مجلة جدارا للبحوث والدراسات، (8) (2022)
مجلة جدارا للبحوث والدراسات
Website: http://journal.jadara.edu.jo/index.php/JRS
ورقة بحثية، ورقة مراجعة، ورقة تقنية

البراعة التنظيمية المستدامة بإطار أبعاد إدارة الموهبة في ظل جائحة كورونا الجهود الدولية في مكافحة الجرائم الالكترونية

فاديا سامي علي الخصاونة*

أستاذ مساعد، قسم العلوم السياسية – جامعة جدارا

*corresponding authar email: fadiakhasawneh@yahoo.com

ملخص الدراسة :

تتجه الجهود الدولية بين مختلف أشخاص المجتمع الدولي الى المحافظة على متانة وديمومة العلاقات الدولية واستمراريتها ، إلا أن التطور الالكتروني والمعلوماتي

ساهم بايجاد آثار سلبية نجمت عن استغلال بعض الجهات للتقنيات الالكترونية في غير الغرض الذي خُلقت من أجله ، مما أدى الى توفر وسائل جديدة في أيدي مجرمي المعلوماتية تعمل على تسهيل ارتكاب العديد من الجرائم بدقة واحترافية عالية ، لذا سعت دول العالم المتقدمة منها والنامية إلى اتخاذ إجراءات مشتركة للتصدي لتلك الجرائم والحد من انتشارها ، وذلك من خلال إبرام اتفاقيات دولية لمواجهة تلك الجرائم والعمل على محاربتها، منها اتفاقيات عالمية ضمن إطار عالمي لمكافحة الجرائم المعلوماتية، ومنها الاتفاقيات الثنائية والمتعددة لتسليم المجرمين، والتي تعد من أهم أساليب مكافحة تلك الجرائم نظراً لما تتمتع به تلك الجرائم من خاصية لا حدودية تتم عن طريق هجمات واختراقات وتسلل داخل الأنظمة الالكترونية ، بغرض أما تدمير تلك النظم أو الحصول على معلومات سرية بهدف الاساءة سواء كانت عسكرية أو سياسية أو اقتصادية، مما ينبه إلى مدى أهمية تدارك تلك الظاهرة وتلافي مخاطرها على الصعيدين الدولي والوطني ، خاصة وأن التعاون الدولي والاتفاقيات الدولية تواجه بعض التحديات والصعوبات نظرا لطبيعة اختلاف القوانين الداخلية بين الدول ، إضافة إلى التحديات الكبيرة التي أوجدتها العولمة والتغيرات التقنية المتسارعة وغير المدركة.

الكلمات المفتاحية : القانون الدولي ، العلاقات الدولية ، الجرائم الالكترونية .

Abstract

International activities by many members of the international community are aimed at preserving the strength, durability, and continuity of international relations. However, electronic and information development has contributed to the creation of negative effects as a result of the exploitation of electronic technologies by some parties for purposes other than those for which they were designed, resulting in the availability of new means in the hands of informational criminals that facilitate the commission of many crimes with high accuracy and professionalism. Joint measures to address those crimes and limit their spread, including the conclusion of international agreements to confront and combat them, including global agreements within a global framework to combat information crimes, as well as bilateral and multiple agreements to combat criminal extradition. These borderless crimes are carried out through attacks, penetrations, and infiltration within electronic systems, with the goal of either destroying those systems or obtaining confidential information with the intention of offending, whether military, political, or economic, which highlights the importance of combating this phenomenon and avoiding international and national cooperation, especially since cooperation does not exist. Due to the nature of differing internal laws across nations, international and international agreements confront some hurdles and difficulties, in addition to the tremendous issues generated by globalization and the quick and unconscious technology advances.

Keywords: international law, international relations, electronic crimes.

المقدمه

ألقى التطور الالكتروني مسؤولية كبيرة على عاتق المشرع الجنائي لمواجهة الجرائم المعلوماتية الناشئة عن إساءة استخدام الأنظمة المعلوماتية خاصة في ظل قصور نصوص قانون العقوبات عن الإحاطة بهذه الجرائم لأن قواعده وضعت ابتداء لحماية الأموال ذات الطبيعة المادية الملموسة التي لها كيان في الفضاء الخارجي الأمر الذي يتعذر معه حماية القيم غير المادية المتولدة عن المعلوماتية ، فالتطور المذهل للكمبيوتر أدى إلى نشوء جرائم ناتجة عن ذلك الاستخدام، وهذه الجرائم تقع بواسطة الكمبيوتر حيث يصبح أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية أو ما يصطلح علي تسميته بالجريمة الالكترونية ، لذا فإن مكافحة الهجوم الالكتروني وجرائم الإنترنت اصبح من الأهمية بمكان أن نبحث في السبل التي يجب اتباعها للتصدي لتلك الجرائم العابرة للحدود و التي تستلزم تحديد ماهيتها وخصائصها وطبيعتها وخصائص مرتكبيها وكذلك لا بد من أن نبحث في أساليب وإجراءات التعاون دولي الذي يتفق مع طبيعة الجرائم المتعلقة بالشبكة المعلوماتية والتي تتميز بطابع خاص يقتضي من المجتمع الدولي أن تكون لديه ردود فعل سريعة للحد من الهجوم الالكتروني ومكافحة الجريمة الالكترونية والوقوف أمام التحديات التي تواجه هذا التعاون و تحد من استمراريته .

أهمية الدراسة :

برزت أهمية هذه الدراسة من أهمية موضوع الجرائم الالكترونية وحداثته ، ومدى ضرورة ايجاد اتفاق دولي وسياسة دولية واحدة يتم الاتفاق عليها واعتمادها بين الدول ، نظراً لازدياد الجرائم العابرة للحدود واتساع حجمها وتعدد أنواعها وأساليبها، بحيث أصبح من الصعب جداً السيطرة عليها أو الحد من مخاطرها إذا لم يتوافر لها قوانين دولية واحدة يتم الاتفاق عليها والاستعداد لها .

المبحث الاول : الإطار المفاهيمي للجريمة الإلكترونية وخصائصها :

اولا : مفهوم الجريمة الالكترونية

هي الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال بالإنترنت ، يكون هدفها اختراق الشبكات أو تخريبها أو التحريف أو التزوير أو السرقة والاختلاس أو قرصنة وسرقة حقوق الملكية الفكرية ، وهي جريمة بأركانها المادية والمعنوية ولا عبرة فيها بالدافع الأساسي لارتكابها .

وقد تعددت الآراء بشأن تعريف الجريمة الإلكترونية ، فكل رأي تبنى مفهوماً مختلفاً بالنظر إلى الزاوية التي يراها ، وهذا ما حدا بالأمم المتحدة إلى عدم التوصل لتعريف متفق عليه دولياً ، ورغم صعوبة وضع تعريف لظاهرة هذه الجريمة وحصرها في مجال ضيق ، إلا أن مكتب تقييم التقنية في الولايات المتحدة الأمريكية عرفها بأنها « نشاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني « ، وعرفت أيضاً بأنها « كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية ، يهدف إلى الاعتداء على أي مصلحة مشروعة ، سواء أكانت مادية أو معنوية [1] .

وعرفها آخرون بأنها: الجريمة ذات الطابع المادي، التي تتمثل في كل سلوك غير قانوني غالباً ما يكون الهدف منه هو القرصنة من أجل سرقة أو إتلاف المعلومات الموجودة في الأجهزة ومن ثم ابتزاز الأشخاص باستخدام تلك المعلومات.

ومن هنا يمكن القول: إن الجريمة الإلكترونية هي عبارة عن أفعال غير مشروعة ، يكون الحاسب الآلي محلا لها أو وسيلة لارتكابها .

ومع غزو الإنترنت لدول العالم أصبح من الصعوبة بمكان ضبط وكشف هذه الجرائم نظراً لكونها عابرة للحدود، تحدث في مكان معين وضحاياها في مكان آخر ، وتتم بسرعة فائقة ودون رقابة من أي دولة ، مما أدى الي ارتكاب كافة صور النشاط الإجرامي المتعارف عليه عبر الإنترنت كالسطو على برامج الحاسوب بغرض سرقة البيانات وقاعدة المعطيات المعلوماتية حتى السرية منها واستخدامها في التجسس، أو تلك المتعلقة بالقرصنة والسطو على الأموال إلى جانب ظهور ما اصطلح عليه بالإرهاب الإلكتروني وتهديد الأمن القومي للدول، وكذا جرائم الآداب العامة والمساس بالأخلاق من خلال الإباحية الإلكترونية التي تجسدها المواقع الإباحية، خاصة التي يتم فيها استخدام الأطفال والنساء باستعمال وسائل الترغيب والترهيب كالإغراء والتحذير أو التهديد[2].

وقد اتفقت جميع النظريات والدراسات المنجزة حول نقطة أساسية، تتمثل في الغاية المادية البحتة التي يسعى الى تحقيقها المجرم الالكتروني، من سطو على الأموال، أو اعتداء على البيانات السرية أو تدمير البرامج المعلوماتية لأية دولة لتهديدها في أمنها القومي وسلامة أراضيها.

ثانياً : خصائص الجرائم الإلكترونية

لقد تنوعت الدراسات التي تحدد الجريمة الالكترونية وخصائص مرتكبيها كأساس لتبرير

وتقدير العقوبة و لا يمكن أن يكون هناك نموذج محدد للجريمة الالكترونية، وإنما هناك بعض السمات المشتركة بين هذة الجرائم ، يمكن إجمالها فيما يلي :

1- **عالمية الجريمة الالكترونية وصعوبة اثباتها :**

فحدودها ترتبط بالفضاء الرقمي الالكتروني لا صلة لها بالمكان الجغرافي ، فالجريمة المرتكبة جريمة عابرة للحدود والقارات فلا تحتاج لفترة زمنية طويلة من التخطيط بل تنفذ بثوانٍ معدودة وعبر معلومات متناقلة من أماكن متباعدة ،كما أنها صعبة الإثبات والتيقن لكونها مرتبطة ببيانات حاسوبية يمكن نقلها بسرعة فائقة من مكان إلى آخر بحيث أصبح مسرح الجريمة ارتكابها عالمياً لكونها لا وجود لاثر مادي ملموس لها، وهذا يعسر إجراءات اكتشافها ومعرفة مرتكبيها .

2- **الجريمة الالكترونية جريمة ناعمة**

فمقارنة مع الجريمة التقليدية التي تتطلب اسلوباً عنيفاً وادوات خاصة للقيام بها ، فإن الجريمة الالكترونية ناعمة ولا تحتاج لجهد عضلي أو عنيف ، أو حاجة إلى استخدام القوة فجُل ما تحتاج اليه هو الجهد الذهني لإدراك تقنيات الحاسوب ومهاراته وإثبات الذات لقهر الأنظمة الالكترونية والتغلب عليها و الإلمام التام بمسرح الجريمة وأدواتها ، بما يجنبه فجائية المواقف التي قد تؤدي إلى إفشال مخططه وافتضاح أمره [3].

3- **مجرموها أذكياء وذوو قدرات احترافية ومهارية وتخصصية عالية**

حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية، حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات أو داخل أجهزة الحواسيب. فالإجرام المعلوماتي هو إجرام الذكاء، وهذا الذكاء هو مفتاح المجرم المعلوماتي لاكتشاف الثغرات واختراق البرامج المحصنة ،و له قدرة فائقة في المهارة التقنية والمهارات في اختراق الشبكات وكسر كلمات المرور أو الشيفرات ليحصل على البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات. كما يملكون القدرات والمهارات التقنية ما يؤهلهم لأن يوظفوا مهاراتهم في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال[4].

وعادة ما تتراوح أعمار تلك الفئة من المجرمين ما بين45-18 عام.

وقد اختلفت المسميات التي تطلق على فاعلي الجرائم الالكترونية منها :

1- المتسللون « Hackers » وهم عادةً مجرمون محترفون يستغلون خبراتهم وإمكاناتهم في مجال تقنية المعلومات للتسلل إلى مواقع معينة للحصول على معلومات سرية أو تخريب وإتلاف نظام معين وإلحاق الخسائر به بقصد الانتقام أو الابتزاز .

2- المخترقون، سواء كان من الهواة أو المحترفين، وهناك (الكرا كرز» Crackers «) وعادةً ما يستخدم مجرمو هذا النمط قدراتهم الفنية في اختراق الأنظمة والأجهزة تحقيقاً لأهداف غير شرعية كالحصول على معلومات سرية أو للقيام بأعمال تخريبية... إلخ .

3- العابثون بالشيفرات ومؤلفو الفيروسات Malecions hackers

ثالثاً : أهداف الجرائم الإلكترونية

يهدف المجرم المعلوماتي من جريمته إلى :

1- تحقيق مكاسب مادية معينة

2 - إثبات مهارته الفنية وقدرته على اختراق أجهزة الحاسوب ،

3- قد يرتكب مجرمو هذه الفئة جرائمهم بهدف التسلية أو الترفيه

4- أو لمجرد الرغبة في الإضرار بالآخرين كالموظف الذي يتم فصله من وظيفته ويلجأ إلى الانتقام .

رابعاً : أنواع الجرائم الالكترونية

1. الجرائم ضد الأفراد : وتسمى جرائم الإنترنت الشخصية مثل سرقة الهوية ومنها البريد الإلكتروني أو سرقة الاشتراك في موقع شبكة الإنترنت .

2. الجرائم ضد الملكية : انتقال برمجيات ضارة وهي المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها لتدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى ممتلكات شخصية

3. الجرائم ضد الحكومات: مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الإنترنت وهي تتركز على تدمير الخدمات والبنى التحتية ومهاجمة شبكات الكمبيوتر وغالباً ما يكون هدفها سياسيا [5].

خامساً : صور الجريمة الإلكترونية :

١. تخريب المعلومات وإساءة استخدامها. ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تحريف المعلومات، تحريف السجلات الرسمية. الخ.

٢. سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات المهمة أو ذات العلاقة بالتطوير التقني، أو الصناعي، أو العسكري، أو تخريبها، أو تدميرها. الخ.

٣. تزوير المعلومات ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب.

٤. تزييف المعلومات وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي وإصدارها.

٥. انتهاك الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الافراد الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها.

٦. التصنت وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.

٧. التجسس ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.

٨. التشهير ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.

٩. السرقة العلمية الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.

١٠ . سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.

١١ . الدخول غير القانوني للشبكات بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.

١٢ . قرصنة البرمجيات ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.

١٣ . قرصنة البيانات والمعلومات ويشمل اعت ا رض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.

١٤ . خلاعة الأطفال وتشمل نشر صور خاصة للأطفال «الجنس السياحي» للأطفال خاصة، وللإناث على الشبكات. بشكل عام، ونشر الجنس التخيلي .

١٥ . القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملغومة إلكترونية.

١٦ . إفشاء الأسرار وتشمل الحصول على معلومات خاصة جداً ونشرها على الشبكة.

١٧ . الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أو الهاتف ..الخ.

١٨ . سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.

١٩ . التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة.

٢٠ . المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما

، وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.

٢١ . الإرهاب الإلكتروني والتي تشمل تكتيكات الإرهاب وأسلحته وأهدافه في التدخل بسياسات وأمن الدول . (4)

سادساً : أركان الجريمة الالكترونية : (5)

لكي يمكن القول بوجود جريمة ما، فإن المشرع يتطلب وجود ركن شرعي وركن مادي وركن معنوي فيها. وبغير هذه الأركان لا يمكن القول بوجود جريمة. فالركن المادي هو النشاط أو السلوك الذي جعل الجريمة تحدث، حتى ولو لم تتوافر علاقة السببية بين هذا النشاط أو السلوك والنتيجة الإجرامية.

أولا : الركن المادي :

إن النشاط او السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال بالأنترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته .

فمثلا يقوم مرتكب الجريمة بتجهيز الحاسب لكي يحقق له حدوث الجريمة. فيقوم بتحميل الحاسب ببرامج اختراق، او أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلي تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها أو يمكن أن يقوم بجريمة إعداد برامج ، Hosting Server الجهاز المضيف فيروسات تمهيداً لبثها.

ليس كل جريمة تستلزم وجود أعمال تحضيرية ، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في جرائم الكمبيوتر والانترنت حتى ولو كان القانون لا يعاقب علي الاعمال التحضيرية- إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور مخلة ، فهذه الاشياء تمثل جريمة في حد ذاتها.

ثانياً: الركن المعنوي :

فإنه يأخذ شكل القصد الجنائي،الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم. فهو تارة يستخدم الإرادة كما هو الشأن قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا أخري اخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي.

وقد برزت تلك المشكلة في قضية موريس الذي كان متهما في قضية دخول غيرمصرح به علي جهاز حاسب فيدرالي وقد دفع محامي موريس علي انتفاء الركن المعنوي الأمر الذي جعل المحكمة تقول « هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به، بحيث تثبت نية المتهم في الولوج إلي حاسب فيدرالي، ثم يلزم إثبات نية المتهم في تحدي الحظر الوارد علي استخدام نظم المعلومات في الحاسب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلي تحديد أركان جريمة الدخول دون تصريح « . وبذلك ذهبت المحكمة إلي تبني معيارين هنا هما الإرادة بالدخول غير المصرح به، واذا معيار العلم بالحظر الوارد علي استخدام نظم

معلومات فيدرالية دون تصريح.

ثالثاً : الركن الشرعي:

يقصد بالركن الشرعي وجود نص قانوني يجرم الفعل ويبين العقاب المترتب علي اتيانه حيث انه لا جريمة ولا عقوبة بغير نص قانوني،غير أن هذه القاعدة الأصلية ليست مطلقة فقد يحدث أن يتطلب المشرع أحيانا وجود جريمة لا يحتاج فيها إلي ركن معنوي وإنما يلزم فيها وجود الركن المادي.

المبحث الثاني : الجهود الدولية في مكافحة الجرائم الالكترونية

أصبح التعاون الدولي ضرورة لا مجال للتغاضي عنها او تأجيلها أو استبدالها بطرق أخرى، في إطار مكافحة الجرائم الالكترونية خاصةً بعد أن وصفت هذه الجرائم بالعالمية من حيث التأثر والتأثير خاصة مع التطورات التكنولوجية المتسارعة وغير المدركة ومع وجود التحدي الكبير باختلاف النظم القانونية بين الدول في إطار المعالجة الفردية لهذة الجرائم وعدم قدرتها على التصدي لها اقتضى هذا كله التعاون الدولي المتكامل بين اعضاء المجتمع الدولي لتحقيق الأهداف المرجوة والمصالح المشتركة من خلال ما يلي :

المطلب الأول: التعاون القضائي الدولي في مواجهة الجرائم الالكترونية

ففيما يتعلق بالجريمة الالكترونية فإن فعالية التحقيق والملاحقة القضائية غالباً ما تقتضي الحاجة الى مساعدة من السلطات في البلد المنشأ للجريمة او في سلطات البلد الذي عبر من خلاله النشاط الإجرامي وهو في طريقه الى الهدف، فقد يكون المجرم في دولة والحواسيب المستخدمة في دولة ثانية وأثار الجريمة في دولة ثالثة مما يؤدي إلى وقوف مبدأ السيادة الجغرافية كعقبة في اكتشاف الجريمة ومتابعتها ، لذا تعرف المساعدة القضائية بأنها كل إجراء قضائي من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم .

وتتخذ المساعدة القضائية الدولية عدة صور من أهمها :

اولا : تبادل المعلومات

تعتبر تبادل المعلومات وسيلة مهمة لمكافحة الجريمة الالكترونية بشكل كبيرة لما توفره من معلومات مثل تقديم بيانات ووثائق ودلائل مادية للنظر في الجريمة المدروسة ، بين الأجهزة القضائية للدول المختلفة لمتابعة النشاط الإجرامي.

وقد نصت نصوص تشريعية دولية على تبادل المعلومات بين الدول مثل اتفاق شنجن للاتحاد الأوروبي واتفاق الرياض للتعاون القضائي العربي .

ثانياً: نقل الإجراءات

والتي يقصد بها قيام دولة ما بمقتضى اتفاقية اتخاذ إجراءات قانونية جنائية عند التحقيق في جريمة معلوماتية ارتكبت في دولة اخرى ولمصلحة دولة معينة ، متى ما توفر عنصر التجريم المزدوج بين الدولتين الدولة الطالبة والدولة المطلوبة وشرعيتها .

وفي الاتفاقيات الدولية بشأن نقل الاجراءات في المسائل الجنائية بين الدول ،هناك معاهدة الامم المتحدة واتفاقية الأمم المتحدة لمكافحة الجرائم المنظمة العابرة للوطنية .

ثالثاً : الإنابة القضائية :

والتي يقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى تتقدم به الدولة الطالبة الى الدولة المطلوب إليها، للضرورة في الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة لتعذر قيامها بهذا الإجراء بنفسها .

ويكون الهدف من الإنابة هو تسهيل الإجراءات الجزائية وتسريعها بين الدول لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادات الجغرافية المختلفة .

ثانياً : تسليم المجرمين :

يعتبر تسليم المجرمين من أشكال التعاون الدولي في مكافحة الجرائم الالكترونية وهذا النوع هو نتيجة التطورات التي حدثت في الاتصالات وتقنية المعلومات ، لكون النشاط الإجرامي لم يعد ينحصر في إقليم معين فالمجرم المعلوماتي مجرم دولي.

لذا لا بد من إيجاد آلية للتعاون بين الدول لتسليم المجرمين الفارين عبر حدودها، وهذا الإجراء قد يسمح للدولة محاكمة المجرم على اراضيها إذا كان قانونها يسمح بذلك أو تقوم بتسليمه للدولة لمحاكمته وبهذا تضمن مصلحة الدولتين الطرفين في عملية التسليم الأولى الدولة التي خالف قوانيننها والثانية لتتخلص منه كفرد خرج عن القانون .

وقد اهتمت كثير من الدول بهذا الإجراء مثل اتفاقية بودابست التي بينت مجموعة من الإجراءات والشروط في تسليم المجرمين بين الدول ، وهناك أيضا الاتفاقية العربية التي نصت على اجراءات التسليم في عام 2014 .

المطلب الثاني : أولا :الجهود الدولية على مستوى المنظمات الدولية في مكافحة الجرائم الالكترونية :

اولا : المستوى العربي

تم الاتفاق بين الدول العربية ضمن نشاطات جامعة الدول العربية على توقيع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والتي نصت في الديباجة على إن رغبة الدول العربية الموقعة في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعا منها بضرورة الحاجة

إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وأخذ اً بالمبادئ الدينية والاخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الانساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومراعاة النظام العام لكل دولة، والتزاما بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الانسان ذات الصلة من حيث ضمانها واحترامها وحمايتها، فقد اتفقت الدول العربية على مجموعة من المبادئ تحقق ابجديات هذا التعاون .

وقد حررت هذه الاتفاقية باللغة العربية في مدينة القاهرة في جمهورية مصر العربية في 21/ 12/ 2010 في الامانة العامة لجامعة الدول العربية (الامانة الفنية لمجلس وزراء العدل العرب)(ونسخة مطابقة للأصل تسلم للامانة العامة لمجلس وزراء الداخلية العرب، وتسلم كذلك نسخة مطابقة للاصل لكل دولة من الدول الاطراف. وإثباتا لما تقدم، قام أصحاب السمو والمعالي وزراء الداخلية والعدل العرب، بتوقيع هذه الاتفاقية، نيابة عن دولهم. (6)

ثانيًا : المستوى الدولي

المنظمة الدولية للشرطة الجنائية (إنتربول)

يعد الانتربول أهم آليات التعاون الشرطي الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بصفة عامة والجريمة المعلوماتية بصفة خاصة. فمهمة الانتربول الاساسية تفعيل التعاون بين أجهزة الشرطة التابعة للدول الاعضاء في المنظمة بتوحيد إجراءات التسليم، ومن خلال تنسيق العمل الشرطي وتجميع البيانات وتبادل المعلومات لتيسير خدمات التحقيق لضبط وملاحقة المجرمين الهاربين وتسلمهم إلى الدولة التي تطلب تسلمهم، وإنشاء وتطوير كل النظم القادرة على المساهمة بفاعلية في الوقاية والعقاب على جرائم القانون العام. هذا ويعهد بتلك المهمة إلى المكاتب المركزية والوطنية في كل دولة عضو وإلى جهاز دائم يتم تعيينه بواسطة السلطات الحكومية الوطنية، وبمساعدة فرق الانتربول للتحرك إزاء الأحداث التي يمكنها تيسير مجموعة من خدمات التحقيق و التحليل في موقع الحدث بالتنسيق مع الامانة العامة. ويقوم الانتربول بتعميم التحذيرات والتنبيهات المتضمنة المعلومات الاستخبارية والإحاطات والمشورة التحليلية والفنية عن الاخطار الاجرامية المحتملة، ويستخدم الانتربول أدواته الخاصة كمنظومة النشرات الدولية بمختلف أنواعها و التقصي في قواعد البيانات وتقديم الخبرات والدورات التدريبية في مجال مكافحة جرائم الإنترنت، وذلك باالاستعانة بمجموعة من الخبراء الدوليين والمختبرات الدولية على الصعيد العالمي، وتيسير تبادل وتحليل وتخزين البيانات الجنائية حيث تقوم المنظمة بتزويد شرطة الدول الاطراف بكتيبات إرشادية حول جرائم الانترنت وكيفية التدريب على مكافحتها والتحقيق فيها. ويعد الاجرام المالي المرتبط بالتكنولوجيا المتقدمة من الجرائم التي تركز عليها منظمة الانتربول،

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 .

المطلب الثالث : الجهود الدولية على مستوى الاتفاقيات الدولية في مكافحة الجرائم الالكترونية :

تعد الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي بصفة عامة وفي مجال مكافحة الجرائم الناتجة عن الهجوم الالكتروني بصفة خاصة ، ومن بين المعاهدات والاتفاقيات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الاكترونية :

أولا- توصيات المجلس الاوروبي :

أدى التطور السريع في مجال تكنولوجيا الكمبيوتر والانترنت وشعور الدول الاوروبية بأهمية إعادة النظر في الإجراءات الجزائية في هذا المجال إلى إصدار المجلس الاوروبي التوصية رقم 13/95 في 1995/9/11 في شأن مشاكل الاجراءات الجزائية المتعلقة بتكنولوجيا المعلومات، وحث الدول الاعضاء بمراجعة قوانين الاجراءات الجزائية الوطنية لكي تتلائم مع التطور في هذا المجال، ومن أهم ما ورد بتوصية المجلس الاوروبي ما يلي :

1 : أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها

2 . أن تسمح الاجراءات الجزائية الوطنية لجهات التفتيش ضبط برامج الكمبيوتر والمعلومات الموجودة بالاجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إبلاغ الشخص القائم على الاجهزة بأن النظام متاحا للتفتيش مع بيان المعلومات التي تم ضبطها، والسماح باتخاذ إجراءات الطعن العادية في قرارات الضبط و التفتيش .

3 .أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ مع احترام الضمانات المقررة بمد التفتيش إلى أنظمة الكمبيوتر الاخرى في دائرة اختصاصهم والتي تكون متصلة بالنظام محل التفتيش وضبط ما بها من معلومات، بشرط ان يكون هذا الاجراء ضرورياً .

4- .أن يوضح قانون الإجراءات الجزائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجودة بأجهزة الكمبيوتر.

5- .تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة في مجال تكنولوجيا المعلومات ويتعين توفير السرية و الاحترام للمعلومات التي يفرض القانون لها حماية خاصة .

6 . .يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لاجراء المراقبة و التسجيل .

7 . .يتعين تعديل القوانين الاجرائية بإصدار أوامر لمن يحوز معلومات سواء أكانت برامج أم قواعد بيانات، تتعلق

بأجهزة الكمبيوتر بتسليمها بهدف الكشف عن الحقيقة .

. 8 .يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ الازم للسماح لرجال التحقيق بالاطلاع عليها . وأن تخول سلطات التحقيق بإصدار أوامر مماثلة الى كل شخص لديه معلومات عن طريق التشغيل والعمل على المحافظة عليها .

. 9 .يجب تطوير و توحيد أنظمة التعامل مع الادلة الالكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة يتعين تطبيق النصوص الإجرائية الخاصة بالادلة التقليدية على الادلة الالكترونية .

-10 يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات

11- قد تتطلب إجراءات التحقيق مد الاجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة وتفترض التدخل السريع، وحتى لا يمثل هذا الامر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الاجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الاجراءات .

12- يجب أن تكون هناك إجراءات سريعة ومناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع ادله معينة ويتعين عندئذ ان تسمح السلطة الاخيرة بإجراءات التفتيش والضبط و اجراء تسجيلات للمعاملات الجارية وتحديد مصدرها ، لذلك يتعين تطوير اتفاقيات التعاون الدولي القائمة. (8)

ثانياً - اتفاقية بودابست لمقاومة جرائم المعلوماتية و الاتصالات

إدراكا من الدول بمدى خطورة الجريمة المعلوماتية بوصفها جريمة عابرة للحدود فقد تم التوقيع عليها من ثلاثون دولة في العاصمة المجرية في 2001/11/23 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 المحاولات 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 .

وبالرغم من تنوع الجهود الدولية في مكافحة الجريمة الالكترونية و 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 التي سيتم توضيحها .

المبحث الثالث : 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 العسكرية 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 انشآء وحدات خاصة بمكافحة الجريمة المعلوماتية أسوة بجهات البحث الجنائي الوطنية و الدولية(الانتربول)، و ذلك لإثبات الجريمة عند وقوعها و تحديد أدلتها وفاعليها 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 ورغم 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 :

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 قانوناً 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 القدرة على الحماية المطلوبة

بالرغم من وجود معاهدات ثنائية أو جماعية بين الدول تسمح بالتعاون المثمر في مجال الجرائم ، 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. (9)

ثالثا: عدم وجود تنسيق بالاجراءات المتبعة

فلا يوجد هناك تنسيق متفق عليه 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 فضلاً عن صعوبة الحصول على الدليل ذاته .

رابعا: إشكالية الاختصاص في الجرائم الالكترونية

فنظراً لطبيعة صعوبة الحصول على الدليل القاطع والواضح لذلك 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 تبقى الحاجة ماسة إلى تشريعات جنائية أكثر مرونة حتى تواكب سرعة التقدم التكنولوجي و عصر المعلوماتية] إن إجراءات التحقيق في بيئة تكنولوجيا المعلومات وفقاً لما جاء في توصية المجلس الأوروبي رقم 35;/5 ، 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 .

وتثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية. فلو قام احد المجرمين في أمريكا بسرقة احد البنوك في الأمارات، وهذا الخادم Server الذي قام بالاختراق موجود لدى جهاز خادم في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين،

ويثور أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن حيث أن هناك بعد دولي في هذا المجال.(10)

الإشكالات القانونية التي يثيرها هذا النوع من الجرائم (الجرائم الالكترونية) :

1- حداثة القوانين المنظمة لها

2- التزايد الكمي المتسارع في أعداد الجرائم الالكترونية

3- التطور النوعي في أساليب ارتكابها

4- عدم القدرة على المواكبة لتشريعات المجتمع الرقمي الذي هو في تطور سريع .

5- صعوبة الوصول لشهود للجريمة .

6- صعوبة إثباتها خاصة في تحقيق الركن المادي الذي يتطلب نصوص قانونية خاصة به في ظل شرعية العقوبات حيث لا جريمة ولا عقوبة بغير قانون .

7- وجود تنازع القوانين خاصة في ظل وجود مبدأ إقليمية القوانين لان في غالبيتها جرائم عابرة للحدود مما يعني صعوبة الملاحقة الأمنية للجرمة داخل وخارج الدولة .

8- صعوبة الكشف عن الشروع في الجرائم الالكترونية . (11)

فيما يتعلق بالعقبة الأولى المتمثلة في عدم وجود نموذج موحد للنشاط الاجرامي فأن الامر يقتضي توحيد النظم القانونية ولاستحالة هذا الامر فأنه يمكن البحث عن وسيلة اخرى تساعد على ايجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم ويخفف من غلو الفوارق بين الانظمة العقابية الداخلة ،وتتمثل هذة الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم الالكترونية وإبرام اتفاقيات خاصة يراعى فيها هذا النوع من الجرائم .

أما المعوقة الثانية والخاصة بتنوع واختلاف النظم القانونية الاجرائية فنجد أن الصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة ، الشي الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعال . فمثلا المادة 20 من اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير الى التسليم المراقب الكترونيا والتي تعتبر من اهم التقنيات لمحاربة الجماعات الاجرامية المنظمة لتجميع الادلة والمعلومات وادلة الاثبات لاستخدامها فيما بعد في الملاحقات القضائية المحلية والدولية في سياق المساعدة القانونية المتبادلة .

وللحد من ظاهرةعدم وجود قنوات اتصال بين جهات انفاذ القانون فنلاحظ انه غالبا ما تشجع الصكوك الدولية الدول الى التعاون فيما بينها وتدعوها الى انشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول على المعلومات وتبادلها .

اما بالنسبة لمشكلة الاختصاص في الجرائم الالكترونية فثمة حاجة ملحة الى ابرام اتفاقيات دولية ثنائية كانت او جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة لجرائم الانترنت بالاضافة الى تحديث القوانين الجنائية الموضوعية منها والاجرائية بما يتناسب والتطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات .

ولأجل القضاء على مشكلة التجريم المزدوج والذي يعد من اهم الشروط الخاصة بنظام تسليم المجرمين ركزت الاتجاهات والتطورات التشريعية الخاصة بتسليم المجرمين على تخفيف التطبيق الصارم لهذا الشرط وذلك

بادراج احكام عامة في المعاهدات والاتفاقيات المعنية بتسليم المجرمين وذلك اما بسرد الافعال الوالتي تتطلب ان تجرم كجرائم او افعال مخلة بمقتضى قوانين الدولتين معا او بمجرد السماح بالتسليم لاي سلوك يتم تجريمه ويخضع لمستوى معين من العقوبة في كل دولة .

الخاتمة

ومن هنا أصبح لزاماً على الدول من أجل ضمان نهضتها وتماشياً مع عصر المعلوماتية الذي لا ينتظر أحداً أن تعمل على مواكبة التطور التكنولوجي والالكتروني الذي نجم عن تحول العديد من المجتمعات إلى مجتمعات معلوماتية تعتمد على التقنية الرقمية في أداء أعمالها.

و استناداً إلى ما سبق وبناءً على المبدأ القانوني الجوهري في القانون الجنائي ألا وهو مبدأ شرعية الجريمة والعقوبة وعدم جواز القياس في النصوص الجزائية فإننا نخلص إلى ما يلي :

1 - **زيادة الوعي لدى المواطنين لجرائم الكمبيوتر وللعقوبات المترتبة عليها.**

وتوفيرالضمانات القانونية الكافية التي تكفل حمايته بالإضافة إلى إحاطته بإجراءات أمنية الكترونية تمنع استغلاله واختراقه من قبل مجرمي المعلوماتية لغاية وقائية تهدف الى منع الجريمة قبل وقوعها .

2- **ضرورة التعاون الدولي لمواجهة الجرائم في البيئة المعلوماتية الالكترونية** وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرم صور هذه الجرائم كلها وتبين كذلك الاختصاص المكاني في حال وقوعها وكيفية تسليم مجرمي المعلوماتية وغير ذلك من الأمور ، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بالجرائم المعلوماتية .

3- **إنشاء وحدات مختصة في التحقيق في جرائم الكمبيوتر في المحاكم والشرطة** ومن الأفضل إحالة الجرائم المعلوماتية إلى قضاء متخصص مؤهل للتعامل مع هذه الجرائم والفصل فيها .

4- **ضرورة أن تتبنى الدولة جهازاً خاصاً للخبرة الجنائية للجريمة المعلوماتية** ، يتكون أعضاؤه من فريق متخصص فنياً في التقنية المعلوماتية ، وذلك لأن البحث عنها يتم داخل نظام الكتروني معقد ، يسهل فيه محو الأدلة إذا تم التعامل الأولي مع الجهاز بشكل خاطئ.

التوصيات التالية:

- إدراك أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالكمبيوتر.
- أن يؤخذ بالحسبان أن الجرائم المتصلة بالكمبيوتر ذات خاصية تحويلية.
- الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني .
- يتعين إدخال مادة « أخلاقيات استخدام الانترنت » ضمن المناهج الدراسية في التعليم ما قبل الجامعي

الهوامش

١- ما هي الجرائم الالكترونية، علاء الكساسبة ، المركز الديمقراطي العربي

٢- سيد طنطاوى محمد سيد - المركز الديمقراطي العربي / الجريمة المعلوماتية والصعوبات التي تواجهها/ المركز الديمقراطي العربي 17 يونيو 2018

٣- الجريمة الالكترونية، كامل مطر ، التعاون الدولي في مكافحة الجرائم الالكترونية / مجلة القانون الدولي للدراسات البحثية العدد الاول تموز يوليو 2019 صورية /الجزائر

٤- اسراء جبريل رشاد مرعي - المركز الديمقراطي العربي/ 2016/ https://democraticac.de/?p=35426

٥- أليات تفعيل الحماية والوقاية من الجرائم الالكترونية د. عبد العزيز موسى الدبور ، جامعة المنوفية مصر المؤتمر الدولي الرابع عشر في طرابلس 25-24 مارس 2017عنوان المؤتمر : الجرائم الالكترونية

عن خصائص الجرمين

٦- د.كامل مطر ، الجريمة الالكترونية ، 2018 المؤتمر الدولي لمكافحة الجرائم الالكترونية / فلسطين / جامعة النجاح https://repository.najah.edu/handle/20.500.11888/13488?show=full

٧- تحت عنوان : الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لمكافحة الجريمة الالكترونية

٨- التعاون الدولي في مواجهة الهجوم السيبراني /شيخه حسني الزهراين مجلة جامعة الشارقة للعلوم القانونية / مجلد 17/العدد 1 يونيو 2020 شوال 1441

٩- Journal of International Law for Research Studies The first issue - 2019 International cooperation in the fight against information crime BOURBABA SOURAYA. D

١٠- السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية/. ليندة شرابشة ، مجلة دراسات وابحاث ، المجلة العربية للابحاث في العلوم الانسانية والاجتماعية / تصدر عن جامعة زيان عاشور بالجلفة / الجزائر السنة الثالثة عدد25 ديسمبر 2016 ربيع الاول 1438 ، صفحة 241- 253 .

١١- المركز الديمقراطي العربي ، أنواع الجرائم الالكترونية وإجراءات مكافحتها 22 فبراير 2017