التدابير الدولية لمواجهة الجرائم الالكترونية

(اتفاقية بودابست) نموذجاً

د/ رمضان عبد الله العموري – أستاذ القانون الدولي المساعد كلية القانون جامعة خليج السدرة –

ومدير إدارة الدراسات العليا والتدريب بجامعة خليج السدرة

Ramdan20102010@gmail.com

الملخص:

تعد الجرائم الالكترونية من الجرائم التي لا حدود جغرافية ولا دولية لها، أي عابرة للحدود وبالتإلى فإن مكافحة هذا النوع من الجرائم يتطلب تكاثف الجهود الدولية والوطنية، وذلك باتخاذ كافة التدابير والإجراءات الضرورية للحد منها ومن انتشارها ومعاقبة مرتكبيها، وباعتبار أن الانترنت لا تخضع لأي حدود ولا ضوابط من الدولة، حيث أخذت بالتوسع والانتشار، حتى أصبحت جرائم ذات تنظيم وأطلق عليها(الجرائم المنظمة)، الأمر الذي جعل المشرع الدولي يسعى إلى إطار قانونى، بحيث يكون فيه التعاون بين الدول أمر ضروري، ومن خلال الجهود خرجت باتفاقية (بودابست – 2001) للجرائم الالكترونية، ومن هذا المنطلق جاءت الدراسة للإجابة على التساؤلات الاتية:

*ماهي التدابير الدولية الساعية إلى مكافحة الجرائم الالكترونية ومدى نجاحها؟ وهل استطاعت اتفاقية (بودبست) وضع الأساس لذلك، وماهي المعوقات التي تعيق التعاون في مكافحة الجرائم الالكترونية؟

أهداف البحث: يهدف البحث إلى بيان خطورة الجرائم الالكترونية على المستو الدولي. وتوضيح جهود المجتمع الدولي في مكافحتها وبيان مدى نجاح اتفاقية بودابست في مكافحتها.

أهمية البحث: يمكن ان يسهم هذا البحث في توضيح التدابير والجهود الدولية في مكافحة الجرائم الالكترونية. وسيعتمد البحث على المنهج الوصفي والمنهج التحليلي.

وتوصل البحث إلى عدة نتائج أهمها: أن الجرائم الالكترونية ذات طابع دولي، ولاحدود لها مما يستدعى تعاون دولي لمواجهتها، وأن أغلب الدول لم تضع تشريعات مناسبة لمكافحتها وكان ذلك له دور كبير في إعاقة تطبيق الاتفاقيات الدولية وكذلك إشكالية القضاء المختص على المستوى الدولي، وذلك راجع إلى اختلاف التشريعات داخل الدول، وعملت اتفاقية بودابست إلى إيجاد إطار قانونى دولي للتعامل مع الجرائم الالكترونية وذلك بإلزام الدول الموقعة عليها بتعديل تشريعاتها، وتوصل البحث إلى توصيات أهمها وضع نظام معلوماتي دولي موحد لتفادى هذه الجرائم و ابرام اتفاقيات دولية يتم فيها توحيد وجهات النظر حول مسائلة الاختصاص القضائي وزيادة الوعى بالجرائم الالكترونية وطنياً ودولياً .

الكلمات المفتاحية: التدابير الدولية – الجرائم الالكترونية – اتفاقية بودابست

International actions against cybercrimes

(Budapest Convention as model)

Summary

Cybercrime is a sort of crime that has no geographical or international borders; it is therefore cross-border, and countering it necessitates concerted international and national efforts that include all required means and activities to halt it, limit its growth, and punish its offenders. Because Internet networks are not bound by geographical borders or state sovereignty, cybercrimes have grown on an international scale, and they have evolved into organized crimes, prompting international legislator to seek a legal framework in which governments must cooperate. The Budapest Convention on Cybercrime was established in 2001 as a result of these efforts. In this light, the study came to answer the following questions:

What international measures are in place to prevent cybercrime, and how effective are they? What are the roadblocks to cooperation in the fight against cybercrime?

Research objective: This study intends to demonstrate the gravity of cybercrime on a global scale, as well as the international community's efforts to combat it and the extent to which the Budapest Convention has been successful in countering it.

The value of research: This research can help to clarify the measures and worldwide efforts in the fight against cybercrime. The descriptive and analytical research approaches will be used in this study.

The study came to several conclusions, the most important of which are that cybercrime is an international problem with no borders, necessitating international cooperation to combat it; and that most countries have not enacted appropriate legislation to combat it, which has hampered the implementation of international agreements. Concerning the issue of judicial competence at the international level due to disparities in legislation between states, the Budapest Convention sought to establish an international legal framework for dealing with cybercrime by requiring signatory governments to adjust their laws.

The study came up with several recommendations, including the creation of a uniform international information system to prevent these crimes, concluding international agreements in which opinions on judicial competence are aligned, and raising national and international awareness of cybercrime.

Keywords: International measures – cybercrimes – Budapest Convention.

المقدمة

تعد الجرائم الالكترونية من الجرائم التي لا حدود جغرافية ولا دولية لها، أي عابرة للحدود وبالتالي فإن مكافحة هذا النوع من الجرائم يتطلب تكاثف الجهود الدولية والوطنية وذلك باتخاذ كافة التدابير والإجراءات الضرورية للحد منها ومن انتشارها ومعاقبة مرتكبيها.

وبما أن شبكات الانترنت لا تخضع لأي حدود أو ضوابط ويسبب ذلك اتساع رقعة توسعها على الصعيد الدولي، حتى أصبحت جرائم ذات تنظيم يوصف (بالجرائم المنظمة)، الأمر الذي جعل المشرع الدولي يسعى إلى إطار قانونى، بحيث يكون فيه التعاون بين الدول أمر ضروري، ومن خلال الجهود خرجت باتفاقية (بودابست 2001) للجرائم الالكترونية.

ومن هذا المنطلق جاءت الدراسة للإجابة على التساؤلات الاتية:

*ماهي التدابير الدولية الساعية إلى مكافحة الجرائم الالكترونية ومدى نجاحها؟

* هل استطاعت اتفاقية بودبست من وضع الأساس لذلك؟

*ماهي المعوقات التي تعيق التعاون في مكافحة الجرائم الالكترونية؟

أهداف البحث:

*بيان خطورة الجرائم الالكترونية على المستو الدولي.

*بيان جهود وتدابير المجتمع الدولي في مكافحة الجرائم الالكترونية لما لها من اثار سلبية.

*بيان مدى نجاح اتفاقية بودابست في مكافحة الجرائم الالكترونية وتوضيح إجراءاتها ومعالجها لها.

أهمية البحث:

الأهمية النظرية: يمكن أن يسهم هذا البحث في إثراء المحتوى العلمي فيما يتعلق بقضية مكافحة الجرائم الالكترونية على الصعيد الدولي والعوامل المرتبطة به.

الأهمية التطبيقية: يمكن أن يسهم هذا البحث في توضيح التدابير والجهود الدولية في مكافحة الجرائم الالكترونية.

وسيعتمد البحث: على المنهج الوصفي والمنهج التحليلي.

خطة البحث: اعتمد البحث على الخطة التالية:

المبحث الأول: ماهية الجرائم الالكترونية

المطلب الأول: تعريف الجرائم الالكترونية

المطلب الثاني: أنواع الجرائم الالكترونية

المبحث الثاني: التدابير الدولية لمواجهة الجرائم الالكترونية

المطلب الأول: الصعوبات التي تواجه التصدي للجرائم الالكترونية

المطلب الثاني: أهم الجهود الدولية الساعية لمواجهة الجرائم الالكترونية

المبحث الأول: ماهية الجرائم الإلكترونية

أدى التطور الزمني مع مرور الوقت إلى القيام بالعديد من الأفعال التي تعتبر أنماط للسلوك الإجرامي وتحديد هذه الأفعال قد شهدت تطوراً سريعاً، بحيث ظهرت جريمة الاستخدام غير المصرح به لخدمات الحاسوب، وجرائم غش الحاسوب وجرائم التلاعب بالمنافذ البنكية بواسطة البطاقات الممغنطة، وجرائم التوصل مع أنظمة الاتصال البعدي واختراق شبكات المعلومات، واستخدام تقنية الفيروس في جرائم التلاعب بالبرامج، والنظم وأنشطة قرصنة البرامج، وهذا أدى إلى انعكاسات سلبية خطيرة جراء سوء استخدام هذه التقنية المتطورة والانحراف عن الأغراض المتوخاة منها، فبدت تفشي طائفة من الظاهرة الإجرامية المستحدثة، ألا وهي الجرائم الإلكترونية ومن خلال هذا التطور السريع أدى إلى المُزاوجة بين تكنولوجيا الاتصالات وتكنولوجيا الحاسب الإلى[1]، والذي أدى إلى ميلاد علم جديد Telematipue(اتصال) عن بُعد Communication (المعلوماتية) عن بُعد والمقصود به موت المسافات.

المطلب الأول

تعريف الجرائم الإلكترونية

الجرائم الإلكترونية نظراً لاستخدامها وتطورها بشكل سريع وارتباطها بتكنولوجيا متطورة لم يضع لها الفقه تعريف موحد جامع، وذلك لغياب التعريف القانوني لها في أغلب التشريعات، وكذلك عدم وجود مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، وهذا ما بينته اتفاقية بودابست في المادة الاولى وعدة التصرفات الى تعد جرائم الكترونية.[2]

وقد بينت اتفاقية بودابست لسنة 2001 في المواد(2–9) انواع التصرفات التي تعبر جرائم الكترونية، وقد وضحت الاتفاقية في الباب الثاني من القسم الأول من الفصل الاول في المادة 2 شملت تعريفات لعدة مصطلحات اوردتها الاتفاقية ومنها النفاذ غير المشروع و الاعتراض غير المشروع و التدخل في البيانات و التدخل في النظام و اساءة استخدام الاجهزة، أما الفصل الثاني في المواد (7–8) فوضح التزوير المرتبط بالكمبيوتر والاحتيال المرتبط بالكمبيوتر[3].

---

[1] حسنين المحمودي بوادي، إرهاب الإنترنت الخطر القادم، الطبعة الأولى، دار الفكر العربي، الاسكندرية، 2006، ص49 وما بعدها.
- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص7.

[2] المادة 1 من اتفاقية بودابست لسنة 2001

[3] المواد 7 – 8 من اتفاقية بودابست لسنة 2001

لم يكن هناك إجماع على تعريف الجرائم الإلكترونية وذلك لعدم معرفة ما هي الجرائم التي تتضمنها الجريمة الإلكترونية، وكما يقول "فان دير هلست وونيف" هناك غياب لتعريف عام وإطار نظري منسق في هذا الحقل من الجريمة.

وكلمة الجرائم هي جمع لكلمة جريمة ومشتقة في اللغة من الجرم أي التعذيب أو الذنب، فتعريف الجريمة عموماً هي فعل غير مشروع صادر عن إرادة جنائية يقرر له القانون عقوبة أو تدبير احترازي، فهي كل فعل ضار يأتيه المواطن ويكون هذا الفعل أثر ضار على غيره من المواطنين[4].

إلا أن الجرائم الإلكترونية هناك من عرفها على أنها تلك الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال[5].

وهناك من عرفها بأنها: سلوك غير مشروع معاقب عليه قانوناً صادراً عن إرادة جريمة محلها معطيات الكمبيوتر[6].

والبعض الأخر عرف الجرائم الإلكترونية بأنها ذات الطابع المادي التي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الإلكترونية ينتج منها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة، وغالباً ما يكون هدف هذه الجرائم هو القرصنة من أجل السرقة أو إتلاف المعلومات الموجودة في الأجهزة، ومن ثم ابتزاز الأشخاص باستخدام تلك المعلومات[7].

إلا أن هناك اتجاهات حول تعريف الجرائم الالكترونية وهما:

الاتجاه الضيق وعرف الجريمة الالكترونية على أنها: كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازماً من ناحية وملاحقته من ناحية وملاحقته من ناحية أخرى وكذلك عرفها بأنها هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط.

---

[4] سلام فارس تنوري، جرائم الحاسوب والإنترنت، دراسة تم تقديمها في الجامعة اللبنانية، قسم الدراسات العليا، قانون الأعمال المحلي والدولي.

[5] دياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، ملتقى علمي بالمملكة الأردنية الهاشمية، بتاريخ 2014/9/4، ص2.

[6] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الإلى ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية 2005، الطبعة الثانية، ص179.

[7] مجلة تكنولوجيا المعلومات، قسم نظم المعلومات، بدون دار نشر، وبدون سنة.

أما الاتجاه الموسع فيعرفها بأنها: كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو هي كل جريمة تقع في محيط أجهزة الكمبيوتر[8].

والعمل الإيجابي والامتناع عن الفعل يمثل السلوك، وهذا السلوك غير مشروع باعتبار أن المشروعية تنفي عن الفعل الصفة الجرمية، والعقاب عليها قانوناً، لأن اصباغ الصفة الإجرامية لا يتحقق من ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفاً للأخلاق.

وتعرف أيضاً بأنها: " ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الإلى ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعلها، كما يمكن تعريفها بأنها " الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الإلى بعمل غير قانوني[9].

وهناك من عرفها أيضاً بأنها: " كل محاولة لابتزاز، أو إيقاع، أو إجبار شخص ما على أن يقدم لك خدمة مقابل المفاوضة على صور، أو مقاطع صوتية، أو مرئية، أو حتى محادثات ومعلومات شخصية".

والهدف من هذه الجرائم الحصول على أهداف مادية يسعى من خلالها الجاني لتحقيق الربح الكبير، أو على خدمات جنسية يقدمها الضحايا مقابل المحافظة على عدم نشر صورهم ومعلوماتهم.

ومع ذلك فإن مصطلح الإلكترونية يستخدم لوصف فكرة أن الجريمة تتم من خلال التقنية الحديثة، والجريمة هي تلك الأفعال المخالفة للقانون.

والجريمة الإلكترونية يعرفها البعض الأخر بأنها تلك المخالفات التي ترتكب ضد الأفراد أو مجموعة من الأفراد، أو بعض ممثلي مؤسسات الدولة بدافع الجريمة، أو القيام بالتهديد بكشف معلومات معينة عن شخص أو فعل شيء، لتدمير الشخص المهدد بالامتثال لطلبات المبتز وعادة ما تكون هذه المعلومات محرجة أو ذات طبيعة مدمره اجتماعياً، وذلك بقصد إيذاء سمعة الضحية أو أذى مادي أو معنوي سواء كان بشكل مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل: الإنترنت، وغرف الدردشة، والبريد الإلكتروني.

أما الموسوعة الحرة "ويكيبيديا" فقد عرفت الجريمة الإلكترونية بأنها عملية تهديد وترهيب للضحية بنشر صور أو مواد فيلميه، أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية أو استغلال الضحية للقيام بأعمال

[8] محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الاسكندرية، الطبعة الأولى، 2014، ص118.
[9] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي والاحكام الموضوعية للجرائم المتعلقة بالإنترنت، الطبعة الأولى، ص23.

غير مشروعة لصالح المبتزين كالإفصاح بمعلومات سرية خاصة بجهة العمل أو غيرها من الأعمال غير القانونية[10]، وهذا ما اشارت إليه اتفاقية بودابست في المادة (6) فيما يتعلق بإساءة استخدام الاجهزة والمواد (7-8) المتعلقة بالجرائم ذات الصلة بالكمبيوتر[11].

المطلب الثاني

أنواع الجرائم الإلكترونية

أجريت العديد من الدراسات حول كيفية تحديد معايير معينة لوضع الجرائم الالكترونية في وضع معين بحيث يمكن أن تحدد لها أنواع، ولكن مع التطور المستمر وإقبال العالم واعتماده على التكنولوجيا وخاصة في مجال الشبكة والخدمات والأجهزة الالكترونية، أصبح المجرم الالكتروني له من الكفاية والاحتراف في القدرات والمهارات الالكترونية ما يؤهله لأن يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية، وغيرها من الجرائم مقابل المال.

وهذا الإجرام الذي يقوم به الشخص المنفذ لديه القدرة أيضاً على التعديل والتطوير في الأنظمة الأمنية، وذلك حتى لا تستطيع هذه الأنظمة تتبع وملاحقة هذه الأعمال الإجرامية من خلال الاتصالات أو الشبكات أو حتى الأجهزة الالكترونية.

ومع هذا التطور الحاصل في العالم اليوم وخاصة في هذا المجال ونتيجة لذلك بدأ نهوض العديد من الجرائم الالكترونية الجديدة والتي ما كانت لتبصر النور لولا ظهور الكمبيوتر، حيث شهد العالم اليوم أنواعاً لجرائم الكمبيوتر وترافق ذلك مع ظهور الانترنت، وبدأت أنشطة الهاكر باختراق مواقع المعلومات ونظمه عبر الانترنت والدخول دون تصريح أو تخويل إلى النظم والعبث بالبيانات والمعلومات المخزنة فيه أو تدميرها.

ونشير إلى أن الجرائم الالكترونية فيها خطورة كبيرة على جميع دول العالم اليوم، ومع تزايد هذه الجرائم وتعددها وانتشارها تتزايد أحجام هذه الأضرار الناشئة عنها وأخطار الاعتداءات على البيانات الشخصية للدول، والمنظمات، فترتب على ذلك إنشاء العديد من المؤتمرات وإبرام اتفاقيات متعددة دولية في محاولة لترسيخ مبدأ العمل مع الدول الأخرى وذلك لمواجهة الجرائم الالكترونية.

---

[10] عبدالرحمن عبدالعزيز الشنيفي، حرب المعلومات، الحرب القادمة "الدليل الشامل لحرب المعلومات"، مكتبة الملك فهد، الرياض، ص103.

[11] المواد (6-7-8) من اتفاقية بودابست لسنة 2001

إلا أن هذه الجرائم تتعدد وتتنوع وتتزايد كل يوم، باختلاف مرتكبيها والذين يختلفون عن المجرمين التقليدين لأنهم في الغالب أشخاص ذو كفاءة عالية من الدراية والعلم والمعرفة، وهذا الوضع يجعلنا بطبيعة الحال نخرج عن الإطار التقليدي للنظرة إلى المجرم العادي[12].

حيث ضمت أيضاً جرائم الكمبيوتر أنشطة التجسس الصناعي والأمني والاستلاء على البيانات ذات القيمة الاقتصادية أو الاستيلاء على أرقام بطاقات الائتمان واستخدامها بشكل غير مشروع للاستحواذ على الاموال، وكذلك تشويه سمعة الأفراد وتحقيرهم عبر الرسائل الالكترونية، وكذلك تعطيل أنظمة البرمجيات الخبيثة أو التدمير المادي لها أو استغلالها دون تصريح أو الهجوم عبر الانترنت على مواقع المعلوماتية لتعطيل عملها[13].

وتختلف أعمار وأهداف منفذي الجريمة الالكترونية مع اختلاف دوافعهم، فهناك من منفذي الهجمة الأطفال والمراهقين الذين تكون في الغالب دوافعهم لمجرد التسلية، غير مدركين حجم الأضرار التي يقومون بها وهناك المحترفين والمختصين والإرهابيين، الذين من الممكن أن تحكم أعمالهم شركات ضخمة وتضر بدول كبيرة.[14]

أم عن أنواع الجرائم الالكترونية فهناك جرائم ضد الأفراد ويطلق عليها مسمى جرائم الانترنت الشخصية والتي تقتضي على الحصول بطريقة غير شرعية على هوية الأفراد الالكترونية، أو سرقة الاشتراك في موقع الانترنت كالبريد الالكتروني، وكلمة السر الخاصة بهم، وكما تمتد لتصل إلى انتحال الشخصية الالكترونية وسحب الصور والملفات المهمة من جهاز الصفحة لتهديده بها وإخضاعه للأوامر.

أما النوع الأخر وهو يتعلق بالجرائم ضد الملكية ويختص في ذلك الجهات الحكومية والخاصة والشخصية ويركز على تدمير الملفات الهامة، أو البرامج ذات الملكية الخاصة ويكون ذلك عبر برامج ضارة يتم نقلها إلى جهاز المستخدم بعدة طرق.

النوع الثالث وهو فيما يتعلق بالجرائم التي تستهدف الحكومات وهي هجمات قوية يشنها مرتكب الجريمة وتكون على المواقع الرسمية، وأنظمة الشبكات الحكومية، ويكون هذا النوع من أخطر أنواع الجرائم الإلكترونية، سواء كان على المستوى المحلي، أو الدولي كالهجمات على النظام الشبكي للإنترنت سواء كان بتعطيله أو تدميره بشكل

---

[12] وليد العكوم، مفهوم ظاهرة الإجرام المعلوماتي، القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الأول 2004، الطبعة الثالثة.

[13] يونس عراب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، الطبعة الأولى، 2002م، ص306.

[14] مجلة تكنولوجيا المعلومات- مرجع سابق- ص121.

كلي، حيث يركز على الخدمات والبنية التحتية ومهاجمة جميع الشبكات المعلقة بالأجهزة الإلكترونية، الغاية والغرض من ذلك هو تحقيق هدف وغالباً ما يكون الهدف سياسياً[15].

ومع هذا كله نجد بأن أنواع الجرائم الإرهابية عديدة ومن خلال التعدد لم يستطع المختصين بوضع معايير محددة من أجل تصنيفها، وهذا يرجع إلى التطور الإلكتروني، وذلك حسب شخصية المجني عليه باعتباره الضحية في الجريمة فقد يكون المجني عليه شخصية اعتبارية في الدولة، والمتمثلة في الحكومات والشركات والمؤسسات ذات الشخصية الاعتبارية، وتتم عن طريق الحصول على معلومات سرية لها خصوصية خاصة بالضحية كمؤسسة أو وزارة حكومية، والتهديد بالإعلان عنها ونشرها للأخرين أو تتم من خلال اختراق الموقع الإلكتروني للمؤسسة عن طريق قراصنة غالباً ما يكون هدفهم من الاختراق هو أهداف سياسية.

ومن هنا يكون الابتزاز في هذه الحالة لا يكون إلا في حالات التأزم واستغلال الفوضى في البلاد وانعدام الخيارات، ولهذا فكل من لديه أجندات ومصالح ومنافع لا يمكن تحقيقها في ظل الأحوال الهادئة والمستقرة، ينتهز فرصة خروج الظروف عن المجرى العادي للأمور فيدفع بمصالحه وأجنداته ومنافعه إلى بؤرة الحدث الذي يجري في ظل ظروف غير عادية تعصف بالواقع، كي يتم حشرها في واقع متأزم ليتم إغراقه إن لم يستطع استيعابها، وتوصف هذه الحالة من حالات الابتزاز السياسي.

ومع ذلك قد يكون المجني عليه فرداً أو مجموعة أفراد وفي الغالب تكون (أنثى)، ويعد ابتزاز النساء أكثر أنواع الابتزاز الإلكتروني شهرة وانتشاراً حيث يقوم المبتز بالضغط على الضحية وتهديده بنشر معلومات شخصية أو صورة أو تسجيل مرئي، أو محادثات على مواقع الدردشة أو أية مادة، عن واقعة أو وقائع يكون من شأنها تشويه سمعته وتدميره اجتماعياً.

إلا أنه يتم الحصول على تلك المعلومات إما مباشرة من الضحية أو بطريقة غير مباشرة من خلال الدخول غير المشروع للحسابات الإلكترونية (التهكير).

والوصول لتلك المعلومات من خلالها، وتهديدهم بها لإجبارهم على القيام بأعمال غير أخلاقية ولغايات دنيئة.

بعد دراسة 1400 حالة ما بين السنوات 1980 و1984م قالت منظمة خيرية معنية بشؤون الطفل أن جرائم الجنس ضد الأطفال تزايدت 15 مرة وأن الانترنت المتاح على الهواتف المحمولة التي تتمتع بإمكانيات تصوير

[15] مجلة تكنولوجيا المعلومات، مرجع سابق، ص4.

الفيديو قد يزيد الأمر سوءً، إن شبكة الإنترنت مسؤولة إلى حد كبير عن الارتفاع الهائل في جرائم الإباحية ضد الأطفال، وهذا ما نصت عليه اتفاقية بودابست في المادة (9)[16].

وشهد عام 2002م 549 جريمة جنسية ضد الأطفال مقابل 35 جريمة عام 1988م، ويستغل مرتكبو جرائم الجنس صعوبة تحديد هوياتهم على الإنترنت، لافتراس الأطفال لكن الشرطة تمكنت من تعقب بعضهم وأجهزة الكمبيوتر الشخصية بهم.[17]

ومن هنا أصبحت هذه الجريمة ظاهرة خطرة دقت ناقوس الرهبة والرعب في المجتمع الليبي، كون أن هذا الفعل قد استهدف النسيج الاجتماعي العائلي الآمن، مما دفع وزير العدل بالحكومة المؤقتة إلى إصدار القرار رقم 26 لسنة 2016م بإنشاء "إدارة أبحاث ودراسات مكافحة الجرائم الإلكترونية" تبعيتها لإدارة الخبرة القضائية.

كما يوجد بجهاز المباحث العامة بوزارة الداخلية لحكومة الوفاق "إدارة مكافحة جرائم تقنية المعلومات" إلا أن جهود هذه الإدارة تقتصر على جرائم تزوير الوثائق والبيانات الشخصية دون إجراءات واضحة اتجاه جريمة الابتزاز الإلكتروني.

وقد تضاربت الآراء لتحديد أنواع جرائم الإنترنت وتعددت التصنيفات، فهناك من عددها بحسب موضوع الجريمة، وأخر قسمها بحسب طريقة ارتكابها[18].

1) جريمة إلكترونية تستهدف الأفراد ويطلق عليها أيضاً مسمى جرائم الإنترنت الشخصية والتي تقتضي على الحصول بطريقة غير شرعية على هوية الأفراد الإلكترونية، كالبريد الإلكتروني وكلمة السر الخاصة بهم، وكما تمتد لتصل إلى انتحال الشخصية الإلكترونية وسحب الصور والملفات المهمة من جهاز الضحية لتهديده بها وإخضاعه للأوامر، كما تُعتبر سرقة الاشتراك أيضاً من الجرائم ضد الأفراد[19].

2) جريمة إلكترونية تستهدف الملكية يستهدف هذا النوع من الجريمة الجهات الحكومية والخاصة والشخصية ويركّز على تدمير الملفات الهامة أو البرامج ذات الملكية الخاصة ويكون ذلك عبر برامج ضارة يتم نقلها إلى جهاز المستخدم بعدة طرق من أبرزها الرسائل الإلكترونية.

---

(16) المادة 9 من اتفاقية بودابست لسنة 2001

(17) تقرير لمنظمة ناشيونال تشايلدز هوم، تحمل حاليا اسم ان سي اتش NCH.

(18) أحمد حسام تمام، الجرائم الناشئة عن استخدام الحاسب الإلى، رسالة دكتوراه، جامعة طنطا، 2000، ص457.

(19) اسراء جبريل رشاد مرعي، الجرائم الإلكترونية، الأهداف، الأسباب، وطرق الجريمة ومعالجتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير، 2018، ص443-444.

3) جريمة إلكترونية تستهدف الحكومات وهي هجمات يشنها القراصنة على المواقع الرسمية الحكومية وأنظمة شبكاتها والتي تركز جل اهتمامها على القضاء على البنية التحتية للموقع أو النظام الشبكي وتدميره بالكامل، ومثل هذه الهجمات في الغالب يكون الهدف منها سياسياً.

4) النصب والاحتيال.

5) الجرائم السياسية الإلكترونية والتي تركز على استهداف المواقع العسكرية لبعض الدول؛ لسرقة المعلومات التي تتعلق بأمن الدولة.

6) سرقة المعلومات الموثقة إلكترونياً ونشرها بطرق غير شرعية.

7) جرائم الشب والسب والقدح.

8) جرائم التشهير ويكون هدفها الإساءة لسمعة الأفراد.

9) جرائم الاعتداء على الأموال أو الابتزاز الإلكتروني.

10) الوصول إلى مواقع محجوبة.

11) الإرهاب الإلكتروني.

12) الجرائم الجنسية الإلكترونية.

13) جرائم الاعتداء على الأموال (مؤسسات مصرفية ومالية وبنوك).

وهذا ما اشارت إليه اتفاقية بودابست في المواد (2–6) من الباب الثاني والفصل الثاني المواد (7–8) وتحدثت المادة9 من الاتفاقية عن الجرائم ذات الصلة بمواد الاباحية عن الاطفال، اما المادة 10 تحدثت فيها عن الجرائم المتعلقة بانتهاك حقوق النشر والتالف والحقوق ذات الصلة[20]

ولهذه الجرائم الإلكترونية خصائص تتسم بسهولة الوقوع في فخها، حيث إن غياب الرقابة الأمنية تساهم في انتشارها، والضرر الناجم عن الجرائم الإلكترونية غير قابل للقياس إذ أنها تلحق إضراراً جسيمة، وصعوبة الكشف عن مرتكب الجريمة إلا بأساليب أمنية وتقنية عالية، وذات سلوك خارج غير أخلاقي مجتمعياً، وجريمة غير مقيدة بزمان ومكان.

[20] المواد (2-3-4-5-6-9-10) من اتفاقية بودابست لسنة 2001

قد حدد الخبراء الجرائم التي ترتكب عبر الإنترنت تكون أفعالها وخصائصها منفردة، لا تتوفر في أي من أفعال الجرائم التقليدية إلا في أسلوبها، وطريقة ارتكابها والتي ترتكب يومياً في كافة دول العالم، ومن خصائص تلك الجرائم هي:

1) الحاسب الإلى كأداة لجرائم الإنترنت: أي أن يكون الحاسب الإلى هو الأداء لارتكاب تلك الجرائم لأنه هو وسيلة الدخول إلى نظم المعلومات عبر الإنترنت بطريقة غير مصرح بها لتنفيذ الجريمة أياً كان نوعها.

2) الجريمة الإلكترونية عابرة للحدود: شيوع الإنترنت قد ألغى الحدود الجغرافية بين دول العالم ويمكن للشخص أن يتحدث إلى شخص أخر أو أشخاص، عن طريق الدردشة والجرائم التي ترتكب عبر الإنترنت في نفس الدولة يمكن للجريمة أن تتخطى حدود تلك الدولة وأثارها تصل إلى كافة الدول الأخرى.

3) صعوبة اكتشاف الجرائم: الجرائم لا تترك أثراً خارجياً مرئياً وصعوبة إثباتها، فيمكن تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات مدة تقل عن الثانية، كما يتقمص الجاني اسماً مستعاراً أو يرتكب فعله من خلال إحدى مقاهي الإنترنت.

4) الخسائر المادية: تعتبر الخسائر المادية الناجمة عن جرائم الإنترنت كبيرة إذا ما قيست بالخسائر والأضرار الناشئة من الجرائم التقليدية[21].

المبحث الثاني

التدابير الدولية لمواجهة الجرائم الالكترونية

تنوعت وتعددت الجهود الدولية في مواجهة الجرائم الالكترونية حيث اتخذت العديد من التدابير للحد منها، غير أن هذه الجهود تبقى غير كافية نظراً للتقدم التكنولوجي الذي يشهده العالم في مجال استخدام الكمبيوتر والانترنت في كافة المجالات الاقتصادية والامنية والذي زاد من انتهاك خصوصية المعلومات والقصد منها التجسس والسرقة، مما دعا بعض الدول إلى المناداة بإنشاء وحدات خاصة بمكافحة الجرائم الالكترونية على المستويين الوطني والدولي، والقصد منه إيجاد صيغة ملائمة للتعاون الدولي لمكافحة جرائم الاعتداء على المعلومات.

[21] المواد (7- 8) من اتفاقية بودابست لسنة 2001

المطلب الاول

الصعوبات التي تواجه التصدي للجرائم الالكترونية

إن غالبية الدول في العالم اليوم تنظم الانترنت بما يتماشى مع قيمها الاخلاقية والسياسية والقانونية، وبما أن التطور التكنولوجي في مجال الاتصالات يكون على مستوى دولي، ويكون خارج سيطرة الدول، ولذلك فإن وضع تشريعات فعالة ووضعها لمكافحة الجرائم الالكترونية تحدى كبير للدول[22] .

حيث تعتبر الجرائم الالكترونية تحدى كبير للأجهزة الامنية في كافة الدول؛ وذلك لأن التشريعات فيها تأخذ وقت أطول والذي بدوره يعرقل مكافحة الجرائم الالكترونية بسرعة.

وبهذا نجد أن المحاكم الجنائية الوطنية تواجه صعوبات وهي الوقت الضائع بين اكتشاف الانتهاكات للتقنيات الحديثة وبين التعديلات للقوانين الجنائية الخاصة بمكافحتها؛ حيث أن التعديلات تأخذ وقت طويل ولاتتسم بالسرعة [23].

وهذا ما وضحته المادة 13 من اتفاقية بودابست وبيت العقوبات والتدابير في الفقرة (1-2)[24]

وكذلك انتشار الانترنت خارج حدود الدول يضع صعوبات قانونية تتعلق بسيادة الدولة ومدى صلاحية محاكمها، التي يكون نطاقها على أرض الدولة ولايمتد إلى خارجها، وكل ذلك يتطلب تنسيق وتعاون بين الدول فيما يتعلق بالقوانين الداخلية والمعاهدات الدولية والتعاون يكون بين كل الدول أي يكون هناك تعاون وفق اليات معينة مع الدولة، التي يجب أن تقام الإجراءات القضائية فوق إقليمها، ولكي يحدث ذلك لا بد من وجود التعاون الدولي تشريعاً وقضاءً وتنفيذاً [25].

وكون التعاون الفعال له أهمية كبيرة في مجال مكافحة الجرائم الالكترونية، وذلك بعد أن أصبحت هذه الجرائم تتجاوز وتتعدى حدود الدول، الا أن الملاحظ قصور وضعف هذا التعاون مقارنة بتطور هذا النوع من الجرائم[26].

فالتعاون يصبح صعب بسبب الاختلاف في التشريعات بين الدول، وكذلك العدد المحدود للمعاهدات [27] ،والاتفاقيات المتاحة للدول بشأن التعاون الدولي [28].

---

[22] جورج ليكي، مجلة الدفاع الوطني، المعاهدات الدولية للأنترنت حقائق وتحديات، العدد83 ، 2013، ص 102
[23] تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الامم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، المنعقد في بانكوك، 2005
[24] المادة 13 الفقرة (1-2) من اتفاقية بودابست لسنة 2001
[25] جميل عبدالباقى الصغير، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار المنهضة العربية، القاهرة،1998، ص75
[26] محمد منصور الضاوي، أحكام القانون الدولي في مكافحة الجرائم الدولية، دار المطبوعات الجامعية، بلا تاريخ، الاسكندرية، مصر، ص648

فمع وجود هذه الجرائم توجد العديد من الصعوبات الخاصة بتحديد القانون واجب التطبيق والقضاء المختص بنظر تلك الجرائم ومنها:

• عدم وضوح المفاهيم القانونية للنشاط الإجرامي، ويرجع ذلك إلى عدم الاتفاق على مفهوم موحد للجريمة الالكترونية، لأن الاختلاف في تعريف الفعل المجرم يعد سبب في فشل التعاون الدولي في مكافحة الجرائم الإلكترونية.

• ازدواجية التجريم حيث أن اختلاف النظم القانونية والتشريعات لها دور كبير وبارز في وضع العقبات والعراقيل أمام تحقيق التعاون الدولي في مجال مكافحة الجرائم الالكترونية [29].

ونرى أن أغلب الدول لم تضع تشريعات مناسبة لمكافحة الجرائم الالكترونية وهذا له دور كبير في إعاقة تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين مثلاً [30]، وهذا ما وضحته اتفاقية بودابست في المادة 13.

• عدم وجود مساعدات قضائية وتعتبر من أهم صور التعاون الدولي في مكافحة الجرائم الالكترونية ونعنى به طلب المساعدة القضائية الدولية [31] ، ومنها الإنابة القضائية والتي تعتبر من أهم صور التعاون الدولي، غير أنها عادة ما تتم بين الدول بالطرق الدبلوماسية مما يجعلها تتسم بعدم السرعة في الإجراءات وتؤدى لتعقيدها.

• عدم وجود تبادل للمعلومات ويعتبر من صور التعاون الدولي مع جهات أجنبية وهي بصدد النظر في جريمة وجمع الأدلة [32] .

• إشكالية القضاء المختص بنظر الجرائم الالكترونية حيث تعتبر من أصعب الجرائم التي تثير مسالة الاختصاص، فعلي المستوى الوطني لا توجد إشكاليات في مسألة الاختصاص حتى يتم العودة إلى المعايير المنظمة لذلك، وهي مكان القبض ومكان وقوع الجريمة ومكان إقامة المتهم [33] ، وهذا ما بينته اتفاقية بودابست في المادة 22 بفقراتها[34].

---

[27] علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، ايتراك للنشر والتوزيع، القاهرة،2000، ص175
[28] براء منذر عبد اللطيف، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الاول، تحولات القانون العام فى مطلع الالفية الثالثة، كلية القانون، جامعة تكريت، العراق،2009، ص11
[29] براء منذر عبداللطيف، المرجع السابق، ص12
[30] لبنا محمد الأسدي، مدى فاعلية القانون الجنائي في مكافحة الجرائم المعلوماتية، دراسة مقارنة، الطبعة الاولى، الاردن، 2015، ص256
[31] تعرف المساعدة القضائية الدولية بانها ((كل اجراء قضائي تقوم به دولة من شانه تسهيل مهمة المحاكمة في دولة اخرى بصدد جريمة من الجرائم))
[32] حسين بن سعيد الغافرى، الجهود الدولية في مواجهة جرائم الانترنت،2007، ص12
[33] شيحة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبرانى، مجلة جامعة الشارقة، مجلد17، العدد1 ، سنة2020، ص748
[34] المادة 22 من اتفاقية بودابست لسنة 2001

ولكن الإشكالية تكون على المستوى الدولي، وذلك راجع إلى اختلاف التشريعات والأنظمة القانونية التي يخرج عنها تنازع في مسالة الاختصاص بين الدول، فيما يتعلق بالجرائم الالكترونية، وذلك لكونها جرائم عابرة للحدود سواء تم الاستناد إلى مبدأ العينية أو مبدأ الاقليمية [35].

• ضعف التعاون في مجال التدريب حيث أن بعض المتدربين نظرتهم سطحية في مجال التدريب وهي أنها مجرد دورات لا فائدة منها، وهذا ما يهدد التعاون في هذا المجال، كذلك البيئة التدريبية وعدم قدرتها على تجسيد الواقع لبيئة العمل الطبيعية بشكل متقن، بحث ما يدور بها من وقائع وإجراءات بحيث لا تتوافق مع طبيعة المهام التي سيقوم بها المتدربون في البيئة الطبيعية.

المبحث الثاني

أهم الجهود الدولية الساعية لمواجهة الجرائم الالكترونية

نظراً للتطور الكبير في تقنية المعلومات واهتمام الأنظمة الدولية بالجرائم الالكترونية، تم توقيع العديد من الاتفاقيات والمواثيق الدولية من جانب الدول التي أدركت مدى خطورة الجرائم الالكترونية وخصوصاً بوصفها من الجرائم العابرة للحدود.

• دور الأمم المتحدة في مكافحة الجرائم الالكترونية:

قامت الامم المتحدة بدور كبير وبارز في الحفاظ على الأمن والاستقرار والسلم، وتحقيق التعاون الأمني من خلال التصدي للجرائم ذات الطابع الدولي، ومن بينها الجرائم الالكترونية وذلك بالمصادقة على العديد من الاتفاقيات الدولية [36] .

والعمل من خلال اللجان المتخصصة ومن بينها اللجنة الاستشارية لخبراء منع الجريمة ومعاملة المجرمين الذى أنيط لها مهمة مكافحة الجريمة، وتقديم الاستشارات للأمين العام، ووضع البرامج ورسم السياسات والتدابير الدولية في مكافحة الجريمة، وعقد مؤتمرات دورية كل خمس سنوات وذلك لتعزيز التبادل والخبرات، والمتخصصين من

[35] قد ترتكب جريمة في اقليم دولة من طرف أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الاولى استنادا إلى مبدأ الاقليمية، وتخضع الدولة الثانية على اساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون الجريمة تهدد أمن وسلامة دولة اخرى فيدخل الاختصاص استنادا إلى مبدا العينية - جميل عبد الباقي الصغير، مرجع سابق، ص748

[36] ايهاب خليفه، موقف ميثاق الامم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية، مركز المستقبل للأبحاث والدراسات المتقدمة، نشر 2009، الموقع الإلكتروني www.futureuae.com ، تاريخ الزيارة2022/5/6م.
- مراد مشوش، الجهود الدولية لمكافحة الاجرام السيبرانى، مجلة الواحات للبحوث والدراسات، جامعة غرداية، الجزائر،2020، ص6

كافة الدول؛ من أجل زيادة التعاون الدولي والإقليمي في مكافحة الجريمة، ويعتبر مؤتمر الأمم المتحدة السابع لمنع الجريمة المنعقد في ميلانو سنة 1985م قد خرج بمجموعة من المبادئ والتي توجت بالتوقيع عليها في (هافانا سنة1990م)[37] .

حيث نص المؤتمر على تطبيق التطورات الجديدة في مجال التكنولوجيا، ولمنع الجريمة فإنه يجب اتخاذ تدابير وإجراءات ملائمة، ضد الإساءات والاستعمال المسيء لهذه التكنولوجيا، وكذلك تشجيع التشريعات الحديثة التي تجرم الجرائم الالكترونية حيث تعتبر نوع من أنواع الجرائم المنظمة.

وكذلك عقد الأمم المتحدة مؤتمرها التاسع لمنع الجريمة ومعاملة المجرمين في القاهرة سنة 1995م ومن أهم ما توصل إليه العمل من أجل حماية الملكية الفكرية من مواجهة مخاطر التكنولوجيا، وتعزيز التعاون من أعضاء المجتمع الدولي للحد من الجرائم المتعلقة بالكمبيوتر.

ونظرا لكثرة الجرائم الالكترونية وما تسببه من إشكاليات قامت الأمم المتحدة بعقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية سنة2000م، حيث أكدت على الحاجة على تعزيز وزيادة التعاون بين الدول في مكافحة الجرائم الالكترونية [38] ، وهذا وما تناولته اتفاقية بودابست في المواد 23-24-25 منها[39]

وعقد الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية في البرازيل سنة2010م، حيث نوقش فيه أخر التطورات في استخدام التكنولوجيا من طرف المجرمين.

وهكذا تكون منظمة الأمم المتحدة الإطار الأمثل لمواجهة الجريمة المعلوماتية، حيث وضعت مجموعة من القواعد الموضوعية والإجرائية لمواجهة هذه الجرائم.

وقد نصت القواعد الموضوعية على الأفعال التي تعتبر إجرام الكرتوني وتحدث دورياً ومنها جرائم الاحتيال المتعلق بالكمبيوتر وجرائم التزوير الخاصة بالكمبيوتر، وجرائم التخريب، وجرائم الدخول والاعتراض غير المصرح به، أما القواعد الإجرائية فهي تتضمن بعض القواعد الواجب مراعاتها ومنها تحديد السلطات التي تقوم بالتفتيش والضبط.

---

[37] محمد الامين ومحسن عبد الحميد، معايير الامم المتحدة في مجال العدالة الجنائية ومنع الجريمة، أكاديمية نايف العربية للعلوم الامنية، الرياض، السعودية، الطبعة الاولى،1998، ص19

[38] مراد ماشوش، الجهود الدولية لمكافحة الاجرام السيبرانى، مجلة القانون والاعمال، جامعة الحسن الثاني، المغرب، على الموقع الإلكتروني www.droiteteotreprise.com تاريخ الزيارة2022/5/3

[39] المواد 23- 24- 25 من اتفاقية بودابست لسنة 2001

. اتفاقية بودابست لمواجهة الجرائم الالكترونية سنة 2001م:

إيماناً من الدول بمدى خطورة الجرائم الالكترونية، قد تم التوقيع على الاتفاقية في العاصمة المجرية بودابست وجاءت هذه الاتفاقية نتيجة الجهود التي يبذلها المجلس الأوروبي، من أجل الوصول إلى وضع إطار قانوني فعال لمكافحة الجرائم الالكترونية [40].

وتنبع أهمية هذه الاتفاقية من كونها تسعى إلى إيجاد إطار قانوني دولي، للتعامل مع الجرائم الالكترونية حيث تلتزم الدول الموقعة على الاتفاقية بتعديل تشريعاتها لمواجهة الجرائم الالكترونية [41].

وتعتبر الاتفاقية أوروبية المنشأ إلا أن المجال قد ترك مفتوحاً مفتوح للدول الأخرى لطلب الانضمام إليها لتصل الفائدة منها إلى جميع الدول [42].

حيث تناولت الاتفاقية أهم وأكثر الجرائم انتشاراً على المستوى الدولي، وحاولت الاتفاقية تحقيق التوازن بين مقترحات أجهزة الشرطة، وما قدمته المنظمات المدافعة عن حقوق الإنسان.

وتسعى كافة الدول الموقعة عليها إلى اتخاذ ما يلزم من تدابير تشريعية وغيرها من الإجراءات والتدابير لتجريم النفاذ غير المشروع إلى أنظمة الكمبيوتر، والتدخل في البيانات لإفسادها أو تعديلها أو حذفها [43] .

وقد بينت المادة 13 العقوبات والتدابير التشريعية، والجرائم المنصوص عليها في المواد من 2 – 11 المعاقب عليها بعقوبات فعالة متناسبة ورادعة، وكذلك مسائلة الأشخاص الاعتبارية وفقاً للمادة 12 [44].

---

[40] يعيش تمام شوقي، الجريمة المعلوماتية، دراسة تأصيلية مقارنة، سلسلة مطبوعات المخبر، جامعة محمد خيصر ، بسكرة، الجزائر، 2009، ص46

[41] هلالي عبداللاه أحمد، الجوانب الموضوعية والاجرائية للجرائم المعلوماتية، (على ضوء اتفاقية بودابست2001)، دار النهضة العربية، 2001، ص30

[42] عمر زكى عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات ورقة عمل مقدمة لمؤتمر الجوانب القانونية للتجارة الالكترونية، جامعة الدول العربية،2001، مشار إليها لدى شيحة حسين الزهراني، مرجع سابق، ص754

[43] المواد (2-3-4-5-6) من اتفاقية بودابست 2001م

[44] المادة 13 من العقوبات والتدابير من اتفاقية بودابست 2001م

الخاتمة:

النتائج:

1- عدم وجود جهاز موحد للدول للتصدي لمثل هذه الجرائم.

2- بعض المجتمعات لم تعرف ماهي الجريمة الإلكترونية، وذلك لارتباطها بالتجارة الدولية وهذا يساهم في العديد من الجرائم.

3- الجرائم الالكترونية هي جرائم ذات طابع دولي ولايوجد لها حدود وطنية مما يستدعى تعاون دولي لمواجهتها والحد منها.

4- أغلب الدول لم تضع تشريعات مناسبة لمكافحة الجرائم الالكترونية وهو بدوره له دور كبير في إعاقة تطبيق الاتفاقيات الدولية.

5- إشكالية القضاء المختص على المستوى الدولي وذلك راجع إلى اختلاف التشريعات داخل الدول وما ينتج عنها من تنازل الاختصاص بين الدول

6- عملت اتفاقية بودابست على إيجاد إطار قانونى دولي، للتعامل مع الجرائم الالكترونية وذلك بإلزام الدول الموقعة عليها بتعديل تشريعاتها لمواجهة الجرائم الالكترونية.

التوصيات:

1- وضع خطة نموذجية يكون من خلالها مراقبة جميع الشبكات الإلكترونية وذلك عن طريق أجهزة أمنية وهي ما يسمى بالأمن المعلوماتي.

2- على الدول النامية بأن تحدو حدو الدول المتقدمة في مجال مكافحة الجرائم المعلوماتية وذلك من خلال تجارب هذه الدول في هذا المجال.

3- تعاون الدول فيما بينها للتصدي لمثل هذه الجرائم، وذلك من خلال وضع نظام معلوماتي موحد لتفادي هذه الجرائم

4- السعي من أجل إبرام اتفاقيات دولية، يتم فيها توحيد وجهات النظر حول مسائلة تنازع الاختصاص القضائي الخاص بالجرائم الالكترونية.

5- زيادة الوعي وطنيا ودوليا بالجرائم الالكترونية وخطورتها

المصادر

أولا: الكتب:

1. جميل عبدالباقى الصغير، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار المنهضة العربية، القاهرة،1998
2. محمد منصور الضاوي، أحكام القانون الدولي في مكافحة الجرائم الدولية، دار المطبوعات الجامعية، بلا تاريخ، الاسكندرية، مصر
3. لبنا محمد الأسدي، مدى فاعلية القانون الجنائي في مكافحة الجرائم المعلوماتية، دراسة مقارنة، الطبعة الاولى، الاردن، 2015،
4. حسين بن سعيد الغافرى، الجهود الدولية في مواجهة جرائم الانترنت،2007،
5. محمد الامين ومحسن عبد الحميد، معايير الامم المتحدة في مجال العدالة الجنائية ومنع الجريمة، أكاديمية نايف العربية للعلوم الامنية، الرياض، السعودية، الطبعة الاولى،1998،
6. يعيش تمام شوقي، الجريمة المعلوماتية، دراسة تأصيلية مقارنة، سلسلة مطبوعات المخبر، جامعة محمد خيصر ، بسكرة، الجزائر، 2009،
7. هلإلى عبداللاه أحمد، الجوانب الموضوعية والاجرائية للجرائم المعلوماتية، (على ضوء اتفاقية بودابست2001)، دار النهضة العربية، 2001،
8. حسنين المحمودي بوادي، إرهاب الإنترنت الخطر القادم، الطبعة الأولى، دار الفكر العربي، الاسكندرية، 2006
9. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004
10. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الإلى ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية 2005، الطبعة الثانية،
11. محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الاسكندرية، الطبعة الأولى، 2014

12. جميل عبد الباقي الصغير، الانترنت والقانون الجنائي والاحكام الموضوعية للجرائم المتعلقة بالإنترنت، الطبعة الأولى 2

13. عبد الرحمن عبد العزيز الشنيفي، حرب المعلومات، الحرب القادمة "الدليل الشامل لحرب المعلومات"، مكتبة الملك فهد، الرياض

14. يونس عراب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، منشورات اتحاد المصارف العربية، الجزء الأول، الطبعة الأولى، 2002م

ثانياً: البحوث والمقالات:

1. شيحة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبرانى، مجلة جامعة الشارقة، مجلد17، العدد1 ، سنة2020،

2. مراد مشوش، الجهود الدولية لمكافحة الاجرام السيبرانى، مجلة الواحات للبحوث والدراسات، جامعة غرداية، الجزائر،2020

3. مراد ماشوش، الجهود الدولية لمكافحة الاجرام السيبرانى، مجلة القانون والاعمال، جامعة الحسن الثاني، المغرب،2020

4. مجلة تكنولوجيا المعلومات، قسم نظم المعلومات، بدون دار نشر، وبدون سنة.

5. اسراء جبريل رشاد مرعي، الجرائم الإلكترونية، الأهداف، الأسباب، وطرق الجريمة ومعالجتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير، 2018.

ثالثاً: الرسائل العلمية:

1- أحمد حسام تمام، الجرائم الناشئة عن استخدام الحاسب الإلى، رسالة دكتوراه، جامعة طنطا، 2000.

ثالثاً: الاتفاقيات والقرارات والتقارير الدولية:

1. تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الامم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، المنعقد في بانكوك، 2005

2. براء منذر عبد اللطيف، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الاول، تحولات القانون العام في مطلع الالفية الثالثة، كلية القانون، جامعة تكريت، العراق،2009

3. عمر زكى عبد المتعال، المعاهدة الدولية لمقاومة جرائم الحاسبات ورقة عمل مقدمة لمؤتمر الجوانب القانونية للتجارة الالكترونية، جامعة الدول العربية،2001

4. دياب موسى البداينة، الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، ملتقى علمي بالمملكة الأردنية الهاشمية، بتاريخ 2014/9/4،

5. تقرير لمنظمة ناشيونال تشايلدز هوم، تحمل حالياً اسم ان سي اتش NCH.

6. اتفاقية بودابست لسنة2001.