الإطار القانوني الدولي
لمكافحة الجرائم السيبرانية
International Legal Framework for Combating Cybercrimes

م.م. ورود استبرق هادي

Asst. Inst. Worood Astebraq Hadi

worood_istabraq@ijsu.edu.iq

كلية العلوم الإدارية والمالية/

جامعة الامام جعفر الصادق عليه السلام

College of Administrative and Financial Sciences/Imam Ja’afar Al-Sadiq University

الملخص

إن المخاطر الالكترونية أضحت واقعا مفزعا يهدد الدول والأفراد ويعود ذلك أساسا الى الإمكانيات المتاحة للمجرم المعلوماتي الذي يستطيع تعطيل موقع الكتروني، يهم الأمن الوطني أو يقرصن حساب أحد الشخصيات المعروفة، كما يمكنه اختراق البنوك والاستيلاء على أرصدة عملائها أو بيع معطياتهم البنكية السرية على صفحات الشبكة العنكبوتية، وتعد الجريمة الالكترونية من أهم جرائم العصر التي تحدث أضراراً فادحة في اقتصاد الدول تفوق الأضرار تلك تحدثها جرائم المعروفة او الشائعة، الأمر الذي لحق بسلطات الدول خسائر مادية ومعنوية مما دفعها الى الإسراع في إيجاد حلول تشريعية للحد من هذه الظاهرة التي تفاقمت، وبدأت الدول الواحدة تلو الأخرى بسن تشريعات تكافح بها هذه الجرائم، كون المجرمون يستخدمون تقنيات جديدة لغرض ارتكاب هجمات سيبرانية ضد الحكومات والشركات والأفراد، ولا تقف هذه الجرائم عند الحدود، سواء أكانت مادية أم افتراضية، وتسبب أضرارا خطيرة وتشكل تحديدات ملموسة للضحايا في جميع أنحاء العالم، ونظراً للتحول الكبير في شبكة الانترنت واندماج وسائلها الحديثة في جميع جوانب الحياة، فضلا عن ذلك الى زيادة دورها بشكل غير محدود.

الكلمات المفتاحية: الفضاء السيبراني، اتفاقيات دولية، الجرائم الالكترونية، انواع الجرائم السيبرانية، الجهود الوطنية.

Abstract

Electronic risks have become a terrifying reality that threatens countries and individuals. This is mainly due to the capabilities available to the cybercriminal who can disable a website that concerns national security or hack the account of a well-known person. He can also hack into banks and seize their customers' balances or sell their confidential banking data on the Internet. Cybercrime is one of the most important crimes of the era that causes severe damage to the economies of countries that exceeds the damage caused by known or common crimes. This has caused material and moral losses to the authorities of countries, which prompted them to quickly find legislative solutions to limit this phenomenon that has worsened. Countries have begun, one after the other, to enact legislation to combat these crimes, as criminals use new technologies to commit cyber attacks against governments, companies and individuals. These crimes do not stop at borders, whether physical or virtual, and cause serious damage and constitute tangible challenges for victims all over the world. This is due to the major transformation in the Internet and the integration of its modern means into all aspects of life, in addition to the unlimited increase in its role.

Keywords: Cyberspace, International Agreements, Electronic Crimes, Types of Cybercrimes, National Force.

المقدمة

هذا ولقد ان وسائل التواصل الاجتماعي وشبكة الانترنت انتشار في جميع انحاء العالم، وزيادة استعمالها والامتداد في التعامل معها، وفر كل شخص فرصة التبادل المعلومات والتواصل عبر الحدود، ومع توفر القدرة على نقل وتلقي المعلومات والتقنيات والوصول الى البيانات والبرامج بسهولة ويسر، وعلى الرغم من الآثار الإيجابية التي ظهرت في كل المجالات الحديثة، إلا أن جاءت مع ظهور العديد من التحديات، فقد بانت مخاطر يرتكبها جزء من مستعملو شبكة الانترنت، وقد تتسم بمخاطرها وسهولة القيام بها، ومعضلة تجاوزها للحدود الوطنية، ويمكن أن نطلق على هذه الجرائم اسم الجرائم السيبرانية التي تتوافق مع هذه التحديات.

أهمية البحث:

إن تظهر كونه يتناول التأثيرات السلبية للثورة الرقمية، والجرائم الالكترونية من جرائم مستحدثة التي تشكل تهديدا كبيرا للفرد والمجتمع وكذلك على الأجهزة الأمنية للدولة، مما يجب علينا أن نتطرق لدراستها لمكافحة هذه الجرائم من وضع الأنظمة والعقوبات الرادعة، والتصدي لهجمات فايروسات المجرمين ومحاكمتهم أمام القضاء.

اشكالية البحث:

تعد الجرائم او المخاطر الالكترونية من أخطر وأحدث الجرائم التي تعاني منها مختلف دول العالم، وهذا نتيجة الانتشار والاستخدام الواسع للتكنولوجيا الحديثة في مجال الاتصالات، لذلك سارعت الكثير من الدول الى إيجاد الحلول المناسبة للتصدي لها ومكافحتها، وعلى هذا الأساس يعد هذا الموضوع من المواضيع المتشعبة التي تحتاج الى دراسة معمقة.

وعليه تكمن الإشكالية التي نحن بصدد معالجتها في هذا الموضوع، في بيان مدى نجاح القوانين الداخلية والجهود الدولية المبذولة لمكافحة المخاطر الالكترونية؟ هذه الاشكالية الرئيسة تتفرع عنها اسئلة فرعية ابرزها:

- ❖ دور التعاون الدولية لمكافحة الجرائم الالكترونية.
- ❖ وما مدى حماية العالمية للأفراد من انواع الجرائم الالكترونية.
- ❖ وماهي اوجه الحماية الوطنية لمكافحة الجرائم السيبرانية.

منهج البحث:

فقد اتبعنا المنهج الوصفي كان لإعطاء وصف عام لمفهوم الجرائم الالكترونية، وبيان انواع جرائم الالكترونية، وكذلك بيان التعاون الدولية والوطنية لمكافحة جرائم الالكتروني.

هيكلية البحث:

ولأجل ذلك قسمنا بحثنا الى مبحثين تطرقنا في الأول منها الى لمفهوم جريمة الالكترونية وانواعها، أما المبحث الثاني فقد خصصناه لدور التعاون الدولي والوطني في مكافحة الجرائم الالكترونية.

«المبحث الأول»

مفهوم الجريمة الالكترونية وانواعها

إن الجريمة لغة هو التعدي أو الذنب والجريمة هي ظاهرة إنسانية أزلية تختلف في أشكالها وأنماطها عبر الزمن لكنها تتوحد في كونها تمثل عملاً غير مشروع يمثل عدواناً على مصلحة إنسانية جديرة بالحماية والاعتبار القانوني، وتعد ظاهرة الجرائم في البيئة الالكترونية رافقت نماء وتطور نظم الحاسب الآلي والشبكات وثورة تكنولوجيا الاتصالات والمعلوماتية، على الرغم من الفوائد في مجال التقدم التكنولوجي أصبح استخدامها منطوياً على مخاطر كبيرة وكان حافزا لتطور العقلية السلوك الإجرامي، التي أفرزت الانواع جديدة من الإجرام يسمى الإجرام السيبراني.

عليه سنقسم هذا المبحث على مطلبين، إذ سنخصص المطلب الاول التعريف بالجريمة الالكترونية وخصائصها، وسنخصص المطلب الثاني انواع الجرائم الالكترونية.

المطلب الاول: التعريف بالجريمة السيبرانية وخصائصها

اولا: تعريف الجريمة السيبرانية

أن الجريمة السيبرانية، تتضمن الحاسوب أو الشبكات الحاسوبية، إذ يستخدم الحاسوب في ارتكاب الجريمة، وهي جريمة حديثة، ونظراً لارتباطها بتكنولوجيا متطورة هي تكنولوجيا المعلومات ونتيجة الحداثة هذه الجريمة فقد تباينت التعاريف التي تناولتها في مضامينها وفي صياغاتها، ويمكن تعريف الجريمة الإلكترونية على أنها "تلك الجريمة التي يتم فيها استخدام الآليات والأسلحة الإلكترونية السابق ذكرها للقيام بهجوم الكتروني بهدف تحقيق مكاسب مالية بالأساس" (العيساوي، ٢٠٢٢، صفحة١٩٦)

كما عرفت بأنها " كل تصرف غير قانوني يتم عبر الأجهزة الالكترونية، يؤدي الى حصول الجاني على مكاسب مادية أو معنوية مع تحميل الضحية، خسائر متقابلة، وغالبا ما يكون هدف هذه الأفعال هو الاختراق لسرقة أو تدمير المعلومات" (الطاهر، ٢٠٢٢، صفحة٣) أو أنها "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جريمة محلة معطيات الكمبيوتر" (قاسمي، ٢٠٢٠، صفحة ١٩)، وكذلك قد عرف خبراء منظمة التعاون الاقتصادي والتنمية انها "اي تصرف غير قانوني أو غير أخلاقي أو غير مصرح به يتعلق بمعالجة البيانات آليا أو نقلها، إذ يعتمد التعريف على معيار السلوك، فضلا عن الوسيلة المستخدمة في ارتكاب الجريمة" (محمد وحمزة، ٢٠٢٣، صفحة٨).

هذا ولقد تعرف الجريمة في اطار القانون الجنائي بانه" ”فعل غير مشروع تقوم به الإدارة الجنائية ويحدد له القانون عقوبة أو تدابير احترازية، ويعتمد ذلك على عنصرين: عناصر الجريمة وسلوكها، فضلا عن النص القانوني الذي يجرم هذا السلوك ويحدد العقوبة المناسبة له" (القرعان، ٢٠١٧، صفحة٣٦)، وتعرف الجريمة السيبرانية، وفقا للاتفاقية العربية واتفاقية بودابست وقانون الجرائم الامريكية والاتحاد الدولي للاتصالات، بأنها " كل من جناية أو جنحة ترتكب ضد شخص أو جماعة، تكون بدافع غير مشروع وبنية الإساءة الى سمعة الضحية، أو جسده أو فكره أو ماله أو حياته، سواء تم ذلك بشكل مباشرة او غير مباشرة باستخدام وسائل الاتصالات الحديثة مثل الانترنت" (الهام، ٢٠٢٠، صفحة٨٩)، ومع تطور الحديث في مجتمع يتطور من النظام الاجتماعي التقليدي الى النظام الاجتماعي العصري على جميع انحاء الدول والاعلى تقدما وسرعة في الاداء، تتزايد عمليات والاندماج مع العالم الخارجي والمجتمعات المحلية من خلال شبكة الانترنت المتاحة والمباحة، مع حرية كاملة دون أي قيود أو ضوابط أو قوانين محددة، يتم تحديد نطاق العقوبات الجنائية في حال انتهاك الخصوصية أو الحقوق والحريات (دبوزا، ٢٠٢٢، صفحة ١٣٦).

عليه، يمكننا القول إن جريمة لها عناصرها تصنع خصوصيتها، إذ لابد من توفر وسائل إلكترونية من حاسوب، وشبكة إنترنت تستخدم لأغراض إجرامية، أي قصد الإضرار بالأفراد أو مؤسسات دولية، تمتلك تلك المعلومات التي تستخدم ضدها أو يتم إتلافها أو تسريبها الى العدو.

ثانيا: خصائص الجريمة السيبرانية

١) الجريمة السيبرانية تعتبر عابرة للحدود من حيث الزمان والمكان

مما يعني ان المخاطر او الجرائم لا يتقيد بالحدود الجغرافية القارات او الدول، ولا بالمكان ولا بالزمان، في عالم المعلومات، تختفي الحدود بين الدول، إذ يرتبط العالم بشبكة واحدة، غالبا ما تحدث الجرائم عبر الانترنت في بلد معين، لكنها تمر عبر دول اخرى وتظهر نتائجها في اماكن مختلفة، كل ذلك في ثواني معدودة.

٢) جرائم خفية:

يصعب اكتشافها بسبب ضعف القدرة الفنية لدى الضحية مقارنة بالمجرم، فضلا عن المهارات الفنية والعلمية المتقدمة للجاني تساعده على إخفائها، كما ان خوف الضحية من الإبلاغ عن الجريمة لتجنب للإساءة الى سمعتها قد يزيد من صعوبة اكتشاف هذه الجرائم (عطية الله الصحفي، ٢٠٢٠، صفحة ١١).

٣) جرائم يصعب اثباتها:

تعود جرائم صعوبة إثباتها الى اكتشافها ومتابعتها يتم غالبا بواسطة الصدفة، من الصعوبة حصرها في مكان محدد، إذ لانها لا تترك أثرا واضحا للعيان، أو لا يمكن رؤيتها بالعين المجردة، بل تظل مجرد أرقام تتداول في شبكة الانترنت، وان الجرائم التي لم يتم اكتشافها بعد تفوق بكثير تلك التي تم الكشف عنها، تعود الصعوبة لعدة أسباب:

أ) تتطلب خبرة فنية يصعب على المحقق التقليدي التعامل معها.

ب) صعوبة الحفاظ الفني على اثارها ان وجدت.
ج) لأنها تشبه الجريمة لا تترك أثرا بعد حدوثها
د) إذ تعتمد على الخداع في تنفيذها، والتضليل في التعريف على مرتكبيها.
ه) تعتمد على مستوى مرتفع من الذكاء في تنفيذها (التميمي، ٢٠١٦، صفحة ١٦).

٤) من حيث الهدف:

تستهدف الجرائم السيبرانية الأنظمة المعلوماتية، عن طريق اختراقها بهدف التلاعب أو تشويه المعلومات والبيانات الخاصة بمستخدمي البيئة الرقمية، هذا يشبه ما يحدث في الجرائم التقليدية (الربيعي، ٢٠٢٤، صفحة ٧٦).

٥) اختلاف اسلوب ارتكاب الجريمة السيبرانية وطريقتها:

بينما تتطلب الجرائم التقليدية نوعاً من المجهود العضلي، مثل ممارسة العنف كما في جريمة القتل أو الاختطاف، أو استخدام القوة مثل الخلع أو الكسر، وتقليد المفاتيح كما في مخاطر او جريمة السرقة، إذ ان المخاطر او الجرائم الالكترونية تتميز بان طبيعتها الهادفة، فهي لا تتطلب استخدام العنف، فقد تحتاج فقط الى مهارات تقنية، للتعامل مع جهاز الحاسوب من اجل تنفيذ الاعمال التي تتعارض مع القوانين المعمول بها (حمادي، ٢٠١٧، صفحة ١٠٩).

مما تقدم، نستنتج بأن الجاني يرتكب الجريمة الالكترونية يتميز بمهارات عالية، إذ يعتمد على قدراته العقلية بالذكاء والدهاء ومعرفة الطرق الالكترونية التي تمكنه من اتلاف البرامج واختراق الحواجز الأمنية، وقد يتنوع دافع هؤلاء المجرمين، فقد يكون دافعهم المال، مما يدفعهم الى اللجوء الى طرق غير مشروعة بسبب ما يعانونه من بطالة، كما قد تكون لديهم دوافع عقائدية أو سياسية، أو حتى دوافع شخصية، مثل انتقام موظف من المؤسسة أو الشركة التي تم فصله منها، أو للتجسس وانتهاك الخصوصية.

المطلب الثاني: انواع الجرائم الالكترونية

لقد تتنوع صور هذه جرائم او مخاطر نظراً لاختلاف محل ارتكابها والهدف منه فضلا عن اختلاف شخصية المجني عليه، ومن هذه الأنواع هي كالآتي:

اولاً: الاعتداء على حرمة الحياة الخاصة

يتمثل في عدة اشكال، منها الافشاء العلني للمعلومات المتعلقة بحياة الشخص، مثل الكشف عن إصابته بمرض أو وضعه المالي كالإفلاس وعدم القدرة على سداد ديونه، كما يمكن ان يتضمن نشر صور تهدف الى تشويه سمعة الشخص والتشهير به، أو الاستيلاء على بياناته الشخصية كاسمه وصورته، من بين القضايا الأكثر شهرة في كل مخاطر او جرائم الالكترونية على جميع مستوى العالم هو الابتزاز الالكتروني وطلب دفع الفدية، إذ يقوم المبتزون بتهديد الضحية بنشر صور أو تسريب معلومات سرية تخصها، مقابل دفع مبالغ مالية، أو استغلال الضحية للقيام بأعمال غير مشروعة لصالحهم، مثل الإفصاح عن معلومات سرية تتعلق بجهة معينة (الزعبي، ٢٠٠٢، صفحة ٥).

ثانيا: جرائم السيبرانية ضد الحكومات

تعد من اخطر التهديدات التي تتعرض الامن القومي في العصر الحالي، وان الجرائم تشمل الاعتداءات على المواقع الرسمية للهيئات حكومية وأنظمة الشبكات الخاصة بها، إذ يسعى القراصنة الى تدمير البنى التحتية او تعطيل الخدمات الحيوية، غالباً ما تكون الدوافع وراء هذه الهجمات سياسية، إذ يسعى المهاجمون الى زعزعة استقرار الحكومات او التأثير على القرارات السياسية، وتشمل هذه الجرائم ايضا استهداف المواقع العسكرية للحصول على معلومات حساسة تتعلق الامن القومي والاسرار العسكرية، القراصنة يستخدمون تقنيات متقدمة لاختراق الانظمة والحصول على بيانات سرية، والتي قد تتضمن خطط استراتيجية او معلومات عن الأسلحة، بعد ذلك الحصول على هذه البيانات، قد يقومون بنشرها بطرق غير قانونية،

مما يعرض الامن الأمن الوطني للخطر، فضلا عن ذلك، يمكن أن تتضمن جرائم الإرهاب الالكتروني هجمات منسقة تهدف الى إحداث الفوضى أو الخوف بين السكان، هذه الأفعال قد تشمل ايقاف الخدمات الأساسية كمثل الكهرباء والمياه، فقد يؤثر على المواطنين، ويزيد من حالة عدم الاستقرار، لذلك، تستلزم مكافحة هذه المخاطر تعاونا متكاملة من كافة الحكومات والمجتمع الدولي لحماية البنى التحتية الحيوية وضمان الأمن السيبراني(عبابنة، ٢٠٠٩، صفحة ٤٧).

ثالثا: جرائم الابتزاز عبر الانترنت

لقد تعرض نظام حاسوبي، أو موقع ويب لتهديدات تهدف الى حرمانه من خدمات محددة، أذ يقوم قراصنة محترفون بشن هذه الهجمات بشكل متكرر، بغرض الحصول على مقابل مادي لوقف هذه الهجمات.

رابعا: جرائم النصب والاعتداء على الأموال

تتضمن مجموعة واسعة من الممارسات، مثل إدخال بيانات خاطئة أو تعليمات غير مصرح عنها، أو استعمال بيانات وعمليات غير مسموح بالوصول اليها، بهدف النهب من قبل موظفين فاسدون في الشركات العامة او الخاصة والمؤسسات المالية والاقتصادية، كما تشمل هذه الجرائم تعديل او حذف المعلومات او البيانات المخزنة، أو تكون إساءة استخدام الادوات والبرامج المتاحة Nguyen and Golman، 2021، (p.2).

خامسا: الاعتداء الالكتروني على حقوق الملكية الفكرية

يتمثل في التعدي على براءات الاختراع والعلامات التجارية، فضلا عن الاستنساخ وتكرار البرامج وإعادة إنتاجها وصنعها دون الحصول على ترخيص، مما يشكل انتهاكا للحقوق المالية والأدبية.

سادسا: التجسس الالكتروني

هو استعمال برنامج على جهاز الفرد المستهدف، مما يتيح الاطلاع والاستماع الى جميع المحادثات والمراسلات الصادرة من هذا الشخص، يتم إدخال هذا البرنامج الى جهاز الضحية عبر البريد الإلكتروني أو من خلال مواقع جذابة يزورها، إذ يقوم الشخص المتضرر بتحميل بعض البرامج، بما في ذلك برنامج التجسس، في هذه حالة، يقوم الجاني بإغراء الضحية بأن البرنامج يحتوي على ألعاب مثيرة أو محتوى جذاب آخر، مما يدفع الضحية الى تلقي الملف، يمكن أن تكون جريمة التجسس إما بالالتقاط، إذ يتم مشاهدة المعلومات عبر الشبكة الانترنت أو أحد أجهزة الكمبيوتر، أو بالاعتراض، إذ يتم اعتراض ما يتم إرساله

(Communications from the commission ،2007, p.3)

سابعا: التنمر السيبراني والمضايقات الرقمية

يمثلان ظاهرة متزايدة الخطورة في العصر الرقمي، والتنمر هو سلوك عدواني متكرر يهدف الى إيذاء شخص آخر، وعندما يحدث هذا عبر الانترنت أو وسائل الاتصال الحديثة، والتنمر السيبراني يمكن أن يتخذ عدة أشكال، مثل:

١) المضايقات المستمرة: إرسال رسائل مسيئة أو تهديدات عبر البريد الالكتروني أو الرسائل النصية.
٢) نشر الشائعات: توزيع معلومات كاذبة أو مضللة عن الضحية على وسائل التواصل الاجتماعي.
٣) التصيد الالكتروني: استخدام وسائل التواصل الاجتماعي أو الألعاب الالكترونية للاستهزاء أو الإيذاء.
٤) التحرش: إرسال محتوى غير مرغوب فيه أو مسيء.

أحد الأسباب التي تجعل التنمر السيبراني أكثر خطورة هو انه يمكن أن يحدث بشكل مجهول، مما يمنح المعتدي شعورا بالحصانة، كما يمكن ان تواجه الضحية تحديات في الهروب من هذا الاساءة، إذ يمكن أن تستمر التعليقات السلبية في الظهور على الانترنت، مما يؤثر على صحتها النفسية وسلوكها في الحياة اليومية، ومن المهم أن يكون هناك وعي حول هذه الظاهرة وطرق التعامل معها، مثل الإبلاغ عن السلوكيات المسيئة، دعم الضحايا، وتعليم المستخدمين كيفية حماية أنفسهم عبر الانترنت (عبد اللطيف، ٢٠٢٠، صفحة٥٢).

ثامنا: مجموعة أخرى من الجرائم الالكترونية العديدة

تتضمن المخاطر او الجرائم الالكترونية مجموعة متنوعة من الأفعال، مثل جرائم التشهير التي تهدف الى تشويه سمعة الأفراد، والمطاردة الالكترونية التي تتعلق بتعقب الأفراد عبر الوسائل الالكترونية بهدف مضايقتهم أو إحراجهم في الأماكن العامة، كما تشمل هذه الجرائم السرقة المالية وتهديد الضحايا، إذ يقوم مرتكبو هذه الأفعال بجمع المعلومات الشخصية عن الضحية من خلال مواقع التواصل الاجتماعي وغرف المحادثة، فضلا عن ذلك، هناك جرائم السب والشتم والمخاطر المرتبطة بالجنس (الطاهر، صفحة ٨).

عليه، يتضح لنا بان الجريمة السيبرانية، هي جرائم تحصل عبر التقنيات المعاصرة من الحواسيب وشبكات الانترنت، ونظم المعلومات والهواتف النقالة وغيرها، وعلى الرغم من ان بعضها غير مرئي لكن لها تأثيراتها السلبية كبيرة، وتتخذ اشكال وانواع عدة، وما يفاقم خطورتها انها تتطور مع التقدم العلمي والتقني.

«المبحث الثاني»

دور التعاون الدولي والوطني في مكافحة الجرائم الالكترونية

أن جرائم سيبرانية أو جرائم الحاسوب هي ظاهرة محلية ودولية إلا أن التنبيه لخطورتها انتشر على النطاق الدولي بل إن الخوف من مخاطرها تزايد لما تجاوزت الحدود الوطنية وأصبحت جريمة منظمة عابرة للحدود، فتناولها الفقه والقانون والقضاء والإعلام والدراسات المختلفة الاقتصادية والأمنية والسياسية والقانونية وعليه لابد أن نتعرف على اهم وسائل مكافحتها وطنيا ودوليا، عليه سنقسم هذا المبحث على مطلبين، إذ سنخصص المطلب الاول الجهود الدولية لمكافحة الجرائم السيبرانية، وسنخصص المطلب الثاني الجهود الوطنية لمكافحة الجرائم السيبرانية.

المطلب الاول: الجهود الدولية لمكافحة الجرائم السيبرانية

لقد يتمثل الجهود الدولية في إبرام المعاهدات الدولية التي تهدف الى الوقاية والحد من جرائم الانترنت، فضلا عن الى التعاون القضائي من خلال تقديم المساعدة القضائية وتسليم المجرمين لضمان عدم إفلاتهم من العقاب، ومن بين هذه الاتفاقيات، تأتي اتفاقية بودابست ٢٠٠١ لمكافحة الجرائم المعلوماتية، التي أكدت على اهمية مواءمة التدابير التشريعية بين الدول للوقاية من هذه المخاطر.

كما شددت الاتفاقية على تفعيل خطة العمل على الجانب الموضوعية، والإجرائية للحد من هذه الظاهرة، مما يعكس اهمية التعاون الإقليمي والدولي في مواجهة المخاطر الالكترونية، واكدت ايضا على الحاجة الى ملاءمة الاجراءات التنفيذية التقليدية مع البيئة التكنولوجية الجديدة، ولهذا تم وضع مجموعة من الاجراءات التنفيذية المناسبة.

لقد يتمثل الجهود الدولية من إبرام الاتفاقيات الدولية لغرض وقاية وللحد من جرائم الانترنت والتعاون القضائي من خلال المساعدة القضائية وتسليم المجرمين وعدم إفلاتهم من العقاب، لذلك نجد أن اتفاقية بودابست اهتمت بالجانب الإجرائي، إذ وضعت القواعد تتعلق بالبحث والتحري والتعاون الدولي (العيساوي، صفحة ٢٠٢)، وان المادة (٢٢) من اتفاقية بودابست تبرز أهمية تحديد الولاية القضائية في حالات مخاطر شبكة الانترنت، خاصة في وقت الذي تدعو الى المزيد من دولة بالاختصاص، من خلال مبدأ التشاور، يمكن للدول الأطراف أن تتعاون لتحديد الولاية الأنسب، مما يعزز من فعالية الإجراءات القانونية.

كما أن نظام تسليم المجرمين بين الدول الأطراف يعد خطوة مهمة لضمان عدم إفلات المجرمين من العقاب، إذ تحدد الاتفاقية القواعد والإجراءات اللازمة لذلك، فضلا عن ذلك، فإن إنشاء نقاط اتصال تعمل على مدار ٢٤ ساعة يعزز من التنسيق بين الدول الأعضاء، مما يسهل تبادل المعلومات والتعاون في مواجهة الجرائم المعلوماتية، هذه الإجراءات تسهم في انشاء شبكة دولية متينة لمكافحة الجرائم الالكترونية وتعزيز الأمن الالكتروني، وذلك بهدف ضمان وتقديم المساعدة الفورية، والفعالة أثناء التحقيق، الجرائم المرتبطة بنظم وبيانات الكترونية أو جمع الأدلة ذات الطابع الالكتروني عن هذه الجرائم، كما أكدت اتفاقية بودابست على ضرورة التوفيق بين مكافحة الجرائم الالكترونية واحترام حقوق الإنسان، من خلال فرص التزام على الدول المشاركة في الاتفاقية بتقديم المساعدات المتبادلة، الى أقصى حد ممكن وذلك الأغراض المتعلقة بعمليات التحقيق أو الإجراءات المرتبطة بالجرائم التي تخص بنظم وبيانات الكمبيوتر، أو بالنسبة التي تتعلق بتجميع الأدلة الالكترونية الخاصة بالجريمة (Unctad ecretariat, 2005,p.2).

اما مؤتمر الفضاء السيبراني بلندن لعام ٢٠١١ كان حدثا بارزا، إذ جمع بين الحكومات والمنظمات الدولية والشركات الكبرى لمناقشة التحديات والفرص في

الفضاء السيبراني مشاركة اكثر من ٦٠ دولة، بما في ذلك الولايات المتحدة الأمريكية ودول الاتحاد الأوروبي والصين وروسيا، تعكس الاهمية العالمية لهذا الموضوع، في خطاب، اكد نائب الرئيس الأمريكي جو بايدن على التزام الولايات المتحدة بتعزيز الأمن السيبراني من خلال استثمارات استراتيجية، بما في ذلك تعيين منسق قومي للفضاء السيبراني في البيت الأبيض، وكما نعمل سوياً مع دول أخرى، لمحاربة المخاطر التي تجتاز حدود الدول، بما في ذلك تقديم المساعدة الدول الأخرى على بناء قدراتها في فرض تطبيق القانون لتتعاون مع بعضها البعض لأجل القضاء على التهديدات المنتشرة في الفضاء السيبراني، هذه الخطوات تهدف الى معالجة التحديات المعقدة التي تواجه الفضاء السيبراني وتعزيز التعاون الدولي في هذا المجال الحيوي (Clough,2010,p21).

وأشار في كلمته الى أن الفضاء السيبراني يمثل تحديات فريدة تختلف عن أي تحديات سابقة، مما يثير تساؤلات جديدة ويجبرنا على ابتكار أساليب جديدة، إذ لم تعد الأساليب التقليدية كافية، إن تحديد الإجراءات الفعالة وبناء الثقة في مجال الفضاء السيبراني يشكلان تحديا، وعلينا أن نبحث عن طرق لحل هذه المسألة (قرينح، ٢٠٢١، صفحة ٦١٣)، واتفقت الدول المشاركة في هذا المؤتمر على أن الانترنت يعد أداة أساسية وحيوية للنمو الاقتصادي، خاصة في الدول النامية، كما تم التأكيد على الفوائد الإيجابية للانترنت في تحسين حياة المواطنين وقدرته على كشف انتهاكات حقوق الإنسان عند حدوثها، واتفق المشاركون على ضرورة أن لا تكون جهود تعزيز أمن الإنترنت على حساب حقوق الإنسان، وقد أبدى المشاركون تأييداً قوياً لمبدأ ضرورة تسامح واحترام مستخدمي الانترنت لتنوع اللغات والأفكار والثقافات، مع التشديد على أهمية عدم استخدام حماية هذا المبدأ كذريعة للإخلال بحرية التعبير عن الرأي.

كما أشار مؤتمر الفضاء السيبراني الى أن جرائم المعلوماتية تمثل تهديدا كبيراً للرفاه الاقتصادي والاجتماعي، وكما انها تتطلب بذل جهود دولية عاجلة ومتكاتفة لمواجهة

هذه التهديدات وضمان عدم وجود ملاذ آمن لمجرمي الانترنت (Westby,2003,p11).

طالب المشاركون في المؤتمر بضرورة توافق القوانين المتعلقة بالمخاطر الالكترونية على مستوى دولي، وتعزيز الشراكة بين الدول عند الضرورة، كما حثوا الدول على التفكير في الانضمام الى الاتفاقية الدولية بودابست لمكافحة الجرائم المعلوماتية، والتي يعتبرونها أفضل نموذج للاتفاق الدولي في هذا المجال، فضلا عن ذلك، دعا المشاركون القطاع الخاص الى قيادة تطوير تقنيات وأنظمة متطورة لتعزيز أمن شبكة الانترنت، وتم الاتفاق ايضا تكون الحكومات أنموذجاً يحتذى به من خلال اعتبار أمن الانترنت معياراً أساسياً عند تقديم خدماتها عبر الانترنت (العبيدي، ٢٠١٥، صفحة ١٤٩).

ان المعاهدات والاتفاقيات الدولية تعد من ابرز اشكال التعاون الدولي، خاصة في مجال مكافحة جرائم الحاسب الآلي والانترنت، ومن هذه الاتفاقيات التي تقوم بالعمل في مجال مكافحة المخاطر او الجرائم المعلوماتية توصيات مجلس اوروبا مهمة جدا لأنها تساعد الدول على تحديث وتعديل قوانينها بما يتناسب مع التغيرات السريعة في تقنية المعلومات، فعلاً، مع تطور التكنولوجيا، من الضروري أن تكون هناك إجراءات قانونية فعالة تواكب هذه التغيرات وتحمي المجتمع من الجرائم الإلكترونية، إذ اصدر مجلس اوروبا مجموعة من التوصيات بشأن التحديات التي تواجه الإجراءات الجنائية المرتبطة بتقنية المعلومات، وقد يحث الدول في مجلس اوروبا على مراجعة وتعديل قوانين الإجراءات الجنائية المحلية، حتى تلائم القدم في هذا المجال، ومن أهم هذه التوصيات ما يأتي:

١) يجب توضيح القوانين في دول المجلس بشأن إجراءات تفتيش أجهزة الحاسب الآلي.

٢) كما انه من الضروري أن توفر الإجراءات الجنائية في دول مجلس للجهات المختصة بالتفتيش ضبط برامج الحاسب الآلي والمعلومات والبيانات المخزنة

فيها، وفقا لنفس الشروط المعمول بها إجراءات التفتيش العادية، ويجب ايضا إبلاغ الشخص المسؤول عن الأجهزة بأن النظام قد خضع للتفتيش مع توضيح المعلومات والبيانات التي تم ضبطها.

٣) يجب السماح للجهات المعنية بالتنفيذ اثناء اجراء التفتيش باحترام الضمانات المقررة بعد التفتيش لأنظمة الحاسب الآلي ضمن اختصاصهم، والتي تكون مرتبطة بالنظام الذي يتم تفتيشه، وضبط المعلومات والبيانات المتواجدة فيه.

٤) كما يجب تنفيذ إجراءات المراقبة والتسجيل في مجال التحقيق في الجرائم عند الحاجة في مجال تكنولوجيا المعلومات، مع ضمان الخصوصية والاحترام للمعلومات والبيانات التي يمنحها القانون حماية مميزة.

٥) يجب إلزام العاملين بالمؤسسات التي تقدم خدمات التواصل بالتعاون مع سلطات التحقيق لإجراء المراقبة والتسجيل.

٦) كما يجب تشكيل وحدات متخصصة لمكافحة جرائم الحاسب الآلي، فضلا عن إعداد برامج تأهيل خاصة للعاملين في مجال العدالة الجنائية لتعزيز معرفتهم في مجال تقنية المعلومات (رحمونة، ٢٠٢٠، صفحة ٢٢٤).

المطلب الثاني: الجهود الوطنية لمكافحة الجرائم الالكترونية

إن واقع المخاطر الالكترونية في العصر الحديث، يتطلب تطوير تشريعات تتناسب مع التغيرات السريعة في هذا القطاع، في العراق يواجه هذا التحدي غياب تشريع خاص بالجرائم السيبرانية، مما يجعل التعامل معها يعتمد بشكل رئيسي على قانون العقوبات رقم (١١١) لسنة ١٩٦٩، هذا الاعتماد على نصوص قديمة لا يتماشى مع طبيعة الجرائم الالكترونية المعقدة والمتطورة، يجب على العراق العمل على صياغة أطر قانونية حديثة تتماشى مع المعايير الدولية وتساهم في تحقيق مواجهة فعالة للجرائم الالكترونية، يتطلب ذلك تعاوناً بين مختلف القطاعات، بما في ذلك القطاع الحكومي والخاص، لتطوير استراتيجيات أمنية شاملة، فضلا عن ذلك، من الضروري تعزيز

الوعي المجتمعي حول مخاطر الجرائم السيبرانية وكيفية الحماية منها، مما يسهم في بناء بيئة رقمية أكثر أماناً (جواد، ٢٠٢٠، صفحة ٣).

تتم ملاحقة بعض الجرائم المرتكبة عبر الكمبيوتر والانترنت من خلال تفعيل نصوص قوانين العقوبات السارية في العراق، مثل نصوص السرقة والتزوير وخيانة والابتزاز والإتلاف وتقليد الأختام والتزوير والقذف والتشهير وإفشاء الأسرار والحض على الفجور، يتم استعمال هذه النصوص عندما ترتكب هذه المخاطر باستخدام كمبيوتر أو شبكة، إلا أن هذه النصوص تعتبر غير كافية لتلبية المتطلبات اللازمة لمواجهة هذه الجرائم بشكل فعا (Brenner, 2010, p21) .

إن الحاجة تدعو الى وضع نصوص قانونية جديدة تجرم هذه الجرائم، إذ إن النصوص الحالية تنطبق فقط عندما يكون كمبيوتر طريقة تنفيذ السلوك، وأحيانا عندما تقع الجريمة على الكمبيوتر نفسه، ومع ذلك، فإن المجرم غالبا ما ينجو من العقاب بسبب عدم وجود التشريع المناسب الذي يجرم هذه الأفعال (رضا، ٢٠٠٣، صفحة ١٠٨).

إن العراق لم يعتمد حتى الآن قانون حماية من الجرائم الالكترونية لعام ٢٠١٩، على الرغم من تزايد حالات انتهاكات الأمن السيبراني، وخاصة جرائم الابتزاز الإلكتروني، وقد حدد الفصل الثالث من مشروع القانون المذكور، الذي يركز على إجراءات جمع الأدلة والتحقيق والمحاكمة، أن المجلس الأعلى للقضاء يجب أن يؤسس محكمة مختصة للنظر في الدعاوى الجنائية المتعلقة بالجرائم السيبرانية، ويتولى النظر في هذه الجرائم قاضي أو أكثر من ذوي الخبرة والاختصاص، ممن حصلوا على تدريب متخصص في مجال الجرائم السيبرانية، كما تنص المادة (١٢) على أن "تتولى جهات المسؤولة عن اجراءات التحقيق مباشرة، وجمع الأدلة وطلبها من مصادرها في الجرائم المنصوص عليها في هذا القانون، " وقد أكد بأنه لا يجوز لجهات المسؤولة المباشرة بإجراءات التحقيق، والتفتيش دون أمر قضائي يصدره القاضي التحقيق المختص، وأن

يتولى قاضي أو المحقق المباشرة في عمليات الضبط وجمع الأدلة أو أي إجراء تحقيقي نص عليه قانون أصول المحاكمات الجزائية المعمول به (جواد، صفحة ٥) .

لقد تتعدد وسائل مكافحة الجرائم السيبرانية، ولكنها تواجه تحديات كبيرة نتيجة التطور السريع للتكنولوجيا، ومن بين أبرز الوسائل الوقائية لحماية وسائل التواصل الاجتماعي من الاستخدام غير القانوني وهي:

١) يمكن إنشاء وحدات خاصة تتولى مسؤولية الرصد والمتابعة، إذ تعمل هذه الوحدات على متابعة الأنشطة الإجرامية عبر وسائل التواصل الاجتماعي، بما في ذلك الاحتيال والإرهاب الالكتروني وغيرها.
٢) استخدام تقنيات لمراقبة المحتوى التي تطورها الشركات التكنولوجية، بهدف رصد وجمع المعلومات من وسائل التواصل الاجتماعي وتحليلها واستخراج المؤشرات منها بشكل فوري وآلي.
٣) إبرام اتفاقات بين الحكومة وشركات التواصل الاجتماعي، يمكن الحكومة من الحصول على معلومات شاملة حول أنشطة المجرمين والإرهابيين.
٤) تقديم الحكومة طلبات الى إدارات مواقع التواصل الاجتماعي للكشف عن بيانات أشخاص، أو صفحات محددة لأسباب تتعلق بالأمن والجريمة، اعتماد سياسات الإبلاغ أي ابلاغ إدارة مواقع التواصل الاجتماعي عن المخالفات في بعض الصفحات ليتم حذفها.
٥) اعتماد سياسات الإبلاغ، إذ يتم إبلاغ إدارة مواقع التواصل الاجتماعي عن المخالفات في بعض الصفحات ليتم حذفها.
٦) تمكين الحكومة من الحصول على برامج لمراقبة المستخدمين لأغراض المتابعة الأمنية وكشف المجرمين.

٧) تنفيذ الحجب الكلي أو الجزئي لمواقع التواصل الاجتماعي التي تحتوي على تحريض أو عنف أو أي محتوى يشكل تهديدًا لسلامة وأمن واستقرار الدولة والمجتمع (الدوري، ٢٠٢٢، صفحة٦٠٢).

ان وسائل مواجهة الجرائم السيبرانية تتطلب جهدا جماعيا من جميع الاطراف، بما في ذلك الافراد والمؤسسات الحكومية، ان من الضروري نكون واعين للمخاطر التي يمكن أن تنجم عن المعلومات المضللة وأن نتبنى سلوكيات آمنة على الانترنت، مثل استخدام كلمات مرور قوية وتحديث البرامج بانتظام، وهناك ايضا برامج الحماية المتقدمة بما توفره من سياسة امان عالية على الحسابات الافتراضية، والتأكد من مصدر نشر الاخبار، وعدم الترويج لأية اشاعة لمجرد وجودها في صفحة مهما كان حجم متابعيها، وخاصة وان الكثير منها تعمل على بعث الانقسام المجتمعي عبر بث الاخبار الكاذبة والدعاية المضللة، علاوة على ذلك، يجب تعزيز التعاون بين الدول لمواجهة هذه التهديدات، إذ أن الجرائم السيبرانية لا تعترف بالحدود الجغرافية، من تبادل الخبرات والمعلومات، يمكن للدول أن تكون أكثر فعالية في التصدي لهذه التحديات، فإن مواجهة الارهاب والجريمة السيبراني يكون من خلال توظيف التقنية المعاصرة والخبراء المختصين وبرامج وانظمة الحماية اللازمة وتحصين الامن المعلوماتي، مما يوفر خاصية الكشف المبكر عن الجرائم والاعمال إرهابية.

فضلا عن توعية المجتمع عن طريق الندوات والابحاث المختصة، وهنا تؤدي وسائل الاعلام دورا مهما في التوعية، ولعل من المؤشرات الايجابية التي تعكس التطور الأمني الالكتروني نجاح فريق الامن الرقمي المختص بالعمليات النفسية ومكافحة التطرف في جهاز مكافحة الارهاب العراقي من ابطال (٦٥٠٠) حساب تابع لتنظيم داعش الارهابي (قرينح، صفحة ٦١٥) .

مما تقدم، نستنتج مواجهة الجرائم السيبرانية هي قضية جماعية تشمل الجميع، بدءا من الأسرة والمجتمع، وصولا الى رجال القانون والمؤسسات الأمنية وعلماء الدين

والباحثين المتخصصين، من الضروري توعية المجتمع بخطورة هذه الجرائم وآثارها الكبيرة ووسائل الوقاية منها، يجب تشديد العقوبات على مرتكبي هذه الجرائم لتكون رادعا لهم، فضلا عن التعاون مع جميع الوكالات الدولية الإقليمية المختصة وشركات التواصل الاجتماعي، بهدف خلق بيئة داخلية ودولية معادية لهذه الجرائم بكافة أشكالها.

الخاتمة

بعد أن انتهينا من البحث توصلنا الى جملة من الاستنتاجات والمقترحات هي:

أولاً: الاستنتاجات

١) ان المخاطر الالكترونية تتميز بخصائص فريدة تميزها عن غيرها من الجرائم، مما يسبب العديد من الصعوبات في إثباتها، إذ إن الجناة يقومون بمحو أي دليل يدل عليها بعد ارتكابها.

٢) الجريمة السيبرانية تتمتع بطابع عالمي، فهي لا تعترف بحواجز الزمان أو المكان، ولا حتى بالحدود الإقليمية للدول.

٣) سعى المجتمع الدولي الى إبرام اتفاقيات دولية لمكافحة الهجمات والجرائم السيبرانية، وذلك من خلال إبرام معاهدة دولية لمكافحة جرائم الانترنت، التي تعد أول معاهدة تتعلق بمكافحة هذه الجرائم.

ثانيا: المقترحات

١) يجب العمل على إبرام اتفاقيات دولية تهدف الى توحيد وجهات النظر بين الدول بشأن مسألة تنازع الاختصاص القضائي فيما يتعلق بجرائم الانترنت، وتعديل القوانين الجنائية الموضوعية والإجرائية لتتناسب مع خصوصيات المخاطر او الجرائم الالكترونية.

٢) من الضروري رفع مستوى الوعي المجتمعي العام تجاه مخاطر الجرائم السيبرانية على الأفراد والمجتمعات.

٣) ينبغي العمل على إنشاء قاعدة بيانات على المستوى المحلي تختص بالمخاطر او بالجرائم الالكترونية، وخصوصا جرائم متعلقة بالتجسس والإرهاب والقرصنة السيبرانية، فضلا عن مختلف الجرائم التي تمس بالأمن الوطني.

قائمة المصادر

اولا: المصادر العربية

أ) الكتب

١) جواد، علي نعمة. (٢٠٢٠). *الجريمة المعلوماتية الماسة بالحياة الخاصة (دراسة مقارنة)* (الطبعة ١). القاهرة: المكتب الحديث.

٢) عبابنة، محمود احمد. (٢٠٠٩). *جرائم الحاسوب وابعادها الدولية* (الطبعة ١). عمان: دار الثقافة للنشر.

٣) الزعبي، محمد بلال. (٢٠٠٢). *الحاسوب والبرمجيات الجاهزة (مهارات الحاسوب)* (الطبعة ١). عمان: دار وائل للنشر.

٤) القرعان، محمود احمد. (٢٠١٧). *الجرائم الالكترونية* (الطبعة ١). الاردن: دار وائل للنشر.

٥) التميمي، تميم سيف. (٢٠١٦). *الجرائم الالكترونية في الاعتداء على الافراد* (الطبعة ١). الرياض: مكتبة القانون والاقتصاد.

ب) الرسائل والاطاريح

١) رضا، بيان عبد الله. (٢٠٠٣). الجرائم الجنسية الواقعة على الاطفال وتطبيقاتها على شبكة الانترنت (دراسة مقارنة) (رسالة ماجستير). كلية القانون، جامعة السليمانية.

٢) قاسمي، شعيب. (٢٠٢٠). الاستراتيجيات العالمية في مكافحة الجريمة الالكترونية (دراسة حالة الجزائر) (رسالة ماجستير). كلية الحقوق والعلوم السياسية، جامعة العربي التبسي.

٣) دبوزا، سعيد.(٢٠٢٢)الحماية القانونية للأطفال من الاستخدام غير المشروع لتكنولوجيات الاعلام والاتصال (على ضوء الصكوك الدولية والتشريعات

الوطنية) (اطروحة دكتوراه). كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح.
٤) عبد اللطيف، والي. (٢٠٢٢). الحماية الجزائية للطفل من الجرائم الالكترونية (رسالة ماجستير). كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف.

ج) البحوث والمقالات

١) العبيدي، اسامة بن غانم. (٢٠١٥). الجهود الدولية في مكافحة الجرائم المعلوماتية. *مجلة الحقوق*، ٣٩(٤٩)، ١١٢- ١٥٦.
٢) حمادي، الاء محمد رحيم. (٢٠١٧). الجريمة السيبرانية ومخاطرها على الاطفال (الاشكاليات والحلول). مجلة كلية التربية للبنات، ٢٨ (٤)، ١٠٤ – ١٢٠.
٣) الربيعي، نورهان محمد. (٢٠٢٤). الجريمة السيبرانية واليات مكافحتها (دراسة مقارنة). مجلة الفارابي للعلوم الانسانية، ٣(١)، ٧٣- ٩٠.
٤) الصحفي، روان. (٢٠٢٠). الجرائم الالكترونية. المجلة الالكترونية الشاملة متعددة التخصصات، ٤(٢٤)، ١- ٥٣.
٥) العيساوي، عمار مراد. (٢٠٢٢). الإطار القانوني للجريمة الالكترونية. المجلة الشاملة للحقوق، ٢(٤)، ١٩٢- ٢٠٨. اي
٦) الطاهر، ياكر. (٢٠٢٢). مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية. ٤(٤)، ١ – ٣٩.
٧) الدوري، حلا أحمد محمد. (٢٠٢٢). أثر التطورات التكنولوجية على الحق في الخصوصية. مجلة كلية القانون للعلوم القانونية والسياسية، ١١(٤٢)، ٥٦٥ – ٧٠٠.
٨) الهام، زاير. (٢٠٢٠). حماية الطفل من الاستخدام في المواد الاباحية عبر الانترنت: دراسة تحليلية لاتفاقية الطفل لسنة ١٩٨٩. مجلة القانون والعلوم السياسية، ٦ (١)، ٨٣- ٩٢.

٩) محمد، عباس و حمزة، وليد. (٢٠٢٣). أمن الفضاء السيبراني: قراءة في المفهوم القانوني. مجلة العلوم القانون، 37 عدد خاص، ١-٢٥. https://doi.org/10.35246/jols.v38i٢,٦٦٦.

١٠) قرينح، فاطمة الزهراء. (٢٠٢١). حماية الطفل من الاستغلال في المواد الاباحية عبر الانترنت (في القانون الدولي والتشريع الجزائري). مجلة الدراسات القانونية المقارنة، 7 (٢)، ٦٠٥١- ٦٢٥.

١١) رحمونة، قشيوش. (٢٠٢٠). الحماية القانونية للطفل ضحية الاستغلال الجنسي في ظل الفضاء الرقمي. مجلة نوميروس الاكاديمية، ١(٢)، ٢١٥-٢٣٥.

ثانيا: المصادر الاجنبية

1) Chat Le Nguyen and Wilfred Golman. (2021). Diffusion of the Budapest convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: Law on the books vs law in action. *Computer Law & Security Review, 40*. Collage of Rights, University of Canterbury, p.1- 55.

2) Communications from the commission to the European parliament. (2007). The council and the district committee. Towards a general policy on the fight against cybercrime. European Communities Committee, p.1- 10.

3) Jonathan Clough. (2010). Principles of cybercrime. Cambridge University Press. Cambridge, p.1-31.

4) Susan W. Brenner. (2010). Cybercrime: Criminal threats from cyberspace. Praeger, pp. 1-180.

5) Unctad Secretariat. (2005). Information Economy Report. United Nations conference on trade and development, pp. 1-209.

6) Westby, Jody. (2003). International guide to combating cybercrime. ABA Publishing. American Bar Association, p1-260.