مجلة
البحوث والدراسات القضائية والقانونية

الطبيعة القانونية للجريمة الإلكترونية

الباحثة / ندى عبدالله عبدالله طامش

تمهيد:

تعد الجريمة الالكترونية من الجرائم الحديثة نسبياً والتي شهدت تطوراً في الآونة الأخير، خاصة فيما يتعلق بالأساليب والطرق الفنية والتقنية...، حيث ظهر مفهوم الجريمة الالكترونية في التسعينات من القرن الماضي، فيما يخص الجرائم الإلكترونية الخاصة بالجانب المالي مثل الجرائم المالية المتعلقة بالأسواق المالية، واختراقات أنظمة البنوك وغيرها.

ونظراً لتسارع إيقاع التقدم التكنولوجي والتقني الهائل والذي أدى إلى استغلالها لتباين الذهنيات والمستويات العلمية لمستخدميها ولعدم وجود قانون متكامل- حتى الآن- يجرم جميع صور الاستخدام غير المشروع للإنترنت، الأمر الذي أدى إلى ظهور طائفة جديدة من الجرائم مختلفة عن باقي الجرائم المرتكبة عبر الإعلام الالكتروني المنظم وفقاً لقوانين الصحافة والنشر، والتي لا تنطبق على هذه الوسائل على الرغم من أنها أحد وسائط النشر ويتوافر بها ركن العلانية، فهذه الجرائم المبتكرة والمستحدثة تمثل ضرباً من ضروب الذكاء الإجرامي، الأمر الذي أثار إشكاليات التكييف القانوني لها (الفعل- السلوك الإجرامي).

والجدير بالذكر أن الجرائم الالكترونية من الجرائم العابرة للحدود، والتي لا تقتصر على دولة بعينها، إنما ترتكب في مختلف دول العالم بغض النظر عن المستوى التقني والعلمي الذي تتمتع به تلك الدولة، وقد بدأت هذه الجرائم بالانتشار بشكل كبير في الوقت الحاضر، وتلك الجرائم تتخذ صوراً وأشكالاً متعددة، ويمكن ارتكابها بشكل سهل ويسير، دون أن يتم اكتشاف مرتكبها، وذلك لطبيعة تلك الجرائم، والتي سيتم بيانها بمشيئة الله تعالى في هذا البحث.

لذلك كان لا بد للدول على مستوى تشريعاتها الوطنية أن تسعى جاهدة لمكافحة تلك الجرائم، وذلك من خلال وضع النصوص القانونية التي تهدف إلى تحقيق تلك الغاية، وهذا الأمر يتطلب كذلك منح الإدارة (الجهات الحكومية ذات العلاقة) عن طريق أجهزة الضبط الإداري بصفة عامة، والإلكتروني منها بصفة خاصة الوسائل والأدوات التي تجعلها تنهض بتلك المهمة على أكمل وجه.

أهداف البحث:

يهدف البحث إلى بيان المفردات التالية:

١- تعريف الجريمة الإلكترونية ومجالاتها وأنواعها وأساليبها.

٢- الخصائص التي تنفرد بها الجريمة الإلكترونية عن غيرها.

٣- أدوات وأساليب ارتكاب الجريمة الإلكترونية.

٤- القوانين المنظمة والقوانين ذات العلاقة بالجريمة الإلكترونية.

٥- الأدوات والوسائل المعينة على مكافحة الجريمة الإلكترونية.

أهمية البحث:

في ظل واقع يتسم بالتغيرات المتلاحقة في جميع جوانب الحياة الاقتصادية والسياسية والاجتماعية والثقافية، برز على الساحة الاقتصادية متغير جديد ارتبط بثورة تكنولوجيا المعلومات والاتصالات وهو الأمن الالكتروني والذي يعد نتاجاً لتطبيقات التقنيات الحديثة وما رافقها من خطر التجسس على المعلومات والجرائم الالكترونية التي باتت موازية من ناحية الخطورة للجرائم التي يتم ارتكابها بالطرق التقليدية، إذ باتت تهدد الاقتصاديات العالمية والنامية على حد سواء وأصبحت ترصد لها المبالغ الهائلة والجهود والخبرات من أجل تلافي خسائرها الفادحة، وهذا ما أثر في مسيرة عجلة التنمية الاقتصادية في معظم المؤسسات الإنتاجية وأدى إلى التأخير في العمل أو سرقة المشاريع والأفكار الجديدة نتيجة استخدام برامج ووسائل التجسس على الحواسيب أو تحويل الأموال عن طريق حسابات شخصية في البنوك بصورة غير مشروعة من شخص إلى آخر ...الخ.

وتبرز أهمية البحث في تسليط الضوء على موضوع حيوي وهو الطبيعة القانونية للجريمة الإلكترونية وعلاقتها بالجرائم الأخرى، وكذلك القوانين المنظمة والقوانين ذات العلاقة بالأنشطة المعرضة لأخطار ارتكاب الجرائم الإلكترونية، وبيان ما إذا كانت الجريمة الإلكترونية جريمة قائمة بذاتها أو أنها مجرد أداة لتنفيذ جريمة أخرى.

مشكلة البحث:

تتلخص مشكلة البحث في السؤال الرئيسي التالي:

ما هي الطبيعة القانونية للجريمة الإلكترونية؟

وتتفرع منه عدة أسئلة وهي:

١- ما هي مجالات وأنواع الجريمة الإلكترونية؟

٢- هل يوجد خصائص للجريمة الإلكترونية تميزها عن غيرها أم لا؟

٣- هل هناك قانون يمني ينظم مواضيع الجريمة الإلكترونية؟

٤- الجريمة الإلكترونية أداة أم جريمة؟

فروض البحث:

١- هناك فروقات بين الجريمة الإلكترونية والجرائم المالية.

٢- الجريمة الالكترونية أداة حديثة لتنفيذ الجرائم الأخرى وليست جريمة مستقلة بذاتها.

٣- التشريعات اليمنية مرنة بالنسبة للجريمة الإلكترونية ولا تحتاج إلى تعديل.

منهجية البحث:

سيتم اتباع المنهج الوصفي التحليلي بالاستقراء والتحليل للواقع.

هيكل البحث:

سيتم تقسيم البحث إلى محورين على النحو الآتي:

- المحور الأول: الإطار النظري لمفاهيم الجريمة الإلكترونية، ويشتمل على ثلاثة مباحث:
  - المبحث الأول: المفاهيم النظرية للجريمة الإلكترونية.
  - المبحث الثاني: مجالات وأنواع الجريمة الإلكترونية.
  - المبحث الثالث: خصائص الجريمة الإلكترونية.
- المحور الثاني: التوصيف القانوني للجرائم الإلكترونية، ويشتمل على ثلاثة مباحث:
  - المبحث الأول: أركان الجريمة الإلكترونية.
  - المبحث الثاني: المسؤولية الجنائية للجرائم الإلكترونية.
  - المبحث الثالث: قراءة في مشروع مكافحة الجرائم الالكترونية.

المحور الأول
الإطار النظري لمفاهيم الجريمة الإلكترونية

إن الحديث عن مفاهيم الجرائم الإلكترونية يقتضي استيعاب التحول الجذري في طبيعة الفعل الإجرامي ذاته، فلم تعد ترتكب بأدوات مادية في مكان معلوم ضد ضحية واضحة، بل بات يكفي نقرة زر أو سطو برمجي يؤدي إلى الإضرار بمصلحة قانونية[1]، سواء كانت أكانت مالاً أو سمعة أو خصوصية أو حتى كياناً معنوياً بأكمله.

الشبكات المعلوماتية كما هو معلوم لا مركز لها، مما يجعل التحكم بها ومراقبتها صعباً، إن عالم الشبكات المعلوماتية عالم يمكن فيه نقل للبيانات والمعلومات دون أية قيود، سواء كانت بيوعاً أم تجارة أم أخباراً أم كلاماً أم برامج إذاعية أو إخبارية، وليس بهذه الشبكات نمط موحد في نقل المعلومات، بل تتغير من وقت إلى آخر حسب إمكانيات حركة المعلومات بين نقاط الشبكة وبحسب الزحام عليها (كرتزمن، ١٢٣، ٢٠١٢).

ومن المعلوم أن القانون يتضمن مجموعة من القواعد القانونية العامة والمجردة والمقترنة بالجزاء في حالة مخالفة هذه القواعد، والجدير بالذكر أن هناك أنواعاً عديدة من الجرائم والمخالفات والتي تم تقسيمها وفقاً للقانون اليمني – جرائم القصاص وجرائم الحدود وجرائم التعازير والمخالفات (المرورية مثلاً)، وبالنظر إلى العرض السابق سوف نحاول تصنيف الجريمة الالكترونية وفقاً للقوانين اليمنية، وسوف يتم تقسيم هذا المحور إلى المباحث التالية:

(١) المصلحة القانونية: هي المصالح المباحة والتي لا يوجد قانون أو تشريع إسلامي يمنع أو يقيد استفادة الشخص منها.

المبحث الأول
المفاهيم النظرية للجريمة الإلكترونية

مفهوم الجريمة من المفاهيم القديمة قدم البشرية، والتي تتطور بتطور حياة الإنسان الاجتماعية والسياسية والاقتصادية، ولقد تعددت ألفاظ ومفردات وصيغ ومصطلحات ومفاهيم الجرائم الإلكترونية، فقد أطلق عليها البعض بجرائم الكمبيوتر والانترنت وجرائم التقنية العالية (high-tech crimes) أو الجرائم السيبرانية (cyber crimes) أو جرائم الحاسب الآلي (computer crimes) أو الجرائم الرقمية (digital crimes) أو الجرائم الناعمة (soft crimes) أو جريمة أصحاب الياقات البيضاء[1] (white collar crimes) أو الجرائم النظيفة (clean crimes)، وبغض النظر عن التسمية المستخدمة سنحاول بيان تعريفها وأنواعها وأهم خصائصها وكذلك وبالرجوع إلى أدبيات القانون نجد النظرية العامة للجريمة والتي تبين أركان الجريمة المادية والمعنوية[2]، وسيتم عرض مفاهيم الجريمة الالكترونية كالتالي:

توجد عدة تسميات للجرائم الإلكترونية منها جرائم الانترنت، وهناك من يسميها (جرائم الكمبيوتر) وآخرون يسمونها (جرائم المعالجة الآلية للبيانات والمعطيات) كما تعددت المقاربات التي حاولت الوصول إلى جوهر الجريمة الالكترونية، حيث ذهب فريق ذو اهتمامات تقنية بتحديد الجريمة الإلكترونية من زاوية الأداة المستخدمة، ويرى أنها كل نشاط إجرامي يرتكب باستخدام الحاسوب أو شبكة الانترنت، سواء بشكل مباشر أو غير مباشر، طالما أن الوسيط الرقمي يشكل جزءاً من البنية التحتية للفعل الإجرامي، ويستوجب هذا التعريف فهم المصطلحات التقنية المرتبطة به مثل: الحاسب الآلي، البرامج، البيانات، الممتلكات الرقمية، الدخول غير المشروع، الخصوصية وحماية البيانات.

وذهب فريق ذو اهتمامات قانونية فقهية بوصف الجريمة الالكترونية على أنها ظاهرة مستحدثة تنتمي إلى صنف خاص من الجرائم ذات الطبيعة اللاعنفية، والتي تتصف بالخفاء والدقة وسرعة التنفيذ وتكاد تنفلت من قبضة الإثبات التقليدي، إذ تخلو في الغالب من الأثر المادي المحسوس وتمكن مرتكبها من تخريب الأدلة الرقمية بلمح البصر، فهي جريمة ذات طابع متجاوز للحدود السيادية، مما يجعل من مواجهتها

(١) أصحاب الياقات البيضاء مفهوم يقصد به العاملون في البنوك وشركات الصرافة والمؤسسات المالية.
(٢) أركان الجريمة المادية: الفاعل، الأداة، السبب، النتيجة، وأركان الجريمة المعنوية: الإرادة والقصد الجنائي.

أمراً عسيراً في ظل قصور التشريعات وضعف الوعي التقني لدى السلطات الضبطية والقضائية، فضلاً عن التعقيد الإثباتي الذي تفرضه بنيتها التكنولوجية.

أما بعض التعريفات فقد سعت لتجريد الجريمة الإلكترونية من البواعث الشخصية والغايات الربحية، مركزة على الفعل ذاته، بوصفه انحرافاً قانونياً يستند إلى المعالجة المعلوماتية ويستدعي تدخل المشرع والعقاب، ما جعلها جرائم مستقلة بذاتها، لا بمجرد الوسيلة المستخدمة، بل بطبيعة البنية القانونية والرقمية التي تنطوي عليها.

وذهبت منظمة التعاون الاقتصادي والتنمية لتعريف الجريمة الإلكترونية في اجتماع باريس عام ١٩٨٣م والذي يعد من أقدم التعاريف وعلى النحو الآتي: «كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها» (العبدلي، ٥، ٢٠٢٥).

وفيما يلي محاولة لتعريف الجريمة الإلكترونية بحسب علاقتها بالعلوم الأخرى كما يلي:

- التعريف القانوني للجريمة الإلكترونية: فعل أو امتناع عن فعل ينتج عنه ضرر مادي أو معنوي ويوجد له نص في القانون بمعاقبة مرتكب هذه الجريمة.
- التعريف الاجتماعي للجريمة الإلكترونية: فعل أو امتناع عن فعل يحدث ضرراً بالمجتمع ويزعزع أمنه واستقرار معاملاته.
- التعريف الاقتصادي للجريمة الإلكترونية: فعل أو امتناع عن فعل اقتصادي يحدث خسائر اقتصادية في الأجل القصير والأجل الطويل.
- التعريف التقني للجريمة الإلكترونية: أساليب وطرق تقنية وحاسوبية لإحداث ضرر، بحيث يعاقب القانون مسبب هذا الضرر.
- التعريف الشامل للجريمة الإلكترونية: هي كل سلوك إيجابي أو سلبي يقترف بوسيلة معلوماتية لاعتداء على حق أو مصلحة يحميها القانون، إما بغية إحداث الضرر على مكونات الوسيلة المعلوماتية أو مضمونها (البقلي، ١٣، ٢٠١٠).

والملاحظ أن فقهاء القانون اختلفوا في المسميات الخاصة بالجرائم الإلكترونية، فهناك من يقول أن الجريمة السيبرانية تختلف عن الجريمة الإلكترونية في أن الأولى تهدف إلى اختراق الأنظمة الخاصة بالمنشآت التجارية والصناعية أو الجهات الحكومية، وتدميرها أو سرقة بياناتها باستخدام الانترنت، أما الجريمة الإلكترونية فتهدف إلى

استخدام التواصل الإلكتروني لإحداث ضرر شخصي على الأفراد، بينما الجريمة المعلوماتية تهدف إلى الإضرار بأنظمة التشغيل ومعلومات المنشآت.

وهنا لابد أن ننوه إلى أهمية التوصيف الفني (التقني) للجرائم الإلكترونية، وذلك قبل توصيفها قانونيا كأفعال محظورة ومجرمة، ولحسم اللبس حول ماهية الجرائم الإلكترونية وتسمياتها إن صح التعبير، وبعد البحث والتدقيق وجدنا أن الخلاف بين فقهاء القانون حول ما إذا كانت الجرائم الإلكترونية نوعاً واحداً أم أنها تختلف عن الجرائم السيبرانية والرقمية والمعلوماتية... إلى غير ذلك من التسميات، ما هو إلا خلاف لغوي ناتج عن اختلافات في الترجمة من دولة إلى أخرى، حيث نذكر هنا أن اتفاقية الأمم المتحدة الخاصة بمكافحة الجرائم الإلكترونية لعام ٢٠٢١م لم تفرق بين التسميات المختلفة للجرائم الإلكترونية، ومن جانب آخر نجد أن الجرائم الإلكترونية بمختلف مسمياتها ترتكز على استخدام الإنترنت، سواء لإحداث ضرر شخصي على المجني عليه أم أضرار بمنشآت أو حتى دول بأكملها، حيث أن اختراق البيانات الشخصية والأنظمة التشغيلية وسرفرات التخزين لا يتم إلا عبر شبكة الإنترنت، حتى رسائل التهديد باستخدام رسائل sms تتم عبر الإنترنت الخاص بشركات الاتصالات، وليس الإنترنت الخاص بالمرسل أو المستقبل لهذه الرسائل[1]، أي أنه مهما اختلفت مسميات الجريمة الإلكترونية فلا يمكن أن ترتكب بدون إنترنت سواء بشكل مباشر أو غير مباشر، وبدون أنظمة تشغيل وأجهزة تخزين للبيانات والمعلومات.

ومن المهم هنا أن نذكر أن الجرائم الإلكترونية تستخدم لغة الآلة أو لغة الكمبيوتر (machine language) بحيث أن كل ما يتم إدخاله في الحواسيب أو الأجهزة الإلكترونية الأخرى مثل الهواتف الذكية أو السيرفرات وغيرها تحوله هذه الأجهزة إلى لغتها الرقمية والمعبر عنها بأرقام مثل (١٠١١)، حتى لو كانت المدخلات كلمات، بالإضافة إلى أن الجرائم الإلكترونية لا تتم إلا عبر أجهزة إلكترونية لها نظام تشغيل مثل الويندوز في الحواسيب أو الماكنتوش في حواسيب شركة آبل أو الأندرويد في الهواتف الذكية أو نظام الجافا في أجهزة الهاتف المحمولة (التي تستخدم الأزرار)، بحيث لا يتصور حدوث جريمة إلكترونية باستخدام جهاز الكتروني لا يوجد به نظام تشغيل وتخزين مثل الغلاية الكهربائية والتلفزيونات غير الذكية والثلاجات ...إلخ.

(١) يجب الانتباه إلى أن البيانات تختلف عن المعلومات، فالبيانات تعني مجموعة من الأرقام والكلمات المعبرة عن موضوع معين والمخزنة في جهاز إلكتروني، أما المعلومات فغالباً تنتج من استخراج المؤشرات وعمل الدراسات والتقارير المبنية على بيانات مدخلة حاسوبياً أو في أي جهاز تخزين آخر كالهواتف المحمولة والسرفرات ...إلخ، لذلك فتسمية (جريمة معلوماتية) غير دقيقة.

وخلاصة القول، فإن الجريمة الإلكترونية ليست مجرد امتداد رقمي للجرائم التقليدية، بل هي نمط جديد من الاعتداءات القانونية، يتميز بسمات خاصة تنبع من الفضاء السيبراني من حيث الوسيلة والمجال والأثر، ومن ثم فهي تستلزم مقاربة قانونية جديدة تراعي تعقيداتها وتداخلها مع النظام المعلوماتي العالمي، كما تستوجب ملاءمة التشريعات الوطنية مع القواعد الدولية، لتوفير إطار منظم يحقق التوازن بين حماية الأمن السيبراني واحترام الحقوق الرقمية وتحقيق العدالة في عالم تتلاشى فيه الحدود الجغرافية أمام التحولات الرقمية المتسارعة.

وتتعدد صور ارتكاب الجريمة الإلكترونية باختلاف النتيجة الإجرامية، فمثلاً يرتكب الفاعل جريمة خيانة الأمانة والسرقة باستخدام وسائل الكترونية وبالتالي تصبح هنا جريمة الكترونية، فالمعيار هنا هو وسيلة ارتكاب الجريمة (الأداة)، وفيما يلي عرض استقصائي لمعايير اعتبار الجرائم من ضمن الجرائم الإلكترونية كالتالي:

المعيار الأول (الرئيسي): معيار الأداة المستخدمة لارتكاب الجريمة الإلكترونية:

ويعتبر هذا المعيار من أهم معايير تمييز الجريمة الإلكترونية عن غيرها من الجرائم، حيث يتم استخدام وسائل تقنية وبرامج حاسوبية لارتكابها مثل أجهزة الحاسوب والهواتف التي يتم تزويدها ببرامج القرصنة واختراق البيانات (غالباً البيانات المالية) والمزودة بالإنترنت، وذلك إما لنسخها فقط أو نسخها ثم تدميرها من خلال برامج تدمير وفيروسات ضرب النظام أو تغيير برمجة النظام الإلكتروني لتعطيل العمل الذي ينظمه هذا النظام.

المعيار الثاني: النتيجة الإجرامية:

حيث تحدث النتيجة الإجرامية مثلاً من خلال قرصنة الحواسيب المستهدفة للمجني عليه (أفراد، مؤسسات، حكومات) لسحب بياناتها أو تدمير أنظمة التشغيل الخاصة بها.

المعيار الثالث: الفاعل (المجرم):

حيث لابد في الجريمة الإلكترونية أن يكون الفاعل ملماً وعارفاً بمهارات التعامل مع الحاسوب، بالإضافة إلى أنه في بعض الحالات لا تتم الجريمة الإلكترونية إلا عن طريق شخص مبرمج أو مهندس حاسوب متمكن.

المبحث الثاني
مجالات وأنواع الجريمة الالكترونية

تنطوي الجرائم الإلكترونية على صور متعددة ومتنوعة، تعزى إلى طبيعة الوسائط التقنية المستخدمة ومجالات الأضرار الناتجة عنها، ويمكن تصنيف هذه الجرائم على النحو التالي:

أولاً: مجالات الجرائم الإلكترونية:

١- الجريمة الإلكترونية في مجال الصناعة:

وتكون النتيجة الإجرامية لها متمثلة في قرصنة وتهكير أجهزة الحاسوب والسرفرات الخاصة بالمصانع وذلك لسرقة تصاميمها ورسومها الصناعية أو تعطيل أنظمة التشغيل الخاصة بالآلات والمعدات الصناعية، وقد تصل إلى معارك ضارية تجسد تنافساً تجارياً بين الشركات في محاولة للإيقاع بالمنافس أو القضاء عليه.

٢- الجريمة الإلكترونية في مجال الأنشطة المصرفية:

وتكون نتيجتها الإجرامية متمثلة في سحب (سرقة) الأموال من الحسابات المصرفية عن طريق تدمير أنظمة الحماية للبنوك والمحافظ الإلكترونية واختراق كلمات المرور...

٣- الجريمة الإلكترونية في المجال المالي:

وتهدف الى سرقة أموال المتعاملين في السوق المالية، ويكمن الفرق بينها وبين الجريمة الإلكترونية المصرفية في أنها ترتكب على المتعاملين في السوق المالية[١] وأصحاب بطائق (البتكوين) مثلاً.

٤- الجريمة الإلكترونية في مجال الاقتصاد:

وتكون نتيجتها الإجرامية منصبة على الإضرار بالاقتصاد الوطني مثلاً من خلال منصات توظيف الأموال الإلكترونية والوهمية والبيع والشراء عبر الإنترنت لبضائع قد تكون مخالفة للمواصفات والمقاييس اليمنية، بالإضافة إلى أنها قد تكون مهربة وممنوعة وغير صالحة للاستخدام الآدمي ومضرة بالبيئة ...إلخ

(١) الأسواق المالية أربعة أنواع: سوق السلع، سوق العملات، سوق المعادن، أسواق السندات والأسهم.

٥- الجريمة الإلكترونية الإرهابية:

وتتم من خلال عمليات غسل الأموال وتمويل الإرهاب الدولي.

٦- جرائم التهديد والابتزاز الإلكترونية:

وهي الجرائم التي ترتكب من خلال تهديد المجني عليه / عليهم ببيانات ومعلومات خاصة بهم سواء كانت معلومات شخصية أو بيانات مالية أو تصاميم صناعية (مسجلة) أو غير ذلك بهدف إجبار المجني عليه وحمله على تنفيذ ما يطلبه الجاني والذي في الغالب ما يكون ارتكاب جريمة أخرى مثل السرقة والاختلاس وخيانة الأمانة وتسريب معلومات ...إلخ.

٧- جرائم سياسية وأمنية:

وتهدف إلى الحصول على الأسرار العسكرية والأمنية، مما يعكس انتهاج بعض الحكومات نهج التجسس على الأفراد والجماعات المعادية لها، لإحباط محاولاتها الهجومية ومعرفة خططها الآنية والمستقبلية، ومن طريف القصص ما حدث في الولايات المتحدة الأمريكية عندما تم القبض على مجموعة من الهاكرز المحترفين، وبعد عدة جولات من التحقيقات تم تجنيدهم لصالح وكالة الاستخبارات الأمريكية (CIA) لاستغلالهم بمهام أمنية (الوائلي، ٤، بدون سنة).

٨- الجرائم الإلكترونية باستخدام الذكاء الاصطناعي:

ويشمل هذا النوع استخدام الذكاء الاصطناعي التوليدي لمحاكاة الإعلانات والرسائل الترويجية الحقيقية، وتتميز هذه الرسائل والإعلانات المزيفة بدقة عالية، وهذا النوع من الجرائم لديه القدرة على الهروب من حلول وتدابير الأمن السيبراني التقليدية التي تعجز عن اكتشافه، ونظراً لأنها ترتكب بواسطة الذكاء الاصطناعي، فيمكنها التعلم والتكيف مع أنظمة أمن السيبراني الإضافية واكتشاف طرق جديدة لتجاوزها (الجرموزي، ١٧، ٢٠٢٥).

ثانياً: أنواع الجرائم الإلكترونية (العبدلي، ٦، ٢٠٢٥):

١- الجرائم الماسة بالمعطيات الإلكترونية للحاسوب: يقسم هذا النوع من الجرائم إلى نوعين رئيسين وفقاً للمعطيات الالكترونية للحاسوب:

٢. الجرائم الواقعة على المعطيات ذاتها: وهي الجرائم التي تستهدف البيانات والمعلومات المخزنة في الأنظمة الالكترونية، عبر تشويهها أو تعديلها أو إتلافها،

ويرتكب هذا النوع عبر وسائل تقنية ضارة مثل: الفيروسات والبرمجيات الخبيثة.

٣. الجرائم الواقعة على مدلول المعطيات الالكترونية: وهي التي تستهدف ما تمثله تلك المعطيات من قيمة مالية أو تجارية، كأن يتم الاستيلاء على الأموال المرتبطة بالحسابات البنكية أو بطاقات الائتمان من خلال الحاسوب (الجريمة الإلكترونية المصرفية)، أو يتم الاتجار غير المشروع بالمعلومات المستخلصة الناتجة عن ارتكاب هذا النوع من الجرائم.

٤- الجرائم الماسة بالمعطيات ذات الطابع الشخصي: وتتجسد في الاعتداء على المعلومات أو البيانات المخزنة الكترونياً، والتي تتصل بحياة الأفراد الخاصة، كالمراسلات، والصور، والمعلومات الصحية أو المالية (جريمة الابتزاز الإلكتروني)، ما يشكل مساساً خطيراً بالحق في الخصوصية المكفول قانوناً.

٥- الجرائم الماسة بحقوق الملكية الفكرية: وهي الأفعال التي تمس الحقوق الأدبية والمالية لأصحاب الابتكارات والمصنفات الفكرية، ومن أبرزها نسخ أو استخدام البرامج الإلكترونية دون ترخيص مسبق، إعادة تدوير البرمجيات أو التلاعب بمحتواها أو نسبتها زوراً، انتهاك العلامات التجارية[١] وبراءات الاختراع باستخدام الوسائط الإلكترونية، تحميل الكتب والمصنفات الإلكترونية المحمية بحقوق المؤلف (أو في بعض الأحيان محمية بحقوق الناشر) دون سداد المقابل المالي أو دون الحصول على إذن مشروع.

٦- جرائم أخرى متعددة: وتشمل الجرائم الالكترونية من حيث الهدف الذي تسعى إلى تحقيقه:

أ- جرائم التشهير: وهي تلك الأفعال التي يقصد بها تشويه سمعة الأفراد والنيل من مكانتهم الاجتماعية أو الوظيفية، عبر نشر معلومات أو صور أو أقوال مسيئة تمس شرفهم أو اعتبارهم، باستخدام المنصات الرقمية ومواقع التواصل الاجتماعي.

ب- المطاردة الإلكترونية: وتتمثل في تتبع الأفراد ومراقبة تحركاتهم وأنشطتهم عبر الوسائل الإلكترونية المختلفة (مثل: اختراق الهواتف، كاميرات المراقبة،

(١) تذكر أدبيات المحاسبة المالية أن الملكية الفكرية (براءة الاختراع) للابتكارات الصناعية (التصاميم والرسومات الصناعية مثلاً) تظل سارية حتى أربعين سنة ثم تصبح متاحة للجميع، ولا يعاقب من استخدم هذه الابتكارات بعد هذه المدة، ولا يطلب منه دفع رسوم أو مقابل مادي لاستخدامها.

...إلخ)، سواء بغرض الإحراج العلني، أو لتحقيق مكاسب غير مشروعة، كارتكاب جرائم السرقة المالية، أو ابتزاز الضحايا وتهديدهم بنشر معلومات شخصية تم جمعها دون رضاهم، أو حتى لارتكاب جرائم القتل والاغتيالات...إلخ.

ج- جرائم القذف والسب والشتم: وتتضمن توجيه عبارات أو ألفاظ تنطوي على إهانة صريحة أو اتهام بغير حق، تمس شرف الشخص وكرامته أو تنال من اعتباره في محيطه المجتمعي.

د- جرائم إيقاف الخدمات: وتتم من خلال إغراق الخدمات في المؤسسات (لاسيما تلك المرتبطة بالإنترنت) بعدد هائل من طلبات التشبيك مما يؤدي إلى إيقاف عملها وتحقق خسائر كبيرة.

هـ- حصان طروادة: وهو البرنامج الذي يقوم على توفير مدخل للمخترقين إلى أجهزة تحتوي معلومات غير مصرح لها بالدخول إليها ولا يتطلب استخدامها خبرات تقنية، ويكثر ارتكاب هذا النوع على مواقع الانترنت، حيث يقوم المخترق بتعديل أو تغيير المعلومات الموجودة في الموقع (الوائلي، ٥، بدون سنة).

وتتسم هذه الجرائم بخطورة بالغة، إذ لا تقتصر آثارها على النواحي النفسية والمعنوية للمجني عليه/ عليهم، بل تمتد إلى تهديد أمنه الشخصي واستقراره الاجتماعي، مما يحتم ضرورة مواجهتها بتشريعات رادعة ووسائل تقنية مضادة تكفل الحماية القانونية الفاعلة.

المبحث الثالث

خصائص الجريمة الإلكترونية

أمام تصاعد وتيرة هذه الجرائم وتعقد أساليب ارتكابها، سعت الكثير من الدول إلى مواجهتها والحد من آثارها، سواء من خلال إعداد دراسات متخصصة أو بحوث أمنية معمقة تعنى بكشف طرائق ارتكاب هذه الجرائم وتحليل الخصائص السلوكية لمرتكبيها، فضلاً عن الوقوف على الدوافع النفسية والاجتماعية المحركة لهم، ومن أجل التصدي المنهجي للجرائم الإلكترونية، فإن الوقوف على خصائصها الجوهرية يعد مدخلاً أساسياً لفهم طبيعتها، وتتلخص أبرز هذه الخصائص في الآتي (العبدلي، ٨، ٢٠٢٥):

أولاً: جرائم يصعب إثباتها والكشف عنها: حيث تتسم بقدر عال من التعقيد والغموض، يجعل من عملية إثباتها والكشف عنها أمراً بالغ الصعوبة، وذلك بسبب طبيعتها الرقمية المجردة، إذ لا تخلف آثاراً مادية ملموسة كما في الجرائم التقليدية، بل تتم عبر رموز ومعطيات الكترونية متغيرة باستمرار، يصعب تعقبها أو الاحتفاظ بها كدليل مادي مباشر.

وغالباً ما يتم اكتشافها عن طريق المصادفة، وبعد مرور فترة زمنية طويلة على ارتكابها، دون أن تترك خلفها بصمات إلكترونية كافية تيسر مهمة المحقق الجنائي، ويضاف إلى ذلك أن مرتكبي هذا النوع من الجرائم غالباً ما يتحلون بالتمكن التقني، مما يمنحهم القدرة على إخفاء آثارهم والتلاعب بالأدلة، وهو ما يجعل الوسائل التقليدية للتحقيق التي يعتمدها المحقق الكلاسيكي غير كافية أو فاعلة.

ثانياً: جرائم عابرة للحدود: أي أنه يمكن أن ترتكب في عدة دول ولا يمنعها أو يقيدها حدود جغرافية.

ثالثاً: جرائم ماسة بالقيم الأخلاقية والآداب العامة: تشكل بعض الجرائم الإلكترونية تهديداً مباشراً للمنظومة الأخلاقية للمجتمع، لاسيما من خلال نشر وتداول المحتويات المخلة بالحياء، مما يؤدي إلى تقويض القيم والضوابط الاجتماعية والهوية الإيمانية الراسخة.

رابعاً: الفئة العمرية لمرتكبي الجرائم الالكترونية: تشير المؤشرات الإحصائية المتوفرة إلى أن الفئة العمرية الغالبة على مرتكبي الجرائم الإلكترونية تتراوح بين (١٨-٤٦) عاماً، مع متوسط عمري يقدر بـ (٢٥) عاماً، وتدل هذه المعطيات على أن أغلب مرتكبي هذا النوع من الجرائم هم من فئة الشباب، وهو ما يعزى إلى إلمامهم الواسع

باستخدام تقنيات الحاسوب والأنظمة الرقمية، وتعد هذه السمة مؤشراً دالاً على الطبيعة المعاصرة والمرتبطة بالتطور التكنولوجي في تكوين الجريمة المعلوماتية.

خامساً: محل الجريمة: توجه الجريمة الالكترونية أساساً إلى النيل من المعطيات الإلكترونية بصورها المختلفة، باعتبارها تمس المعنويات لا الماديات.

ومن ناحية أخرى نجد أن الجرائم الإلكترونية لها آثار باهظة خاصة بعد القيمة الاقتصادية المتزايدة للبيانات المخزنة، وبعد أن تحولت إلى سلعة تباع وتشترى، حيث انعكست آثارها الخطرة على والمدمرة على المؤسسات المالية العالمية وأمن الدول وحقوق الأفراد الخاصة (الحمداني، ٣٢، ٢٠١١).

المحور الثاني
التوصيف القانوني للجرائم الإلكترونية

تتيح التكنولوجيا الحديثة القيام بالكثير من الأعمال التي كان يستحيل إنجازها في وقت قصير، فلقد وفرت تكنولوجيا الاتصالات والمعلومات الإلكترونية تحقق التواصل السريع وإنجاز المعاملات في سهولة ويسر، وتعد شبكات المعلومات ونظم التبادل الإلكتروني للبيانات تطبيقاً لاستخدام التكنولوجيا الحديثة في مجال الاتصالات ونقل المعلومات وهي تختلف بذلك كثيراً عن غيرها من الوسائل التقليدية للاتصال والإعلام، وهذا الاختلاف يؤدي إلى أمرين، الأول: هو تعدد أوجه استعمالات هذه الوسائل واتساعها، والثاني: هو الحاجة إلى تنظيم قانوني يضع الإطار لهذه الاستعمالات، غير أن هذه التكنولوجيا قد يساء استخدامها وذلك بتهديد السلامة العامة والمصلحة الوطنية، فإذا كانت وسائل الاتصال الإلكترونية الحديثة تتيح إنجاز المعاملات المالية على سبيل المثال بشكل سريع وموثوق به أياً كان مكان المتعاملين، فإن استخدام هذه الوسائل لا يخلو من المخاطر، فقد يستغل بغض المجرمين هذه الوسائل في ارتكاب جرائمهم عن طريق الاحتيال أو المساس بخصوصية هؤلاء المتعاملين وسرية معاملاتهم، وإذا كان التقدم التقني قد حاول مكافحة الجرائم في مجال الاتصالات الإلكترونية، وذلك بأن استحدث الكثير من إجراءات سلامة وأمن هذه الاتصالات ولجأ إلى تشفيرها بما يحفظ سريتها، فإن هذه الإجراءات– مع ذلك– قد أدت إلى استغلال الجناة لهذه الإجراءات في ارتكاب جرائمهم باستخدام وسائل اتصال يصعب اختراقها أو الوقوف على محتواها، وهو ما يعني أن التقدم التقني قد زود المجرمين بوسائل بالغة القوة والفاعلية لارتكاب جرائمهم (شمس الدين، ٥، ٢٠٠٣).

وقبل الحديث عن الجريمة الالكترونية في طيات مشروع قانون مكافحة الجرائم الالكترونية، لزم الإشارة إلى أركان الجريمة الإلكترونية والتي لا تختلف في مضمونها عن الجرائم المذكورة في قانون العقوبات اليمني، وسوف نستعرض هذا المحور من خلال المباحث الآتية:

المبحث الأول

أركان الجريمة الإلكترونية

بالاستناد إلى أدبيات القانون الجنائي نستعرض أركان الجرائم الإلكترونية المادية والمعنوية لأهم أنواع الجرائم الإلكترونية والأكثر انتشاراً كما يلي:

أولاً: الجرائم الإلكترونية في مجال الأنشطة المصرفية:

١- أركان الجريمة المادية:

١. الفاعل: ومن أهم الجناة في هذا النوع من الجرائم هم موظفو البنوك والمؤسسات المالية[١].

٢. الأداة: مثل: برامج التجسس واختراق وتدمير الأنظمة البنكية وأنظمة الدفع الإلكترونية وشبكات التحويلات المالية.

٣. الرابطة السببية: بين الفعل أو الامتناع عن الفعل المحظور قانوناً والذي ينتج عنه ضرريرتقي إلى مرتبة الجريمة الالكترونية.

٤. النتيجة: الضرر المتمثل في على سبيل المثال: سرقة الأموال من خلال اختراق الأنظمة البنكية.

٢- أركان الجريمة المعنوية:

أ- الإرادة (القصد الجنائي الخاص): اتجاه إرادة الجاني لإحداث النتيجة الإجرامية، سواء بشكل مباشرة بارتكاب الجريمة أو عن طريق الإهمال.

ب- القصد الجنائي العام: وينقسم إلى القصد العمدي وغير العمدي، فالقصد العمدي يعني ارتكاب الفعل بقصد حصول النتيجة الإجرامية مثل: الاختراق المتعمد لأنظمة المؤسسة المالية للاستيلاء على أموال أو تحويلها أو تدمير بياناتها ...، والقصد غير العمدي يعني حدوث النتيجة الإجرامية بغير قصد سواء بارتكاب فعل أحدث النتيجة الإجرامية ولم يكن في نية الفاعل حدوثها، أو الإهمال المؤدي إلى النتيجة الإجرامية وهنا نلاحظ أن الإهمال

(١) المؤسسات المالية مثل البنوك، شركات الصرافة، شبكات التحويل، مشغلو أنظمة السداد الإلكتروني، شركات الاستثمار المالي، الصناديق السيادية للدولة (كمؤسسات التأمينات الاجتماعية، صندوق تشجيع الإنتاج الزراعي والسمكي،...إلخ).

قد يتحقق عندما لا يلتزم الفاعل بالإجراءات وخطوات العناية الواجبة للشخص العادي.

ثانياً: الجرائم الإلكترونية في مجال التجارة والصناعة:

١- أركان الجريمة المادية:

أ- الفاعل: ومن أهم الجناة في هذا النوع من الجرائم هم القراصنة من الشركات المقلدة للمنتجات أو في بعض الأحيان قد يكونون من الشركات المنافسة (منافسة غير شريفة)، بالإضافة إلى موظفي الشركات أو المصانع وذلك لمصلحة الغير أو لمصلحتهم الشخصية (استغلال نفوذ)، وذلك لسرقة التصاميم والرسوم الصناعية أو تدمير أنظمة التشغيل الخاصة بالمصانع.

ب- الأداة: الاختراق الالكتروني للأنظمة المشغلة للمصانع أو الشركات.

ج- الرابطة السببية: وذلك بين الفعل أو الامتناع عن الفعل والذي أدى إلى إحداث النتيجة الإجرامية المتمثلة في الضرر (السرقة أو تدمير الأنظمة أو تشويه سمعة منتج معين ... إلخ).

د- النتيجة الإجرامية: وهي الضرر الناجم عن الجريمة والمتمثلة في على سبيل المثال: تقليد المنتجات الأصلية أو إتلاف وتدمير الأنظمة المعلوماتية ... إلخ.

٢- أركان الجريمة المعنوية:

١- الإرادة (القصد الجنائي الخاص): وتتمثل في اتجاه إرادة الفاعل لإحداث الضرر والنتيجة الإجرامية.

٢- القصد الجنائي العام: ويكون عمداً عندما يتم استخدام برامج وأدوات تقنية بهدف الوصول إلى البيانات أو سرقتها أو إتلافها، ويكون القصد غير عمدي، وذلك بإهمال إجراءات العناية الواجبة لتجنب حدوث أي ضرر وذلك بعمل برامج حماية تقنية وسرفرات في مكان آمن، وتعيين موظفين تقنيين ذوي أمانة ونزاهة، وهذا الإهمال يجب أن تظهر تحقيقات الأجهزة الأمنية المعنية أنها هي سبب النتيجة الإجرامية.

ثالثاً: الجرائم الواقعة على العرض: وترتكز على ثلاثة أركان كالآتي (البقلي، ٢١، ٢٠١٠م):

١- الركن المفترض: وهو وجود جهاز إلكتروني كركن مفترض يشكل الوسيلة المستخدمة لارتكاب السلوك الإجرامي في الركن المادي لجرائم الإنترنت في ظل وجود البيئة الرقمية المتصلة به.

٢- الركن المادي: وهو السلوك المادي الإيجابي بإتيان أفعال تشكل الركن المادي للجرائم الواقعة على العرض وقد تتضمن تعدداً معنوياً لأكثر من جريمة بذات السلوك في بعضها أو تقتصر على السلوك المادي لجريمة العرض بالوسيلة الإلكترونية وتحقق النتيجة بناء على هذا السلوك.

٣- الركن المعنوي: وهو القصد الجنائي العام، المستخلص من الأفعال المادية بتوافر عنصرية من العلم بتجريم السلوك واتجاه إرادة الجاني على إتيان ذلك السلوك وتحقق نتيجته.

المبحث الثاني

المسؤولية الجنائية للجرائم الإلكترونية

ذكرت اتفاقية بودابست صعوبة البلوغ إلى مرتكب الجريمة عبر الإنترنت في المادة (٢١) الخاصة بمكافحة جرائم الفضاء المعلوماتي، حيث تبنت الدول المنظمة إلى المعاهدة تدابير تشريعية لضمان قيام مسؤولية الأشخاص الطبيعية عن جرائم الإنترنت وكذا الأشخاص المعنوية، حتى وإن قام الأشخاص الطبيعيون بارتكابها لصالح الأشخاص المعنويين، وقد ضمنت غالبية الدول في تشريعاتها مسؤولية مرتكب الجريمة عبر الإنترنت عن جريمته، وقد ثار الخلاف حول مقدم الخدمة أو المستضيف للمواقع الالكترونية ومدى مسؤوليته عن الجرائم الإلكترونية بمختلف أنواعها، والمستخلص من أحكام القضاء والفقه في بعض الدول قيام مسؤولية مؤجر أو صاحب السيرفر عن هذه الجرائم إذا علم بها ولم يتخذ الإجراءات الكفيلة بمنع وقوعها.

والجدير بالذكر أن المساهمة الجنائية لها أيضاً وجود في الجرائم الإلكترونية بمختلف أنواعها، حيث يسأل المساهم عن جريمة الفاعل الأصلي ويعاقب بذات العقوبة المقررة الفاعل الأصلي سواء كان مباشراً أو متسبباً، وإن كانت المحاكم جرت على تخفيف عقوبة المساهم في نطاق الحد الأقصى والأدنى للعقوبة، وفيما يلي بيان الأحوال الخاصة بالمساهمة الجنائية في الجرائم الإلكترونية (البقلي، ٢٧، ٢٠١٠):

١- إذا كانت ظروفاً عينية تتعلق بالأمن المادي للجريمة كحمل السلاح، فإن المساهم تسري عليه ذات العقوبة المقررة للفاعل.

٢- إذا كانت ظروفاً شخصية كصفة المتهم (موظف عام)، وتغير وصف الجريمة من غير جسيمة إلى جسيمة، فلا تسري إلا على صاحبها، إلا إذا كان المساهم عالماً بها.

٣- إذا توافر عذر يعفي من العقاب (الجنون مثلاً) - وهذا مستبعد بالنسبة للجرائم الإلكترونية - أو مخفف كصغر السن (الأهلية الناقصة)، فلا تسري إلا على الفاعل الأصلي فقط.

٤- إذا توافر عذر خاص بالجريمة كالدفاع الشرعي فتنتفي المسؤولية الجنائية عن المساهم والفاعل الأصلي.

٥- إذا توافر سبب إباحة كحق التأديب أو صفة الطبيب في الأعمال الطبية يستفيد منها المساهم، فهي ذات طبيعة موضوعية تتعلق بالجريمة نفسها بشرط أن تتوافر

صفة معينة في المستفيد منها، فلا ينصرف أثر الإباحة إلى الفاعل مع المساهم إذا لم تتوافر فيه تلك الصفة.

٦- إذا توافر مانع من المسؤولية لدى الفاعل الأصلي كغير المميز أو المجنون، فلا يستفيد المساهم من ذلك المانع، ويسأل بقدر تمييزه.

٧- إذا توافر القصد الجنائي للفاعل الأصلي والمساهم فيسأل عن الجريمة كلاهما، أما إذا لم يتوافر في المساهم فيسأل عن جريمة خطأ غير عمدية، وقد لا يسأل إذا كان لا يتصور بها الخطأ كجريمة التزوير الالكتروني في محررات لم يعلم المساهم ولم تتجه إرادته إلى سلوك تغيير الحقيقة.

٨- يسأل المساهم عن الجريمة المحتملة للفاعل الأصلي ولو كانت غير التي قصد ارتكابها متى كانت الجريمة التي وقعت نتيجة محتملة للمساهمة الجنائية التي حصلت.

المسؤولية التقصيرية للمجني عليه في الجرائم الالكترونية:

نذكر هنا أنه من الواجب على المتعاملين في الجانب الإلكتروني القيام بعدد من الإجراءات والتدابير للعناية الواجبة للوقاية ولمنع حدوث الجرائم الالكترونية، وبالتالي فإن أي إهمال أو تقصير من جانب المجني عليه يعرضه للمساءلة القانونية، خاصة إذا أهمل إجراءات العناية الواجبة الملزمة بحسب القوانين المنظمة للنشاط الواقع عليه الجريمة الالكترونية، وقد تتفاقم المسؤولية إلى أن تصل إلى مستوى المساهمة الجنائية إذا كان الإهمال والتقصير عمدياً بحسب ما تم عرضه أعلاه.

المبحث الثالث

أمن المعلومات الإلكترونية

في ظل واقع يتسم بالتغيرات المتلاحقة في جميع جوانب الحياة الاقتصادية والسياسية والاجتماعية والثقافية، برز على الساحة الاقتصادية متغير جديد ارتبط بثورة تكنولوجيا المعلومات والاتصالات وهو الأمن الالكتروني والذي يعد نتاجاً لتطبيقات التقنيات الحديثة وما رافقها من خطر التجسس على المعلومات والجرائم الالكترونية التي باتت موازية من ناحية الخطورة للجرائم التي يتم ارتكابها بالطرق التقليدية، إذ باتت تهدد الاقتصاديات العالمية والنامية على حد سواء وأصبحت ترصد لها المبالغ الهائلة والجهود والخبرات من أجل تلافي خسائرها الفادحة، وهذا ما أثر في مسيرة عجلة التنمية الاقتصادية في معظم المؤسسات الإنتاجية مثل: التأخير في العمل أو سرقة المشاريع والأفكار الجديدة نتيجة استخدام برامج ووسائل التجسس على الحواسيب أو تحويل الأموال عن طريق حسابات شخصية في البنوك بصورة غير مشروعة من شخص إلى آخر ...إلخ.

من ناحية أخرى نجد أن الجرائم الإلكترونية تثير الكثير من المشكلات القانونية، بدءاً من مرحلة التحريات والتحقيقات وجمع الأدلة إلى صدور الحكم القضائي، خاصة فيما يتعلق بإثباتها وحجية أدلتها الرقمية (شيخ، ٩، ٢٠٢٠).

ويمكن أن تتعرض النظم لأنواع كثيرة مختلفة للتهديد والهجوم على الأنظمة الالكترونية يمكن تصنيفه كأنواع متعددة (حسين، ٨، ٢٠٠١):

- التنصت (استراق السمع): تداخل وقراءة رسائل مخصصة لمستخدمين آخرين.
- التنكر: إرسال واستقبال رسائل باستعمال هوية مدير آخر.
- العبث بالرسائل: تداخل وتغيير رسائل مخصصة لمستخدمين آخرين.
- التلاعب: استعمال رسائل سبق إرسالها لاكتساب حقوق مستخدم آخر.
- التسريب: إساءة استعمال سلطة مدير حتى ينفذ برامج خبيثة أو عدائية.
- تحليل حركة: ملاحظة (مراقبة) الحركة من أو الى مدير النظام.
- رفض الخدمة: من قبل مدير النظام.

الجدير بالذكر أن التهديدات الالكترونية لابد لها من نظام لإدارة المخاطر للمنشآت المستخدمة لتقنية المعلومات بهدف دعم أنظمتها بنظام أمني يبدأ عمله بتحليل شامل

لمعظم التهديدات المحتملة، يسمى تحليل المخاطر وهنا لا بد أن ننوه إلى أن من يقوم بهذا التحليل هم تقنيون تابعون للمنشأة في إدارة متخصصة لأمن المعلومات (أحياناً تسمى إدارة الامتثال المعلوماتي) ويكون التحليل تبعاً لنشاطها وأنواع المعاملات الالكترونية الخاصة بها بحيث يقيم الخطر وعدد مرات حدوثه وتكاليف تنفيذ آلية حماية مناسبة، التي تقاس بتكاليف الإصلاح والتلف الناتج من أي هجوم متوقع.

تحليل المخاطرة يجب عمله في طور التخطيط قبل تنفيذ نظام الحماية الالكترونية بناء على التكلفة والعائد (اقتصاد المعلوماتية)، وهذه العملية في بعض الدول تتم بإشراف جهات رقابية حكومية مثل سلطة ضبط الاتصالات الإلكترونية الموجودة في بعض الدول.

ومن المهم هنا أن نؤكد على ضرورة وجود جهة رقابية حكومية للأعمال والأنشطة الإلكترونية، حيث يمكن تعريف الرقابة الإلكترونية بأنها عملية مراقبة شبكة الاتصالات باستخدام التقنيات الإلكترونية، بحيث تجمع بواسطتها بيانات ومعلومات حول المشتبه به لتحقيق غرض أمني يقوم به مراقب حكومي ذو كفاءة تتماشى مع نوع الجريمة التي يحقق فيها. وهو إجراء وقائي يمكن أن تلجأ إليه أجهزة السلطة القضائية حتى قبل وقوع الجريمة، في حالة الاشتباه بارتكاب أفعال تمس النظام العام والأمن القومي للدولة (عمر، ١٤، ٢٠١٩).

وعلى أساس سياسة نتائج تحليل المخاطرة، يمكن تعريفها بأنها: التي تحدد بوضوح ما هو المطلوب تأمينه وكيفية التنفيذ، وسياسة الأمن لا يمكنها عادة أن تغطي كل المخاطر المحتملة للنظام، ولكن تعتبر تناوباً معقولاً بين المخاطر والموارد المعقولة.

ومن الوظائف التي تقوي سياسة الأمن: خدمات الأمن، وتنفيذ الخدمات بآليات ووسائل أمنية والتي يتم التحقق منها بالمقابل بخطوات حل مشفرة وبروتكولات آمنة.

ومن اللازم هنا أن ننوه إلى وجود معايير دولية للأمن الالكتروني صادرة من الهيئة الدولية للمعايير (الأيزو) حيث ذكرت خدمات الأمن الأساسية التالية:

١. التوثيق: يؤكد أن كينونة مدير النظام أو أساس بيانات حقيقية وغير زائفة.
٢. التحكم بالوصول والثقة في الحصول على البيانات: يؤكد أن المدراء المخول لهم، هم فقط الذين يمكنهم الوصول إلى البيانات المحمية وإعطاء صلاحيات لموظفيهم بحسب الأعمال الموكلة إليهم.
٣. تكامل البيانات: أي أنه لا يتم تعديل البيانات إلا بواسطة المدراء المخول لهم فقط.

٤. عدم فرض السلطة: أي عدم منع مدراء الأنظمة الالكترونية من أداء أعمالهم والمتعلقة بالبيانات.

ومن المفيد هنا أن نذكر استراتيجيات الوقاية من الجرائم الإلكترونية التي قدمها البنك المركزي اليمني بمنشوره الدوري رقم (١) لسنة ١٤٤٥ والخاصة بالمؤسسات المالية، والتي يمكن اعتمادها أيضاً بالنسبة للمتعاملين الكترونياً من الجهات العامة أو القطاع الخاص، وهي تحقيق ثلاثية الأمن المعلوماتي (CIA) كالتالي (الجرموزي، ٢١، ٢٠٢٥):

- السرية: ضمان حماية للبيانات من الوصول غير المصرح به، والحفاظ على خصوصية المعلومات المهمة سواء كانت تخص المؤسسة أو عملاءها.
- السلامة: ضمان دقة وموثوقية البيانات، والتأكد من عدم تعرضها للتعديل أو التلاعب، مما يحافظ على مصداقية للبيانات.
- التوافر: ضمان توفر البيانات والأنظمة للمستخدمين المصرح لهم في الوقت المناسب، مما يضمن استمرارية العمليات والخدمات دون انقطاع.

المبحث الرابع

قراءة في مشروع قانون مكافحة الجرائم الإلكترونية

تعد السويد أول دولة تسن تشريعات لاسيما الخاصة بجرائم الحاسب الآلي والانترنت، إذ صدر قانون البيانات السويدي عام (١٩٧٣م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي فضلاً عن شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها.

وتبعتها الولايات المتحدة الأمريكية إذ شرعت قانوناً خاصة بحماية أنظمة الحاسب الآلي (١٩٧٦-١٩٨٥م)، وفي عام (١٩٨٥م) حدد معهد العدالة القومي خمسة أنواع رئيسية للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بالجرائم الالكترونية، إذ أقرت قانون مكافحة التزوير والتزييف عام (١٩٨١م) الذي شمل تعاريف أداة التزوير بوسائط التخزين الحاسوبية المختلفة أو أي أداة أخرى يتم التخزين عليها سواء بالطرق التقليدية أو الالكترونية أو بأي طريقة أخرى.

هناك عدة دول عدلت قوانينها بتضمينها أحكاماً خاصة بالجرائم الالكترونية، مثل: كندا وفرنسا وهولندا وفنلندا وألمانيا إذ عدلت قوانينها الجنائية بأن شملت نصوصاً خاصة بهذه الجرائم والعقوبات المحددة لكل نوع منها(الوائلي، ١٠، بدون سنة).

وفي ظل التحولات والتغيرات المحلية والعالمية التي شهدتها بلادنا كان لابد من مواكبة هذه التغيرات والتطورات خاصة فيما يتعلق باستخدام التكنولوجيا الحديثة في كافة المجالات ابتداء بالصناعة والتجارة وصولاً إلى الخدمات التقنية سواء في القطاع الحكومي أو الخاص، ولما كانت التقنيات الحديثة من أهم مقومات أي اقتصاد قوي، نرى أن الدولة أولت اهتماماً بالغاً بتشجيعها في كافة المجالات وهذا ما يظهر جلياً في طيات قانون الاستثمار الذي أعطى مميزات استثمارية كبيرة لشركات التكنولوجيا والخدمات اللوجستية المساندة للقطاعات الاقتصادية المختلفة.

والجدير بالذكر أن أي نشاط تقني لابد له من وجود الحماية القانونية التي تضمن عدم التعدي على حقوق وحريات المواطنين، ونلاحظ أن القانون الجنائي التقليدي غير مؤهل لدرجة كافية للاضطلاع بدوره في مكافحة الجرائم الإلكترونية، ذلك أن صلابة

المبادئ القانونية التي تحكم الإكراه الجنائي المقرر للجرائم التقليدية، هي صلابة ضرورية لا تنسجم بصورة جيدة مع حركية الأنشطة والمعاملات الإلكترونية والصبغة الاصطناعية لأغلب تطبيقاته (موسى، ٢٧، ٢٠٢٢)، وفيما يلي عرض لأهم المواضيع التي تطرق لها مشروع قانون مكافحة الجرائم الإلكترونية:

١- انتهج المشرع اليمني نهج الدول التي أفردت قانوناً مستقلاً لتنظيم الأحكام المتعلقة بالجرائم تقنية المعلومات، وذلك استناداً إلى القوانين الأساسية الأخرى ومن أهمها: قوانين الجرائم والعقوبات والإجراءات الجزائية وحماية المستهلك وغسل الأموال وتمويل الإرهاب بالإضافة إلى قانون حق الحصول على المعلومات.

٢- نظم مشروع القانون الأنشطة الرقمية بمختلف أنواعها من خلال إنشاء جهاز حكومي تنظيمي ورقابي لهذه الأنشطة وهو المركز الوطني لأمن تقنية المعلومات، والذي من الواضح أنه يتبع وزارة الاتصالات وتقنية المعلومات.

٣- من أهم أهدافه حفظ الحقوق وتعزيز الثقة في التعاملات الإلكترونية، وكذا تحديد الإجراءات الخاصة بجمع الأدلة الإلكترونية وحجيتها في الإثبات الجنائي، بالإضافة إلى تحديد الأحكام الموضوعية للجرائم الإلكترونية وبيان التدابير والإجراءات وجوانب التعاون الدولي الكفيلة بمكافحتها.

٤- تضمن القانون أسس ومبادئ العمل في القانون الدولي العام والخاص وأحكام تنازع القوانين وتنازع الاختصاص القضائي الدولي، وكذا ضيق من تطبيق مبدأ إقليمية القوانين، وذلك لطبيعة الجريمة الإلكترونية العابرة للحدود.

٥- تطرق في الباب الثالث منه على أنواع الجرائم الإلكترونية والعقوبات المقرة لها، وقسمها إلى مجموعات كالتالي:

أ- جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية.

ب- جرائم الاحتيال الإلكتروني.

ج- جرائم التزوير الإلكتروني.

د- جرائم التعدي على الملكية الفكرية.

هـ- الجرائم المرتكبة من مدير الموقع.

و- الاعتداء على المبادئ أو القيم الاجتماعية أو انتهاك حرمة الحياة الخاصة وجرائم المحتوى المعلوماتي غير المشروع.

ز- جرائم المعلوماتية ضد الدولة والسلامة العامة.

٦- وتضمن مشروع القانون في الباب الرابع منه أحكاماً عامة في عدة فصول كالتالي:

- المسؤولية الجزائية للشخص الاعتباري.
- العقوبات التكميلية.
- الظروف المشددة للعقوبة.
- المساهمة والشروع في ارتكاب الجريمة والإعفاء منها.

٧- وتطرق في الباب الخامس للقواعد الإجرائية الملزمة لمستخدمي الحاسوب والبرامج الإلكترونية وذلك من خلال الفصول التالية:

- التزامات مزود الخدمة.
- التزامات الجهات.
- الإجراءات والقرارات الصادرة بشأن طلبات حجب المواقع.
- الإجراءات القضائية والتدابير.
- الأدلة الإلكترونية.

٨- وفي الباب السادس تطرق مشروع القانون إلى مظاهر التعاون الدولي لمكافحة الجرائم الإلكترونية، إلا أنه لم ينظم مسألة التوازن الدولي في ضبط المجرمين والقبض عليهم (الانتربول الدولي)، وكيفية تسليم المطلوبين أمنياً-خاصة حاملي الجنسية اليمنية- أو المجرمين الذين ارتكبوا الجريمة في أراضي الجمهورية اليمنية وفروا إلى الدول الأخرى، حيث لم يرحل مشروع قانون مكافحة الجرائم الكترونية هذه المواضيع إلى القوانين اليمنية الأخرى ذات العلاقة، لتلافي التداخل أو الفراغ التشريعي.

من العرض السابق نجد أن المشرع اليمني قد واكب التطورات والمستجدات المحلية والإقليمية والدولية وإن كان متأخراً قليلاً في بعض تشريعاته، إلا أنه تلزم الإشارة هنا أن وجود فجوة تشريعية (قانونية) لا تعني إفلات الجاني من العقاب أو ارتكاب فعل ضار بحجة أنه لا يوجد نص قانوني يجرمه، فلدينا أحكام الشريعة الإسلامية الغراء والتي هي مصدر جميع القوانين اليمنية وما تحويه من توصيفات فقهية ومقاصديه تدعم وبشكل كبير منع وتجريم أي سلوك يهدف إلى الإضرار

بالكليات الخمس (المال، النفس، النسل، العقل، الدين).

وكذلك لا ننسى أسس ومبادئ النظام العام في الجمهورية اليمنية والقواعد القانونية الآمرة والتي لا يجوز مخالفتها، بالإضافة إلى الإجراءات الاحترازية والتدابير الوقائية المنظمة لعمل الأنشطة التي تستخدم الأعمال الإلكترونية كالأنشطة المالية والمصرفية والحكومة الإلكترونية أو حتى إجراءات الأمن والسلامة الشخصية عند استخدام الهواتف الذكية وأجهزة الحاسوب الشخصية.

ونلاحظ أن مشروع القانون لم يتطرق إلى الجهة المحددة والمنظمة لإجراءات العناية الواجبة لتجنب الجرائم الإلكترونية، هل ستكون مركز الأمن المعلوماتي فقط أم أن هناك جهات أخرى ستشاركه الجانب الرقابي أو التنظيمي، ونقترح أنه من الضروري أن يكون هناك ضابط ارتباط)[1] بين مركز الأمن المعلوماتي والمنشأة المستخدمة للعمليات الإلكترونية سواء كانت منشأة مصرفية أو خدمية، حكومية أو خاصة، وذلك بنفس فكرة مسؤول الامتثال ومكافحة الاحتيال المالي (ضابط ارتباط البنك المركزي اليمني) الموجود في البنوك وشركات الصرافة العاملة داخل أراضي الجمهورية اليمنية.

ومن جانب آخر نجد أن القانون سالف الذكر لم يتطرق أيضاً إلى المحكمة المختصة بنظر قضايا الجرائم الإلكترونية، لكن الأمر ليس صعباً ولا معقداً، حيث أنه وببساطة يمكن للمحاكم العادية أو المتخصصة النظر في هذه القضايا بناء على أركان الجريمة الموضحة في طيات هذا البحث بحسب الاختصاص المكاني والنوعي لهذه المحاكم، وبالنسبة إلى الجرائم الإلكترونية التي تمس الاقتصاد فنقترح أن يتم نظرها عبر المحكمة الاقتصادية والتي أكد قانون الاستثمار اليمني الجديد على أهميتها.

ولعلاج مشكلة عدم توفر كادر إداري وقضائي في المحاكم والنيابات قادر على التعامل مع الأدلة الإلكترونية ومعرفة حقيقتها من زيفها، يمكن عمل دورات تدريبية تخصصية للموظفين العاملين، بحيث يكونون على استعداد تام للتعامل مع قضايا الجرائم الإلكترونية حال ورودها للمحكمة، وذلك لما سيسببه تأخير نظر هذه القضايا من خسائر فادحة للفرد والدولة، مع ملاحظة أن هذا التأخير قد يساعد المجرمين في إكمال الجريمة أو الهروب من قبضة العدالة.

(١) ضابط الارتباط: هو موظف لدى المنشأة يكون عمله استلام التعاميم والقرارات المنظمة ومتابعة تنفيذ منشأته لتعليمات الجهة المنظمة، حيث يمكن اعتباره حلقة الوصل بين المنشأة والجهة الرقابية، مثل ما تم العمل به حديثا بين جهاز الأمن وشركات الحراسة الخاصة.

وفي الأخير نجد أنه وبشكل عام إذا لم يوجد نص تجريمي في القوانين اليمنية لأي فعل ضار، فلا يعني إفلات الجاني من العقوبة وضياع حق المجني عليه، لأنه ولحسن الحظ أن جميع التشريعات الوطنية مصدرها ومرجعها الأساسي هو الشريعة الإسلامية وهو ما يعني مرونة تطبيق القانون على جميع الأنشطة الفردية أو المؤسسية، باستخدام مقاصد الشريعة الإسلامية ونصوص القرآن الكريم والسنة النبوية الشريفة.

الخاتمة

وتحتوي على النتائج والتوصيات، على النحو الآتي:

أولاً: النتائج:

١- ترتبط الجريمة الإلكترونية بالتطورات الناتجة عن ثورة تكنولوجيا المعلومات والاتصالات الحديثة، لذلك يتطلب مكافحتها الاعتماد على وسائل تقنية لا تقل حداثة عن الوسائل المستخدمة في ارتكابها.

٢- لا ترتبط الجريمة الإلكترونية بفئة معينة من الأفراد، وإنما تعتمد على القابلية للتعامل مع التقنيات الحديثة.

٣- نوعية هذه الجرائم تكون على معلومات ذات قيمة مادية وفكرية عالية.

٤- أغلب الجرائم الإلكترونية تحدث نتيجة عدم توخي الحذر والاستخدام غير المسئول لشبكة المعلومات (الإنترنت) من قبل الأفراد.

٥- تظهر خطورة الجرائم الإلكترونية في كونها عابرة للحدود وصعبة الاكتشاف والإثبات ويصعب فيها تحديد الاختصاص القضائي، لكون شبكة الإنترنت هي المجال الحيوي لارتكابها.

٦- ترتكب الجرائم الإلكترونية في عالم افتراضي غير ملموس، لكنه موجود حقيقة وغير مقيد بحدود زمنية أو مكانية، وهذا ما يتطلب إعادة النظر في بعض القواعد والمسلمات الثانوية مثل: قواعد الاختصاص القضائي وتنازع القوانين وغيرها من القواعد.

٧- جرائم التجارة الإلكترونية زادت من تكاليف المنشآت، فبالإضافة لخسائر هذه الجرائم، تتحمل الشركات تكاليف الحماية الإلكترونية.

٨- المساهمة الجنائية في مشروع قانون مكافحة الجرائم الإلكترونية لها حيز كبير، يؤكد تجليات موضوع المسؤولية العمدية والتقصيرية عند التعامل مع التقنيات والمعاملات الإلكترونية.

٩- إن التدريب الفاعل والمدروس للجهات ذات العلاقة ومنها أجهزة السلطة القضائية حتى بالنسبة للمحكمة العليا، سوف يقلل وبشكل كبير من تأخير الفصل في قضايا الجرائم الإلكترونية، وبالتالي التقليل من الخسائر الناتجة عنها.

ثانياً: التوصيات:

١- ضرورة تنظيم العمليات الإلكترونية المصرفية وغير المصرفية، وذلك من خلال القرارات والتعاميم المنظمة من الجهات الحكومية ذات العلاقة، وننصح بسن قانون خاص منظم للعمليات المالية والتجارة الإلكترونية، لما لها من تداخلات كبيرة في العديد من القطاعات الإنتاجية والخدمية الحيوية.

٢- من المفيد تعيين ضابط ارتباط بين المنشأة (مثل: مدير مركز المعلومات، مدير النظام المالي...إلخ) وبين الجهة المنظمة سواء كانت مركز الأمن المعلوماتي حال إنشائه، أو وزارة الاتصالات وتقنية المعلومات.

٣- ضرورة عمل أدلة إجراءات خاصة بوسائل وتدابير العناية الواجبة، والهادفة إلى تجنب حدوث أي مشكلات تقنية أو جرائم الكترونية.

٤- من أهم طرق ووسائل تجنب الوقوع في فخ الجرائم الإلكترونية، هو اختيار وتعيين موظفين تقنيين (أو مستخدمي الأنظمة الإلكترونية مثل الأنظمة المالية، والأنظمة الخدمية الأخرى) من ذوي الكفاءة المهنية والتدريب المتخصص، والنزاهة والأمانة الوظيفية، ونقترح أن يتم عمل تعميم من وزارة الاتصالات وتقنية المعلومات بالاشتراك مع وزارة الخدمة المدنية والتطوير الإداري لجميع الجهات الحكومية والخاصة بشروط وضوابط توظيف المشتغلين بالجانب التقني (ضباط الارتباط والعاملين التقنيين).

٥- ضماناً لاستقرار العمليات والأنشطة الإلكترونية، يلزم منع أي شخص ليس موظفاً أو لا تنطبق عليه شروط وضوابط العمل التقني من مباشرة المهام والأعمال التقنية، ما لم فتتحمل الجهة المسؤولية العمدية أو التقصيرية إذا حدثت أي جريمة الكترونية أو جريمة عادية، سواء كانت جسيمة أو غير جسيمة.

٦- ضرورة وجود سيرفرات وخوادم (داخل الجمهورية اليمنية) تجنباً لأي مخاطر اختراق محتملة، وكذلك لسهولة الصيانة الدورية والتحديث...إلخ.

٧- نوصي بتفعيل دور المحكمة الاقتصادية- عند إنشائها بمشيئة الله- بالنظر في القضايا المتعلقة بالجرائم الإلكترونية في المجالات والأنشطة الاقتصادية.

٨- من المهم تطعيم مركز الأمن المعلوماتي- عند إنشائه- بالكوادر النوعية والمتخصصة في القانون والاقتصاد، إضافة إلى مهندسي الحاسوب والبرمجيات،

وذلك لضمان سلامة وقانونية العمليات الإلكترونية، وتحقيقها للمنافع المرجوة منها للفرد والمنشأة والوطن بأكمله، وذلك لأن معظم الأنشطة الإلكترونية ذات طابع اقتصادي.

المراجع

١- مشروع قانون مكافحة الجرائم الإلكترونية في الجمهورية اليمنية، اللجنة الدستورية والقانونية والقضائية، مجلس الشورى اليمني، ٢٠٢٥م.

٢- العبدلي، محمد جبار جدوع وآخرون، المسؤولية عن الجرائم الالكترونية العابرة للحدود وفقاً لقواعد القانون الدولي، مجلة آداب الكوفة، العدد ٦٥، ٢٠٢٥م.

٣- الجرموزي، أكرم أحمد، أهمية الأمن السيبراني واستراتيجيات الوقاية لدى القطاع المصرفي، ورشة بعنوان: دور القضاء في مواجهة الجرائم الإلكترونية وفض المنازعات المصرفية، وزارة العدل وحقوق الإنسان، المعهد العالي للقضاء، ٢٠٢٥م.

٤- موسى، روسم عطية، أثر التنظيم الجنائي للعلاقات التعاقدية الاقتصادية على النظرية العامة العقد، مجلة أكاديمية الدراسات العليا للبحوث والدراسات العلمية، العدد السادس، يونيو، ٢٠٢٢م.

٥- شيخ، عبد الصديق، الوقاية من الجرائم الإلكترونية في ظل قانون ٠٤-٠٩، مجلة معالم للدراسات القانونية والسياسية، المجلد ٤، العدد ١، لسنة ٢٠٢٠م، الجزائر.

٦- بن عمر، ياسين، المعالجة القانونية للجرائم الإلكترونية في القانون الجزائري والتشريعات المقارنة (التشريع المغربي والإماراتي أنموذجاً)، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد ٣، ٢٠١٩م.

٧- جويل، كرتزمن، ترجمة محمد العصيمي، دار الميمان للنشر والتوزيع، الطبعة الأولى، ٢٠١٢م.

٨- الحمداني، محمد حسين، جريمة سرقة المعلومات المعالجة آليا، مجلة الرافدين للحقوق، المجلد ١٢، العدد ٤٧، ٢٠١١م.

٩- البقلي، هيثم عبدالرحمن، الجرائم الإلكترونية الواقعة على العرض، دار العلوم، الطبعة الأولى، ٢٠١٠م.

١٠- شمس الدين، أشرف توفيق، الحماية الجنائية المستند الإلكتروني، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، ٢٠٠٣م.

١١- الوائلي، نادية صالح مهدي، الآثار الاقتصادية للجرائم الالكترونية، مجلة الإدارة والاقتصاد، المجلد الثالث، العدد التاسع، كربلاء، بدون سنة.

١٢- حسين، فاروق سيد، التجارة الالكترونية وتأمينها، الطبعة الأولى، ٢٠٠١م، الجيزة.