

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



الجمهورية العربية
النيابة العامة
مكتب النائب العام

الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر - الدمار البيضاء - المملكة المغربية

للفترة 19-20 يونيو 2007م

**المواجهة التشريعية للجرائم المتصلة بالكمبيوتر
في ضوء التشريعات الدولية والوطنية**

القاضي/سيناء عبد الله محسن

محامي عام

عضو المكتب الفني بمكتب النائب العام

المقدمة

تعد الجريمة جزءاً لا يتجزأ من سلوك الإنسان غير القويم في المجتمع بصرف النظر عن درجة ثقافته وتطوره الاقتصادي والعلمي وتسعى كل دولة جاهدة إلى وضع حدود للحد منها ورغم ذلك فإن المؤشرات الإحصائية تفيد بزيادة ارتفاع معدلاتها خاصة بعد التقدم التقني الذي يشهده العالم، حيث أفرز التطور التكنولوجي لاسيما في الدول المتقدمة ظهور جرائم جديدة تختلف عن الجرائم التقليدية في أطرافها ومكانها وموضوعها وأساليب ارتكابها أطلقت عليها تسميات مختلفة كالجرائم المستحدثة، الجرائم الالكترونية، الجرائم المعلوماتية، جرائم التكنولوجيا المتقدمة، جرائم الانترنت والجرائم النظيفة.... الخ.

وتعد في مجملها بصرف النظر عن التسميات المختلفة جرائم التقنية الناتجة عن التقنية الحديثة والتي يعد الحاسوب الآلي أساس ظهورها.

وقد عرفت جرائم الانترنت بأنها تلك الجرائم العابرة للحدود التي تقع على شبكة الانترنت أو بواسطتها من قبل شخص ذي دراية فائقة بها⁽¹⁾.

ويرجع ظهور أول جرائم الانترنت إلى عام 1988م وكانت أول الجرائم هي جرائم العدوان الفيروسي المعروفة باسم (دودة موريس 1988م).

ويستخدم الانترنت في ارتكاب جميع أنواع الجرائم الالكترونية المختلفة كسرقة بطاقات الائتمان لاستخدامها في شراء المنتجات عبر الانترنت وسرقة كلمات المرور الخاصة بالدخول إلى الموقع وإبعث الرسائل الالكترونية بهدف تعطيله وإيقافه وجعله عاجزاً عن العمل والاستيلاء على البيانات الأمنية، العسكرية، السياسية، الاقتصادية، التجارية، وزرع الفيروسات المدمرة للأجهزة، التلصص على الأسرار الشخصية ونشر المواد الإباحية التي تمس قيم المجتمع الأخلاقية بشتى وسائل عرضها المصورة أو المسجلة⁽²⁾.

¹نبيلة هبه هروال- الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة- دار الفكر الجامعي ص 30 .

² Http://www.c4arab.com/showac.php?acid الموسوعة العربية للكمبيوتر والانترنت.

وقد تم تقسيم جرائم الانترنت إلى قسمين:

أولهما: عندما تكون شبكة الانترنت هي هدف الجريمة أو كما يسمى بالإجرام المعلوماتي على الانترنت كمهاجمة الشبكة بالفيروسات أو إحداث أضرار بالشبكة أو بنظام التشغيل وجعل الأجهزة غير صالحة للعمل أو الاكتساح أو التشويش والتفخيخ.

ثانيهما: عندما تكون شبكة الانترنت هي الوسيلة المستخدمة في ارتكاب الجريمة أو ما يسمى بالإجرام غير المعلوماتي في شبكة الانترنت وتشمل الجرائم التالية:-

- 1 جرائم تقع على الأشخاص وتضم جرائم الأخلاق كالقذف والسب والتشهير عبر الانترنت والاستغلال الجنسي للأطفال، وكذا الاعتداء على حرمة الحياة الخاصة.
- 2 جرائم تقع على الأموال وتشمل السرقة والنصب وغسيل الأموال وترويج المخدرات وجرائم التجارة الالكترونية وأبرزها جرائم السرقة والنصب والاحتيال عبر الانترنت.
- 3 جرائم الاعتداء على الملكية الفكرية كالاعتداء على حقوق النسخ وبرمجيات الحاسوب وكذا العدوان على براءات الاختراع.

4 ظاهرة جرائم الإرهاب الالكتروني عبر الانترنت (3).

وتختلف جرائم الانترنت أو الجرائم الالكترونية عن الجرائم التقليدية في أطرافها حيث يتميز مرتكبها بمهارات تقنية عالية إذ أن له خبرة فائقة بالقدر اللازم بأمور الحوسبة والانترنت لذلك فأن معظم من يرتكبون هذه الجرائم هم من الخبراء في مجال الحاسوب الآلي وأول من تبحث عنهم الشرطة عند ارتكاب مثل هذه الجرائم هم خبراء الكمبيوتر والانترنت. وبهذا الصدد فقد صنف الباحثون فاعل الجريمة الالكترونية إلى ثلاث مجموعات وذلك على النحو الآتي:-

- 1 -العاملون بمراكز الكمبيوتر من الشباب الهواه حديثي العهد بالمعلوماتية الذين ليست لديهم نوايا سيئة لارتكاب الجريمة وإنما تحقيق انتصارات تقنيه فقط وهم يمثلون الغالبية العظمى.
- 2 -العاملون بمراكز الكمبيوتر الخاصة بالشركات والوزارات الذين تحولت لديهم الهوايات إلى الاحتراف فارتكبوا بحق المنشآت التي يعملوا بها أفعال غير مشروعة.
- 3 -الهاكر الخبيث (كراكر) الذي يعد مجرم الانترنت المتميز والخطير.

³ نبيلة هبه هروال نفس المرجع السابق ص 57-62-63

أما عن الضحية في هذه الجرائم فقد يكون شخص طبيعي أو اعتباري، وأداة ارتكابها ذات تقنية عالية و مكان ارتكابها لا يتطلب بالضرورة انتقال فاعلها إلى ذلك المكان بشخصه كون الجريمة تتم باستخدام شبكات الاتصال بين الجاني ومكان الجريمة.

ليس ذلك فحسب بل أن الجرائم الالكترونية تعد من الجرائم النظيفة لصعوبة اكتشاف دليل ثبوتها فلا أثر فيها لأية عنف أو دماء وإنما مجرد أرقام وبيانات يتم تغييرها أو محوها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي⁽⁴⁾.

وهذا يعود إلى أن فاعلها يتمتع بدرجة فائقة في مجال الانترنت الأمر الذي سهل إخفاء معالم الجريمة والتخلص من آثارها، وبالتالي صعوبة التحقيق فيها وتتبع مرتكبيها فضلا عن اعتمادها على الذكاء والمهارة والخداع في ارتكابها.

ومملا شك فيه بأن ظاهرة الجرائم الالكترونية كظاهرة ناتجة عن التقدم التقني عامة وتقنية الحاسوب خاصة كانت بحاجة إلى قانون ينظمها بهدف إحداث مواءمة بين المجتمع وبين التنظيم الطبيعي لتلك الظاهرة الناشئة في أرض الواقع⁽⁵⁾.

وسوف نتحدث في هذه الورقة عن المواجهة التشريعية لهذا الخطر المتنامي في المجتمع وذلك على النحو الآتي:-

أولاً: المواجهة التشريعية الدولية لجرائم الكمبيوتر.

ثانياً: المواجهة التشريعية الوطنية لجرائم الكمبيوتر.

أولاً: المواجهة التشريعية الدولية لجرائم الكمبيوتر.

لقد سارعت الدول المتقدمة تقنياً إلى سن قوانين خاصة لمواجهة هذا النوع من الجرائم ومنها:-

● قانون تكنولوجيا المعلومات أو قانون الكمبيوتر والانترنت (السيبر) الذي كان له تأثيره على فروع القوانين الأخرى، حيث وردت في نطاقه بعض من القواعد القانونية الجزائية عن سوء استخدام نظم التقنية الحديثة.

⁴ محمد علي العريان- الجرائم المعلوماتية- دار الجامعة الجديدة للطباعة والنشر ص 53-63.

⁵ الدكتور/عمر محمد أبو بكر بن يونس- الجرائم الناشئة عن استخدام الانترنت (الأحكام الموضوعية والجوانب الإجرائية) - دار النهضة العربية ص85.

• قانون الخصوصية أو الحق في الخصوصية وذلك في مجال حماية الحقوق والحريات لحماية البيانات الشخصية والأسرار كالحالة الصحية للفرد والهويات وبطاقة الائتمان في ظل البيئة الاتصالية الشاملة، وذلك بطابعها المعنوي وليس المادي التي ضمنت له دساتير دول العالم الحماية القانونية ولم تأت تلك الحماية إلا بعد أن تم التوقع بأن مثل تلك المعلومات يمكن أن تكون محلاً للانتهاك.

• قانون التجارة الالكترونية ويتعلق هذا القانون بالمعاملات المصرفية الالكترونية باعتبار البنوك أول من يتأثر بالتقنية الحديثة فكان من الطبيعي أن تلجأ إلى استخدام التقنية الحديثة في تعاملها مع الآخرين فاستخدامها للكمبيوتر وشبكات نقل المعلومات وتطبيقات بطاقات الائتمان والخدمة المصرفية الشاملة عبر الانترنت اقتضى بالضرورة وجود تنظيم تشريعي يكفل تبادل البيانات والمستندات البنكية بالصورة الالكترونية وما إلى ذلك، فظهرت مثل هذه القوانين على المستوى العربي والدولي⁽⁶⁾.

مثل قانون المعاملات الالكترونية في الأردن، دبي، تونس، البحرين وفي اليمن صدر القانون رقم (40) لعام 2006م وسيتم التطرق إليه لاحقاً.

وهناك جهود دولية بذلت لمكافحة جرائم الانترنت أهمها:-

1- المؤتمر الدولي الأول لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان (مؤتمر طهران 1968) التي تبنت الجمعية العامة للأمم المتحدة توصياته، حيث تم الاعتراف بحق الخصوصية وبأن من حق الإنسان أن يعيش لوحده بعيداً عن كشف أسرارهم، فسنت بعض دول العالم في أوروبا وآسيا وأمريكا واليابان تشريعاتها في مجال حماية الخصوصية من الاعتداء عليها ألزمت من خلالها مواقع الانترنت المعنية بجمع المعلومات بتسجيل أغراضها وإخضاع عملياتها لرقابة مفوض الخصوصية في الدولة باعتباره جهة قضائية معنية بحماية الأفراد من أي اعتداء عليهم. ومثل هذه الحماية لا وجود لها في التشريعات العربية، وإنما مجرد نصوص فرعية متفرقة في قوانين مختلفة مثل حماية سجلات الأحوال المدنية في قانون الأحوال المدنية، وكذا حماية بيانات الضمان الاجتماعي وعدم جواز استخدامها لأغراض أخرى كما هو في قانون الضمان الاجتماعي

⁶ [Http://www.ammanet/look/artide.tpl?dlange=181d](http://www.ammanet/look/artide.tpl?dlange=181d)

publication=3oonrarticle=1759&NrISSUe=5&Nrsection=1&search.x=17&search.y=13

وهذه النصوص في مجملها لا يمكن إعتبارها تشريعاً خاصاً يحمي حق الخصوصية، وإنما مجرد تطبيقات بسيطة لمثل هذا الحق مما يستلزم سنها في تشريعات خاصة تتواءم معها.

2- قانون الانسيترال النموذجي بشأن التجارة الالكترونية التي اعتمدته لجنة الأمم المتحدة عام 1996م حيث يعتبر من الجهود الدولية لمكافحة جرائم الانترنت في مجال التجارة الالكترونية قامت اللجنة بإعداده كقانون نموذجي انطلاقاً من ولايتها المتمثلة في تعزيز تنسيق وتوحيد القانون التجاري الدولي بغية إزالة أية عقبات لا لزوم لها أمام التجارة الدولية تنتج عن أوجه القصور والاختلاف في القانون المتعلق بالتبادل التجاري، وقد جاء إعداده في الأساس استجابة للتغير الرئيسي الذي حدث في الوسائل التي تتم فيها الاتصالات بين اطراف يستخدمون في أعمالهم التقنيات الحاسوبية أو غيرها من التقنيات الحديثة.

وقد كان القصد منه أن يكون نموذجاً تهتدي به البلدان فيما يتعلق بتقييم وتحديث جوانب معينة من قوانينها وممارساتها في ميدان العلاقات التجارية ومساعدة جميع الدول على تحسين تشريعاتها وعلى تدارك المساوى الناجمة عن قصور التشريعات على الصعيد الوطني مع تقديمه للمشرعين الوطنيين مجموعة من القواعد المقبولة دولياً في هذا المجال⁽⁷⁾.

3- القانون النموذجي بشأن التوقيعات الالكترونية في عام 2001م باعتباره صك قانوني جديد مستمداً من قانون الانسيترال النموذجي بشأن التجارة الالكترونية ومتسقاً معه تماماً وبشكل مفصل⁽⁸⁾.

4- الاتفاقية الأوروبية التي كانت بمثابة دعوة موجهة إلى دول العالم للتفاعل مع الانترنت جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها النهائي في 23/11/2001م في بودابست وقعت عليها ثلاثون دولة أوروبية بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوروبي المشاركة في إعداد هذه الاتفاقية وهي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية.

وقد تضمنت هذه الاتفاقية الأقسام التالية:-

القسم الأول: تحديد المصطلحات.

⁷ قانون الانسيترال النموذجي بشأن التجارة الالكترونية مع دليل تشريعه 1996م - الأمم المتحدة - نيويورك - الفقرات (128-150) ص 59.

⁸ قانون الانسيترال النموذجي بشأن التوقيعات الالكترونية - 2001م ص 39.

القسم الثاني: الخطوات الواجب اتخاذها في إطار التشريع الوطني.

القسم الثالث: التعاون الدولي.

القسم الرابع: الشروط النهائية حول الانضمام إلى الاتفاقية.

كما حددت الجرائم التي يجب أن تتضمنها التشريعات الوطنية للدول الأعضاء وذلك على النحو التالي:

1 -الجرائم المتعلقة بأمن الشبكات (الدخول والمراقبة غير المشروعة والعدوان على الثقة في البيانات أو على النظام والإساءة إليه).

2 -الجرائم المعلوماتية كما هو الشأن في الاختلاق والانتحال والنصب والاحتيال المعلوماتي...الخ.

3 -جرائم الأخلاق مثل إنتاج أو بث أو حيازة ما يتعلق بدعارة الأطفال.

4 -جرائم العدوان على حقوق الملكية الأدبية والفكرية كإستنساخ المصنفات المشمولة بالحماية.

5 -المسؤولية الجنائية للأشخاص المعنوية.

وكذلك الاهتمام بالإجراءات الجنائية لاسيما في مرحلة التحقيق والملاحقة القضائية مثل التحفظ على الأدلة والتفتيش والضبط وما إلى ذلك.

وقد حملت هذه الاتفاقية الطابع التوجيهي للخطوات التي يلزم اتخاذها في إطار التشريع الوطني في كل دولة فيما يتعلق بالأحكام الموضوعية والإجرائية كما اشرنا أعلاه.

وألزمت الدول الأعضاء بمراعاة حقوق الإنسان وحرياته الأساسية التي تضمنتها الاتفاقيات الدولية والتشريعات الوطنية على حد سواء والالتزام بعدم انتهاكها.

مع إمكانية الدول الأخرى غير الأعضاء في الاتفاقية الاستعانة بهذه الاتفاقية عند إعداد التشريعات الوطنية باعتبارها مصدر تاريخي في مجال مكافحة الجريمة على الانترنت⁽⁹⁾.

ثانياً: المواجهة التشريعية الوطنية لجرائم الكمبيوتر.

فيما يتعلق بالتشريعات الجزائية الوطنية في الجمهورية اليمنية في مجال جرائم الكمبيوتر.

فإنه ومما لاشك فيه بأن القانون الجنائي اليمني له جذور في مكافحة الجريمة في مجال الاعتداء على الأموال كالسرقة والاحتيال والابتزاز وخيانة الأمانة والتزوير وذلك في المواد التالية (210، 310، 313، 318) من القانون رقم (12) لعام 1994م بشأن الجرائم والعقوبات.

⁹ الدكتور/عمر محمد ابو بكر بن يونس نفس المرجع السابق ص213-214.

وكذا في مجال الاعتداء على الأشخاص كجريمة التهديد، انتهاك حرية المراسلات، الاعتداء على حرمة الحياة الخاصة والتهديد بإذاعة الأسرار الخاصة كما هي ثابتة في المواد (254، 255، 256، 257) من نفس القانون.

وجرائم الأخلاق كهتك العرض والفعل الفاضح وجريمة الدعارة كما هو منصوص عليه في المواد (270، 274، 279) من القانون المذكور آنفاً.

إلا أنه ومع الاستخدام المتزايد لتقنية المعلومات في شتى مجالات الحياة وظهور المعلوماتية وتطبيقاتها المتعددة وما ترتب على ذلك من ظهور تقنيات جديدة في ارتكاب الجريمة التقليدية كالاستيلاء على الأموال عن طريق الاحتيال المعلوماتي أو كإرسال بريد الكتروني يتضمن تهديد بالقتل أو اختراق شبكات المعلومات مما جعل القانون الجنائي أمام قصور بيّن في مواجهة تلك الجرائم⁽¹⁰⁾.

وهذا يرجع في الأساس إلى أن مواد القانون الجنائي المنصوص عليها في القوانين القائمة نصوص تقليدية وضعت أساساً لحماية الأشياء المادية في مواجهة صور الاعتداء التقليدي عليها، وبالتالي فقد تعذر تطبيق تلك النصوص على حالات الاعتداء على المكونات غير مادية للأنظمة المعلوماتية⁽¹¹⁾.

فضلاً عن الطبيعة الخاصة للجرائم المعلوماتية وحادثة الحاسب الآلي والمجرم المعلوماتي فيها وعليه فقد أصبح هناك فراغاً تشريعياً في مجال الجرائم المعلوماتية فكان لأبد من تدخل الشارع في إصدار تشريعات وطنية تتضمن نصوصاً قانونية تكفل تجريم الأنشطة الناشئة عن التقنية الحديثة في ظل النصوص التقليدية التي أصبحت غير ملائمة للتطبيق في مجال الجريمة المعلوماتية ومحاولة إعادة صياغة القوانين النافذة بحيث تعكس خصوصية هذه الجرائم واستيعاب جوانب التقنية فيها.

فأصدر المشرع اليمني القانون رقم (40) لعام 2006م وذلك بتاريخ 2006/12/28م بشأن أنظمة الدفع والعمليات المالية والمصرفية الالكترونية وذلك لمكافحة الجريمة الالكترونية التي تعد من أهم وأخطر التحديات التي تواجه التجارة الالكترونية بسبب المخاطر العديدة التي تسببها لكل من الجهة المالكة للموقع ومستخدمي هذا الموقع⁽¹²⁾.

وقد قسم المشرع اليمني هذا القانون إلى تسعة فصول وذلك على النحو الآتي:-

¹⁰ نبيله هبه هروال نفس المرجع السابق ص9.

¹¹ محمد علي العريان - نفس المرجع السابق ص103.

¹² acid.1037 <http://www.c4arab.com/showac.php?> المؤسسة العربية.

الفصل الأول: بعنوان /التسمية والتعاريف المادتين (2،1).

الفصل الثاني: بعنوان /الأهداف ونطاق السريان المواد من (3) إلى (6).

الفصل الثالث: بعنوان /أنظمة الدفع المواد من (7) إلى (9)

الفصل الرابع: بعنوان /الآثار المترتبة على السجل والعقد والرسالة والتوقيع الالكتروني المواد من (10) إلى (19) وهو من أهم الفصول لكونه يتضمن الأحكام الموضوعية للمعاملات الالكترونية .

الفصل الخامس: بعنوان /شروط قابلية السند الالكتروني للتحويل المواد من (20) إلى (25).

الفصل السادس: بعنوان /إجراءات الدفع والتحويل الالكتروني للأموال المواد من (26) إلى (31) .

الفصل السابع: بعنوان /إجراءات توثيق السجل والتوقيع الالكتروني المواد من (32) إلى (36).

الفصل الثامن: بعنوان /العقوبات المواد من (37) إلى (41).

الفصل التاسع: بعنوان الأحكام الختامية المواد من (42) إلى (46).⁽¹³⁾

والهدف من هذا القانون تطوير أنظمة الدفع وتسهيل استعمال الوسائل الالكترونية في إجراء المدفوعات وتعزيز دور البنك المركزي اليمني في إدارة وتحديث أنظمة الدفع والإشراف والرقابة عليها سعياً لتسيير إجراءاتها وقواعدها والتشجيع على استخدامها بهدف رفع الكفاءة التشغيلية للنظام المالي والمصرفي بشكل خاص والنظام الاقتصادي بشكل عام والحفاظ على الاستقرار المالي والنقدي. ويسري على أنظمة الدفع الالكترونية وسائر العمليات المالية والمصرفية التي تنفذ بوسائل الكترونية ورسائل البيانات والمعلومات الالكترونية وتبادلها والسجلات الالكترونية والتوقيع الالكتروني والترميز والتوثيق الالكتروني.

كما فرض القانون على البنوك التي تشغل لديها أجهزة صراف آلي تكييف أوضاعها طبقاً لأحكامه خلال عامين من تاريخ صدوره.

وأعطى القانون للبنك المركزي صلاحية تحديد مواصفة الصراف الآلي وتحديد عدد الأجهزة لكل بنك مرخص مع منح الترخيص لأي مؤسسة مالية ترغب بتشغيل جهاز صراف آلي وفقاً للضوابط والشروط التي يضعها لذلك وإجراءات الدفع والقبض بواسطة النظام الالكتروني لتحويل الأموال وإبلاغ البنوك بذلك ويكون لهذه الإجراءات حجية في الإثبات ⁽¹⁴⁾.

¹³ القانون رقم (40) لعام 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية.

¹⁴ http://www.newsymen.net/showdetails.asp?subno=12007_0512_13213

وفي جانب العقوبات تضمنت نصوصه حماية جنائية لبعض الصور التي تُعد من قبيل الجرائم الإلكترونية نبيها فيما يلي:-

المادة (37) من القانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية التي نصت على انه (مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر نافذ يعاقب كل من يخالف أحكام هذا القانون بالعقوبات الواردة في هذا الفصل).

والمادة (38) التي نصت على انه (يعاقب كل من قام بإنشاء أو نشر أو تقديم شهادة توثيق مستعينا بطرق إحتيالية بغرض الاستيلاء أو التوصل إلى الحصول على فائدة مادية له أو لغيره بالحس مدة لا تقل عن سنتين وبغرامة لا تقل عن مليون ريال مع إرجاع المبالغ التي قام بالاستيلاء أو الحصول عليها و سهل للغير الحصول عليها).

ويلاحظ أن المشرع اليمني قد جمع بين عقوبة الحبس والغرامة المالية معاً الحبس لمدة لا تقل عن سنتين والغرامة لا تقل عن مليون ريال مع إرجاع المبالغ التي تم الاستيلاء عليها وبهذه العقوبة يكون المشرع اليمني قد وضع جزاءً رادعاً لمرتكبي هذه الجرائم لجمعه بين تلك العقوبتين (الحبس والغرامة) دون إعطاء الحق للقاضي في اختيار إحدى العقوبتين انطلاقاً من سلطته التقديرية كما هو معمول به في القوانين الجنائية.

وبالنظر إلى حداثة صدور القانون اليمني رقم (40) لعام 2006م لكونه صدر في أواخر عام 2006م فإنه وإلى الآن لم يفرز الواقع عن أية مشاكل أو صعوبات اعترضت تطبيقه شأنه في ذلك شأن أي قانون جديد.

إلا انه يمكننا القول بأن القانون اليمني المذكور أعلاه مثله مثل القوانين الأخرى في الدول العربية كقانون المعاملات الإلكترونية رقم (85) لعام 2001م في الأردن وكذا قانون إمارة دبي رقم (2) لعام 2002م وكذا القانون التونسي والبحريني وان كانت قد جاءت بالحماية القانونية للوسائل الإلكترونية المصرفية إلا أنها ما زالت فيها من القصور والنقص لكونها لم تضمن الحماية الكافية للوسائل الإلكترونية المصرفية خاصة مع تزايد حوادث السطو والسرقة على حسابات المواطنين وتزوير بطاقات الائتمان وإساءة استخدامها.

هذا فضلاً عن عدم وجود تشريع عربي يجرم صور جرائم الكمبيوتر بأنواعها بحيث يضع لكل صورته منها العقوبة التي تتناسب مع خطورتها لأن الدخول الغير مشروع إلى النظام ليس كسرقة الأرصدة من البنوك عبر الاحتيال المعلوماتي أو كإثارة الفتن والتشهير وترويج الأفكار عبر وسائل الكمبيوتر والبريد الإلكتروني التي تحدث إخلالاً في المجتمع (15).

وهذا لا يمكن تحقيقه إلا من خلال استحداث تشريعات خاصة لمواجهة الجرائم الإلكترونية بصورها المتعددة ووضع العقوبة التي تتناسب مع خطورتها عبر الاستفادة من خبرات الدول المتقدمة في هذا المجال وزيادة مستوى التعاون العربي عن طريق المعاهدات والاتفاقيات وإقامة الندوات المشتركة مع ضرورة إلحاق رجال القضاء والنيابة العامة ببرامج تدريبية على هذا النوع من الجرائم حتى يساعدهم ذلك في إصدار الأحكام القضائية.

¹⁵ [Http://www.ammanet/look/artide.tpl?/dlange=181d](http://www.ammanet/look/artide.tpl?/dlange=181d)

[publication=3oonrarticle=1759&NrISSUe=5&Nrsection=1&search.x=17&search.y=13](http://www.ammanet/look/artide.tpl?/dlange=181d&publication=3oonrarticle=1759&NrISSUe=5&Nrsection=1&search.x=17&search.y=13)

الخاتمة

في الختام لا يسعنا القول إلا أنه ومع التطور العلمي المستمر تتزايد نسبة ارتفاع الجرائم الالكترونية وأنواعها وتشتد خطورتها على المجتمع لأن مرتكبيها دائماً ما يعملوا على تطوير أدواتهم مستفيدين من التقدم الحاصل في استخدام التكنولوجيا في شتى المجالات، الأمر الذي يترتب عليه بالضرورة العمل على مكافحة تلك الجرائم على النحو الذي يؤدي إلى الحد منها إن لم يكن القضاء عليها وذلك من خلال البحث عن آخر ما تم التوصل إليه في مجال الحماية الالكترونية وسن وتطبيق التشريعات التي تتناسب مع الجرائم الالكترونية التي تنتهك خصوصية الأفراد أو التي تعتدي على التحويلات والمعاملات النقدية والتجارية عبر شبكة الانترنت أو التي تتعلق بالاعتداء على القيم الأخلاقية المتعارف عليها أو على الحقوق الفكرية.... الخ وتنمية الوعي في المجتمع خاصة بين أوساط الشباب باعتبارهم أكثر الفئات استخداماً للكمبيوتر والانترنت والعمل على تدريس التشريعات المتعلقة بالجرائم الالكترونية في الجامعات للتعرف على مخاطر استخدام شبكة الانترنت والعقوبات المفروضة عليها بموجب القوانين الصادرة مع التأهيل المستمر لمأموري الضبط القضائي على النحو الذي يساعدهم في مواجهة هذا الإجرام المستحدث في مجال عملهم عند البحث والتتقيب عنها بطرق أخرى تختلف عما هو متبع في الجرائم التقليدية.

،،، والله ولي التوفيق،،،

قائمة بأهم المراجع

أولاً الكتب والمؤلفات:-

- 1 - د. عمر محمد أبو بكر بن يونس-الجرائم الناشئة عن استخدام الانترنت - الأحكام الموضوعية والجوانب الإجرائية -دار النهضة العربية -القاهرة.
 - 2 - د. عبد الفتاح بيومي حجازي -المستشار بمجلس الدولة- المستشار القانوني بالمجلس الوطني الاتحادي- الأحداث والانترنت-دراسة متعمقة عن أثر الانترنت في انحراف الأحداث-دار الفكر الجامعي -الطبعة الأولى 2002م.
 - 3 - محمد علي العريان- باحث دكتوراه -كلية الحقوق - جامعة الإسكندرية -الجرائم المعلوماتية - دار الجامعة الجديدة للنشر 2004م.
 - 4 - خيله هروال - ماجستير في القانون-الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات- دراسة مقارنة - دار الفكر الجامعي 2006م.
- ثانياً الدراسات والمقالات على مواقع الانترنت:-
- حوار مع المحامي/يونس عرب -من مؤسسة مجموعة العرب حول قانون الكمبيوتر وأمن المعلومات الخصوصية -منشور بتاريخ 26/آذار/2005م على الانترنت على موقع <http://www.ammannet/Look/article.tp>
- مقال بعنوان- الجرائم الالكترونية -بواسطة عمرو احمد عزت -منشور بتاريخ 16/مايو/2007م على الانترنت على موقع <http://www.c4arab.com>
- دراسة بعنوان -الجرائم الالكترونية - عادل حماد أبو عزه -منشور بتاريخ 16/5/2007م على الانترنت على موقع <http://www.al-JAZirah.com>