موقف القانون الليبي من الجريمة الإلكترونية

إعداد . أ. الفاخرية حسين بوبكر مفتاح
كلية القانون
جامعة عمر المختار

ملخص البحث

الجريمة الإلكترونية وان كانت تحدث في عالم افتراضي الا انها واقعه لابد التسليم بوجودها وإزالة المعوقات التي تحول دون مواجهتها، والملاحظ أن مشرعنا الوطني لم يقم بأي محاولات جادة لمواجهة الجريمة الإلكترونية، فالقوانين العقابية التقليدية غير كافيه في مواجهة هذا النوع من الجرائم.

ومن خلال هذا البحث نوصي المشرع الليبي بسن قانون خاص لمواجهة الجريمة الإلكترونية،يراعي فيه الطبيعة الفنية لهذه الجرائم، وما تتطلبها من تخصيص جهاز شرطه ونيابة على دراية فنية واسعة بهذا المجال.

Abstract

Electronic crime, even if it occurs in a virtual world

However, it is a fact that must be acknowledged and remove the obstacles that prevent facing them.

It is noticeable that our national legislator has not undertaken any serious intervention, Intellect and rational laws are insufficient in facing this type of crime.

Through this research, we recommend the Libyan legislator a special law to protect against electronic crimes.

It takes into account the technical nature of these crimes and what it requires from allocating a police force with extensive technical expertise to this area**.**

مقدمة

مما لاشك فيه ان القوانين شرعت في جميع البلدان لحماية الحريات و المصالح الاجتماعية، وبناء على ذلك كان لابد من المراقبة المستمرة للمستجدات من الوقائع الماسة بالحقوق والحريات محل الحماية، وسن التشريعات الكفيلة لتحقيق هذه الحماية وردع كل من يحاول المساس بها متخذ من الوسائل المستحدثة مخرجا للإفلات من العقاب، ولما كان التطور التكنولوجي وما تبعه من تطورات في المعاملات الالكترونية أدى الى ظهور ما يسمى بجرائم الانترنت والتي تسببت في الإضرار بالمجتمع على جميع الأصعدة ، والذي أداء بدوره إلى قيام الدول والمنظمات إلى محاولة التغلب على ما فرضته هذه الجرائم من تحديات بسن قوانين أو إضافة مواد قانونية للقضاء على هذه الجرائم ومواجهتها، كان يجب علينا الاستفادة من تجارب هذه الدول والمنظمات في تشريعنا الوطني وتطوير نصوصه بما يتلأم مع مواجهة هذا الشكل من أشكال الإجرام.

وفي سبيل ذلك كان لابد لنا من تسليط الضوء على ماهية الجريمة الالكترونية وخصائصها وموقف المنظمات والتشريعات منها وماذا كان من الممكن مواجهتها بالنصوص التقليدية وما هي الصعوبات التي تقف عائق أمام مواجهتها.

- هدف البحث

نحاول من خلال هذه البحث التغلب على تحديات جرائم الانترنت من خلال تسليط الضوء على مفهومها والتوعية بمخاطرها ودعوة المشرع إلى إقرارها من خلال الاستفادة من تجارب المنظمات والدول التي أقرت ذلك.

- أهمية البحث

لهذا الموضوع أهمية كبيرة من الناحيتين العملية والنظرية، فمن الناحية العملية يفيد في التوعية بمخاطر الجريمة الالكترونية ليتم تفاديها، ومن الناحية النظرية يسلط الضوء على مخاطر الفراغ التشريعي الليبي في هذا المجال ليتم تداركه.

- إشكالية البحث

ترجع إشكالية البحث إلى ما تتميز به جرائم الانترنت من طبيعة خاصة، فبالإضافة الى الوعاء الذي ترتكب فيه هذه الجريمة، فهي جريمة عابرة للحدود، ومن هنا باتت الحاجة ملحة للتعرف على ماهيتها وتصنيف مجرميها والتعرف على الأهداف الكامنة وراء ارتكابها ليتسنى لنا بعد ذلك تحديد الوسائل المناسبة لمواجهتها من خلال الاستفادة من الجهود الدولية وموقف التشريعات من هذه الجريمة.

- منهج البحث

سنعتمد في بحثنا على المنهج الوصفي المقارن من خلال وصف الظاهرة الإجرامية محل البحث وعرض موقف الجهود الدولية والتشريعات الغربية والعربية من الجريمة الالكترونية ومقارنة موقف المشرع الليبي بهذه الجهود.

المبحث الأول

ماهية جرائم الانترنت

بالرغم من الايجابيات التي يساعد بها الحاسب الآلي في كافة مجالات الحياة وخاصة مجال الملاحقة الجنائية وذلك من خلال تسهيله لعمليات القبض على المجرمين والتعرف عليهم من خلال بصمات العين والصوت وعرض صورهم على الشاشة، وما أضافه نظام المراقبة الالكترونية من بديل لتنفيذ عقوبة السجن قصير المدة خارج المؤسسة العقابية، إلا انه في المقابل اظهر سلبيات ومشاكل قانونية تتمثل في جرائم الانترنت، ومن خلال هذا المبحث نحاول التعرف على ماهية هذه الجرائم من خلال تعريفها وبيان خصائصها وأسباب ارتكابها وأنواعها.

المطلب الأول

تعريف جرائم الانترنت

حاولت العديد من الجهود الدولية والإقليمية والكتابات الفقهية تعريف جرائم الانترنت، إلا انه لا يوجد تعريف محدد ومتفق عليه حول تعريفها، وإنما اختلفت الآراء في تعريف هذه الجريمة تبعا للمعيار المعتمد في تعريفها.

فقد عرفها البعض بأنها (هي كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات)[1].

ويرى البعض بأنها هي الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا[2].

---

[1]- هدى قشقوش -جرائم الحاسب الالكتروني في التشريع المقارن -الطبعة الاولى -دار النهضة العربية -1992-ص(20).

[2]-محمد عبيد الكعبي -الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت -دار النهضة العربية -1992 ص(33).

وعرفت بأنها الأنشطة أو الأفعال غير المشروعة التي يقوم بها شخص على دراية كافية بتقنية المعلومات متوسلا بشبكة المعلومات الدولية في تحقيق مأربه الشريرة للإضرار بالآخرين[1].

كما عرفها البعض بأنها جرائم الشبكة العالمية التي يستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة مثل استخدمه في النصب والاحتيال وغسيل الأموال وتشويه السمعة[2].

المطلب الثاني

صفات المجرم الالكتروني

يتمتع المجرم المعلوماتي بصفات خاصة، وذلك يرجع للطبيعة الخاصة لهذه الجريمة وللعالم الافتراضي الذي ترتكب فيه وتتمثل أبرز صفات مرتكبي هذه الجرائم فيما يلي: –

1. يتمتع بالذكاء والمثابرة فهذا النوع من الأجرام يتم ارتكابها من قبل أشخاص لهم القدرة على التعامل مع أجهزة الحاسب الآلي بتقنية عالية وقد يتطلب الوصول الى هذه التقنية في التعامل مع أجهزة الحاسب الحصول على دورات وتطوير البرمجيات، لذا تعد المثابرة

[1]-د-موسى مسعود ارحومة -الاشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية - المؤتمر المغاربي الاول حول المعلوماتية والقانون -اكاديمية الدراسات العليا -طرابلس -2009 - ص(4).

[2]-مصطفى محمد موسى -التحقيق الجنائي في الجرائم الالكترونية، الطبعة الاولى، مطابع الشرطة 2009 ص(112).

والذكاء من أهم صفات المجرم المعلوماتي، فهو لديه القدرة على التصور الكامل لجريمته من خطوات ارتكابها الى اخفاء أثارها[1].

2. عادة ما يكون المجرم الالكتروني من ذو الياقات البيضاء الذين لا تترك جرائمهم أي أثر مادي فجرائمهم لا تحتاج سوء الى قدرة على التعامل مع أجهزة الحاسب الآلي بتقنية عالية[2].
3. لا يميلون مرتكبي هذه الجرائم إلى العنف ويتمتعون بقدرة فنية عالية تمكنهم من تنفيذ جرائمهم بدقة متناهية[3].
4. المجرم المعلوماتي متكيف مع المجتمع فالمجرم الذي يرتكب جريمته مستعينا بشبكة الاتصالات ومواقع التواصل الاجتماعي هو بلا شك شخص اجتماعي قادر على التكيف مع المجتمع ولا يوجد عداء بينه وبين بيئته الاجتماعية، وقد يوجد لديه شعور بان ما يقوم به لا يدخل في نطاق الأعمال غير الأخلاقية خاصة عند قيامه بأفعال تضر بمؤسسة اقتصادية ضخمة قادرة على تحمل نتائج أفعاله[4].

---

[1]- احمد خليفة الملط -الجرائم المعلوماتية-دار الفكر الجامعي، الطبعة الثانية 2006 -ص107، انظر ايضا -د. طارق ابراهيم الدسوقي -الامن المعلوماتي -النظام القانوني لحماية المعلوماتية -دار الجامعة الجديدة للنشر -2009-(176-177).

[2]- عباس ابو شامة عبد المحمود -عولمة الجريمة الاقتصادية -جامعة نايف للعلوم الامنية -2007 - ص (52).

[3]- محمد عبيد كعيب -المرجع السابق -ص32، انظر ايضا سيناء عبد المحسن محسن -المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية -الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر -الدار البيضاء -المملكة الغربية -من 10 الى 20 يوليو 2007 ص (52).

4- ايمن عبد الحفيظ -الاتجاهات الفنية والامنية لمواجهة الجرائم المعلوماتية دون دار نشر-2005 ص(16-17)، انظر ايضا نهلا عبد القادر المؤمني -الجرائم المعلوماتية -دار الثقافة للنشر-الطبعة الاولى -عمان -2007-ص(78).

المطلب الثالث

أسباب الإجرام الالكتروني

تتعدد أسباب الأجرام في نطاق جرائم الانترنت، كغيرها من الجرائم، ولمعرفة أسباب ارتكابها أهمية بارزة في تصنيف طوائف المجرمين، وفيما يلي نقوم تسليط الضوء على هذه الأسباب محاولين من خلالها تصنيف فئات المجرمين وفقا دوافعهم: –

1. يعد الفضول والتسلية من أبرز أسباب الأجرام المعلوماتي وهي دوافع ذهنية تبرز في تحقيق الذات وإظهار التحدي للأنظمة الرقمية وغالبا ما ترتكب من المراهقين النوابغ الذي يرغبون في تحقيق ذاتهم من خلال تحديهم للأنظمة المعلوماتية وفك شفراتها، دون أن يكون لديهم أي رغبة في الأضرار بالآخرين، فهم يندفعون إلى ذلك بدافع التسلية فقط ويطلق على الفئة التي ترتكب هذه الجرائم بهذا الدافع بالهواة[1].
2. تحقيق الكسب المادي ويتم بفك شفرات البطاقة الائتمانية أو اعتراض الأرصدة أثناء عملية التحويل وتصميم برامج معدة للاختراق وعادة ما تحتاج هذه الجرائم الى تقنية عالية لذا غالبا ما ترتكب من قبل قراصنة متخصصين في مجال التقنية المعلوماتية يطلق عليهم مصطلح القراصنة المحترفين[2].
3. تحقيق أغراض شخصية كالتسلية من قبل مستخدمي الحاسب بالمنازل ويطلق على مرتكبي الجرائم تحت هذا الهدف بالمجرم بالصدفة.
4. تحقيق مكاسب سياسية بالتجسس على أنظمة الدول وبيانات الحكومة وتحريفها لتشويه صورة فكر سياسي لصالح اتجاهات سياسية معادية، أو إنشاء مواقع تبث الفتن بين

1- د-عبد الفتاح بيومي حجازي -مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت -دار الفكر الجامعي -الطبعة الاولى -2006 -ص(46)، انظر ايضا طارق ابراهيم الدسوقي -المرجع السابق - ص (180).

2- د-محمد دباس الحميد -ماركو ابراهيم نينو-حماية انظمة المعلومات -دار الحامد للنشر والتوزيع - عمان -الطبعة الاولى -2007-ص(73).

أفراد الشعب لصالح جهات خارجية، أو ترويج فكرة التطرف الديني والتعصب الاجتماعي وغالبا ما ترتكب الجرائم تحت هذا الغرض من قبل طائفة المجرمين المتطرفين فكريا[1].

5. الانتقام والثأر ويبرز هذا السبب من الإجرام في قيام عمال المنشآت بنشر معلومات وبيانات خطيرة عن المؤسسة التي يعملون بها أو باستخدام الفيروسات والبرامج الضارة للانتقام من رب العمل على سوء تقديره لخدماتهم أو الاستغناء عنهم، ويطلق عليهم طائفة المجرمين الحاقدين[2].

المطلب الرابع

التحديات الكامنة وراء صعوبة مواجهة جرائم الانترنت

تتعدد التحديات الكامنة وراء صعوبة مواجهة جرائم الانترنت، فبالنظر إليها والى ومكان ارتكابها نجد أنها جريمة واقعية تقع في عالم افتراضي عابر للحدود، من الصعب أن نجد لها أثار مادية، ومن خلال النقاط التالية سنحاول إبراز هذه التحديات بشيء من الإيجاز: –

1. تقع الجريمة المعلوماتية في بيئة افتراضية، فهي بذاتها غير ملموسة ويسهل محوها وإخفاء أثارها بسهولة فبمجرد الضغط على الأزرار يتم محو معالم الجريمة[3].
2. أنها عابرة للحدود لذا يعد نطاق تطبيق القانون من حيث المكان من أبرز التحديات التي تواجه مكافحة هذه الجريمة [4].

1- د-نهلا عبد القادر المؤمني -المرجع السابق -ص (85-68).
2- د. محمد بن عبد الله بن علي المنشاوي -جرائم الأنترنت في المجتمع السعودي -رسالة مقدمة لكلية الدارسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية -اكاديمية نايف للعلوم الامنية -2003 -ص(38).
3- د-محمد عبد الرحيم سلطان -جرائم الانترنت والاحتساب عليها -مؤتمر القانون والكمبيوتر والانترنت -من 1-3 مايو 2000-جامعة الامارات العربية المتحدة؛ كلية الشريعة والقانون،المجلد الثالث،الطبعة الثالثة،2004، ص(877).
4- د-نهلا عبد القادر المؤمني،المرجع السابق -ص(51).

3. سهولة ارتكابها وصعوبة اكتشافها فعادة ما ترتكب من قبل أشخاص يتمتعون بذكاء فائق لهم القدرة على ارتكابها بسهولة وتقنية عالية ولهم القدرة الأكبر على إخفاء الأدلة المادية بسرعة فائقة مما يصعب معه على المحقق التقليدي التعامل معهم، كما أنها قد تقع على شركات ومؤسسة مالية ضخمة قد تحجم عن الإبلاغ عن الجريمة والكشف عنها حتى لا يتم تقليدها من قبل الآخرين[1].

المطلب الخامس

أهم صور الإجرام المعلوماتي

تتمثل أهم صور جرائم الانترنت فيما يلي: –

1. جرائم سياسية ترتكب ضد الحكومات غرضها العبث بالبيانات الحكومية ومهاجمة المواقع الحكومية الرسمية والتجسس الالكتروني عليها، وغيرها من الجرائم التي تهدد الحكومات والأمن القومي ومن أشهر تلك الجرائم قيام (هيس لاندر) الألماني الجنسية باختراق قاعدة بيانات شبكة البنتاجون والحصول على 29 وثيقة متعلقة بالأسلحة النووية[2].
2. جرائم تقع على برامج الحاسب الآلي كجرائم العبث بالبرمجيات والأنظمة وتدميرها وحذفها وتعطيل الخدمة وبث الفيروسات باستخدام برامج معدة خصيصا لذلك.
3. جرائم الاعتداء على الحياة الشخصية للأفراد كالإعتداء على براءة الاختراع والتعدي على حقوق الملكية الفكرية وسرقة المعلومات وابتزاز مالكيها وتشويه السمعة وسرقة الهوية ودخول أجهزة الغير عبر شبكة الانترنت.

---

[1]-د-جمال محمد غيطاس -امن المعلومات والامن القومي -دار النهضة العربية -الطبعة الاول -2007- ص(214).

2-محمد سيد سلطان، قضايا قانونية في امن المعلومات وحماية البيئة الالكترونية -دار ناشري للنشر الالكتروني -2012-ص35 متوفر على الموقع التاليwww.nashiri.net.

4. جرائم تقع بواسطة برامج الحاسب الآلي مثل جرائم اختراق وتدمير المواقع والاستيلاء عليها وإغراقها بالمعلومات والاستيلاء على الأرقام السرية وإرسال الفيروسات لتدمير المواقع.
5. جرائم اقتصادية يستخدم الحاسب الآلي في تنفيذ العديد من الجرائم المالية كجرائم غسيل الأموال بتحويل كمية كبيرة من الأموال بسرعة وأمان ولعب القمار وسرقة الحسابات المصرفية وتزوير بطاقات الائتمان أو فك شفرات البطاقات المالية والتلاعب بها [1].

المبحث الثاني

الجهود الرامية للحد من جرائم الانترنت

تعددت الجهود الرامية للحد من تدفق جرائم الانترنت، وهي وان لم تختلف على ضرورة التصدي لهذا النوع من الجرائم، إلا أنها اختلفت في كيفية ودرجة الاهتمام بمواجهته ومن خلال هذا المبحث نحاول تسليط الضوء على هذه الجهود محاولين تحديد مدى استجابة المشرع الليبي لها.

المطلب الأول

الجهود الدولية في مواجهة جرائم الانترنت

إدراكا من المجتمع الدولي لخطورة جرائم الانترنت وخاصيتها العابرة للحدود، عملت العديد من الدول لمحاولة وضع سياسة جنائية عالمية تتصدي لهذه الجرائم على المستوى الإقليمي والدولي، وتكللت هذه المحاولات بعقد العديد من الندوات والمؤتمرات وإبرام المعاهدات التي تحمل روح الجماعة في التصدي للأجرام المعلوماتي ومن ذلك: –

1-د-محمود ابراهيم محمد الشافعي -النقود الالكترونية مجلة الامن والحياة -اكاديمية الشرطة -دبي 2004 (ص142 182).

أوصى المؤتمر الثامن للأمم المتحدة بشأن منع الجريمة ومعاملة المجرمين بضرورة تكثيف الجهود في مواجهة إساءة استخدام الحاسب الآلي على صعيد التشريعات الداخلية وتقرير الجزاء الرادع على مرتكبيها، كما أوصى باعتماد تدابير لتدريب القضاة والأجهزة الأمنية على منع الجرائم ذات الصلة بأجهزة الحاسوب، إضافة إلى حماية حقوق ضحايا جرائم الانترنت[1].

كما أكد على ضرورة أن تتجه الجهود الدولية إلى إرساء تعاون قضائي وأمني دولي لمكافحتها نظرا لكونه جريمة عابرة للحدود فغالبا ما تتعدى حدود الدولة الواحدة، لذا أكد على أهمية اتخاذ التشريعات التي تكفل الانضمام لمعاهدات تسليم المجرمين والتعاون في إجراءات الملاحقة الجنائية[2].

أما المجلس الأوربي فقد أصدر اتفاقية بودابست لمكافحة الجرائم المعلوماتية عام 2001 والتي دخلت حيز النفاذ سنة 2004وكان من بين أهدفها التأكيد على أهمية التعاون الدولي والإقليمي في مواجهة جرائم الانترنت، ومنع اي اختراق لأنظمة الحاسب الآلي فنصت في المادة (2) منها على تجريم الدخول غير المشروع على النظام المعلوماتي. كما نصت الاتفاقية على معاقبة أي شخص يتسبب بأي خسائر مادية للغير عن طريق تعديل أو محو أو إيقاف لأي بيانات مخزنة في أي نظام معلوماتي أو عن طريق أي تدخل فيه.

وأضافت للجانب الموضوعي للتجريم اهتمت الاتفاقية بالقسم الإجرائي حيث نصت في المادة (16) على أنه (على الدول الأعضاء العمل على تطبيق أنظمة فنية لحماية

1- د-محمد فتحي عيد -الانترنت ودوره في انتشار المخدرات -اكاديمية نايف للعلومالامنية– الرياض -ص(943).

2- د-عمرو الفارق الحسين -المشكلات الهامة في الجرائم المتصلة بالحاسوب وابعادها -الطبعة الثانية -1995-ص(1333).

البيانات المخزنة مع إلزام العاملين في أي نظام معلوماتي بحفظ كل العمليات المنطقية التي تجري على الأجهزة لمدة لا تقل على 90 يوما).

كما نصت الاتفاقية ذاتها على حل مشكلة تحديد النطاق المكاني الواجب التطبيق على الجريمة في حالة تنازع القوانين ففي المادة (22) منها نصت على"أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها من الإجراءات الأزمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقاً لما هو وارد في المواد من (2 إلى 11) من الاتفاقية الحالية[1].

وتنص الفقرة(4) من المادة من الاتفاقية على عدم استبعاد أي اختصاص ينعقد للقضاء الوطني طبقا للقانون المحلي وفي حالة حدوث تنازع في الاختصاص فان يجب أن يتم حله بالتشاور بين الدول الأطراف حول المكان الأكثر ملائمة، كما أفردت الاتفاقية بندا خاصا لضرورة التعاون بين الدول الأطراف فيما يخص بتسليم المجرمين وتعقبهم والبحث عن الدليل وتيسير عملية الملاحقة القضائية (2).

كما قام المجلس الأوربي سنة 1991 بإنشاء جهاز شرطة أوربية تختص بملاحقة الجرائم العابرة للحدود وهو الأمر الذي يساعد في ملاحقة مرتكبي هذه الجرائم ومما لا شك فيه أن الجريمة المعلوماتية بطبعتها داخلة في اختصاص هذا الجهاز(3).

أضف إلى ما أوله كل من المؤتمر الدولي الثامن لمنع الجريمة ومعاملة المجرمين 1990 واتفاقية بودابست سنة 2001 من اهتمام دولي بمواجهة الجريمة الالكترونية، كرست الجمعية الدولية لقانون العقوبات المؤتمر الدولي الخامس للجمعية الذي عقد سنة 1994 لجرائم الحاسب الآلي والذي أوصت من خلاله بضرورة تجريم الاحتيال والغش والتزوير بواسطة الكمبيوتر وتخريب وإتلاف الحاسوب والدخول والاعتراض غير

1- د -موسى ارحومة -المرجع السابق -ص22

2- محمد عبد الله أبوبكر سلامة -جرائم الكمبيوتر والانترنت -منشأة المعارف، الإسكندرية -2006- ص(120).

3- د. جميل عبد الباقي الصغير -الجوانب الاجرائية المتعلقة بالأنترنت-دار النهضة العربية -2001 -ص(86).

المصرح به للحاسب الآلي، والإضرار بالبيانات والبرامج، كما أوصى بتعيين السلطات التي تقوم بالتفتيش والضبط وتخويلها سلطة اعتراض الاتصالات مع وجوب تحديد قواعد قبول الأدلة تحديدا واضحا[1].

كما قامت المنظمة العالمية للحقوق الفكرية بنص في معاهدة صدرت سنة 1996 على انه (تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية وتطبق تلك الحماية على برامج الحاسب الآلي أيا كانت طريقة التعبيرعنها أو شكلها وحثت الاتفاقية على ضرورة تطوير تشريعات حق المؤلف[2].

المطلب الثاني

موقف التشريعات الغربية من الجريمة الالكترونية

ان التقدم الهائل والمتسارع الذي تشهده الدول الغربية وبشكل مستمر في مجال التكنولوجيا جعل لها النصيب الأوفر من انتشار السلوكيات الإجرامية الالكترونية وهو ما داعي هذه الدول إلى الإسراع في تفعيل سياستها الجنائية للقضاء على هذا النوع من الإجرام، فقد اصدر المشرع السويد سنة 1973 قانون البيانات جرم من خلاله الاختراق المعلوماتي وتزوير المعلومات الالكترونية والدخول غير المشروع على البيانات الالكترونية، كما كانت الولايات المتحدة الأمريكية من أوائل الدول التي تطرقت لهذه الجرائم حيث أصدرت سنة 1976 قانون خاص بحماية الحاسوب، وبعد ان سجلت سنة 1985 حالتا سرقة برامج وبيانات قدرت الخسائر فيها بـ 18 ألف دولار لكل حالة حدد

1 -د. موسارحومة-المرجع السابق -ص (27).

2-د. عبد الرحمن جميل محمود حسين -الحماية القانونية لبرامج الحاسب الالي-جامعة النجاح الوطنية فلسطين-سنة 2009-ص(86-87)، انظر ايضا غازي عبد الرحمن هيان الرشيد -الحماية القانونية من جرائم المعلوماتية -الجامعة الاسلامية -لبنان 2004 ص(181).

معهد العدالة القومي خمسة أنواع رئيسية للجرائم المعلوماتية، ثم أصدرت القانون الفدرالي للمعلوماتية لسنة 2000[1].

كما قامت الولايات المتحدة الأمريكية بإنشاء جهاز شرطة خاصة بجرائم الانترنت سنة1987 تحول بعدها لجهاز شرطة دولية لمكافحة الجريمة المعلوماتية له اتصالا بأفراد متطوعين من 61 دولة على مستوى العالم.

كما صدر في بريطانيا قانون يجرم التزوير باستخدام الطرق الالكترونية منذ سنة1981.

وذلك قبل أن يعتمد القانون رقم 19 لسنة 1988 بشأن الجرائم في المواد المعلوماتية والذي قام بدمجه ضمن الفصل الثاني من قانون العقوبات وخصصت له المواد من (3/432 إلى 462/ 9) ثم أصدر سنة 1994 قانونا جديد عدل بموجبه بعض نصوص القانون الصادر في 1988[2].

كما قامت بريطانيا بتشكيل وحدة قوات شرطة وكلفتها بمتابعة الجرائم الالكترونية المتصلة بالأجرام المعلوماتي[3].

كما صدرت مجموعة كبيرة من الدول الغربية تشريعات ونصوص لمواجهة الجريمة الالكترونية من ذلك القانون رقم (147) الصادر في الصين سنة 1994، وفي البرازيل اقر القانون رقم(9.983)الصادر في 14 يوليو 2000 والذي عقاب المشرع من خلاله على إخفاء وإدخال البيانات المزورة في النظام المعلوماتي، وفي ايطاليا أضاف المشرع

1-يونس عرب -قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وسلطنةعمان-ورشة عمل لتطوير التشريعات في مجال مكافحة الجرائم الالكترونية المنعقدة بسلطنة عمان2-4 ابريل 2006ص(8)، انظر ايضا د احمد خليفة الملط -الجرائم المعلوماتية -رسالة دكتورة جامعة القاهرة -2005 -ص(102).

2-د. احمد خليفة الملط -مرجع سابق -ص(126).

3-د. موسى ارحومة -مرجع سابق -ص(17)،انظر ايضا -د محمد منبر الجهميني -جرائم الحاسبات ووسائل مكافحتها -دار الفكر الجامعي -الطبعة الثانية -2006.

البند رقم 615 لقانون العقوبات تحت مسمى حظر الدخول لأنظمة الحاسب والاتصالات، وفي اليابان صدر قانون حظر الدخول للكمبيوتر رقم 128 لسنة 1999، وفي البرتغال صدر القانون المعلومات الجنائي عام 1991 وفي تركيا عدل قانون العقوبات في القسم رقم 525 /ا بشان الدخول المحظور الى برامج وقواعد البيانات وغير ذلك الكثير من التشريعات الغربية المواجهة للجريمة الالكترونية كبلجيكا وتشيلي والمجر واليونان كندا وغيرها[1].

والملاحظ أن كل هذه الدول حاولت بمختلف الطرق التصدي للأجرام المعلوماتي الذي بات يجتاح أجهزة الحاسب الآلي، محاولات التصدي لهذه الجريمة على النطاقين الداخلي والدولي.

المطلب الثالث

موقف الدول العربية من جرائم الانترنت

بدأت بعض الدول العربية بمحاولات للقضاء على جرائم الانترنت، وذلك أما بإضافة نصوص قانونية إلى تشريعاتها النافذة او بإصدار قوانين خاصة بذلك وتطوير الأجهزة العاملة على مكافحة هذه الجريمة، وكانت من بين هذه المحاولات قيام جمهورية مصر العربية بإضافة المواد(72-73-74)لقانون الأحوال المدنية رقم 143 لسنة 1994، كما قامت باستحداث إدارة لمواجهة الجرائم المعلوماتية في وزارة الداخلية.

كما قامت السعودية سنة 2007بإصدار نظام مكافحة الجرائم المعلوماتية في التعاملات الالكترونية جرم من خلاله الدخول غير المشروع للبريد الالكتروني أو تغييرها

1-راجع في موقف الدول الغربية احمد خليفة الملط (162-163) و (145-146) -انظر ايضاً د-هشام فريد رستم-قانون العقوبات ومخاطر تقنية المعلومات،جامعة اسيوط 1992-ص(81) وما بعدها- وايضا-د. محمد غيطاس امن المعلومات والامن القومي-ص(229) د-موسى ارحومة ص(15) ومابعدها.

أو إتلافه أو تعديلها أو المساس بالحياة الخاصة عن طريق إساءة استعمال الهواتف المزودة بالكاميرات وما في حكمها، كما شدد العقوبة على من ينشئ مواقع لمنظمات إرهابية أو يروج أفكارها حيث يعاقب بالسجن مدة لاتزيد عن عشرة سنوات وبغرامة لا تزيد عن خمسة ملايين ريال[1].

وفي سلطنة عمان أضاف المشرع العماني المواد 276 مكرر 1 و276 مكرر 2 لمعالجة الجرائم الالكترونية جرم من خلالها الالتقاط غير المشروع للبيانات والمعلومات أو جمعها وإعادة استخدمها أو تسريبها كما جرم الدخول غير للمشروع لأنظمة الحاسب الآلي والتعدي على برامجه[2].

وفي المغرب تم نشر القانون رقم (02-07) لسنة 2003بشان الإخلال بسير المعالجة الآلية للمعطيات والبيانات وأصبح هذا القانون يشكل الباب العاشر من الجزء الأول من الكتاب الثالث من القانون الجنائي المغربي تحت عنوان المس بنظم المعالجة الآلية للمعطيات.

ويحتوي هذا القانون على تسعة فصول من الفصل 3-607 إلى الفصل 11-607 من مجموعة القانون الجنائي المغربي جرم من خلالها المشرع مجموعة من الأفعال التي تشكل اعتداء على النظم المعلوماتية من ذلك عرقلة هذه النظم المعلوماتية أو إحداث أي اضطراب فيها بصورة عمدية كما جرم تزوير وتزييف الوثائق المعلوماتية أو استعمالها مع العلم بأنها مزورة[3].

كما كانت مواجهة الإمارات العربية المتحدة للجرائم المعلوماتية من ابرز المواجهات العربية حيث أصدرت القانون الاتحادي رقم 2 لسنة 2006 في شان مكافحة جرائم

1-انظر جريدةالرياض السعودية موقع الجريدةwww.alryadh.com.

3- عبد الحق باسو -الارهاب المعلوماتي في القانون المغربي والدولي -ابحاث لدورة الخاصة بمكافحة الجرائم المعلوماتية -جامعة نايف للعلوم الامنية -2006-ص(15).

تقنية المعلومات، والذي تناول العديد من الجرائم المعلوماتية، مقررا الجزاءات الرادعة لها ومن بين هذه الجرائم جريمة الدخول على موقع معلوماتي بدون وجه حق، جريمة تزوير المستندات الالكترونية، جرائم إعاقة أو تعطيلاً واختراق أو التلاعب بالنظام المعلوماتي، جريمة الابتزاز والتهديد، جريمة الحصول على أرقام بطاقات الائتمان، كما جرم إتلاف الفحوص الطبية أو تعديلها بما يضر بسلامة المرضى، كما جرم اختراق النظم المعلوماتية للوصول إلى معلومات سرية بدون وجه حق، وغير ذلك من الجرائم التي من شانها ان تشكل اعتداء على القيم الأسرية كإنشاء مواقع الاتجار بالمخدرات أو لنشر الأفكار المخلة بالآداب العامة أو نشر الدعارة أو الترويج للجماعات الإرهابية، كما أضفى القانون صفة مأمور الضبط القضائي على بعض الموظفين الذين يصدر بتحديدهم قرار من وزير العدل والشؤون الإسلامية [1].

والجدير بالذكر أن الإمارات العربية المتحدة، تعرضت لمجموعة من السلوكيات الإجرامية كان من بينها 33 ألف قضية سطو سنة2000 وحدها[2]

وفي اليمن صدر القانون رقم 40 لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية، تناول المشرع في الفصل الثامن منه العقوبات التي تجرم الجرائم المعلوماتية في الماد من 37 الى41[3].

أما المشرع التونسي فقد أصدر قانون التجارة والمعاملات الالكترونية سنة 2000اعترف من خلاله بحجية المستندات الالكترونية في الإثبات، تلته في الاعتراف بهذا الدليل الإمارات العربية سنة2002 ومصر سنة 2004.

1- عبد الحق باسو -مرجع سابق -ص(16).
2هشام فريد رستم – قانون العقوبات ومخاطر المعلومات-مكتبة الآلات الحديثة -1992ص (81).
3سيناء عبدالله المحسن -المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية -ابحاث الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر -الدار البيضاء -2007 ص (8).

كما صدر في السودان قانون الجرائم المعلوماتية لسنة 2007م، والذي أسس لتجريم الأفعال التي تستهدف نظم ووسائط وشبكات المعلومات.

كما حاول المشرع الجزائري تدارك الفراغ التشريعي في مجال جرائم الانترنت بنصه على القانون 04-15-2004 والذي عدل بموجبه نصوص قانون العقوبات لتتضمن بعض صور الإجرام الالكتروني من ذلك تجريم الدخول غير المشروع للمنظومة المعلوماتية أو حذفها أو تغييرها أو تخريبها كما نص على تجريم التزوير الالكتروني أو الاستيلاء على المعطيات المخزنة في المنظومة المعلوماتية[1].

أما على الصعيد العربي الإقليمي فيعد التشريع العربي النموذجي الصادر من جامعة الدول العربية من أهم المراجع المتعلقة بالجهود العربية المكافحة للجريمة الالكترونية العربية، فهناك قرار صادر عن مجلس وزراء العدل العرب بجامعة الدول العربية بشأن مشروع قانون عربي استرشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، يتكون من 27 مادة [2].

نص في المادة 2 منه على تجريم الدخول غير المشروع إلى أي نظام معلوماتي، ونصت المادة 3 منها على أن تجرم الدول الأعضاء كل اعتراض لهذه البيانات بأي وسيلة الكترونية دون وجه حق، أما المواد من 4 الى 6فنصت على تجريم أي تعديل في البيانات أو تحريفها أو تدميرها أو تعديلها أو تغيير مسارها، و تجريم التدخل في النظام المعلوماتي ، كما جرمت إساءة استخدام النظام المعلوماتي بشكل يؤدي إلى إفشاء نظم الحماية الخاصة به، أو استخدام بطاقة ائتمانية للسحب الالكتروني من

---

1 - خثير مسعود -الحماية الجنائية لبرامج الكمبيوتر اساليب وثغرات -دار الهدى -2010-ص (123).

2-اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم 495 -د19 – 2003/10/8؛ ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 – د 2004/21-انظر محمود احمد عباينة-جرائم الحاسوب وابعاده الدولية -دار الثقافة للنشر والتوزيع - عمان 2005 ص(181).

الرصيد خارج حدود رصيده الفعلي أو كما جرم استخدام بطاقة مسروقة أو تحصل عليها بغير حق أو استخدامها في المعاملات المالية مع العلم بذلك.

والجدير بالذكر أن هذا القانون لم ينص بشأن الجرائم المعلوماتية على أي قواعد لتحديد الاختصاص بنظر هذه الجرائم، بالرغم من أن الجريمة الدولية لا يمكن مواجهتها إلا بالتعاون الدولي.

المطلب الرابع

الفراغ التشريعي الليبي أمام تحديات الجريمة المعلوماتية

أمام الفراغ التشريعي الليبي بات من الضروري استحداث آليات قانونية لمواجهة الجريمة المعلوماتية، أسوة بالتشريعات الأخرى،فالاكتفاء بالنصوص العقابية التقليدية الموضوعية منها والإجرائية لا يتماشى مع الطبيعة الخاصة لهذه الجرائم.

فعليه نوصي المشرع الليبي بسن قانون خاص بالجرائم المعلوماتية حتى لا يفلت مرتكبي هذه الجرائم بجرائمهم بحجة مبدأ الشرعية أو بحجة التقيد بالتفسير الضيق للنصوص العقابية، بحيث يكون هذا القانون شامل على تجريم كافة النشاطات الالكترونية الضارة بمصالح المجتمع المعلوماتية، فلم تعد الخصوصية تقتصر على المسكن والمحادثات الهاتفية ، وإنما استجدت عناصر أخرى أفرزتها المعلوماتية تستدعي الحماية الجنائية للخصوصية المعلوماتية، كما ان جريمة السرقة وان كانت من الجرائم ذات القالب الحر وبالتالي يمكن انطباق وصف العديد من الجرائم الالكترونية المالية عليها، كجريمة سرقة الأرقام السرية للبطاقات المالية واستخدمها من أشخاص لا حق لهم فيها باعتبار أن هذا السلوك يؤدي إلى حصول على نفع غير مشروع إضرارا بالغير مادة 461 عقوبات.

إلا أن وسائل وإجراءات الضبط والمحاكمة العادية لن تفلح في تعقب مرتكبيها ومواجهتها، أضف إلى أن بعض الجرائم المالية الالكترونية لا يمكن انطباق وصف السرقة عليه، كما انه لا تدخل ضمن جرائم التزوير والنصب التقليدية التي قد يتطلب ارتكابها استخدام وسائل محددة كالوثيقة أو التزام صفة الموظف العام وغير ذلك من الإشكاليات التي تثار اثر محاولات تكييف النصوص التقليدية على الجرائم الالكترونية، فعلى المشرع ان يقرر عقاب رادع على كل من تسول له نفسه باستغلال الفراغ التشريعي في هذا المجال للإضرار بمصالح الأفراد والجماعات الالكترونية، ولضمان عدم إفلات المجرم من العقاب ندعو المشرع إلى تبني مبدأ العالمية على نطاق تطبيق القانون من حيث المكان فبالنظر إلى أسلوب ووسائل ارتكاب هذه الجريمة فإنها غالبا ما تكون عابرة للحدود الدولة الواحدة، ولا يخفى علينا ماتثيره الجرائم العابرة للحدود من إشكاليات في تحريك ورفع الدعوى الجنائية وتحديد القانون الواجب التطبيق.

كما يجب أن يراعى في الناحية الإجرائية منه الطبيعة الغير مادية لهذه الجرائم وان ينص على إنشاء أجهزة شرطة وضبطية فنية متخصصة في الجرائم المعلوماتية، على أن يراعى فيه أيضا ضرورة تخصص القضاة وكفاءتهم في هذا المجال من الجرائم، وان يستوعب إجراءات الضبط الالكتروني وتدريب جهاز الضبطية وأجهزة الشرطة بحيث يكونوا على قدر عالي من التقنية والفنية لأن أي خطأ قد يؤدي الى محو الأثر وبالتالي ضياع الأدلة، وعلى المشرع مراعاة أن يستوعب قانونه وسائل الإثبات الالكتروني.

والجدير بالذكر أن التطور التشريعي الوحيد الذي صدر في ليبيا بخصوص الإجرام المعلوماتي كان بصدور القانون رقم 4 لسنة 1990 بشأن النظام الوطني للمعلومات والتوثيق والذي نص فيه على الحماية الجنائية للبيانات المخزنة في هذا النظام بتجريم

سوء استعمال، أو حيازة هذه البيانات، أو التقصير في التزام تسجيلها، أو الإخلال بواجب الحفاظ عليها باعتبارها دليلا وطنيا للمعلومات والإحصاءات[1].

كما قام المشرع الليبي بإنشاء إدارة خاصة بمكافحة جرائم تقنية المعلوماتية تابعة للإدارة العامة للأدلة والبحث الجنائي وذلك بموجب القرار رقم (63) لسنة 2005 من بين مهامه مكافحة جرائم الانترنت والقيام بأعمال التحري وجمع الاستدلالات المتعلقة بها، إضافة إلى القيام ببرامج توعية وإجراء البحوث ونشر الإحصائيات ذات الصلة بجرائم الحاسب الآلي [2].

1د-محمد سامي الشوا – ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية – القاهرة 1994 ص (155).
2-د -موسى ارحومة -ص(19).

الخاتمة

توصلنا من خلال بحثنا لموضوع الجريمة الالكترونية إلى النتائج والتوصيات الآتية:

أولا: النتائج: -

1. أن الجريمة الالكترونية وان كانت تحدث في عالم فتراضي إلا أنها واقعة لابد من التسليم بوجودها وإزالة المعوقات التي تحول دون مواجهتها.
2. الجريمة الالكترونية ذات طابع عالمي فهي جريمة عابرة للحدود غالبا.
3. مرتكبي الجرائم الالكترونية يتمتعون بقدر عالي من الذكاء ولهم القدرة على إخفاء أثار جريمتهم بسرعة فائقة.
4. الجريمة الالكترونية ذات صبغة فنية لذا تحتاج الى أشخاص لهم دراية ببرامج الحاسب الآلي والنظم المعلوماتية لمواجهتها.
5. إن القوانين العقابية التقليدية غير كافية في مواجهة هذا النوع من الجرائم، وحتى الدول التي أضافت بعض المواد الى قوانينها لمواجهة هذه الجريمة لم توفق في ذلك نظرا لما تمتاز به هذه الجرائم من طبيعة خاصة ستستدعى سن قانون متكامل لمواجهتها بحيث يشمل الشقين الموضوعي والإجرائي للحماية الجنائية.
6. أن المشرع الليبي لم يقوم بأي محاولات جادة لمواجهة الجريمة الالكترونية.

ثانياً : التوصيات: -

1. نوصي المشرع الليبي بسن قانون خاص لمواجهة الجريمة الالكترونية.
2. ضرورة قيام مؤسسات المجتمع المدني برفع درجة الوعي بمخاطر الجرائم الالكترونية، والقيام بحملات وورش عمل تثقيفية تستهدف توعية المجتمع بمخاطرها وتحذيرهم من فتح الملفات القادمة من مجهولي الهوية لتجنب ان تكون حاملة لملفات تجسس أو تدمير.

3. نوصي المشرع بان يأخذ بعين الاعتبار الطبيعة الفنية لهذه الجرائم، وما تتطلبها مواجهتها من تخصيص جهاز شرطة وضبطية على دراية فنية واسعة بهذا المجال، وما قد تتطلبها سرعة مواجهتها من تخصص القضاة.
4. ندعو مختلف الدول إلى التعاون الدولي في مواجهة الجرائم الإلكترونية، بحيث يكون هناك اتفاق دولي على تبني مبدأ العالمية في تحديد مكان سريان القانون الجنائي المعلوماتي نظر لما يتسم به هذا النوع من الإجرام كونه عابر للحدود، فضلا عن ان هذا النوع من الجرائم بات مسرحا سهلا للجريمة المنظمة ولقيادة الجماعات الإرهابية عن بعد، لذا نوصي بتكثيف اتفاقيات التعاون الدولي المشترك لمكافحة الجريمة الالكترونية.
5. فرض مناهج دراسية في كليات القانون والضباط تتضمن مادة عامة عن الشبكات المعلوماتية.

قائمة المراجع

1- د.أيمن عبد الحفيظ -الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية دون دار نشر -2005.

2- د.جمال محمد غيطاس -امن المعلومات والأمن القومي -دار النهضة العربية - الطبعة الأول -2007.

3- د.جميل عبد الباقي الصغير -الجوانب الإجرائية المتعلقة بالانترنت-دار النهضة العربية -2001.

4- د.خثير مسعود -الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات -دار الهدى - 2010.

5- د.خليفة الملط -الجرائم المعلوماتية -رسالة دكتورة جامعة القاهرة -دار الفكر الجامعي-الطبعة الثانية-2006.

6- د.سيناء عبد المحسن محسن -المواجهة التشريعية للجرائم المتصلة بالكمبيوتر في ضوء التشريعات الدولية والوطنية -الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر - الدار البيضاء -المملكة الغربية -من 10 الى 20 يوليو 2007.

7- د.طارق ابراهيم الدسوقي -الأمن المعلوماتي -النظام القانوني لحماية المعلوماتية - دار الجامعة الجديدة للنشر - 2009.

8- د.عباس أبو شامة عبد المحمود -عولمة الجريمة الاقتصادية -جامعة نايف للعلوم الأمنية -2007.

9- د.عبد الحق باسو -الإرهاب المعلوماتي في القانون المغربي والدولي -أبحاث لدورة الخاصة بمكافحة الجرائم المعلوماتية-جامعة نايف للعلوم الأمنية -2006.

10- د.عبد الرحمن جميل محمود حسين -الحماية القانونية لبرامج الحاسب الآلي -جامعة النجاح الوطنية فلسطين-سنة 2009.

11- د.عبدالفتاح بيومي حجازي -مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت -دار الفكر الجامعي -الطبعة الأولى -2006.

12- د.عمرو الفاروق الحسين -المشكلات الهامة في الجرائم المتصلة بالحاسوب وأبعادها -الطبعة الثانية -1995.

13- د.غازي عبد الرحمن هيان الرشيد -الحماية القانونية من جرائم المعلوماتية - الجامعة الإسلامية -لبنان 2004.

14- د.محمد بن عبد الله بن علي المنشاوي -جرائم الانترنت في المجتمع السعودي -رسالة مقدمة لكلية الدارسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية -أكاديمية نايف للعلوم الأمنية -2003.

15- د.محمد دباس الحميد -ماركو ابراهيم نينو-حماية أنظمة المعلومات -دار الحامد للنشر والتوزيع -عمان -الطبعة الاولى -2007.

16- د.محمد سامي الشوا - ثورة المعلومات وانعكاساتها على قانون العقوبات - دار النهضة العربية - القاهرة 1994.

17- د.محمد سيد سلطان،قضايا قانونية في امن المعلومات وحماية البيئة الالكترونية -2012-متوفر على الموقع التالي www.nashiri.ne.

18- د.محمد عبد الرحيم سلطان -جرائم الانترنت والاحتساب عليها -مؤتمر القانون والكمبيوتر والانترنت -من 1-3 مايو 2000-جامعة الامارات العربية المتحدة؛كلية الشريعة والقانون، المجلد الثالث،الطبعة الثالثة،2007.

19- د.محمد عبد الله أبوبكر سلامة -جرائم الكمبيوتر والانترنت -منشأة المعارف،الإسكندرية -2006.

20- د.محمد عبيد الكعبي -الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت -دار النهضة العربية -1992.

21- د.محمد فتحي عيد -الانترنت ودوره في انتشار المخدرات -أكاديمية نايف للعلوم الأمنية-الرياض.

22- د.محمود ابراهيم محمد الشافعي -النقود الالكترونية مجلة الامن والحياة - أكاديمية الشرطة -دبي 2004.

23- د.مصطفى محمد موسى-التحقيق الجنائي في الجرائم الالكترونية،الطبعة الأولى،مطابع الشرطة 2009.

24- د.موسى مسعود ارحومة -الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية -المؤتمر المغاربي الاول حول المعلوماتية والقانون - أكاديمية الدراسات العليا -طرابلس-2009.

25- د.نهلا عبد القادر المؤمني -الجرائم المعلوماتية -دار الثقافة للنشر-الطبعة الأولى -عمان -2007.

26- د.هدى قشقوش -جرائم الحاسب الالكتروني في التشريع المقارن -الطبعة الأولى -دار النهضة العربية-1995.

27- د.هشام فريد رستم،قانون العقوبات ومخاطر تقنية المعلومات،مكتبة الآلات الحديثة -1992.

28- د.ياكوفميخايلوبيلسون-الانتربول في الصراع ضد الجريمة الجنائية -ترجمة: عماد محمود طحينة ومازن محمد نقاع -دار معد للنشر والتوزيع -1991.

29- د.يونس عرب -قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وسلطنة عمان-ورشة عمل لتطوير التشريعات في مجال مكافحة الجرائم الالكترونية المنعقدة بسلطنة عمان 2-4 ابريل 2006-دار الفكر الجامعي - الطبعة الثانية -2006.

30- جريدة الرياض السعودية موقع الجريدة .www.alryadh.com