مجلة
البحوث والدراسات القضائية والقانونية

الأداة المستخدمة في ارتكاب الجريمة الإلكترونية

الأستاذ. الدكتور/ عبد الخالق صالح معزب

أستاذ القانون التجاري المشارك- جامعة صنعاء

مقدمة:

الجرائم الإلكترونية من الجرائم الوليدة التي ظهرت حديثاً مصاحبة للأنشطة والمعاملات الإلكترونية فأصبحت تهدد معاملات البشر في شتى مجالات الحياة لما تشكله هذه الجرائم من خطورة على المعلومات والبيانات ومعالجتها أو الاستفادة منها بطرق غير قانونية، وعلى الرغم من تعدد صور ارتكاب الجريمة الإلكترونية التي قد ترتكب ضد قواعد البيانات الخاصة بإحدى المؤسسات أو الشركات أو ترتكب ضد الشخص فتؤذيه في نفسه وعرضه كجريمة الإرهاب والقذف الإلكترونية وغيرها من الجرائم، على الرغم من ذلك إلاَّ أن هذه الجرائم تعتبر أكثر المهددات لمستقبل التجارة الإلكترونية الوطنية أو حتى الدولية، خاصة وأن انتشار وتتطور هذه الجرائم يزيد بسرعة كبيرة تفوق سرعة تطور وسائل مكافحتها والحد منها، كما أن هذه الجرائم تكبد المجتمعات خسائر فادحة تزيد يوماً بعد يوم بأضعاف كبيرة، وذلك- حتماً- يؤثر في مستوى الإقبال على هذا النوع من الأنشطة التجارية ويزيد من مخاوف الأطراف أثناء التعاملات والتعاقدات الإلكترونية، إضافة إلى أن الجرائم الإلكترونية تتسم بخصائص تميزها عن الجرائم التقليدية فيزيد ذلك من صعوبة مكافحتها وملاحقة مرتكبيها، حيث وبمقارنة بسيطة نجد أنه خلال عشرين عاماً انتشرت الجرائم الإلكترونية بصورة كبيرة، ففي الوقت الذي يشير تقرير مركز شكاوى احتيال الإنترنت الأمريكي أن عدد الشكاوى التي تلقاها المركز في العام ٢٠٠٢م قد بلغت (٦٠٨٧) شكوى، منها (٥٢٧٣) شكوى تتعلق باختراق الكمبيوتر عبر الإنترنت، و(٨١٤) شكوى تتعلق بوسائل الدخول والاقتحام الأخرى كالدخول عبر الهاتف أو الدخول المباشر إلى النظام[١]، بشكل مادي، وسجلت تلك الجرائم خسائر متصلة بهذه الشكاوى بلغت ما يقارب (٤,٦) ملايين دولار. منها (٢٢٪) نجمت عن شراء منتجات عبر الإنترنت دون أن يتم تسليم البضاعة فعلياً للمشترين، و(٥٪) منها نشأت عن احتيال بطاقات الائتمان[٢]، بينما بلغ عدد الشكاوى التي قدمت للمركز في العام ٢٠١٠م (٣١٤٢٤٦) شكوى، ارتفعت في العام ٢٠١١م بنسبة (٣,٤٪) فبلغت أكثر من (٣٢٤٩٣٠) شكوى[٣]، وهو رقم يزيد عن عدد الشكاوى التي قدمت في العام ٢٠٠٢م بأكثر من (٥٣)

(١) النظام هو: عبارة عن جهاز أو مجموعة من الأجهزة أو الأجزاء المرتبطة أو المتصلة مع بعضها أو ذات علاقة، والتي يقوم واحد منها أو أكثر وفقاً لبرنامج معين بوظيفة المعالجة الآلية للبيانات. الاتفاقية العالمية (الأوربية) لجرائم الكمبيوتر لعام ٢٠٠١م، المادة (١).

(٢) عرب، يونس. جرائم الكمبيوتر والإنترنت، ورقة عمل قدمت إلى مؤتمر الأمن العربي ٢٠٠٢م - تنظيم المركز العربي للدراسات والبحوث الجنائية - أبو ظبي ١٠-١٢/٢/٢٠٠٢م، ص٢.

(٣) الاحتيال الإلكتروني كلف الأمريكيين (٤٨٥) مليون دولار في ٢٠١١م، مقال نشره تلفزيون الشرقية على موقعه في شبكة الإنترنت (www.alsharqiya.com) بتاريخ ١٩/ ٥/ ٢٠١٢م.

ضعفاً، أيضاً تتزايد معدلات الخسارة بسبب هذه الشكاوى بشكل كبير فبلغت عام ٢٠٠٨م مبلغ (٢٧٩,٥) ملايين دولار، وزادت الخسارة إلى الضعف في عام ٢٠٠٩م فبلغت (٥٥٩) مليون دولار[١] أي بمعدل يزيد عليها في العام ٢٠٠٢م بأكثر من (١٢٤) ضعفاً، وبمقارنة ذلك بحجم الجرائم الإلكترونية التي سجلت في أمريكا في العام ٢٠٢٢م (٥٣) مليون جريمة بزيادة على العام ٢٠١٩ بنسبة (٣٥٨٪) وبلغت خسائر الجرائم الإلكترونية حول العالم (٧٨٧٦٧١) دولاراً في الساعة الواحدة، وهي أرقام تعكس مدى خطورة هذه الجرائم على العالم بأسره، خاصة وأن أغلب دول العالم لا تمتلك التقدم التكنولوجي الذي يمكنها من حماية التعاملات الإلكترونية فيها وتأمين المعلومات ليعمل على تقليل الخسائر وذلك كله يزيد من خطورة الجرائم الإلكترونية على أمن التعاملات الإلكترونية والتجارة الإلكترونية على وجه الخصوص، وحتى على مستوى الدول الغنية حيث تشير إحصائية سعودية -على سبيل المثال- إلى أن (١٣٨٦٦) جريمة إلكترونية قد رصدت من قبل السلطات في العام ٢٠٢٢م، كان أبرزها ابتزاز الكتروني، واحتيال إلكتروني، وسرقة إلكترونية، واختراق، وتضاعفت في الأردن بقدر (٦) أضعاف عنها في العام ٢٠١٥م لتصبح في العام المنصرم ٢٠٢٣م أكثر من (١٦) ألف جريمة إلكترونية، وتشير بعض الدراسات إلى أن خسائر الجرائم الإلكترونية سوف تكون في العام ٢٠٢٥ أكثر من (١٠) تريليون دولار وأن هذه الجرائم تزداد بنسبة (١٥٪) سنوياً، وهذه أرقام مخيفة خاصة وأن المجرم يستطيع ارتكاب جريمته عن بعد وذلك يشكل صعوبة في ملاحقته أمنياً، وهو الأمر الذي جعلنا نسلط الضوء في دراستنا هذه على هذا النوع من الجرائم والتي سوف نفصلها في هذه الدراسة من خلال تقسيم الدراسة إلى مطلبين، نخصص المطلب الأول للحديث عن تعريف الجريمة الإلكترونية وخصائصها، ونتحدث في المطلب الثاني عن الأداة المستخدمة في ارتكاب الجريمة الإلكترونية.

(١) (٥٥٩) مليون دولار تكبدها الأمريكيون في ٢٠٠٩م بسبب جرائم الاحتيال عبر الانترنت، نقلًا عن سان فرانسيسكو الألمانية مقال منشور على شبكة الإنترنت (www.swalif.net) بتاريخ ٦/ ٤/ ٢٠١٠م.

المطلب الأول
تعريف الجريمة الإلكترونية وخصائصها

تعريف الجريمة الإلكترونية:

لا يخرج مفهوم الجريمة الإلكترونية[1] بشكل عام عن وصف الجريمة التقليدية إذ أن كل فعل يرتكب بالمخالفة للقانون يعتبر جريمة، وبذا فإن الجرائم الإلكترونية هي أفعالٌ ترتكب بالمخالفة للقوانين المتعلقة بتجريم بعض الأفعال الإلكترونية. لكن الاختلاف بين الجريمة التقليدية والجريمة الإلكترونية يتمثل في اختلاف أداة تنفيذ هذه الأخيرة، فبينما يستخدم الجاني لتنفيذ الجرائم العادية أو الجرائم التقليدية أدواتٍ صناعية تساعد على ارتكاب الجريمة كالأسلحة وأدوات فتح الأبواب والخزائن وغيرها، فإن الجاني في الجريمة الإلكترونية يستخدم أدوات ليست بالمعاول ولا بالأسلحة أو المفكات، بل أدوات إلكترونية تقترب في صفاتها من صفات المعلومات والبيانات والمواقع الإلكترونية.

كما تختلف الجرائم الإلكترونية عن الجرائم التقليدية في أن الجرائم الإلكترونية تتعدد نتائجها مع اتحاد موضوعها بعكس الجرائم التقليدية التي تتنوع نتائجها بتنوع موضوعاتها، فبينما نجد أن الجرائم التقليدية ترتكز نتائجها على مواضيع متعلقة بتلك النتائج مثل السرقة تتعلق بموضوع المال والقتل ويتعلق بموضوع النفس البشرية وما دون النفس، ويتعلق موضوع السرقة بمحلها وهو المال، وموضوع القتل بمحلها وهي النفس، وغيرها من الجرائم التقليدية، نجد في الجرائم الإلكترونية تتعدد النتائج وصور الجرائم إلى جرائم عديدة منها ما يتعلق بالشرف ومنها ما يتعلق بالمال ومنها ما يتعلق بالإرهاب وغيره بينما موضوع هذه الجرائم كاملة مرده واحد وهو التلاعب بالمعلومات فقط.

---

(١) يطلق عليها البعض اسم جرائم التقنية العالية أو جرائم تقنية المعلومات (Cyber Crime) كما في قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم ٢ لسنة ٢٠٠٦م، ، ويطلق عليها البعض تسمية جرائم أصحاب الياقات البيضاء (White Collar) www.alsharq.net.sa، كما يسميها آخرون بجرائم الكمبيوتر والإنترنت www.f-law.net، كما أطلق عليها مصطلح جرائم الانترنت (Internet Crimes) في مؤتمر جرائم الإنترنت الذي انعقد في استراليا للفترة من ١٦- ١٩٩٨/٢/١٧م. إلا أن مصطلح الجرائم الإلكترونية يعد أكثر شمولاً من مصطلح جرائم الإنترنت لأن في بعض الحالات قد ترتكب جرائم واقعة على المعلومات الرقمية أو الإلكترونية دون استخدام شبكة الإنترنت، كسرقة وتدمير بعض المعلومات من جهاز الكمبيوتر، أو وقوع جريمة إلكترونية عبر شبكة ربط واتصال داخلية (local area network) كشبكة الـ»الإنترانت» أو باستخدام بعض أجهزة الاتصال المحمولة التي تستطيع الاتصال مع بعضها بدون رابط شبكي يربط بعضها البعض عن طريق إحدى شركات الاتصال وغيرها.

لم يرد في غالب القوانين[1] تعريف محدد لوصف الجريمة الإلكترونية لكن الفقه بدوره قد وضح ماهية هذا النوع من الجرائم وفي ذلك عرف الفقيه الألماني »تيدمان« (Tiedemann) الجريمة الإلكترونية أو جريمة المعلوماتية على أنها تشمل كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي (الكمبيوتر)[2].

كما عرفها الفقيه الفرنسي (Leslie D.Ball)على أنها: كل فعل إجرامي يستخدم الحاسوب فيه كأداة رئيسية.

أما الفقيه (Totty et hardcastle) فيعرفها على أنها تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسب، وبعبارة أخرى هي الجرائم تلك الجرائم التي يكون دور الحاسب فيها إيجابياً أكثر منه سلبياً[3].

كما أن غالب الفقه العربي يعرف هذه الجرائم على أنها: تلك الجرائم التي لا تعرف الحدود الجغرافية والتي يتم ارتكابها بأداة هي الحاسب الآلي (computer) عن طريق شبكة الإنترنت وعن طريق شخص على دراية فائقة بها[4].

غير أننا نلاحظ على هذا التعريف ما يلي:

١. أنه تضمن وصفاً للجريمة الإلكترونية أكثر من تضمنه تحديداً واضحاً لمفهومها، فمن المعروف أن الجريمة لا ترتبط أو تتقيد بحدود ومساحات جغرافية لبلد معين، إذ أنها جرائم لا وجود مادي لها، لكن التعريف لم يبين ماهية الجريمة الإلكترونية، وما هو الفعل الذي يمكن أن يوصف ارتكابه بالجريمة الإلكترونية.

٢. اشترط التعريف السابق لقيام جريمة الإنترنت ارتكاب الجريمة بواسطة شخص يتمتع بدراية فائقة بالإنترنت والكمبيوتر، وذلك يضيق من وصف جريمة الإنترنت إذ أنه

---

(١) أوردت بعض القوانين تعريفاً لمعنى الجريمة الإلكترونية مثل القانون السعودي الذي أورد في المادة الأولى من المرسوم الملكي رقم م/١٧ لسنة ١٤٢٨هـ بشأن نظام مكافحة جرائم المعلوماتية تعريفاً للجريمة الإلكترونية تحت مسمى جريمة المعلوماتية فعرفها على أنها: (أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام)، ونلاحظ أن القانون السابق لم يخرج عن قول الفقهاء في تعريفه لجريمة المعلوماتية أو الجريمة الإلكترونية في اعتبار الحاسب الآلي (الكمبيوتر) أداة رئيسة لارتكاب مثل هذه الجرائم.

(٢) قارة، آمال. الجريمة المعلوماتية، بحث مقدم لنيل درجة الماجستير في القانون، جامعة الجزائر، الجزائر، ٢٠٠٢م، ص١٨.

(٣) المرجع السابق، ص١٨.

(٤) الجنبيهي، منير محمد. الجنبيهي، ممدوح محمد، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، ٢٠٠٦م، ص١٣.

من حيث الأصل ينفي الجريمة عن الشخص الذي ارتكبها بالصدفة، أو كان على غير دراية بالشبكة أو ارتكبها بواسطة شخص آخر له دراية بالإنترنت أو الكمبيوتر في حين أن كافة التشريعات تتفق على عدم اشتراط الخبرة لوصف الفعل بالجريمة إذا توافرت كافة أركان قيامها من الركن المادي والركن المعنوي والنص المجرم للفعل، هذا من ناحية ومن ناحية أخرى أنه أصبح بالإمكان الاتصال بشبكة الإنترنت بواسطة أجهزة أخرى غير الحاسوب مثل أجهزة التلفزيونات والهواتف السيارة[1]، كما أن الجريمة قد ترتكب من غير وجود شبكة الإنترنت كالاعتداء على ممتلكات الغير المخزنة في جهاز الحاسوب الشخصي الخاص به، وبالتالي فان وجود مثل هذا الشرط في التعريف يضيق من نطاق وصف الفعل المرتكب عبر شبكة الإنترنت بالجريمة حتى وإن توافرت أركان قيام الجريمة الثلاثة المذكورة سابقاً.

التكييف القانوني للجرائم الإلكترونية:

انقسم الفقه بشأن التكييف القانوني للجرائم الإلكترونية إلى قسمين:

القسم الأول: يرى فقهاء هذا القسم[2] أن المعلومات والبرامج الموجودة على جهاز الحاسوب ما هي إلا عبارة عن طاقة كهربائية، وبالتالي فإن تنظيمها يدخل ضمن الأحكام التي تنظم الطاقة الكهربائية، ويتم التعامل معها على هذا التصنيف بصفتها أموالاً منقولة، فتسري عليها أحكام القوانين الجنائية وقوانين العقوبات الخاصة بالأموال المنقولة، وتشمل الطاقة الكهربائية الإشعاعات والبرامج والمعلومات الموجودة داخل جهاز الحاسوب، ومن هذه القوانين القانون العراقي والأردني والليبي الذي نص هذا الأخير في المادة (٤٤٤) عقوبات على أنه: (يعد في حكم المنقولات في قانون العقوبات الطاقة الكهربائية وجميع أنواع الطاقة ذات القيمة الاقتصادية)[3].

---

(١) سارعت بعض التشريعات إلى تلافي هذه الثغرة فعرفت جهاز الحاسوب تعريفاً واسعاً ليشمل أي جهاز إلكتروني يمكنه أن يؤدي وظائف إلكترونية مثل التشريع السعودي الذي أورد تعريف الحاسب الآلي على أنه: أي جهاز إلكتروني ثابت أو منقول، سلكي أو لا سلكي، يحتوي على نظام معالجة البيانات أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها يؤدي وظائف محددة بحسب الأوامر والبرامج المعطاة له. المرسوم الملكي السعودي رقم م/١٧ لسنة ١٤٢٨هـ بشأن نظام مكافحة جرائم المعلوماتية، المادة (٦/١).

(٢) الهيتي، محمد حماد مدهج. الصعوبات التي تعترض تطبيق نصوص جريمة السرقة على برامج الحاسب الآلي، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد ٢٠، ذي القعدة ١٤٢٤هـ، يناير ٢٠٠٤م، ص٨٩.

(٣) قانون العقوبات الليبي لسنة ٢٠٠٨م، المادة (٤٤٤).

القسم الثاني: يرى أن هذه الجرائم تتميز بالحداثة وبالتالي لا يمكن تصنيفها على أنها أموال منقولة، إذ أنها أقرب ما تكون إلى الحقوق الفكرية والذهنية منها إلى الأموال المنقولة، وقد أيدت كثير من التشريعات هذا الرأي ودرجت على إفراد قوانين خاصة لتنظيم هذه الجرائم، مثل القانون المصري والإماراتي والسوداني وغيرها.

ولعل ما ذهب إليه القسم الثاني هو الأرجح، فقد ظهرت الجرائم الإلكترونية بكيانها المستقل عن جرائم الأموال ومميزاته الخاصة التي جعلت المشرعين يضعون ذلك في حسبانهم عند وضع القواعد المنظمة لأحكام هذه الجرائم باعتبارها جرائم مستقلة لها محيطها الخاص وقالبها القانوني الخاص.

خصائص الجريمة الإلكترونية:

تتمتع جرائم الإنترنت أو الجريمة الإلكترونية بعدة خصائص تميزها عن الجرائم العادية تجعلها تحتاج بالضرورة لتنظيم خاص يتوافق مع سمات هذه الخصائص، ومن أهم خصائص الجرائم الإلكترونية التالي:

١. من الجرائم الذكية: فلا يمكن للشخص العادي الذي لا يمتلك الخبرات والمهارات في استعمال والتعامل مع أجهزة الحواسيب وشبكة الإنترنت أن يقوم بارتكاب هذه الجرائم، ولكن نلاحظ أن هذه الخاصية لا تنفي الجريمة عن الشخص الذي يفتقر إلى الخبرة في التعامل مع جهاز الحاسوب والشبكة إذا توافرت أركان قيام الجريمة، إنما قد تكون نوعاً من أنواع الحماية الذاتية للتعاملات الإلكترونية بين الأطراف.

٢. جرائم حديثة: فوجودها نتيجة لتطور تكنولوجيا المعلومات ومرتبط بها إذ أن الجريمة الإلكترونية لا تقع على أشياء مادية ولا يكون موضوعها إلحاق الضرر بالموجودات الفيزيائية، إنما تعتبر البرامج الإلكترونية وأنظمة المعلومات والبرامج الحاسوبية وشبكة الإنترنت هي مسرح هذه الجرائم، كما أنها جرائم متنوعة عديدة لا يمكن حصرها وإن كانت بعض التشريعات قد أدرجت تسميات لبعض الجرائم الإلكترونية، إلا أنه لا يمكن في الواقع حصر هذه الجرائم والسبب في ذلك كما ذكرنا يعود إلى ارتباط هذه الجرائم بتكنولوجيا المعلومات وتطور الاتصالات التي لا يكاد يمر بعض الزمن حتى نسمع بتكنولوجيا حديثة ظهرت للبشرية.

٣. جرائم الحاسوب والإنترنت من الجرائم الخطيرة: ونقصد بذلك مدى عواقب هذه الجرائم ونتائجها ليس على المجني عليه أو الشخص المتضرر جراء ارتكاب هذه

الجرائم فحسب، بل على المجتمع ككل خاصة مع ازدياد توجه الدول بكافة مؤسساتها للتعامل الإلكتروني واعتمادها الكلي على شبكة الإنترنت لتسيير مرافق الحياة فيها، وبالتالي فإن الجرائم الإلكترونية تشكل تهديداً لكافة مرافق الحياة بالدولة، فقد أظهرت نتائج الإحصائيات التي أجرتها الجمعية الأمريكية للأمن الصناعي الأمريكي الخسائر التي قد تسببها جرائم الحاسب الآلي للصناعات الأمريكية قد وصلت إلى ثلاثة وستين بليون (٦٣,٠٠٠,٠٠٠,٠٠٠) دولار أمريكي في العام ١٩٩٨م، وأنّ ما يمكن تقدير نسبته بـ(٢٥٪) من الشركات الأمريكية تتضرر من جرائم الحاسب الآلي، وأظهرت دراسة أخرى أجرتها منظمة (Business Software Alliance) أن خسائر المملكة العربية السعودية التي تسببت فيها الجرائم الإلكترونية أو جرائم الإنترنت بلغت في العام ١٩٩٨م ثلاثين مليون (٣٠,٠٠٠,٠٠٠) دولار[١].

٤. جرائم بعيدة عن المراقبة الأمنية: ونقصد بذلك قصور الأجهزة الأمنية في توفير الحماية اللازمة للمعلومات الإلكترونية، وهذا القصور يرجع لعوامل عديدة كطبيعة شبكة الإنترنت التي تعتبر منطقة بلا قانون من جهة، ومتطلبات الخبرة والمهارة اللازمتين لدى أجهزة الدولة لحماية المعلومات من جهة أخرى، خاصة وأن الجرائم الإلكترونية من الجرائم التي لا تترك أي أثر مادي وراءها يستدل به على مرتكبها، أضف لذلك أن الجرائم الإلكترونية جرائم لا يمكن التنبؤ بها (can't be predicted) وذلك يجعل من مهمة وضع التدابير الاحترازية لحماية المعلومات والتعاملات الإلكترونية أمراً في غاية الصعوبة، فكثيراً ما نسمع عن خسائر كبيرة تكبدتها الدول العظمى جراء الجرائم الإلكترونية رغم التقدم التكنولوجي الذي تعيشه هذه الدول، كما أن الجرائم الإلكترونية توفر لمرتكبها الأمان من ناحيتين، الأولى: عدم الحاجة لاستخدام القوة أو العنف والمخاطرة أو الانتقال إلى مسرح الجريمة لإتمامها، فيمكن ارتكاب جريمة إلكترونية في الولايات المتحدة الأمريكية بواسطة شخص يوجد في روسيا دون الحاجة لانتقال الجاني لأراضي الولايات المتحدة الأمريكية، وهذا ما يشكل صعوبة حقيقية في ملاحقة الجاني. الثانية: تتمثل في الفارق الزمني المناسب الذي يحصل عليه الجاني بين ارتكاب جريمته وبدء ملاحقته، فالكثير من الجرائم الإلكترونية لا يتم اكتشافها إلا عن طريق الصدفة لعدم معرفة الأطراف والجهات ذات العلاقة

(١) الجنبيهي، ممدوح. والجنبيهي، منير. مرجع سابق، ص، ١٩. وأيضاً: جرائم الانترنت من منظور شرعي وقانوني، بحث منشور على شبكة الإنترنت على الرابط: www.adawy.bavr.org/t٨١٩-topic»، فبراير، ٢٠١١م.

كالأجهزة الأمنية وغيرها بوقوع الجريمة، أو لعدم معرفة الجاني أو المجني عليه، أو بعد مدة زمنية من ارتكابها، يكون الجاني خلالها قد استفاد منها في ارتكاب جرائم أخرى أو تأمين نفسه من الملاحقة الأمنية[1].

٥. جرائم متنوعة: فلا تتخذ الجرائم الإلكترونية مسلكاً معيناً ليتم تصنيفها على أساسه[2]، بل تتنوع هذه الجرائم فمنها ما يقع على الشخص كالقذف والسب والتشهير والتهديد والاستدراج وغيرها، ومنها ما يقع على الأموال كالسرقة والاختلاس وتزوير المستندات، ومنها ما يقع على المجتمع كالمساس بالنظام العام والقيم أو المعتقدات الدينية أو الإرهاب الإلكتروني أو الترويج للبغاء وغيرها. كما أن الجرائم الإلكترونية تعتبر جرائم متنوعة الدوافع أيضاً فقد ترتكب هذه الجرائم لدوافع شخصية كإحساس مرتكبيها بالقوة وبقدرة الذات على اختراق المواقع وتدميرها أو العبث بمحتوياتها رغبة في تحقيق الذات والقدرات الذهنية، أو الحقد والكراهية أو الانتقام أو غيرها من الدوافع، أو كمحاولة لكسب المال، أو لدوافع خارجية كالرغبة في الانتقام أو التهديد أو غيرها, كما أن هذه الجرائم تتنوع في صورها أيضاً كالدخول غير المشروع والسرقة أو الإتلاف أو التجسس أو الاحتيال أو تدمير البيانات أو نقلها وغيرها.

---

(١) في كثير من الجرائم الإلكترونية لا يتم التعرف على الجاني، وبالتالي تصبح إمكانية ملاحقته قضائياً أمراً صعباً مثل ما يحدث في القنوات الفضائية التجارية التي نسمع كثيراً عن إعلانها بوجود تشويش متعمد على باقاتها بقصد قطع الإرسال أو تقليل جودته من دون أن يتم التعرف على الجاني ولا تحديد موقعه.

(٢) فالجرائم الإلكترونية كما ذكرنا تتنوع لجرائم ضد الأشخاص وجرائم ضد الحكومات وجرائم ضد الأموال والنوع الأخير هو ما يهمنا في دراستنا هذه التي تعتبر معه الجرائم الإلكترونية من أهم معوقات ومهددات قيام التجارة الإلكترونية وازدهارها، ذلك لأن الجرائم الإلكترونية المتعلقة بالأموال تهدد رؤوس أموال التجار والمتعاقدين، كما تهدد اقتصاديات البلدان بشكل عام، ومن أمثلة هذه الجرائم: سرقة معلومات الحاسب، قرصنة البرامج وسرقتها، سرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الحاسب، تزوير البريد الإلكتروني أو الوثائق والسجلات والهوية، جرائم المقامرة، تملك وإدارة مشروع مقامرة على الانترنت، الحيازة غير المشروعة للمعلومات، إفشاء كلمة سر الغير، إساءة استخدام المعلومات، نقل معلومات خاطئة، أنشطة اقتحام أو الدخول أو التوصل غير المصرح به مع نظام الحاسب أو الشبكة، خلق البرمجيات الخبيثة والضارة ونقلها عبر النظم والشبكات، استخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص، إدخال معطيات خاطئة أو مزورة إلى نظام حاسب، التعديل غير المصرح به في الكمبيوتر أو مهام نظم الحاسب الأدائية، أنشطة إنكار الخدمة أو تعطيل أو اعتراض عمل النظام أو الخدمات، أنشطة الاعتداء على الخصوصية، استخدام الحاسب للحصول على البطاقات المالية أو استخدامها للغير دون ترخيص أو تدميرها، الاختلاس عبر الحاسب أو بواسطته، استخدام الانترنت لترويج الكحول ومواد الإدمان للقصر. وغيرها من الجرائم التي لا حصر لها وتعتمد بصفة أساسية على الذكاء أو الخبرة في مجال المعلوماتية في ارتكابها ودراية التعامل مع الكمبيوتر أو الإنترنت. العادلي، محمود صالح. الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، جامعة الأزهر الشريف، القاهرة، ٢٠٠٩م، ص٧.

المطلب الثاني
الأداة المستخدمة في ارتكاب الجريمة الإلكترونية

من خلال التعريف المذكور في المطلب الأول وجدنا أن أيضاً كالدخول غير المشروع والسرقة أو الإتلاف أو التجسس أو الاحتيال أو تدمير البيانات أو نقلها وغيرها.

٣. كما أن التعريف السابق - يسانده آخرون[١] - يذهب إلى القول بأن الجناة الإلكترونيين - إن جاز التعبير - يعتمدون على الأجهزة الإلكترونية عند ارتكاب جرائمهم، وبناء عليه فإن جهاز الحاسوب يعتبر أداة تنفيذ الجرائم الإلكترونية أو جرائم المعلوماتية، ولكن نلاحظ على هذا القول الآتي:

١. إن الجرائم الإلكترونية تعتبر من الجرائم »اللامادية« أو الافتراضية وبالتالي لا يتطابق استخدام أدوات مادية لتنفيذ هذه الجرائم.

٢. لابد لتنفيذ الجريمة الإلكترونية من الارتباط بشبكة الإنترنت بحسب التعريف السابق، وبالتالي فإن الأداة هنا تصبح الشبكة أو الاتصال بالشبكة وليس الحاسوب.

٣. القول بأن الحاسوب أداة ارتكاب الجرائم الإلكترونية يخل بتعريف الجرائم الإلكترونية نفسها؛ إذ أن الحاسوب قد يستخدم لارتكاب جرائم أخرى ليست جرائم إلكترونية مثل جريمة التزوير التقليدية المنصوص عليها في القوانين الوطنية التي تختلف عن جريمة التزوير المعلوماتية أو الالكترونية، فعلى الرغم من أن الحاسوب يستعمل في تنفيذ كل من هاتين الجريمتين، إلا أن جريمة التزوير المعلوماتية لا تتم أو تقوم إلا إذا تعلقت بإدخال أو إتلاف أو محو أو تحوير المعطيات أو المعلومات والبيانات أو البرامج الالكترونية أو برامج الحاسوب وأثرت على المجرى الطبيعي لمعالجة البيانات وإلا عدّت من قبيل جرائم التزوير التي نصت عليها القوانين الجنائية الوطنية كتزوير البطاقة الشخصية أو جوازات السفر حتى وإن استخدم الحاسوب أداة لتنفيذها.

---

(١) الرزو، حسن مظفر. المفاهيم المعلوماتية لجرائم الفضاء الافتراضي بالحاسوب، مجلة الشريعة والقانون، جامعه الإمارات العربية المتحدة، العدد١٦ شوال ١٤٢٢هـ، يناير ٢٠٠٢م. ص٢٤٢. وذهب البعض في تعريف الجريمة الإلكترونية إلى جعل الحاسوب مرتكزاً لقيامها فعرفها على أنها: فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية. خالد، بو كثير. الجرائم المعلوماتية، مذكرة نهاية تدريب، المنظمة الجهوية للمحامين، سطيف، ٢٠٠٦م، ص٥، ٦.

٤. إشارة مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء إلى أن جهاز الكمبيوتر يستعمل لتخزين بيانات قد تكون في غاية الأهمية السياسية أو الاقتصادية أو الشخصية أو غيرها، وإلى أن الاعتداء على جهاز الكمبيوتر بالنفاذ إلى نظامه وبياناته أو برامجه ومن ثم استعمالها أو مراقبتها أو التدخل فيها بأي شكل بدون إذن يعد سلوكاً إجرامياً، ومن ذلك فإن جهاز الحاسوب يعتبر بمثابة الحرز الذي يفصل بين تكييف وتصنيف الأفعال الواقعة على محتوياته وتجريمها من عدمه.

٥. ما ذكره البعض[١] بشأن مواصفات مرتكبي جرائم تكنولوجيا المعلومات بضرورة توافر ثلاثة شروط أساسية في الشخص المرتكب للجريمة الإلكترونية, وهذه الشروط هي :

أ. المعرفة(Knowledge): بأن يكون الشخص على علم ودراية كاملة باستخدام الحاسوب وتفاصيل برامجه ولاسيما نقاط الضعف في الأنظمة المطبقة والبرامج المثبتة عليه.

ب. القدرة على اختراق وسائل التخزين (Access): لاسيما تلك التي لا تحتوي على أنظمة حماية كتشفير لبياناتها أو إخفاء أو نحوه.

ج. القابلية على استخدام الوسائل (Resources): كوسائل الاتصال وأدوات التشفير وفك التشفير وغيرها.

ومما سبق نخلص إلى أن الحاسوب لا يعتبر أداةَ تنفيذ الجرائم الإلكترونية بيد أنه يعتبر أداة اتصال بشبكة الإنترنت، وبالتالي فإن أداة ارتكاب الجرائم الإلكترونية تعتبر افتراضية كالجريمة نفسها وتتمثل بالمهارات والخبرات ولذلك نجد أن هذه الجرائم لا ترتكب إلا من أصحاب المهارات وذوي الخبرات العالية في التعامل مع الشبكة وأجهزة الحواسيب، إذ وعلى عكس ما هو الحال عليه في ارتكاب الجرائم التقليدية التي تصبح ممكنة إذا توافرت نية الجاني للإجرام وأداة التنفيذ والضحية أو المجني عليه، على عكس ذلك لا تَسْلم شبكة الإنترنت من المستخدمين والمتصفحين الذين تولدت لديهم نية الإجرام بالدخول إلى المواقع المملوكة للغير بطرق غير قانونية أو اختراق[٢] المواقع

(١) الطائي، جعفر حسن جاسم. جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، الطبعة الأولى، دار البداية، ٢٠٠٧م، عمان. ص١٥١، ١٥٢.

(٢) الاختراق : قيام شخص أو أكثر بمحاولة الوصول إلى جهاز خاص أو شبكة خاصة عن طريق شبكة الإنترنت باستخدام برامج متخصصة لفك الرموز والكلمات السرية وكسر حواجز الحماية الأمنية، واستكشاف

المالية وسرقة الأموال، وغيرها من الأفعال المجرمة، وعلى افتراض القول السابق أن الحاسوب هو أداة لتنفيذ الجريمة فنجد أنه وعلى الرغم من وجود نية الإجرام وتوافر أداة التنفيذ وهي الحاسوب إلا أن الجاني لا يستطيع ارتكاب أي جريمة معلوماتية افتراضية إذا انعدمت الأداة الحقيقية لتنفيذ الجريمة وهي الخبرة أو المهارة اللازمة لكسر حماية المواقع أو اختراقها، ومن ثم القرصنة عليها[1].

ونخلص مما سبق إلى إمكانية تعريف الجريمة الإلكترونية على أنها: ارتكاب فعل بالمخالفة للقانون عن طريق موقع إلكتروني أو نظام معلوماتي.

والموقع الإلكتروني هو: مكان إتاحة المعلومات على الشبكة المعلوماتية[2]، والمعلومات الإلكترونية هي: كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والأصوات والأرقام والحروف والرموز والإشارات وغيرها[3]، أما النظام المعلوماتي (Information system) فهو عبارة عن: مجموعة

مواصفات ضعف الجهاز، أو الشبكة، من خلال بوابات عبور للوصول إلى الملفات أو البرامج، وعند اختراق أجهزة الحواسيب الخاصة يظهر ذلك عليها بعلامات تؤثر على تشغيلها أو أدائها مثل: عرض صور مفاجئة على الشاشة أو تغيير إعدادات الشاشة نفسها، فتح وغلق باب مشغل القرص المضغوط (CD-Room)، توقف حركة معينة أو تغيير شكل معين أو الحركة العشوائية لمؤشر الفأرة (Mouse)، عرض رسائل أو نوافذ على الشاشة أو إغلاق رسائل أو نوافذ مفتوحة، تغيير إعدادات التحكم بالصوت، حركة القرص الصلب (HardDisk) لرفع ملفات إلى الشبكة أو لتنزيل ملفات إليه من الشبكة (Upload or download data and files) أو حذف ملفات من القرص نفسه. بسيوني، عبد الحميد. طرق وبرامج الهاكرز وقرصنة المعلومات، دار الكتب العلمية للنشر والتوزيع، القاهرة، ٢٠٠٤م. صـ ٢٩ ـ ٣١.

(١) ولهذا السبب يقول خبراء مكافحة الجرائم الإلكترونية أن أفضل وسيلة للتعرف على الأشخاص ذوي الميول الإجرامية هي تحليل وتقييم مهاراتهم ومعرفتهم وخبراتهم الفريدة في مجال علوم الحاسوب وتكنولوجيا المعلومات، والتي يتميز معها مقترفو جرائم الحاسوب أو الجرائم الإلكترونية عن باقي المجرمين التقليديين. الطائي، جعفر حسن جاسم، مرجع سابق، ص١٥٢.

(٢) القانون الاتحادي الإماراتي في شأن مكافحة جرائم تقنية المعلومات رقم ١ لسنة ٢٠٠٦م، المادة (١)، وقانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧م، المادة (٣). إلا أن القانون السوداني قد أضاف إلى التعريف السابق عبارة: (من خلال موقع محدد)، ولعل المشرع السوداني بذلك يشترط سوء النية في الجاني وقصد ارتكاب الفعل المخالف للقانون، وعلى الرغم من ذلك فالقانون السوداني لم يورد توضيحاً يفسر معنى عبارة (من خلال عنوان محدد) فإذا كان القصد من ذلك اشتراط وجود عنوان محدد للمجني عليه في شبكة الإنترنت، فإنه- أي القانون- قد ضيق من تجريم الأفعال التي ترتكب على شبكة الإنترنت ويمكن أن تلحق ضرراً بالآخرين لمجرد أن الجاني لم يدخل عناوين هؤلاء الأشخاص، أو أنه لا يوجد لديهم عنوان محدد على شبكة الإنترنت، أما إن كان القصد غير ذلك بمعنى أن الفعل يعد جريمة إن ارتكب بالمخالفة للقانون على أي عنوان داخل شبكة الإنترنت، حتى ولو لم يكن هذا العنوان يتعلق بالشخص المضرور أو يتبع له، فإن هذه العبارة لا تحقق أي قيمة قانونية والسبب أنه لا يمكن ارتكاب الجريمة الإلكترونية على أحد المواقع الإلكترونية إلا من خلال عنوان إلكتروني معين.

(٣) إبراهيم، حسني عبد السميع. الجرائم المستحدثة عن طريق الإنترنت، دار النهضة العربية، القاهرة، ٢٠١١م، ص٦١.

برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الإلكترونية ورسائل البيانات[١] أو غير ذلك[٢]. والتعريف السابق يشمل تجريم الأفعال التي ترتكب بالمخالفة للقانون على شبكة الإنترنت، كما يتضمن أيضاً أي فعل مخالف للقانون يضر بنظام معلوماتي معين سواء كان على شبكة الإنترنت أو على جهاز إلكتروني حتى وإن لم يكن مرتبطاً بالشبكة، كالدخول غير المشروع لأجهزة الكمبيوتر المملوكة للغير أو كسر أنظمة حمايتها وتغيير أو تعديل أو سرقة المعلومات المخزنة عليها أو تدميرها، وغير ذلك من الجرائم المرتبطة بالبرامج والمعلومات الرقمية.

مسؤولية متعهد الوصول أو مزود الخدمة:

متعهد الوصول أو مزود الخدمة هو شخص طبيعي أو معنوي يقوم بدور فني لتوصيل المستخدمين (الجمهور) إلى شبكة الإنترنت بمقتضى عقود اشتراك تضمن توصيل العميل للمواقع التي يريدها[٣].

كما تعرف اتفاقية »بودابست« بشأن الجريمة الإلكترونية مزود الخدمة بأنه: (أي هيئة عامة أو خاصة تقوم بتزويد المستخدمين بخدمه الاتصال عن طريق أنظمة الكمبيوتر أو أي هيئة تقوم بمعالجة أو تخزين بيانات الكمبيوتر نيابة عن خدمة الاتصال هذه أو مستخدمي هذه الخدمة)[٤].

---

(١) عرف القانون اليمني رقم ٤٠ لسنة ٢٠٠٦م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية في المادة الثانية منه رسائل البيانات على أنها: (مجموعة من الأوامر والأرقام التي تحتاج إلى معالجة وتنظيم، أو إعادة تنظيم لكي تتحول إلى معلومات، وقد تأخذ شكل نص الاتفاقية أو أرقام أو أشكال أو رسومات أو صور أو تسجيل أو أي مزيج من هذه العناصر).

(٢) القانون الاتحادي الإماراتي في شأن مكافحة جرائم تقنية المعلومات رقم ١ لسنة ٢٠٠٦م، والمادة (١) من قانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧م، والمادة (٣). ويشمل النظام المعلوماتي كل وسيلة مخصصة لصناعة المعلومات أو لمعالجتها أو لتخزينها أو لعرضها أو لإتلافها، يتطلب تشغيلها الاستعانة بشكل أو آخر بالوسائل الإلكترونية، كما يعنى أيضًا المعدات والآلات المعلوماتية والحاسبات الآلية والبرامج وقواعد وبنوك المعلومات والملقمات ومواقع الويب ومنتديات المناقشة والمجموعات الإخبارية وكل وسيلة معلوماتية أخرى مخصصة لصناعة أو لمعالجة أو لتخزين أو لاسترجاع أو لعرض أو لنقل أو لتبادل المعلومات. عبد المطلب، ممدوح عبد الحميد. استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر، الدليل الإلكتروني للقانون العربي (www.arablawinfo.com)، ص٥.

(٣) إبراهيم، حسني عبد السميع. مرجع سابق، ص٦٠.

(٤) any public or private entity that provides to users of its service the ability to communicate by means of computers system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service. Convention on cybercrime .Budapest, **23 -11-2001**, article **1**

وقد دار جدل فقهي حول مسؤولية مزود الخدمة عن الجرائم التي ترتكب على شبكة الإنترنت، فذهب رأي من الفقه إلى عدم تحمل مزود الخدمة لأية مسؤولية عما يجري على الشبكة، لقيامه فقط بدور فني يقتصر على توصيل الزبائن والعملاء بالشبكة، ويذهب رأي آخر إلى تحمل مزود الخدمة للمسؤولية القانونية على أساس قواعد المسؤولية المفترضة أو التوجيهية، إذ يتوجب عليه محو المعلومات أو البيانات غير المشروع تداولها وحماية المعلومات على الشبكة خاصة مع استطاعته مراقبة كل ما يجري على الشبكة عن طريقه وسهولة حجب المواقع التي يريد حجبها[1]، وتدقيق النظر في هذا الأمر يجعل من متعهد الوصول أو مزود الخدمة بمنأىً عن تحمل أي مسؤولية وذلك لعدم ارتكابه أي فعل مجرَّم قانوناً إذ لا تقوم جريمة دون ركنها المعنوي المتمثل بقصد الإجرام وارتكاب الفعل، ومجرد تسهيل مزود الخدمة لعملية وصول الجاني للإنترنت وربطه بالشبكة دون نية إجرام أو اتفاق جنائي لا يعد جريمة، فصانع الأسلحة لا يتحمل مسؤولية استخدامها غير القانوني, وشركات الاتصالات غير مسئولة عن المكالمات التي يجريها عملاؤها، وإن المساءلة القانونية لمزود الخدمة عن مساعدته للجاني في ارتكاب الجريمة الإلكترونية ليس بصفته مزود خدمة أو متعهد وصول إنما بصفته شخصاً مشتركاً في الجريمة أو متفقاً فيها.

الخاتمة:

في خاتمة هذه الدراسة توصلنا إلى عدة نتائج وتوصية نوصي بها المشرع اليمني كما يلي:

أولاً: النتائج

١- الجرائم الإلكترونية من الجرائم الوليدة والحديثة تسبب في وجودها وتطورها تطور وانتشار استخدام المعاملات الإلكترونية.

٢- تشكل الجرائم الإلكترونية خطورة على المعلومات والبيانات ومعالجتها أو الاستفادة منها بطرق غير قانونية.

٣- تعدد صور ارتكاب الجريمة الإلكترونية، ويصعب ملاحقة مرتكبيها أمنياً.

٤- تختلف الأداة المستخدمة في الجريمة الإلكترونية عن الأدوات التي يمكن أن تستخدم في الجرائم التقليدية.

(١) المرجع السابق، صـ٦١-٦٣.

ثانياً: توصية

من خلال مطالب ونتائج هذه الدراسة فإننا نوصي المشرع اليمني بسرعة سن قانون خاص بتجريم الأفعال الإلكترونية التي تسبب للغير ضرراً مادياً على نفسه أو ماله أو ضرراً أدبياً في سمعته أو غيره، حيث وأن المعاملات الإلكترونية باتت تشغل حيزاً كبيراً في المعاملات اليومية للأفراد سواء كانت تلك المعاملات تتعلق بشؤون المواطنين المدنية أو الإدارية أو التجارية.

قائمة المـراجع:

أ. كتب ومؤلفات قانونية:

١. إبراهيم، حسني عبد السميع. الجرائم المستحدثة عن طريق الإنترنت، دار النهضة العربية، القاهرة، ٢٠١١م.

٢. الجنبيهي، منير محمد. الجنبيهي، ممدوح محمد، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، ٢٠٠٦م.

٣. الرزو، حسن مظفر. المفاهيم المعلوماتية لجرائم الفضاء الافتراضي بالحاسوب، مجلة الشريعة والقانون، جامعه الإمارات العربية المتحدة، العدد ١٦ شوال ١٤٢٢هـ، يناير ٢٠٠٢م.

٤. العادلي، محمود صالح. الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، جامعة الأزهر الشريف، القاهرة، ٢٠٠٩م.

٥. الطائي، جعفر حسن جاسم. جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، الطبعة الأولى، دار البداية، عمان، ٢٠٠٧م.

٦. الهيتي، محمد حماد مدهج. الصعوبات التي تعترض تطبيق نصوص جريمة السرقة على برامج الحاسب الآلي، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، العدد ٢٠، ذي القعدة ١٤٢٤هـ، يناير ٢٠٠٤م.

٧. بسيوني، عبد الحميد، طرق وبرامج الهاكرز وقرصنة المعلومات، دار الكتب العلمية للنشر والتوزيع، القاهرة، ٢٠٠٤م.

٨. جرائم الانترنت من منظور شرعي وقانوني، بحث منشور على شبكة الإنترنت على الرابط :(topic-www.adawy.bavr.org/t٨١٩) (، فبراير، ٢٠١١م.

٩. خالد، بو كثير. الجرائم المعلوماتية، مذكرة نهاية تدريب، المنظمة الجهوية للمحامين، سطيف، ٢٠٠٦م.

١٠. عبد المطلب، ممدوح عبد الحميد. استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر، الدليل الإلكتروني للقانون العربي (www.arablawinfo.com).

١١. قارة، آمال. الجريمة المعلوماتية، بحث مقدم لنيل درجة الماجستير في القانون، جامعة الجزائر، الجزائر، ٢٠٠٢م.

ب. قوانين واتفاقيات:

١٢. Convention on cybercrime Budapest, ٢٣ -١١-٢٠٠١.

١٣. القانون اليمني رقم ٤٠ لسنة ٢٠٠٦م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.

١٤. المرسوم الملكي السعودي رقم م/١٧ لسنة ١٤٢٨هـ بشأن نظام مكافحة جرائم المعلوماتية.

١٥. القانون الاتحادي الإماراتي في شأن مكافحة جرائم تقنية المعلومات رقم ١ لسنة ٢٠٠٦م.

١٦. قانون جرائم المعلوماتية السوداني لسنة ٢٠٠٧م.

١٧. القانون الاتحادي الإماراتي في شأن مكافحة جرائم تقنية المعلومات رقم ١ لسنة ٢٠٠٦م.

١٨. قانون العقوبات الليبي لسنة ٢٠٠٨م.