النظام القانوني الملائم لطبيعة الجريمة المعلوماتية

أ مدور جميلة

أستاذة مساعدة " أ "

كلية الحقوق والعلوم السياسية جامعة محمد خيضر – بسكرة

ملخص

نسعى من خلال هذه المداخلة إلى تحديد الطبيعة القانونية للجريمة المعلوماتية للتأسيس عليها ومن ثم النظر في كيفية معالجتها والتصدي لها بتقرير العقوبات المناسبة لها ذلك أن هذه الجريمة تمثل أحد مظاهر تطور فن الإجرام الذي ما دئب يواكب التطورات الحادثة في المجتمع ويحاول الاستفادة منها إلى أقصى حد خاصة وأن التطور التكنولوجي يوفر له الفاعلية والسرعة وإمكانية التستر والتملص من العقاب، كما أن قانون العقوبات الحالي في تصديه للجريمة لم يتجاوز نطاق الجرائم التقليدية، ورغم وجود بعض أوجه الشبه بين الجريمة المعلوماتية وبعض تلك الجرائم إلا أن الأمر يحتاج إلى معالجة خاصة وتفصيلية تأخذ بعين الاعتبار الطبيعة المميزة لهذ الجريمة، وقبل تقرير العقوبات لابد من وجود تشريع تنظيمي يتكفل ببيان الأحكام التي تنظم خدمات النشر على المواقع الالكترونية وتبادل المعلومات ويحدد مسؤولية الأشخاص الذين يقومون بعمليات النشر والتبادل وكيفيات الحصول على ترخيص للحصول على معلومة ونشرها وشروطه ونطاقه ، سواء كان ذلك بإضافة مواد إلى القانون المدني أو بتقنين خاص.

ونريد من خلال هذا البحث التعرض لبعض الجوانب المهمة في التشريع المراد وضعه من قبيل معرفة متى نعتبر المعلومة لها ماهية قانونية وأنه يتوجب حمايتها، ومتى نعتبر الدخول إلى المعلومة الالكترونية غير مشروع ؟ وكذلك بالنسبة لتداولها واستخدامها واستغلالها؟

كما نريد من خلال هذا البحث إثارة بعض الإشكالات التي يواجهها تطبيق قانون العقوبات كتلك المتعلقة بمسألة الإثبات.

المنارة للاستشارات

مقدمة:

إن الجريمة كفعل غير مشروع حدث قديم لازم المجتمعات عبر امتداد التاريخ الإنساني، غير أن التقدم التقني أتاح الفرصة لإلباسها ثوبا جديدا يمكنها من التخفي وفي لمح البصر، فلا نرى إلا آثارها وكأنها من أفعال السحر والشعوذة.

لقد وجد المجرمون ضالتهم في المزايا التي تتمتع بها النظم المعلوماتية وهي على الأخص السرية في العالم الافتراضي والسرعة والفعالية إضافة إلى القدرة على إخفاء الآثار التي تشير إليهم، وهذا كل ما يلزم لارتكاب الجريمة بنجاح والعود إليها مرارا وتكرارا، بل وإغراء من كان حذرا على خوض غمار المغامرة والتجربة.

ولا يتوقف إغراء المزايا عند هذا الحد في ظل العولمة كعنصر آخر يضاف إلى العناصر الأخرى ويعطيها بعدا آخر وهو البعد المكاني اللامحدود، فتتخطى الجريمة حدود الدول مما يزيد من صعوبة محاصرتها في نطاق معين، وأصبح أمن المعلومات ومراقبة شبكة الانترنت وما تقدمه من خدمات من الإشكالات المطروحة التي تبحث عن حلول لها من الناحيتين الفنية والقانونية؛ فأما الناحية الفنية فلها أهلها من أصحاب الاختصاص، وأما الناحية القانونية فإني أقول أن الفكر القانوني لا ينبغي أن يقف ساكنا وحائرا أمام هذا التسارع المذهل للتكنولوجيا أو يقف عاجزا أمام الاستخدام غير المشروع لها وإلحاق الضرر بالغير، بل عليه أن يسعى جاهدا لابتكار الطرق والصيغ المناسبة من أجل مراقبة جميع التصرفات الجارية في العالم الافتراضي والبحث عن المعايير الموضوعية لتصنيف تلك التصرفات وإيجاد صيغ وآليات فعالة للتنسيق والتعاون الدولي من أجل التغلب على مشكلة زوال الحدود الجغرافية أو اختلاف التشريعات وما يترتب عن ذلك من نتائج تصب في خانة إفلات الجاني من العقاب، وللتمكن من كل ذلك يتعين على المختصين في مجال التشريع فهم طبيعة الجريمة المعلوماتية انطلاقا من فهمهم لطبيعة المعاملة الإلكترونية وكيفية إجرائها، فهذا الجانب الفني أساسي ولا غنى عنه، ثم تحديد الوصف أو الأوصاف التي تجعلها جريمة ليتسنى لا حقا وضع النظام القانوني الملائم لها ومعرفة نوعية وصيغ النصوص التي يجب تطبيقها على خدمات الانترنت، لأن الحكم على الشيء جزء من تصوره وإلا كان الحكم خاطئا لا محالة، وتقديرا لأهمية هذا الجانب كمدخل للحل القانوني اخترت أن تكون مداخلتي عن النظام القانوني الملائم لطبيعة الجريمة المعلوماتية.

إن التصدي للجريمة المعلوماتية بتقرير العقوبات المناسبة يقتضي منا كما أسلفت تحديد الطبيعة القانونية لهذه الجريمة وهو ما يتوقف على بيان العناصر المكونة لها وتحديد ماهية هذه العناصر وخصائصها ومقارنتها بنظيرتها في الجريمة العادية، ولعل أهم هذه العناصر هو المحل وهو موضوع الجريمة والقصد الجنائي الذي به تتقرر الحماية القانونية، إضافة إلى العنصرين الآخرين وهما الجاني والمجني عليه، ثم ننظر في نوع ومضمون النصوص التي يجب تطبيقها على خدمات الانترنت وذلك بالنظر إلى طبيعة الجريمة المعلوماتية وما تتميز به من خصوصية، ولذلك سنقسم هذا البحث إلى مبحثين:

المبحث الأول: أركان الجريمة المعلوماتية

المبحث الثاني: النصوص التشريعية الملائمة لطبيعة الجرائم المعلوماتية

المبحث الأول: أركان الجريمة المعلوماتية

الجريمة المعلوماتية لا تختلف عن الجريمة العادية في الأركان التي يجب استيفاؤها في الفعل ليعتبر مجرما، وأن ذلك بمثابة المبدأ، فلابد من توافر المحل باعتباره الركن المادي

المنارة للاستشارات

ووجود القصد الجنائي الذي يخرج الفعل من الإباحة إلى الحظر ويمثل الركن المعنوي في الجريمة ووجود الجاني والمجني عليه.

المطلب الأول: المحل

المحل هو موضوع الجريمة ويتمثل في المعلومة الإلكترونية وهي الركن المادي للجريمة.

والمعلومة بشكل عام هي الفكرة إذا تبلورت في الذهن وأصبحت جاهزة لإيصالها إلى الغير لتحدث أثرا ما؛ قد يكون تصورا معينا أو علما أو قناعة أو رغبة في سلوك أو موقف ما...، وهي تختلف عن البيانات من جهة أن هذه الأخيرة عبارة عن مجموعة من المعطيات أو القياسات أو النتائج الأولية أو الحقائق الجزئية التي تحتاج إلى تحليل ومعالجة وقراءتها في سياق معين من أجل التوصل إلى نتائج أو حقائق ذات مدلول متكامل وأكثر شمولا.[i]

وهذه البيانات قد تتخذ صورة أرقام أو حروف أو رموز أو أشكال خاصة وعند تجميعها وتحليلها وترتيبها في سياق معين يمكن أن تعبر عن فكرة أو موضوع أو حدث أو هدف معين، فالبيانات هي المادة الخام للمعلومات.[ii]

والمعلومة الإلكترونية هي موضوع العملية التي يطلق عليها المعلوماتية عند القيام بالمعالجة المنطقية لكم هائل من المعلومات بالاستعانة بأجهزة الحاسوب واعتماد طرق فنية خاصة ، وإن ما تتطلبه هذه العملية من وسائل التخزين والمعالجة والعرض والحفظ تشكل النظام المعلوماتي.[iii]

المطلب الثاني: القصد الجنائي وتقرير الحماية القانونية للمعلومة الإلكترونية

إن المعلومة وفقا للبيان السابق هي نتاج النشاط الذهني، ولذلك فهي ملك لصاحبها الذي تبلورت لديه، وبناء على ذلك فإنه المخول بالاحتفاظ بها لنفسه أو نقلها وإيصالها للغير بمقابل أو بدونه، وهذا ما يعبر عنه بحق الملكية الفكرية، واستخدام هذه الملكية الخاصة بغير إذن صاحبها يمثل تعديا على حق الغير، وإذا اقترن هذا الاستخدام بسوء نية انطوى الفعل على جرم ما، ويتحدد وصف هذا الجرم بالنظر إلى هدف المستخدم والأثر الذي رتبه فعله؛

فقد يكون الهدف من الدخول قاصرا على مجرد الاطلاع وقد يكون بدافع التجسس والتصرف في البيانات والمعلومات وبرامج التشغيل وأنظمة التحكم، سواء بالعبث بها أو نسخها أو محوها أو تغيير محتواها أو نقلها وإرسالها للغير أو إعاقة تشغيل نظم معالجتها وتعطيل الأجهزة... ومحاولة الاستفادة من ذلك بأي شكل من الأشكال.[iv]

وهذا الدخول غير المشروع لمواقع البيانات والمعلومات قد يكون بقصد الإضرار أو بدونه بأن يكون غرض المستخدم مجرد اللهو وإرضاء الذات من خلال الشعور بالتفوق على الآلة وواضعي برامج التشغيل وإظهار ضعف أنظمة الأمن المعتمدة، ولكن رغم عدم قصد الضرر في هذه الحالة فإن أثره قد يمس الغير، وقد يتجلى في صورة ضرر مادي أو معنوي لأن هذا السلوك غير الواعي قد يتسبب بأضرار جسيمة.[v]

إن الدخول غير المشروع لمواقع البيانات والمعلومات واستخدام الملكية الفكرية ومحاولة الاستفادة من كل ذلك بغير إذن صاحب الحق فيها لا يعتبر مجرد غش كما ذهب إلى ذلك البعض، بل هو جريمة موضوعها الاعتداء على حق الغير، كذلك الأمر في حال التعرض لأمن وسلامة الأنظمة المعلوماتية وسرية البيانات والمعلومات، فلا تختلف من حيث الجوهر عن الجرائم التقليدية إلا في الوسيلة وهي استخدام الأنظمة المعلوماتية

المنارة للاستشارات

والموضوع حيث أنه ينحصر في المعلومات والبيانات والأنظمة والبرامج المتصلة بجهاز الحاسوب، أما الفروق التي يذكرها البعض من قبيل عدم وجود مسرح جريمة ملموس كما في الجريمة العادية وكون الجناة يتميزون بمواصفات معينة.. فلا تعد فروقا جوهرية تؤثر على وصف التجريم.

وعليه فإن الجريمة المعلوماتية هي مجموعة الجرائم المرتبطة بعلم المعالجة المنطقية للمعلومات[vi]، أو أنها كل سلوك غير مشروع يتعلق بالمعلومات المخزنة في جهاز الحاسوب لتحقيق مكاسب غير مشروعة أو إلحاق ضرر بصاحب الجهاز[vii].

وتحدث الجريمة المعلوماتية بأساليب وطرق متنوعة، وتظهر بأشكال وصور متعددة ولا يمكن حصرها لأنها في تطور مضطرد وتساير تسارع التقدم التكنولوجي، منها ما هو موجه للحواسيب قصدا كاختراقها لتدمير ما فيها من برامج وبيانات باستخدام الفيروسات، ومنها ما يستخدم فيها جهاز الحاسوب كأداة بقصد تحقيق مكاسب معينة كسرقة أرقام بطاقات الائتمان واستخدامها في شراء المنتجات عبر شبكة الأنترنت وسرقة كلمات المرور للدخول إلى مواقع إلكترونية محددة والاطلاع على ما فيها من معلومات للعبث بها أو سرقتها، والقيام بعمليات النصب والتزوير[viii]...، لأجل ذلك يعتبر هذا النوع من الجرائم من أهم التحديات التي تواجه التجارة الإلكترونية والأعمال المصرفية ومختلف المعاملات التي تتم في الفضاء الإلكتروني المفتوح [ix]؛

فالتجارة الإلكترونية يخشى أن تكون ملاذا لغسل الأموال القذرة الناتجة عن التجارة غير المشروعة كالمخدرات والأسلحة والاتجار بالبشر والأعضاء البشرية... ومكمن التحدي هنا يتمثل في صعوبة التعرف على مصدر المال وإمكانية إجرائها بسرية تامة إضافة إلى البعد الدولي الذي يعتبر عاملا مساعدا للتحرك والإفلات من الرقابة والمتابعة.

كما يخشى على هذه التجارة من تزوير الاتفاقات والعقود المبرمة بين أطرافها؛ بتزوير العقد أو التوقيع والقيام بالنصب على أطراف المعاملة الحقيقيين للفوز بما يمنحه العقد أو الاتفاق من حقوق ومزايا.

وبالنسبة للأعمال المصرفية يخشى على الوسائط الإلكترونية باعتبارها وسيلة التعامل مع المصارف أن تتخذ كوسيلة لسرقة أموال الناس بالاستيلاء على البطاقات الائتمانية وتحويل الأرصدة من حسابات إلى أخرى والعبث بالمستندات الإلكترونية كالشيك والكمبيالة والبطاقات الممغنطة...

وإذا كانت المعلومة على قدر من الأهمية فإنه قد يجري مقايضتها أو نشرها، والمقايضة عادة تكون في حال التجسس على الأسرار الصناعية إن في مجال صناعة السيارات أو صناعة الأدوية أو تكنولوجيا المعلومات وغيرها من المجالات الحيوية، وأما النشر فيكون بغرض التشهير وكشف أسرار المجني عليه صاحب المعلومات أو البيانات، وكمثال على ذلك ما قام به موقع ويكيليكس من نشره أخبارا سرية تتعلق بالبنتاغون والحرب على العراق وغيرها من الأخبار، فإن الفعل في نظر الحكومة الأمريكية يعد جريمة تمس الأمن القومي لذلك سعت للقبض على مسؤول الموقع واعتبرته متهما بارتكاب الجريمة.

المطلب الثالث: الجاني والمجني عليه في الجريمة المعلوماتية

المنارة للاستشارات

قد يكون الجاني شخصا طبيعيا أو معنويا، واحدا أو أكثر كما في الجريمة العادية، وكذلك بالنسبة للمجني عليه.

ونظرا لما تتطلبه الجريمة المعلوماتية من تقنية عالية وتحكم في نظم الحواسيب وبرامج التشغيل فإن ما يميز جناتها - كأشخاص طبيعيين - هو أنهم في الغالب من النابغين المتميزين والمتفوقين في مجال التكنولوجيا والمعلوماتية الذين يسعون إلى الاستفادة من مهاراتهم وخبراتهم، ونجد منهم الهواة الذين يرتكبونها بدافع الفضول والتسلية وإظهار التفوق ومنهم المحترفون الذين يمارسونها كحرفة عن سبق إصرار وتعمد بعد أن اكتسبوا الخبرة اللازمة ويسعون لتحقيق مكاسب معينة على حساب الغير أو لمجرد الإضرار بالغير، ولذلك فإنه من الوارد أن يتحول الهواة إلى محترفين بانجذابهم إلى الجريمة ومغرياتها[x].

والمحترف يكون في العادة من أحد العاملين أو المستخدمين في مؤسسة تدار بالنظام المعلوماتي، وقد يحتاج الأمر إلى الاستعانة بآخرين من أجل المساعدة الفنية والمادية.[xi]

أما الشخص المعنوي فقد يكون أحد الكيانات المستقلة، سواء كان تابعا لدولة ما أو لا[xii]، وقد يكون مؤسسة مالية أو غير مالية، لها وجود في الواقع أو في العالم الافتراضي، قد تكون حقيقية أو همية، ولعل أشهر المؤسسات التي تتهم بجرائم غسل الأموال عبر شبكة الأنترنت شركات الأوف شور[xiii].

المبحث الثاني: النصوص التشريعية الملائمة لطبيعة الجرائم المعلوماتية

ببيان طبيعة النصوص التي يجب تطبيقها على الجريمة المعلوماتية بالتركيز على الجوانب ذات الخصوصية والتي تجعلها متميزة عن الجرائم العادية مع الأخذ بعين الاعتبار بأوجه الشبه بينهما وهو ما يحتاج إلى ضرورة التفرقة بين ما هو جوهري وما ليس كذلك، ونظرا لأن الوقاية خير من العلاج فعلى المشرع أن يبادر أولا إلى تنظيم خدمات الانترنت والمعاملات الإلكترونية تنظيما شاملا يغطي كافة جوانبها ويتعرض لكل تفاصيلها وأن يضع النظام القانوني لمسؤولية النشر المعلوماتي ويبين كيفية التعامل مع الجاني من دولة أخرى أو في حال وقوع الجريمة في دولة أخرى وكيفية معالجة مشكلة اختفاء آثار الجاني في الجريمة المعلوماتية.

المطلب الأول: طبيعة النصوص الواجب تطبيقها على خدمات الانترنت

بسبب شيوع المعاملات الإلكترونية بين الناس ونظرا لاجتماع المزايا والمخاطر فيها يتعين على المشرع التدخل لتنظيمها وجعلها أكثر أمانا، بأن يبين موقفه منها ويضع القواعد التي تحكمها

وينظم أدوات التعامل وآلياته ويعالج آثاره من التزامات وحقوق من جهة التنفيذ والتحصيل، ويعرض للمعوقات المحتملة وكيفية التعامل معها، ويحدد أطراف المعاملة وطبيعتها والمسؤوليات التي تقع على كل طرف، فليس من الصواب أن يترك لهؤلاء الأطراف وضع قواعد التعامل لاحتمال أن يكون أحدهم في مركز أقوى فيلحق الطرف الآخر الغبن جراء ذلك، وقد يخل أحدهم بالقواعد المتفق عليها، وكمثال على ذلك أن يخل المصرف بقاعدة سرية المعاملات المصرفية، فيكشف عن حسابات عملائه وودائعهم وخزائنهم أو عن العمليات والأعمال المرتبطة بعلاقتهم بالمصرف، أو أن لا يحتاط بما يكفي لمنع المتطفلين من الاطلاع على حسابات عملائه أو إتلاف مستنداتهم الإلكترونية، أو أن يجري تحويلا بطريق الغلط...، ففي هذه الحالات وغيرها على المشرع أن يحدد الإجراء الواجب اتخاذه تجاه من أخل بالتزامه، وأن يبن طبيعة المسؤولية المترتبة عليه.

المنارة للاستشارات

المطلب الثاني: طبيعة النصوص الواجب تطبيقها على الجريمة المعلوماتية

يرى البعض أن التشريع في مجال الجريمة المعلوماتية يجب أن يراعي التمييز بين نوعي المجرمين الهواة والمحترفين على أساس توافر القصد الجنائي بالنسبة للمحترفين وانتفائه بالنسبة للهواة، بأن يكون تقدير العقوبة بالنظر إلى الهدف من الدخول غير المشروع إلى البيانات،[xiv] وهو رأي له وجاهته لأنه من المبادئ المقررة في التشريع الجنائي عدم إطلاق وصف التجريم من دون وجود هذا العنصر الهام في قيام الجريمة، ولكن بالنظر إلى الأضرار الجسيمة التي قد يلحقها التلاعب والعبث بالبيانات والمعلومات ذات القيمة الكبيرة وذات السرية الخاصة قد لا يكفي ترتيب المسؤولية المدنية لجبر الضرر، وقد لا يكون مجرد التعويض المالي مناسبا أصلا، كما قد يعجز المدين به عن الوفاء به، وهو ما يطرح تساؤلا عن الخيارات البديلة الممكنة كخيار التأمين ضد هذا النوع من المخاطر وإقرار تشريع خاص بذلك.

ومن الأمور التي يجب أن تراعى في تقدير العقوبة طبيعة الفعل الذي تم؛ إن كان مجرد تصفح للبيانات أو نسخا أو تعديلا للعبث أو التضليل أو تزويرا أو تحويلا أو تعطيل الجهاز أو تخريب المعلومات والبيانات المخزنة فيه... والنظر فيما لو ترتب عن ذلك آثار أخرى كتحويل الأرصدة المالية ومقدار ما حول منها...

ولئن بدا مجرد الاطلاع وتصفح المعلومات أمرا هينا، فإنه في حقيقة الأمر ليس كذلك لأنه إن كان بغير إذن صاحب الشأن فهو تجسس على الغير.

أما التعديل فقد يكون فيه تفويت مصلحة أو إحداث إرباك بمستوى معين أو ضرر، وتحديد الضرر يتوقف على طبيعة التعديل المحدث.

وأما النسخ فإن أثره يتوقف على الغرض منه، ولكن في كل الأحوال يوحي بسوء النية.

وبالنسبة لسائر الأفعال فالضرر فيها ظاهر، ويبقى تقدير الضرر متوقفا على نتيجة الفعل.

وفي جميع الحالات السابقة يجب أن يؤخذ بالحسبان الأثر المترتب وحجم الضرر وما إذا كان يمكن جبره كليا أو جزئيا أو لا.

على المشرع أن يبين موقفه من إهمال المجني عليه الحفاظ على بياناته وسرية معلوماته كالرقم السري لبريده أو بطاقاته الائتمانية وسائر المستندات.

وفي حال العمل على تضييع الأدلة والآثار التي من شأنها أن تكشف عن هوية الجاني أو ترشد إليه، فإنه ينبغي معاملته بعد التمكن من ضبطه على أنه فار من العدالة ويحاكم على هذا الأساس.

ومن الإشكالات التي يجب على التشريع الجنائي أن يعالجها هي كيفية التعامل مع الجاني من دولة أخرى أو وقوع الجريمة في دولة أخرى، وذلك بالبحث عن إجراءات وآليات التنسيق مع الدول الأخرى وإبرام اتفاقات معها لتسليم المجرمين وتوحيد التشريعات الجنائية في موضوع الجريمة المعلوماتية غير أن الاتفاقات الثنائية قد لا تكفي ولا تفي بالغرض وهو سد جميع المنافذ لمحاصرة الجريمة والمجرمين، ولا سبيل إلى ذلك إلا باجتماع المجتمع الدولي كافة، وهو هدف يبدو بعيد المنال من الناحية الواقعية بالنظر إلى

المنارة للاستشارات

اختلاف التشريعات وتضارب المصالح ووجود مصالح خفية تعتبر استراتيجية لدى بعض الدول قد تفقد الاتفاقات المعلنة مصداقيتها وفاعليتها.

المطلب الثاني: كيفية التعامل مع مشكلات إثبات الجريمة الإلكترونية من خلال التشريع

من أهم المشكلات التي تواجه تطبيق التشريع العقابي في مجال الجريمة الإلكترونية وتؤرق العاملين فيه ضبط الجاني وتحديد هويته، وعلى التسليم بصعوبة المهمة، فإنه ينبغي استغلال الوسائل والطرق المتاحة إلى أقصى حد، والتشجيع على تعلم التقنيات الحديثة خاصة فيما يتعلق بالأساليب الفنية المساعدة على فك الشفرات، والسعي الدؤوب للحصول على ما هو أحدث وهو ما يتطلب توفير تكوين عال ومتخصص لكل العاملين في هذا الشأن من قضاة وضباط شرطة وخبراء فنيين للاستعانة بهم عند الحاجة.

إنه لا يمكن التصدي للجريمة الإلكترونية ما لم تكن الوسائل المستخدمة متكافئة أو أكثر تفوقا عن تلك التي استخدمت في ارتكابها، ولا سبيل إلى ذلك إلا عن طريق التعليم والتدريب والتطوير والتحفيز.

وفي سياق البحث عن حلول لمشكلات الإثبات الإلكتروني على المشرع أن يحدد طبيعة الآثار المادية الكافية لإدانة الجاني ووسائل وطرق الحصول عليها وضوابط فك الشفرات والحالات التي تستدعي ذلك ضمن تشريع خاص بالإجراءات الجزائية يأخذ بعين الاعتبار بالمبادئ المقررة في التشريعات الجزائية للجرائم العادية كاحترام الخصوصية وأن المتهم برئ حتى تثبت إدانته ونحو ذلك.

خاتمة

إن الجريمة المعلوماتية هي جريمة متى تكونت أركانها وبالأخص الفعل غير المشروع والقصد الجنائي، وأن الطابع التكنولوجي الذي يميزها ما هو إلا أداة للجريمة جعلها أكثر يسرا وفاعلية وسرعة وأعطى للجاني ميزة إضافية هي القدرة على التخفي وربما التملص من العقاب، غير أن ذلك لا يتوقع أن يكون إلى ما لا نهاية لأن التكنولوجيا في تطور مستمر، وأثناء تطورها قد تقدم حلولا مثيرة، وقد تتحول هذه الحلول إلى مشكلات.. وهكذا دواليك، وما على المشرع إلا أن يساير حركة التطور بنفس نمط سرعتها ويتفاعل مع ما تقدمه من ابتكارات قبل أن يبادر المجرمون إلى ذلك، وأن يجعل تلك الابتكارات في خدمة المجتمع بتنظيم العلاقات الناشئة فيه انطلاقا مما تحدثه من روابط بين أفراده، فإن فاته شيء من ذلك وبادره المجرمون بما يعرض استقرار المجتمع وأمنه للخطر سارع بفرض التشريع العقابي الذي من شأنه أن يحد من نشاط هؤلاء وانحرافهم.

الهوامش

[i] محمد علي سالم وحسون عبيد هجيج، الجريمة المعلوماتية، (مجلة جامعة بابل للعلوم الإنسانية، العراق، م14، ع2، 2007)، ص86، عبد العال الديربي، الجريمة المعلوماتية: تعريفها، أسبابها، خصائصها، (المركز العربي لأبحاث الفضاء الإلكتروني، 2013، نقلاعن: www.acconline.com تم الاطلاع يوم2015/11/10)، عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، (دار الفكر العربي، مصر، ط1، 2002)، 278/2.

المنارة للاستشارات

[ii] المراجع نفسها
[iii] المراجع نفسها.
[iv] محمد علي سالم، ص88.
[v] حازم نعيم الصمادي، المسؤولية في العمليات المصرفية الإلكترونية، (دار وائل للنشر والتوزيع، الأردن، ط1، 2003 ص14-15، عبد الفتاح بيومي، النظام القانوني لحماية التجارة الإلكترونية 22/2، محمد على سالم، ص88.
[vi] محمد علي سالم، ص78.
[vii] المرجع نفسه.
[viii] جريمة غسل الأموال عبر شبكة الانترنت، عبد الفتاح بيومي حجازي، (دار النهضة العربية، ط1، 2009)، ص45-48، 69)، حازم الصمادي، ص14-17.
[ix] عبد الفتاح بيومي، جريمة غسل الأموال، ص9، حازم الصمادي، ص14، 34.
[x] عبد الفتاح بيومي،جريمة غسل الأموال، ص48-49، محمد علي سالم، ص89.
[xi] اعبد الفتاح بيومي،لنظام القانوني للتوقيع الإلكتروني، ص70، محمد علي سالم، ص89.
[xii] من الشواهد الدالة على لجوء بعض الدول إلى أسلوب الإجرام الإلكتروني (حرب غير معلنة) قيام الكيان الصهيوني بواسطة جهاز مخابراته بضرب أحد المفاعلات النووية لإيران سنة 2014 بإرسال فيروس لنظام تشغيله فأحدث أضرارا به، وقد أثار الخبر ضجة إعلامية.
[xiii] شركة الأوف شور هي شركة يكون مقرها في دولة ما وتباشر أعمالها فيها ولكن من أجل أن تنفذ خارج تلك الدولة، فنشاطها محصور خارج الدولة التي يكون فيها مقرها الرئيسي، وهي بذلك تختلف عن الشركة متعددة الجنسيات. أنظر: عادل إلياس بطرس،الوجيز في الشركة القابضة وشركة الأوف شور، (المؤسسة الحديثة للكتاب، لبنان، ط1، 2013)، ص37.
[xiv] عبد العال الديربي، ص 88-89.

المنارة للاستشارات