السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية.
الاتجاهات الدولية في مكافحة الجريمة الالكترونية.

ليندة شرا بشة.
الدرجة العلمية: أستاذة مساعدة.
التخصص: قانون عام.
ماجستير في القانون الدولي العام
المركز الجامعي سوق أهراس.

مقدمة:

تعد جرائم الكومبيوتر و الانترنت أو ما يطلق عليها بالجريمة الالكترونية من الجرائم المعلوماتية المعاصرة و العابرة للحدود و التي ظهرت مؤخرا مع الانتشار التكنولوجي خاصة لارتباطها بجهاز الحاسب الآلي(الكومبيوتر)، و أداة الجريمة تتمثل في شبكة الانترنت هذه الجريمة التي تثير في مجملها الكثير من الإشكاليات من مختلف النواحي كصعوبة اكتشافها وكذا إثباتها لا سيما و أنها تتسم بطابع الحيلة و الدهاء من طرف مرتكبيها من خلال استعمال تقنيات معلوماتية عالية الكفاءة مما يؤدي إلى اختراق الشبكات و أجهزة الحاسب الآلي المرتبطة بالانترنت حيث يتم اختراق نظام الأمن بالشبكة و الدخول إلى الجهاز للكشف عن محتوياته أو إتلافها و التلاعب بالمعلومات المخزنة فيها.

بالنظر لخطورة هذه الجريمة و صعوبة الكشف عنها و غياب الدليل المادي الذي يدين مرتكبها فإنها أصبحت تطغى على ساحة الإجرام و بشكل كبير نتيجة لغياب استراتيجة فعالة لمحاربتها و التقليل منها خاصة على المستوى الدولي في ظل قلة الاتفاقيات الدولية وصعوبة التعاون الدولي للحد منها و هذا طبعا بالنظر لطبيعتها الخاصة.هذا الأمر يجعلنا نطرح التساؤلات الآتية:

ماهي أهم الاتفاقيات الدولية المتعلقة بمكافحة الجريمة الالكترونية؟

وماهي الجهود الدولية الرامية لمكافحتها ؟و ما مدى نجاعتها؟ و للإجابة عن هذه التساؤلات قسمنا هذه المداخلة إلى مبحثين:

المبحث الأول: الجريمة الالكترونية في المواثيق الدولية

المبحث الثاني:السياسة الدولية في مكافحة الجريمة الالكترونية.

المبحث الأول: الجريمة الالكترونية في المواثيق الدولية

تعد الجريمة الالكترونية نشاطا إجراميا تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود[1][1].و قبل التطرق إلى أهم الاتفاقيات الدولية المتعلقة بهذه الجريمة لا بأس و أن نشير إلى بعض أشكال هذه الجريمة من الناحية الدولية مع تبيان بعض الأمثلة عنها.

المطلب الأول: نماذج عن الجريمة الالكترونية على المستوى الدولي.

تتنوع الجريمة الالكترونية و تأخذ أشكالا متعددة سوف نحاول التطرق اليها على سبيل المثال مع تدعيمها ببعض الأمثلة في دول من العالم.

الفرع الأول: حرائم التجسس الالكتروني و جرائم القرصنة

أولا: جرائم التجسس الالكتروني: يعتمد هذا النوع من الجرائم على تقنيات عالية التقدم حيث لم يعد يقتصر التجسس على ما يتعلق بالمعلومات العسكرية أو السياسية بل تعداه إلى المجال الاقتصادي و التجاري و الثقافي، و لقد ظهر هذا النوع من الجرائم خصوصا بعد أحداث الحادي عشر من سبتمبر التي شهدتها الولايات المتحدة الأمريكية [2][2]، و من الأساليب المعتمدة أسلوب إخفاء المعلومات داخل المعلومات بحيث يتم إخفاء تلك المعلومات المهمة و المستهدفة داخل معلومات عادية في جهاز الحاسب الآلي و من ثم يتم تهريبها باستعمال أساليب متطورة لا يتم اكتشافها و لو ضبط الشخص متلبسا، و مثال ذلك: قيام شبكة دولية ضخمة للتجسس الالكتروني التي تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات في كندا و بريطانيا لرصد المكالمات الهاتفية بهدف التعامل مع الأهداف غير العسكرية، و لا يقتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية و الشبكات الدولية بل يشمل الاتصالات التي تجري عبر أنظمة الاتصالات الأرضية[3][3].

ثانيا: جرائم القرصنة: اتسعت و تطورت صور القرصنة من خلال العثور على مواقع الانترنت لترويج البرامج المقرصنة مجانا أو بمقابل مبلغ رمزي مما ألحق العديد من

1- أنظر: عد الفتاح بيومي حجازي- الإثبات الجنائي في جرائم الكومبيوتر و الانترنت -دار الكتب القانونية- 207-ص 13.

2- راجع في هذا الصدد: عبد الفتاح مراد- شرح جرائم الكومبيوتر و الانترنت-دون ذكر دار النشر- ص 382.

3- عبد الفتاح بيومي حجازي- المرجع السابق- ص29.

الخسائر المادية الباهضة مما أدى بالشركات المتخصصة في صناعة البرامج إلى إنشاء منظمة خاصة لمراقبة و تحليل ما يعرف بسوق البرمجيات، و منها منظمة اتحاد برمجيا الأعمال التي أجرت دراسة حول ذلك و تبنت الحلول المناسبة[4][4].

و مثال ذلك: تعرض أنظمة تشغيل مايكروسوفت لبرامج الكومبيوتر لعملية قرصنة مستعملين في ذلك عامل ذكي لبرامج الكومبيوتر يمكنه التجول بحرية عبر الشبكات لالتقاط المعلومات و نقلها دون قيام المتسلل باختراق الكومبيوتر نفسه، حيث تم فتح تحقيق في هذا المجال[5][5].

كما يتم أيضا إرسال فيروسات لتخريب الجهاز و محتوياته حيث بمجرد كتابة كلمة أو فتح البرنامج الحامل للفيروس أو الرسالة البريدية المرسل معها الفيروس تتم إصابة الجهاز و من ثم يقوم بمسح محتوياته أو العبث بالملفات الموجودة فيه.

الفرع الثاني: جرائم الإرهاب الالكتروني و الجرائم المنظمة:

أولا: جرائم الإرهاب الالكتروني: أدى التطور الالكتروني ، و قيام ما يعرف بالحكومات الالكترونية إلى تغيير أنماط الجريمة الالكترونية ، و ظهور ما يعرف بالإرهاب الالكتروني، حيث تم إنشاء لجنة خاصة لحماية البنية التحتية في الولايات المتحدة الأمريكية ،وتم تحديد الأهداف المحتملة من قبل الإرهابيين و هي مصادر الطاقة الكهربائية، و الاتصالات، و شبكات الحاسب الآلي.

وما تجدر الإشارة إليه أنه بعد أحداث 11 سبتمبر 2001 تمت ممارسة الإرهاب الالكتروني ضد المواقع الإسلامية و العربية أيضا.

ثانيا: الجرائم المنظمة:

تم استغلال الإمكانيات المتاحة ي وسائل الانترنت لتخطيط و تمرير و توجه المخططات الإجرامية و تنفيذ و توجيه العمليات غر المشروعة بكل سهولة من خلال إنشاء مواقع خاصة بها على شبكة الانترنت لمساعدتها في إدارة العمليات، و الترويج بتجارة المحذرات عبر الانترنت أيضا و تعليم كيفية زراعتها و صناعتها .

و كذا جرائم غسل الأموال التي تعتمد على إخفاء المصدر غير المشروع الذي تكتسب منه الأموال[6][6].

1- أنظر: عبد الفتاح مراد- المرجع السابق- ص 385.

2- هناك حادثة أخرى أطلق عليها **"حادثة الأصدقاء الأعداء"**حيث تمكن احد الإسرائيليين من اختراق أنظمة معلومات حساسة سنة 1998 في كل من الو.م.أ و إسرائيل لمؤسسات عسكرية و مدنية و تجارية حيث تمت متابعة نشاطه من قبل محققين في الو.م.أ و تبين أن مصدر الاختراق هو جهاز الكومبيوتر، و تم فتح تحقيق في ذلك.

3- عبد الفتاح مراد- المرجع السابق- ص ص 384-385.

حيث يجد المتصفح للانترنت مواقع عديدة تتحد عن غسيل الأموال غير المشروعة التي تتميز بالسرعة و إغفال التوقيع و استعمال بطاقات مزورة شبيهة ببطاقات البنوك المستخدمة التي تساهم في تحويل الأموال عبر الانترنت مع ضمان تشفير و تأمين العملية كل ذلك ساعد على سهولة و سرعة الجريمة دون ترك الأثر[7][7]

إضافة إلى العديد ن الجرائم الأخرى كالجرائم الماسة بالتجارة الالكترونية من خلال الاستيلاء على بطاقات الائتمان[8][8]، و كذلك الجرائم الاقتصادية كسرقة خطوط الهاتف و العبث بها و إتلافها، و تحويل الأرصدة النقدية و غيرها [9][9].

و عليه بالنظر الى الطبيعة الخاصة التي تتميز بها الجريمة الالكترونية باستخدام الوسائل الالكترونية المستحدثة تمتد لتشمل البعد العالمي هذا الأخير الذي لا يتقيد بحدود دولة معينة وهذا ما يجعله ينعكس على آليات مكافحتها.

المطلب الثاني:أهم الصكوك الدولية الخاصة بالجرائم الالكترونية.

مع تطور تقنية المعلومات، و اهتمام الأنظمة الدولة بموضوع الجرائم المعلوماتية وقعت العديد من الصكوك و المواثيق الدولية من طرف دول أدركت فعلا مدى الخطورة التي تشكلها هذه الجريمة بوصفها من الجرائم العابر للحدود، فقد يكون الجاني في بلد و المضرور في بلد آخر، و مزود الخدمة في بلد ثالث و المستضيف للموقع و الذي صر منه الفعل المجرم في بلد آخر ومن هنا أثيرت مسألة تطبيق نصوص القانون الجنائي، لذلك سنحاول التطرق إلى المواثيق الدولية لجرائم الكمبيوتر و الانترنت.

الفرع الأول:القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة و معاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر.

يعد هذا القرار من الجهود التي بذلتها الأمم المتحدة حيث عقد هذا المؤتمر في هافانا سنة 1990و قد حث في قراره المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء أن تكثف جهودها لمكافحة إساءة استعمال هذا الجهاز و بتجريم تلك الأفعال جنائيا[10][10].

1- راجع في هذا الصدد: عبد الفتاح مراد- قانون مكافحة غسل الأموال و لائحته التنفيذية و القوانين المكملة له- ص ص 42، 43.

2- أنظر: محمد الشناوي- إستراتيجية مكافحة جرائم النصب المستحدثة(الانترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة)- الطبعة الأولى-دار البيان للطباع و النشر- القاهرة- 2006-ص ص 81، 84.

- و كذلك: عبد الفتاح بيومي حجازي- المرجع السابق-ص ص 60، 61.

4- عبد الفتاح مراد- المرجع السابق- ص237.

و اتخاذ الإجراءات التالية متى دعت الضرورة لذلك:

* ضمان أن الجزاءات و القوانين الراهنة بشأن سلطات التحقيق و الأدلة في الإجراءات القضائية تنطبق على نحو ملائم ، و إدخال تغييرات مناسبة عليها إذا دعت الضرورة لذلك.

* النص على جرائم و جزاءات و إجراءات تتعلق بالتحقيق و الأدلة حيث تدعو الضرورة للتصدي لهذا الشكل الجديد و المعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم [11]11

كما حث أيضا الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالكمبيوتر بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين و تبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة ، و نصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين و تبادل المساعدة في المسائل الجنائية تنطبق بكل تام على الأشكال الجديدة للإجرام مثل الجرائم الالكترونية ، و أن تتخذ خطوات محددة نحو تحقيق هذا الهدف.

كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة المعلوماتية بصفة عامة بضرورة وضع أو تطوير [12]12:

1- معايير دولية لأمن المعالجة الآلية للبيانات.

2- اتخاذ تدابير ملائمة لحل إشكالية الاختصاص القضائي التي تثيرها الجرائم المعلوماتية العابر للحدود أو ذات الطبيعة الدولية.

3- إبرام اتفاقيات دولية تنطوي على نصوص تنظيم و إجراءات التفتيش والضبط المباشر الواقع عبر الحدود، على الأنظمة المعلوماتية المتصلة فيما بينها و الأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد و حرياتهم و سيادة الدول.

<u>الفرع الثاني</u>: مقررات و توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 1994 البرازيل بشأن جرائم الكمبيوتر.

يمكن اعتبارها انعقد هذا المؤتمر سنة 1994 بالبرازيل حيث نص على الأفعال المجرمة التي

جرائم معلوماتية كالاحتيال، و الغش المرتبط بالكمبيوتر من خلال إتلاف و محو المعطيات ، و أيضا ما يعرف بالتزوير المعلوماتي و يشمل إتلاف و محو البرامج و البيانات و تعطيل

1- راجع في هذا الصدد:عبد الفتاح مراد- المرجع السابق- ص 237.

2- أنظر: عبد الفتاح بيومي حجازي- المرجع السابق- ص 190.

وظائف الكمبيوتر و نظام الاتصالات(الشبكات)، أو الدخول غير المصرح به عن طريق انتهاك إجراءات الأمن.

أما من الناحية الإجرائية فان القرار الصادر عن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات تضمن جملة من القواعد الإجرائية في بيئة الجرائم المعلوماتية تتمثل فيما يلي[13][13]:

* القيام بإجراء التفتيش و الضبط في بيئة تكنولوجيا المعلومات، و أيضا تفتيش شبكات الحاسب الآلي.

* التعاون الفعال بين المجني عليهم و الشهود و كذا مستخدمي المعلومات من أجل إتاحة استخدام المعلومات للأغراض القضائية.

* اعتراض الاتصالات داخل نظام الحاسب الآلي ذاته و ممارسة الرقابة عليها.

الفرع الثالث: اتفاقية برن الدولية لحماية المصنفات الأدبية و الفنية.

بهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام اتفاقية برن الدولية في 9 سبتمبر 1886، و المكملة بباريس في ماي 1896، و المعدلة في برلين في 13 سبتمبر 1908، و المكملة ببرن في 20 مارس 1914، و المعدلة بروما في جوان 1928، و بروكسل سنة 1948، و استوكهولم في جويلية 1967، و باريس في جويلية 1971، حيث تشكل الدول الأطراف في هذه الاتفاقية اتحادا لحماية حقوق المؤلفين على مصنفاتهم الأدبية و الفنية.

و بموجب اتفاقية برن الدولية تتمتع برامج الحاسب الآلي" الكمبيوتر" سواء كانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية وفقا لما جاء فيها [14]14

" المتعلقة بالجوانب المتصلة بالتجارة الدولية حيث تسعى الدول TRIPISإضافة إلى اتفاقية "

الأطراف في الاتفاقية إلى تشجيع الحماية الفعالة و الملائمة لحقوق الملكية الفكرية من أجل التخفيف العراقيل التي تعوق التجارة الدولية.

1- عبد الفتاح مراد- المرجع السابق- ص 242.

2- للاطلاع على هذه الاتفاقية أنظر: محمد عد الله أبو بكر سلامة- موسوعة جرائم المعلوماتية "جرائم الكمبيوتر و الانترنت"- المكتب العربي الحديث- الإسكندرية.

- و كذلك: عبد الفتاح مراد- المرجع السابق- ص 280 و ما يليها.

الفرع الرابع: اتفاقية بودابست لمقاومة جرائم المعلوماتية و الاتصالات 2001.

إدراكا من الدول بمدى خطورة الجريمة المعلوماتية بوصفها جريمة عابرة للحدود فقد تم التوقيع عليها من طرف ثلاثون دولة في العاصمة المجرية " بودابست" نذكر منها: دول أعضاء من الاتحاد الأوروبي ، إضافة إلى كندا، اليابان، جنوب إفريقيا، أمريكا، و جاءت هذه الاتفاقية لتعالج إشكالية دولية الجريمة الالكترونية و تجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة و تعقب مرتكبيها و المساعدة على الاستدلال عليهم و ضبطهم كما تحدد أفضل الطرق الواجب إتباعها في التحقيق في جرائم الانترنت التي تعهد الدول الموقعة بالتعاون الوثيق من أجل محاربتها،كما فصلت الاتفاقية النصوص الجنائية الموضوعية للجريمة و أنواعها كما تشمل جوانب عديدة من جرائم الانترنت من بينها الإرهاب، عمليات تزور بطاقات الائتمان و غيرها....

و تعتبر هذه الاتفاقية أحد محاولة و أكثرها تنوعا من أجل تنسيق قوانين جديدة في دول عديدة ضد إساءة استخدام الانترنت.كما نشير إلى أنها تأتي بعد فترة طويلة من المشاورات بين الحكومات و أجهزة الشرطة و قطاع الكمبيوتر و قد صاغ نصها عدد من الخبراء القانونين في مجلس أوروبا بمساعدة دول أخرى.

الفرع الخامس: قانون الأونستيرال النموذجي.

اقتناعا من الدول بضرورة منع هذه الجرائم و مكافحتها خاصة و أن ذلك يتطلب استجابة ديناميكية في ضوء الطابع الدولي و الأبعاد الدولي لإساءة استخدام الكمبيوتر و الجرائم المتعلقة به تم صياغة قانون الأونيسترال النموذجي بشأن التجارة الالكترونية،و الآخر بشأن التوقيعات الالكترونية.

أولا: قانون الأونيسترال النموذجي بشأن التوقيعات الالكترونية.

اعتمد هذا النص في 5 جويلية 2001 و ينطبق هذا القانون حيثما تستخدم توقيعات الكترونية[15][15] خاصة بعدما أصبح التوقيع بمفهومه التقليدي لا يستجيب لمتطلبات السرعة،

1- عبد الفتاح مراد- المرجع السابق-ص 244.

- و كذلك: محمد عبد الله أبو بكر سلامة- المرجع السابق- ص 14.

- منير محمد الجنبيهي و ممدوح محمد الجنبيهي- تزوير التوقيع الالكتروني- دار الفكر الجامعي- الإسكندرية- 2006- ص ص 111، 115.

- كذلك: شريف محمد غنام- حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني- دار الجامعة الجديدة- 2007-ص 194.

و الحداثة التكنولوجية حيث أنه أمام هذه التطورات تلاشت وظيفة التوقيع التقليدي ليحل محله التوقيع الالكتروني و هو عبارة عن كود سري أو شفرة سرية يتم الحصول عليها بعد إتباع جملة من الإجراءات.

ثانيا: قانون الأونيسترال النموذجي بشأن التجارة الالكترونية.

تنطبق نصوص هذا القانون على أي نوع من المعلومات التي تكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية، بحيث يتم استلامها أو تخزينها بوسائل الكترونية، و يتم تبادل هذه البيانات من خلال نقلها الكترونيا من حاسوب إلى آخر باستخدام معيار متفق عليه، مع الأخذ بعين الاعتبار تفسير هذا القانون لمصدره الدولي و لضرورة توحيد تطبيقه[16][16].

المبحث الثاني:السياسة الدولية في مكافحة الجريمة الالكترونية.

تنوعت الجهود الدولية في مكافحة الجريمة الالكترونية حيث تم اتخاذ العديد من الآليات و الإجراءات للحد و التقليل منها إلا أن هذه الجهود تبقى غير كافية مقارنة بالتقدم التكنولوجي الذي تشهده الدول على مستوى المعلوماتية و الاستعمال اللامتناهي للكمبيوتر و الانترنت و سنتطرق إلى إبراز هذه الجهود مع تبيان صعوبة التعاون الدولي للقضاء على هذه الجريمة الدولي العابرة للحدود لتظافر العديد من العوامل سيتم توضيحها لاحقا.

المطلب الأول:الجهود الدولية لمكافحة الجريمة الالكترونية.

الفرع الأول: الجهود الحكومية.

إزاء تزايد الجرائم المعلوماتية الخطيرة فقد بذلت جهودا كبيرة لمحاربتها من مختلف جوانبها ، حيث تم تشريع العديد من القوانين التي تقضي بمعاقبة المتسببين في زرع الفيروسات، كما فرضت العديد من الشركات ما يعرف" **بنظام الحجر الصحي** "على أجهزتها المعلوماتية بحيث تمنع الاتصال بالأجهزة خارج الشركة على الرغم من أن عزل هذه الأجهزة يلغي العديد من الفوائد التي توفرها المعلوماتية، و في المقابل هناك فيروسات لا تزرع في البرامج و إنما تصيب الجهاز مباشرة.[17][17]

كما بذلت جهودا دولية لمواجهة هذه الجريمة بمختلف أنواعها و مثال ذلك: مواجهة القرصنة الالكترونية لحماية العلامات التجارية من مسجلي العناوين الالكترونية، و على الرغم من تنوع الجهود إلا أنها تشترك جميعا في أنها تتضمن مجرد توجيهات و توصيات للجهات المسؤولة في تسجيل العناوين الالكترونية.

1- عبد الفتاح مراد- المرجع السابق-ص 225.

2- عبد الفتاح مراد- المرجع نفسه- ص424.

و هناك البروتوكول المشترك للعناوين الالكترونية الدولية و هو أيضا يعد من المجهودات الدولية لمحاربة القرصنة الالكترونية و حماية مالكي العلامات التجارية و في المقابل تم تكوين لجنة دولية خاصة بهدف الوصول إلى أفضل الحلول و الاقتراحات.والعمل على خلق تعاون دولي شامل في حقل امتداد إجراءات[18][18] التحقيق و الملاحقة خارج الحدود وهي كانت و لا تزال محل اهتمام على الصعيدين الوطني و الدولي.

كما تعتبر الشرطة (الانتربول) الأداة المثلى لتفعيل القوانين المختلفة و تنفيذها لما لها من دور رئيسي في المحافظة على الأمن العام لذلك فهي أيضا تتمتع بالمؤهلات اللازمة لقيامها بهذا الدور من خلال تعقب الجريمة و المجرمين[19][19]

الفرع الثاني: أساليب المكافحة التقنية.

بدأ عدد من خبراء المعلوماتية يتخصصون في محاربة فيروسات الكمبيوتر عن طريق إعداد برامج خاصة بذلك إما لتطهير الجهاز نفسه أو بتلقيح الجهاز من الفيروس.

و هناك رق مكافحة تقني بإمكان أي شخص القيام ها يمكن أن نلخصها فيما يلي:

أ/ اتخاذ ما يعرف بالإسعافات الأولية عند اكتشاف جريمة معلوماتية من خلال إعداد نسخ احتياطية من أسطوانات البيانات و أيضا إعداد نسخ احتياطية من اسطوانات البرامج.

ب/ هناك إجراءات فنية كعدم استخدام البرامج المسروقة للتقليل من احتمالات العدوى من الفيروس، و حماية البرامج الأصلية و عدم استعمال البرامج المجانية.

المطلب الثاني:صعوبة التعاون الدولي لمكافحة الجريمة الالكترونية.

لقد قدمت شبكة المعلومات الدولية مجموعة متنوعة و معقدة من الاستخدامات في شتى المجالات السياحية، الثقافية، الاقتصادية، و الأمنية و حتى الشؤون العسكرة الأمر الذي زاد من حالات الاعتداء على خصوصية سرية المعلومات بقصد السرقة، التجسس، القرصنة، و التخريب. حيث أصبح هاجسا لكل دول العالم خاصة بسبب الانتشار الواسع لتبادل المعلومات المشفرة ذات الصلة بالتجسس السياسي أو العسكري أو الصناعي، أو أية نشاطات إجرامية . فنادى البعض بضرورة انشآ وحدات خاصة بمكافحة الجريمة المعلوماتية أسوة بجهات البحث الجنائي الوطنية و الدولية(الانتربول)، و ذلك لإثبات الجريمة عند وقوعها و تحديد أدلتها و

1-سامي علي حامد عياد– الجريمة المعلوماتية و إجرام الانترنت– دار الفكر الجامعي– الإسكندرية– 2007– ص 103.

2– فتوح الشاذلي، عفيفي كامل عفيفي– جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون– دراسة مقارنة– منشورات الحلبي الحقوقية– ص 349.

– و كذلك: مصطفى محمد موسى– الجهاز الالكتروني لمكافحة الجريمة– دار الكتب القانونية– مصر– 206– ص 223.

فاعليها مما يعني إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات الخاصة و تبادل الخبرات و المعلومات حول هذا النوع من الجرائم و مرتكبيها و سبل مكافحتها.

و رغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة المعلوماتية، إلا أن هناك عوائق تحول دون ذلك بل و تجعل من هذا التعاون صعبا، و يمكن إيجاز ذلك في الأسباب التالية:[20][20]

أولا: عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي، بسبب أن الأنظمة القانونية في بلدان العالم لم تتفق على صور محددة يندرج ضمنها ما يسمى: بإساءة استخدام نظم المعلومات الواجب إتباعها، كما انه لا يوجد تعريف محدد للنشاط المفروض أن يتفق على تجريمه و هذا راجع إلى قصور التشريع ذاته في كافة بلدان العالم و عدم مسايرته لسرعة التقدم المعلوماتي ومن ثم الجريمة المعلوماتية.

و ما تجدر الإشارة إليه أن العديد من الدول العربية لم تصدر قانونا يتعلق بالجريمة المعلوماتية سواء ارتكبت عن طريق الكمبيوتر أو عن طريق الانترنت، و لا يزال الخلاف قائما حول أفضلية تعديل التشريعات العقابية لكي تستوعب نماذج الجريمة المعلوماتية أم أنه تعدل قوانين حماية الملكية الفكرية كي تستوعب هذه الأنشطة من السلوك و يتم تجريمها، أم من الأفضل إصدار تشريعات جديدة خاصة بالجريمة المعلوماتية ،حتى أن الأمر لا يتوقف هنا بل يتعداه ، حيث أن عدم اتفاق الأنظمة القانونية المختلفة على صورة موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على تنظيم أنفسهم و ارتكاب جرائمهم دون التقيد بالحدود الجغرافية الأمر الذي يؤكد حتمية التعاون الدولي لمكافحة هذه الجريمة.

ثانيا: عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرام ، و حتى في حالة وجودها فان هذه المعاهدات تبقى قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم و برامج الحاسب الآلي و شبكة الانترنت، و من ثم تطور الجريمة المعلوماتية بذات السرعة على نحو يؤدي إلى إرباك المشرع و سلطات امن الدول، و يظهر الأثر السلبي في التعاون الدولي و هو ما حاولت الأمم المتحدة الاهتمام به و كذلك بعض البلدان الأوروبية.

1- عبد الفتاح بيومي حجازي- المرجع السابق- ص188.

- وكذلك: شريف محمد غنام- المرجع السابق-ص 194.

ثالثا: عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة المتعلقة بالجريمة المعلوماتية بين الدول المختلفة خاصة فيما يتعلق بالتحقيق و الحصول على الأدلة لا سيما و أن الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة عن طريق الضبط أو التفتيش في نظام معلوماتي معين أمر في غاية الصعوبة فضلا عن صعوبة الحصول على الدليل ذاته.

رابعا: إشكالية الاختصاص في الجرائم الالكترونية كونها تعد من المشكلات التي تعرقل الحصول على الدليل فيها خاصة و أنها من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي و الدول بسبب التداخل و الترابط بين شبكات المعلومات لأن الجريمة قد تقع في مكان معين و تنتج آثارها في مكان آخر.

و ما يلاحظ أن جل التشريعات الجنائية المطبقة حاليا في معظم دول العالم ترتكز على الصفة الإقليمية فيما يتعلق بتطبيق قواعد الإجراءات الجنائية عن طريق السلطات غير الوطنية لذلك لا مناص من الاتفاقيات الثنائية و الجماعية بين الدول لتسهيل تحقيق جرائم المعلوماتية و رغم إبرام بعض الاتفاقيات إلا أنها لم تف بالغرض في حل مشكلات الاختصاص و تبادل الأدلة الجنائية و تسليم المجرمين. لذلك تبق الحاجة جد ماسة إلى تشريعات جنائية أكثر مرونة حتى تواكب سرعة التقدم التكنولوجي و عصر المعلوماتية[21][21].

إن إجراءات التحقيق في بيئة تكنولوجيا المعلومات وفقا لما جاء في توصية المجلس الأوروبي رقم(13/95) تقتضي التدخل السريع لمد الإجراءات إلى أنظمة كمبيوتر قد تكون موجودة خارج الدولة، و حتى لا يمثل هذا الأمر اعتداء على سيادة دولة معينة أو على أحكام القانون الدولي يجب وضع قاعدة قانونية صريحة تسمح بهذا الإجراء .

لذلك فان الحاجة ملحة لاتفاقيات دولية تنظم كيفية اتخاذ هذه الإجراءات كما يجب أن تتوافر إجراءات سريعة و مناسبة و نظم اتصال تسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة و هو ما يوجب تطوير اتفاقيات التعاون الدولي.

1- عبد الفتاح بيومي حجازي- المرجع السابق- ص 192.

خاتمة:

إن الجريمة الالكترونية باعتبارها من الجرائم المعلوماتية المعاصرة التي واكبت عصر التقدم التكنولوجي خصوصا بعد ظهور شبكة المعلومات الدولية " انترنت" بسبب التقدم العلمي الحاصل ساعد على انتشار و تنوع هذا السلوك الإجرامي و الذي أصبح يهدد الإنسان في مختلف المجالات لا سيما الاقتصادية و الاجتماعية و الثقافية، و الأخلاقية و حتى المعتقدات الدينية لذلك و أمام الانتشار الواسع لهذا النمط الإجرامي الجد متطور و الذي تستخدم فيه أحدث التقنيات التكنولوجية العالية و المتطورة و سرعة و حيلة و بداهة مرتكبيه و التي تجعلهم دائما يفلتون من العقاب في ظل غياب الدليل المادي للجريمة إضافة إلى غياب منظومة تشريعية وطنية تحدد الفعل، تجرمه، ثم تحدد العقوبة المناسبة لمرتكبه انعكس ذلك سلبا على المستوى الدولي، فعلى الرغم من وجود العديد من الاتفاقيات الدولية المتعلقة بالجريمة الالكترونية التي سبق التطرق إليها إلا أنها تبقى غير كافية في غياب تظافر للجهود الدولية و التي تسعى في مجملها إلى اتخاذ التدابير اللازمة للحد من هذه الجرائم بالنظر إلى الطبيعة الخاصة لها كونها من الجرائم الدولية العابرة للحدود لذلك يجب على جميع الدول أن تسعى إلى تعديل قوانينها الداخلية و جعلها تواكب التطور العلمي و التكنولوجي، و العمل على إبرام اتفاقيات دولية ثنائية و متعددة الأطراف لاحتواء الجريمة و التخفيف منها.

قائمة المراجع:

1- سامي علي حامد عياد- الجريمة المعلوماتية و إجرام الانترنت- دار الفكر الجامعي- الإسكندرية- 2007.

2- شريف محمد غنام- حماية العلامات التجارية عبر الانترنت في علاقتها بالعنوان الالكتروني- دار الجامعة الجديدة- 2007.

3- عبد الفتاح مراد- شرح جرائم الكمبيوتر و الانترنت-دون ذكر دار النشر أو السنة.

- عبد الفتاح مراد- قانون مكافحة غسل الأموال و لائحته التنفيذية و القوانين المكملة له.

4- عبد الفتاح بيومي حجازي- الإثبات الجنائي في جرائم الكمبيوتر و الانترنت- دار الكتب القانونية- 2007.

5- فتوح الشاذلي، عفيفي كامل عفيفي- جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون- دراسة مقارنة- منشورات الحلبي الحقوقية.
6- محمد الشناوي- إستراتيجية مكافحة جرائم النصب المستحدثة(الانترنت، بطاقات الائتمان، الدعاية التجارية الكاذبة)- الطبعة الأولى-دار البيان للطباع و النشر- القاهرة- 2006.
7- مصطفى محمد موسى- الجهاز الالكتروني لمكافحة الجريمة- دار الكتب القانونية- مصر.
8- منير محمد الجنبيهي و ممدوح محمد الجنبيهي- تزوير التوقيع الالكتروني- دار الفكر الجامعي-الاسكندرية- 2006.
9- محمد عد الله أبو بكر سلامة- موسوعة جرائم المعلوماتية "جرائم الكمبيوتر و الانترنت"- المكتب العربي الحديث- الإسكندرية.