فعالية التشريعات العقابية في مكافحة الجرائم الإلكترونية

الأستاذة حسينة شرون
كلية الحقوق والعلوم السياسية
جامعة محمد خيضر بسكرة

مقدمة:

تعد الأعمال الالكترونية اللاسلكية أحد تجليات حالة الدمج بين نظم الحوسبة والاتصال، بل هي فتح جديد من فتوح التقنية في حقلي الاتصال والحوسبة، وتعد أبرز تطبيق لفكرة تكاملية وسائل تقنية المعلومات وتسهيل استخدامها فتقنية المعلومات استلزمت ضمن مسيرة تطورها، جهودا مبدعة في حقل صناعة الحواسيب ومكوناتها المادية (كأجهزة) وفي حقل صناعة البرمجيات التي مثلت الدم الحي والمتدفق لنظم المعلومات وأتاحت عبر تطبيقاتها أوسع إفادة من أجهزة الكمبيوتر. وأما نظم ووسائل الاتصالات، فقد شهدت تطورا مذهلا نقلها من الاستخدام البدائي لشبكات التلغراف، مرورا باستخدام أنماط متعددة كالأسلاك النحاسية فالضوئية وغيرها – تنامت من حيث السعة والكفاءة – من أجل فعالية وسرعة وسائل التخابر ونقل البيانات، إلى أن وصلت إلى مرحلة الاتصال عبر الأقمار الصناعية ونقل البيانات عبر شبكات الهاتف ومختلف ووسائل الائتمار عن بعد والتبادل الاتصالي اللاسلكي الذي يجد تجليه في وقتنا الحاضر بظاهرة (الهاتف الخليوي).

إن الدمج والتزاوج بين وسائل الحوسبة والاتصال، أفرز مفهوما جديدا لكل منهما وخلق إطارا أوسع يعرف بتقنية المعلومات في وقتنا الحاضر، هذا التزاوج الذي قام على فكرة توفير وسائط وبيئات لمعالجة البيانات وتبادلها، وكانت شبكات المعلومات – وفي مقدمتها الانترنت – العنوان الجديد لعصر المعلومات أتاحت وتتيح التبادل الواسع لمختلف أنماط المعلومات وتتيح التراسل الفوري، وفي الوقت ذاته خلقت بيئة للاستثمار والأعمال فيما يعرف بالأسواق الافتراضية أو بيئة الأعمال الالكترونية.

فقد انطلقت الأعمال الالكترونية بمختلف صورها ونمت بشكل واسع، وتنامي سوق التجارة الالكترونية وتنامت الأعمال الالكترونية ما بين المؤسسات الإنتاجية والخدماتية، كما برزت ظاهرة الهواتف النقالة التي تتيح تلقي المعلومات المالية والاستثمارية واستعراض مواقع مؤسسات الأعمال على شبكة الانترنت بفضل بروتوكولات اتصالات ملائمة مثل (الواب

Web) وبلوتوث وغيرهما. ويعد أوسع تطبيق للأعمال الالكترونية بواسطة الهواتف النقالة الأعمال المصرفية الالكترونية أو ما يعرف ببنوك الواب أو بنوك الخليوي.

ولأن تقنية المعلومات عموما، أفرزت ولا تزال تفرز تحديات قانونية، فان الجهات التشريعية والقانونية في النظم المقارنة أولت تأثير تقنية المعلومات على النظم القانونية عناية استثنائية وذلك من أجل تنظيم أثرها وإيجاد البيئة الملاءمة لضمان سلامة استخدام هذه التقنية وتشجيع اعتمادها وسيلة للأداء والإنتاج. ومن بين أكثر التحديات القانونية إثارة للجدل وتأثيرا على الثقة بالتقنية وتطبيقاتها مسائل أمن المعلومات والاعتداءات الواقعة عليها.

إن هذه المداخلة تهدف إلى الوقوف على أبرز التحديات القانونية الجزائية في بيئة الأعمال الالكترونية، أما المعالجة التفصيلية فإنها أمر متعذر في ضوء مساحة البحث المتاحة، بحيث نكتفي بالأطر الرئيسة محيلين القارئ الكريم إلى الأبحاث والدراسات التفصيلية في هذا الحقل.

وعلى هذا الأساس فإننا سنتطرق أولا إلى الإطار المفاهيمي للجرائم الإلكترونية من خلال تحديد تعريف لها وبيان خصائصها وأنواعها حتى يتسنى لنا معرفة مدى ملائمة التشريعات العقابية الموجودة لها.

وفي نفس السياق وجدنا أنه من اللازم التعرف على الإطار التشريعي للجرائم الالكترونية على مستوى التشريعات الغربية والتشريعات العربية قبل التطرق إلى واقع مكافحة الجرائم الالكترونية واتجاهاتها التشريعية في الجزائر.

أولا/ الإطار المفاهيمي للجرائم الالكترونية:

إن ظاهرة الجرائم الإلكترونية تعد ظاهرة إجرامية مستحدثة، وذلك لارتباطها بتكنولوجيا المعلومات والاتصالات والكومبيوتر، وقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع للجرائم الالكترونية، كما تزاحمت المصطلحات في التعبير عن مدلولها، إذ نجد من يعتمد مصطلح الجرائم المعلوماتية، وأخر يسميها جرائم التقنية العالية، وأخر يربطها بجهاز الكومبيوتر فيطلق عليها تسمية جرائم الكومبيوتر أو جرائم الحاسب الآلي، وهناك من يربها بالشبكة العنكبوتية فيسميها جرائم الانترنيت...

وإن كانت كل هذه التسميات مرتبطة بالتقنية الرقمية المتطورة الحديثة، فإننا نجد انه من الضروري ضبط المفاهيم وتحديد مدلول الجرائم الالكترونية من أجل تحديد الضوابط القانونية التي تحكم تلك الجرائم.

ونعرض فيما يلي لأهم آراء الفقه التي حاولت محدد لهذا النوع المستحدث من الجرائم، ثم نبين خصائصها، لنتطرق إلى أنواع الجرائم الالكترونية وأنماط ارتكابها.

أ/ تعريف الجرائم الالكترونية:

يجمع كل من بحث في مجال الجرائم الالكترونية أو المعلوماتية أو جرائم الكومبيوتر أو الحاسب الآلي أو الغش المعلوماتي، على أن هذه الجرائم تشمل العديد من الأفعال المتنوعة غير المشروعة في استغلال ما ينتجه الكومبيوتر من معلومات بغرض ارتكاب جريمة ما، سواء بإدخال بيانات أو سجلات مزورة من الحاسب الآلي، أو تدمير بيانات وبرامج الكومبيوتر أو سرقة الخدمات والأموال المسجلة فيه.

ولارتباط هذا النوع من الجرائم بجهاز الكومبيوتر أكثر من غيره من الأجهزة الالكترونية، فقد اتجه الفقه في محاولة وضع تعريف محدد لماهية الجرائم الالكترونية إلى استعمال الجريمة المعلوماتية كمرادف لها.

وحيث أن الجريمة الالكترونية حديثة النشأة، فقد نتج عن ذلك انعدام الاتفاق على تعريف موحد لها ومن ذلك نجد التعاريف التالية:

فقد عرفتها الشرطة البريطانية بأنها:" استعمال شبكة الحاسوب لعمل إجرامي"، بينما عرفها الاتحاد الأوروبي بأنها:" كل مخالفة جرمية ترتكب ضد أو باستعمال شبكة الحاسوب"[1].

في حين يذهب أغلبية الفقه إلى المزاوجة بين الجريمة الالكترونية والجريمة المعلوماتية والتعامل معهما كمترادفين، وفي هذا الإطار ينقسم الفقه بين اتجاهين[2]؛ الاتجاه الأول يضيق من مفهوم هذه الجرائم فيعرفها بأنها:" كل فعل غير مشروع يكون العلم بتكنولوجيا الكومبيوتر بقدر كبير لازما لارتكابه من ناحية، ومتابعته من ناحية أخرى"[3]، ويحصر هذا الاتجاه الجرائم الالكترونية والمعلوماتية في تلك الواقعة على جهاز الحاسب الآلي أو داخل نظامه فقط.

بينما يعرف أصحاب الاتجاه الثاني الجريمة المعلوماتية تعريفا موسعا، على اعتبار أنها:" كل سلوك بمساعدة الكومبيوتر"[4]، فهو يجعل من الجريمة المعلوماتية كل جريمة تتم في محيط لأجهزة الكومبيوتر.

غير أن ثمة تباينا بشأن الاصطلاحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر وفيما يعد بيئة الشبكات، وهو تباين رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط أو المتصل بتقنية المعلومات، فابتداء من اصطلاح إساءة استخدام الكمبيوتر، مرورا باصطلاح احتيال الكمبيوتر، الجريمة المعلوماتية، فاصطلاحات جرائم الكمبيوتر، والجريمة المرتبطة بالكمبيوتر، جرائم التقنية العالية، وغيرها، إلى جرائم الهاكرز أو الاختراقات فجرائم الإنترنيت فجرائم الكمبيوتر والإنترنيت والسيبركرايم، وصولا للجرائم السيبيرية[5].

واختيار المصطلح يتعين أن يزاوج بين البعدين التقني والقانوني، فإذا عدنا للمراحل الأولى المتصلة بولادة وتطور تقنية المعلومات، نجد أن تقنية المعلومات، كما متعارف عليه تشمل

فرعين جرى بحكم التطور تقاربهما واندماجهما، الحوسبة والاتصال، أما الحوسبة، فتقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، أما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدراجة.

ومع تزاوج واندماج وسائل كلا الميدانين (الحوسبة والاتصال) سار التدليل على هذا الاندماج بالتقنية العالية، ولأن موضوعها المعلومات مجردة أو مجسدة لأسرار وأموال أو أصول، ساد اصطلاح تقنية المعلومات والتي تعرفها منظمة اليونسكو – من بين أشمل تعريفاتها – بأنها " الفروع العلمية والتقنية والهندسية وأساليب الإدارة الفنية المستخدمة في تداول ومعالجة المعلومات وفي تطبيقاتها، والمتعلقة بالحواسب وتفاعلها مع الإنسان والآلات، وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية"[6].

أمام هذا الواقع التقني، ظهرت مصطلحات عديدة دالة على الأفعال الجريمة المتصلة بالتقنية، بعضها دل على الأفعال المتصل على نحو خاص بالحوسبة، وبعض شمل بدلالته قطبي التقنية، وبعضها دل على عموم التقنية باعتبارها تحقق من اندماج وتألف بين ميادينها، ومع ولادة وأتساع استخدام الإنترنيت برزت اصطلاحات جديدة تحاول التقارب مع هذه البيئة المجمعة للوسائط التقنية ولوسائل المعالجة وتبادل المعلومات.

أما الجانب الثاني المحدد لدقة اختيار الاصطلاح، فيتعين أن ينطلق من أهمية التمييز بين الاصطلاحات المنتمية لما يعرف بأخلاقيات التقنية أو أخلاقيات الكمبيوتر والإنترنيت، وبين ما يعرف بإجرام التقنية أو جرائم الكمبيوتر، وهو ما يجيب عن التساؤل الرئيسي بشأن الحدود التي ينتهي عندها العبث وتلك التي تبدأ عندها المسؤولية عن أفعال جنائية[7].

والجانب الثالث في تحديد المصطلح، هو أن يكون الاصطلاح قادرا على أن يعبر – بقدر الإمكان – عن حدود محله، فيكون شاملا لما يعبر عنه، فلا يعبر مثلا عن الجزء ليعني الكل أو يكون على العكس مانع الحدود يطال مالا ينطوي تحت نطاقه، ومن هذا المنطلق، فإن كل اصطلاح وصف الظاهرة بدلالة إحدى جرائم الكمبيوتر كان قاصرا عن الإحاطة الشمولية المعبر عنه، فاصطلاح احتيال الكمبيوتر أو غش الكمبيوتر ونحوه من تعابير عن جرائم الكمبيوتر والإنترنيت، وذات استخدام الإنترنيت، وتظل تعبيرات واسعة الدلالة تحيط بأكثر مما تحتوي عليه ظاهرة جرائم الكمبيوتر والإنترنيت[8].

وفي هذا المقام لا يسعنا أن نتناول بالتفصيل تحديد مدلول كل مصطلح مما سبق الإشارة إليه، ولكننا سنحاول التمييز بين كل من الجريمة الالكترونية والجريمة المعلوماتية للفصل بينهما.

هناك عدة تعريفات للجريمة المعلوماتية ؛ ومن هذه التعريفات ماذهب إليه خبراء متخصصون من بلجيكا من أن جريمة الكمبيوتر هي:" كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية"[9]. في حين يذهب الفقيه الفرنسي الأستاذ Massa إلى أن المقصود بالجريمة المعلوماتية هو:" الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[10]. بينما يذهب رأي ثالث إلى أنها كل:" فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب ، أو التي تحول عن طريقه"[11]. في حين يذهب رأي رابع إلى أنها:" سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها " في حين أن منظمة التعاون الاقتصادي والتنمية OCDE وضعت التعريف التالي للجريمة المعلوماتية من أنها:" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[12]. بينما يذهب آخرون إلى تعريف هذه الجريمة بأنها:" كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات و نقل هذه البيانات"[13].

غير أننا نرى أن التعرض لتعريف الجريمة المعلوماتية يقتضي تقسيم هذا المصطلح إلى مقطعين؛ الأول: الجريمة، والثاني: المعلوماتية، وحيث تعرف الجريمة بأنها:" كل فعل أو امتناع يحظره القانون ويقرر له عقوبة" وبأنها:" فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبيرا احترازيا". فإن المعلوماتية يقصد بها:" المعالجة الآلية للمعلومات" وهي ترجمة للمصطلح الفرنسي Informatique وتعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكومبيوتر، وقد استعمل مصطلح Traitematique Automatise de Données ويعني المعالجة الآلية للبيانات، ومصطلح Télématique والذي يعني تقنيات بث المعلومات عبر شبكة اتصالات بعدية[14].

وعليه تعرف الجريمة المعلوماتية بأنها:" كل نشاط إجرامي يتعلق بالمعالجة الآلية للمعطيات أو نقلها" فهي كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكومبيوتر أو تلك التي يتم تحويلها عن طريقه.

بينما تكون الجريمة الكترونية إذا ما تم اقتراف الجرم باستخدام التقنية الحديثة، سواء كان جهاز حاسوب أو أي جهاز الكتروني آخر حديث، والذي بدونه لا يمكن اقترافه، وعليه يمكن أن يتفرع الجرم الالكتروني على أكثر من جريمة واحدة في نفس الواقعة[15].

غير أننا نرى بأن تعرف الجريمة الالكترونية بأنها:" كل فعل غير مشروع يتم عن طريق الاتصال من جهاز حاسوب إلى أي جهاز حاسوب آخر أو أي جهاز الكتروني أخر بواسطة شبكة محلية أو دولية كشبكة الانترنيت".

فحتى تكيف جريمة ما على أنها جريمة إلكترونية وجب حدوث اتصال بين جهازين الكترونيين، لأنه لا يمكن ارتكاب جريمة الكترونية من خلال العمل على جهاز منفرد مهما كان نوع الجرم المقترف، ذلك أنه يمكن استخدام الكومبيوتر في كثير من الجرائم لكن ليس بالضرورة يتم تكييفها على أنها جريمة إلكترونية؛ كفعل التزوير في المستندات والوثائق، أو كنشر مطبوعات يجرمها القانون، فمثل هذه الأفعال إذا ما تمت باستخدام جهاز الحاسوب فهي ترد إلى أصل الفعل ويمكن أن تكون جريمة معلوماتية، وهي في الوقت ذاته تشكل جريمة الكترونية بمجرد إرسالها من جهاز الكتروني إلى جهاز آخر.

وبناء على ما تقدم فإن الجريمة الالكترونية لا تختلف عن الجريمة المعلوماتية في كثير من الأحوال، باستثناء أنها تتم عن طريق جهازين الكترونيين أو أكثر يمكن الاتصال بينهما بواسطة شبكة محلية أو دولية أو بواسطة إحدى التقنيات الحديثة كتقنية البلوتوث.

لذلك فإنه من الصعب القول بوجود حدود فاصلة بين الجريمة المعلوماتية والجريمة الالكترونية، فكلاهما مرتبط بوجود جهاز الكتروني حديث، طالما أنه في الوقت الحاضر لم يعد يتم استخدام جهاز الكومبيوتر فقط، وإنما تعداه إلى اختراع العديد من الأجهزة الالكترونية التي تسمح بتخزين المعلومات والاتصال فيما بينها؛ كالمفكرة الالكترونية وأجهزة الهاتف النقال وغيرها مما يتم اختراعه يوميا.

ب/ خصائص الجريمة الالكترونية:

من الطبيعي أن تتميز الجريمة الالكترونية بخصائص تميزها عن الجريمة التقليدية، باعتبار أنها الجريمة الناتجة عن استخدام تكنولوجيا العصر الحديث، لعل من أبزها ما يلي:

1- **الجريمة الالكترونية جريمة عابرة للحدود**[16]: تتسم الجريمة الالكترونية في غالب الأحيان بالطابع العابر للحدود، وذلك بالنظر للطابع العالمي لشبكة الانترنيت، فعولمة هذه الجرائم يؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم؛ فهذه الجرائم هي صورة صادقة من صور العولمة؛ فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد وقد يتعدد هذا المكان بين أكثر من دولة؛ حيث لا يتواجد الفاعل على مسرح الجريمة، ومن الناحية الزمنية تختلف المواقيت بين الدول؛ الأمر الذي يثير التساؤل حول: تحديد القانون الواجب التطبيق على هذه الجريمة.

2- **لا يتم – في الغالب الأعم – الإبلاغ عن جرائم الالكترونية:** وذلك إما لعدم اكتشاف الضحية لها وإما خشيته من التشهير. لذا نجد أن معظم جرائم الالكترونية تم اكتشافها بالمصادفة؛ بل وبعد وقت طويل من ارتكابها، زد على ذلك أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الستار عنها[17].

3- **الجريمة الالكترونية جريمة صعبة الإثبات:** فهي لا تترك أثارا مادية لها بعد ارتكابها؛ فمن الناحية النظرية يسهل ارتكاب الجريمة ذات الطابع التقني؛ كما أنه من السهل إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها، لذا فهذه الجرائم لا تترك أثرا لها بعد ارتكابها؛ علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت. فهذه الجرائم لا تترك أثرا، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم جرائم الانترنت تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها، فهذا النوع من الجرائم ليس له شهود يمكن استجوابهم و لا أدلة مادية يمكن فحصها، ومن هنا تتأتى صعوبة الكشف عنها وإثباتها[18].

4- **الجريمة الالكترونية جريمة تعتمد هذه الجرائم على قمة الذكاء في ارتكابها:** ويصعب على المحقق التقليدي التعامل مع هذه الجرائم. إذ يصعب عليه متابعة جرائم الانترنت والكشف عنها وإقامة الدليل عليها. فهي جرائم تتسم بالغموض؛ وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية. والوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى[19].

5- **الجريمة الالكترونية جريمة تعتمد على الخداع والتضليل**[20]: فهي تعتمد على الذكاء في ارتكابها، فالإجرام الالكتروني هو إجرام الأذكياء بالمقارنة مع الإجرام التقليدي الذي يميل على العنف، ذلك أن المجرم الالكتروني يملك مهارات تقنية عالية وهو ذو إلمام بتكنولوجيا النظم المعلوماتية، كما أن الدافع لارتكابها يكون في أغلب الحالات هو إثبات القدرة على قهر النظام والتغلب على الأنظمة، وفي حالات أخرى إشباع الرغبة في الانتقام أو من اجل تحقيق الكسب المادي.

ج/ أنواع الجرائم الالكترونية:

إن أكثر مسائل ظاهرة الإجرام الالكتروني إثارة للجدل إلى جانب تعريفها وتحديد موضوعها، مسألة تحديد قائمة الجرائم الالكترونية،وتحديد أنماط السلوك الإجرامي والأفعال المكونة له، فالجرائم الالكترونية تختلف عن بعضها البعض باختلاف الكيفية التي تم تنفيذ تلك الجريمة، أو أهدافها أو الشخص الذي قام بتلك الجريمة، وفي هذا الموضوع سنتطرق إلى تلك الأنواع بشيء من التفصيل لإلقاء المزيد من الضوء كي نتعرف على طرق وأساليب تنفيذ الجرائم الالكترونية:

1- **التصنيف حسب التنفيذ**[21] **:**

فردي - فردي: ويقصد به أن يكون منفذ الجريمة الالكترونية فرداً ولا ينتمي لأي جماعة أو حزب أو منظمة وأن يكون الدافع شخصيا، كما أن المستهدف في هذه الحالة يكون أيضا فردا ومستهدفا لذاته ويكون مسرح الجريمة إما بريده الإلكتروني أو جهازه أو موقعه الشخصي.

فردي – جماعي: ويكون هنا المجرم فردا وبدوافعه الشخصية أيضا يقوم بمهاجمة أو التعرض لمجموعة أفراد في نفس الوقت كأن يهاجم منظمة أو مؤسسة أو شركة، وذلك بهدف الانتقام أو التشهير أو لأي سبب كان.

جماعي– فردي: هنا يكون المهاجمون جماعة تتكون من أكثر من شخص يقومون بأعمال تخريبية أو تجسسية أو أي نوع من أنواع الجرائم الالكترونية؛ ويكون الهدف بالنسبة لها فردا واحدا كأن يقوموا جميعا بإرسال رسائل متكررة إلى بريد شخص بذاته أو التآمر للدخول على موقعه في نفس الوقت مما يسبب له الخراب والتدمير .

جماعي– جماعي: وفي هذه الحالة يقوم عدة أشخاص بمهاجمة موقع جهات ذات شخصيات اعتبارية كالمنظمات والهيئات والشركات وغيرهم، بهدف القيام بأي عمل تخريبي أو التجسس على معلومات تلك المنظمات والهيئات.

2– التصنيف حسب النوع :

التسلل والتجسس[22]: حيث إن هناك فئة من الناس يعشقون التجسس على الآخرين بطرق مختلفة؛ فمن استراق السمع في الماضي، إلى تركيب أجهزة تنصت صوتية ومرئية، إلى ابتكار طرق وأساليب حديثة للدخول بها إلى أجهزة الحاسب الآلي الخاصة بالشخص المستهدف للحصول على أكبر معلومات ممكنة .

إن هذه الطريقة وفرت الكثير من المعلومات للأشخاص المتجسسين بحكم أن الحاسب الآلي أصبح المستودع الحقيقي والكبير في هذه الأيام، فالصورة تخزن في الحاسب الآلي وكذلك ملفات الصوت والفيديو، ناهيك عن الوثائق المهمة والمراسلات باختلاف أنواعها الرسمية والمالية والشخصية وغيرها، فجميعها موجودة في الحاسبات الشخصية، ولذلك فبمجرد دخول المخترق لذلك الجهاز فإنه يكون قد كشف أسرار وخفايا ذلك الضحية.

الإتلاف والتدمير: بإمكان الشخص الذي يستطيع الدخول إلى جهاز شخص آخر من إتلاف محتويات ذلك الجهاز وتدميرها وحذفها أو نقلها إلى مكان آخر داخل ذلك الجهاز أو خارجه، والتي قد تكون وثائق رسمية أو معلومات مالية أو ميزانية شركات مساهمة أو أسرار حربية.

التزوير والتغيير: إن الدخول إلى حاسوب آخر من قبل شخص له أهداف غير مشروعة يعني أن بإمكانه أن يغير الحقائق ويغير الأسماء والتواريخ في الوثائق والمستندات الموجودة في ذلك الجهاز، كما أن التزوير وتغيير الحقائق قد يطال الصور وتغيير الوجوه والأشخاص الموجودين في تلك الصورة واستخدامها لأهداف إجرامية، كما أن ملفات الفيديو وتغييرها وتركيب بعض وجوه المشاهير من علماء وفضلاء المجتمع أو من نجوم السينما والرياضة بهدف التشهير وإساءة السمعة، كل ذلك يعد جريمة من الجرائم الالكترونية.

الخداع والتغرير: إن الخداع والتغرير أمر مرفوض شرعا وعرفا، مما سبب في انتشاره هذه الأيام هو تطور التقنية والبرامج الحاسوبية التي استخدمت الاستخدام السيئ، حيث إنه باستخدام البرامج الاحترافية يستطيع الشخص الحصول على صور محسنة غير الصور الحقيقية إلى إخفاء العيوب منها، كما أنه ومن مظاهر الخداع أيضا انتحال شخصية غير الشخصية الأساسية كأن يدعي أنه مسئول ما، أو أنه أنثى وهو عكس ذلك تماما، بل هناك بعض البرامج ساعدت على ذلك منها تغيير الصوت، من ذكر إلى أنثى والعكس مع إمكانية تحسينه وعمل المؤثرات عليه.

3- التصنيف حسب الأهداف[23]:

إثبات الذات أو التشفي والانتقام: قد يكون الداعي إلى ارتكاب الجريمة الالكترونية هو إثبات شخصية ضعاف النفوس الذين يجدون في تركيبة شخصياتهم خللا ما، وبالتالي يستخدمون هذه الأساليب لإكمال مركب النقص لديهم، أو بغرض الانتقام من أشخاص آخرين.

المتعة والتسلية: هناك بعض الأشخاص يستمتع باختراق الأجهزة أو تشويه سمعة الآخرين ببرامج الصور كالتي تدمج أو تغير ملامح الوجه أو تغييره تماما واستبداله بآخر،كما توجد رغبة لدى بعض الأفراد في التعرف على خبايا الفنانين وخفايا اللاعبين والمشهورين والعلماء وأهل المناصب العليا وغيرهم.

الضغط والابتزاز: من أهداف المجرمين الإلكترونيين ابتزاز ضحاياهم والذين يبدؤون معهم بالاستدراج حتى يتمكنوا من الإمساك بشيء ذي قيمة للضحية كصور شخصية في أماكن مشبوهة، أو ملفات فيديو خليعة، ثم يجعلها وسيلة للضغط حتى يستسلم الضحية للأوامر والمطالب التي يرغب فيها المجرم الالكتروني كالحصول على المال.

4- التصنيف حسب الدوافع :

بعد أن تعرفنا على التصنيفات السابقة للجرائم الالكترونية، سوف نلقي الضوء على الدوافع الباعثة على القيام بتلك الجرائم المختلفة، حيث وجد في بعض المواقع على الشبكة العالمية للمعلومات (الإنترنت) موقع تعلم كيفية الانتحار خطوة بخطوة مع النصائح والتوجيهات اللازمة حتى تنفيذ العملية، ويمكن تصنيف الدوافع على النحو التالي[24]:

دوافع نفسية: يأتي العامل النفسي في المقام الأول بالنسبة للدوافع، فالشخص الذي يكون في صحته النفسية خللا واعتلالا؛ تجده غير منضبط في التصرفات والأفعال، ولا يبالي بالنتائج المترتبة على ما يفعل، لأنه لا يعتبر بمبدأ الموازنة وقياس الأمور قبل فعلها والشروع فيها، ولا يعتبر بالمحاذير الدينية أو القانونية أو العرفية.

دوافع جنسية: إن الدوافع الجنسية غير المنضبطة تتحول إلى قائد لصاحبها في غير هدى منه أو روية، ويزداد الأمر سوءا عندما يقع بين يديه الوسيلة التي تمكنه من الحصول على رغباته الجنسية اللامحدودة دون رقابة ودون إمكانية التعرف عليه، وبالتالي فإنه يستمر قدر المستطاع في الاختراق أو التجسس على من يقع عليهم اختياره ليفوز بما يصبو إليه من المتعة المحرمة.

دوافع عقائدية: إن العقيدة من أقوى الدوافع والقوى المحركة للأشخاص، والتي بها يكون لدى الإنسان الاستعداد للتخلي عن الحياة بأسرها، فما هو الظن بما هو أيسر من ذلك، إن كثيراً من الأشخاص يبررون محاولات اختراقاتهم لأجهزة الغير بتأويلات غريبة وأفكار سيئة، فمنهم من يحاول اختراق جهاز أو موقع بحجة أنه على غير المذهب أو الطائفة الدينية أو بحجة تكفيره أو الاطلاع على أسراره لفضحه والتشهير به.

دوافع عنصرية: ومن الدوافع أيضا الدوافع العنصرية، والتي تميز بين عنصر وآخر أو قبيلة أو عرق وبين آخرين، حيث تجد أن هناك بعض القبائل أو الأعراق لا يحبون القبيلة الأخرى أو العرق الآخر فتجد بعضهم يحاول عمل أعمال تخريبية من شأنها جر مشاكل على القبيلة أو العرق الآخر سواء باستخدام التدمير أو الإتلاف أو نشر الشائعات والأكاذيب أو غيره من طرق وأنواع الجرائم الالكترونية.

5- التصنيف حسب الوسائل[25]:

إن الجرائم الإلكترونية باختلاف أنواعها وأهدافها ودوافعها وطرق تنفيذها تتم بالطرق الرئيسية التالية:

البريد الإلكتروني: حيث يستخدم البريد الإلكتروني لإرسال الفيروسات وأحصنة طروادة، أو إرسال روابط لمواقع مشبوهة، أو يستخدم أيضا لإرسال الشائعات والأكاذيب وغيرها.

الحاسب الآلي وملاحقاته وبرامجه: يعتبر الحاسب الآلي الوسيلة الأولى للجرائم الالكترونية؛ وذلك لسهولة استخدامه وانتشاره، وتنوع برامجه، والاحترافية التي يتعامل بها بعض الناس والتي بدأت تزداد يوما بعد يوم.

الهاتف النقال وبرامجه وملحقاته: حيث إن الهاتف النقال وخاصة المتطورة والتي أصبحت تقارب في خصائصها أجهزة الحاسب الآلي، كما أنه تعتبر أسهل في تناقل الأخبار والصور ومقاطع البلوتوث وعلى نطاق واسع.

الشبكات المحلية والعالمية: كما أن الشبكات المحلية في الشركات والمؤسسات وغيرها تعتبر بيئة تناقل الإشاعات وذلك في ظل عدم وجود أنظمة تمنع ذلك، وحتى إن وجدت فلا يتم تطبيقها وبصرامة، أما الشبكة العالمية للمعلومات (الإنترنت)، فان الأمر يكون أكثر خطورة باعتبارها فضاء مفتوحاً أمام الجميع لنشر ما بدا له.

ثانيا/ الإطار التشريعي للجرائم الالكترونية في التشريعات المقارنة:

بالرغم من أن أول حادثة موثقة لإساءة استخدام الكمبيوتر ترجع إلى عام 1959، فان التشريعات التي وضعت لمواجهة خطر جرائم الكمبيوتر تأخرت حتى أواخر السبعينات مطلع الثمانينات، وتوصف بأنها موجة التشريع الثانية لتقنية المعلومات وأنها موجة الثمانينات مع أن ثمة انطلاق لقوانين جرائم الكمبيوتر في مطلع السبعينات، وبقيت في حدود ضيقة وفي إطار عدد محدد من الدول والاهم من ذلك بقي نطاق الحماية من جرائم الكمبيوتر حتى الوقت الحاضر قاصرا عن الإحاطة بكل جرائم الكمبيوتر كما سنرى فيما يأتي:

أ/ موقف التشريعات العقابية في الدول الغربية:

تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشرع عليها[26].

1- الولايات المتحدة الأمريكية[27]:

تبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصة بحماية أنظمة الحاسب الآلي (1976م – 1985م)، وفي عام (1985م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية، وحاليا ينظم جرائم الكمبيوتر والانترنت مجموعة من التشريعات على المستوى الفدرالي وكذلك على المستوى المحلي في مختلف الولايات، فعلى المستوى الفدرالي يمثل القسم (18) من قانون الولايات المتحدة التشريع الرئيس لجرائم الكمبيوتر(المادة 1030) حيث تتضمن اعتبار الأفعال التالية من قبيل الجريمة:

– التوصل غير المصرح به (الدخول) إلى أحد أنظمة الكمبيوتر الحكومية وكشف المعلومات السرية، وكشف المعلومات من جهة غير مصرح بها تلقيها.

– الدخول غير المصرح به إلى أي كمبيوتر والتوصل إلى معلومات غير مسموح الاطلاع عليها.

– الدخول غير المصرح به إلى أي كمبيوتر ومن ثم ارتكاب احتيال.

– إلحاق أضرار جراء الدخول غير المصرح به سواء للنظام أو البرامج أو للمعلومات المخزنة فيه.

– بث أو تهديد بارتكاب ضرر لأي كمبيوتر عبر الولايات أو للتجارة الأجنبية بغرض ابتزاز أموال أو منافع من أي شخص طبيعي أو معنوي.

أما القسم (1462) من الفصل (18) من قانون الولايات المتحدة فانه يحظر استخدام الكمبيوتر لاستيراد مواد مخلة بالآداب إلى داخل الولايات المتحدة الأمريكية، في حين أن القسم (1463) من الفصل (18) يحظر نقل أية مواد فاحشة عبر الولايات أو الجهات خارجية، ويجرم القسم (2251) من ذات الفصل توظيف أي قاصر أو إغرائه في المشاركة في أنشطة جنسية بما فيها خلق وتصوير مواد وبثها لجهات خارجية، ويحظر القسم (22051) من ذات الفصل استخدام الكمبيوتر الإخلال برعاية قاصر بقبول استغلاله – مع العلم – في إنتاج مواد تنطوي على استغلال جنسي، ويعتبر القسمين (2252، 2252 /أ) من ذات الفصل نقل وتبادل المواد الفاحشة ذات الصلة بالأطفال جريمة.

أما القسم (1028) من الفصل (18) من قانون الولايات المتحدة فانه يعتبر إنتاج أو نقل أو إدارة جهاز يتضمن نظام كمبيوتر بقصد استخدامه بتزوير الوثائق أو إنتاج وثائق تعريف مزورة جريمة ويعتر القسم (2319) من ذات الفصل الإخلال بحق المؤلف جريمة فدرالية.

وعلى مستوى الولايات، فان الإطار العام لتشريعات الولايات المتحدة في حقل جرائم الكمبيوتر والانترنت يتمثل بما يلي:

* كل ولاية من الولايات الخمسين تملك حرية التشريع الخاص بها وليس هناك آلية على مستوى الولايات أو المستوى الفدرالي تتطلب تبني الولاية شكلا أو محتوى محددا لقوانينها، وذلك بالرغم من وجود مشاريع توحيدية ومحاولات وتصريحات تهدف إلى توحيد التدابير التشريعية.

* إن الإطار العام لتوحيد قوانين جرائم الكمبيوتر يعتمد على مشروع قانون نموذجي تم وضعه من قبل هيئة أكاديمية عام (1998)، حيث يقسم أحكام جرائم الكمبيوتر والانترنت إلى ثماني طوائف ويجب أن يلاحظ أن هذا هو تقسيم القانون النموذجي لكنه يعتمد هنا كإطار للوقوف على مواقف التشريعات القائمة والنافذة في الولايات.

2 – بريطانيا[28]:

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى، ثم سن المشرع البريطاني قانون إساءة استخدام الحاسوب لسنة 1990(Computer Misuse Act) وبدء سريانه بتاريخ 29 أوت 1990، وقد خلق هذا القانون ثلاث جرائم جديدة لمواجهة جرائم الاختراق والتوصل غير المصرح به لتعديل معطيات الحاسوب وإتلافها بشكل عام وجرائم إدخال الفيروس بشكل خاص. هذه الجرائم هي:-

أ – الدخول غير المصرح به لنظام الحاسوب (النشاط الرئيسي للعبث أو التطفل)
ب – نفس الفعل السابق، ولكن بقصد ارتكاب أو تسهيل ارتكاب فعل آخر.
جـ – التعديل أو التحوير غير المصرح به لنظام الحاسوب بقصد إضعاف أو تعطيل النظام.

وبالرغم من أن الاستجابة البريطانية للتدابير التشريعية الجديدة في حقل تقنية المعلومات، وصفت بأنها متأخرة عن غيرها من الدول الأوروبية ومتأخرة بالتأكيد عن الاستجابة الأمريكية إلا أن السنوات الأخيرة وتحديدا الأعوام من 1998 وحتى الآن تشهد تميزا في التجربة البريطانية سواء من حيث محتوى التنظيم أو الحلول التشريعية المقررة، ليس في نطاق امن المعلومات فحسب، بل في نطاق حماية البيانات الشخصية والخصوصية وتنظيم حرية البيانات والمعلومات وفي مختلف الفروع الأخرى لقانون تقنية المعلومات.

3- فرنسا[29]:

سن المشرع الفرنسي القانون رقم 19 – 88 بتاريخ 5 كانون ثاني 1988 الخاص ببعض جرائم المعلوماتية وضمنه قانون العقوبات الفرنسي في المادة (462) وجرم فيه مجرد الولوج إلى نظام المعالجة الآلية أو البقاء فيه بطريق غير مشروع (2/462) وشدد العقوبة في الأحوال التي ينجم عن هذا الولوج محو أو تعديل في المعطيات المعالجة آليا. ونص القانون على تجريم إتلاف المعطيات وتزوير المستندات المعالجة آليا، واستعمال هذه المستندات. وعاقب على هذه الجرائم بعقوبة الحبس أو الغرامة. وقد خضع هذا القانون لتعديلات في العام 1993 وسعت من نطاق السلوكيات محل التجريم إضافة إلى تعديل بعض العقوبات لتحقيق مزيد من الأبعاد الردعية.

4- ألمانيا الاتحادية[30]:

صدر بتاريخ 15 ماي 1986 (قبل اتحاد الألمانيتين) القانون الثاني لمكافحة الجريمة الاقتصادية، وسرى مفعوله في الأول من أوت 1986، وقد جرم هذا القانون إتلاف أو محو أو تغيير أو تزوير البيانات المعالجة آليا، وشدد العقوبة بالنسبة للبيانات ذات الأهمية الأساسية لقطاع الأعمال أو السلطة الإدارية لتصل إلى حد السجن لمدة خمس سنوات والغرامة، وكذلك جرم هذا القانون غش الحاسوب أو الاحتيال بواسطة الحاسوب وعاقب عليه بذات العقوبة المذكورة كما عاقب على الحصول دون تصريح من قبل الفاعل لنفسه أو غيره على بيانات غير معدة أو مخصصة له ومحمية بوجه خاص ضد الوصول غير المصرح به.

5- الدنمـــــــارك[31]:

سن المشرع بتاريخ 6 حزيران / يونيو 1985 القانون الخاص بجريمة الحاسوب، وضمنه المواد 193 و 263 من قانون العقوبات، وعاقب فيه على مجرد الوصول إلى معلومات أو

برامج الغير وشدد العقوبة في حال ارتكاب فعل التوصل بغرض الاطلاع على الأسرار التجارية (م2/263). وجرم إتلاف وتعطيل أنظمة المعالجة الآلية وتخزين البيانات (م193).

6- النرويج[32]:

عدل المشرع قانون العقوبات عام 1985 وجرم الوصول غير المصرح به عن طريق تخطي الحماية إلى البيانات المخزنة أو المنقولة بالوسائل الإلكتروني أو الفنية الأخرى، وجرم إتلاف وتعطيل البيانات والاستخدام غير المصرح به لوقت وخدمات الحاسوب.

7- سويسرا[33]:

تضمن القانون السويسري بشأن جرائم المعلوماتية نصوصا تعاقب على الحصول دون تصريح على بيانات مخزنة الكترونيا أو على البرامج بقصد الإثراء على نحو غير مشروع وعلى التوصل مع نظم الحاسوب وإتلاف المعطيات.

8- فنلندا[34]:

في أواخر الثمانينات اقترح فريق العمل المكلف بدراسة جرائم الحاسوب تجريم كل صور الوصول إلى نظم البيانات المرتكبة باستخدام غير مأذون لكلمة السر أو تخطي الرقابة أيا كانت وسائلها. وانتهج المشرع الفنلندي لاحقا نهج تعديل قانون العقوبات، تجريم هذه الصور فشهد قانون العقوبات تعديلين الأول في عام 1990، والثاني عام 1995 وغطى التعديلين تجريم مختلف صور الاعتداء على البيانات إضافة إلى استخدام الكمبيوتر كوسيلة في ارتكاب جرائم الاحتيال والتزوير.

إن التتبع الأولي لنصوص التشريعات الخاصة أو نصوص القوانين المعدلة لقوانين العقوبات والخاصة بمواجهة ظاهرة جرائم الحاسوب، يظهر لنا الحقائق التالية:

- إن هذه التشريعات تتفاوت في تحديد الأنماط الجرمية الجديدة والنص على تجريمها وعقابها، لكنها في مجموعها لا تخرج عن نطاق الحد الأدنى لهذه الجرائم الذي سنبينه عند استعراض جهود المنظمات الإقليمية الدولية.
- إن النصوص التي انطوت عليها التشريعات المقارنة بشأن جرائم الحاسوب تحدد محل الاعتداء بمعطيات الحاسوب بمدلولها التقني الواسع سواء ارتكب الفعل عليها مباشرة أو استخدمت لتسهيل ارتكاب فعل آخر، وأساس التجريم الاعتداء على المعطيات لا وصف الفعل الذي سهل استخدام الحاسوب، أو الأدق، معطيات الحاسوب لارتكابه.
- إن العديد من النظم القانونية المقارنة اتجهت إلى إضافة صور التجريم الجديدة إلى نصوص القسم الخاص من قوانين العقوبات في نظمها القانونية، وفي ذلك إقرار بانطباق الأحكام العامة عليها من جهة، وتفضيل لآلية ضم هذه الجرائم إلى قانون العقوبات بدلا من

إفراد قوانين خاصة من جهة أخرى، ونجد هذا المسلك قد تبنته توصيات المؤتمر السادس للجمعية المصرية للقانون الجنائي. في حين اتجهت العديد من الدول إلى إفراد قوانين خاصة تنظم مسائل جرائم الكمبيوتر والانترنت،كما في القانون الأمريكي والقانون البريطاني وغيرها، حيث أفردت قوانين خاصة بجرائم الحاسوب.

– إن العقوبات التي قررتها هذه القوانين، تجمع في غالبيتها بين العقوبات المانعة للحرية والعقوبات المالية لأثرهما مجتمعتين في مواجهة مخاطر وخسائر هذه الجرائم، كما أن بعض القوانين، كالفرنسي مثلا، نص على عقوبات تكميلية تتمثل بمصادرة الأجهزة المستخدمة في الجريمة وهذا مسلك حسن لأثره الشخصي (في نفسية الفاعل) والموضوعي في فعالية مواجهة هذا النوع من الجرائم.

– تظهر الصياغة الفنية لنصوص التجريم في القوانين المقارنة بشأن جرائم الحاسوب، مراعاة الجوانب التقنية (التوصل بالنظام، البقاء في النظام الاختراق، المحو والتعديل، المعالجة الآلية وغير ذلك)، كما تبتعد الصياغة من حيث استخدام المصطلحات القانونية الدالة على الجرائم عن المصطلحات التقليدية – في أغلبها. والمستخدم من المصطلحات التقليدية (كالاحتيال، أو الغش، أو الإتلاف، أو الاستيلاء، أو السرقة في جريمة سرقة وقت الحاسب فقط) تتخذ مدلولات تختلف في جوانب كثيرة عن مدلولاتها التقليدية.

هذه أبرز المعالم الرئيسة لتشريعات حماية استخدام الحاسوب في الدول الغربية.

أما عن تأثير التقنية العالية على القواعد الجزائية الموضوعية والإجرائية فان الكمبيوتر لعب أدوارا ثلاثة في حقل الجريمة، فهو إما وسيلة متطورة لارتكاب الجرائم التقليدية بفعالية وبسرعة اكبر من الطرق التقليدية، أو هو الهدف التي تتوجه إليه الأنماط الحديثة من السلوك الإجرامي التي تستهدف المعلومات ذاتها بأنواعها المختلفة، أو هو البيئة التي تسهل ارتكاب الجرائم خاصة العابرة للحدود بما أتاحه من توفير مخازن للمعلومات والأنشطة الجرمية[35].

ومع شيوع الانترنت، تزايدت جرائم الكمبيوتر واستغلال الكمبيوتر والشبكات في الأنشطة الإجرامية. أضف إلى ذلك أن كشف الجرائم استلزم استخدام التقنيات الحديثة في عمليات التحري والتحقيق والكشف عن الأدلة الجرمية. ومن الطبيعي في ظل نشوء أنماط جرميه تستهدف مصالح معترف بحمايتها، وتستهدف محلا ذات طبيعة مغايرة لمحل الجريمة فيما عرفته قوانين العقوبات القائمة أن يتدخل المشرع الجزائي لتوفير الحماية من هذه الأنماط الخطرة من الجرائم لضمان فعالية مكافحتها سيما وأن نظام العقاب الجزائي محكوم بقاعدتين رئيستين هما مبدأ الشرعية الموجب لعدم إمكان العقاب على أي فعل دون نص قانوني محدد، وقاعدة حظر القياس في النصوص التجريمية الموضوعية. كما أنه وبفعل الطبيعة الخاصة لأنماط الجريمة والقدرة على ارتكابها عبر الحدود والقدرة على إتلاف أدلة الجرمية، فان

القواعد الإجرائية الجنائية في ميدان التفتيش والضبط والتحقيق والاختصاص القضائي يتعين أن تواكب هذا التغير وتضمن تحقيق التوازن بين حماية الحق في المعلومات وبين متطلبات فعالية نظام العدالة الجنائي في الملاحقة والمساءلة، من هنا كان تأثير التقنية العالية أو تقنية المعلومات على قواعد القانون الجنائي الموضوعية والإجرائية الأبرز من بين تأثيراتها على بقية فروع القانون.

ب/ موقف التشريعات العربية:

رغم أنه لم تظهر جرائم إلكترونية بحجم تلك التي تعيشها الدول المتقدمة، لكن هذا لا يعني انه ليس هناك وجود لهذه الظاهرة عربيا، فضلا عن أن مخاطر جرائم الكمبيوتر في بيئتنا قد تزيد عن مثيلاتها إذا ما قارنا مستويات الجاهزية التقنية والقانونية لمكافحة هذه الظاهرة، وإذا كان مجرموا التقنية يركزون منذ أعوام على نظم الكمبيوتر والشبكات في الدول المتقدمة فان الوقت لن يطول قبل أن تتجه أنشطتهم لنظم المعلومات في الدول النامية أو يولد في بيئاتنا من يساير أنشطتهم كما ظهر خلال الأعوام الخمسة الماضية.

وفي دراسة بحثية وتحليلية شاملة أجراها المركز العربي للقانون والتقنية العالية (عمان – الأردن) في منتصف العام 2001، للوقوف على حجم هذه الظاهرة عربيا، وجد المركز أن نحو 23% من المؤسسات المشاركة في الدراسة (وعددها 1032 مؤسسة موزعة على 13 دولة عربية) قد عانت من صورة أو أكثر من صور جرائم الكمبيوتر، منها نحو 59% تعرضت لمشكلات خاصة بمواقعها على الانترنت تتراوح بين محاولات الاقتحام إلى إنكار الخدمة إلى أنشطة إساءة استعمال البريد الالكتروني إضافة إلى أنشطة اعتداء على أمن التعاملات المالية على بعض هذه المواقع[36].

ونجد في البيئة العربية أن ثمة نقص في الإحصاءات وتحليل عمليات الاختراق، لكن هذا لا يعني عدم توفرها، ومن أشهر حالات الاختراق الهجوم الذي تعرضت له شركة اتصالات الإمارات من قبل أحد الهاكرز[37] الذي يحمل جنسية بريطانية في العام الماضي، كما تعرضت بعض المواقع المصرية الخاصة إلى أنشطة إنكار الخدمة وحصلت عدد من الحالات لدى بعض المواقع الأردنية، حيث قام عدد من طلبة إحدى الجامعات الأردنية بإرسال رسائل بريد إلكتروني بأسماء الغير متضمنة إساءات لشخص المرسل أو المرسل إليهم كما كشف مؤخرا عن قيام أحد الشباب حديثي السن بالشراء عبر الإنترنت باستخدام أرقام البطاقات المالية لأشخاص أردنيين وجرى كشف الحادثة ومتابعتها من خلال الشركة مصدرة البطاقات. وأصبح من المألوف مؤخرا أن نجد العديد من المواقع العربية على الانترنت غير فاعلة بوقت معين لتعرضها لأنشطة إنكار الخدمة خاصة المواقع الإخبارية الرئيسة، حيث شهدت الفترة المبتدئة من أكتوبر 2000 وحتى 2002 هجمات مكثفة على

مواقع الأخبار العربية والشبكات الإستراتيجية من قبل جهات إسرائيلية في إطار حرب معلومات استهدفت تعطيل مواقع عربية فاعلة تتناول الانتفاضة الفلسطينية. ومؤخرا تزايدت عمليات تعطيل المواقع وإنكار الخدمة في ضوء أحداث نيويورك وواشنطن[38].

ووفقا للنظم القانونية العربية، فقد تأسست قواعد حماية الأموال من مخاطر الجريمة بوجه عام على حماية المال المادي، أي المال ذو الوجود المادي، وكذلك التعامل مع محل الجريمة الملموس ذي الطبيعة المادية، والتعامل أيضا مع سلوك جرمي ينتمي إلى عالم السلوكيات المادية. وهذا ليس وقفا على النظام القانوني العربي، إنما هو الاتجاه التشريعي العام لمختلف قوانين العقوبات الموضوعية أيا كان النظام القانوني الذي تنتمي إليه أو يمثل مصدرا لها. وفي هذا الإطار، فان جرائم السرقة بوجه عام تقع على المال المنقول (المادي) وتتطلب فعل الأخذ أو الاستيلاء (سلوك مادي). وجرائم الاحتيال بوجه عام تتطلب سلوكا ماديا يهدف إلى إيهام فرد لدفعه لتسليم مال (مادي) أو ما في حكمه. وجرائم التزوير، تتضمن تغييرا في الحقيقة عن طريق فعل مادي من حيث الأصل، يقع على محرر (مادي). وجرائم الاعتداء على حرمة المساكن أو الأماكن الخاصة، أفعال دخول مادية (بالجسد) إلى موضع ذو وجود مادي (المكان). وجرائم إساءة الأمانة أو الاختلاس، أفعال استيلاء (مادية) من الموظف العام بالنسبة للاختلاس، وغير الموظف بالنسبة لإساءة الائتمان، محلها المال (المادي) أو ما هو في حكمه مما حدده النص والمحاز على سبيل الأمانة (الحيازة هنا مادية). وجرائم الإتلاف والتدمير والاعتداء على أموال الغير تنطوي على سلوكيات أضرار (مادية) توجه إلى أموال (مادية). وبالعموم فان النصوص العقابية العربية في هذا الحقل – مع اختلاف طفيف فيما بينها بالنسبة لعناصر الجريمة وأركانها – تعمل مع وقائع مادية وسلوكيات مادية تجاه محل مادي، من هنا أثيرت مسالة مدى كفاية نصوص التجريم المقررة في قوانين العقوبات التي تعالج الجرائم العادية (التقليدية) كالسرقة والاختلاس والاحتيال وإساءة الأمانة والإتلاف والتجسس والتزوير لمواجهة أنماط الإجرام المستحدثة في ميدان الإجرام الالكتروني[39].

وقد كانت هذه المسالة محل جدل فقهي في النظم القانونية المقارنة استمر منذ مطلع السبعينات في أوروبا وأمريكا، بل امتد الجدل إلى القضاء حيث حاولت بعض الأحكام إنزال معطيات الكمبيوتر منزلة المال المادي المنقول وتطبيق النصوص عليه وتكييف الفعل لإدخاله ضمن جرائم الاعتداء على الأموال، وحاول جانب من الفقه والقضاء اعتبار المعطيات – بوصفها نبضات كهربائية الكترونية – من قبيل مفهوم القوى المحرزة كالكهرباء أو النبضات الهاتفية والتلغرافية لكن كل محاولات تطويع النصوص القائمة لتشمل جرائم الكمبيوتر فشلت، وبالنتيجة فان الدراسة التحليلية لمختلف الاتجاهات الفقهية والقضائية

أظهرت قصور نصوص التجريم التقليدية السائدة عن الإحاطة بهذه الجرائم[40]، ومرد ذلك إلى ثلاث أمور أساسية:

– وهي أن جرائم الكمبيوتر تستهدف المعطيات ذات الطبيعة المعنوية، فعندما يكون الكمبيوتر هدفا للجريمة فان السلوك يستهدف المعلومات المخزنة فيه أو المنقولة منه أو إليه وعندما يكون وسيلة لارتكاب الفعل، فان السلوك يستهدف بيانات تمثل قيما مالية أو اعتبارا ماليا، ويجري الفعل أو السلوك بتوسل طرق تقنية في بيئة معنوية وليست في بيئة سلوكيات مادية. وعندما يكون بيئة للجريمة فان محتوى الفعل غير المشروع هو المعلومات غير المشروعة كما هو الحال في جرائم المحتوى المعلوماتي الضار.

– أن مبدأ الشرعية الجنائية يمنع المساءلة الجنائية ما لم يتوفر النص القانوني، فلا جريمة ولا عقوبة إلا بنص، ومتى ما انتفى النص على تجريم مثل هذه الأفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصور في مكافحة هكذا جرائم.

– إن القياس في النصوص الجنائية الموضوعية محظور وغير جائز، ويكاد ينحصر في الحقل الجنائي بنصوص الإجراءات الجنائية كلما كانت أصلح للمتهم، ومؤدى ذلك امتناع قياس أنماط جرائم الكمبيوتر على الجرائم التقليدية التي تستهدف الأموال والاعتبار المالي. ومن جهة أخرى لا يصلح القياس على نصوص خاصة بنوع من الجرائم كقياس سرقة المعلومات أو سرقة وقت الكمبيوتر على الاستيلاء على القوى المحرزة كالكهرباء لتخلف علة القياس.

هذه الحقائق التي بدت واضحة أمام جهات التشريع والقضاء في النظم المقارنة بعد جدل طويل وتقييم واسع، استدعت أن تتدخل العديد من الدول الأجنبية لتعديل القوانين الجنائية أو سن قوانين جديدة لمواجهة هذه الظاهرة المستجدة، فبعض الدول عدلت قوانينها بالنص صراحة على إنزال معطيات الكمبيوتر منزلة المال المادي المنقول وذلك لتحقق إمكانية تجريم المعتدين على هذا المال بنصوص جرائم السرقة والاحتيال والإتلاف وغيرها ، وبعضها اتجه نحو سن تشريعات مستقلة لتجريم جرائم الكمبيوتر أو استحداث نصوص مستقلة وإضافتها إلى تشريعاتها القائمة، وهذا المسلك امتد ليشمل نفس الدول التي نحت المسلك الأول فعادت لسن تشريعات جديدة لعدم كفاية التعديلات التي أحدثتها[41].

لكن مجتمعاتنا لم تعرف مثل هذه التشريعات ولم تتقاطع مع موجات التشريع العالمية في هذا الميدان ، أضف إلى ذلك أن ثمة عشرات الاتفاقيات الدولية والثنائية في حقل حماية البيانات ونقلها وفي حقل الحماية الجنائية من الأنشطة الجرمية في عالم المعلومات ، نحن لسنا طرفا فيها وليس بين دولنا العربية حد أدنى من مثل هذا التعاون . لهذا لا يصلح معنا كدول عربية تبني وجهة النظر التي تطالب بحد أدنى من التدخل التشريعي دون تقييم هذه

الدعوى ، فهي صحيحة للغير وليست صحيحة لنا ببساطة لأنهم أنجزوا وينجزون مئات التشريعات والأطر القانونية في هذا الحقل ونحن بعد لم نقف على أي من موجات التشريع هذه ، ولهذا فان الدول العربية مدعوة لوقفة أكثر شمولية ودقة في إرساء تنظيم تشريعي شمولي لإفرازات عصر المعلومات.

وانطلاقا من هذا التوجه فقد تدخل المشرع المغربي عن طريق قانون رقم 07/03 بتجريمه لمجموعة من الأفعال المتعلقة بنظم المعالجة الآلية للمعطيات كالدخول عمدا أو عن طريق الخطأ والبقاء في الداخل من خلال الفصول 3/607- إلى 607/ 11 ق.ج[42].

وكذلك المشرع العماني من خلال قانون الجزاء العماني الذي لحقه التعديل بموجب القانون 72 لعام 2001 وادخل أربعة نصوص تجرم عددا من صور جرائم الكمبيوتر كالالتقاط غير المشروع للمعلومات أو البيانات والدخول غير المشروع على أنظمة الحاسب الآلي، والتجسس والتصنت على البيانات والمعلومات، وانتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم، وإتلاف وتغيير ومحو البيانات والمعلومات، وتسريبها...[43]

وكذلك أصدر المشرع اليمني في 28 ديسمبر 2006 القانون رقم 06/40 بشأن أنظمة الدفع والعمليات المصرفية الالكترونية، والذي من خلاله جرم بعضا من صور الجرائم الالكترونية[44].

ومن التجارب الرائدة في هذا المجال تجربة دولة الإمارات العربية التي أصدرت قانونا خاصا فيما يتعلق بهذه المسالة هو القانون الاتحادي رقم 02 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، حيث حاول هذا القانون تجريم مختلف صور الجرائم المتعلقة بإساءة استخدام الحاسب الآلي، وهو ما يعد لغاية كتابة هذه الأسطر نموذجا يتعين دراسته بعمق والاحتذاء به من طرف الدول العربية الأخرى[45].

أمام هذا الواقع تعدو نصوص التجريم المقررة في قوانين العقوبات العربية عاجزة عن مواجهة خطر جرائم الكمبيوتر، ونقصد هنا خطر الجرائم الواقعة على البيانات المالية أو المتعلقة بالذمة المالية، فإذا ما أضيف إلى هذا الواقع عدم وجود نصوص تجرم أفعال الاعتداء على البيانات الشخصية المخزنة في نظم المعلومات وبنوكها أو نصوصا تحمي البيانات من خطر المعالجة الآلية وتكفل حماية الخصوصية – بوجه عام طبعا وفي جميع الدول العربية– فإننا نكون أمام واقع قاتم لن تزيل قتامته غير جهود وتدابير تشريعية حثيثة لسد النقص الحاصل وإيجاد قواعد تحيط بهذا النمط الخطر والمستجد من أنماط الإجرام وهو ما تسعى الدول العربية جاهدة لتحقيقه.

ثالثا/ واقع مكافحة الجرائم الالكترونية واتجاهاتها التشريعية في الجزائر:

على الرغم من انتشار الجرائم الالكترونية في مختلف أرجاء العالم، فإن الظاهرة تمس أيضا عددا من المواقع العامة والخاصة في الجزائر، لذلك فقد كان لزاما على المشرع الجزائري التدخل من اجل محاولة الحد من هذه الظاهرة الإجرامية الخطيرة والتي تأخذ أبعادا جديدة يوما بعد يوم.

وفي هذا السياق فإن الإطار القانوني الوحيد الموجود في الجزائر هو القانون 15/04 الصادر بتاريخ: 10 نوفمبر 2004 المعدل لقانون العقوبات تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات، والذي نصت المادة 394 مكرر منه على أنه:" يعاقب بالحبس من ثلاثة أشهر لسنة وبغرامة مالية من 50.000دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الألية للمعطيات أو يحاول ذلك.

وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 500.000 دج إلى150.000 دج"

والملاحظ على هذا النص أن الجريمة تقوم بمجرد الدخول الغير مصرح به بل تكفي محاولة الولوج للمنظومة وهو الأمر الذي يصعب إن لم نقل يستحيل إثباته، كما أن هذا النص لم يشترط أن تكون تلك المنظومة محمية أم لا فالجريمة تقوم في كل الحالات وهو ما يضع حسني النية تحت طائلة العقاب.

كذلك نصت المادة 394 مكرر1 على أنه:" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة مالية من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"، ثم في المادة 394 مكرر2 على أنه:" يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

تصميم أو بحث أو تجميع أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

وباستقراء هذه النصوص القانونية نجد وبدون شك أن المشرع الجزائري إنما عالج في هذه النصوص الجرائم المعلوماتية وليست الجرائم الالكترونية، وإن كانت تبدو أنها منظمة بشكل كافي من المشرع الجزائري إلا أنها تثير العديد من الصعوبات و خصوصا ما يتعلق بالإثبات وشخص الجاني، لذلك يجب على التشريع ألا يكون قاصرا على تنظيم ما هو موضوعي فقط

إنما عليه أن يصاحب ما هو موضوعي بما هو إجرائي لكي يتم تحقيق نوع من التوازن بين الحق وطريقة الوصول إليه.

أما عن الجرائم الالكترونية كما تم تحديد مدلولها في هذه المداخلة، فقد صادق مجلس الوزراء الجزائري على مشروع قانون يتعلق أساسا بالوقاية من المخالفات المتصلة بتكنولوجيات الإعلام والاتصال ومحاربتها، ومن المتوقع أن يعاقب مشروع قانون محاربة الجريمة الالكترونية؛ على اختراق وتخريب المواقع الالكترونية والحواسيب، وسرقة المعلومات المحمية وأرقام البطاقات الائتمانية وإنشاء المواقع التي تروج للإرهاب.

وإن كنا لم نتعرف بعد عن محتوى هذا المشروع، فإننا نأمل أن يأخذ بتجارب وتشريعات الدول التي سبقتنا في هذا المجال مع مراعاة أن يتضمن المشروع القواعد الموضوعية والإجرائية التي تكفل تحقيق الفعالية المرجوة منه بالنظر لخصائص هذا النوع من الجرائم كما سبق وبيناه.

وفي نفس السياق ومن اجل تحقيق فعالية اكبر للتشريعات التي سيتم سنها للحد من الجرائم الالكترونية وملاحقتها، فقد تم الإعلان عن إنشاء مركز لمكافحة الجريمة الالكترونية؛ والذي سيباشر مهامه عن قريب، خاصة وأنه ولغاية اليوم لم يعالج القضاء أيا من الجرائم المعلوماتية والتي مازالت قيد التحقيق.

خاتمة

ختاما لمداخلتنا هاته فإننا نرى أنه من الضروري ليس فقط سن تشريعات عقابية لمكافحة الجرائم الالكترونية، بل أن تأخذ هذه التشريعات بعين الاعتبار ضبط المصطلحات بدقة بالنظر لخصوصية الجرائم الالكترونية من جهة، واعتبارا لمبدأ الشرعية الجنائية الذي يحكمها من جهة أخرى.

وعليه يجب أن يراعى عند سن هذه التشريعات ما يأتي:

* أن يتم تعديل قوانين ونظم الإجراءات الجنائية؛ بالقدر الذي يسمح ببيان الأحكام اللازم إتباعها حال التفتيش على الأجهزة الالكترونية وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته.

* ينبغي أن تنص على السماح للسلطات القائمة بالضبط والتحقيق بضبط البريد الإلكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل؛ والكشف عن الحقيقة.

* ضرورة النص صراحة في القوانين المنظمة للإثبات الجنائي بما يسمح للقاضي بأن يستند إلى الأدلة المستخرجة من الحاسب الآلي والانترنت في الإثبات؛ طالما أن ضبط هذه الأدلة جاء وليدة إجراءات مشروعة، على أن تتم مناقشة هذه الأدلة بالمحكمة وبحضور الخبير؛ وبما يحقق مبدأ المواجهة بين الخصوم.

* ضرورة أن تتضمن تشريعات مكافحة الجرائم الإلكترونية كافة صور السلوك الضار والخطر على المجتمع التي يستخدم فيها انترنت أو الشبكات المحلية بواسطة مختلف الأجهزة الالكترونية الحديثة.

ولتحقيق فعالية هذه التشريعات العقابية يتوجب مراعاة ما يلي:

* ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم الالكترونية.

* ضرورة تخصيص شرطة خاصة لمكافحة الجرائم الالكترونية؛ وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت وكل ما يتم اختراعه من أجهزة الكترونية.

* يتعين تدريب وتحديث رجال النيابة العامة والقضاء بشأن التعامل مع أجهزة الحاسوب والإنترنت.

يتعين إتاحة الفرصة للمواطنين في المشاركة في مكافحة الجرائم الالكترونية ؛ وذلك من خلال إيجاد خط الساخن يختص بتلقي البلاغات المتعلقة بهذه الجرائم؛ ولاسيما الجرائم الأخلاقية كحالات الإعلان عن البغاء وممارسة الفجور أو الاستغلال الجنسي للأطفال عبر الانترنت.

* ضرورة نشر الوعي بين صفوف المواطنين – ولاسيما الشباب – بمخاطر التعامل مع المواقع السيئة علي شبكة الإنترنت؛ مع ضرورة نشر الوعي المجتمعي بالمخاطر النفسية والاجتماعية وغيرها الناجمة عن الاستخدامات غير الآمنة للانترنت.

*من المناسب تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم الالكترونية؛ وخصوصا الإنتربول؛ وفي هذا المقام من الممكن أن تنضم الدول العربية إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة جرائم ا الالكترونية والانترنت والعمل على دراسة ومتابعة المستجدات على الساحة العالمية.

نأمل في الأخير أن تسعي الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم الالكترونية عبر الانترنت؛ مع تشجيع قيام اتحادات عربية تهتم بالتصدي لجرائم الانترنت وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي

الهوامش:

(1) احمد حسام طه تمّام، **الجرائم الناشئة عن استخدام الحاسب الآلي**، القاهرة : دار النهضة العربية، 2000، ص 15.

(2) نائلة عادل محمد فريد، **جرائم الحاسب الآلي الاقتصادية**، بيروت: منشورات الحلبي الالكترونية، 2005، ص 28 وما بعدها؛ خالد ممدوح إبراهيم، **أمن الجريمة الإلكترونية**، الإسكندرية: الدار الجامعية، 2008، ص ص: 42- 43.

(3) محمود صالح العادلي، " **الجرائم المعلوماتية ماهيتها وصورها**"، ورشة العمل الاقليمية حول: تطوير التشريعات في مجال مكافحة الجرائم الالكترونية" مسقط 02- 04 أفريل 2006

(4) Adrian roben, **computer and the law**, C L J, 1991, vol 15, P 399

(5) محمد أمين الرومي، **جرائم الكومبيوتر والانترنت**، الإسكندرية: دار المطبوعات الجامعية، 2003، ص 16.

(6) نبيل علي، **العرب وعصر المعلومات**، سلسلة عالم المعرفة، العدد 184، الكويت: المجلس الوطني للثقافة والفنون والآداب، 1990 ص 41 وما بعدها

(7) يونس عرب، " **جرائم الكمبيوتر والانترنت المعنى والخصائص والصور وإستراتيجية المواجهة القانونية**"، ص 01، بحث منشور في الانترنيت على موقع: www.arablaw.org.

(8) يونس عرب، " **جرائم الكمبيوتر والانترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات**"، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – أبو ظبي 10-12 فيفري 2002، ص 05 وما بعدها، منشور على موقع: www.arablaw.org.

(9) هدى قشقوش ، **جرائم الحاسب الالكتروني في التشريع المقارن**، القاهرة: دار النهضة العربية، 1992، ص 20. عفيفي كامل عفيفي، **جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون" دراسة مقارنة**"، بيروت: منشورات الحلبي الحقوقية، 2003، ص 32.

(10) محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، القاهرة: دار النهضة العربية، 2000، ص 3.

(11) هشام محمد فريد رستم ، **قانون العقوبات ومخاطر تقنية المعلومات**، أسيوط (مصر): مكتبة الآلات الحديثة، 1992، ص 31.

(12) يونس عرب، " **جرائم الكمبيوتر والانترنت إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات**، مرجع سابق، ص 10.

(13) هدى حامد قشقوش، مرجع سابق، ص 20.

(14) هلالي عبد اللاه أحمد، **جرائم المعلوماتية عابرة الحدود**، القاهرة: دار النهضة العربية، 2007، ص 32 وما بعدها؛ خالد ممدوح ابراهيم، مرجع سابق، ص 43.

(15) احمد بن سالم السيابي وعبد الحق عبد الجبار العاني،" **الأدلة القضائية في أمن الفضاء الحاسوبي**" بحث منشور في الانترنيت على الموقع: www .Itu.int

(16) عبد الله حسين علي محمود، **سرقة المعلومات المخزنة في الحاسب الآلي**، القاهرة: دار النهضة العربية، 2002، ص 351.

(17) محمود صالح العادلي، مرجع سابق، ص 05.

(18) سعود وصل الله سعد الثبيتي، **جرائم الكومبيوبر والانترنيت**، ورقة بحث مقدمة حول الجريمة المعاصرة والاستخدامات السلبية للتقنية، ص 07 وما بعدها

(19) منير محمد الجهيني وممدوح محمد الجهيني، **جرائم الانترنت والحاسب الآلي ووسائل مكافحتها**، الإسكندرية: دار الفكر الجامعي، 2006، ص 15.

(20) محمد محمد شتا، **فكرة الحماية الجنائية لبرامج الحاسب الآلي**، الإسكندرية: دار الجامعة الجديدة، ص 103،

(21) إياس الهاجري ،**جرائم الإنترنت**، ص 02، بحث منشور في الانترنيت على الموقع www.arabcin.net/gold.

(22) محسن بن سلمان الخليفة، **جرائم الحاسب الآلي وعقوباتها في الفقه والنظام**، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 2007، ص 47 وما بعدها.

(23) إياس الهاجري، مرجع سابق، ص 03.

(24) عبد الله حسين علي محمود، مرجع سابق، ص 68 وما بعدها؛ موسى مسعود ارحومة، " **السياسة الجنائية في مواجهة جرائم الانترنيت**"، مجلة دراسات قانونية، العدد 17، بنغازي: منشورات جامعة قاريونس، 2008، ص 87 وما بعدها.

(25) إيهاب السنباطي،" **ماهية الجريمة الالكترونية– المفهوم والخصائص**–" ورقة بحث مقدمة للندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر، الدار البيضاء – المغرب، 19–20 جوان 2007.

(26) موسى مسعود ارحومة، مرجع سابق، ص ص: 100 – 101؛ عبد الله حسين علي محمود، مرجع سابق، ص ص: 308 – 309.

(27) لؤي ديب، "**أهمية وجود تشريعات لحماية الخصوصية من أجل الالتحاق بالثورة الرقمية**"، مقال منشور على الموقع: http. Elibs.info/lib-law.

(28) منير محمد الجهيني وممدوح محمد الجهيني، مرجع سابق، ص 188؛ مرشد الأمم المتحدة لعام 1999، **التحكم في جرائم الحاسوب وردعها** "**المراقبة الدولية للسياسة الجنائية**"، ترجمة: عمر محمد بن يونس، القاهرة: دار النهضة العربية، 2005، ص ص: 46، 47.

(29) محمد عبدالله منشاوي، **جرائم الانترنت من منظور شرعي وقانوني**، بحث منشور في الموقع الالكتروني: www minshawi.com.

هلالي عبد اللاه أحمد، مرجع سابق، ص 57.

(30) هلالي عبد اللاه احمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي**، عابدين (مصر) : النسر الذهبي للطباعة، 2000، ص 222 وما بعدها؛ منير محمد الجهيني وممدوح محمد الجهيني، مرجع سابق، ص 189.

(31) عيد محمد فتحي، **الإجرام المعاصر**، الرياض: أكاديمية نايف العربية للعلوم الأمنية، 1419هـ ، ص 255.

(32) يونس عرب، " **قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان**" بحث مقدم ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية مسقط – سلطنة عمان 2-4 نيسان / ابريل 2006، ص 15.

(33) سعود وصل الله سعد الثبيتي، مرجع سابق، ص 14.

(34) يونس عرب، " **قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان**"، مرجع سابق، ص 16.

(35) يونس عرب،" **متطلبات ومخاطر الانفتاح الالكتروني من النواحي الفنية والتشريعية** "، ورقة عمل مخاطر الانفتاح الالكتروني مقدمة للملتقى السابع لمجتمع الأعمال العربي – البحرين 18-20 اكتو بر 2003، ص 05 وما بعدها.

(36) كما أظهرت نفس الدراسة حول إساءة استخدام البريد الالكتروني أن أكثر من 82% من الأنشطة غير المشروعة الموجهة للأنظمة مصدرها مقاهي الانترنت العامة، وان 73% من المؤسسات ليس لديها سياسة داخلية لتنظيم استخدام البريد الالكتروني من قبل موظفي المنشأة نفسها، في حين ظهر أيضا وبنفس القدر تنامي الاهتمام بتنظيم قطاع المقاهي العامة للانترنت، بحيث ارتفعت نسبة الوعي لمخاطر عدم التنظيم إلى 86% عن الوضع السائد قبل عام 2001. واحتلت هجمات الفايروس – التي ظهر أن مصدرها الخارجي بلغ 96% من نسبة الهجمات – المرتبة الأولى في الأنشطة التي تعرضت لها المواقع العربية ونظم الكمبيوتر العربية، ولم تتمكن الدراسة من تقديم أرقام موضوعية حول حجم الخسائر أو معدلاتها، وذلك للتباين الكبير بين الأرقام التي قدمتها المؤسسات المشاركة وعلى نحو يظهر غياب أية معايير في البيئة العربية لحساب الخسائر الحقيقية الناجمة عن هذه الجرائم. يونس عرب، " **قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان**"، مرجع سابق، ص ص: 24 – 25.

(37) منير محمد الجهيني وممدوح محمد الجهيني، مرجع سابق، ص 47 وما بعدها ؛ سعود وصل الله سعد الثبيتي، مرجع سابق، ص 10.

(38) يونس عرب، " **قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان**"، مرجع سابق، ص: 26 .

(39) جميل عبد الباقي الصغير، **الإنترنت والقانون الجنائي**، القاهرة: دار الفكر العربي، 2001، ص 80.

(40) يونس عرب، "**مشروع قانون نموذجي عربي لجرائم الكمبيوتر والانترنت وللجرائم الإلكترونية**"، ورقة عمل مقدمة في ملتقى: "تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية"، مسقط – عمان، 02 – 04 أفريل 2006، ص 09، منشور على موقع: www.arablaw.org.

(41) محمد محي الدين عوض،" **مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)**"، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة 25-28 تشرين أول 1993، ص 06. منشور على موقع: www.arablaw.org.

(42) موسى مسعود ارحومة، مرجع سابق، ص ص: 95 وما بعدها، محمد أمين الرومي، مرجع سابق، ص ص: 07 -06.

(43) يونس عرب، " **قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان**"، مرجع سابق، ص 28 وما بعدها.

(44) سيناء عبد الله محسن،" **المواجهة التشريعية للجرائم المتصلة بالكومبيوتر في ضوء التشريعات الدولية والوطنية**"، ورقة بحث مقدمة للندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر، الدار البيضاء – المغرب، 19–20 جوان 2007.

(45) موسى مسعود ارحومة، مرجع سابق، ص ص: 96 وما بعدها؛ أنظر القانون على الموقع الالكتروني: www.openarab.net/ law/ 2006_ ؛ .يونس عرب، "**مشروع قانون نموذجي عربي لجرائم الكمبيوتر والانترنت وللجرائم الإلكترونية**"، ورقة عمل مقدمة في ملتقى: "تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية"، مسقط – عمان، 02 – 04 أفريل 2006، ص 09، منشور على موقع: www.arablaw.org.