الجرائم المعلوماتية: خصائصها وكيفية مواجهتها قانونيًّا

DOI:10.26735/13191241.2017.004

د. محمد بن أحمد علي المقصودي(*)

أستاذ القانون العام المشارك بمعهد الإدارة العامة ـ الرياض

قدم للنشر في ٥/ ٤/ ٢٠١٦... وقبل في ٤/ ١٢/ ٢٠١٦

الملخص

تتناول هذه الدراسة ما تتصف به الجريمة المعلوماتية من صفات تميزها من غيرها من الجرائم التقليدية، فهي تشتمل على جوانب فنية إلكترونية، وتحتوي على مصطلحات ومفردات حديثة مثل: البيانات والبرامج محل الاعتداء الجرمي، كما نلمس أن غالبية موضوعات الجريمة الإلكترونية تكون عبارة عن تسجيلات إلكترونية تتم عبر شبكات الاتصال السيبراني.

وقد توصلت الدراسة إلى أن عدم وجود قانون عالمي حديث يجرم التقنيات الفنية الجديدة الناشئة عن استخدام الإنترنت في ارتكاب الجرائم التقليدية أدى إلى اللجوء إلى التفسير القانوني، وهو ما أثار بعض الإشكاليات في الوصول للتكييف القانوني للفعل المرتكب بشكل دقيق، وأثار كذلك مشكلة التمييز بين العمل التحضيري والبدء في تنفيذ الجريمة وغيرها، وبينت الدراسة أن التعامل مع الدليل في هذا النوع من الجرائم أوجد مجالًا حديثًا في الإثبات، فبعد أن كان مجال الإثبات ينحصر فقط في المستند الورقي أصبح الدليل الرقمي ينازعه في هذه المرتبة، إضافة إلى وجود العديد من الصعوبات العملية في تطبيق الأفكار التقليدية والمستقرة بالقانون الجنائي كمبدأ الشرعية القانونية ومبدأ سريان القانون من حيث الزمان والمكان واختصاص القضاء الوطني دون الأحكام الأجنبية، ووفقًا لكل ما تقدم يتضح لنا خطورة تحديات الجريمة الإلكترونية وضرورة التعاون الدولي لمكافحتها للوصول إلى أفضل السبل القانونية للحد من انتشارها، وبعد ذلك فقدان السيطرة على مرتكبيها في ظل غياب عالم افتراضي واسع المجال.

الكلمات المفتاحية: الجريمة الإلكترونية، المعلوماتية، النظام السعودي، الجرائم المعلوماتية، الأمن السيبراني.

(*) المراسلات الخاصة بهذا البحث توجه إلى محمد بن أحمد المقصودي malmagsodi@yahoo.com

لقد شـــهد القرن العشرون تطـــورًا هائلًا في مجال الاتصال، وأصبحت الشـــبكة المعلوماتيـــة الدولية من عجائبه التى امتدت عبر أنحاء المعمورة وربطت بين شـــعوبها، فأصبحت وسيلة التعامل اليومي بين أفراد مختلف الطبقات والمجتمعات.

ومقابل تباين الذهنيات والمســـتويات العلمية لمســـتعملي شبكة الإنترنت ظهرت ممـارسات غيـر مشروعة، فأصبحت هذه الشبكة أداة ارتكابها أو محلًّا لها حسب الحالة؛ مـــا أدى إلى ظهور طائفة جديدة من الجرائم العابـــرة للحدود، مختلفة عن باقي الجرائم التقليدية، وقد سميت بالجرائم المعلوماتية أو الإلكترونية أو جرائم الإنترنت. وقد أدى تســـارع إيقاع التقدم التكنولوجي والتقني الهائل، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفاكس والإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الاصطناعية إلى اســـتغلاله من قبل مرتكبي الجرائم الإلكترونية في تنفيذ جرائمهم؛ إذ لم تعـــد تقتصر على إقليم دولة واحدة، بل تجـــاوزت حدود الدول، وهي جرائم مبتكرة ومســـتحدثة تمثل ضربًا من ضروب الذكاء الإجرامي، وقد اســـتعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.

ونظرًا لما يتعلق بضعف نظم الملاحقة الإجرائية التي تبدو قاصرة عن استيعاب هذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية، فقد وجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المســـتوى القانوني وســـائر جوانب وأبعاد تلـــك التقنيات الجديدة، بما يضمن في الأحوال كافة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وضرورة التكامل في الدور والهدف مع المعاهدات الدوليـــة. وإدراكًا لأهمية تنظيم التعاملات الإلكترونية، وافق مجلس الوزراء في المملكة العربية الســـعودية في ٧/ ٣/ ١٤٢٨هـ الموافق ٢٦/ ٣/ ٢٠٠٧ على نظامي مكافحة جرائم المعلوماتية والتعاملات الإلكترونية، وكان ذلك للحد من وقوع الجرائم المعلوماتية وتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة أو مخالفة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات.

مشكلة الدراسة

مشـــكلة البحث تعود إلى ما يتميز به من صفات فنيـــة، ومفردات ومصطلحات جديدة كالبرامج والبيانات التي تشـــكل محلًّا للاعتداء أو تستخدم كوسيلة له، ومعظم مستندات موضوعه (الجريمة الإلكترونية) عبارة عن تسجيلات ومستندات إلكترونية تتم عبر شـــبكات الاتصال المعلوماتي، ذات طبيعة خاصة متميزة، وذلك راجع إلى عدة عوامل: منها طبيعة المال المعلوماتي (محل الجريمة المعلوماتية) وحداثة ظهور الحاســـب الآلي وتقنية تشـــغيله، ولهذا أصبح لا يكفي أن يكـــون الباحث ورجل الضبط الجنائي والمحقق والقـــاضي متخصصًا في القانون، بل يتعين عليه أن يكون ملمًّا بالجوانب الفنية للحاســـب الآلي والإنترنت؛ ليتمكن من إيجاد الحلول للتحديات والمشكلات القانونية التي تثيرها شبكة الاتصال والمعلومات وجرائمها الإلكترونية، كما أن عدم وجود قانون متكامل يجرم جميع صور الاســـتخدام غير المشروع للتقنيات الفنية الجديدة الناشئة عن استخدام الإنترنت في ارتكاب الجرائم التقليدية أدى إلى اللجوء إلى التفسير، الأمر الذي أثار إشكاليات التكييف القانوني للفعل، كما يثير مشكلة التمييز بين العمل التحضيري والبدء في تنفيذ الجريمة وغيرها، كما أن التعامل مع دليل هذا النمط من الجرائم فتح مجالًا جديدًا في الإثبات، فبعد أن كان مجال الإثبات ينحصر فقط في المستند الورقي أصبح الدليل الرقمـــي ينازعه في هذه المرتبة، ناهيك عن وجود بعـــض الصعوبات العملية في تطبيق الأفكار التقليدية والمستقرة بالقانون الجنائي كمبدأ الشرعية وسريان القانون من حيث الزمان والمكان واختصاص القضاء الوطني. وفقًا لكل تلك الاختلافات والإشكاليات لزم الجواب عن ســـؤال جوهري وهو: ما الوسيلة المثلى لتوحيد الجهود الدولية لضبط جرائم المعلوماتية وتقنية المعلومات؟

أهمية الدراسة

تتمثل أهمية موضوع بحث ضرورة التعاون الدولي لمكافحة الجرائم المعلوماتية من الناحية النظرية والعملية في اعتباره من الموضوعات التي تلامس بشـــكل مباشر الكثير من مصالح أفراد المجتمـــع والدول وعلى وجه الخصوص المصارف من خلال التعامل

الإلكتروني والسحب من الأرصدة بواسطة البطاقة الممغنطة أو الدفع الإلكتروني، وأيضًا المساس بالحياة الخاصة للأفراد عن طريق التسجيل وغيرها من المجالات التي تدخل في استعمال الحاسب الآلي، كما أن الإجرام الإلكتروني أصبح يستخدم من قبل المنظمات الإرهابية لتهديد مصالح الدول الاقتصادية والأمنية.

تساؤلات الدراسة

لكل دراسة تساؤلات ينبغي الإجابة عنها، والتساؤل الرئيس الذي تتطلب الإجابة عنه هو: ما خطورة الجريمة الإلكترونية على المستوى الدولي؟

ومن ثم تقتضي دراستنا الإجابة عن مجموعة من التساؤلات الفرعية على النحو التالي:

١ ـ ما المقصود بمفهوم الجرائم الإلكترونية وطبيعتها القانونية وخصائصها؟

٢ ـ ما مدى كفاية القوانين الجنائية التقليدية الوطنية في ضبط السلوك الإجرامي لهذا النوع من الجرائم؟ وهل هناك حاجة لتطوير البنية التشريعية الجنائية الوطنية لاستيعاب هذه الظاهرة الإجرامية الجديدة؟

٣ ـ ما الصورة المثلى للتعاون الدولي للوصول إلى الملاحقة الجنائية في إطار القوانين الوطنية وعلى صعيد الملاحقة الجنائية الدولية؟

٤ ـ ما الصعوبات العملية في تطبيق الأفكار التقليدية والمستقرة بالقانون الجنائي كمبدأ الشرعية وسريان القانون من حيث الزمان والمكان واختصاص القضاء الوطني؟

منهج الدراسة

تعتمد الدراسة على المنهج الوصفي التحليلي الذي يقوم على أساس تحديد خصائص ظاهرة الجرائم المعلوماتية ووصف طبيعتها ونوعية العلاقة بين متغيراتها وأسبابها واتجاهاتها المحلية والدولية، وما إلى ذلك من جوانب تدور حول سبر أغوار المشكلة وفقًا لنظام جرائم مكافحة المعلوماتية السعودي وما ورد به، كما تم استعراض آراء الفقهاء

وبيان موقفهـــم من مدى اعتبار خطورة تحديات الجريمة الإلكترونية، وحاجة المجتمع الـــدولي للتعاون الأمثل لمكافحتها، وما يترتب على ذلك من التزامات قانونية، وخاصة مع انتشار ظاهرة الإرهاب الدولي.

المبحث الأول: ماهية الجريمة المعلوماتية

مـــن المتفق عليه أنه لبحث أي فرع من فروع المعرفة وجب بيان مفهومه من خلال تعريف ســماته الأساسية؛ لكي يتم رســم الصورة العامة لهذا البناء المعرفي (عبد اللاه، ١٩٩٧، ٢٥)، فالبحث في مفهوم الجريمة المعلوماتية شـــأنه في ذلك شـــأن أي بحث في فرع من فروع المعرفة؛ لذلك سوف يتم تقسيم هذا المبحث إلى مطلبين: الأول: يخصص لتعريف الجريمة المعلوماتية والثاني: لتحديد أشخاص الجريمة المعلوماتية.

المطلب الأول: مفهوم الجريمة المعلوماتية

تعددت التوجهات حول تعريف الجريمة الإلكترونية، فكل رأي تبنى مفهومًا بالنظر إلى الزاوية التي رآها، فهناك جانب من الفقه عرفها من زاوية فنية، وأخرى قانونية، وهناك جانب آخر يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو اســتنادًا لمعايير أخرى حسب القائلين بها (حجازي، ٢٠٠٧م، الشوا، ١٩٩٤). ولم تحدد الأمم المتحدة في مدونتها بشأن الجريمة المعلوماتية تعريفًـــا متفقًا عليه دوليًّا، ومع ذلك نجد أن مكتب تقييـــم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاســـب الآلي بأنها «الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيس» (رستم، ١٩٩٥، ٤٥)، كما عرفت أيضًا بأنها «نشـــاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني» (حجازي، ٢٠٠٧، ٧ـ٨)، وعرفت أيضًا بأنها «كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية، يهدف إلى الاعتداء على أي مصلحة مشروعة، سواء أكانت مادية أم معنوية» (حجازي، ٢٠٠٧، ٧ـ٨).

وتجب الإشـــارة إلى أن جرائم الإنترنـــت لا تقع على ماديـــات، وإنما على برامج الكمبيوتر وما يحتويه من معلومات أو ما يحمله من أسرار حتى لو كانت النتائج المحققة

أو الخسائر الواقعة على الضحية تتجسد في شكل مادي في كثير من الأحوال؛ لذلك فهو يجعل منها جرائم تخرج عن المألوف باختلافها عن الجرائم التقليدية المعروفة ضمن القسم الخاص لقانون العقوبات التي تنطبق عليها القواعد الواردة في القسم العام منه، وهذا ما استوجب معه أن تسن تشريعات تعرف من خلالها الأفعال المجرمة وتحددها مقابل وضع العقاب المناسب لها؛ لأن تعريف الجريمة في إطار فقهي أو من الجانب الاقتصادي أمرٌ غير كافٍ، إذا لم يتبن القانون هذه التعريفات، وبقيت خارج إطار مبدأ الشرعية، فلا يمكن معه الحديث عن جرائم الإنترنت؛ لأن الهدف من التجريم ضمن نص قانوني، هو تحديد الفعل المجرم وما يقابله من عقوبة؛ لأن الأصل في الأفعال الإباحة، وقد عرَّف نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/ ١٧ في ٨/ ٣/ ١٤٢٨هـ الموافق ٢٧/ ٣/ ٢٠٠٧، الجريمة المعلوماتية في الفقرة ٨ من المادة الأولى بأنها «أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية، بالمخالفة لأحكام هذا النظام».

كما عرّف نظام مكافحة جرائم المعلوماتية في المملكة الدخول غير المشروع في المادة الأولى فقرة ٧ منه بقوله: «دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها». وأشارت الفقرة السادسة من المادة السابقة إلى تعريف الحاسب الآلي بأنه (أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له) كما أشارت الفقرة التاسعة إلى تعريف الموقع الإلكتروني بأنه (مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد) ووفقًا للفقرة الثانية من ذات المادة الأولى يعرف النظام المعلوماتي بأنه (مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية)، كما عرفت الفقرة الثالثة الشبكة المعلوماتية بأنها (ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل: الشبكات الخاصة والعامة والشبكة العالمية «الإنترنت»). وترى منظمة التعاون الاقتصادي والتنمية (OCDE) أن الجريمة المعلوماتية هي، كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجًا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية (رستم، ١٩٩٥).

وأرى أن أفضل تعريف للجريمة المعلوماتية يشمل كل استخدام، في صورة فعل أو امتناع، غير مشروع للتقنية المعلوماتية، يهدف إلى الاعتداء على أي مصلحة مشروعة، سواء أكانت مادية أم معنوية.

المطلب الثاني: أشخاص الجريمة المعلوماتية

الجرائم المعلوماتية كغيرها من الجرائم تشـــمل طرفين: جانيًـــا ومجنيًّا عليه إلا أن أطراف الجريمة المعلوماتية يختلفون نوعًا ما عـــن أطراف باقي الجرائم، وعليه فجوهر البحـــث بهذا الصدد ينصب على مصدر وجود الأفعال وتوجيهها، ومما لاشـــك فيه أن الشـــخص الطبيعي هو الذي يهيئ فرصة استغلال الوسيلة المعلوماتية، ولكن هل يعد كذلك حين ترتبط شبكة المعلومات عامة بحواسيب متعددة؟ يبدو أن الأمر يختلف بعض الشيء في المؤسسات العامة والبنوك وغيرها التي تحمل صفة الشخص المعنوي معرضة لاعتداءات عن طريق هذه الشبكة من المعلومات، فعلى الرغم من وسائل الحماية المتعددة فإنه ثبت عدم فاعليتها أمام قرصنة شبكة المعلومات (Johnson,1997:66)ويمكن تحديد أشخاص الجريمة المعلوماتية كما يلي:

١ ـ المجرم المعلوماتي

بطبيعة الحال في الجريمة المعلوماتية نكون أمام مجرم يحمل مهارات تقنية وصاحب علم بتقنية نظام الحاســـبات الآلية، فشـــخصية المجرم المعلوماتي، ســـواء أكان طبيعيًّا أم معنويًّا وكيفية ارتكاب الجريمة تجعل منه شـــخصًا يتســـم بسمات خاصة تضاف إلى الصفات الأخرى التي يجب أن تتوافر في المجرم العادي (قشـــقوش،١٩٩٧) وأهم ما يتميز به المجرم المعلوماتي أنه يتوافر لديه خبرة بالمســـائل المعلوماتية ومعرفة كافية بآلية عمل الحاســـب الآلي وتشـــغيله باعتبار أن الإجرام المعلوماتي ينشأ من تقنيات التدمير الهادئة التي تتمثل بالتلاعب بالمعلومات والكيانات المنطقية أو البيانات، بيد أن ذلك لا يعني إمكانية تصور العنف الموجه ضد النظام المعلوماتي، فقد يكون محل الجريمة إتلاف الحاســـب الآلي ذاته أو وحدة المعالجة المركزيـــة أي أن ما يمكن الاعتداء عليه قد يكون بهيكلية الحاســـبات لا بمعلوماتها المتنقلة عبر شبكة المعلومات، فوحدة المعالجة المركزية

هي محور الحاسب الآلي وأساسه، فهي تمثل الدماغ المسيطر على جميع العمليات التي يقوم بها الحاسب الآلي، سواء أكانت منطقية أم حسابية ولا وجود له بدونها، حيث تقوم بنقل البيانات والمعطيات من الوحدة المساعدة وإليها مع ضمان تحرك المعلومات من الذاكرة الرئيسة وإليها (المناعسة،٢٠٠١).

ولا يمكن لأي عقوبة أن تحقق هدفها سواء في مجال الردع العام أو الردع الخاص ما لم نضع في الاعتبار شخصية المجرم حتى يمكن إعادة تأهيله اجتماعيًّا لكي يندمج بالمجتمع مرة أخرى ليعود مواطنًا صالحًا على اعتبار أن إصلاح المجرم هو نقطة الارتكاز للنظام العقابي الحديث، فالإجرام المعلوماتي يعد إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف على الرغم من تصور الإجرام العنيف الموجه ضد النظام المعلوماتي الذي يتجسد بإتلاف الحاسب الآلي.

ووفقًا لما سبق فإن مرتكبي الجرائم المعلوماتية ليسوا على درجة واحدة من الخطورة أو الكفاءة، وعلى هذا الأساس يمكن تصنيفهم حسب إمكاناتهم ومقصدهم من ارتكاب الجريمة إلى صنفين: الأول: مجرمون مستخدمون وهم من تتوافر لديهم خبرة لا بأس بها في مجال عمل الحاسب الآلي ومكوناته ووظائفه الأساسية ومعرفة بعض البرامج التي يجري العمل بها كالبرامج المحاسبية؛ لذا فإن هؤلاء يمارسون مواهبهم لغرض الولوج في نظم المعلومات لأجل ممارسة هواية اللهو وهم لايدركون ولايقدرون النتائج المحتملة التي يمكن أن تؤدي إلى أفعالهم غير المشروعة بالنسبة إلى نشاط معين؛ لذا فإن هذه الفئة من المجرمين تعد أقل خطورة مقارنة بغيرها (المناعسة، ٢٠٠١) مع ملاحظة ازدياد الأعداد المستخدمة لتكنولوجيا الإنترنت وما سيتبعه بلا شك من ازدياد نسبة الجرائم في هذا المجال، فليس من المستبعد احتمال انزلاق هذه الفئة من غير المحترفين للأفعال غير المشروعة إلى محترفين للإجرام، وخاصة إذا ما تم احتضانهم من قبل منظمات إجرامية لتحقيق أغراض خطرة تؤثر بصورة أو بأخرى على معطيات التطور العلمي (سرور، ١٩٩٣).

والصنف الثاني: مجرمون محترفون يسمون بالمبرمجين؛ نظرًا إلى المستوى المهارى الذي يتمتع به المجرمون المحترفون من دخول واقتحام للأنظمة الحاسوبية بكل سهولة واقتدار على الرغم من احتياطات الأمن المتعددة مما تبدو معه خطورة هذه الفئة من

المجرمين واضحة بصورة كبيرة؛ إذ غالبًا ما تكون جرائم التحويل والنسخ والإضافة للمعلومات على البرامج وتفسير محتواها من هذه الفئة ضخمة (الشنيفي، ١٩٩٤)، إضافة إلى ذلك فإن باستطاعة هذه الفئة استخدام الإمكانات والأساليب المعلوماتية ليس في ارتكاب الجريمة فقط، بل حتى في التهرب من محاولة كشف أمرهم، بل وبالعمل على إعاقة ملاحقتهم من خلال تضييع الأدلة الموجودة المؤدية إلى إدانتهم (بكري، ١٩٩٠).

ومما سلف يتضح أن مرتكب الفعل الجرمي المعلوماتي قد يكون فاعلًا أصليًّا أو شريكًا في ارتكابه للجريمة، فصفة الفاعل الأصلي في الجريمة المعلوماتية غالبًا ما تكون من أحد العاملين أو المستخدمين في منشأة تدار بالنظام المعلوماتي بصرف النظر عن المستفيد من وراء ارتكاب مثل هذه الأفعال. ولما كان هذا النوع من الإجرام يستلزم الدقة في تنفيذ العمليات غير المشروعة، فإنه قد يستلزم كذلك مشاركة أو مساعدة أشخاص آخرين، سواء أكانوا فنيين أم مجرد وسطاء، وقد يكون هذا الاشتراك سلبيًّا يتمثل في الامتناع بيد أنه في الغالب الأعم يتمثل في المساعدة الفنية والمادية، وخاصة عندما تستلزم آليات الابتكار لمخادعة الحاسب الآلي الاستعانة بمجموعة من الوسطاء أو الشركاء والمؤتمنين على أسرار أسطوانات الحاسبات الآلية؛ إذ يؤدي هؤلاء الدور الرئيس في نجاح العملية غير المشروعة أو المستهدفة (الشوا، ١٩٩٤).

وتجدر الإشارة إلى أن المجرم المعلوماتي قد يكون شخصًا معنويًّا كالشركات والمؤسسات، وتعد جريمة المساس بأنظمة المعالجة الآلية للمعطيات، وهي أي جريمة ضد المال كجريمة غسل الأموال مرتبطة باستخدام المعالجة الآلية للمعلوماتية، وتتسع هذه العبارة على إطلاقها لتشمل كل صور الدخول الاحتيالي من طرف أحد ممثلي الشخص المعنوي ولحسابه (سالم، ٢٠٠٣).

٢ ـ المجني عليه في الجريمة المعلوماتية

اتضح لنا أن جرائم المعلوماتية يمكن أن يباشرها شخص طبيعي أو معنوي، كما أن المجني عليه في تلك الجرائم قد يكون كذلك شخصًا طبيعيًّا أو معنويًّا مع أن الغالبية العظمى من هذه الجرائم تقع على شخص معنوي يتمثل بمؤسسات وقطاعات مالية

وشركات ضخمـــة (Grieve, 2012:23). إلا أن المعلومـــات المجردة تعد في الوقت الحاضر من أهم المصالح المســـتهدفة بعد الأموال، وخصوصًا إذا كانت هذه المعلومات ذات أهميـــة بالغة، وكان هدف المجرم المعلوماتي هـــو الحصول على مقابل وعوض عن طريق المقايضة غير المشروعة لهذه المعلومات أو بيعها لغير أصحابها الشرعيين، وســـواء أكانت المعلومات مخزنة بذاكرة الحاسوب أم مدخلة في بنوك المعلومات؛ إذ يتم تشويشها وإظهارهـــا على غير حقيقتها، ويدخل في هذا النوع ما يتعلق بأسرار الدولة والمشـــاريع الصناعية وجرائم المنظمات الإرهابية عالية التنظيم (قشقوش، ٢٠٠٠، رمضان، ٢٠٠٩، Vitalis, 1991:135).

وتكشـــف الدراســـات والواقع أن هذا النوع من الجرائم يكون دور المجني عليه ضئيلًا وسلبيًّا إلى حد كبير؛ إذ يفضل الكثير من المجني عليهم الإبقاء على ما لحقهم من اعتداء سرًّا، حيث يميلون إلى التكتم عما لحقهم من أضرار ناتجة عن الجريمة المعلوماتية ومرد ذلك يكمن برغبتهم في الحفاظ على مركزهم الاجتماعي أو سمعتهم التجارية حماية لمركزهم المالي وثقة العملاء بهم؛ لذا لا يرغبون بالكشف عن الاختلافات الحاصلة على أجهزتهم الحاسوبية حتى لا ينظر إلى تدابير الحماية لديهم على أنها ضعيفة غير فعالة؛ فتسبب ضعف الثقة بالمؤسسة، ومن ثم عزوف العملاء عنها (الأوجلي، ٢٠١١)، بالإضافة إلى عجز المجني عليهم عن الإثبات المادي للجريمة وخشيتهم احتمالية المساءلة القانونية في الوقت الذي يقع عليهم واجب الإشراف على المعلومات المستهدفة وامتلاكهم السلطة اللازمة لإمكان التقدير ووضع الإجراءات الضرورية في حالة حدوث أضرار ناشئة من إفشاء معلومات على قدر من الحساسية والخطورة (لطفي، ٢٠٠٧).

المبحث الثاني: الطبيعة القانونية للجريمة المعلوماتية وخصائصها

سوف يتم تقســـيم هذا المبحث إلى مطلبين: المطلب الأول: عن الطبيعة القانونية للجريمة المعلوماتية، ثم أعرض في المطلب الثاني خصائص الجريمة المعلوماتية.

المطلب الأول: الطبيعة القانونية للجريمة المعلوماتية

إن دراســـة الجرائم عامة والجرائم المعلوماتية خاصة تدخل في نطاق دراسة القسم

الخـــاص بقانون العقوبات، وهو الفرع المختص بدراســـة كل جريمة على حدة متناولًا عناصرها الأساســـية والعقوبة المقررة لها إلا أن الجرائم المعلوماتية تمثل ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي (أبو عامر وآخرون، ١٩٩٩).

وقد عرف نظام مكافحة جرائم المعلومات السعودي لعام ١٤٢٨هـ المشار له سلفًا البيانات في المادة الأولى فقرة ٤ بأنها (المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها).

وبما أن لهذه الجرائم طبيعة خاصة، وهي قدرة شـــبكة المعلومات على نقل وتبادل معلومات ذات طابع شـــخصي وعام في وقت واحد كالاعتداء على الخصوصية، والعلة في ذلك توســـع بنوك المعلومات بأنواعها علاوة على توســـع الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة المذكورة، ما يطرح تساؤلًا حول طبيعة الخدمات والتطبيقات في هذه الشبكة ليتســـنى معرفة ماهية النصوص والقوانين التي يجب تطبيقها على خدمات نشر المواقع وتبادل المعلومات فيها عامة وبشكل خاص معرفة النظام القانوني للمسؤولية التي يفرض تطبيقها على الأشخاص المسؤولين عن هذا النشر أو التبادل (عوض، ١٩٩٣)، وبعبارة أخرى هل يمكن وصف الخدمات والتطبيقات في شبكة المعلومات بأنها داخلة ضمن أحكام خدمـــات البريد أو التخابر الخاص أم أنها تدخل ضمن مفهوم الصحافة والمطبوعات أو الوسائل السمعية والبصرية أو المؤسسات التلفزيونية والإذاعة، أم هل يجب في كل الأحوال اعتبار شـــبكة المعلومات (الإنترنت) فضاء جديدًا للمعلومات لا علاقة لها بشـــبكة البريد والاتصالات الخاصـــة ولا بعلم القواعد والمبادئ العامة حول المســـؤولية واجبة التطبيق على الخدمات والتطبيقـــات فيها (عوض، ١٩٩٣، الصغير، ٢٠٠١، عيسى، ٢٠٠٥).

وقد عرف نظام مكافحة جرائم المعلومات السعودي لعام ١٤٢٨ الشبكة في المادة الأولى فقـــرة ٣ بأنها (ارتباط بين أكثر من حاســـب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل: الشبكات الخاصة والعامة والشبكة العالمية «الإنترنت»).

وإن البحث عن النظام القانوني الملائم لطبيعة الجرائم المعلوماتية عبر شبكة المعلومات يهدف بشـــكل جوهري للوصول إلى تحديد ماهية النصوص القانونية التي يجب تطبيقها على خدمات نشر المواقع والمعلومات فيها، علاوة على معرفة النظام القانوني للمسؤولية الذي يفترض تطبيقه على الأشخاص المسؤولين عن هذا النشر وخصوصًا لتباين موقف الدول بهذا الشأن، ومن هنا تتضح الطبيعة القانونية الخاصة لهذه الجرائم من خلال المجال الذي يمكن أن ترتكب فيه، ومن جانب آخر المحل الذي يقع عليه الاعتداء المشـــار إليه، فطبيعة التطور السريع في مجال المعلوماتية قد يفسح المجال لاقتناء وسائل إلكترونية تمكن المتجاوزين لاســـتخدامها من ارتكاب جرائم مختلفة؛ لأن الإجرام المعلوماتي يتعلق بكل سلوك غير مشروع فيما يتعلق بالمعالجة الآلية لبيانات وإدخال المعلومات ونقلها، ومن ثم يتحتم ضمـــه إلى نطاق القانون الجنائي على الرغم من أن معظم نصوصه المقارنة عاجزة عـــن مواكبه التطور المعلوماتي أو لما يحويه من فـــراغ تشريعي في هذا المجال؛ لذا كان من الضروري تحديث قوانين الجزاءات للجريمة المعلوماتية.

ويعد الأمن المعلوماتي هدفًا عامًّا لطبيعة الجريمة المعلوماتية، حيث نجد نص المادة الرابعة من نظام جرائم المعلوماتية الســـعودي ينص على (يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

١ ـ المساعدة على تحقيق الأمن المعلوماتي.

٢ ـ حفظ الحقوق المترتبة على الاســـتخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

٣ ـ حماية المصلحة العامة، والأخلاق، والآداب العامة.

٤ ـ حماية الاقتصاد الوطني).

ومن جهة أخرى تتميز هذه الجرائم بطبيعة خاصة من حيث تكييفها القانوني؛ إذ لم تكن القواعد التقليدية مخصصة لهذه الظواهر الإجرامية المستحدثة، فالنصوص التقليدية وضعت وفقًا لمعايير معينة في حين كان مفهوم الحقوق الشـــخصية في شبكة المعلومات هو الذي يرد على نتاج الفكر البشري، وهو يتعلق بشـــخص المرء وأمواله وممتلكاته، كما

أن تطبيق النصوص التقليدية على الجرائم المعلوماتية يثير مشـــكلات عديدة في مقدمتها مسألة الإثبات كالحصول على أثر مادي؛ إذ يمكن للجاني محو أدلة الإدانة في وقت قصير لا يتجاوز لحظات، وخاصة في حالة تفتيش الشـــبكات أو عمليات اعتراض الاتصال، فقد تكون البيانات التي يجري البحث عنها مشـــفرة، ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة، ومن هنا تثار مسألة مدى مشروعية إجباره على فك الشفرة، ولعل مـــا يزيد الوضع صعوبة وتعقيدًا ملاحقة جناة جرائم المعلوماتية الذين يقيمون في دولة أخرى لا تربطها اتفاقية بالدولة التي تحقق فيها السلوك الإجرامي أو جزء منه، وفي ضوء الاعتبارات الســـابقة التى تم تناولها يمكن القول: إن هذه الجرائم تتمتع بطبيعة قانونية خاصة (الصغير، ٢٠٠١، عبد اللاه، ١٩٩٧).

المطلب الثاني: خصائص الجريمة المعلوماتية

أدى انتشـــار شـــبكة المعلومات إلى التغير التقني المطـــرد والمتعاظم في هذا المجال وإلى سهولة تداول المعلومات، ومن ثم أسهم في ارتكاب الجريمة المعلوماتية عن طريق الحاسب الشخصي أو الحواســـيب الأخرى المستخدمة في دولة معينة على الرغم من أن النتيجة الإجرامية قد تتحقق في دولة أخرى؛ وبذلك أصبحت الجريمة المعلوماتية شكلًا جديدًا من الجرائم العابـــرة للحدود الإقليمية؛ ما جعلها تتخذ طابعًا يميزها من غيرها من الجرائم.

وبذلك يتضح لنا أن جرائم المعلوماتية تتميز بعدة خصائص لعل من أبرزها ما يلي:

١ ـ عالمية هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم؛ فهذه الجرائم هي صـــورة صادقة من صور العولمة؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عـــن بعد، وقد يتعدد هذا المكان بين أكثر من دولة، ويؤكد ذلك نص المـــادة ٧/ ٢ من نظام مكافحة جرائم المعلوماتية الســـعودي، حيث يقول: (الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشـــبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصـــول على بيانات تمـــس الأمن الداخلي أو الخارجـــي للدولة، أو

اقتصادها الوطني)؛ ومن الناحيـــة الزمنية تختلف المواقيت بين الدول؛ الأمر الذي يثير التســـاؤل حول: تحديد القانون الواجب التطبيق عن هذه الجريمة (المناعسة وآخرون، ٢٠٠١).

٢ ـ تعتبر جرائم صعبة الإثبات، حيث يصعب في كثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية، والسبب في ذلك يعود إلى استخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان، كما يتمثل السلوك المكون للركن المادي فيها بعمل سريع قد لا يســـتغرق أكثر من بضع ثوانٍ، علاوة على سهولة محو الدليـــل والتلاعب به في الوقت الذي تفتقر فيه هذه الجرائم إلى الدليل المادي التقليـــدي؛ لذا فهذه الجرائم لا تترك أثرًا لها بعد ارتكابها؛ علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات؛ ولذا فإن معظم جرائم الإنترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها.

٣ ـ تعد الجرائم المعلوماتية أقل عنفًا من الجرائم التقليدية أي أنها لا تحتاج إلى أدنى مجهود عضلي؛ بل تعتمد على القدرة الذهنية والتفكير العلمي المدروس المستند إلى معرفة بتقنيات الحاسب الآلي، فلا يوجد في واقع الأمر شعور بعدم الأمان تجاه المجرمين في مجال المعالجة الآلية للمعلومات باعتبار أن مرتكبيها ليسوا من محترفي الإجرام بصيغته المتعارف عليها.

٤ ـ أن الباعـــث على ارتـــكاب الجرائم المعلوماتية يختلف عنه بالنســـبة إلى الجرائم التقليديـــة، ففي الحالـــة الأولى يتمثل الباعث بالرغبـــة في مخالفة النظام العام والخروج عن القوانين أكثر من اســـتهداف الحصول على الربح في حين نجد أن الباعث لدى مرتكبي الطائفة الثانية هو الحصول على النفع المادي السريع، وإذا ما اقترن الباعث في ارتكاب الجرائم المعلوماتية بهدف تحقيق النفع المادي، فـــإن المبالغ التي يمكن تحقيقها من وراء ذلك تكون طائلة (الصغير، ٢٠٠١، الشوا، ١٩٩٤).

٥ ـ تعتمد هذه الجرائم على قمة الذكاء في ارتكابها؛ ويصعب على المحقق التقليدي التعامل مع هذه الجرائم. إذ يصعب عليه متابعة جرائم الإنترنت والكشف عنها

وإقامة الدليل عليها. فهي جرائم تتسم بالغموض؛ وإثباتها من الصعوبة بمكان والتحقيــق فيها يختلف عن التحقيق في الجرائم التقليدية، والوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى (المقاطع،١٩٩٢).

المبحث الثالث: السبل الدولية لمكافحة الجرائم المعلوماتية

ترتب على انتشــار الجريمة الإلكترونية تحديات واجهت المجتمع الدولي، فتزايد الأنشــطة الإجرامية الإلكترونية وتسلح ممارسيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيــا المعلومات والاتصالات يسرت لهم ارتكاب هذه الأنشــطة داخل حدود الدولة وخارجها، الأمر الذي أدى إلى انشــغال المنظمات والمؤتمرات الدولية بهذا النوع من الجرائم ودعوتها الدول إلى التصدي لها ومكافحتها، حيث تفوت بعض الأنشــطة على إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، ولما ارتبط بضعف نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة، ســواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية. وفي هذا المطلب سأعرض لمطلبين: الأول: يتناول الحلول المقترحة لمواجهة الجرائــم الإلكترونية والمطلب الثاني: القواعد التي يجب على المجتمع الدولي اتباعها لمواجهة الجرائم الإلكترونية.

المطلب الأول: الحلول المقترحة لمواجهة الجرائم الإلكترونية

إدراكًا مــن الدول لضرورة أهمية التعاون الدولي، وذلك لتجاوز تحديات الجرائم الإلكترونية، عمدت الكثير منها إلى عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الكمبيوتر العابرة للقارات (البشري،٢٠٠٠)، ففي عام ١٩٨٣ أجرت منظمة التعاون والإنماء الاقتصادي دراسة حول إمكان تطبيق القوانين الجنائية الوطنية وتكييف نصوصها لمواجهة تحديات الجرائم الإلكترونية وســوء استخدامه، وفي عام ١٩٨٥ أصدرت هذه المنظمة تقريراً عن تضمن قائمة بالحد الأدنى لعدد من أفعال ســوء استخدام الحاسب الآلي التي يجب على الدول أن تجرمها، وتفرض لها عقوبات في قوانينها، ومن أمثلة هذه الأفعال: الغش أو التزوير في الحاسب الآلي، وتغيير برامج الحاسب الآلي أو المعلومات

المخزنة فيه، وسرقة الأسرار المدعمة في قواعد الحاسب الآلي؛ وتفعيل التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، كما عالجت اتفاقية فيينا لسنة ١٩٨٨ الموضوع ذاته، وحثت الكثير من الدول على عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في هذه الجرائم، وكذلك لفت اللقاء التمهيدي الإقليمي لآسيا والباسفيك المنعقد في ١٩٨٩ الممهد للمؤتمر الثامن للأمم المتحدة المنعقد في كوريا ١٩٩٠ النظر إلى نتائج التطور والتقدم التكنولوجي فيما يتعلق بالجريمة الإلكترونية، واقترح تشجيع اتخاذ إجراء دولي حيال هذه الجريمة، والمؤتمر الأخير ناشد في قراره المتعلق بالجرائم ذات الصلة بالحاسب الآلي الدول الأطراف إلى ضرورة تكثيف جهودها لمكافحة الجرائم الإلكترونية من عدة وجوه (عوض،١٩٩٣، ٣٦٢)، منها تحديث القوانين الإجرائية وتبادل المساعدة في المسائل الخاصة بالجرائم الإلكترونية، وعقد اتفاقيات دولية تنطوي على نصوص تنظم إجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية، ووضع المجلس الأوروبي عام ٢٠٠١ اتفاقية بودابست، وتشكل نصوصها منظومة تعاون دولي تتسم بالمرونة والفاعلية، وتعمل على إحداث تقارب بين التشريعات الجنائية الخاصة بهذه الجرائم، وتكفل استخدام الوسائل الفعالة في البحث والتحقيق وملاحقة مرتكبيها، وكل ما يتعلق بالنصوص الخاصة بالتعاون الدولي، ولكن الأمر في الأحوال كافة منوط بقابلية التطبيق من جانب الدول من ناحية، وإيجاد آليات جديدة ونشطة من جانب الأمم المتحدة من ناحية أخرى في إطار من المساعدة المادية والتقنية، وتبادل الخبرات وإعداد قواعد بيانات تمكن الجميع من الإسهام بفاعلية في التصدي للجريمة الإلكترونية.

ومن الملاحظ أن المعاهدات تقوم سواء بطريق مباشر أو غير مباشر بدور يكاد يمثل في الآونة الأخيرة مصدرًا للقوانين الجنائية الوطنية، الأمر الذي يتعين معه إثارة اهتمام الدول ببذل مزيد من صور التعاون الدولي المادي والتقني للدول الأقل إمكانات بالنظر للكلفة الباهظة لمكافحة الجرائم الإلكترونية، ولاسيما وهي تواصل العمل في عالم التقنيات الواسع، ويرتبط ذلك بدور الأمم المتحدة من خلال لجنة منع الجريمة، وكذلك دور المنظمات والآليات الدولية الأخرى المعنية بالجريمة.

وتظهر أهمية وضرورة التعاون الدولي وتضافر الجهود من أجل تفعيل مكافحة الجرائم الإلكترونية، وذلك بإزالة العديد من العقبات التي تعترض سبيله من أبرزها:

إيجاد اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، مع محاولة وجود توافق بين قوانين الإجراءات الجنائية للدول بشـــأن التحقيق في تلك الجرائم، ومعالجة النقص في مجال الخبرة لدى الشرطة وجهات الادعاء والقضاء. ولذلك برز التعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المتعلقة بشبكة الإنترنت، ويكون بين الدول وأجهـــزة العدالة الجزائية لديها، فعلى الصعيد العربي نجـــد مثلًا أن هناك اجتماعات تم عقدها في إطار التنسيق بين المعاهد القضائية العربية لتوفير التدريب والتأهيل المناسبين لأعضاء الهيئات القضائية العربية، وقـــد تمخضت الاجتماعات عن الاتفاق على إعداد مشروع اتفاقية للتعاون بين المعاهد القضائية العربية تسمى اتفاقية عمّان للتعاون العلمي بـــين المعاهد القضائية العربية التي وقعـــت في ٩ إبريل ١٩٩٧ (الغافري، ٢٠٠٨). وفي سياق تأكيد جهود المملكة العربية السعودية لمكافحة هذه الجريمة الدولية ورد نص المادة الثانية عشرة من نظام مكافحة الجرائم المعلوماتية: «لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة، وخاصة ما يتعلق بحقوق الملكية الفكرية والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفًا فيها». وبذلك تؤكد هذه المادة إقرار المنظم السعودي بأهلية الأحكام الواردة في الاتفاقيات العربية والدولية التي تكون السعودية طرفاً فيها. وبذلك يكون المنظم السعودي قد أسس لعلاقة تكامل وتعاون وليس تعارضًا أو مخالفة بين نظام مكافحة الجرائم المعلوماتية، وبين السابق واللاحق من أنظمة أخرى شريكة داخلية أو دولية في تنظيم التقنية المعلوماتية أو استخدامها، وقد أقر مجلس الوزراء السعودي في جلســـته التي عقدها يوم الإثنين ٢٤ جمادى الأولى ١٤٣٣هـ الموافقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٢، وكل ذلك من شأنه تفعيل التعاون الدولي لمكافحة هذه الجريمة العابرة للقارات.

ويعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء الإلكتروني، وقد أسّست مجموعات عمل لوضع إستراتيجيات لمكافحة جرائم الإنترنت، ويستخدم مصطلح «الأمن السيبراني» لتلخيص أنشطة مختلفة كجمع المعلومات ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة الأخطار، والحماية، والتدريب، ودليل لأفضل الممارسات المهنية، ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت. وتشمل هذه السياسات المعلومات وأجهزة الكمبيوتر، والأفراد،

والبنية التحتية، وبرامج المعلوماتية، والخدمات، ونظم الاتصالات السلكية واللاسلكية، ومجمل المعلومات المنقولة أو المخزنة في الأجهزة الإلكترونية. ويهدف الأمن السيبراني جاهدًا لضمان تحقيق سلامة المؤسسات والأفراد في مواجهة الأخطار الأمنية، وكل ما يتعلق بشبكة الإنترنت. وأبرز المجموعات والمنظمات الدولية التي عملت في موضوع جرائم شبكة الإنترنت، مجموعة الدول الثماني G8 والأمم المتحدة ومنظماتها والاتحاد الدولي للاتصالات ومجلس أوروبا، ووفقًا لذلك تم صدور مبادئ وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر (١٩٩٧) ومبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول (١٩٩٩) وتوصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية (٢٠٠٢) ومبادئ توافر البيانات الأساسية لحماية السلامة العامة (٢٠٠٢) وإعلان بيان دول G8 على نظم حماية المعلومات، وعن الجمعية العامة للأمم المتحدة صدرت القرارات التالية:

- القرار ٤٥/ ١٢١ عام ١٩٩٠، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في عام ١٩٩٤.
- القرارات ٥٣/ ٧٠ في ٤ كانون الأول/ ديسمبر ١٩٩٨، و٥٤/ ٤٩ في ١ كانون الأول/ ديسمبر ١٩٩٩، و٥٥/ ٢٨ في ٢٠ تشرين الثاني/ نوفمبر ٢٠٠٠ و٥٦/ ١٩ في ٢٩ تشرين الثاني/ نوفمبر ٢٠٠١ و٥٧/ ٥٣ في ٢٢ تشرين الثاني/ نوفمبر ٢٠٠٢ و٥٨/ ٣٢ في ١٨ كانون الأول/ ديسمبر ٢٠٠٣ حول موضوع «التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي».
- القراران ٥٥/ ٦٣ في ٤ كانون الأول/ ديسمبر ٢٠٠٠، و٥٦/ ١٢١ في ١٩ كانون الأول/ ديسمبر ٢٠٠١ بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». ويدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، إلى أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.
- القرار ٥٧/ ٢٣٩ في ٢٠ كانون الأول/ ديسمبر ٢٠٠٢ بشأن «إنشاء ثقافة عالمية للأمن السيبراني».

ـ قرارا الجمعية العامة رقم ٥٧/ ٢٣٩ في ٣١ كانون الثاني/ يناير ٢٠٠٣ و٥٨/ ١٩٩ في ٣٠ كانون الثاني/ يناير ٢٠٠٤ بشأن «إنشاء ثقافة عالمية للأمن السيبراني»، اللذان يدعوان الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.

ومن ناحية أخرى، هناك العديد من القرارات الصادرة عن منظمة الأمم المتحدة في مجموعة من المجالات ذات الصلة بأمن الفضاء الإلكتروني مثل: القرار CCPCJ ١٦/ ٢/ ٢٠٠٧ من نيسان/ إبريل ٢٠٠٧ بشأن «المنع الفعال للجريمة والعدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال» (الفقرات ٧، ١٦).

المطلب الثاني: القواعد التى يجب على المجتمع الدولي اتباعها لمواجهة الجرائم الإلكترونية

في ظل تنامي توسع وخطورة الجرائم الإلكترونية وعالميتها نادى فقهاء القانون الجنائي في بعض الدول إلى التدخل بتعديل بعض النصوص القائمة أو وضع نصوص جديدة تتلاءم وتلك الجرائم، ونادى القضاء أيضًا إلى التوسع في تفسير النصوص الجنائية السارية (سلامة، ٢٠٠٦). مع مراعاة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة في صورته التقليدية، وعلى أن يتم هذا التطور في إطار القانون وكفالة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وأن يتكامل هذا التطور في الدور والهدف مع المعاهدات الدولية. والمبادئ التى يتحتم على المجتمع الدولي مراعاتها لتحقيق التكامل الأمثل لمكافحة ظاهرة الجرائم الإلكترونية هي:

أولًا: ضرورة الاتفاق على تحديد مبدأ الطبيعة القانونية للجريمة الإلكترونية

وذلك باعتبار أن المال المعلوماتي ينقسم إلى نوعين منفصلين وفقًا لطبيعته، فهو إما مال معلوماتي ذو طبيعة معنوية، ويتمثل في البرامج والمعلومات أيًّا كان نوعها، وإما أن يكون المال المعلوماتي ذا طبيعة مادية، ويتمثل في أدوات وآلات الحاسب الآلي الملموسة؛ إذ قد يترتب على اختلاف هذه الطبيعة القانونية للمال المعلوماتي اختلاف في النتائج المترتبة على تطبيق بعض نصوص القانون الجنائي التقليدي؛ ولذلك ظهرت هذه الخلافات الفقهية وتبعها في ذلك عدم استقرار الأحكام القضائية، فالاعتداء على برامج

ومعلومات الحاسب الآلي يجعلنا أمام مشكلة قانونية ذات طبيعة خاصة تتطلب البحث في تطبيق الجزاء الجنائي الواجب في حالة الاعتداء على المال المعلوماتي المعنوي أي المحتوى الداخلي للشريط المغنط أو الأسطوانة الممغنطة، وهي ما سميت في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات، وهي جريمة مستحدثة تناولها المشرع الفرنسي بموجب القانون رقم ١٩ لسنة ١٩٨٨ بشأن بعض جرائم المعلوماتية في مادته ٤٦٢/ ٢. ومن خلال تحديد الطبيعة القانونية للمال المعلوماتي المعتدى عليه، يمكن تحديد الطبيعة القانونية للجريمة الإلكترونية والوضع القانوني للبرامج والمعلومات، وهل لها قيمة في ذاتها أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها بأي طريقة كانت.

ثانيًا: تفعيل التطور الحاصل في مبدأ نطاق تطبيق القانون الجنائي الوطني من حيث المكان

أتاح التقدم العلمي الحديث وتطور وسائل الاتصال الحديثة كالإنترنت وسائر صور الاتصال الإلكتروني عبر الأقمار الاصطناعية، صورًا كبيرة للخروج على مبدأ الإقليمية، وتبني مدونة جديدة لفض مثل هذا التنازع أو على الأقل ترتيب معاييره؛ لأن معيار إقليمية القانون لم يعد هو المعيار الوحيد، ولا ربما الأكثر قبولًا في بعض الجرائم، بل ازدادت أهمية معايير أخرى كانت فيما مضى تعد احتياطية كمعيار العينية ومعيار العالمية؛ وظهرت الأهمية البالغة لمبدأ المحاكمة أو التسليم ولو في صورته المعكوسة: التسليم أو المحاكمة، ويمثل تسليم المجرمين مظهرًا من مظاهر التعاون الدولي في مكافحة ظاهرة الإجرام، فتقوم دولة من الدول بمطالبة دولة أخرى بتسليمها شخصًا ينسب إليه ارتكاب جريمة أو صدر حكم بالعقوبة ضده حتى تتمكن الدولة الطالبة ـ باعتبارها صاحبة الاختصاص من محاكمته أو من تنفيذ العقوبة الصادرة في حقه. ويستمد النظام القانوني لتسليم المجرمين مصدره أحيانًا من أحكام التشريع الوطني، ولكن الغالب يكون مصدره الاتفاقيات الدولية أو شبه الدولية أو الثنائية، وقد يستند التسليم إلى قواعد القانون الجنائي الدولي أو العرف الدولي أو اتفاق المعاملة بالمثل. والتسليم أكثر جدوى لإدارة إستراتيجية مكافحة الجرائم الإلكترونية، ولا تتأكد فاعليته إلا بتحقق أمرين أولهما: تجاوز اعتبارات السيادة القضائية ولو بقدر ضرورات التعاون الدولي؛

ثانيهما: قيام التشريعات الوطنية بتفعيل هذا التعاون وتنظيمه وفق ما تقتضيه المعاهدات الدولية ذات الصلة (المقصودي، ٢٠١٢).

ويذهب الفقه والقضاء، وخاصة في فرنسا إلى أنه لا يقتصر تحديد مكان وقوع الجريمة على الحالات المعروفة، بل إنهما يميلان إلى التوسع في تحديد مكان وقوع الجريمة الذي من مظاهره تدويل فكرة مكان وقوع الجريمة من حيث الواقع، واعتبار كل دولة مختصة بنظر هذه الجريمة، ويمكن رصد مظاهر ذلك التوسع في مجال الجرائم الوقتية متعدية الآثار، فعلى الرغم من تنفيذ الجريمة على إقليم دولة فإن آثار هذه الجريمة قد تتعدى حدود دولة التنفيذ، ولم يتنكر القضاء الفرنسي لانعقاد اختصاصه بنظر مثل هذه الجريمة؛ لكون آثارها قد تحققت على الإقليم الفرنسي، كما في إحدى جرائم النشر التي وقعت بواسطة صحيفة تم طبعها وتوزيعها في دولة أجنبية، لكن بعضًا من نسخها قد وزع في فرنسا (Casa, 2011:55)، كما أجاز القانون والقضاء الفرنسيان نظر جريمة اعتداء على الملكية الفكرية وقعت في الخارج متى كانت آثارها قد تحققت في فرنسا (V.Casa,1987)، ولذلك فالحل الأمثل لتجاوز مبدأ الإقليمية هو في القانون الدولي بحيث يمكن أن يتشكل من خلال توافق الآراء على الصعيد الدولي باتجاه السماح بتنفيذ إجراءات الملاحقة للجرائم الإلكترونية في مجال إقليم دولة أخرى حال توافر ظروف معينة يتم تحديدها، كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتية، ووفقًا لذلك أصدر المجلس الأوروبي في ١١ سبتمبر ١٩٩٥ توصية من بين عدة توصيات تناولت مشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، جاء فيها أن تفترض إجراءات التحقيق مد إجراءات إلى أنظمة حاسب آلي آخر قد تكون موجودة خارج الدولة، وتفترض التدخل السريع، وحتى لا يمثل مثل هذا الأمر اعتداء على سيادة الدولة أو القانون الدولي، وجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة ملحة لإبرام اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات؛ كما يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة، ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط، ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية وتحديد مصدرها، وهذا كله لا يتأتى إلا بتفعيل

اتفاقيات التعاون الدولي وتكريسها (البشرى، ٢٠٠٠). وفي نظري أن مبدأ العالمية، يمكن أن يكون هو الملائم لمعظم الجرائم الإلكترونية التي يتوزع النشاط المكون للركن المادي لها في أكثر من دولة، ثم يلحقه في أولوية الترتيب مبدأ الشخصية في شقه الإيجابي، بحيث ينعقد الاختصاص بنظر الجريمة للدولة التي يحمل جنسيتها مرتكب هذه الجريمة، فإن تعددت جنسياته، فيكون من حق الدول التي يحمل جنسياتها حتى لا يأخذ البعض من اكتساب جنسية جديدة سبيلًا للإفلات من الملاحقة، كما يمكن اللجوء إلى هذا المعيار تفاديًا لإفلات المتهم من الملاحقة حين لا يتيسر ملاحقته وفقًا لأي من المعايير السابقة.

وفي هذه الحالة يتطلب الاعتراف بمبدأ المحاكمة أو التسليم كما يقتضي (العريان، ٢٠٠٤) وكذلك الاعتراف بإمكانية إحالة الدعوى الجنائية عن الجريمة الواقعة من دولة إلى أخرى، مع تأكيد ضرورة تبادل جميع أشكال المساعدة القانونية ـ بموجب اتفاقيات ـ بين الدول، وعلى وجه الخصوص فيما يتعلق بالحصول على شهادات الأشخاص، وتبليغ الأوراق القضائية، وفحص الأشياء، وتبادل الأدلة، واللجوء إلى الإنابة القضائية، ويتم ذلك وفقًا لقانون الدولة المطلوب منها مباشرة هذه الإجراءات أي الدولة المستنابة، وليس طبقًا لقانون الدولة التي أنابتها، ولا شك أن خلق آليات جديدة نشطة من جانب الأمم المتحدة في إطار من المساعدة المادية والتقنية، وتبادل الخبرات وإعداد قواعد بيانات، تمكن الجميع من الإسهام بفاعلية في مكافحة الجرائم الإلكترونية (لطفي،٢٠٠٧).

ثالثًا: تضمين بعض صور الإسهام في دورها وآثارها واعتبارها من قبيل الجرائم المستقلة

إن شرط اكتمال البناء القانوني لبعض الأنشطة الإجرامية يستند إلى قيام جريمة أصلية سابقة عليها، كجريمة الاعتداء على الملكية الفكرية، وجريمة تسلم أو إخفاء أشياء مسروقة أو محصلة بأي وجه من الوجوه من جريمة كبيرة أو جرائم عادية (أي المتحصلة من مصدر غير مشروع الذي يشكل الجريمة الأصلية)؛ فثمة قوانين وطنية تعاقب على مثل هذه الأنشطة بوصفها من قبيل المساهمة التبعية في الجريمة الأصلية، بمعنى أن مصير ملاحقة مرتكبيها وعقابهم يكون متوقفًا على مصير ملاحقة وعقاب الفاعلين الأصليين للجريمة الأصلية، وقد تتعذر ملاحقتهم لعدم خضوعهم للاختصاص الإقليمي للدولة التي ارتكبت عليها الجريمة التبعية، وهو نهج يترتب عليه التقليل من الحماية الجنائية،

ويضعف من نظام الملاحقة، على عكس لو اعتبرت هذه الأنشطة جرائم مستقلة بذاتها، وليست من جرائم المساهمة التبعية (عبد الباقي، ٢٠٠١، ١٥٨)، وذلك من شأنه التقليل مـــن فرص الإفلات من الملاحقة والعقاب أمام مرتكبـــي مثل هذه الجرائم، إضافة إلى أن يكون لهذه الأنشـــطة مدة تقادم خاصة بها، تعطي مدة زمنية أطول للملاحقة، كما لا ينحصر الاختصاص القضائي بنظرها في الدائرة التي وقعت فيها الجريمة الأصلية، بل حسب القاعدة العامة في تحديد الاختصاص.

رابعًا: إمكانية تحديث نظام تقادم الجرائم والعقوبات

يعد نظام تقـــادم الجرائم والعقوبـــات في وضعه الحالي وســـيلة لمرتكبي الجرائم والمحكومين للإفلات مـــن الملاحقة أو تنفيذ الأحكام، وللحد من اختراق ثغرات هذا النظام ينبغي تجريم بعض الأنشطة كالجرائم التبعية باعتبارها جرائم ذات طبيعة مستقلة كما ســـبقت الإشارة، على الأقل فيما يتعلق بالقواعد المنظمة لتقادم الجرائم الإلكترونية، وكذلك اعتبار الجريمة الإلكترونية مرتكبة في وقت اقتراف الســـلوك أو وقت حدوث النتيجة الإجرامية، أي اعتبار تاريخ السلوك، وكذلك تاريخ حدوث النتيجة الإجرامية كنقطة بداية لسريان مدة التقادم، أو باعتبار بعض الجرائم الإلكترونية من قبيل الجرائم المســـتمرة، بما يكفل مدة تقادم أطول، وأخيرًا رفع تباين التشريعات الوطنية فيما يخص تحديد مدة التقـــادم وتدقيق فكرة انقطاعه ووقفه، والجدير بالذكر أن القواعد العامة في الفقه الإسلامي على الأغلب من الفقهاء لا تعتد بالتقادم (عوض، ١٩٩٣).

خامسًا: ضرورة الإقرار في بعض الحالات بحجية التشريعات والأحكام الجنائية غير الوطنية

القاعدة العامة هي تلازم الســـيادتين التشريعيـــة والقضائية في المجال الجنائي، بما يعني أن كل دولة لا تعترف ســـوى بأحكام قانونها الجنائي الوطني، ولا تعتد ولا تنفذ على إقليمها ســـوى الأحكام الجنائية الصادرة عن إحدى محاكمها الوطنية، ويجد ذلك ســـنده في أن تطبيق القانون الجنائي الذي يعد تعبيرًا عن ســـيادة الدولة بوصفه يحمي المصالح الأساســـية للمجتمع والدولة والحقوق الجوهرية لأفراده، إضافة إلى أن قواعد

القانــون الجنائي تتعلق في جملتها بالنظام العام، وهو ما يحول دون الخضوع لحكم قانون أجنبــي وتطبيقه، وإذا كان القاضي الوطني يمكنــه تطبيق أحكام قانون أجنبي في مجال القانون الدولي الخاص، فإن ذلك راجع إلى أن قواعد القانون الأخير لا تتعلق بحســب الأصل بفكرة النظام العام، بل تحمي مصالح خاصة مدنية أو تجارية أو مسائل الأحوال الشخصية.

ونظرًا لعالمية الجرائم الإلكترونية وخطورتها العابرة للقارات، فإنني أرى أنه حان الوقت لتجاوز بعض المفاهيم التقليدية، وخاصة فيما يتعلق بتلازم السيادتين التشريعية والقضائيــة في المجال الجنائي، وذلك بالتوجــه نحو الاعتراف في بعض الحالات وعلى نحــو ما بالحجية للتشريــع الجنائي غير الوطني، وبحجية الحكــم الجنائي الصادر عن محاكم دولة أخرى، وتتجلى أهمية ذلك على وجه الخصوص في مجال الجرائم التبعية التي تفترض ارتكاب جريمة أصليــة على إقليم دولة ما، ثم وقوع الجريمة التابعة على إقليم دولة أخرى، ومثال ذلك جريمة الاعتداء على الملكية الفكرية، وقد ظهرت أفكار تنادي بوجــوب الاعتراف فيما بين الدول بالحجية للأحكام الجنائية الأجنبية على إقليم الدول الأخرى، وحجة ذلك اســتفحال ظاهرة الجرائم الإلكترونية وضرورة تعاون دولي فيما بينها لمكافحتها حتى لا يفلت مرتكبوها من العقاب لمجرد أنهم أقاموا في دولة غير تلك التي صدر ضدهم فيها حكــم جنائي بالإدانة وصار ممكنًا الاعتراف بمثل هذه الحجية استنادًا إلى معاهدة دولية تبرم بين الدول، ولعل ما يسند ذلك انتشار استخدام الحاسب في الجرائم الإرهابية أو ما يسمى بالإرهاب الإلكتروني (الغافري، ٢٠٠٨).

الخـاتمـة

توصلت الدراسة للنتائج والتوصيات التالية:

أولًا: النتائج:

١ ـ أوضحت الدراســة أن الجرائم المعلوماتية أقل عنفًا من الجرائم التقليدية، أي أنها لا تحتاج إلى أدنى مجهود عضلي؛ بل تعتمد على الدراســة الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسوب.

٢ ـ العولمة هي حقيقة واقعية، وليس أمام الدول سوى التعامل معها للاستفادة من إيجابياتها وتجنّب سلبياتها أي تجنّب ظهور جرائم منظّمة عبر وطنية مثل: الجرائم المعلوماتية بفعل التطور في وسائل الاتصالات والتكنولوجيا.

٣ ـ الجرائم المعلوماتية جرائم عابرة للحدود؛ لأنها تقع بين أكثر من دولة؛ إذ غالبًا ما يكون الجاني في بلد والمجني عليه في بلد آخر، وقد يكون الضرر المتحصل في بلد ثالث، ما يؤدي إلى صعوبة إثبات هذا النوع من الإجرام والملاحقة القضائية؛ نظرًا إلى ما استحدثه التطور التقني من وسائل جديدة في ارتكاب هذه الجرائم، وفي ضوء هذا أصبحت الإجراءات الجنائية التقليدية في الاستدلال والتحري عن هذه الجرائم غير قادرة على مواجهة هذا النوع؛ إذ إنه من غير الممكن العثور في هذا النوع من الجرائم على دليل مادي تقليدي.

٤ ـ رأينا أن المجتمع الدولي قد بذل جهودًا دولية وإقليمية في نطاق الأمم المتحدة لمكافحة مختلف أشكال الجرائم المنظمة عبر الوطنية والجرائم التقنية.

٥ـ تظهر أهمية وضرورة التعاون الدولي وتضافر الجهود من أجل تفعيل مكافحة الجرائم الإلكترونية، وذلك بإزاله العديد من العقبات التي تعترض سبيله من أبرزها: إيجاد اتفاق عام بين الدول على مفهوم الجرائم الإلكترونية، مع محاولة وجود توافق بين قوانين الإجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم، ومعالجة النقص في مجال الخبرة لدى الشرطة وجهات الادعاء والقضاء.

٦ ـ لم يرد في نظام مكافحة الجرائم المعلوماتية في المملكة نصوص تعالج مسئولية مزودي الخدمات، فهل يسألون عما يقومون ببثه من مواد على شبكة الإنترنت؟ وهل هذه المسئولية مطلقة؟ وهل هي مشروطة بشروط معينة؟ وما مسئولية مالك الموقع؟

٧ ـ لم يعالج النظام في المملكة مسئولية الشخص المعنوي كالشركات مثلًا إذا وقعت جريمة من الجرائم المشار إليها في النظام عن طريق ممثل الشركة أو أحد العاملين لحسابها أو أحد مستخدميها. فهل يمكن حل الشركة؟ وهل يمكن قفل المنشأة؟ وهل يمكن فرض غرامة على الشركة؟

ثانيًا: التوصيات:

١ ـ زيادة استعانة الدول بعضها ببعض وبالمنظمات الدولية والإقليمية على نحو يتم فيه حشد الجهود والطاقات الوطنية والدولية جميعها لمواجهة تحديات وخطورة جرائم من نوع جديد في الأسلوب والقوة والنطاق.

٢ ـ الاستمرار في تعديل النصوص الخاصة لحماية النظام ولحماية المعلومات المتواجدة داخل النظام، إن وجد قصور في القواعد العامة في توفير الحماية المناسبة في هذا المجال، وذلك أن القانون الجنائي التقليدي لا يكفي من حيث المبدأ لمواجهة هذا الشكل الجديد من الإجرام؛ لذلك من الضرورة أن يتم التدخل لفرض حمايتها عن طريق تعديل النصوص القائمة، أو إصدار بعض التشريعات التي تهدف إلى فرض الحماية الجنائية للمعلوماتية على المستويين الداخلي والدولي.

٣ ـ تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية؛ وخصوصًا الإنتربول؛ وفي هذا المقام من الممكن أن تنضم الدول العربية إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإنترنت وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والإنترنت والعمل على دراسة ومتابعة المستجدات على الساحة العالمية.

٤ ـ إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم المعلوماتية عبر الإنترنت؛ مع تشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الإنترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي.

٥ ـ سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، وعلى وجه الخصوص النص صراحة بحجية الأدلة الرقمية وإعطائها حكم المحررات التي يقبل بها القانون كدليل إثبات.

٦ ـ تطوير نظام تقادم الجريمة الإلكترونية الذي لا يؤخذ به في النظام السعودي. مع ضرورة النص على الاعتراف بحجية الأحكام الجنائية غير الوطنية.

٧ ـ تفعيل التعاون الدولي ودور المعاهدات الدولية ومبدأ المساعدة القانونية والقضائية المتبادلة.

٨ ـ تفعيل دور الجهات الأمنية المختصة للقيام بدورها التوعوي والوقائي من الوقوع في براثن الرذيلة والممارسات الخاطئة وخاصة فيما يتعلق بجرائم المعلوماتية.

قائمـة المراجـع

أولًا: المراجع العربية

الأوجلي، سالم محمد (٢٠١١). أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دراسة مقارنة، القاهرة: دار الكتب القانونية.

البشرى، محمد الأمين (٢٠٠٠). التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد الفترة من ١ ـ ٣ مايو، الإمارات: كلية الشريعة والقانون.

بكري، سـعد الحاج (١٩٩٠). شـبكات الاتصال وتوظيـف المعلومات في مكافحة الجريمة، المجلة العربية للدراسات الأمنية والتدريب، السنة السادسة، العدد ١١، الرياض.

حجازي، عبد الفتاح بيومي (٢٠٠٧). مبادئ الإجراءات الجنائية، الطبعة السابعة، دار النهضة العربية.

رستم، هشام محمد فريد (١٩٩٥)، الجوانب الإجرامية للجرائم المعلوماتية، الإسكندرية: مكتبة الآلات الحديثة.

رمضان، مدحت (٢٠٠٩). جرائم الاعتداء على الأشـخاص والإنترنت، القاهرة: دار النهضة العربية.

سـالم، عمر (٢٠٠٣). المراقبة الإلكترونية طريقة حديثة لتنفيذ العقوبة السالبة للحرية خارج السجن، الطبعة الأولى، القاهرة: دار النهضة العربية.

سرور، أحمد فتحي (١٩٩٣). الوسـيط في قانون الإجراءات الجنائية، الطبعة السابعة، دار النهضة العربية.

سـلامة، مأمون محمد (٢٠٠٦). الإجراءات الجنائيـة في التشريع الليبي، الجزء الأول والثاني: منشورات الجامعة الليبية، كلية الحقوق.

الشنيفي، عبد الرحمن (١٩٩٤). أمن المعلومات وجرائم الحاسب الآلي، الرياض: مكتبة الملك الوطنية.

الشوا، محمد سامي (١٩٩٤). ثورة المعلومات وانعكاساتها على قانون العقوبات، القاهرة: دار النهضة العربية.

الصغـــير، جميل عبد الباقي (٢٠٠١). الإنترنت والقانون الجنائي، القاهرة: دار النهضة العربية.

ـــــــــــــ (٢٠٠١). الجوانـــب الإجرائية للجرائم المتعلقة بالإنترنت، القاهرة: دار النهضة العربية.

ـــــــــــــ (٢٠٠١). المواجهة الجنائية لقرصنـــة البرامج التلفزيونية المدفوعة، القاهرة: دار النهضة العربية.

أبو عامر، محمد زكي، القهوجي، علي عبد القادر (١٩٩٩). قانون العقوبات، القســـم الخاص، القاهرة: دار النهضة العربية.

عبد اللاه، هلالي أحمد (١٩٩٧). التزام الشاهد بالإعلام في الجرائم المعلوماتية، القاهرة: دار النهضة العربية.

ـــــــــــــ (١٩٩٧). تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، القاهرة: دار النهضة العربية.

عبـــد الباقي، جميل (٢٠٠١). المواجهة الجنائية لقرصنـــة البرامج التلفزيونية المدفوعة، القاهرة: دار النهضة العربية.

العريان، محمد (٢٠٠٤). الجرائم المعلوماتية، الإسكندرية: دار الجامعة الجديدة للنشر.

عوض، محمد محيي الدين (١٩٩٣). مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومـــات (الكمبيوتر) بحث مقدم إلى المؤتمر الســـادس للجمعية المصرية للقانون الجنائي، المنعقد من ٢٥ ـ ٢٨ أكتوبر.

عيسى، طوني ميشـــال (٢٠٠٥). التنظيم القانوني لشبكة الإنترنت، بيروت، دار صادر للمنشورات.

الغافري، حسين بن سعيد (٢٠٠٨). جرائم الإنترنت بين الشريعة والقانون، القاهرة: دار النهضة العربية.

قشقوش، هدى حامد (١٩٩٧). جرائم الحاسب الإلكتروني في التشريع المقارن، القاهرة: دار النهضة العربية.

ـــــــــــــ، (٢٠٠٠). الإتلاف العمدي لبرنامج وبيانات الحاسب الآلي، بحث مقدم لمؤتمر (القانون والكمبيوتر والإنترنت) المنعقد في الفترة من ١ ـ ٣ مايو بكلية الشريعة والقانون بدولة الإمارات.

لطفي، محمد عبد الحميد (٢٠٠٧). اتفاقية بودابست لمكافحة الجرائم المعلوماتية (معلقاً عليها)، الطبعة الأولى، القاهرة: دار النهضة العربية.

المقاطع، محمد عبد المحسن (١٩٩٢)، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي، الكويت: ذات السلاسل للطباعة والنشر.

المقصودي، محمد أحمد (٢٠١٢). إجراءات الاستدلال والتحقيق في الجرائم الدولية وتسليم المجرمين، طبعة ١، القاهرة: الدار الهندسية.

المناعسة، أسامة أحمد وآخرون، (٢٠٠١)، جرائم الحاسب الآلي والإنترنت، الأردن، دار وائل للنشر.

هيئة الخبراء بمجلس الوزراء السعودي، (١٤٣٧). مجموعة الأنظمة السعودية، تم الحصول عليه بتاريخ ١٥/ ٩/ ١٤٣٧ /https://www.boe.gov.sa/mainlaws.aspx?lang=ar

ثانيًا: المراجع الأجنبية:

AABS (Assurance and Advisory Business Services), (1998). Second Annual Global Information Security Survey. Ernst& Young. http://www. Ey.com/security (also a PDF file)

Adeniran, A.I., 2008. The Internet and Emergence of Yahoo boys sub-Culture. International Journal of Cyber Criminology, 381-368:(2) 2;

Al Badayneh, D. (2013). Human Behavior: When and where virtual Society meets physical Society?. European Journal of Science and Theology, February 2013, Vol.9, No.1-3 ,1

Alshalan, A. (2006). Cyber-crime and Victimization. Unpublished Ph.D. Dissertation in Partial Fulfillment of the Requirements for the Degree

of Doctor of Philosophy in Sociology in Department of Sociology, Anthropology, and Social Work Mississippi State University.

Anti-Defamation League. (1999). Cyberterrorism - Terrorism Update." http://206.3.178.10/ terror/focus/16_focus_a2.html. 1999.

Aransiola, J.O., Asindemade, S.O., 2011. Understanding Cybercrime Perpetrators and the Strategies They Employ. Cyber psychology, Behaviour and Social Networking, 759:(12)14.

Arneklev, B. J., Grasmick, H. G., Tittle, C. R. and Bursik, R. J. Jr. (1993). Low Self-Control and Imprudent Behavior. Journal of Quantitative Criminology, Vol. 9, No. 3, pp. 247-225.

Arquilla, John, Ronfeldt, David and Michele Zanini. "Networks, Netwar and Information-Age Terrorism." in Zalmay M. Khalilzhad and John P. White (eds.). The Changing Role of Information in Warfare. Santa Monica, California, Rand, 1999.

BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. Organised Crime in the Digital Age. Exploring Internet Crimes and Criminal Behaviour. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Benson, M. L. and Moore, E. (1992). Are White-Collar and Common Offenders the Same? An Empirical and Theoretical Critique of a Recently Proposed General Theory of Crime. Journal of Research in Crime and Delinquency, Vol. 29, No. 3, pp. 272-251.

Britz, Marjie. 2004. Computer Forensics and Cyber Crime: An Introduction. New Jersey: Pearson Prentice Hall.