤ .

(٣) د. علي حسن الطويلة، مصدر سابق، ص ٤٩ .

(٤) د. نسرين عبدالحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٨، ص ٥٩ .

(٥) د. راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث منشور، مجلة الحقوق للبحوث القانونية والاقتصادية، العدد الأول، كلية الحقوق، جامعة الإسكندرية، ٢٠٠٨، ص ٨.



(Stein Schiolberg) بأنها: " أية جريمة يكون متطلباً لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب"<sup>(١)</sup>.

وكالعادة لقد أخذ هذا المعيار نصيبه من النقد أيضاً، وذلك لكون الأخذ به يؤدي إلى البحث و التحري عن الظروف الخاصة بالفاعل للوصول إلى حقيقة توافر هذه المهارة من عدمها، وهو الأمر الذي لا يتناسب مع القانون الجنائي، الذي هو بالأصل قانون موضوعي، ولا يعير للظروف الشخصية أهمية إلا في حالات استثنائية<sup>(٢)</sup>، كما أن هذا المعيار قد فاتته ما يحصل من تطورات سريعة في مجال المعلوماتية في وقتنا الحاضر، فلم تعد الأجهزة التقنية بنفس الشكل من التعقيد السابق، بل أصبح من السهل استخدامها حتى من قبل من لا يعرف شيئاً عن علوم الكمبيوتر، مثل الذي يقوم بإتلاف بيانات مخزنة في داخل الحاسب الآلي من دون أن تكون لديه أية معلومات أو معرفة بتقنية المعلوماتية<sup>(٣)</sup>.

#### الفرع الرابع: المعيار المزدوج (المختلط)

كما هو واضح من العنوان فان هذا المعيار يعتمد على الدمج بين معيار أداة الجريمة ومعيار موضوع الجريمة، والمعيارين يمثلان ذات الشيء وهو الكمبيوتر (الحاسب الآلي)، ومن التعريفات التي أخذت بهذا المعيار التعريف الذي اعتمده خبراء من بلجيكا في معرض ردهم على الاستبيان الذي أجرته منظمة التعاون والتنمية الاقتصادية (OCDE) حول الغش المعلوماتي عام ١٩٨٢، والذي جاء فيه أن الجرائم المعلوماتية هي: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو

(١) د. امل فاضل عبد خشان و د. احمد حمد الله، الأثبات الجنائي في جرائم اساءة استعمال الهاتف النقال، بحث منشور، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد ٤، الجزء الأول، العدد ١٢، ٢٠١٥، ص ٣١٧.

(2) Bert-Jaap Koops , Technology and the crime society : (Rethinking legal protection) , 2009 , Vol.2(1) , 1Law Innovation and tech.93 , p.106 .

(٣) د. نسرين عبدالحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، مصدر سابق، ص ٦٠.

المعنوية، يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية<sup>(١)</sup>، ومن الفقهاء الذين اعتمدوا هذا المعيار، الفقيهان جاك بولجنا وروبرت لند كويست (Jack Bologna and Robert J.Lindquist) حيث عرفاها إنها: "جريمة تستخدم الحاسب كوسيلة أو أداة لارتكابها أو يمثل أجراء بذلك أو جريمة يكون الحاسب نفسه ضحيتها"<sup>(٢)</sup>، وقد أخذت منظمة الأمم المتحدة في مؤتمرها العاشر لمنع الجريمة ومعاينة المجرمين الذي عقد في فيينا في الفترة من (٧-١٠/٤/٢٠٠٠) بهذا المعيار وعرفت الجريمة المعلوماتية بأنها: " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي أو شبكة حاسوبية والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"<sup>(٣)</sup>.

ونحن من جانبنا نتفق مع هذا التعريف، لكونه تعريف حاول الإحاطة والإلمام قدر الإمكان بجميع الأشكال الإجرامية للجريمة المعلوماتية سواء التي تقع بواسطة النظام المعلوماتي أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما شمل التعريف جميع الجرائم التي من الممكن أن تقع في بيئة إلكترونية، كما أن هذا التعريف لم يركز على فاعل الجريمة وقدراته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية، بل أنه حاول عدم حصر الجريمة المعلوماتية في نطاق ضيق، الأمر الذي لم يفسح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب .

(١) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مصدر سابق، ص ٣٣.

(٢) رشاد خالد عمر، مصدر سابق، ص ٢٤ .

(٣) د. نهلا عبدالقادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع،

عمان، الأردن، ٢٠١٠، ص ٥٠ .

## المطلب الثاني

### خصائص الجريمة المعلوماتية

إن ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الأنترنت أضفى عليها مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية، والتي منحنتها طابعاً خاصاً، ولذلك سنقوم بتقسيم هذا المطلب أربعة فروع، نبحت فيها أبرز واهم هذه الخصائص وعلى النحو التالي :

#### الفرع الأول: الجريمة المعلوماتية متعددة الحدود (عابرة للدول)

إن الشيء الذي يميز الجريمة المعلوماتية بصورة رئيسية هي أنها غير مقيدة برقعة جغرافية معينة، مفادها أن البيئة المعلوماتية التي تحصل فيها هذه الجرائم لا تعترف بالحدود الجغرافية للدول، حيث لا حدود مرئية أو ملموسة تعرقل نقل المعلومات عبر الدول المختلفة بعد ظهور شبكة الاتصالات<sup>(١)</sup>، والتي بدورها استطاعت أن تربط إعداداً كثيرة من الحاسبات الآلية عبر الدول، حيث أصبح أمر التنقل والاتصال فيما بينها سهلاً ويسيراً<sup>(٢)</sup>، وهذه الميزة جعلت بالإمكان ارتكاب الجريمة عن بعد، فقد يكون الجاني في دولة معينة والمجني عليه في دولة ثانية، وقد تتحقق نتيجة الجريمة خارج إقليم الدولة التي يتواجد فيها الجاني أو المجني عليه<sup>(٣)</sup>، وإن الجرائم المعلوماتية قد لا تتفرد بهذه الخاصية، حيث أن بعض الجرائم التقليدية هي الأخرى لها ذات الخصائص،

(١) نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص٣٨.

(٢) محمد محمد عمر الغياثين، الجرائم المعلوماتية عابرة الحدود، اطروحة دكتوراه، مقدمة إلى كلية الحقوق، جامعة القاهرة، ٢٠١٣، ص٦.

(٣) محسن بن سليمان الخليفة، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، رسالة ماجستير، مقدمة إلى كلية الدراسات العليا، قسم العدالة الجنائية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣، ص٤٥.

مثل جرائم الإرهاب الدولية وتجارة المخدرات وغسل الأموال، إلا أنها تتميز عن الأخيرة من حيث إمكانية ارتكابها من دون الحاجة إلى التنقل أو الحركة أو حتى مغادرة المقعد المقابل للحاسب الآلي<sup>(١)</sup>، وهذه الطبيعة التي تتميز بها الجريمة المعلوماتية، كونها جريمة عابرة للحدود أثارت العديد من المشاكل القانونية حول تحديد الدولة صاحبة الاختصاص القضائي فيما يخص هذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق، ومدى فاعليته فيما يتعلق بجمع وقبول الأدلة المتحصلة من البيئة المعلوماتية، فضلاً عن الإشكاليات التي تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام، الأمر الذي يكشف عن الحاجة الملحة إلى التعاون الدولي في مجال مكافحة هذه الجرائم وضبط مرتكبيها والحد من أضرارها<sup>(٢)</sup>.

### الفرع الثاني: صعوبة الأثبات في الجريمة المعلوماتية واكتشافها

تمتاز الجريمة المعلوماتية بأن أمر اكتشافها في غاية الصعوبة، وفي حالة اكتشافها فإن ذلك يكون من محاسن الصدفة أحياناً<sup>(٣)</sup>، ومن الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة جداً إذا ما قورنت بما تم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف خلف الصعوبة في اكتشاف الجريمة المعلوماتية إلى عدم ترك هذه الجريمة لأي آثار مادية ملموسة، فهي ترتكب في الخفاء ودون أي أثر يشير إلى مرتكبها، على خلاف الجرائم التقليدية التي يترك مرتكبها عادةً آثاراً مادية

(١) محمود احمد عباينة، مصدر سابق، ص ٣٤ .

(٢) محمد عبدالله محمد العوا، المسؤولية الجنائية الناشئة عن جرائم الأموال عبر الأنترنت، اطروحة دكتوراه، مقدمة إلى كلية الحقوق، جامعة الإسكندرية، ٢٠١٢، ص ٢٣ ص ٢٤.

(٣) جميل عبدالباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩٢، ص ١٧ .

لملوسة مثل (الجثة، الدماء، الشعر، البصمات وغيرها)<sup>(١)</sup>، ومفاد ذلك هو أن الجرائم المعلوماتية في أكثر صورها خفية لا يشعر بها المجني عليه أو حتى لا يعلم بوقوعها، والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي يتم تسجيل البيانات عن طريقها أمراً ليس عسيراً في الكثير من الأحوال، وذلك بحكم توافر المعرفة والخبرة في مجال الحاسوب غالباً لدى مرتكبها<sup>(٢)</sup>، ويحتل المجني عليه دوراً بارزاً في مسألة صعوبة اكتشاف وقوع الجريمة المعلوماتية، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك أو تتال خسائر فادحة من جراء ذلك، على عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي عادةً باتخاذ إجراءات إدارية داخلية، دون الإبلاغ عنها للسلطات المختصة تجنباً من الأضرار بسمعتها ومكانتها وإخلال الثقة في كفاءتها<sup>(٣)</sup>، ولأسباب أعلاه والعوامل الأخرى تجعل من الجرائم المعلوماتية صعبة الاكتشاف والأثبات .

### الفرع الثالث: جرائم المعلوماتية جرائم ناعمة

ان الخصوصية التي تتمتع بها الجريمة المعلوماتية تبرز بشكل أكثر وضوحاً

- (١) د. عماد مجدي عبدالملك، جرائم الكمبيوتر والأنترنيت، دار المطبوعات الجامعية، الإسكندرية، ٢٠١١، ص ٤٣. وبيانات المعنى ينظر: د. محمد حماد مرهج الهيكي، الجريمة المعلوماتية نماذج من تطبيقاتها، دار الكتب القانونية، القاهرة، ٢٠١٤، ص ٩٥ وما بعدها .
- (٢) د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، الطبعة الأولى، مكتبة الآلات الحديثة، اسيوط، ١٩٩٤، ص ١٦ .
- (٣) وتشير بعض التقديرات إلى ان ما يتراوح بين (٢٠-٢٥%) من جرائم الحاسبات لا يتم الإبلاغ عنها مطلقاً خوفاً من الإساءة إلى السمعة، وفي دراسة وصفت بانها ملفته للنظر اجريت على الف شركة من الشركات المنتجة لجهاز (Fortuner500) اظهرت نتائجها ان ٢% فقط من كل جرائم الحاسب هي التي يتم الإبلاغ عنها للشرطة أو لمكتب التحقيقات الفيدرالي . ولمزيد من الاستيضاح، ينظر: د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مصدر سابق، ص ٢٥ ص ٢٦ .

في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعاً من المجهود العضلي، الذي قد يكون في صورة ممارسة العنف والإيذاء، كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما في جريمة السرقة، مفاده إن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها (Soft crime)، لا تحتاج إلى العنف ولا سفكاً للدماء<sup>(١)</sup>، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب وكيفية تشغيله على مستوى عالي من التقنية بالشكل الذي يوظف في ارتكاب الأفعال غير المشروعة<sup>(٢)</sup>، وتحتاج أيضاً إلى وجود شبكة المعلومات الدولية (الأنترنت) مع وجود مجرم يسخر خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين كل ذلك دون الحاجة إلى صرف مجهود عضلي أو سفك دماء<sup>(٣)</sup>.

#### الفرع الرابع: خصوصية مجرمي المعلوماتية

إن المجرم الذي يرتكب الجريمة المعلوماتية يسمى بالمجرم المعلوماتي، والذي يتصف بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية، حيث أن الجرائم التقليدية لا علاقة لها بالمستوى العلمي والمعرفي للمجرم في عملية ارتكابها، على اعتبار أنها قاعدة عامة، وعلى خلاف ذلك فإن الأمر بالنسبة للجرائم المعلوماتية مختلف، فهي جرائم فنية تقنية<sup>(٤)</sup>، ومن يقترفها عادة يكون من ذوي المهارة في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والمقدرة على

(١) د. عبدالصبور عبد القوي علي مصري، المحكمة الرقمية والجريمة المعلوماتية، الطبعة الأولى،

مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، ٢٠١٢، ص ٥١.

(٢) محسن بن سليمان الخليفة، مصدر سابق، ص ٤٤.

(٣) أسامة احمد المناعسة و جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة

الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٤، ص ٩٧.

(٤) د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، دار النهضة العربية،

القاهرة، ٢٠٠٩، ص ٥٣.

استعمال الحاسوب والتعامل مع شبكة الأنترنت، وعلى سبيل المثال، فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للأموال يستوجب مهارة ومقدرة فنية تقنية عالية من قبل مرتكبيها<sup>(١)</sup>، ولذلك لزاماً علينا أن نبحث عن هوية مرتكبي الجرائم المعلوماتية وكما يلي :

١- الذكاء والمهارة : أن الإجرام المعلوماتي هو إجرام للأذكاء مقارنة بالإجرام التقليدي الذي يميل إلى العنف، حيث أن المجرم المعلوماتي ذو مهارات تقنية عالية والمأم بتكنولوجيا النظم المعلوماتية<sup>(٢)</sup>، كما أن اكتسابه للذكاء يكون أما من خلال الدراسة المتخصصة أو من خلال التطبيق والخبرة العلمية أو من خلال مخالطة المختصين بالمعلوماتية في الوسط الاجتماعي<sup>(٣)</sup>، ومفاد ذلك إن المجرم المعلوماتي لا ينتمي إلى فئة المجرمين الأغبياء، فمن يسرق أشياء من منزل قد يكون ذو ذكاء واطىء، على خلاف الذي يستخدم حاسوباً ألياً ويخترق النظام المعلوماتي ويستولي أو يتلف ما فيه من معلومات، فذلك يستوجب توافر الذكاء والمهارة<sup>(٤)</sup>، وهو يختلف من مجرم لآخر، ولكن المهم هنا أن يكون على قدر من المهارة والذكاء، فالجريمة المعلوماتية من الصعب ارتكابها دون توافرها، وهما اللذان يحددان الكيفية التي تتم بها هذه الجريمة<sup>(٥)</sup>.

٢- السلطة والمعرفة : ويقصد بالسلطة، هو إن يكون للمجرم المعلوماتي حقوق ومزايا تجاه نظام المعلومات الذي يستهدف من قبله بالشكل الذي تجعله مسيطراً ومتحكماً

(١) نهلا عبدالقادر المومني، مصدر سابق، ص ٥٩ .

(٢) د. ايمن عبدالحفيظ عبدالحميد سليمان، الأحكام الموضوعية للقانون الجنائي والجرائم المعلوماتية، رسالة ماجستير، مقدمة إلى كلية الحقوق، جامعة القاهرة، ٢٠١٠، ص ٧ ص ٨ .

(٣) رشاد خالد عمر، مصدر سابق، ص ٤٩ .

(٤) د. عبدالفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، مصدر سابق، ص ٩٨ .

(٥) د. محمد قدري حسن عبدالرحمن، جرائم الاحتيال الإلكتروني، بحث منشور في مجلة الفكر الشرطي، المجلد (٢٠)، العدد ٧٩، اماره الشارقة، الإمارات العربية المتحدة، ٢٠١١، ص ١١٦ .

به إلى حد ما<sup>(١)</sup>، وهذه السلطة قد تكون مباشرة، في حالة الشخص الذي لديه الشفرة الخاصة والتي تمكنه من الدخول إلى النظام المعلوماتي الذي يحتوي على المعلومات، أو تكون غير مباشرة، في حالة الشخص الذي لديه التصريح في دخول الغرفة أو المكان الذي يوجد فيه الأنظمة المعلوماتية (الحاسبات الآلية وأدواتها)، دون الحق في الدخول إلى النظام المعلوماتي، إلا أنه هذه الصفة ليست مطلقة، حيث إنها لا تتوافر لدى من يخترق النظام المعلوماتي لمؤسسة ما وهو خارجها دون أن يملك تصريح<sup>(٢)</sup>، وفيما يخص المعرفة، فإنها تتمثل بالدراية والمعرفة بكافة الظروف التي تحيط بالجريمة المراد ارتكابها، وكذلك احتمالات الفشل والنجاح، ويتلاني ما هو غير متوقع من الأمور من خلال التصور الكامل للجريمة في الأذهان، ويعود ذلك إلى البيئة التي ترتكب فيها الجريمة، والمجرم المعلوماتي بإمكانه أن يطبق جريمته على أنظمة مشابهة لتلك التي ينوي استهدافها قبل تنفيذ جريمته<sup>(٣)</sup>.

٣- متكيف اجتماعياً وهادئ: المجرم المعلوماتي إنسان اجتماعي، وعلى الأغلب لا يعادي المجتمع ولا يتظاهر بميول عدائية تجاه المجتمع، بل على العكس من ذلك هو متكيف مع المجتمع، إلا أن هذا لا يعني انعدام الخطورة لديه، بل على خلاف ذلك قد تزداد الخطورة لديه إذا ما زاد تكيفه الاجتماعي فيما لو توافر لديه الاستعداد الإجرامي<sup>(٤)</sup>، وهناك من يرى أن صفة الذكاء لدى المجرم المعلوماتي ما

(١) د. طارق ابراهيم الدسوقي عطية، عولمة الجريمة، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠، ص ٢٣٤.

(٢) رشاد خالد عمر، مصدر سابق، ص ٥٠.

(٣) محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، مطابع دار الجمهورية للصحافة، القاهرة، ٢٠١٠، ص ٥٢.

(٤) شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ٤٢.



هي إلا القدرة على التكيف الاجتماعي<sup>(١)</sup>، وكذلك فإن المجرم المعلوماتي هو من المجرمين الذين لا يلجؤون إلى العنف في ارتكابهم الجرائم المعلوماتية، حيث إن هذه الجرائم لا تستوجب استخدام العنف أو حتى الجهد العضلي لارتكابها، على العكس من الجرائم التقليدية<sup>(٢)</sup>، والمجرم المعلوماتي غير قادر على ارتكاب الجرائم التقليدية والتي تستلزم مواجهة مع المجني عليه، حيث إنه لا يستطيع الاعتداء على المجني عليه مباشرة، إلا إنه لا يجد صعوبة في الاعتداء عليه عن طريق النظام المعلوماتي<sup>(٣)</sup>.

## المبحث الثاني

### المعالجة التشريعية للجرائم المعلوماتية على المستويين الدولي والوطني

أن من نتائج التطور التكنولوجي الحاصل على المستويين الدولي والوطني، أن أصبحت المعلومات أو بمصطلح أدق (تقنية المعلومات) من أولويات الحياة في المجتمعات المعاصرة، وكالعادة مثلما تبرز النواحي الإيجابية للمعلوماتية، التي تهدف إلى المزيد من الرفاهية للبشرية، تظهر الآثار السلبية لها، عن طريق لجوء البعض من مستخدمي هذه التقنية المتطورة في تحقيق أهداف خاصة، من خلال اقتناف الجرائم المعلوماتية بواسطة هذه التقنية الحديثة<sup>(٤)</sup>، مفاده أن الجريمة الواقعة هنا هي من نتاج التطور والتكنولوجيا، أي من مستحدثات العصر، ولذلك تسمى عند البعض بأنها

(١) د. سليمان احمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، ٢٠١٣، ص ٢٢ .

(٢) د. محمد حماد مرهج الهيكلي، مصدر سابق، ص ٩٣. وبنفس المعنى ينظر: شمسان ناجي صالح الخيلي، مصدر سابق، ص ٤١ .

(٣) هذا ما توصل إليه الأستاذ باركر من خلال دراسته للفئات المختلفة لمجرمي المعلوماتية . ولمزيد من الاستيضاح، ينظر: د. نائلة عادل محمد فريد قورة، مصدر سابق، ص ٥٦ .

(٤) د. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١١، ص ٢٣ .

جريمة العصر<sup>(١)</sup>، وبظهور هذه الجرائم وعدم كفاية مواد القوانين العقابية التقليدية مواجهتها سعت معظم دول العالم وخاصةً المتقدمة قانونياً منها إلى سن التشريعات وإصدار القوانين لمواجهة هذه الجرائم أولاً ولمواكبة التطور ثانياً والسير تحت ظلال العولمة التي اجتاحت الكون بأسره في ظل الألفية الجديدة من القرن الحالي، ولكل ما سبق سنقوم بتقسيم هذا المبحث على مطلبين، نبحت في المطلب الأول: المعالجة التشريعية للجرائم المعلوماتية على المستوى الدولي، وفي المطلب الثاني: تناول المعالجة التشريعية للجرائم المعلوماتية على المستوى الوطني، وعلى النحو التالي:

## المطلب الأول

### المعالجة التشريعية للجرائم المعلوماتية على المستوى الدولي

أن مكافحة الجرائم المعلوماتية حظيت باهتمام دولي، سواء كان الاهتمام منصباً على الجرائم المعلوماتية بذاتها، أم على الجرائم الإلكترونية بشكل عام، وفي الحالتين فإن الجرائم المعلوماتية أخذت النصيب الأكبر، على اعتبار أنها المدخل الرئيسي لارتكاب الجرائم الإلكترونية بشكل عام<sup>(٢)</sup>، وإذا ما نظرنا إلى الجهود التي تم بذلها على المستوى الدولي، فإنه يتحدد أساساً على ضوء الاتفاقيات الدولية كخطوة أولى، ومن ثم المؤتمرات الدولية التي تم اعتمادها بهذا الشأن، وذلك بهدف إيجاد الحلول التشريعية الناجعة في مواجهة هذه الجرائم، ومن أهم وأبرز هذه الاتفاقيات هي اتفاقية بودابست لكونها حظيت بالاهتمام والالتزام من الدول الأعضاء فيها والموقعين عليها، أما المؤتمرات فإنها لازالت تعقد هنا وهناك وبشكل مستمر دون أن يتكفل جهودها بالنجاح

(١) د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠٩، ص ٦٩ .

(٢) د. محمد عوض الترتوري و د. اغادير عرفات جويحان . علم الإرهاب (الاسس الفكرية والنفسية والاجتماعية والتربوية لدراسة الإرهاب)، الطبعة الاولى، دار الحامد للنشر والتوزيع، عمان، ٢٠٠٦، ص ٣٥٢ .

لكون توصياتها عارية عن الالتزام، وللأسباب أعلاه سنتطرق فقط إلى اتفاقية بودابست الأوربية وبشكل تفصيلي ومن خلال فرع واحد على النحو التالي :

### الفرع الواحد: اتفاقية بودابست Budapest Convention

من الاتفاقيات الدولية المهمة التي تم إبرامها لمكافحة الجرائم المعلوماتية هي اتفاقية بودابست، وتعد الاتفاقية الوحيدة، والمعروفة بالاتفاقية الدولية لمكافحة الجرائم التي ترتكب عبر الأنترنت<sup>(١)</sup>، حيث شهدت العاصمة المجرية بودابست في ٢٣/١١/٢٠٠١ ولادة أول معاهدة دولية هدفها مكافحة جرائم الأنترنت، وتقوية الجهود الدولية من أجل التعاون والتضامن في محاربة هذه الجرائم والحد منها، وخاصة بعد أن أصبحت تلك الجرائم تشكل خطراً يهدد الأشخاص والممتلكات<sup>(٢)</sup>، وقد تم صياغة هذه الاتفاقية من قبل عدد كبير من الأشخاص الذين يمتلكون خبرة قانونية في مجلس أوروبا وبالتعاون مع دول أخرى وخصوصاً الولايات المتحدة الأمريكية، وبعد مشاورات عديدة بين الحكومات وأجهزة الشرطة وقطاع الكمبيوتر على مستوى العالم<sup>(٣)</sup>، وهو الأمر الذي أدى في النهاية إلى التوقيع عليها من قبل ثلاثون دولة بالتاريخ أعلاه وفي عاصمة المجر، وذلك لمواجهة الاستخدام غير المشروع للحاسبات وشبكات المعلومات فيما يعرف بالإجرام الكوني أو الإجرام المعلوماتي أو الجرائم المعلوماتية<sup>(٤)</sup>، وقد تناولت هذه المعاهدة الجرائم التي تعد أكثر انتشاراً على مستوى العالم مثل الإرهاب الإلكتروني وعمليات تزوير بطاقات الائتمان ودعارة الأطفال... الخ، وعلى أثر اتساع النغمة الدولية لمكافحة الجريمة المعلوماتية، من حيث ضرورة السعي إلى تكوين أرضية قانونية تعمل على دعم الكفاح الدولي المشترك ضد الجريمة عبر الأنترنت، وبناءً على

(١) د. هلالى عبد اللاه احمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، ص ٥ وما بعدها.

(٢) د. سليمان احمد فضل، مصدر سابق، ص ٤٢٩ .

(٣) ايمن عبدالحفيظ عبدالحميد سليمان، مصدر سابق، ص ٣٢ .

(٤) د. محمد عبيد الكعبي، مصدر سابق، ص ٧٤ .

توصية مجلس وزراء أوروبا وقراراته المختلفة حول المشاكل والحلول التي يمكن طرحها وأعداد مشروعات قوانين تيسير على هديها المجموعة الأوروبية<sup>(١)</sup>، فقد قام مجلس أوروبا<sup>(٢)</sup>، منذ ثمانينات القرن العشرين بمحاولات عدة، من أجل أعداد مشروعات عمل لمواجهة الأنشطة الإجرامية والتهديدات المحتملة كالاختراق والأنشطة الإجرامية الأخرى ذات العلاقة بالحاسوب، ومن تلك المحاولات أعداد اتفاقية تتضمن في محتواها ضرورة تسهيل التعاون الدولي في الإجراءات الجنائية في الجرائم الناشئة عن استخدام الحاسوب والأنترنت<sup>(٣)</sup>، ولقد تم توجيه الدعوة إلى الولايات المتحدة الأمريكية واليابان وكندا وجنوب أفريقيا، لكي تشارك كل منها في أعداد هذه الاتفاقية بصفة مراقب، وذلك لكون الولايات المتحدة الأمريكية تحديداً ذات علاقة ومصالحة مباشرة بموضوع الجريمة عبر الأنترنت، أما مشاركة كل من اليابان وكندا وجنوب أفريقيا في أعداد هذه الاتفاقية، هو الأمر الذي يجعل الاتفاقية صالحة لكي تمتد إلى الدول غير الأعضاء في الاتحاد الأوروبي<sup>(٤)</sup>، من حيث إمكانية الدول غير الأعضاء في الاتحاد من الدخول فيها، ومن ثم فقد سمح للدول غير الأعضاء في الاتحاد التقدم بطلب عضوية هذه الاتفاقية<sup>(٥)</sup>، ولعل من موجبات القول هنا، أن الاتفاقية قد لبثت دعوات العولمة وتضمنت ما يفيد

(١) د. عمر محمد أبو بكر بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية، مؤسسة آدم للنشر والتوزيع، الطبعة الثانية، مالطا، ٢٠٠٨، ص ١٣ .

(٢) مجلس أوروبا (COE) The council of Europe يتكون من ٤١ دولة، وقد تأسس في عام ١٩٤٩ كاتحاد Forum مضاد للأفكار الدكتاتورية التي سادت أوروبا في النصف الأول من القرن العشرين ولتقوية حركة الدفاع عن حقوق الإنسان وتطوير الحركة الديمقراطية ودور القانون في هذه الإطار، وعلى مدى سنوات عد المجلس الأوروبي الملاذ الآمن للدول الأوروبية لكل حوار يمكن ان يكون مفيداً وتتبنى عنه اتفاقيات في هذه الإطار بين الدول الأعضاء.

موقع مجلس أوروبا متاح على الأنترنت : تاريخ اخر زيارة ٢٠١٥/١٢/١٤ <http://www.COe.int>

(٣) د. علي حسن الطوالبة، مصدر سابق، ص ٩٤ .

(٤) د. عمر محمد أبو بكر بن يونس، مصدر سابق، ص ١٤ .

(٥) ينظر: نص المادة (٤٨) من اتفاقية بودابست لسنة ٢٠٠١ .

اهتمام المجتمع الدولي بموضوع الجريمة عبر الأنترنت، فهي تعبير حقيقي عن الاهتمام الدولي بهذه النوعية من الجرائم، وقد تضمنت الاتفاقية في موضوعها ثلاثة أقسام، يتناول القسم الأول منها مجموعة الجرائم التي يمكن أن تتعرض لها الأنترنت والحاسوب، ويشار هنا إلى أن مجموعة الجرائم، إنما هي نقل موسع عن الجرائم المقررة في التشريع الأمريكي أساساً<sup>(١)</sup>، ويتناول القسم الثاني من الاتفاقية مجموعة الإجراءات الجنائية التي يمكن أن تتخذ في مواجهة هذه الجرائم، كما تضمن القسم الثالث من الاتفاقية موضوع التعاون الدولي بين الدول الأعضاء الموقعين على الاتفاقية<sup>(٢)</sup>، وأن الذي يهمننا في دراستنا هو القسم الأول المتعلق بالجانب الموضوعي، أي التجريم ومدى مواكبتها للعصر، وحيث تنص المادة الخامسة من اتفاقية بودابست بشأن مكافحة الإجرام المعلوماتي على أنه: " يجب على كل طرف في الاتفاقية أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للتجريم، تبعاً لقانونه المحلي، الإعاقة الخطيرة، إذا تم ذلك عمداً، ودون حق، الوظيفة نظام الحاسب، عن طريق إدخال، أو نقل، أو اضرار، أو محو، أو تعطيل، أو إتلاف أو طمس البيانات المعلوماتية"، والمصلحة القانونية المحمية وفقاً لهذا النص، هي حماية مصلحة مستخدمي ومشغلي نظم الحاسب الآلي في الاستخدام الصحيح لها، وتم صياغة نص هذه المادة بطريقة طبيعية بحيث تشمل كافة الوظائف التي يمكن حمايتها بمقتضاه<sup>(٣)</sup>،

(١) د. عمر محمد أبو بكر بن يونس، مصدر سابق، ص ١٦ .

(٢) د. محمد عبيد الكعبي، مصدر سابق، هامش ص ٧٤ .

(٣) رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكة الأنترنت، اطروحة دكتوراه، مقدمة إلى كلية الحقوق، جامعة القاهرة، ٢٠٠٩، ص ١٦٧ . وفيما يلي نص المادة الخامسة باللغة الإنكليزية :

“ Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law , when committed intentionally , the serious hindering without right of the = =functioning of a computer system by inputting , transmitting , damaging , deleting , deteriorating , altering or suppressing computer data .

كما وتنص المادة السابعة من نفس الاتفاقية على أنه : " يجب على كل طرف من أطراف الاتفاقية أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى إنها ضرورية من أجل اعتبارها جريمة جنائية، وفقاً لقانونه الوطني، الإدخال، الأتلاف، المحو، أو الطمس العمدي، وبدون وجه حق، للبيانات المعلوماتية، الذي ينتج عنه بيانات غير صحيحة، لاستخدامها لأغراض قانونية كما لو كانت صحيحة، بصرف النظر عما إذا كانت سهل القراءة مباشرة وواضحة أم لا، ويمكن لأي طرف أن يشترط في قانونه الداخلي نية الغش أو نية إجرامية مشابهة من أجل تقرير المسؤولية الجنائية "، ويلاحظ أن المصلحة المشمولة بالحماية القانونية وفقاً لهذا النص هي الأمن والثقة في البيانات المخزنة في الحاسب الآلي، والتي يمكن أن تؤثر على العلاقات القانونية<sup>(١)</sup>، وتتضمن هيكلية المشروع النهائي للاتفاقية<sup>(٢)</sup>، ثلاثة اتجاهات كسياسة عامة للاتفاقية وهذه الاتجاهات تتمثل في (أولاً) لزوم أن تكون الاتفاقية مرتكزاً تلتقي عنده حركة التشريع في كل دولة عضو في الاتحاد، فضلاً عن الدول الأربعة المشاركة وفقاً للمادة (١/٣٦) من الاتفاقية، مع مراعاة ما تقرره المادة (٤٨) التي سمحت لغير الدول المشار إليها في الانضمام إلى الاتفاقية، طالما قبلت بما تتضمنه من شروط تتعلق بها، حيث عملت الاتفاقية على تحديد ملتقى مركزي لأنواع الجرائم التي يجب أن تكون متضمنة في التشريعات الوطنية للدول الأعضاء<sup>(٣)</sup>، وكما يأتي :

١- الجرائم المتعلقة بأمن الشبكات، كما هو الشأن في الدخول والمراقبة غير المشروعة، العدوان على الثقة في البيانات أو على النظام أو الإساءة إليه،

(١) رشدي محمد علي محمد عيد علي، مصدر سابق، ص ٢٧٠ .

(2) EXPLANATORY Report , adopted 8 NOV .2001 committee of Ministers of the council of Europe / 10th session (8 NOV. 2001) , available online in NOV.2001 at :

<http://convention . coe .int / treaty /EN/ projets / final cvber Rapex , htm .>

(3) Explanatory Report Eu conv . p7 (sec .1. Art -13) established a common minimum standard of relevant offence .

وموضوع الإساءة هنا يتضمن بيع كلمات المرور أو شفرة الدخول بقصد ارتكاب جرائم<sup>(١)</sup>.

٢- الجرائم المعلوماتية، كما هو الشأن في الاختلاق والانتحال والنصب والاحتتيال المعلوماتي، وكذلك القيام بالتدخل أو الإضافة أو تعطيل حركة استدعاء المعلومة<sup>(٢)</sup>.

٣- جرائم الأخلاق وذلك مثل إنتاج وبيع وحيازة ما يتعلق بدعارة الأطفال<sup>(٣)</sup>.

٤- جرائم العدوان على حقوق الملكية الأدبية والفكرية والحقوق المجاورة، مثل جرائم استنساخ المصنفات المشمولة بالحماية<sup>(٤)</sup>.

٥- جرائم ضد الجنس البشري، وذلك مثل العنصرية والعرقية عبر الأنترنت<sup>(٥)</sup>.

وعلى الرغم من أن القاعدة الموضوعية الجنائية تتعلق بالجرائم التي يتم فيها استخدام تكنولوجيا المعلومات، فإن الاتفاقية تستخدم لغة التكنولوجيا المحايدة، لذا فإن القاعدة الموضوعية الجنائية يمكن أن يتم تطبيقها على كل من التكنولوجيا الحالية والمستقبلية على السواء<sup>(٦)</sup>، كما وقد اضيفت مادة جديدة إلى نص المشروع النهائي للاتفاقية، وهي المادة (١٥) التي نصت على التزام الدول الأعضاء بمراعاة حقوق

(١) ينظر: المادتين (٣،٢) من الاتفاقية .

(٢) ينظر: المادتين (٨،٧) من الاتفاقية .

(٣) ينظر: المادة (٩) من الاتفاقية .

(٤) ينظر: المادة (١٠) من الاتفاقية .

(٥) وقد تم اضافتها إلى الاتفاقية بموجب بروتوكول خاص في هذا الإطار .

(٦) د. هلالى عبد اللاه احمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مصدر سابق، ص ٣٨،

وهذا هو النص باللغة الإنكليزية: Although the substantive law provision relate to: offences using information technology , the convention uses technology – neutral language so that the substantive criminal law offences maybe applied to both current and future technologies involved .

الإنسان وحرياته الأساسية التي تضمنتها الاتفاقيات الدولية والتشريعات الوطنية، والالتزام كذلك بعدم انتهاكها<sup>(١)</sup>، ومن النقاط الهامة التي ركزت عليها المذكرة التفسيرية أيضاً، ضرورة أن يكون ارتكاب الجرائم المحصاة في هذه الاتفاقية " دون حق " ويتجلى ذلك في قولها : يشترط في تجريم الأفعال المذكورة في هذه الاتفاقية أن يكون القيام بالفعل " دون حق san droit "<sup>(٢)</sup>، وهذا المصطلح يأخذ في الاعتبار أن السلوك قد لا يعاقب عليه دائماً في حد ذاته، إذ يمكن أن يكون سلوكاً شرعياً أو مبرراً ليس فقط عن طريق الاستثناءات القانونية التقليدية مثال ذلك الرضاء، والدفاع الشرعي، وحالة الضرورة<sup>(٣)</sup>.

ويتضح لنا مما تقدم أن الجرائم المعلوماتية ومنها الجرائم ضد المعلومات المنصوص عليها في الاتفاقية أعلاه، يشترط لارتكابها أن ترتكب عن عمد، وبالتالي فلا يوجد أي مجال هنا لارتكاب إحدى هذه الجرائم بطريقة غير عمدية، كما أنه يشترط في بعض هذه الجرائم وجود قصد جنائي خاص فضلاً عن القصد الجنائي العام، مفادها أن البعض من هذه الجرائم لم تكتفي بالقصد الجنائي العام لوحده، بل لابد من توافر القصد الجنائي الخاص .

## المطلب الثاني

### المعالجة التشريعية للجرائم المعلوماتية على المستوى الوطني

نتناول في هذا المقام موقف التشريع من تجريم الجرائم المعلوماتية سواء في الدول الأجنبية أو في الدول العربية، وسنتكلم عن موقف التشريعات الأجنبية من الجريمة المعلوماتية في الفرع الأول، ثم نبحث في موقف التشريعات العربية من الجريمة المعلوماتية في الفرع الثاني، وعلى النحو التالي :

(١) ينظر: نص المادة (١٥) من الاتفاقية .

(٢) ويقابل ذلك في المصطلح الإنكليزي " without right " .

(٣) د. هلالى عبد اللاه احمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مصدر سابق، ص ٣٩.



## الفرع الاول: موقف الدول الأجنبية من الجرائم المعلوماتية

ولكل ما سبق ذكره من أسباب مجتمعة ليس غريباً أن يصف المفكر الإنكليزي الشهير انتوني جيندنز (Anthony Giddens)<sup>(١)</sup>، العالم الذي نعيش فيه بأنه عالم منفلت (Runaway world)، لا يمكنه الإمساك بعصمته أو إخضاعه للسيطرة، وأن يصدر كتاباً يحمل هذه التسمية<sup>(٢)</sup>، وربما شمل هذا الانفلات كافة نواحي الحياة، بما فيها الانفلات الديني والأخلاقي والاجتماعي والاقتصادي والسياسي، وقد يعطي ذلك تفسيراً مقنعاً لما نراه اليوم من النمو المتزايد والمطرود للجرائم المعلوماتية، والتي من أجلها حرص مجلس أوروبا على صياغة الاتفاقية التي سبق ذكرها، لمكافحتها والتغلب عليها، كما حرصت بعض الدول على أن تضمن تشريعاتها هذه الجرائم، أما عن طريق النص عليها استقلالاً في تشريعات مستقلة<sup>(٣)</sup>، وأما عن طريق تحديث قوانينها وإدماجها في هذه القوانين<sup>(٤)</sup>، وتعد دولة السويد من الدول السبّاقة في مجال اصدار تشريعات

(١) هو استاذ علم الاجتماع بجامعة كمبردج، ويعد من اشهر علماء هذا التخصص الذين ذاعت شهرتهم، لا لكثرة مؤلفاتهم فقط، بل لما يقدموه من اسهامات نظرية ومنهجية، كتب ما يزيد على مائتي مقال، ما بين مقال بحثي أو مراجعة كتب أو مقال صحفي، اما قائمة الكتب التي كتبها فتضم (٣٦) كتاباً من بينها كتاب " عالم منفلت : كيف تشكل العولمة حياتنا، سنة ١٩٩٩ والذي تم ترجمته إلى العربية .

(2) Giddens (Anthony) : " Runaway world : How Globali Zationis reshaping our lives " , London, Profile books , 1999 .

(٣) ومثال ذلك قانون اساءة استخدام الحاسب في المملكة المتحدة الصادر في ٢٩ يونيو سنة ١٩٩٠، والذي طبق اعتباراً من ٢٩ اغسطس سنة ١٩٩١ .

(٤) ومن ابرز هذه التشريعات قانون العقوبات الفرنسي الجديد الصادر في سنة ١٩٩٢، والمعمول به منذ اول مارس سنة ١٩٩٤، والذي اضاف فصلاً ثالثاً للباب الثاني من القسم الثالث من قانون العقوبات تحت عنوان: " انتهاكات نظم المعالجة الآلية للبيانات "، وسمي هذا القانون بقانون = Godfrain ، وذلك تيمناً باسم النائب الفرنسي (Jacques Godfrain) الذي تقدم به امام المجلس النيابي، ويتكون هذا الفصل من المواد (١/٣٢٣) إلى (٧/٣٢٣) . ينظر: د. محمد عبيد الكعبي، مصدر سابق، هامش ص ٧٠ .

قانونية جديدة ومستقلة خاصة بجرائم الأنترنت والحاسب الآلي، لكي تستطيع متابعة ومعاينة المتهمين بارتكاب الجرائم الإلكترونية، وقد صدر أول قانون خاص بها سمي بقانون البيانات وذلك في عام ١٩٧٣، وقد عالج هذا القانون قضايا الاحتيال عن طريق الأنترنت، وكذلك كان من بين فقرات نصوصه تجريم الدخول غير المشروع على البيانات الإلكترونية أو تزوير المعلومات الإلكترونية، أو تحويلها أو الحصول غير المشروع عليه<sup>(١)</sup>، وكذلك تعد الولايات المتحدة الأمريكية الدولة التالية بعد السويد، من حيث إصدار قوانين خاصة بها ومستقلة، والتي تجرم الجرائم الإلكترونية، إذ أنها شرعت قانوناً مستقلاً لحماية أنظمة الحاسب الآلي (١٩٦٧-١٩٨٥) وفي سنة ١٩٨٥، حدد معهد العدالة القومي الأمريكي، خمسة أنواع رئيسية للجرائم المعلوماتية<sup>(٢)</sup>، وهي :

- ١- جرائم الحاسب الآلي الداخلية . ٢- جرائم الاستخدام غير المشروع عن بعد .
- ٣- جرائم التلاعب بالحاسب الآلي . ٤- دعم التعاملات الإجرامية .
- ٥- سرقة البرامج الجاهزة والمكونات المادية للحاسب .

وفي سنة ١٩٨٨ ثمة قانونين متخصصين بالجرائم المعلوماتية، تم إصدارهما، هما قانون الغش والتعسف في الكمبيوتر، أما القانون الثاني فهو قانون سرية الاتصالات الإلكترونية الخاصة، أو التصنت عليها بشكل غير مرخص به<sup>(٣)</sup>، وفي سنة ١٩٩٦ صدر قانون الاتصالات، الذي تضمن نصوصاً خاصة بقانون آداب الاتصالات، وتناول تقييد حرية الاطلاع على الصور والمواد المخلة بالآداب العامة المنتشرة على شبكة الأنترنت<sup>(٤)</sup>، وفي سنة ١٩٩٧ أصدرت المحكمة العليا الأمريكية

(١) د. سليمان احمد فضل، مصدر سابق، ص ٤٣٣ .

(2) Scott Charney And Kent Alexander , COMPUTER CRIME , 1996 , Vol.45, 45 Emory L.J, p.949 .

(٣) د. طوني ميشال عيسى، التنظيم القانوني لشبكة الأنترنت، دار صادر، لبنان، ٢٠٠١، ص ١٩١ .

(١) د. محمد عبيد الكعبي، مصدر سابق، ص ٧١ .

حكماً بعدم دستورية البعض من نصوص قانون آداب الاتصالات<sup>(١)</sup>، وهذا القانون وإن كان قد أثار ضجة وردود أفعال رافضة له، على اعتبار أنه يتعرض لحرية التعبير، إلا أنه قد عكس تصوراً واضحاً وملموساً باتجاه إيجاد حلول تقنية لمواجهة مخاطر التكنولوجيات الحديثة في الاتصال عن بعد، وخاصة البث الرقمي<sup>(٢)</sup>، وكذلك أصدر الرئيس الأمريكي بيل كلينتون في ٢٨ أكتوبر ١٩٩٨ قانوناً سمي بـ (The Digital Millennium Copyright Act) ومما تجدر الإشارة إليه، هو أن المشرع الأمريكي لم يقف عند هذا الحد، بل أن الولايات المتحدة الأمريكية هي أول دولة في العالم أهتمت بتوفير التدريب اللازم لمكافحة الجرائم المعلوماتية، والتحقق فيها من خلال الدورات المتخصصة، التي تعقدتها أكاديمية التحقيقات الفيدرالية في بعض الولايات مثل فرجينيا، لتدريب محققي الشركة والعاملين في إدارة العدالة الجنائية، وذلك كله من أجل رفع كفاءة القائمين على هذه الأعمال، وذلك لسهولة الكشف عن الجرائم المستحدثة والضرب على أيدي مرتكبيها<sup>(٣)</sup>، ولا بد من الإشارة إلى أن الولايات المتحدة الأمريكية قد قامت بتغطية واجباتها التشريعية، وكملت بنيتها التشريعية مع نهاية القرن العشرين فيما يخص التشريعات التي تحكم التعاملات الإلكترونية وتتصدى الجريمة المعلوماتية، سواء في تشريعاتها المحلية على مستوى الولايات، أو الاتحادية على مستوى الدولة الفيدرالية، وأن أكثر هذه التشريعات حداثة هو قانون التوقيع الإلكتروني الصادر عام ٢٠٠٠<sup>(٤)</sup>.

(٢) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والأترنت، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ٢٥.

(٣) د. طوني ميشال عيسى، مصدر سابق، ص ٢٣٤.

(٤) د. هشام فريد محمد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مصدر سابق، ص ٤٨.

(١) عادل يوسف عبدالنبي الشكري، الجريمة المعلوماتية وازمة الشرعية الجزائية، بحث منشور، مجلة كلية القانون، جامعة الكوفة، العدد السابع، ٢٠٠٨، ص ١٢٥.

## الفرع الثاني: موقف الدول العربية من الجرائم المعلوماتية

عندما نبحث عن النصوص والتشريعات العربية عموماً تجاه الجرائم المعلوماتية، نجد أنه هناك فراغ تشريعي كبير، حيث أن الغالبية من الدول العربية تفتقر إلى قانون لتجريم الجرائم المعلوماتية، ولكن في ذات الوقت هناك دول عربية قد تصدت لهذه الظاهرة بقوانين مستقلة، وما يلفت النظر هو أن نشير هنا إلى القانون العربي النموذجي<sup>(١)</sup>، وقد تم إقرار هذا القانون في صورته النهائية في عدد (٢٧) مادة، حيث تناولت المادة (٦) منه جريمة تعطيل أو إتلاف البيانات، وكذلك تناولت المواد (٢٤) - (٢٧) منه الإجراءات المتعلقة بالجرائم المعلوماتية وهي تعد بمثابة خطوة إيجابية للموقف العربي من أجل خدمة الدول العربية في السير نحو خطى فعلية لسن وإصدار التشريعات في مكافحة الجرائم المعلوماتية ومواكبة التطورات الدولية والإقليمية في مجال المعلوماتية وسد الفراغ التشريعي، وقد كانت المملكة العربية السعودية سباقة في التصدي للثورة المعلوماتية، وأصدرت تشريعاً خاصاً بذلك، إذ سبقت المملكة العربية السعودية نظيراتها من الدول العربية في إصدار قانون جديد لمواجهة الجرائم المعلوماتية، فقد وافق مجلس الوزراء في المملكة في ١٤٢٨/٣/٨ هـ الموافق ٢٠٠٧/٣/٢٧ م على نظامي مكافحة الجرائم المعلوماتية والتعاملات الإلكترونية<sup>(٢)</sup>، وكان ذلك للحد من وقوع الجرائم الإلكترونية وتحدد الجرائم المستهدفة للنظام والعقوبات المقدره لكل جريمة، وهدف هذا النظام قد تم تحديده من خلال المادة الثانية منه: "يهدف هذا النظام إلى ضبط التعاملات والتوقيعات الإلكترونية، وتنظيمها وتوفير إطار

(٢) القانون العربي النموذجي في شأن مكافحة جرائم الكمبيوتر والأنترنيت، الذي تم اقراره في سنة ٢٠٠٣، بوصفه منهجاً استرشادياً يلزم به المشرع الوطني عند اعداد تشريع في الجرائم المعلوماتية.

(٣) د. شيماء عبدالغني محمد عطاالله، مكافحة جرائم المعلوماتية في المملكة العربية السعودية، بحث منشور، متاح على الموقع الإلكتروني الشخصي للدكتورة شيماء :

. ٢٠١٥/١٢/٢٠، تاريخ آخر زيارة Faxulty .Ksu .cdu.sa/Shaimaaatalla

نظامي لها بما يؤدي إلى تحقيق ...<sup>(١)</sup>، وجاءت المواد (٣-١٠) لتحديد أنواع الجرائم المعلوماتية والعقوبة المقررة لها<sup>(٢)</sup>، كما ونصت المواد المتبقية على جرائم الدخول غير المشروع لإلغاء البيانات أو حذفها وإيقاف الشبكة أو تعطيلها أو إعاقة الوصول إلى الخدمة أو تشويشها، وكذلك إنشاء المواقع للإتجار بالجنس البشري وإنشاء المواد أو البيانات الإباحية، وأيضاً يعاقب القانون على إنشاء مواقع لمنظمات إرهابية أو الإتجار بالمخدرات<sup>(٣)</sup>.

أما دولة الإمارات فهي الأخرى أيضاً تصدت للجرائم المعلوماتية بسنها تشريع خاص في شأن مكافحة جرائم تقنية المعلومات، وفي خلال عقد من الزمن عالج المشرع الإماراتي الثورة المعلوماتية بقانونين، حيث أصدر مرسوماً بقانون اتحادي رقم (٥) لسنة ٢٠١٢ فيما يخص مكافحة جرائم تقنية المعلومات، وقد تضمن تعديلات لما ورد في القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ فيما يخص مكافحة جرائم تقنية المعلومات، والذي تم الغاؤه بموجب المرسوم بقانون الذي تم نشره بالجريدة الرسمية، وهو موقف يحمي المشرع الإماراتي، ويعد دافعاً معنوياً للتشريعات العربية للاقتداء به والسير على خطاه وانتهاج نهجه وسد الفراغ التشريعي فيما يخص الجرائم

(١) لمزيد من التفصيل ينظر: تكملة نص المادة (٢) من قانون مكافحة جرائم المعلوماتية السعودي ٢٠٠٧.

(٢) مثلاً تنص المادة (٣) من قانون مكافحة جرائم المعلوماتية السعودي ٢٠٠٧ على انه: " يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة الف ريال، أو احدى هاتين العقوبتين كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو احد اجهزة الحاسب الآلي دون مسوغ نظامي صحيح أو التقاطه أو اعتراضه، والدخول غير المشروع لتهديد شخص أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً، والمساس بالحياة الخاصة عن طريق اساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها، والتشهير بالآخرين والحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة " .

(٣) د. عماد مجدي عبدالملك، مصدر سابق، ص ١٨٤ .

المعلوماتية، وقد تضمن القانون أعلاه العديد من المواد التي من شأنها توفير الحماية القانونية والجنائية لخصوصية ما يتم نشره وتداوله على الشبكة المعلوماتية، من معلومات وبيانات وأرقام تتعلق بالبطاقات الائتمانية، وأرقام بيانات الحسابات المصرفية، أو أية وسيلة من وسائل الدفع الإلكتروني، وكذلك كل استخدام لأي من وسائل تقنية المعلومات في تزوير أو تقليد أو نسخ للبطاقات الائتمانية أو البطاقات المدنية، كما يعاقب بموجب المرسوم بقانون كل من أبتز أو هدد شخصاً آخر لحمله على القيام بفعل أو الامتناع عنه، وذلك باستخدام شبكة معلوماتية أو وسيلة تقنية ...، وكذلك كل من أنشأ أو أدار موقعا إلكترونياً أو أشرف عليه ...، وذلك لجماعة إرهابية أو أي مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة، ...<sup>(١)</sup>.

ولا بد من الوقوف عند المشرع المصري ومدى مواكبته للتطورات الحاصلة في شأن تقنية المعلومات وما يترتب عليها من آثار سلبية متمثلة بالجرائم العديدة التي ترتكب باستخدام الوسائل التقنية الحديثة، فتبين لنا عدم وجود قانون خاص بشأن تجريم الجرائم المعلوماتية في مصر، كما إن قانون العقوبات المصري هو الآخر لم ينص على الجرائم المعلوماتية، ولا يتناول موضوعها في أي مادة من مواده العديدة، سوى أن هناك قانون الأحوال المدنية<sup>(٢)</sup>، الذي نص في بعض نصوصه على النظام المعلوماتي والجرائم المتصلة بها، ومن خلال اطلاعنا على بعض نصوص هذا القانون وجدنا أنها لا تتناول مكافحة الجرائم المعلوماتية، فعلى سبيل المثال، تنص المادة (٧٢) منه على أنه: " في تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز الأحوال المدنية ومحطات الإصدار الخاصة بها..."، وكذلك المادة (٧٥) تنص على أنه: " يعاقب بالحبس ... كل من عطل أو

(١) ولمزيد من التفصيل ينظر: نصوص مواد القانون الاتحادي لدولة الإمارات العربية لمكافحة جرائم تقنية المعلومات رقم (٥) لسنة ٢٠١٢ .

(٢) قانون الأحوال المدنية المصري رقم ١٤٣ لسنة ١٩٩٤ .

أُتلف الشبكة الناقلة لمعلومات الأحوال المدنية أو جزء منها ... "، ومواد أخرى<sup>(١)</sup>، وهذه المواد التي تناولت موضوع الجرائم المتصلة بالنظام المعلوماتي، وهي نصوص خاصة بالأحوال المدنية فقط، ولا تسري على غيرها من الجرائم، ويمكننا القول بأن الوضع في مصر لا يحمي عقاباً بشأن الجرائم المعلوماتية، علماً بأن هذه النوعية من الجرائم في تزايد مستمر، ومن ناحية أخرى القوانين ثابتة ولا تتغير، وأنه يتحتم على المشرع المصري أن يسن تشريع خاص بالجرائم المعلوماتية، وأن يعدل القوانين الحالية لكي تواكب هذه الجرائم، وفي نهاية المواقف التشريعية العربية: نتناول موقف المشرع العراقي ومدى تصديه للجريمة المعلوماتية لمواكبة التطور الحاصل بشأن الإجراء المعلوماتي، فأنا وجدنا خلو الساحة العراقية من أي قانون يكافح الجريمة المعلوماتية، إلا أننا عثرنا على مشروع مسودة قانون خاص لمكافحة جرائم المعلوماتية في التشريع العراقي مقدم إلى مجلس النواب العراقي منذ سنة ٢٠١٢<sup>(٢)</sup>، وإلى حد أعداد هذه الاطروحة المشروع لم يصدر، وحسب تقديري بأن للمشروع مبررات عدم الإصدار، منها هناك قوانين<sup>(٣)</sup>، تستوجب التعديل، وهناك إجراءات يجب أن تتخذ، وهناك أمور تحتاج إلى تنظيم، ولذلك فأنا أوردنا ما يلي فيما يخص المشروع :

١- إن الجرائم المعلوماتية جرائم حديثة العهد، ومتطورة في أسلوب ارتكابها ومصطلحاتها غير مألوفة في القوانين العقابية العراقية، والمجتمع العراقي لم يألّف هذه السلوكيات من قبل .

٢- الجرائم المعلوماتية تحتاج إلى مراجعة في نصوص قانون أصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١ المعدل .

(١) المواد (٧٥،٧٤،٧٢) من قانون الأحوال المدنية المصري رقم ١٤٣ لسنة ١٩٩٤ .

(٢) مشروع مكافحة الجرائم المعلوماتية في التشريع العراقي لسنة ٢٠١٢ . متاح على الموقع الإلكتروني : <http://www.Iraqja.iq/view.1645> ، تاريخ اخر زيارة ٢٠/١٢/٢٠١٥ .

(٣) مثل قانون اصول المحاكمات الجزائية العراقي رقم (٢٣) لسنة ١٩٧١ المعدل .

٣- إذا كان هناك ثمة اتجاه جدي في تشريع هذا القانون، لا بد من إعادة النظر في العقوبات المنصوص عليها في مشروع قانون الجرائم المعلوماتية الموضوع على طاولة مجلس النواب العراقي لكونه مبالغ في البعض منها .

٤- يجب أن تكون هناك توعية قانونية بمخاطر الأنترنت ومخاطر استخدامه، خصوصاً من قبل الأحداث، فضلاً عن التوعية الإعلامية، بعد الاجتياح الكبير لثورة المعلوماتية ومخاطرها .

٥- يرجى البدء بخطوات عملية جدية تضمن حسن سير وتطبيق هذا القانون، ومنها تنظيم عمل مكاتب الأنترنت، وشركات الاتصال المسؤولة عن توفيرها .

٦- ضرورة الإسراع في تشريع هذا القانون من قبل مجلس النواب، مع عدم المساس بالحريات الشخصية، وعلى شرط أن ينسجم القانون مع الدستور .

إلا أنه وفي جزء من العراق وهو إقليم كردستان العراق والذي يتمتع بسلطات دستورية<sup>(١)</sup> ومنها سلطة إصدار القوانين، بالشكل الذي لا يتناقض مع الدستور العراقي، فقد بادر المشرع الكوردستاني إلى إصدار قانون فيما يخص الإجرام المعلوماتي<sup>(٢)</sup>، حيث تنص المادة الثانية من هذا القانون على أنه : " يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن مليون دينار ولا تزيد على خمسة ملايين دينار أو بإحدى هاتين العقوبتين كل من أساء استعمال الهاتف الخليوي أو أية أجهزة اتصال سلكية أو لاسلكية أو الأنترنت أو البريد الإلكتروني وذلك عن طريق التهديد أو القذف أو السب أو نشر أخبار مختلقة... "، وكذلك تنص المادة

(١) مشروع دستور إقليم كردستان العراق لسنة ٢٠٠٦، حيث نصت الفقرة (أولاً) من المادة (٤) منه: " الشعب مصدر السلطات و أساس شرعيتها، ويمارسها عبر مؤسساته الدستورية، ولدستور اقليم كردستان وقوانينه السيادة والسمو على كافة القوانين الصادرة من الحكومة العراقية خارج الاختصاصات الحصرية للحكومة الاتحادية، المنصوص عليها في المادة (١١٠) من دستور جمهورية العراق الاتحادية " .

(٢) قانون منع اساءة استعمال اجهزة الاتصالات رقم (٦) لسنة ٢٠٠٨ .



الثالثة من نفس القانون على أنه : " يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن سبعمائة وخمسون الف دينار ولا تزيد على ثلاثة ملايين دينار أو بإحدى هاتين العقوبتين كل من تسبب عمداً باستخدام واستغلال الهاتف الخليوي أو أية أجهزة اتصال سلكية أو لاسلكية أو الأنترنت أو البريد الإلكتروني في إزعاج غيره في غير الحالات الواردة في المادة الثانية من هذا القانون "، ونحن لسنا بصدد إبداء الملاحظات على هذا القانون، إلا أنه هناك ثمة عوارض عملية تحول دون تطبيق هذا القانون في العديد من الحالات، وذلك لكون شركات الاتصالات تطرح بعضاً من شرائحها للبيع مقابل سعر ضئيل لا يتجاوز ثلاثة آلاف دينار دون مطالبة الحائز أو المشتري بأية مستمسكات رسمية تعريفية، ودون تسجيل الشريحة، ونحن نعلم أن مسألة الأثبات في الجرائم المعلوماتية معقدة وصعبة للغاية، وبهذا العمل يرتكبون الجناة جرائمهم بواسطة هذه الشرائح دون عقاب يذكر، ولكن على الرغم من ذلك فإن إصدار هذا القانون يعد خطوة إيجابية على مواكبة التطور الحاصل على مستوى الجرائم المعلوماتية وآلية التصدي لها، كما إنها تدفع بالعراق إلى مصاف الدول التي عالجت مشكلة الفراغ التشريعي، وإننا نطمح من المشرع الكوردستاني المزيد من التشريعات المكافحة لجرائم التقنية المعلوماتية، التي في تطور وزيادة مستمرة يوماً بعد يوم، وفي نفس الوقت لنا مأخذ على المشرع الكوردستاني بخصوص هذا القانون، حيث كان بإمكانه ان يستغل الفرصة ويرصد كافة الجرائم المعلوماتية في هذا القانون، وعلى وجه الخصوص الجرائم المعلوماتية الخطيرة، ومنها على سبيل المثال ارتكاب الأعمال الإرهابية عبر الوسائل التقنية الحديثة، أو ما يسمى بالإرهاب الإلكتروني حالياً، وأخيراً فأننا لاحظنا، أن الوضع فيما يخص الدول العربية قليلة الاهتمام بهذا النوع من الجرائم وطرق التصدي لها، الأمر الذي نرى ضرورة تدخل المشرع في هذه الدول بتشريع قوانين لمواجهة الجرائم الناجمة عن الاستخدام غير المشروع لشبكة الأنترنت، وخاصة إذا ما عرفنا أن القواعد التقليدية لا تستطيع الوقوف أمام هذه الجرائم ومعالجتها، وإن انطبقت في بعض الأحيان بعض النصوص عليها، إلا أنها لا تعد سوى أحكام

استثنائية، وأعمالاً لمبدأ الشرعية، ويعيداً عن اللجوء إلى القياس والذي يتعارض مع مبدأ الشرعية، يستوجب على المشرع التدخل وبسرعة بنصوص تشريعية لمواجهة هذه الجرائم، وكذلك مما تجدر الإشارة إليه حول الأخذ بمصطلح الجريمة المعلوماتية، بحسب ورود تسميات ومصطلحات أخرى مثال جرائم الأنترنت، أو جرائم شبكة المعلوماتية، إلا أننا نرى بأن الأخذ والاستقرار عند مصطلح الجريمة المعلوماتية يعد الأفضل والأدق من بين المصطلحات التي أثرت، وذلك لما تتميز به هذه الجريمة من خصائص لذاتها لعل أهمها أنها ترد على محل ذات طبيعة خاصة، الأمر الذي يستوجب أن تعامل هذه الجرائم وفق قواعد لا ينبغي للجرائم الأخرى أن تعامل بموجبها، وعلى وجه الخصوص الجرائم التقليدية، والتي يتضمنها قانون العقوبات، والتي تختلف عنها ليس في جانب المحل، الأمر الذي ينعكس على طبيعتها، بل وفي القواعد والأصول الجنائية التي ينبغي تطبيقها .

## الخاتمة

بعد ان انتهينا من كتابة هذا البحث المتواضع بعونه تعالى توصلنا إلى مجموعة من الاستنتاجات والتوصيات نوردته على الشكل التالي :

### أولاً : الاستنتاجات :

- ١- الجريمة ظاهرة اجتماعية معقدة جداً، والتصدي لها أو الحد من ارتكابها، مسؤولية تقع على عاتق المجتمع بكافة قطاعاته وشرائحه، ومنها القطاع الخاص بالتجريم، اما الاقتصار على معالجتها عن طريق الجزاء الجنائي، فهو يعد نوع من القصور أو الفشل أو على الأقل هروب من معالجة الأسباب الحقيقية للجرائم، وقد اثبتت التجارب على ان اغلب الجرائم تنشأ في اوضاع اقتصادية أو اجتماعية غير سوية، ومن ثم فان معالجة هذه الأوضاع، والعمل على تصحيح مسارها يجزّد الجريمة من أسبابها، ويغني بالتالي من استخدام الخيار الجنائي .
- ٢- جرائم الأنترنت لا تقتصر على دولة معينة، وانما تتخذ العالم كله مسرحاً لها، ولذلك فإن عولمة الجريمة بهذا المعنى تقتضي عولمة المواجهة التشريعية، حيث لم تعد السلطات القضائية في بلد ما قادره بمفردها على التصدي لهذا الجرائم دون مساندة أو مشاركة غيرها من السلطات في الدول الأخرى ومن هنا يظهر دور التعاون الدولي من اجل مكافحة تلك الجرائم، ومن اهم المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، معاهدة بودابست لمكافحة جرائم الأنترنت، وتوصيات المجلس الأوربي المتعلقة بتكنولوجيا المعلومات .
- ٣- إن التطور التكنولوجي الذي صاحب ثورة الحاسب الآلي وتطبيقاته قد انعكس على وسائل الاتصالات الحديثة، سواء تم ذلك عن طريق الهواتف العادية أو المحمولة عن طريق الأقمار الصناعية، أو عن طريق شبكات الأنترنت، ومما لا شك فيه ان استعمال وسائل التكنولوجيا الحديثة، على الرغم من جانبه الإيجابي

المشرق المضيء في حياة البشر جميعاً، إلا أن الأمر لا يخلو من خطر يرجع سببه إلى قيام البعض بإساءة استعمال وسائل التكنولوجيا الحديثة وهذا هو الجانب السلبي من السلوك، والذي قد يتضمن الإساءة إلى وسائل التكنولوجيا الحديثة ذاتها، وبعض الجوانب السلبية الأخرى، قد يمثل في الإساءة للغير، سواء أفراد ام جماعات ام مؤسسات، وهي جرائم كثيرة لا مجال لحصرها .

- ٤- لم نعثر على تعريف جامع مانع للجريمة المعلوماتية، إلا أنه وجدنا من يرى ان المعيار المزدوج (موضوع الجريمة واداة ارتكابها) هو المعيار الأفضل لتعريفها، كما ان ما تتميز به الجرائم المعلوماتية من خصائص متميزة، وتنفرد بها على سائر خصائص الجرائم الأخرى، وذلك لكونها جرائم عابرة للحدود، وصعبة الأثبات والاكتشاف، وجرائم ناعمة وترد على محال غير مادية، مما فرض على المشرعين في مختلف الدول عند وضع النصوص التشريعية، اخذاً بنظر الاعتبار، وكذلك فإن هذه الخصائص تظهر قصور النصوص الجنائية التقليدية عن مواجهتها .
- ٥- المجرم المعلوماتي يمتاز بخصائص وسمات ينفرد بها بعيداً عن المجرم التقليدي، مثل الذكاء والمهارة والخبرة والسلطة والمعرفة والتكيف الاجتماعي، وغير عنيف ولا يكثرث بالمسؤولية الجنائية عن أفعاله كما يختلف في تصنيفاته ودوافع واهداف ارتكابه الجريمة .

### ثانياً : التوصيات :

- ١- ينبغي في حالة قيام المشرع بسن تشريع جنائي خاص لمواجهة الأنشطة غير المشروعة، والتي ترد على المعلوماتية، ان ينظر إلى المعلومات ويعاملها معاملة المال على اعتبار أنها مالاً معنوياً مساوياً في الأهمية للمال المادي، ويوفر لها الحماية الجنائية الموضوعية من الاعتداء عليها، مع مراعاة عدم تعارض هذه الحماية مع ما يكفل حرية تدفق المعلومات والحصول عليها .
- ٢- التخطيط الجيد والسليم لنشر ثقافة المعلوماتية واستخدام الحاسب الآلي وتطبيقاته وكذلك شبكة الأنترنت ينبغي خضوعه لجهة حكومية عليا، ذات اختصاصات

- وصلاحيات وسلطات، وان تضم في عضويتها كل القائمين على هذا الأمر، ويهمهم نشر هذه الثقافة تمهيداً لتحويلها إلى واقع علمي .
- ٣- ندعو المشرع العراقي إلى الاسراع في سن قانون خاص بجرائم تقنية المعلومات، وذلك لما له من تأثير في تقليل الاستخدام السيء للوسائل التقنية بشكل عام، ومنها ارتكاب جرائم المعلوماتية على وجه الخصوص، ناهيك عن العديد من الجرائم الاخرى الخطيرة التي تتخذ من تقنية وسائل الاتصالات سبيلاً لارتكابها جرائم مختلفة، لا سيما ان هذه الجرائم تحمل سمات تستوجب معالجة خاصة من حيث التجريم .
- ٤- خلق وتأسيس الآليات والأجهزة الأمنية الدولية للرقابة والأشراف على استخدامات التقنية الحديثة في الاتصالات والمعلومات في مكافحة الجرائم التي تقع في هذا الإطار، وضبط وتتبع المجرمين في اي مكان من العالم وتقديمهم للعدالة بهدف استقرار العلاقات الدولية وتحقيق السلم والأمن الدوليين .

## قائمة المصادر

أولاً: الكتب :

- ١- أسامة احمد المناعسة و جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، ٢٠١٤ .
- ٢- جميل عبدالباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الطبعة الأولى، دار النهضة العربية، القاهرة، ١٩٩٢ .
- ٣- د. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩ .
- ٤- د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١١ .
- ٥- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، ٢٠١٣ .
- ٦- د. سامي جلال فقي حسين، التنقيش في الجرائم المعلوماتية، دار الكتب القانونية، الإسكندرية، ٢٠١١ .
- ٧- د. سليمان احمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، ٢٠١٣ .
- ٨- شمسان ناجي صالح الخيلي، الجرائم المستخدمة بطرق غير مشروعة لشبكة الأنترنت، دار النهضة العربية، القاهرة، ٢٠٠٩ .
- ٩- د. شيماء عبدالغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٧ .
- ١٠- د. طارق ابراهيم الدسوقي عطية، عولمة الجريمة، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠ .

- ١١- د. طوني ميشال عيسى، التنظيم القانوني لشبكة الأنترنت، دار صادر، لبنان، ٢٠٠١ .
- ١٢- د. عبدالصبور عبد القوي علي مصري، المحكمة الرقمية والجريمة المعلوماتية، الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، ٢٠١٢ .
- ١٣- د. عبدالفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٨ .
- ١٤- د. عبدالفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٩ .
- ١٥- د. علي حسن الطوالبه، الجرائم الإلكترونية، الطبعة الثانية، مؤسسة فخرآوي للدراسات والنشر، مملكة البحرين، ٢٠٠٩ .
- ١٦- د. عماد مجدي عبدالملك، جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠١١ .
- ١٧- د. عمر محمد أبو بكر بن يونس، الاتفاقية الأوربية حول الجريمة الافتراضية، مؤسسة آدم للنشر والتوزيع، الطبعة الثانية، مالطا، ٢٠٠٨ .
- ١٨- د. محمد حماد مرهج الهيكي، الجريمة المعلوماتية نماذج من تطبيقاتها، دار الكتب القانونية، القاهرة، ٢٠١٤ .
- ١٩- محمد عبدالله أبو بكر سلامة، جرائم الكمبيوتر والأنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦ .
- ٢٠- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، الطبعة الثانية، دار النهضة العربية، القاهرة، ٢٠٠٩ .
- ٢١- د. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١١ .

- ٢٢- محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، مطابع دار الجمهورية للصحافة، القاهرة، ٢٠١٠ .
- ٢٣- د. محمد عوض الترتوري و د. اغادير عرفات جويحان . علم الإرهاب (الاسس الفكرية والنفسية والاجتماعية والتربوية لدراسة الإرهاب)، الطبعة الاولى، دار الحامد للنشر والتوزيع، عمان، ٢٠٠٦ .
- ٢٤- محمود احمد عباينة، جرائم الحاسوب وابعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠٠٩ .
- ٢٥- د. مدحت رمضان، جرائم الاعتداء على الأشخاص والأنترنترنت، دار النهضة العربية، القاهرة، ٢٠٠٠ .
- ٢٦- د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٥ .
- ٢٧- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦ .
- ٢٨- د. نسرين عبدالحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية، ٢٠٠٨ .
- ٢٩- د. نهلا عبدالقادر المومني، الجرائم المعلوماتية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠١٠ .
- ٣٠- د. هدى حامد قشقوش، جرائم الحاسوب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢ .
- ٣١- د. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، الطبعة الأولى، مكتبة الآلات الحديثة، اسيوط، ١٩٩٤ .
- ٣٢- د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، اسيوط، ١٩٩٤ .



- ٣٣- د. هلالى عبد اللاه احمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة .
- ٣٤- د. هلالى عبد اللاه احمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٣ .

#### ثانياً: الرسائل والأطاريح الجامعية :

- ٣٥- ايمن عبدالحفيظ عبدالحميد سليمان، الأحكام الموضوعية للقانون الجنائي والجرائم المعلوماتية، رسالة ماجستير، مقدمة إلى كلية الحقوق، جامعة القاهرة، ٢٠١٠ .
- ٣٦- رشدي محمد علي محمد عيد علي، الحماية الجنائية للمعلومات على شبكة الأنترنت، اطروحة دكتوراه، مقدمة إلى كلية الحقوق، جامعة القاهرة، ٢٠٠٩ .
- ٣٧- عفيفي كامل عفيفي، جرائم الكمبيوتر، رسالة ماجستير، مقدمة إلى كلية الحقوق، جامعة الإسكندرية، ٢٠٠٣ .
- ٣٨- محسن بن سليمان الخليفة، جرائم الحاسب الآلي وعقوباتها في الفقه والنظام، رسالة ماجستير، مقدمة إلى كلية الدراسات العليا، قسم العدالة الجنائية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، ٢٠٠٣ .
- ٣٩- محمد عبدالله محمد العوا، المسؤولية الجنائية الناشئة عن جرائم الأموال عبر الأنترنت، اطروحة دكتوراه، مقدمة إلى كلية الحقوق، جامعة الإسكندرية، ٢٠١٢ .
- ٤٠- محمد محمد عمر الغياثين، الجرائم المعلوماتية عابرة الحدود، اطروحة دكتوراه، مقدمة إلى كلية الحقوق، جامعة القاهرة، ٢٠١٣ .

#### ثالثاً: البحوث والتقارير :

- ٤١- د. امل فاضل عبد خشان و د. احمد حمد الله، الأثبات الجنائي في جرائم اساءة استعمال الهاتف النقال، بحث منشور، مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، المجلد ٤، الجزء الأول، العدد ١٢، ٢٠١٥ .

- ٤٢- د. راشد بن حمد البلوشي، الدليل في الجريمة المعلوماتية، بحث منشور، مجلة الحقوق للبحوث القانونية والاقتصادية، العدد الأول، كلية الحقوق، جامعة الإسكندرية، ٢٠٠٨ .
- ٤٣- د. عادل عبدالله خميس المعمري، التفتيش في الجرائم المعلوماتية، بحث منشور، مجلة الفكر الشرطي، المجلد ٢٢، العدد ٨٦، مركز بحوث الشرطة، الإمارات العربية المتحدة، ٢٠١٣ .
- ٤٤- عادل يوسف عبدالنبي الشكري، الجريمة المعلوماتية وازمة الشرعية الجزائية، بحث منشور، مجلة كلية القانون، جامعة الكوفة، العدد السابع، ٢٠٠٨ .
- ٤٥- د. فايز الظفيري، الأحكام العامة للجريمة الإلكترونية، بحث منشور، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، العدد ٢، السنة ٤٤، يوليو ٢٠٠٢ .
- ٤٦- د. محمد قدري حسن عبدالرحمن، جرائم الاحتيال الإلكتروني، بحث منشور في مجلة الفكر الشرطي، المجلد (٢٠)، العدد ٧٩، امارة الشارقة، الإمارات العربية المتحدة، ٢٠١١ .
- ٤٧- د. هشام محمد فريد رستم، جريمة الحاسب كصورة من الجرائم الاقتصادية المستحدثة، بحث منشور، مقدم لمؤتمر الأمم المتحدة لمنع الجريمة الذي عقد في ٢٩ أبريل، منشور في مجلة الدراسات القانونية، كلية الحقوق، جامعة اسيوط، العدد ١٧، يونيو ١٩٩٥ .

#### رابعاً: المصادر الأجنبية :

- 48- Bert-Jaap Koops , Technology and the crime society : (Rethinking legal protection), 2009, Vol.2(1), 1Law Innovation and tech.93.
- 49- Explanatory Report Eu conv . p7 (sec .1. Art -13) established a common minimum standard of relevant offence.

- 50- Giddens (Anthony):“ Runaway world : How Globali Zationis reshaping our lives “ , London, Profile books , 1999 .
- 51- Scott Charney And Kent Alexander , COMPUTER CRIME , 1996 , Vol.45, 45 Emory L.J.
- 52- Timothy J.o’hearn , Crime and Technology : (New rules in a new World), 1998, Vol.7(2) ,Information & Communications Technology Law.

#### خامساً: المواقع الإلكترونية :

- ٥٣- موقع مجلس اوربا متاح على الأنترنت : <http://www.COe.int> .
- 54-EXPLANATORY Report available online in NOV.2001 at : <http://convention . coe .int / treaty /EN/ projets / final cvber Rapex , htm .>
- ٥٥- شيماء عبدالغني محمد عطاالله، مكافحة جرائم المعلوماتية في المملكة العربية السعودية، بحث منشور، متاح على الموقع الإلكتروني الشخصي للدكتورة شيماء: [Faxulty .Ksu .cdu.sa/Shaimaatalla](http://Faxulty .Ksu .cdu.sa/Shaimaatalla) .
- ٥٦- مشروع مكافحة الجرائم المعلوماتية في التشريع العراقي لسنة ٢٠١٢، متاح على الموقع الإلكتروني : <http://www.Iraqja.iq/view.1645> .
- سادساً: القوانين والدساتير :
- ٥٧- قانون اصول المحاكمات الجزائية العراقي رقم ٢٣ لسنة ١٩٧١ المعدل .
- ٥٨- قانون اساءة استخدام الحاسب في المملكة المتحدة الصادر في ٢٩ يونيو سنة ١٩٩٠، والذي طبق اعتباراً من ٢٩ اغسطس سنة ١٩٩١ .
- ٥٩- قانون الأحوال المدنية المصري رقم ١٤٣ لسنة ١٩٩٤ .

- ٦٠- قانون العقوبات الفرنسي الجديد الصادر في سنة ١٩٩٢، والمعمول به منذ اول مارس سنة ١٩٩٤ .
- ٦١- قانون العربي النموذجي في شأن مكافحة جرائم الكمبيوتر والأنترنيت، الذي تم اقراره في سنة ٢٠٠٣ .
- ٦٢- دستور جمهورية العراق الدائم لسنة ٢٠٠٥ .
- ٦٣- القانون الاتحادي بشأن مكافحة جرائم تقنية المعلومات رقم (٢) لسنة ٢٠٠٦ .
- ٦٤- مشروع دستور إقليم كردستان العراق لسنة ٢٠٠٦ .
- ٦٥- قانون مكافحة جرائم المعلوماتية السعودي ٢٠٠٧ .
- ٦٦- نظام مكافحة جرائم المعلوماتية السعودي رقم ١٧ لسنة ٢٠٠٧ .
- ٦٧- قانون منع اساءة استعمال اجهزة الاتصالات رقم (٦) لسنة ٢٠٠٨ .
- ٦٨- قانون الاتحادي لدولة الإمارات العربية لمكافحة جرائم تقنية المعلومات رقم (٥) لسنة ٢٠١٢ .

#### سابعاً: الاتفاقيات الدولية :

- ٦٩- اتفاقية بودابست Budapest Convention .

## المخلص:

إن ظاهرة جرائم الكمبيوتر أو الانترنت أو جرائم التقنية العالية أو الجريمة المعلوماتية، أو (السيبر)، أو جرائم اصحاب الياقات البيضاء، ظاهرة إجرامية حديثة نسبياً تفرع في جنباتها اجراس الخطر لتنبه مجتمعات العصر الحالي عن حجم المخاطر وهول الخسائر والاضرار الناجمة عنها، على اعتبار أنها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة (بيانات ومعلومات وبرامج على كافة أنواعها)، فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون اذكياء يمتلكون ادوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الانترنت، هذه المعطيات هي موضوع هذه الجريمة وما تستهدفه اعتداءات الجناة، وهذا بحد ذاته يظهر مدى خطورة الجرائم المعلوماتية فهي في الوقت الذي تطال الحق في المعلومات، ايضاً تمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية وتشيع فقدان الثقة بالتقنية وتهدد ابداع العقل البشري، لذا فإن إدراك ماهية الجرائم المعلوماتية والطبيعة الموضوعية لهذه الجرائم، واستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها، وسمات مرتكبيها ودوافعه يتخذ اهمية استثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والاجتماعية والثقافية والأمنية، وإذا كانت مجتمعاتنا العربية لم تتأثر بعد بشكل ملموس بمخاطر هذا النمط المستحدث من الإجرام، فإن خطر جرائم المعلوماتية المحتمل في البيئة العربية يمكن ان يكون كبيراً، على اعتبار ان الجاهزية التقنية والتشريعية والادائية (استراتيجيات حماية المعلومات)، لمواجهتها ليست بالمستوى المطلوب إن لم تكن غائبة تماماً، وبالمقابل فقد امست جرائم المعلوماتية من اخطر الجرائم التي ترتكب في الدول المتقدمة، تحديداً الامريكية والاوروبية، ولهذا تزايدت خطط مكافحة هذه الجرائم وانصبت الجهود سواء على المستوى الدولي ام الوطني على دراستها المتعمقة وآليات مكافحتها، مع خلق آليات قانونية للحماية من اخطارها، حيث برز في هذا المجال المنظمات الدولية والاقليمية خاصة المنظمات والهيئات الاقليمية الاوروبية، وإدراكاً لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية، كان لا بد للعديد من الدول وضع قوانين وتشريعات خاصة، أو العمل على جبهة قوانينها الداخلية لجهة تعديلها من اجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم .

## **ABSTRACT :**

The phenomenon of computer, network, and informatics crimes - cybercrimes or white collar- relatively is a new phenomenon of serious crimes in which signalize our society to be acquainted. This is based on the ground that these kinds of crimes target all kinds of confidential data and information. Furthermore, cybercrimes is committed by professional criminals and they commit it in a hidden way. Hence, the object of these types of offense is data and information in computers and when this information is transformed via network, in particularly via internet. This indicates the seriousness of informatics crimes which affect the right of information, affects individuals' privacy, threaten national security and sovereignty, effect on community confidence, and it will affect human's thinking and inventions. Therefore, apprehending the essence of informatics crimes, its nature, clarification object of the crime, its merits, seriousness, the damage and loss in which results from it, perpetrators attribute and motivation is very substantial to deal with the scope of this dangerous phenomenon pertaining to economic, social, cultural, and security .

Although Arab societies have not been affected by the informatics crimes in a wide scope, the dangerous and seriousness of this crime will be a lot due to the preparedness of technical, legislatively, and its performance- information protection strategy- is not sufficient to encounter these kinds of crimes, or they might not have regulated at all. On the other hand, informatics crimes have been increased in developed countries, such as United States and Europe. Thus, most of these developed countries have regulated and set laws in both national and international level's to encounter these types of crimes. In addition, regional and international organizations- specifically regional organization in Europe- have called upon regulating and encountering informatics crimes; likewise many countries which had no laws to regulate it, they have commenced to pass laws or amend the existed law which was not adequate to provide efficient legal protection against this crime.