التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست

إعداد
السيد الدكتور/ وليـــد طـــه
رئيس محكمة
عضو قطاع التشريع بوزارة العدل
جمهورية مصر العربية

التنظيم التشريعي للجرائم الإلكترونية في اتفاقية بودابست

تمهيد:

الحياة الافتراضية. لا شك من أن التقدم العلمي الحديث في مجال المعلومات لاسيما في العقود الثلاثة الأخيرة، قد أحدث ثورة إلكترونية تطبق الآن في جميع مناحي الحياة، وأضحى من الصعوبة بمكان الاستغناء عن هذه الخدمات اللامحدودة، وكما هو الحال في الحياة خارج الانترنت استغل البعض المخترعات العلمية وما تقدمه من وسائل متقدمة في ارتكاب العديد من الجرائم الإلكترونية الحديثة، جرائم تقليدية في الأصل، مستغلين الإمكانيات الهائلة لهذه المستحدثات، أو استحداث صور أخرى من الإجرام يرتبط بهذه التقنيات التي تصير محلا لهذه الجرائم أو وسيلة لارتكابها، وقد تزايدت معدلات هذه الجرائم في العقدين الآخرين على وجه الخصوص، بصورة أدت إلى بزوغ فجر ظاهرة إجرامية جديدة، تعرف بالإجرام المعلوماتي أو الإجرام الإلكتروني.

فظهر السطو على البنوك بمساعدة هذه الوسائل المستحدثة، ونمت الجريمة المنظمة وترعرعت في ظل هذه الثورة العلمية في مجال المعلومات والاتصالات، على وجه الخصوص في مجالات الإرهاب وتجارة المخدرات، والاتجار بالسلاح والدعارة المنظمة باستخدام الإنترنت، وارتكبت العديد من الجرائم التقليدية كالسرقة والنصب وخيانة الأمانة، وتزوير المحررات، والاعتداء على حرمة الحياة الخاصة، وعلى البيانات الشخصية، والتجسس، وظهرت جرائم ملازمة لهذه المستحدثات، منها الغش الإلكتروني، بالتلاعب في المدخلات وفي البرامج، والنسخ غير المشروع للبرامج، والعديد من الجرائم المتعلقة بالتجارة الإلكترونية، وإتلاف الأجهزة الإلكترونية، وإتلاف السجلات المدونة على الحاسب الآلي، وبث الصور أو الأفلام الجنسية من خلال الأجهزة، والقذف أو السب عن طريق الإيميل، وغسيل الأموال القذرة باستخدام النقود الإلكترونية.

المشاكل العملية: وخطورة هذه الظاهرة الإجرامية المستحدثة أنها تثير العديد من الأسئلة القانونية إذ أن الجريمة يسهل ارتكابها على هذه الأجهزة أو بواسطتها، وأن تنفيذها لا يستغرق غالبا إلا دقائق معدودة، بل و في أحيان كثيرة تتم في بضع ثوان، وأن محو آثار الجريمة وإتلاف أدلتها غالباً ما يلجأ إليه الجاني عقب ارتكابه للجريمة، فضلا عن أن مرتكبي هذه الجرائم، وبالذات في مجال الجريمة المنظمة يلجئون إلى تخزين البيانات المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية مع استخدام شفرات أو رموز سرية لإخفائها عن أعين أجهزة العدالة، مما يثير مشكلات كبيرة في جميع الأدلة الجنائية وإثبات هذه الجرائم قبلهم

اتفاقية بودابست 2001 للجرائم الالكترونية: لما كانت شبكة الانترنت لا تخضع لأية حدود ولا لسيادة دولة وبالتالي للسيادة القانونية لدولة معينة ظهرت الجرائم الالكترونية على الصعيد الدولي فمرتكب الجريمة يكون في دولة مختلفة عن الدولة التي تقع فيها جريمته وأصبحت الجرائم منظمة **organised crime** الأمر الذي حدا بالمشرع الدولي للبحث عن إطار قانوني دولي يكون فيه التعاون بين الدول أمرا يكاد يكون ليس اختياريا لإيجاد حل لهذه الجرائم الحديثة وبتاريخ 20 نوفمبر 2000 تقدمت اللجنة الأوروبية

لمشكلات الجريمة **CDBC** ولجنة الخبراء في حقل جرائم التقنية–**CYBERCRIME** – **(pc-cy)** بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست 2001 (اتفاقية الجرائم الالكترونية – سايبر كرايم) وجدير بالذكر أن مشروع الاتفاقية للعامة قد طرح للحوار المجتمعي عن طريق مواقع عديدة أوروبية وأمريكية على شبكة الانترنت وذلك بغرض التشاور و التباحث وإبداء الرأي. ولا شك في أن الاتفاقية قد بذل فيها جهد واسع ومميز يذكر للاتحاد الأوروبي ومجلس أوروبا لاسيما في المسائل المتعلقة بجرائم الكمبيوتر وأغراضها منذ أواخر القرن الواحد والعشرون.

بناء الاتفاقية وأقسامها : سنتناول في هذا المقام التنظيم القانوني للاتفاقية متبعين منهج الشرح على المتون أي شرح نصوص الاتفاقية ، والبين من الاتفاقية أنها تتكون من مقدمة وأربعة فصول، استعرضت المقدمة فيها الأهداف العامة للاتفاقية و بواعثها ومرجعياتها السابقة وما تقوم عليه من جهود إرشادية وتوجيهية وتدابير محلية وإقليمية ودولية، جاء الفصل الأول لتغطية المصطلحات الأساسية (مادة 1)، تضمن الفصل الثاني الذي جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى ألوطني ثلاثة أقسام: الأول، ويضم المواد من 2– 13 ويعالج النصوص الموضوعية لجرائم الكمبيوتر والقسم الثاني ويضم المواد من 14– 21 وتتعلق بالقواعد الإجرائية والقسم الثالث ويضم المادة 22 وتعلق بالاختصاص. أما الفصل الثالث من الاتفاقية والذي جاء تحت عنوان التعاون الدولي، فقط تضمن قسمين، الأول تحت عنوان المبادئ العامة ويضم المواد من 23-28 والقسم الثاني ويتعلق بالنصوص الخاصة ويضم المواد من 29-35. أما الفصل الخامس فيتضمن الأحكام الختامية ويضم المواد من 36 – 48.

خطة الدراسة: تقتضي هذه الدراسة البحث في أنواع الجرائم الالكترونية (مبحث أول) الإجراءات القانونية (مبحث ثاني) التعاون الدولي (مبحث ثالث) و أخيرا الآثار القانونية للاتفاقية الدولية (مبحث رابع).

المبحث الأول
أنواع الجرائم الإلكترونية

قبل الحديث عن أنواع الجرائم الإلكترونية التي سردتها اتفاقية بودابست (ثالثا) لابد من معرفة أركان الجرائم الإلكترونية (أولا) ثم ماهية الجرائم الإلكترونية (ثانيا).

أولا: أركان الجريمة الالكترونية:

الركن المادي في جرائم الانترنت:

لا شك أن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال بالانترنت على الأقل في العصر الحالي وفي ضوء المعطيات التكنولوجية الموجودة الآن، وعادة ما تكون رقمية متصلة بالانترنت و هذا يتطلب معرفة بداية هذا النشاط والشروع فيه ونتيجته. فتجهيز الحاسب بوضع البرامج علية وتحميل برامج الاختراق ، أو إعداد هذه البرامج على الحاسب، وتهيئة الصفحات التي تحمل في طياتها مواد غير قانونية مثل الداعية للفجور أو الإخلال بالنظام أو الآداب العامة وتحميلها علي الجهاز المضيف Hosting Server ، كما يمكن أن توجد جريمة إعداد برامج فيروسات تمهيداً لبثها حتى لو لم يتم بثها على الشبكة العنكبوتية.

بداية النشاط : والجرائم الالكترونية ليست مثل أي جريمة تستلزم وجود أعمال تحضيرية، إذ أنة يصعب الفصل بين العمل التحضيري والبدء في التنفيذ أو النشاط الإجرامي في جرائم الكمبيوتر والانترنت – حتى ولو كان القانون لا يعاقب علي الأعمال التحضيرية- إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشئ. فشراء برامج اختراق، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال أو حتى بعض الفيروسات التي لم يتم إطلاقها على الشبكة الالكترونية، كل هذه الأفعال تمثل جريمة في حد ذاتها.

النتيجة الإجرامية: و هنا يلاحظ أن مسألة النتيجة الإجرامية في جرائم الانترنت تثير مشاكل عدة، فعلي سبيل المثال مكان وزمان تحقق النتيجة الإجرامية. فلو قام أحد المجرمين في بلد ما باختراق جهاز خادم Server احد الشركات في أوروبا، وهذا بلد موجود في كندا فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد الشركة أم توقيت الجهاز الخادم، و القانون الواجب التطبيق في هذا الشأن.

الركن المعنوي في جرائم الانترنت:

العلم و الإرادة. الركن المعنوي هو علم الجاني بالفعل الإجرامي أي الحالة النفسية له، و كل ما يربط بين ماديات الجريمة وشخص الجاني، وقد قنن الفقه والقضاء الفرنسي مبدأ أو منطق سوء النية في شان جرائم الانترنت، حيث يشترط المشرع الفرنسي وجود سوء نية في الاعتداء أيا ما كان نوعه سواء كان علي بريد إلكتروني خاص أو عام مفتوح أم مغلق، فالعبرة هي وجود سوء النية.

أما المشرع الأمريكي فيأخذ في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم. فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا أخري اخذ بالعلم مثلما هو الحال في قانون مكافحة الاستنساخ الأمريكي.

وقد تواتر الفقه على الحديث عن دعوى موريس الذي كان متهما في قضية دخول غير مصرح به علي جهاز حاسب فيدرالي وقد دفع محامي موريس علي انتفاء الركن المعنوي، و ذلك بناءاً على المعيار التقليدي للقصد الجنائي في الجرائم التقليدية خارج الشبكة، 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** أي أن الجاني قد دخل بدون تصريح إلى جهاز غير مصرح بالدخول إلية، وكذا معيار **العلم** أي أن الجاني كان يعلم أيضا بوجود حظر علي استخدام هذه النظم فلا شك أن التطور التكنولوجي أدى أيضا لتطور النظام القانوني المصاحب له.

ثانيا : ماهية الجرائم الإلكترونية :

لا يزال يوجد خلاف بين الفقه حول الجرائم الالكترونية و لسنا هنا في مجال للتطرق إلية، ولكن ما يعنينا هو ماهية الجرائم الالكترونية وإن كان يمكن تلخيص ذلك إلى نوعين، منها ما يتم ضد الحواسب الآلية (أولا) و منها ما يتم باستخدام هذه الحواسب (ثانيا).

أولا : الجرائم التى تتم ضد الحواسب الآلية ونظم المعلومات:

يمكن إجمال هذه الجرائم إلى ثلاث جرائم :

(1) جرائم الاعتداء على الأشخاص:

جرائم الاعتداء على الأشخاص ليست كما هو الحال خارج الشبكة الإلكترونية أي وجود اعتداء مادي و إنما المقصود بالاعتداء هنا هو السب و القذف و التشهير و بث أفكار و أخبار من شانها الإضرار الأدبي أو المعنوي بالشخص أو الجهة المقصودة.

فالدخول على الموقع الشخصي لأحد الأشخاص للتشهير به وتغيير محتوياته والذي يندرج تحت الجرائم التي تتم ضد الحواسب و الشبكات أو عمل موقع أخر يتم نشر أخبار ومعلومات غير صحيحة والذي يندرج تحت الجرائم باستخدام الحواسب الآلية والشبكات والذي غالبا ما يتم من خلال إحدى مواقع الاستضافة المجانية لصفحات الانترنت والتي أصبح عددها بالآلاف في كافة الدول المتصلة بالانترنت والتي تسمى (Free Web Hosting Services).

وليس أدل على ذلك ما حدث في مصر لموقع البنك المركزي المصري على شبكة الانترنت حيث قام المهاجم بالدخول بصورة غير مشروعة على جهاز الخادم الذي يتم بث الموقع منه مستغلا إحدى نقاط الضعف فيه و قام بتغيير الصفحة الرئيسية للموقع الأمر الذي أحدث بلبلة في أوساط المتعاملين مع البنك خوفا من أن يكون الاعتداء قد امتد إلى المعاملات البنكية الأخرى.

كذلك توجد عدة صور لهذه الجريمة التي تمثل اعتداء على الملكية الفكرية للأسماء ما يحدث من اعتداءات على أسماء مواقع الانترنت (Domain Names) حيث أن القاعدة العالمية في تسجيل أسماء النطاقات (والتي تتم أيضا باستخدام بطاقات الائتمان من خلال شبكة الانترنت) هي أن التسجيل بالأسبقية وليس بالأحقية (First Come First Served) الأمر الذي أحدث الكثير من المخالفات التي يتم تصعيدها إلى القضاء وبتدخل من منظمة الايكان التي تقوم بتخصيص عناوين وأسماء المواقع على شبكة الانترنت ICANN (Internet Corporation for Assigned Names and Numbers) وذلك من اجل التنازل عن النطاق للجهة صاحبة الحق مع توقيع العقوبة أو الغرامة المناسبة و إن كان قد تم تلافي ذلك الآن.

يحدث أيضا في تسجيل النطاقات عبر الانترنت والتي يتم تسجيلها لمدد تتراوح من عام إلى تسعة أعوام أن لا تنتبه الجهة التي قامت بالتسجيل إلى انتهاء فترة تسجيل النطاق ووجوب التجديد حيث توجد شركات يطلق عليها صائدو النطاقات (Domain Hunters) تقوم بتجديد النطاق لها ومساومة الشركة الأصلية في التنازل عليه نظير ألاف الدولارات مستغلة اعتماد الشركة على هذا الاسم و معرفة العملاء به لمدد طويلة هذا فضلا عن الحملات الدعائية له وكم المطبوعات الورقية التي أصدرتها الشركة و تحمل ذلك العنوان.

مثال أيضا للجرائم الأخرى المتعلقة بأسماء النطاقات على شبكة الانترنت ما يعرف بإعادة التوجيه (Redirection) أي توجيه المستخدم إلى مكان أخر غير الذي يريد الدخول إلية مثلما حدث لموقع شركة Nike في شهر يونيو عام 2000 حيث قامت جماعة من المحترفين بالدخول على موقع شركة تسجيل النطاقات الشهيرة و المعروفة باسم (Network Solutions) و تغيير بيانات النطاق لضعف إجراءات امن المعلومات بالشركة في ذلك الحين

و بذلك تم إعادة توجيه مستخدمي الانترنت إلى موقع لشركة انترنت في اسكوتلاندا.

(2) جرائم تطوير و نشر الفيروسات:

وهي أيضا من الجرائم الخطيرة والتي تدمر أجهزة الحاسبات و تضعف إمكانياتها وبدايتها في منتصف الثمانينات من القرن الماضي في باكستان على أيدي اثنين من الإخوة العاملين في مجال الحواسب الآلية واستمرت الفيروسات في التطور والانتشار حتى بات يظهر العديد شهريا. والتي تعددت خصائصها وأضرارها فالبعض ينشط في تاريخ معين والبعض الأخر يأتي ملتصقا بملفات عادية وعند تشغيلها فان الفيروس ينشط و يبدأ في العمل الذي يختلف من فيروس لأخر بين أن يقوم بإتلاف الملفات الموجودة على القرص الصلب أو إتلاف القرص الصلب ذاته أو إرسال الملفات الهامة بالبريد الالكتروني و نشرها عبر شبكة الانترنت.

ظهرت مؤخرا نسخ مطورة من الفيروسات تسمى الديدان التي لديها القدرة على العمل والانتشار من حاسب لأخر من خلال شبكات المعلومات بسرعة رهيبة وتقوم بتعطيل عمل الخوادم المركزية والإقلال من كفاءة وسرعة شبكات المعلومات أو إصابتها بالشلل التام.
النوع الأخر والذي يدعى حصان طروادة (Trojan Horse) يقوم بالتخفي داخل الملفات العادية ويحدث ثغرة أمنية في الجهاز المصاب تمكن المخترقين من الدخول بسهولة على ذلك الجهاز والعبث بمحتوياته ونقل أو محو ما هو هام منها أو استخدام هوية هذا الجهاز في الهجوم على أجهزة أخرى فيما يعرف بالـ(attack Leapfrog) والذي يتم من خلال الحصول على عنوان الانترنت الخاص بجهاز الضحية ومنه يتم الهجوم على أجهزة أخرى (IP Spoofing).

(3) جرائم الإضرار بالبيانات:
هذا الفرع من الجرائم الالكترونية من أشد الأنواع خطورة و تأثيرا وأكثرها حدوثا وتحقيقاً للخسائر للإفراد والمؤسسات. بل لا نغالي أن قلنا أن غالبية الجرائم الإلكترونية توجد هنا ويشمل هذا الفرع كل أنشطة تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانات الموجودة بصورة الكترونية (Digital Form) على الحواسب الآلية المتصلة أو غير المتصلة بشبكات المعلومات أو مجرد محاولة الدخول بطريقة غير مشروعة عليها.

وهذا النوع من الجرائم له عدة أشكال وإن كنا نحصر تأثيره في أمرين الأول سلبي والثاني إيجابي.

التأثير السلبي: هو الدخول و الخروج من و إلى أنظمة المعلومات وقواعد البيانات بصورة غير مشروعة دون إحداث أي تأثير سلبي عليها. (ويقوم بذلك النوع من الأنشطة ما يطلق عليهم المخترقون ذوى القبعات البيضاء (White Hat Hackers) الذين يقومون بالدخول بطريقة غير مشروعة على أنظمة الحاسب أو شبكات المعلومات أو مواقع الانترنت مستغلين بعض الثغرات في تلك النظم مخترقين بذلك كل سياسات و إجراءات أمن المعلومات التي يقوم بها مديري تلك الأنظمة والشبكات (System And Network Administrators) وكما ذكر عدم ارتباط ذلك النشاط بالشبكات فاختراق الأمن الفيزيقي للاماكن التي يوجد بها أجهزة الحاسب التي تحتوى على بيانات هامة بالرغم من وجود إجراءات أمنية لمنع الوصول إليها و بمعنى أخر وصول شخص غير مصرح له و إمكانية دخوله إلى حجرة الحواسب المركزية بالمؤسسة ثم خروجه دون إحداث أي أضرار

فانــه يعتبــر خــرق السياســة وإجــراءات امــن المعلومات بتلك المؤسسة)[1].

التــأثير الايجــابي: تعـديل أو محـو أو سـرقة أو إتلاف أو تعطيل العمل لنظم المعلومـات فان تلك الأنشـطة تـتم بواسـطة أفـراد هـواه أو محترفـون يطلـق علـيهم المخترقـون ذوى القبعـات السـوداء (Black Hat Hackers) الذين قد يقومون بهذه الأعمال بغرض الاستفادة المادية أو المعنوية من البيانـات والمعلومـات التـي يقومـون بالاسـتيلاء عليهـا أو بغـرض الإضـرار بالجهـة صـاحبة تلـك الأنظمة لوجود كره شخصـي أو قبلـي أو سياسـي أو دينـي أو القيـام بـذلك لحسـاب احـد المؤسسـات المنافسة.

مثـال علـى ذلـك مـا ذكـره مكتـب التحقيقـات الفيدراليـة الأميريكـي (FBI) فـي السـادس والعشـرون مـن سـبتمبر عـام 2002 مـن القـبض علـى احـد عملائهـا و يـدعى ماريوكاسـتللو 36 عامـا ومحاكمتـه بتهمـة تخطـى الحـاجز الأمنـي

المسموح له به والدخول على احد أجهزة المكتب سـتة مـرات بغـرض الحصـول علـى بعـض الأموال.

كذلك (فإن تعطيل العمل و الذي يطلق عليه الـ (Denial Of Service Attack) واختصاراً الـ (Dos) والذي يعتمد على إغراق أجهزة الخوادم بـالآلاف أو ملايـين طلبـات الحصـول علـى معلومـات الأمـر الـذي لا تحتملـه قـدرة المكونـات الماديـة (Hardware) أو نظـم قواعـد البيانـات والتطبيقات والبرامج موجودة على تلك الخوادم التي تصاب بالشلل التام لعدم قدرتها على تلبية هذا الكم الهائل من الطلبات و التعامل معه)[2].

ثانيـا : الجـرائم التـي تـتم باسـتخدام الحواسـب الآلية نظم المعلومات:

(1) جـرائم الاعتـداء و التشـهير و الأضـرار بالمصالح الخاصة والعامة:

أ- هـذه الطائفـة مـن الجـرائم يكـون فيهـا الاعتـداء والتشـهير بالأنظمـة السياسـية والدينية مستمر ولعل أشهر تلك الوقائع قيام بعض الهواة بوضع بعض البيانـات فـي شـكل صـور مـن القـران الكـريم وبـدءوا فـي الإعـلان عنهـا مـن خـلال إحـدى مواقـع البـث المجـاني الشـهيرة وهـو موقـع شـركة **Yahoo** وعنوانـه **(http://www.yahoo.com)** الأمر الـذي استدعى تـدخل الكثيـر مـن الـدول العربيـة و الأزهـر الشـريف والمجلـس

الأعلـى للشـئون الإسـلامية والكثيـر مـن الجهـات الإسـلامية الأخـرى فـي شـتى بقـاع الأرض إلـى مخاطبـة المسـئولين عـن الموقـع وتـم بالفعـل إزالـة تلـك الصـفحات ووضـع اعتـذار رقيـق بـدلاً منها.

ب- أيضـا جـرائم الاعتـداء علـى الأشـخاص والتشـهير بهـم و التـي تـتم باسـتخدام الحواسب الآلية و الشبكات.

ج- انتهـاك حقـوق الملكيـة الفكريـة لبـرامج الحاسـب والمصـنفات الفنيـة المسـموعة والمرئية ونشرها وتداولها عبر شبكات

[1]- http://www.tashreaat.com/view_studies2.asp?id=591&std_id=90

[2]-http://www.tashreaat.com/view studies2.asp?id=591&std_id=90

الانترنت فيما يعرف بالقرصنة الأمر الذي يلحق الضرر المادي والمعنوي بالشخص أو الجهة مالكة تلك المواد.

ج- التخابر أو الاتصال بين أفراد منظمة أو نشاط يهدد امن و استقرار الدولة أو نشاط محرم قانونا مثل شبكات الدعارة والشذوذ التى باتت وسيلة الاتصال الرئيسية لها هي حجرات الدردشة (**Chatting Rooms**) المنتشرة عبر شبكة الانترنت.

(2) <u>جرائم الاعتداء على الأموال:</u>

أ- ظهرت الكثير من الجرائم الالكترونية التي تقوم بالاعتداء على المؤسسات المالية، فبعد أن تمت ميكنة نظم الإدارة والمحاسبة وربط الأفرع المختلفة لتلك المؤسسات بعضها ببعض من خلال شبكات المعلومات لضمان سهولة و يسر إدارة العمليات المالية داخلها وفي تعامل تلك المؤسسات مع العملاء عن بعد فقد تم تحقيق ذلك عن طريق الاتصال المباشر من خلال شبكات المعلومات الخاصة غير المتاحة لمستخدمي الانترنت (**Private Networks**) التي كان لها بعض القيود المكانية للاتصال أو من خلال شبكة الانترنت من خلال تواجد واجهة لتلك التعاملات (**Web Interface**).

ب- كما لا يجب أن ننسى أيضا أنة تم دخول بطاقات الائتمان و الدفع الالكتروني (**Credit Cards**) بأنواعها المختلفة لتسهيل المعاملات والتوجه للإقلال من التعاملات بالنقد المباشر في إطار التحول إلى المجتمع اللا نقدي (**Cash-less Society**) وظهور الأسواق الالكترونية (**Electronic Marketplace**) لتسويق وبيع السلع والخدمات ونتيجة ذلك ظهور خدمات كثيرة يمكن أن تؤدي من خلال الشبكة مثل الاشتراك في النوادي الخاصة أو الاشتراك في مسابقات علي الشبكة أو لعب القمار أو ألعاب أخري نظير أجور محددة كما تعد ظاهرة غسل الأموال المتحصلة من أنشطة غير مشروعة من أبرز الأنماط الإجرامية المستحدثة التي تقوم بها شبكات منظمة تمتهن الإجرام وتأخذ درجات عالية من التنسيق والتخطيط والانتشار في كافة أنحاء العالم. وتشير إحصائيات الأمم المتحدة وصندوق النقد الدولي إلي أن أكثر من 30 مليار دولار أمريكي من الأموال القذرة تغسل سنوياً عبر الانترنت مخترقة حدود 67 دولة في العالم.

<u>ثالثا: أنواع الجرائم الالكترونية التى ضمنتها اتفاقية بودابست:</u>

الفصل الثاني من الاتفاقية والمعنون (المعايير المتعين إتباعها على المستوى الوطني – measures to be taken at the national level) تضمن أقساما ثلاث، **الأول حول التدابير الموضوعية، والثاني حول التدابير الإجرائية، والثالث حول الاختصاص**، وبهذا الفصل تكون الاتفاقية قد قدمت الإطار القانوني للتدابير التشريعية الموضوعية والإجرائية المتعين اتخاذها لمواجهة جرائم الكمبيوتر والانترنت في حالة انضمام أي دولة لهذه الاتفاقية.

أوجدت الاتفاقية نوع جديد من التقسيمات بشان جرائم الكمبيوتر المختلفة وأحكامها (القواعد

الموضـوعية)، وتضـمن بشـكل واضـح أربـع طوائف رئيسة لجرائم الكمبيوتر، وأخرى خامسة تتعلق بأحكام المساهمة والعقوبات لهذه الجرائم الأربعة، ويجري تقسيم هذه الطوائف على النحو التالي:-

الطائفة الأولى – العنوان الأول : - الجرائم التي تستهدف عناصر امن المعلومات وهي السرية والسلامة وتوفر معطيات نظم الكمبيوتر، وتشمل جريمـة الـدخول غيـر القـانوني (مـادة 2) والاعتراض غير القانوني (مادة 3) والتدخل في المعطيات (مادة 4) والتدخل في نظم الحاسوب (مادة 5) وإساءة استخدام الأجهزة (مادة 6) .

الطائفـة الثانيـة – العنـوان الثـاني: - الجـرائم المرتبطة بـالكمبيوتر ، وتشمل التزوير المرتبط بـالكمبيوتر (مـادة 7) والاحتيـال المـرتبط بالكمبيوتر (مادة 8) .

الطائفـة الثالثـة – العنـوان الثالـث : - الجـرائم المرتبطة بالمحتوى ، وتشمل صورة واحدة من هذه الجرائم هي جرائم دعارة الأطفال (المادة9).

الطائفـة الرابعـة – العنـوان الرابـع : - الجـرائم المرتبطـة بحـق المؤلـف والحقـوق المجـاورة وتشمل الجرائم الجنائية التي تعد اعتداءا على المصـنفات المحميـة بحـق المؤلـف والحقـوق المجاورة (مادة 10) .

الطائفـة الخامسـة – العنـوان الخـامس: - المساهمة الجرمية والعقوبة ، ويعالج هذا الجزء الشـروع attempt والمسـاعدة aiding والتحـريض abetting (مـادة 11) ومسـؤولية الأشـخاص المعنويـة corporate liability (مادة 12) ومعايير العقاب sanctions and measures (مادة 13) .

ولا يزال الخلاف لا ينتهي حول تقسيم طوائف جـرائم الكمبيـوتر وتصـنفيها الأمـر الـذي حـدا بمشرعي الاتفاقية أن يقوموا بعمل حصر مبدئي للجرائم، مع الوضع في الحسبان تطور المنظومة الآليـة واحتماليـة تغيـر الجـرائم فـي المسـتقبل، وبغـض النظـر عـن التقسـيم الأكـاديمي، فـان الاتفاقية وضعت هذه النصوص التجريمية تطبيقا لمبدأ لا عقوبة ولا جريمة إلا بنص .
واستنادا إلـى المـواد المشـار إليهـا (2-13) فـان الاتفاقية تلزم الدول الأعضـاء فيهـا (دول الاتحـاد الأوروبي وأية دولة توقع عليها أو تريد أن تنضم إليهـا) باتخـاذ الإجـراءات والتـدابير التشـريعية الملائمـة لتجـريم تسـع جـرائم فـي ميـدان الجـرائم المعلوماتية وهي:-

1– الـدخول غيـر القـانوني المتعمـد : وقـد اسـتخدمت الاتفاقيـة مصـطلح illegal access في حين أن غالبية إن لم يكـن جميـع التشـريعات الوطنيـة تسـتخدم تعبيـر الدخـول غـير المصـرح بـه unauthorized access ، وذلك بالدخول المتعمد إلى أي نظام كمبيوتر أو جزء منه دون حـق أو إذن سـواء أكـان بنيـة انتهـاك وسـائل الأمـن infringing security megsures أو بنيـة الحصـول علـى معطيـات الكمبيـوتر أو لأيـة نيـة غيـر مشروعة (مادة 2).

2 – الاعتـراض غيـر القـانوني illegal interception المتعمد ودون حق بواسـطة وسـائل تكنولوجيـة technical means للبيانات المرسلة غير العامـة non-public إلـى أو مـن نظـام كمبيـوتر وكـذلك اعتـراض الإشـعاعات الكهرومغناطيسـية المنبعثـة مـن أي نظـام كمبيـوتر تحمـل مثـل هـذه المعطيـات. (مادة3).

3 – التدخل المتعمد أو الإرادي في المعطيات data interference بالتدمير damaging أو الحذف deletion أو التشويه والإفساد deterioration أو تبديلها أو تغيرها أو تعديلها alteration أو تعطيلها أو كبتها أو إخمادها supperession ، "وقد ذهبت لجنة الخبراء إلى أن تعديل البيانات يشمل خلطها (الغش) أما تعطيل أو إخماد أو كبت البيانات فيتعلق بإجراءات منع وصولها إلى العنوان المرسلة إليه كحذف جزء منها على نحو لا يتيح وصولها إلى الموضع الفيزيائي المطلوب أو تصبح غير قادرة على ذلك أو منع الغير من الوصول إليها وذهب بعض الخبراء إلى وجوب اشتراط حصول الضرر جراء التدخل في البيانات كعنصر من عناصر التجريم إلا أن النص لم يشر لهذا العنصر فجرم كل تدخل في المعطيات على أن يكون مقصودا (المادة 4) "[3].

4 – التدخل المتعمد في الأنظمة system interference وهنا نقوم ببث وإرسال inputting or transmitting (مادة 5) ذات الأفعال المشار إليها في المادة 4 المتعلقة بالتدخل في المعطيات بغية تعطيل أداء وعمل الأنظمة بالتدمير والحذف والتعديل والتعطيل.

5 – إساءة استخدام الأجهزة Misuse of devices، (مادة 6) سبق وسميت هذه الجريمة في المسودات الأولى للاتفاقية السابقة (الأدوات غير القانونية illegal devices) وإن كان بعض يرى أن هذا العنوان أكثر دقة[4]، وتحتوى هذه الجريمة على نوعين من الأفعال الأولى المنصوص عليها في الفقرة الأولى من المادة السادسة وتشمل الإنتاج المتعمد production أو بيع sale أو شراء procurement أو استخدام use أو استيراد import أو توزيع distribution أو غير ذلك من أدوات ووسائل توفير الأجهزة بما فيها برامج الكمبيوتر بهدف ارتكاب أية فعل إجرامي من الأفعال المنصوص عليها في المواد 2-5 المشار إليها سابقا وكذلك كلمات السر computer password ورموز الدخول access code أو أية برامج مشابهة بحيث تتيح اختراق نظام الكمبيوتر أو الدخول إليه أو إلى أي جزء منه بنية ارتكاب أي فعل من الأفعال المنصوص عليها في المواد 2-5، كما تشمل هذه الجريمة وفق الفقرة الثانية من المادة 6 الحيازة والتملك لأي عنصر أو أداء مما ورد ذكره في الفقرة الأولى أعلاه بنية ارتكاب أي من الأفعال المشار إليها في المواد 2-5 من الاتفاقية .

6 – التزوير المتعمد باستخدام جهاز الكمبيوتر computer-related forgery وذلك بإدخال أو تعديل أو حذف أو إخفاء بيانات الكمبيوتر على نحو يظهر بيانات غير أصلية لتكون مقبولة قانونا وكأنها بيانات أصلية وبغض النظر عما إذا كانت هذه البيانات مقروءة أو غير مقروءة ويحق للدولة أن تشترك نية أو قصد الغش لقيام المسؤولية الجنائية (مادة 7) .

7 – الاحتيال المتعمد باستخدام الكمبيوتر computer-related fraud بدون حق وعلى نحو يسبب خسارة الغير لممتلكاته عن طريق إدخال أو حذف أو تعديل أو كتم

[3]- د. يونس عرب قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان www.arablaw.org

[4]- د. يونس عرب المرجع السابق

بيانات الكمبيوتر أو من خلال التدخل بعمليات نظام الكمبيوتر أو برامجه بنية الحصول على منفعة اقتصادية economic benefit لنفسه أو لغيره (مادة 8) .

8 – الجرائم المرتبطة بدعارة الأطفال offences related to child pornography ، وهنا يلاحظ أولا أن هناك جرائم كثيرة في المحتوى إلا أن الاتفاقية نصت عليها صراحة على الرغم من إن عددا من التشريعات في عدد من الدول اتجهت إلى تجريم أفعال أخرى كالمقامرة على الشبكة أو إثارة الأحقاد والفتن وغيرها ، إلا أن مشرعي الاتفاقية اقتصروا في جرائم المحتوى على هذه الجريمة فقط ، فقضت في المادة التاسعة منها بوجوب اتخاذ الدولة المنظمة للاتفاقية التدابير التشريعية لتجريم قيام أية شخص وبشكل قصدي (عمدي) عرض offering أو توزيع distributing أو نقل transmitting أو غير ذلك من الأفعال التي من شأنها أن توفر أو تتيح توفير المواد الإباحية المتعلقة بالأطفال child pornography من خلال نظام كمبيوتر وتجريم إنتاج مواد دعارة الأطفال بغرض توزيع عبر نظام الكمبيوتر ، ولا شك أن تفسير تلك الجريمة يؤدى إلى أن عرض المواد الإباحية يتضمن كذلك إعطاء معلومات حول وسائل العرض والاتصال هذه المواد وكذلك ربط المواقع بمداخل إلى مواقع إباحية تعرض هذه المواد ، أما فيما يتعلق بالجدل حول مفهوم المواد الإباحية المتعلقة بالأطفال وما تشمله فمثلما هو الحال في المفاوضات الدولية حينما تختلف الثقافات وتتنوع و تصل لحد عدم الاتفاق يتم ترك ذلك للنظم الوطنية حسب قواعد النظام والآداب العامة لكن تم الاتفاق أنها تشمل كل مادة جنسية (وقد جرى ضرب أمثلة واسعة منها) تتعلق بالاتصال الجنسي بالأطفال وفي ضوء الخلاف حول المحتوى ونطاقه ، جرى الاتفاق على معايير الحد الأدنى التي نص عليها في الفقرتين الثانية والثالثة من ذات المادة ، فقضت الفقرة الثانية من المادة 9 على أن مواد دعارة الأطفال تشمل أية مواد تظهر بشكل مرئي قيام القاصر بتصرفات جنسية أو ظهور أي شخص باتصال أو تصرف جنسي مع قاصر وكذلك الصور الواقعية realistic التي تمثل أو تظهر قاصرا يتدخل بتصرف جنسي. أما الفقرة الثالثة فقد قررت أن المقصود بالقاصر minor يحدد تبعا للقانون الداخلي للدول الأعضاء على أن يتضمن في جميع الأحوال الأطفال (الأشخاص) دون سن الثامنة عشرة ، وللدول الأعضاء اعتماد حد أدنى اقل على أن لا يقل عن 16سنة ، وكان قد ثار الجدل حول الحد الأدنى للسن فاقترح أن يكون 16 أو 18 أو 14 سنة فتم التوفيق بين الآراء المتعارضة بإتاحة الفرصة لكل دولة لتحديد السن على أن يكون حده الأدنى وفقا لما تقدم (المادة 9 بفقراتها الثلاث) .

9 – أخيرا الجرائم المرتبطة بحق المؤلف: copyright and related offences فقد أوجبت الاتفاقية في المادة 10 بفقرتيها الأولى والثانية - الأولى خاصة بحق المؤلف ، والثانية بالحقوق المجاورة - وجوب اتخاذ الدول المنظمة تدابير تشريعية تجرم الإخلال أو الاعتداء على حق المؤلف أو الحقوق المجاورة وفقا لما تحدده القوانين الوطنية للدول الأعضاء الموافقة مع اتفاقية بيرن لحماية المصنفات الأدبية والفنية واتفاقية تربس trips ، واتفاقية الوايبو لحق المؤلف WIPO copyright treaty

واتفاقيـة الوايبـو لـلأداء والفنوغرامـات WIPO performances and phonograms treaty ، ويشـترط أن تكـون هـذه الأفعـال قـد ارتكبـت عمـدا intentionally وبغـرض تجـاري commercial seale وباسـتخدام نظـام الكمبيوتر .

وقد أوجبت الاتفاقية على الدول الأعضاء أو الدول التي تريد الانضمام إلى الاتفاقية اتخاذ التدابير التشريعية لتجريمها ومكافحتها ، وهذه الجرائم بوجه عام شملت طوائف جرائم الكمبيوتر المتعارف على وصفها بجرائم التقنية الاقتصادية وكذلك جرائم الملكية الفكرية التي تستهدف المصنفات الرقمية ، وكذلك ما يعرف بجرائم المحتوى الضار أو غير القانوني، أي إن الاتفاقية غطت الثلاث موجات التشريعية في حقل جرائم الكمبيوتر و لم تتطرق الاتفاقية لجرائم الخصوصية أو الاعتداء على البيانات الشخصية المخزنة في نظم المعلومات والسبب في ذلك وجود الاتفاقية الأوروبية لحماية البيانات ووجود قواعد تشريعية للاتحاد الأوروبي ومجلس أوروبا والمفوضية الأوروبية وكذلك لدى الدول الأعضاء في هذه المنظمات في ميدان حماية الحق في الخصوصية من مخاطر المعالجة الآلية للبيانات وكذلك القواعد التنظيمية لانتقال البيانات عبر الحدود ومبادئ جمعها وتخزينها ومعالجتها .

وقد تناولت الاتفاقية في المادة الحادية عشرة القواعد العامة المتعلقة بالمساهمة الجنائية والعقوبة بشأن الجرائم المشار إليها في المواد من 2 - 10 ، وقد أوجبت الاتفاقية على الدول الأعضاء اتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع والتدخل والتحريض في ارتكاب هذه الجرائم أو ما تختاره الدولة منها وذلك بغرض وجود رادع عام لما لهذه الجرائم من تأثير شديد على اقتصاديات الدول وكذلك النص على مسؤولية الأشخاص المعنوية عن الأفعال التي ترتكب لمصلحة الشخص المعنوي من قبل أي شخص الذي يتصرف لمصلحته سواء كان استنادا إلى تمثيل قانوني أو باعتباره مناطا به اتخاذ القرار عن الشخص القانوني أو لأنه خاضع لسلطته بما في ذلك أفعال التحريض والتدخل والمساعدة الجنائية ، وكذلك مسؤولية الرؤساء عن غياب أو تخلف الرقابة والإشراف والتحكم بتصرفات الأشخاص المعنيين بالعمل. ويلاحظ هنا أنه وفقا للاتفاقية يمتد نطاق المساءلة الجنائية للشخصين الطبيعي والمعنوي معا. أما بالنسبة للعقوبات والتدابير فقد أوجبت الاتفاقية على الدول الأعضاء في الاتفاقية إقرار العقوبات الملائمة والفعالة لهذه الجرائم بما فيها العقوبات المانعة للحرية بالنسبة للأشخاص الطبيعيين مثلما هو الحال في القانون الأمريكي والغرامات المالية بالنسبة للأشخاص المعنوية.

المبحث الثاني
الإجراءات القانونية
ـ

الدول المتقدمة تكنولوجياً وضعت قواعد موضوعية لمواجهة الاستخدام غير المشروع للكمبيوتر والإنترنت، وأجرت أيضاً تعديلات على قوانينها الإجرائية تكفل مكافحة جرائم الكمبيوتر والإنترنت في إطار الشرعية الجنائية، لأنها أدركت بأن هذه الجرائم تُرتكب بتقنيات حديثة في عالم يختلف عن العالم المادي الذي عادة ما تُرتكب فيه الجرائم عن طريق المجابهة بين الأشخاص كالقتل والإيذاء، وأن القانون الجنائي التقليدي بشقيه الموضوعي والإجرائي وضع من الناحية التاريخية لمكافحة الاعتداءات المادية والمواجهة وجهاً لوجه خلافاً لجرائم التكنولوجيا فترتكب في عالم افتراضي وعلى مسافات بعيدة.

أمـا الاعتمـاد علـى التشـريعات القديمـة، سـواء الموضـوعية أو الإجرائيـة، فـي مواجهـة جـرائم الكمبيـوتر والإنترنـت. فإنهـا تشـكل عقبـات لا يسـتطيع المحقـق الجنـائي التحـرر منهـا لكشـف طائفـة الجـرائم الجديـدة (جـرائم الكمبيـوتر والإنترنـت) مـن حيـث وسـيلة ارتكابهـا أو موضـوعها وضـبط أدلتهـا الماديـة وغيـر الماديـة وملاحقـة مرتكبيهـا، الأمـر الـذي أدى إلـى وضـع بـاب خصـت فيـه الاتفاقيـة الإجـراءات القانونيـة الواجب إتباعها عند ضبط هذه الجرائم.

فالتحقيق الجنائي الحديث في هذه الجرائم لم يعد ميسـوراً لكافـة المحققـين وبوسـائل وإجـراءات التحقيـق التقليديـة لأنـه يواجـه تقنيـات حديثـة فـي أسلوب وطريقة بل و مدة ارتكاب الجريمة الأمر الذي يقتضي إحداث تطوير في قانون الإجراءات يستوعب الإجراءات والوسائل الحديثة في كشف الجريمـة وضـبط فاعليهـا بمـا يواكـب اسـتخدام وسـائل التقنيـة والاتصـالات الحديثـة فـي ارتكـاب الجـرائم. وعلـى ذلـك فـإن أهـم الإجـراءات التـي يُعتمد عليها في جمع الأدلـة فـي جرائم الكمبيوتر والإنترنت والتي يثير اتخاذها بعض الإشكاليات وهي المعاينة والتفتيش والضبط وندب الخبراء.

وتناولـت الاتفاقيـة فـي قسـمها الثـاني الجانـب الإجرائـي أي القواعد الإجرائيـة Procedural law وسنتناول هنـا أيضـا بأسلوب الشرح علـى المتـون كمـنهج أهـم القواعـد الإجرائيـة الخاصـة بجمع الأدلـة باعتبارهـا قواعـد لازمـة وضـرورية لكشف وضبط الجرائم الواقعة عبر نظم الاتصال والمعلومات . إذ أن جمع أدلة هذه الجرائم يجب أن تكون متكافئاً وموازياً مع أساليب ارتكابها مع الإشارة إلى ما قرره القانون الفرنسي والأمريكي مـن إجـراءات فـي مجـال البحـث فـي أجهـزة الكمبيوتر والحصول على الأدلـة الالكترونيـة في التحقيـق الجنـائي Searching and seizing computer and obtaining Electronic Evidence in Criminal Investigation

لا شـك فـي أن إتبـاع الإجـراءات التقليديـة مـن (معاينـة وتفتـيش وضـبط وغيرهـا) أصـبح أمـراً عسيراً في جمع أدلة جرائم الكمبيوتر والانترنت (cyber crime) وهـذا أمـراً طبيعيـاً إذ أن استخدام التقنيات الحديثة في ارتكاب هذه الجرائم يلزم بالضرورة استخدام نفس الوسائل في كشفها وضـبط أدلتهـا ولهـذا نصـت الاتفاقيـة الخاصـة بجـرائم الكمبيـوتر والانترنـت (cybercrime convention) علـى إجـراءات تحقيـق جديـدة (criminal investigation) تهدف إلي البحث عـن أدلـة هـذه الجـرائم وضـبطها إذ أن الوسـائل التقليدية للحصول على الأدلة غير ميسر للقائمين علـى مكافحـة هـذه الجـرائم. وغالبيـة هـذه الإجراءات حديثة وجديدة بل لا نغالي إن قلنا أنها تحتاج إلى تحديث دوري وهي غير مألوفة في القوانين الإجرائية التقليدية المستخدمة في جمع الأدلـة ويعبـر عنهـا بمصـطلحات بيئـة التقنيـة ولاشك بـان هـذه الإجـراءات تـتلائم مـع طبيعـة جـرائم التكنولوجيـا ولهـا دور مهـم فـي تحديـد مرتكبـي هـذه الجـرائم وجميـع الأدلـة ضـدهم بـل والأهم سرعة ضبطهم فعامل الوقت مهم جدا و غايـة فـي الخطـورة لضـبط هـذه الجـرائم ولهـذا تلاقى قبولا لدى الكافة إلا إنها يجب أن تتم وفقا لصحيح القانون وفي إطار التوازن بين استخدام الوسائل الحديثة فـي كشف الجرائم وجمع أدلتها وبـين الحريـة الشخصـية للأفـراد فالمبـدأ هـو لا جريمة ولا عقوبة إلا بنص. وتحقيقاً لذلك نصت الاتفاقيـة بضـرورة أن تتبنـى كـل دولـة طـرف الإجـراءات التشـريعية التـي تكفـل القيـام بتلـك الإجراءات مع مراعاة حقوق الإنسان وحرياته الأساسـية . ويمكـن تقسـيم الإجـراءات الجديـدة لجميع الأدلة إلـى نصت عليها اتفاقية بودابست بشان جرائم الكمبيوتر والانترنت إلى مجموعتين – الإجـــراءات الممهـــدة لجمـــع الأدلـــة – والإجراءات الخاصة بجمع الأدلة.

الفرع الأول: الإجراءات الممهدة لجمع الأدلة

ممكن تعريف هذه الإجراءات بالمراقبة والمتابعة لاستخدام وسائل تقنية الاتصالات الحديثة وتسجيل كافة البيانات المخزنة بالأجهزة المستخدمة في هذه الاتصالات (الكمبيوتر والانترنت) وهذه إجراءات تتخذ في الغالب قبل التحقيق في الجريمة ولا يعد اتخاذها تحريكاً للدعوى ضد أي شخص، ويتولى القيام بها مقدمو خدمات الكمبيوتر والانترنت بتكليف من السلطة المختصة (competent authority) وهى السلطات القضائية باعتبارها إجراءات لازمة وضرورية لتسهيل مهمة سلطة التحقيق من كشف تلك الجرائم والبحث عن أدلتها وضبطها مع الأخذ في الاعتبار عامل الوقت وقد نصت اتفاقية بودابست على نوعين من هذه الإجراءات وهى :-

- **إجراءات التحفظ السريع على مضمون البيانات المخزنة.**
- **إجراءات التحفظ على بيانات المتعلقة بخط سير البيانات.**

أولاً: إجراءات التحفظ السريع على مضمون البيانات المخزنة

تتمثل إجراءات التحفظ السريع على مضمون البيانات المخزنة expedited preservation of stored computer data في إصدار أوامر إلى مقدمي الخدمات في مجال الكمبيوتر والانترنت من أفراد وشركات بالحفاظ على البيانات المخزنة بمنظومة وأجهزة الكمبيوتر والانترنت لفترة زمنية معينة وقد نصت المادة 16 من اتفاقية بودابست على هذا الإجراء ((يجب على كل دولة طرف أن تتبنى الإجراءات التشريعية وأية إجراءات أخرى ترى أنها ضرورية لتخويل سلطاتها المختصة أن تأمر بالتحفظ العاجل على البيانات المخزنة)) والغرض من ذلك هو تمكين السلطة المختصة بالتحقيق في جرائم الكمبيوتر والانترنت من معرفة مضمون البيانات التي أرسلها المشترك أو استقبلها سواء عن طريق طلبها من مقدمي الخدمة أو خلال القيام بالتفتيش وهي في الغالب الأعم تكون من شهر إلى ثلاثة أشهر.

وعلى ذلك فان الأمر الذي تصدره السلطة القضائية المختصة أو غيرها إذا كان تشريع الداخلي للدولة يجعل الاختصاص بيد سلطة أخرى مثلا في الدولة يلتزم بمقتضاه مقدمي الخدمة بالحفاظ على البيانات وحمايتها من الضياع أو التعديل أو المحو وبالحفاظ على سريتها ومنع الغير من الحصول أو الوصول إليها. وتختلف مدة التحفظ على البيانات من تشريع لآخر، وإن كانت اتفاقية بودابست قد حددتها بمدة لا تتجاوز 90 يوماً (م 3/16) من الاتفاقية. ويختص بإصدار أمر التحفظ السلطة التي يحددها التشريع الداخل لكل دولة.

وقد نظم المشرع الأمريكي في القانون الخاص بمكافحة جرائم الكمبيوتر والانترنت الصادر تنفيذاً لاتفاقية بودابست إجراءات التحفظ على مضمون البيانات.

بأن نص عليه في المادة (18 2703 usc) ونص عليه المشرع الفرنسي في المادة 56 من قانون الإجراءات الجنائية.

ثانياً : إجراءات التحفظ السريع على البيانات المتعلقة بخط سير البيانات

يقصد بالتحفظ على البيانات المتعلقة بخط سير البيانات (expidious preservation of traffic data) إلزام مقدمي الخدمات من افرد وشركات بالحفاظ على البيانات والمعلومات المخزنة عن مصدر الاتصالات ووقتها ومقدمي

الخدمة الذين ساهموا في نقل البيانات ويرجع السبب في اتخاذ هذا الإجراء في انه يسهم في التعرف على مرتكبي الجرائم المعلوماتية والمساهمين معهم إذ أن مرتكب الجريمة قد يحاول إتلاف الأجهزة أو البرامج التي مكنته من ارتكاب جريمته. و المشكلة هنا عادة تكون أن هذا الإجراء يتطلب سعة تخزينه كبيرة وهي تكاد تكون قد حلت بالتكنولوجيا الحديثة و غالباً ما يتم تحديد مراقبة خط سير بيانات معينة السلطات المختصة بالتحري عنها ومتابعة أصحابها.

ويختلف إجراء التحفظ على البيانات المتعلقة بخط سير البيانات عن التحفظ السريع على مضمون البيانات الذي نصت عليه المادة 1/6 من اتفاقية بودابست في أن التحفظ يقتصر على البيانات المتعلقة بالاتصال من حيث مصدرها ووقتها ومرسلها ومستقبلها بمعنى أخر التحفظ يمكن الأجهزة المختصة من معرفة مرتكب الجريمة ومن ساهم في نقلها ولا يشمل محتوى البيانات وما تتضمنه من معلومات وهذا الإجراء كسابقه يحتاج إلى تقنية عالية تساعد مقدم الخدمة في القيام به في وقت سريع بغية إعطاء السلطة المختصة فرصة اتخاذ الإجراء اللازم لكشف مرتكب الجريمة وضبط أدلتها.

ولأهمية إجراء التحفظ على بيانات المتعلقة بخط سير البيانات قضت المادة 1/17 من اتفاقية بودابست على ضرورة تبنى الدول تشريعات تكفل قيام مقدمي الخدمات بالتحفظ السريع على البيانات المتعلقة بخط سير البيانات وقضت نفس المادة في فقرتها الثابتة ((بضرورة أن تتبنى الدول الإجراءات التي تتضمن قيام مقدم الخدمة بالإفشاء السريع لتلك البيانات للسلطة المختصة)) واستجابة لما قررته المادة 2،1/17 من اتفاقية بودابست نص عليه المشرع الأمريكي في المادة ((18 usc 2703 (F) ونص عليه كذلك قانون الإجراءات الفرنسي في 3/99.

الفرع الثاني: إجراءات جمع الأدلة:

نصت الاتفاقية في المواد 18، 19، 20،21 على مجموعة من القواعد الإجرائية بقصد التثبت من وقوع الجريمة والبحث عن مرتكبها وجمع أدلتها وهى أغلبها إجراءات جديدة ذات مسميات غير مألوفة في إجراءات التحقيق التقليدية وهي وان كانت لا تتضمن أي خرق أو قيد على حرية الأشخاص وحقوقه الأساسية إلا أن اتخاذها يحتاج إلى تشريع خاص يسمح بمباشرتها لمساسها بحقوق الإنسان وإعمالا لمبدأ لا جريمة و لا عقوبة إلا بنص.

ولما كان الحديث دائما عن حقوق الإنسان يثير الكثير من التساؤلات حول هل يجوز التنازل عن بعض الحقوق الشخصية و الحريات العامة في سبيل تحقيق سيادة القانون و النظام في سبيل توفير الأمان و أيهما أولى بالرعاية والتقديم هل هي الحرية أم الأمن و أن كان هذا ليس مجالنا و لكن ممكن بإيجاز شديد التأكيد على أن تحقيق الفعالية للنصوص اتفاقية بودابست الخاصة بمكافحة هذه الفئة من الجرائم بشكل عام يدعو إلى تغليب ما قررته اتفاقية بودابست من إجراءات في مجال البحث والتنقيب عن جرائم الكمبيوتر والانترنت على القواعد الخاصة بحماية حقوق الإنسان وحرياته الأساسية ونبين فيما يلي أهم إجراءات جمع الأدلة التي نصت عليها اتفاقية بودابست.

<u>أولاً :- إصدار أمر بتقديم بيانات محددة :</u>

قضت المادة 18 من اتفاقية بودابست على ضرورة أن تتبنى الدول تشريعات تلزم مقدم الخدمة وغيره من الأشخاص بتقديم بيانات معينة تكون في حيازتهم أو تحت سيطرتهم ومخزنة في منظومة الكمبيوتر أو دعامة التخزين وقد سلك المشرع الأمريكي ذلك فنص على هذا الإجراء

في المادة (18 usc 2703) والمقصود بإصدار أمر بتقديم بيانات محدده " production order to submit specified data تخويل السلطة المختصة كما سبق القول سلطة التحقيق أو غيرها إصدار أمر إلي مقدم الخدمة أو أي شخص في حيازته أو تحت سيطرته بيانات معينه تفيد في الكشف عن الجريمة بتقديم تلك البيانات سواء أكانت تتعلق بالمحتوى أو بخط السير ، وهذا الإجراء كغيرة من الإجراءات السابقة يصدر عن السلطات المختصة وينفذه أشخاص لا يتبعون هذه السلطة إذ هم عبارة عن أشخاص في حيازتهم أو تحت سيطرتهم بيانات مخزنه داخل منظومة الكمبيوتر computer system stored أو في دعامة تخزين المعلومات " computer data sotrage medieum " بمعنى أن الأمر يصدر لمقدمي الخدمة سواء كان صاحب الحيازة المادية للبيانات أو لصاحب السيطرة ولو لم يحوزها حيازة مادية .

ثانياً:- تفتيش وضبط البيانات المخزنة:

قضت المادة (19) من اتفاقية بودابست بضرورة ووجوب تبنى الدول الأطراف تشريعات في القوانين الإجرائية بها تخول أحد سلطاتها اختصاصات تكفل البحث عن أدلة الجريمة وضبطها وترد إجراءات التفتيش والضبط على البيانات المخزنة في النظام المعلوماتى للكمبيوتر أو في دعامة تخزين المعلومات سواء أكانت هذه البيانات مخزنة في جهاز واحد أو في منظومة اتصالات . وقد حددت هذه المادة الإجراءات الخاصة بجمع الأدلة في الأتي :-

1- التفتيش أو الدخول المشابه:

الحرية الشخصية حق طبيعي و هي مصونة لا تمس و فيما عدا حالة التلبس لا يجوز القبض على أحد أو تفتيشه إلا أمر تستلزمه ضرورة التحقيق و صيانة أمن المجتمع هكذا نصت جميع إن لم يكن كل دساتير العالم و هو أمر لا يخفي على المشرعين في الاتفاقية لذلك نصت المادة 1/19 من اتفاقية بودابست بوجوب أن تتبنى كل دولة طرف تشريعات تخول السلطة المختصة اختصاص التفتيش أو الدخول المشابه (search or similarly access) وتحديد مصطلح التفتيش لا يثير أية صعوبة، إذ يقصد به البحث والتنقيب عن أدلة الجريمة بفحص البيانات ومحاولة معرفة محتواها أو خط سيرها. أما المصطلح الجديد هنا و هو الدخول access وما يعبر عنه أحياناً بالولوج فهو مصطلح خاص بنظم التكنولوجيا والاتصال يحقق الوصول إلى البيانات المخزنة ويقتضيه بطبيعة الحال إجراء التفتيش والحصول على الأدلة. ولهذا يوجد فرق بين الاثنين، فالدخول إجراء للتفتيش والتفتيش وسيلة لجمع الأدلة و إن كان من الناحية العملية المصطلحان يرتبان حتميا عل بعضهما البعض. ورغم هذه التفرقة فإنهما يعتبران من إجراءات التحقيق الماسة بحقوق الأفراد. لذا يجب أن يستند اتخاذها إلى نص قانوني، وهذا ما نصت عليه المادة2/19. ولقد تبنى المشرع الأمريكي نظام التفتيش الذي نصت عليه اتفاقية بودابست كوسيلة للحصول المعلومات والبيانات في جرائم الكمبيوتر والانترنت لإضفاء صفة المشروعية (Legitimation) على الإجراءات المتخذة للبحث عن أدلة الجريمة بأن نص عليه في المادة (18 usc 2703) ونص عليه قانون الإجراءات الجنائية الفرنسي في المادتين (56)، (97).

2- الضبط أو الحصول:

وقد نصت المادة 3/19 من اتفاقية بودابست بوجوب أن تتبنى كل دولة طرف تشريعات تخول السلطة المختصة اختصاص الضبط أو الحصول (seize or secure similarly) على

البيانات المخزنة ويشمل هذا الاختصاص الإجراءات الآتية) :-

- الضبط أو الوصول إلى البيانات.
- التحقق والتحفظ على نسخة من البيانات.
- المحافظة على سلامة البيانات.
- منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتى.

ويمكن تقسيم الإجراءات التي نصت عليها المادة 3/19 إلى نوعين من الإجراءات :

أ- إجراءات مبدئية تحفظية : الهدف منها هو الحفاظ على البيانات المخزنة التي تكون لها أهميتها في التحقيق ببقائها في أمكنتها في النظام المعلوماتى للكمبيوتر أو في دعامة التخزين ومنع الوصول إليها أو إلغاؤها أو التصرف فيها وذلك للكشف عن مرتكب الجريمة و سهولة إثباتها علية.

ب- إجراءات لاحقة بالضبط : وهو إجراءات لاحقه للتفتيش والدخول ويقصد بها جمع البيانات سواء بأخذ دعامة تخزين المعلومات ذاتها أو يعمل نسخة من البيانات المخزنة بها أو بالنظام المعلوماتى للكمبيوتر في ورق أو أقراص .

وقد راعى الأمريكي أهمية الإجراءات التحفظية وإجراءات الضبط في تجميع أدلة جرائم الكمبيوتر والانترنت فنص عليه في المادة (18 usc 2703).

ثالثاً: التجميع فى الوقت الفعلى لبيانات خط سير البيانات:

قضت المادة (20) من اتفاقية بودابست على التجميع في الوقت الفعلي لخط سير البيانات (Real time collection of traffic data) وذلك بأن تتبنى الدول الأطراف في تشريعاتها ما يمكن السلطة المختصة القيام بما يمكنها من كشف الجريمة و على الأخص :-

- الجمع أو التسجيل (collection or recording) و هو أصبح ميسرا في الوقت الحالي عن طريق وسائل و برامج توجد عليها البيانات المتعلقة بخط سير البيانات في الوقت الصحيح.
- إلزام مقدم الخدمة ببذل العناية في جمع وتسجيل البيانات المتعلقة بخط سير البيانات في الوقت الملائم.

ولا يخفي على أحد أن كل ذلك للتيسير على سلطات التحقيق في جمع الأدلة الفنية و الكشف عن مرتكب الجريمة ويختلف إجراء التجميع في الوقت الفعلي للبيانات المتعلقة بخط سير البيانات عن إجراء التحفظ السريع على البيانات المتعلقة بخط سير البيانات الذي نصت عليه المادة (16) من اتفاقية بودابست في أن البيانات في حالة التحفظ أثناء وجودها على الشبكة أو حتى بعد مرور وقت عليها موجودة لدى مقدمة الخدمة أي مخزنة بالنظام المعلوماتى للكمبيوتر أو في دعامة التخزين ، بينما في حالة التجميع أو التسجيل فالبيانات ليست مخزنة ويهدف هذه الإجراءات إلى جمعها أو تسجيلها وقت مباشرة الاتصال وهذا ما حددته الاتفاقية بالوقت الفعلي أو الصحيح (Real time) ولهذا فهو يحتاج إلى وسائل تقنية حديثة قد لا تتوفر لدى السلطة المختصة أو قد لا يكون بمقدورها القيام به وعلى ذلك أسندت الاتفاقية القيام بإجراء التجميع أو التسجيل للسلطة المختصة في الدول لتقوم به بنفسها أو تنفذه من خلال مقدم الخدمة أو بمساعدته. ولأهمية هذا الإجراء قد تبناه المشرع الأمريكي في المادة (18 2703 usc) وكذلك

المشرع الفرنسي في قانون الإجراءات في مادته 2/60.

رابعاً : اعتراض مضمون البيانات:

وقد نصت المادة (21) من اتفاقية بودابست على ضرورة تبنى كل دولة طرف في تتشريعاتها ما يمكن السلطات المختصة القيام باعتراض محتوى البيانات (interception of content data) المتعلقة بجرائم خطيرة والتي قد تؤثر على اقتصاد الدولة مثلا ويتم الاعتراض بأحد الإجرائيين.

- قيام السلطات المختصة بذاتها بإجراءات التجميع أو التسجيل لمضمون البيانات.
- إلزام مقدم الخدمة بتجميع أو تسجيل محتوى البيانات.

والمقصود باعتراض مضمون البيانات و هو في نظرنا من الإجراءات الاحترازية جمع أو تسجيل مضمون البيانات التي تنقل عبر وسائل الاتصال في وقتها حتى تتمكن السلطات المختصة في الدولة من التعرف على الاستخدامات غير المشروعة لأنظمة الاتصالات بما يكفل منع ارتكاب العديد من الجرائم والأصل في هذا الإجراء أن يباشر من قبل سلطة مختصة في الدولة إلا انه قد لا تتوافر الإمكانيات الفنية اللازمة لذلك فإن الاتفاقية أجازت إلزام مقدم الخدمة للقيام بذلك.

وقيام السلطات المختصة باعتراض محتوى البيانات يختلف عن إجراء التحفظ السريع على مضمون البيانات الذي نصت عليه المادة (16) من الاتفاقية إذ أن الأخيرة البيانات المطلوب التعرف على مضمونها مخزنة ويلتزم مقدم الخدمة بالتحفظ عليها بينما يعد الاعتراض على مضمون البيانات نوعاً من المراقبة المعاصرة للاتصال (technical surveillance) وجميع وتسجيل مضمون أية اتصالات تتعلق بمسائل غير مشروعة. وقد عبر المشرع الأمريكي عن أهمية هذا الإجراء بأن نص عليه في المادة (usc 18 2703) ونظراً لخطورة هذا الإجراء ومساسه بالحقوق الشخصية للأفراد نصت المادة (usc 2703 18) من القانون الأمريكي الخاص بجرائم الكمبيوتر والانترنت بضرورة أن يصدر الأمر من السلطات القضائية المختصة أي من المحكمة أو من الإدارة العليا للعدل – high level justice department- على أن لا تزيد مدة الاعتراض عن 30 يوماً ونص عليه قانون الإجراءات الفرنسي في المادة 95/706.

المبحث الثالث
التعاون الدولي

قسمت الاتفاقية التعاون الدولي إلى بابين الأول مبادئ عامة والثاني النصوص المحددة للمساعدة المتبادلة، ونبدأ بالمبادئ العامة (أولا) ثم الخاصة (ثانيا).

أولا : المبادئ العامة:

يمكن تقسيم هذه المبادئ إلى نوعين الأول ما يتعلق بتسليم المجرمين. والثاني ما يتعلق بالمساعدة المتبادلة.

أولا : تسليم المجرمين:

لا شك في أن الدولة لها مصلحة بصفتها عضو في المجتمع الدولي أن تعاقب المجرم الذي ارتكب جرمه و فر لديها من دولة أخرى والواقع العملي أثبت أن الدولة غير قادرة وحدها على مكافحة الجرائم الالكترونية الحديثة ولما كانت النظم السياسية تتباين بين الدول بعضها مع بعض الأمر الذي فرض وجوب عقد الدول الاتفاقيات الدولية لتسليم المجرمين ، وكما أكد الفقيه الايطالي بكاريا "من أنجح الوسائل لمنع الجريمة الإتيان بعدم وجود مكان يمكن من أن يفلت المجرم من العقاب".

لذلك لم يفت على مشرعي الاتفاقية النص على أن تطبق في حالة إذا ما كانت الجرائم المنصوص عليها في هذه الاتفاقية معاقب عليها بموجب قوانين كلا من الطرفين المعنيين بعقوبة مقيدة للحرية لمدة سنة على الأقل أو بعقوبة أشد.
وتطبق العقوبة الأقل في حالة إذا ما كان توجد تشريعات موحدة أو متبادلة بالمثل أو بموجب اتفاقية تسليم.
والاتفاقية بها فرضان الأول وهو وجود اتفاقية لتسليم المجرمين حيث أن الجرائم المنصوص عليها في المواد 2 إلى 13 اعتبرتها الاتفاقية من الجرائم التي يجب تسليم المجرمين فيها وفي حالة عدم وجود اتفاقية تسليم مجرمين بين الأطراف يجوز اعتبار هذه الاتفاقية الأساس القانوني لعملية التسليم.

الفرض الثاني وهو بالنسبة للدول التي لا تجعل تسليم المجرمين مشروط على اتفاقية تسليم فإنهم بانضمامهم لهذه الاتفاقية يعتمدون الجرائم المنصوص عليها في الاتفاقية كجرائم يجوز فيها تسليم المجرمين.

ويخضع تسليم المجرمين لقانون الدولة المطلوب منها التسليم أو اتفاقية تسليم المجرمين واجبة التطبيق. وفي حالة الرفض بسبب الجنسية أو الاختصاص القضائي فإن الدولة المراد التسليم منها أن تحيل الدعوى لسلطاته المختصة وإبلاغ النتيجة للطرف للدولة الطالبة. كما أوجبت الاتفاقية الدول عند التوقيع أن تخطر السكرتير العام لمجلس أوروبا باسم السلطة المسئولة عن طلبات التسليم.

ثانيا المساعدة المتبادلة:

نصت الكثير من النظم القانونية على المساعدة المتبادلة وهي من أشكال الإنابة القضائية وهي تخضع بحسب الاتفاقية لقانون الدولة المطلوب منها المساعدة أو إذا وجدت اتفاقية المساعدة واجبة التطبيق ولا يجوز رفض المساعدة على أساس أن الجريمة تعتبر جريمة مالية و يعتبر هذا الشرط مستوفي في حالة وجود جريمة مزدوجة.

و يجوز لأحد أطراف هذه الاتفاقية إخطار

الأطراف الأخرى، في حالة وجود أو بسبب تحقيق يجرى، بمعلومات قد يساعده في البدء بالتحقيق أو اتخاذ إجراءات بصدد جرائم تتعلق بهذه الاتفاقية و الواقع العملي يفرض الإخطار للمساعدة في كشف و تحديد هوية مرتكبي الجرائم على نحو سريع خوفا من تلاشى الأدلة كما نوهنا سابقا وعلى الطرف المتلقي الحفاظ على سرية هذه المعلومات وفي حالة العكس علية إخطار الطرف المعطى للمعلومات لكي يقرر ما إذا كان ينبغي تقديم هذه المعلومات من عدمه.

وقد نصت الاتفاقية في المادة 27 الإجراءات المتعلقة بالمساعدة القضائية في حالة عدم وجود اتفاقية دولية واجبة التطبيق بشأن الطلبات المساعدة المتبادلة بعض الأسباب التي قد تجيز الرفض مثل إذا ما تعلق الطلب بجريمة سياسية أو أن تنفيذ الطلب يمس السيادة أو الأمن أو

النظام العام. إلا انه فيما يتعلق بالتحفظ العاجل على بيانات الكومبيوتر المخزونة فيجوز لأطراف هذه الاتفاقية الطلب من الأطراف الأخرى التحفظ العاجل على بيانات الكومبيوتر يقع في إقليم الطرف الأخر و قد بيت المادة 29 الإجراءات المتبعة ويجوز للطرف الأخر اشتراط ازدواجية الجريمة وله حق الرفض أيضا إذا ما تعلق الطلب بجريمة سياسية أو أن تنفيذ الطلب يمس السيادة الوطنية أو الأمن أو النظام العام.

وقد أوجبت الاتفاقية على الدول الأطراف تعين نقطة اتصال 24/7 لضمان توافر المساعدة الفورية بين الدول الأعضاء وفيما يتعلق بالدخول على بيانات الكومبيوتر في إقليم دولة أخرى فيجوز الدخول عن طريق الموافقة أو إذا ما كانت متاحة علنا.

المبحث رابع
الآثار القانونية للاتفاقية الدولية

أولا: نفاذ الاتفاقية :

نصت الاتفاقية على أنها تخضع للتصديق أو القبول أو الموافقة على أن يتم إيداع الوثيقة الدالة لدى السكرتير العام لمجلس أوروبا.

ويبدأ العمل بهذه الاتفاقية بالنسبة لأي دولة طرف توقع عليها في اليوم الأول من الشهر التالي لانتهاء فترة الثلاثة شهور من تاريخ إيداع وثيقة الانضمام للاتفاقية.

ويجب الإشارة إلى أنه في حالة إذا ما كان قد أبرم بين أحدى أطراف الاتفاقية اتفاقية أخرى بشأن المسائل التي تتناولها الاتفاقية فأنة يحق لهم تطبيق هذه الاتفاقية وفي حالة الخلاف عليهم القيام بطريقة تتفق وأهداف ومبادئ الاتفاقية.

ثانيا : التحفظات:

يجوز للدول أن تعلن أنها تستفيد من التحفظات الواردة في المواد :

4 فقرة 2 المتعلقة بالتدخل في البيانات بشرط الضرر الجسيم.

6 فقرة 3 المتعلقة بإساءة استخدام الأجهزة.

9 فقرة 4 المتعلقة بالجرائم المتعلقة بالمحتوى (صور الأطفال).

10 فقرة 3 المتعلقة بجرائم الملكية الفكرية.

11 فقرة 3 المتعلقة بالمسئولية الإضافية.

14 فقرة 3 المتعلقة بنطاق المواد الإجرائية.

22 فقرة 2 المتعلقة بالاختصاص القضائي.

29 فقرة 4 المتعلقة باشتراط الازدواجية في الجريمة للاستجابة للمساعدة المتبادلة.

41 فقرة 1 المتعلقة بالأمور الفيدرالية.

و أجازت الاتفاقية للدول أن تسحب تحفظاتها كليا أو جزئيا بعد ذلك عن طريق إخطار يرسل إلى السكرتير العام لمجلس أوروبا، وإذا كان تاريخ بدء العمل بسحب التحفظ سابق على استلام الإخطار من قبل سكرتير العام للمجلس الأوروبي فيبدأ العمل بسحب التحفظ في التاريخ اللاحق.

كما أنه يجوز للأطراف اقتراح التعديلات اللازمة على هذه الاتفاقية ويقوم الأمين العام بإخطار الدول المنضمة، على أن يتم إخطار اللجنة الأوروبية التي تحيل رأيها إلى لجنة الوزراء التي يجوز لها إقرار التعديل، على أن

يبدأ العمل بالتعديل بعد قيام الأطراف بإخطار السكرتير العام لمجلس أوروبا بقبولهم التعديل.

ثالثا: تسوية المنازعات :

أخيرا نصت الاتفاقية على أنه في حالة حدوث نزاع بين الأطراف فيما يتعلق بتفسير أو تطبيق هذه الاتفاقية فيتم اللجوء للتفاوض أو أي وسيلة سلمية أخرى من اختيارهم .... طبقا لنص المادة 45 فقرة 2 من الاتفاقية و في نهاية بحثنا هذا يثور التساؤل هل أن للدول العربية الانضمام لهذه الاتفاقية ولاسيما أن الدول المنضمة لها الحق في الخروج من الاتفاقية في أي وقت أو على الأقل إيجاد اتفاقية عربية موحدة تجمع ولا تفرق و إن كان يقتضى ذلك بحث أخر.

المراجع

-

- Cybercriminals Reinvent Methods of Malicious Attacks, by Trend Micro Incorporated, July 11, 2008,

http://www.crime-research.org/analytics/3451/

- Cyber-crimes - Analytical data compiled, by Vladimir Golubev, published on Computer Crime Research Center,

http://www.crime-research.org/analytics/cyber_crimes0108/

- Crime on The Net,

http://rogerdarlington.me.uk/crimeonthenet.html#

Hacking

- What is Cyber-terrorism, by Serge Krasavin Ph.D. MBAv, published by Computer crime research center (CCRC) http://www.crime-research.org/library/Cyber-terrorism.htm

- How Computer Viruses Work, by Marshall Brain

http://computer.howstuffworks.com/virus2.htm

- How Hackers Work, Microsoft,

http://technet.microsoft.com/en-us/library/cc505928.aspx

- Convention on Cybercrime, Budapest, 23.XI.2001

- Additional Protocol to the Convention on Cybercrime - Explanatory Report.

- Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (released 7 November 2002)

- European Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

- European Council Decision of 29 May 2000 to combat child pornography on the Internet, Official Journal L 138 , 09/06/2000 P. 0001 – 0004

- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

- Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer-related crime

- Fraud in the Internet, by Computer Crime Research Center, April 11, 2005

http://www.crime-research.org/articles/Internet_fraud_0405/

Octopus Interface 2004 - Conference on the Challenge of Cybercrime, 15-17 September 2004, Council of Europe, Strasbourg, France.

http://www.cybercrimelaw.net/documents/Strasbourg.

pdf

- Recommendation No. R (89) 9 Of the Committee of Ministers to Member States on Computer-related crime and final Report of the European Committee on Crime Problems.

http://www.oas.org/juridico/english/89-9&final%20

Report.pdf

- Cyber Crime has Surpassed Illegal Drug Trafficking as a Criminal Moneymaker1; 1 in 5 will become a Victim2; http://www.symantec.com/about/news/release/article. jsp?prid= 20090910_01

- Internet Gambling: Overview of federal criminal law; http://books.google.com.lb/

- The Myth of Cyberterrorism: There are many ways terrorists can kill you-computers aren't one of them.

Joshua Green, The Washington Quartlerly Online http:// www.washingtonmonthly.com/features/2001/

- Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption, Winn Schwartau, John Draper, January 2010.

-Prosecuting Computer Crimes Manual, publishedFebruary, 2007.

http://www.justice.gov/criminal/cybercrime/ccmanual/index.html

- Fighting cyber terrorism, by Carol Ko, June 17, 2008, Source: Computerworld.com.my

http://www.crime-research.org/news/17.06.2008/3416/

- Organized crime: from trafficking to terrorism, By FrankShanty

http://books.google.com.lb

- Intellectual Property crimes: are proceeds from counterfeited goods funding terrorism? Hearing before

the committee on International relations House of Representatives, July 16, 2003, Serial No. 108–48

http://www.foreignaffairs.house.gov/archives/108/ 88392.pdf

- Prosecuting Intellectual Property Crimes manual,Third Edition September 2006, CCIPS Criminal Division http://www.justice.gov/criminal/cybercrime/ipmanual/ index.html

- COMPUTER-RELATED OFFENCES. A presentation at the