مجلّة الواحات للبحوث والدراسات
ر ت م د: 7163 -1112 ر ت م د إ :1892-2588
https://www.asjp.cerist.dz/en/PresentationRevue/2

الجهود الدولية لمكافحة الإجرام السيبراني

International efforts to combat cyber crime

مراد مشوش

طالب دكتوراه سنة رابعة – جامعة غرداية

maachouchmourad@ahoo.fr

تاريخ الاستلام: 2019-06-22 تاريخ القبول: 2019-11-24

ملخص -

إن التعاون الدولي في مجال مكافحة الجريمة السبرانية يأخذ مظهران، الأول يتعلق بضرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة والتي تعبر اختصاصات قضائية متعددة ذات نظم قانونية مختلفة، ويتمثل في التعاون القضائي. ، أما المظهر الثاني من مظاهر التعاون الدولي في مجال مكافحة الإجرام السبراني فهو التعاون الفني إذ لا يقتصر هذا التعاون الدولي على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول.

الكلمات المفتاحية-

الإجرام السبراني – الإنتربول – الأمم المتحدة -تسليم المجرمين - الجرائم المتصلة بالحاسب

المؤلف المرسل: مراد مشوش maachouchmourad@ahoo.fr

Abstract –

International Cooperation In Combating Cybercrime Has Two Aspects. The First Concerns The Need To Cooperate In Law Enforcement To Prosecute, And Punish Criminals After Committing The Crime, Which Cross Jurisdictions With Different Legal Systems, Namely, Judicial Cooperation. . The Second Aspect Of International Cooperation In Combating Cybercrime Is Technical Cooperation. International Cooperation Is Not Limited To Mutual Judicial Assistance, But Also Involves Technical Assistance And The Exchange Of Experience Between States.

Keywords-

Cybercrime - INTERPOL - United Nations – Extradition - Illegal Access

1. مقدمة

يتسم الإجرام السبراني بالنظر لطبيعتها بطابع دولي ، لكن اختلاف التشريعات في تأسيس اختصاصها الجنائي نتيجة تعدد الأسس التي يقوم عليها هذا الاختصاص قد يؤدي إلى تنازع الاختصاص بين الدول، فقد يحدث أن ترتكب الجريمة المعلوماتية في دول معينة، و يكون المجرم المعلوماتي مرتكب هذه الجريمة أجنبياً. فتخضع هذه الجريمة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الاقليمية ، وتخضع كذلك لاختصاص الدول الثانية على أساس مبدأ الاختصاص الشخصي في جانبه الايجابي[1] .

و قد تكون الجريمة المرتكبة على اقليم الدولة من الجرائم التي تهدد أمن و سلامة دولة أخرى، فتخضع للاختصاص الجنائي الاقليمي من جهة، و تخضع لاختصاص الدولة المجني عليها استناداً إلى مبدأ الاختصاص العيني من جهة أخرى، كما تثور فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الاقليمية ، كما لو قام الجاني ببث معلومات غير مشروعة على اقليم دولة معينة و تم الاطلاع عليها في دولة أخرى، فوفقاً لمبدأ الاقليمية فإن الاختصاص الجنائي و القضائي يثبت لكل دولة من الدول التي مستها الجريمة،

سواء تلك التي وقع فيها الفعل الإجرامي (فعل البث) أو تلك التي حدثت نتيجة الفعل فيها (تلقي المعلومات غير المشروعة)، الأمر الذي يؤدي إلى الاطاحة بمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة، و لذلك لا بد أن يكون هناك تعاون دولي يتفق مع طبيعة الإجرام السبراني الذي يتميز بطابع خاص يقتضي أن تكون هناك ردود فهل سريعة لأن هذا التنسيق الفعال و العاجل يساعد على الحد من الأضرار الناجمة عن هذه الجرائم و كذلك تجنب المجرم المعلوماتي الافلات من العقاب و مثال ذلك ما قام به " أونيل دو غوزمان" الذي استخدم فيروس "أحبك I love you "[2] سنة 2000 الذي انتشر في كل أنحاء العالم عن طريق البريد الالكتروني حيث قدرت الخسارة ب 7 مليارات دولار[3].

و عليه و مما سبق نطرح الإشكالية التالية:

فيما تتمثل الجهود الدولية في مجال مكافحة الإجرام السبراني؟

و عليه، يهدف هذا المقال إلى تقديم أهم الجهود الدولية و الاقليمية في مواجهة الجرائم المعلوماتية و مدى انعكاسها على التعاون الدولي المشترك.

كما أن هذا المقال بشكل مجمل تقديم صورة عامة لأبرز التحديات المصاحبة لهذه التكنولوجيا، وفق منهجية تطمح إلى تقديم نظرة للظاهرة الإجرامية، لهذا سأعتمد على المنهج الوصفي التحليلي، و ذلك بوصف الجريمة و خصائصها و أنواعها و التحليلي بذكر الجهود الدولية و الإقليمي لمكافحة هذه النوعية من الجرائم و تحليل الأساليب المتبعة من طرف المشرع الجزائري لذلك.

2. على المستوى الدولي:

إذا كان التعاون الدولي هو الآلية الفعال لمكافحة الإجرام السبراني، فإن هذا التعاون يقتضي التخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية لأن التباعد بين هذه الانظمة يجعل المجرم المعلوماتي يبحث عن الأنظمة الأكثر تسامحاً، و لذلك أبرمت العديد من الاتفاقيات الدولية في مجال التعاون الدولي من أجل مكافحة الإجرام السبراني و تظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ اجراءات التحقيق و جمع

الأدلة و تسليم و الاعتراف بالأحكام الجنائية، بحيث أن هذا القانون الدولي لا ينال من سيادة الدولة، بل بالعكس عدم التعاون يزيد من التباعد بين الأنظمة العقابية مما يساعد على تزايد هذه النوعية من الجرائم.

وعليه يجد التعاون الدولي في مجال مكافحة الجريمة السبرانية بصفة عامة تبريره في بعض الاعتبارات منها[4] :

-أنه يعتبر خطوة على طريق تدويل القانون الجنائي، ذلك أن ثمة قواعد موضوعية و اجرائية تهيمن على أذهان العديد من مشرعي هذه الحقبة ومن شأن تشابه هذه القواعد أن يخلق نوعاً من التقارب بين التشريعات الحالية.

-أنه يعتبر من قبيل التدابير المانعة من ارتكاب هذه النوعية من الجرائم، لان المجرم المعلوماتي سوف يجد نفسه محاطاً بسياج مانع من الافلات من المسؤولية الجنائية عن الجريمة التي ارتكبها ، أو من العقوبة التي حكم عليه بها. فإذا ارتكب جريمته في دولة ما و تمكن من الهروب إلى دولة أخرى فإنه سوف يكون عرضة للقبض عليه أو ترحيله إلى البلد الأول ، و من شأن كل ذلك أن يجعل المجرم المعلوماتي يعزف عن سلوك سبيل الجريمة.

1.2 جهود الأمم المتحدة في مجال مكافحة الإجرام السبراني

بذلت الأمم المتحدة جهوداً كبيرة في سبيل العمل على مكافحة الإجرام السبراني، و ذلك لما تسببه هذه الجرائم من أضرار بالغة و خسائر فادحة بالإنسانية جمعاء، و إيماناً منها بأن منع هذه الجرائم و مكافحتها يتطلبان استجابة دولية في ضوء الطابع و الأبعاد الدولية لإساءة استخدام الكمبيوتر و الجرائم المتعلقة به[5] .

توصلت منظمة الأمم المتحدة في مؤتمرها الثامن المنعقد بهافانا 1990 حول منع الجريمة و معاملة المجرمين United Nations Congress on the Revention of Crime and the Treatement of the Offender إلى اصدار قانون خاص بالجرائم المتعلقة بالحاسوب، و أشار القرار إلى أن الأجرام الدولي لمواجهة الجرائم المستحدثة يتطلب من الدول الأعضاء اتخاذ عدة إجراءات[6] تتلخص فيما يلي :

-تحديث القوانين و أغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة من تحقيق و قبول الأدلة على نحو ملائم و إدخال التعديلات إذا دعت الضرورة لذلك.

-اتخاذ تدابير أمن و الوقاية مع مراعاة خصوصية الأفراد و احترام حقوق الإنسان.

-رفع الوعي لدى الجماهير و القضاة و الأجهزة العاملة على مكافحة هذا النوع من الجرائم.

-التعاون مع المنظمات المهتمة بهذا الموضوع ، و وضع و تدريس الآداب المتخذة في استخدام الحاسوب في المناهج التعليمية.

-حماية مصالح الدولة و حقوق ضحايا جرائم الحاسوب.

لكن تزايد الجريمة السبرانية و ما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية ديسمبر سنة 2000 ، رقم 55/63 الجلسة العامة، أين أكدت على الحاجة إلى تعزيز التنسيق و التعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية ، بالإضافة الذي يمكن أن تقوم به المنظمة و المنظمات الإقليمي الأخرى.

عقدت كذلك الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة و العدالة الجنائية بالبرازيل أيام 12 إلى 19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخير في استخدام التكنولوجيا من طرف المجرمين و السلطات المختصة في مكافحة الجريمة، حيث تبقى منظمة الأمم المتحدة الإطار الأمثل لمكافحة الإجرام السبراني حيث وضعت مجموعة من القواعد الموضوعية و إجرائية[7] لمواجهة هذه النوعية من الجرائم.

1.1.2 القواعد الموضوعيـة:

تتضمن هذه القواعد النص على قائمة الحد الادنى للأفعال المتعين تجريمها و اعتبارها من قبيل الإجرام السبراني و تحديثها دورياً و المتضمنة :

-جريمة الاحتيال أو الغش المرتبط بالكمبيوتر : و يشمل ذلك الادخال و الاتلاف و المحو لمعطيات الكمبيوتر أو برامجه أو القيام بأية أفعال تؤثر بمجرى

المعالجة الآلية للبيانات و تؤدي إلى الحاق الخسارة أو فقدان الحيازة أو ضياع ملكية شخص و ذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.

-جريمة التزوير التي تطال برامج الكمبيوتر أو التزوير المعلوماتي : و يشمل ذلك ادخال أو الاتلاف أو المحو أو تحوير المعطيات أو البرامج أو أية أفعال تؤثر على المجرى العادي لمعالجة البيانات ترتكب باستخدام الكمبيوتر و تعد فيما لو ارتكبت بغير هذه الطرق من قبيل أفعال التزوير المنصوص عليها في القانون الوطني.

-جريمة تخريب و اتلاف الكمبيوتر: و يشمل ذلك ادخال أو الاتلاف أو التخريب أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات و الشبكات.

-جريمة الدخول غير المصرح به : و هو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق انتهاك إجراءات الأمن.

-جريمة الاعتراض غير المصرح به : و هو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم او شبكة اتصالات.

2.1.2 القواعد الإجرائية:

تتضمن بعض الأسس الواجب مراعاتها[8] :

-وجوب تحديد السلطات التي تقوم بإجراء التفتيش و الضبط في بيئة تكنولوجيا المعلومات، و خاصة ضبط الاشياء المتعلقة بها و تفتيش الحاسب.

-وجوب أن يكون هناك قدر كبير من التعاون الفعال بين الأطراف لكي تكون المعلومات متاحة في صورة يمكن استخدامها للأغراض القضائية في حل هذه الجرائم

-السماح للسلطات العامة باعتراض الاتصالات داخل البيئة المعلوماتية مه استخدام الأدلة التي يمكن ان يتحصل عليها.

-ادخال بعض التعديلات التشريعية في حالة الضرورة ما يتماشى مع طبيعة الإجرام السبراني داخل القانون الوطني و كذلك القواعد القائمة في مجال الإثبات الالكتروني من حيث مصداقية الأدلة و ما يمكن أن تثيره من مشاكل عند تطبيقها.

-يجب أن يوضع في الاعتبار كل المسائل المرتبطة ببيئة تكنولوجيا المعلومات، مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة ، مخاطر الخسارة الاقتصادية، كلفة إعادة بناء قواعد البيانات كما كانت و إعادتها إلى الواضع السابق قبل اجراء أي تفتيش أو تحقيق.

2.2 جهود المنظمات الدولية في مجال مكافحة الإجرام السبراني

قد اتخذت مبادرات من قبل العديد من المنظمات كالاتحاد الدولي للاتصالات (ITU) ،الإنتربول/يوروبول، منظمة التعاون الاقتصادي والتنمية (OECD)، مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) والمنظمة الدولية لتوحيد المقاييس(ISO) ، واللجنة الكهروتقنية الدولية (IEC) وفرق عمل هندسة الإنترنت و FIRST منتدى الاستجابة للأحداث ومجموعات الأمن لآسيا والمحيط الهادئ، ومنظمة التعاون الاقتصادي للمحيط الهادئ وآسيا (APEC)ومنظمة الدول الأميركية (OAS) ورابطة دول جنوب شرق آسيا (ASEAN)وجامعة الدول العربية، والاتحاد الأفريقي.

1.2.2 منظمة التعاون الاقتصادي والتنمية (OECD)

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي و تناغم التطور الاقتصادي مع التنمية الاجتماعية، بدأت هذه المنظمة الاهتمام بالجريمة السبرانية منذ عام 1978، حيث وضعت مجموعة من الأدلة و قواعد إرشادية تتصل بتقنية المعلومات، و يعد الدليل المتعلق بحماية الخصوصية و قواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها.[9]

فأصدرت سنة 1983 تقريراً بعنوان الجرائم المرتبطة بالحاسوب و تحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة و المقترحات الخاصة في عدد من الدول الأعضاء، وتضمن التقرير الحد الأدنى من لأفعال سوء استخدام الحاسوب و التي على الدول تجريمها و تشمل هذه الأفعال[10] :

-الاستخدام أو الدخول إلى نظام و مصادر الحاسب على نحو غير مصرح به

-الإفشاء غير مصرح به للمعلومات المعالجة آلياً و النسخ و الإتلاف أو التخريب ما يحتويه من بيانات و برامج و الإعاقة غير المشروعة للوصول لمصادر الحاسب من منع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المخزنة داخله.

و في عام 1992 و ضعت المنظمة توصيات و إرشادات خاصة بأنظمة المعلومات و أوصت بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء مبادئ عامة[11] تتمثل في :

-حدود التجميع: يتعين فرض قيود على تجميع البيانات.

-نوعية البيانات: حيث تنص على أن تتعلق البيانات بالغاية و الغرض الذي سوف تستخدم من أجله.

-تعيين الغرض: بحيث يكون الغرض الذي تستخدم فيه البيانات الشخصية محصورة و محددة سلفا.

-حدود الاستخدام: يقتضي الالتزام بعدم إفشاء البيانات الشخصية و نشرها لغير المصرح لهم بذلك.

-الوقاية الأمنية : ضرورة اتخاذ تدابير و إجراءات أمنية ملائمة و حازمة في إحاطة البيانات.

-الانفتاح: أن تكون السياسة العامة للتطوير و الخطط و التطبيقات معلنة فيما يتعلق بالبيانات ذات الطبيعة الشخصية.

-المشاركة الفردية: حق الأشخاص المعنية في الوصول و التعرف على البيانات التي تخصهم فضلاً عن رقابة مدى صحتها.

-المسائلة و المحاسبة : التي تقتضي محاسبة الأشخاص و الجهات المرخص لهم الوصول و الاطلاع على البيانات و التعامل معها في حالة تجاوز أي من الإجراءات التي تكفل حماية البيانات ذات الصفة الخاصة.

2.2.2 الأنتربول

وضعت منظمة الإنتربول[12] نظاما خاصا للتعاون، وهو النظام الوطني الخاص بالنقطة المرجعية المركزية[13] NCRP ويوجد في كل دولة من الدول الأعضاء في الإنتربول مكتب مركزي وطني يُعد نقطة الاتصال مع الإدارات الأجنبية التي

تجري تحقيقات خارج حدودها و تضم شبكة من المحققين العاملين في الوحدات الوطنية المعنية بجرائم لتيسير الاتصالات الميدانية بين البلدان الأعضاء وتسريعها قدر الإمكان ومن مهامها هذا النظام إنماء الاستراتيجيات والتقنيات والمعلومات بشأن أحدث الأساليب الجرمية في مجال جرائم تكنولوجيا المعلومات وهناك فرق عاملة إقليمية لإفريقيا والأمريكيتين وآسيا وجنوب المحيط الهادئ و أوروبا والشرق الأوسط وشمال إفريقيا[14].

كما قامت منظمة الإنتربول بوضع برنامجاً خاصاً لمكافحة الإجرام المعلوماتي يرتكز على التدريب والعمليات ويعمل على مواكبة التهديدات الناشئة مبادرات ويهدف هذا البرنامج[15] :

- توفيردورات تدريبية لوضع معايير مهنية والتقيد بها.

-تعزيز تبادل المعلومات بين البلدان الأعضاء عن طريق الأفرقة العاملة والمؤتمرات الإقليمية.

-تنسيق العمليات الدولية ودعمها

-إعداد قائمة عالمية بأسماء ضباط الاتصال ووضعها بتصرف المحققين في مجال الإجرام السيبيري على مدار الساعة

-مساعدة البلدان الأعضاء على التحقيق في الهجمات أو الجرائم السبرانية عن طريق توفير خدمات في مجال التحقيق وقواعد البيانات

-إقامة شراكات استراتيجية مع المنظمات الدولية الأخرى وهيئات القطاع الخاص.

-تحديد التهديدات الناشئة وتبادل معلومات الاستخبار في هذا المجال مع البلدان الأعضاء.

-توفير بوابة آمنة على الويب لنشر معلومات ووثائق عملياتية.

3. على المستوى الإقليمي (اتفاقية بودابست):

تعد الاتفاقية الأوربية بمثابة دعوة موجهه إلى دول العالم للتفاعل مع الجرائم المستحدثة و التي جاءت نتيجة محاولات عديدة منذ ثمانيات القرن العشرين حتى ظهرت بشكلها، فبتاريخ 20 أفريل 2000 تقدمت اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية، بمشروع اتفاقية جرائم

الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من اصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست 2001 وتعرف باتفاقية بودابست (اتفاقية الجرائم الالكترونية – سايبر كرايم) وكان قد طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات وأطلق ضمن مواقع عديدة أوروبية وأمريكية على شبكة الأنترنت لجهة التباحث وإبداء الرأي، وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ اكثر من عشرة أعوام[16] .

ومن أهم الأسباب التي أدي إلى إبرام الاتفاقية هو الحاجة على اتخاذ تدابير تشريعية لمكافحة الجريمة السبرانية و مخاطرها المدمرة على الدول خاصة في ظل شيوع شبكات المعلومات و في ظل التوسع و النماء الكبير لأنظمة الحوسبة المفتوحة و نقل و تدفق المعلومات، إضافة إلى التشديد على أهمية مكافحة كافة الأنشطة التي تستهدف أمن المعلومات و نظم الكمبيوتر.[17]

هذه التدابير التشريعية و التنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة مع التركيز على اهمية التعاون المحلي والاقليمي والدولي مع وجوب اقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الاساسية والسيادة، ولأن هذه الاتفاقية جاءت حصيلة جهود دولية واقليمية فقد أكدت المقدمة أيضا على أهمية ما أنجز من جهود في حقل الإجرام السبراني من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوربي ومجموعة الدول الصناعية وبالنتيجة فأن مشروع الاتفاقية قد ركزت على عناصر أساسية ثلاثة[18]:

- أهمية التدابير التشريعية الموضوعية) نصوص التجريم.
- أهمية التدابير التشريعية الاجرائية) النصوص الاجرائية.
- أهمية تدابير التعاون الدولي والاقليمي في مجال مكافحة الجرائم.

إن هذه الاتفاقية تقدم ولأول مرة إطاراً لتحديد قائمة جرائم الكمبيوتر وأنماطها وطوائفها، إذ حتى الآن وبالرغم من الجهود التشريعية والتدابير

الاقليمية والدولية على مدى السنوات الثلاثين الماضية لم تتوفر رؤية شاملة او اطار واضح يحدد قائمة الجرائم أو بين أساس التقسيم ، ولهذا فان أهم ما يسجل لهذه الاتفاقية – بعيد عن الاتفاق والخلاف على الأساس الذي اعتمدته – أنها تطرح اطارًا للتقسيم والتحديد بشأن القواعد الموضوعية لجرائم الكمبيوتر والأنترنت، وبالرجوع الى المعيار التي اعتمدته ، نجده بالأساس يقوم على فكرة دور الكمبيوتر بالجريمة"[19].

تتكون الاتفاقية من مقدمة وأربعة فصول، فبعد أن استعرضت المقدمة أهداف الاتفاقية و منطلقاتها و مرجعياتها السابقة وما تقوم عليه من جهود ارشادية وتوجيهية وتدابير اقليمية ودولية، جاء الفصل الأول لتغطية المصطلحات الأساسية (مادة 1)، تضمن الفصل الثاني الذي جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى الوطني ، 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 الاحكام الختامية ويضم المواد من 36 – 48 .

أكدت مقدمة الاتفاقية على الحاجة إلى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر و الأنشطة التي تستهدف العناصر الثلاثة لأمن المعلومات ونظم الكمبيوتر وهي السرية confidentiality وسلامة المحتوى integrity وتوفر المعلومات والنظم availability ، كما أن المقدمة نجدها تلخص أهداف الاتفاقية بما يلي[20]: -

-السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنضمة للاتفاقية من غير الدول الأوروبية .

-التأكيد على أهمية التعاون الاقليمي والدولي في ميدان مكافحة جرائم الكمبيوتر والأنترنت وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة جرائم الكمبيوتر والأنترنت .

-ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة وتوفر المعلومات وأنظمة الكمبيوتر وشبكات الكمبيوتر وأنشطة إساءة استخدام الكمبيوتر والشبكات ، بما في ذلك تحديد الإطار الموضوعي لهذه الانشطة والإطار الإجرائي المتصل بالتحقيق والتحري والمقاضاة في ميدان جرائم الكمبيوتر على المستوى الوطني والدولي .

يضم الفصل الأول مادة واحدة (المادة 1) وهي التعريفات définitions وربما تكون هذه المادة من أهم المواد في ميدان اتفاقيات تقنية المعلومات[21] بسبب الخلاف الكبير بشأن تعريف اصطلاحات الكمبيوتر تبعا لزاوية الرؤيا وهدف استخدام التعريف، إلى جانب التباين بشأن المعايير والمقاييس التقنية وربما تكون لهذه المادة أهمية استثنائية لجهة توحيد التعريفات بعدما ظهر التناقض والتباين في تشريعات جرائم الكمبيوتر التي جرى سنها في أوروبا وأمريكا واستراليا وعدد من دول شرق آسيا، كما عرفت نظام الكمبيوتر computer system وعرفت هذه المادة معطيات الكمبيوتر computer data تعريفاً واسعاً يشمل الحقائق والمعلومات والمفاهيم بشكل مناسب لعمليات المعالجة في نظام الكمبيوتر.

أما الفصل الثاني من الاتفاقية والمعنون (المعايير المتعين اتباعها على المستوى الوطني – measures to be taken at the national level) تضمن أقساما ثلاث، الأول حول التدابير الموضوعية أي القانون الجنائي الموضوعي، والتي تعنى بالسلوكيات التي يجب اعتبارها جريمة جنائية، والثاني حول التدابير الإجرائية، ويتناول التدابير التي تتخذ لإجراء تحقيقات أكثر فعالية فيما يتعلق بجرائم الكمبيوتر، ويجب التأكيد على أن هذه التدابير الإجرائية يمكن استخدامها مع أية جرائم جنائية يشترك فيها نظام للكمبيوتر، والثالث حول الاختصاص، وبهذا الفصل تكون الاتفاقية قد قدمت الإطار

القانوني للتدابير التشريعية الموضوعية والاجرائية المتعين اتخاذها لمواجهة جرائم الكمبيوتر والانترنت[22]، وهذا ما سيتناوله البحث بشيء من التفصيل.

الفصل الثالث تم تخصيصه للتعاون الدولي و الحث على الأطراف أن تتعاون مع بعضها البعض، في تطبيق الأصول الدولية في المواد الجنائية ،والمبادئ المتعلقة بالمساعدات القانونية المتبادلة، والمعلومات المقدمة طواعية، والمساعدة القانونية المتبادلة في حال عدم وجود وثائق دولية معمول بها، والسرية ووضع حد للاستخدام.

أما الفصل الرابع الأحكام الختامية و يهتم هذا الفصل على وجه الخصوص بالدول غير الأوروبية كما ينص على سبل انضمام الدول غير الأعضاء إلى الاتفاقية.

1.3 القانون الجنائي الموضوعي

يعد موضوع القسم الأول من هذه الاتفاقية (المواد من 2 إلى 13) دليلاً ارشادياً لتحسن أو اصلاح و سائل منع و قمع الإجرام المعلوماتي Améliorer les moyens de prévenir et de réprimer la criminalité informatique، بتحديد أدنى القواعد العامة التي تسمح باتخاذ بعض التصرفات القانونية اتجاه هذه الجرائم و يسهل مكافحتها على المستوى الوطني و الدولي، و يحدد قائمة تسمح بتجريم بعض الأفعال و التصرفات غير المشروعة التي ترتكب على بيئة معلوماتية، بعبارة أخرى حصر الإجرام السبراني بتحديد الحد الأدنى في بعض الأفعال غير المشروعة التي تعد من قبيل الجريمة السبرانية.

فإذا كانت هذه الاتفاقية تنطبق على التصرفات التي توصف على أنها جرائم مرتكبة عن طريق تكنولوجيا المعلومات، فإن المذكرة التفسيرية حرصت على ايضاح أن الاتفاقية تستخدم تكنولوجيا محايدة Neutre أي التكنولوجيا الآنية و المستقبلية، كما ركزت المذكرة التفسيرية على ضرورة ارتكاب الجرائم المحصاة دون حق وذلك عندما نصت (يشترط في تجريم الأفعال في هذه الاتفاقية أن يكون القيام بالفعل دون حق (Sans droit)، كما أن كل الجرائم المدرجة يجب ان تكون مرتكبة بطريقة عمدية[23] Facon Intentionnelle

1.1.3 الأفعال غير المشروعة

تناولت المواد من 2 إلى 10 الجرائم الواردة في هذه الاتفاقية

- جرائم ضد سرية وسلامة و توافر البيانات و النظم المعلوماتي: Infraction contre la confidentialité, L'intégrité et la disponibilité des données et systèmes informatique، إن الغرض من الجرائم التي تناولها هذا العنوان هو حماية سرية و سلامة و اتاحة أو تهيئة البيانات و نظم الحاسب للعمل أو التشغيل، وبالتالي يخرج من نطاق التجريم الأنشطة المشروعة و العادية و المرتبطة بتصميم الشبكات و كذلك الممارسات الاستثمارية أو التجارية المشروعة و العادية، و قد تناولتها[24] المواد من 2 إلى 6

-الولوج غير القانوني (المادة2): Accès Illégal و الذي يعد الجريمة الرئيسية التي تهدد سرية و أمن و سلامة المعلومات و توفرها و على ذلك فإن مجرد التدخل غير المصرح به بمعنى القرصنة* Le piratage ، أو الدخول غير المشروع في النظام يعتبر تصرفاً غير مشروع

-الاعتراض غير القانوني (المادة3): تهدف هذه المادة لحماية الحق في احترام نقل البيانات و أن هذه الجريمة تمثل انتهاكاً للحق في احترام الاتصالات مثل التصنت و التسجيل التقليدي للمحادثات و المراسلات بين بين الأشخاص.

-الاعتراض على سلامة البيانات (المادة4): الغرض من هذه المادة هو أن تكون بيانات و برامج الحاسب مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمداً من اتلاف الأجهزة المادية و المنطقية المكونة للحاسب و محو البيانات و البرامج.[25]

-الاعتداء على سلامة النظام (المادة5): تهدف هذه المادة إلى تجريم عرقلة الاستخدام الشرعي لنظام المعلومات، أو التأثير على سيرها العادي و التي تمنع او تبطئ بشكل ملموس سير عمل النظام.

-إساءة استخدام أجهزة الحاسب (المادة6): تشير هذه المادة أن الأعمال غير المشروعة التي تندرج تحت النوع أ من الجرائم المذكورة أعلاه تكون في الغالب عند حيازة و سائل الدخول كحصول المجرم على معدات التشويش أو أجهزة تحاليل الشبكات التي هي في الأصل تستعمل للتحقيق من إمكانية عمل الشبكات

أو أجهزة مراقبة أمن الشبكات كما قد يكون جهاز الكمبيوتر نفسه أداة المزود بالأنترنت أداة لاختراق بعض المواقع أو الحسابات الالكترونية[26]، كما تشمل الإنتاج المتعمد أو بيع أو شراء أو استيراد أو توزيع الأجهزة و الأدوات بهدف ارتكاب أي فعل المنصوص عليه في المواد 2 إلى 5 من هذه الاتفاقية.[27]

- **الجرائم المتصلة بالحاسب:** Infractions Informatiques و هي المادتين 7و8 والتي تتعلق بجرائم عادية يمكن في الغالب ان ترتكب عن طريق الحاسب الآلي:

-التزوير المعلوماتي (المادة7): الغرض من هذه المادة في إنشاء جريمة موازية لجريمة تزوير المستندات الورقية كما تهدف إلى استكمال أوجه النقص[28] التي تعتري قانون العقوبات بالنسبة للتزوير التقليدي، و التزوير المعلوماتي يتكون من خلق Créer أو تعديل Modifier.

-الغش المعلوماتي (المادة8): مع حدوث ثورة تكنولوجية تضاعفت إمكانية ارتكاب جرائم اقتصادية كالغش و بالأخص النصب ببطاقات الائتمان و المعاملات البنكية أو الودائع التي أصبحت هدفاً للنصب من خلال التلاعبات بمدخلات النظام بمعنى ادخال على النظام ببيانات غير صحيحة.

-الجرائم المتصلة بالمضمون: Infraction se rapportant au contenu هذه الجرائم المرتبطة بالمحتوى و التي تربط بإنتاج أو نشر غير المشروع للمواد الإباحية الطفولية عير النظم المعلوماتية.

-الجرائم المتصلة بالمواد الاباحية (المادة9): تسعى هذه المادة إلى تدعيم الإجراءات التي تحمي الأطفال خاصة من الاستغلال الجنسي من خلال تحديث قانون العقوبات تشمل على استخدام الحاسب الآلي في اطار ارتكاب الجرائم الجنسية ضد الأطفال كما تجرم مختلف جوانب الإنتاج و الحيازة و النشر للمواد الإباحية الطفولية.

-الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية و الحقوق المجاورة: Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes و هي الأفعال التي تعتبر عن انتهاكات واقعة على الملكية الفكرية و خاصة المؤلف من خلال المادة 10 من

متخصصي النظام المعلوماتي و خصوصاً شبكة الانترنت و الأفعال[29] هي : إن إعادة إنتاج و بث الأعمال المحمية عبر الأنترنت دون موافقة حائز الحق هو أمر غير شرعي و هذه الأعمال المحمية تشمل الأعمال الأدبية و التصويرية و الموسيقية و السمعية البصرية.

2.1.3 تقرير العقوبات

أشارت المادة 13 من هذه الاتفاقية على ضرورة خضوع المنصوص عليها في المواد من 2 إلى 10 لعقوبات جزائية و بالنظر للالتزامات التي تفرضها هذه المواد فإنه يجب على الاطراف المتعاقدة استخلاص النتائج الخطيرة المترتبة على ارتكاب تلك الجرائم و إقرار عقوبات جزائية فعالة، مناسبة و رادعة تتضمن عقوبات سالبة للحرية.

و في حالة الاشخاص الاعتباريين أن يخضعوا أيضاً لعقوبات فعالة و مناسبة و رادعة و التي يمكن أن تكون جزائية، مدنية أو ادارية، كما تركت نفس المادة المجال مفتوحاً لإمكانية فرض عقوبات أخرى أو إجراءات تتناسب مع خطورة الجرائم المرتكبة مثل قرار الحظر أو المصادرة.

2.3 قانون الإجراءات

إن المواد في القسم الراهن نصت بعض الإجراءات التي يجب اتخاذها على الصعيد الوطني، و التي تخدم التحريات الجنائية التي ترتكب عن طريق المنظومة المعلوماتية، و جمع الادلة ذات الطابع الالكتروني.

فتكمن أحد أصحاب المشاكل في مجال مكافحة الإجرام السبراني في صعوبة تحديد هوية مرتكب الجريمة و مداها و تأثيرها و المشكلة الأخرى تكمن في ضياع البيانات الالكترونية التي يمكن نقلها أو تعديلها أو محوها في ثواني معدودة[30]، فمثلاً يستطيع الشخص الذي يتحكم في البيانات أن يستخدم المنظومة المعلوماتية بمحوها مدمراً بذلك جميع الأدلة التي يقوم عليها التحقيق الجنائي، لذا تعتبر في أغلب الأحيان السرعة و السرية من المكونات الأساسية لنجاح التحريات.

تُقر الاتفاقية إجراءات تقليدية مع المناخ التكنولوجي الحديث مثل التفتيش و المصادرة و بالتوازي وضعت إجراءات جديدة[31]، كالحفظ السريع

للبيانات خلال مدة زمنية محدودة وذلك بهدف إتاحة الفرصة للحصول أو جمع البيانات التي تخدم التحريات أو الإجراءات الجنائية التي يجب القيام بها، و التي بموجبها يجري الإعداد و الاتفاق على نظم حماية تسمح بالسيطرة على هذا المناخ التكنولوجي الجديد و تطوير سلطات إجرائية جديدة.

كما تشير هذا القسم إلى مجال تطبيق بنود هذه الاتفاقية من خلال المادة 14، حيث تلزم كل دولة طرف في الاتفاقية بإقرار الإجراءات التشريعية بما يسمح القانون الداخلي بها لخدمة التحريات و الإجراءات الجنائية الخاصة على :

-الجرائم الجنائية المنصوص عليها في القسم الأول من الاتفاقية.

-جميع الجرائم الجنائية الأخرى التي ترتكب عن طريق المنظومة المعلوماتية.

-جمع الأدلة الالكترونية[32] لكل جريمة من أجل التحريات أو إجراءات جنائية معينة[33].

و تشير الاتفاقية بوضوح إلى أنه يجب ان تقر الأطراف بان القانون الداخلي يتضمن معلومات رقمية أو الكترونية قد تستخدم كأدلة[34] أما القضاء و ذلك في إطار الجنائي أياً كان طبيعة الجريمة المطلوب متابعتها.

1.2.3 الحفظ السريع للمعطيات المخزنة

إن الإجراءات التي تتضمنها المادة 16 و 17 تطبق على جميع البيانات المخزنة (بيانات خط السير أو بيانات المضمون[35]) و التي تم جمعها و حفظها عن طريق أصحابها، أي أنها لا تطبق إلا عندما تكون بيانات المعلوماتية، موجودة آنفاً و في طور التخزين.

و المقصود بحفظ البيانات[36] هو الاحتفاظ السابق بالمعلومات و تخزينها مع حمايتها من كل ما يمكن أن يفسدها أو يتلف نوعيتها أو حالتها الراهنة، فالحفظ هو عملية ضمان لسلامتها و جعلها بمأمن[37]، كما تشير المادة 14 من هذه الاتفاقية أنه يجب العمل بجميع الصلاحيات و الإجراءات و ذلك لخدمة التحريات و الإجراءات الجنائية، فالاحتفاظ بالبيانات يعد صلاحية و إجراء

قانوني جديد تماماً على القانون الداخلي[38]، فالأمر يتعلق بوسيلة جديدة لإجراء التحريات الهامة لمكافحة الإجرام السبراني و ذلك للأسباب التالية:

-نظراً لقابلية البيانات المعلوماتية للتلاشي فإنه من السهل التلاعب بها و تعديلها، و كذلك من السهل فقدان العناصر التي تعد دليلاً على وقوع جريمة ولا سيما إذا كانت الممارسة المتبعة في المعالجة و التخزين تفتقد الدقة.

-إن جزء كبير من الإجرام المعلوماتي غالباً ما يرتكب من خلال انتقال الاتصال عن طريق المنظومة المعلوماتية، و من الممكن أن تتضمن تلك الاتصالات محتوى غير مشروع.

2.2.3 تفتيش و مصادرة البيانات المعلوماتية:

تهدف المادة 19 من هذه الاتفاقية إلى تحديث و تجانس التشريعات الداخلية الخاصة بالتفتيش و مصادرة البيانات المعلوماتية المخزنة للحصول على ادلة مرتبطة بتحريات و إجراءات جنائية معينة، و تنص جميع التشريعات الداخلية الخاصة بالإجراءات الجنائية على صلاحيات التفتيش و المصادرة للعناصر المادية.[39]

غير أنه فيما يتعلق بالبحث عن البيانات المعلوماتية، يتحتم وجود أحكام إجرائية إضافية حتى تضمن الحصول على البيانات المطلوبة بنفس فاعلية التفتيش و مصادرة الدعائم للمعلومات المادية و يرجع ذلك أن تتم قراءة المعطيات عن طريق جهاز معلوماتي و لكن لا يمكن مصادرتها و نقلها بنفس طريقة المستند الورقي، كما يمكن نقل الأجهزة الداعمة التي يتم عليها حفظ البيانات (قرص صلب، ديسك...إلخ)، بالإضافة لكون المنظومة المعلوماتية متصلة فيما بينها، فيكون من السهل الوصول إلى المعلومات المطلوبة من خلال هذه المنظومة في حالة عدم تخزين هذه المعلومات على جهاز الكمبيوتر موضوع أمر التفتيش، حيث تكون مخزنة في حافظة معلومات متصلة بصورة مباشرة بجهاز كمبيوتر آخر و عن بصورة غير مباشرة بواسطة نظام اتصالات كالأنترنت[40] ، عندما ألزمت الفقرة الأولى و الثانية من نفس المادة الأطراف أن تخول لسلطاتها المختصة بمكافحة الجريمة المعلوماتية الحق في فحص و

الدخول على المعطيات سواء الموجودة في نظم معلومات أو جزء من هذه المنظومة مثل الأسطوانة ...إلخ[41].

كما تناولت الفقرة الثالثة السماح للسلطات المختصة بمصادرة البيانات أو الحصول عليها بطريقة مشابهة لها عن طريق نسخها بأي طريقة تقنية و التي لا تعرضها للإتلاف أو فقدانها أو جزء منها. إذا أخذنا بعين الاعتبار البعد الدولي لجرائم الإنترنت، يمكننا أن نستنتج أنه لا يمكن لدولة بمفردها أن تحقق النجاح في هذه المعركة، بل لا يتحقق ذلك إلا عن طريق التعاون على المستوى الدولي و الاقليمي .ولكننا نعلم أن التعاون يعتمد على الأنظمة القانونية للدول والتوفيق بين التشريعات الوطنية المختلفة ، كما يجب على كل البلدان أن تضع إطارا قانونيا مناسبا، سواء على المستوى الوطني أو الدولي، بحيث يكون قادرا على توفير الأدوات التشريعية وأدوات التحقيق اللازمة لمكافحة جرائم الإنترنت مع الوضع في الاعتبار مدى تعقيدها.

4. خاتمة

يتضح جلياً خطورة هذا النوع من الجرائم ، حيث أن القوانين التقليدية المطبقة لم تعد مجدية نظراً لاختلاف الكبير بين الجرائم التقليدية و جرائم المعلوماتية التي يعود بالأساس إلى الطبيعة اللامادية لها و التي هي من أهم الصعوبات التي تعتري سبل مكافحتها وبفعل ما أثاره التطبيق القضائي لنصوص القوانين الجنائية على جرائم الحاسوب من مشكلات ، ولضمان عدم افلات الجناة من العدالة لعدم كفاية القوانين أو عجزها عن الانطباق على هذه الجرائم المستحدثة ، وصونًا لمبدأ الشرعية الذي يقضي بأن لا جريمة ولا عقوبة بغير نص قانوني، ، لهذه الأسباب ، ولمواجهة الخطر المحدق والخسائر الفادحة التي تسببها جرائم الحاسوب اتخذت المواجهة التشريعية لجرائم المعلوماتية عدة مستويات :

أما المستوى الأول فهو المستوى الوطني ، فلقد سارعت دول العالم المتقدم التدابير اللازمة لمواجهة هذه النوعية من الجرائم، فبض هذه الدول حرصت على أن تُضَمن تشريعاتها بخصوص هذه الجرائم إما عن طريق نصوص مستقلة و مثال ذلك قانو اساءة استخدام الحاسب في المملكة المتحدة الصادر في 29 جوان 1990 ، و إما عن طريق تحديث قوانينها و إدماجها في قانون العقوبات ومن أبرز هذه النوعية فرنسا من خلال قانون العقوبات الجديد الصادر سنة 1992 و الذي أضاف فصلاً ثالثاً للباب الثاني من القسم الثالث تحت عنوان " انتهاكات نظم المعالجة الآلية للبيانات Des atteintes aux systèmes de traitement autorisé de données " **و يتكون هذا الفصل من المواد** 1/321 **إلى** 7/323.[42]

و من بين المحطات التالية من محطات التجريم المعلوماتي في فرنسا فكانت عام 2004[43] **عندما أضاف المشرع الفرنسي بموجبه جريمة أخرى هي جريمة التعامل في الوسائل التي تصلح أن ترتكب بها جريمة الدخول أو البقاء غير المصرح بها أو جريمة التلاعب بالمعطيات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات.**

و ثانيها على المستوى الاقليمي ، فلقد حرص المجلس الاوروبي على التصدي للاستخدام غير المشروع للكمبيوتر و شبكات المعلوماتية وفي عام 1989 نشر المجلس الأوروبي دراسة تضمنت توصيات تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسب وهي التوصية التي لحقتها دراسة أخرى في عام 1995 حول الإجراءات الجنائية في مجال الجرائم المعلوماتية، وعلى أساس المبادئ التي تضمنتها التوصيات قام المجلس الأوروبي في عام 1997 بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي وذلك بقصد إعداد اتفاقية في هذا الإطار و تجلى ذلك في اتفاقية بودابست[44] Convention on cyber crime و الموقعة في 23 نوفمبر 2001 و التي سنعكف على دراستها في المطلب الثاني من هذه الدراسة.

وثالثها على المستوى الدولي و تتمثل في جهود الامم المتحدة التي تبتذلها في هذا المضمار.

الهوامش

[1]. جميل عبد الباقي الصغير ، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة ،2002 ، ص 73.

[2]. هي دودة حاسوب ضربت العديد من أجهزة الكمبيوتر في عام 2000، عندما تم إرسالها كمرفق برسالة بريد إلكتروني مع النص "I LOVE YOU" في عنوان الرسالة الدودة وصلت في صناديق البريد في 4 مايو 2000، مع هذا العنوان البسيط "I LOVE YOU" ومرفق "LOVE-LETTER-FOR-YOU.txt.vbs." عند فتح المرفق ،ترسل الدودة نسخة من نفسها للجميع في قائمة العناوين، متنكرة في زي للمستخدم. كما أنها تحدث العديد من التغييرات الضارة لنظام المستخدم. ويكيبيديا، فيروس أحبك 2014/05/14، فيروس أحبك http://ar.wikipedia.org/wiki/

[3]. راسل تاينر، أهمية التعاون الدولي في منع جرائم الإنترنت، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19 06 2007، المغرب، ص 112

[4]. د جميل عبد الباقي الصغير ، المرجع السابق ، ص 74

[5]. عواطف محمد عثمان عبد الحليم ، جرائم المعلوماتية ، مجلة العدل ، العدد الرابع و العشرون ، ص 69 .

[6]. نعيم سعيداني ، المرجع السابق ، ص 93

[7]. عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية و الأنترنت دراسة مقارنة ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، 2007 ، ص111

[8]. المرجع نفسه ، ص 114

[9]. يوسف صغير ، الجريمة المرتكبة عبر الأنترنت ، مذكرة ماجستير حقوق ، جامعة مولود معمري تيزي وزو، الجزائر، 2013 ، ص 96

[10]. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية (الانترنت) ،مذكرة دكتوراه، الجامعة الإسلامية، لبنان ،2004 ، ص92

[11]. د علي جبار الحسناوي ، جرائم الحاسوب و الأنترنت ، دار اليازوي العلمية للنشر و التوزيع ، عمان ، 2009 ، ص 154

[12]. الأنتربول بالإنجليزية Interpol هي اختصار لكلمة الشرطة الدولية بالإنجليزية International Policeوالاسم الكامل لها هو منظمة الشرطة الجنائية الدولية بالإنجليزية International Criminal Police Organizationوهي أكبر منظمة شرطة دولية أنشئت في عام 1923 مكونة من قوات الشرطة لـ 190 دولة ، ومقرها الرئيسي في مدينة ليون بفرنسا، ويكيبيديا، منظمة الشرطة الجنائية الدولية، 2014/05/14 ، http://ar.wikipedia.org/Interpol

[13]. جان فرنسوا هنروت، أهمية التعاون الدولي بين عناصر الشرطة، الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر، 19 -20 جوان 2007 ، المملكة المغربية، ص 100.

[14]. الأنتربول ، الإجرام السبراني، 2014/05/14، مجالات -الإجرام/الإجرام - السيبيري/الإجرام -السيبيريhttp://www.interpol.int/ar.

[15]. الإنتربول ، المرجع نفسه ، ص1

[16]. يونس عرب ، قراءة في الاتجاهات التشريعية للجرائم الالكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، 2 -4 ابريل 2006، مسقط، ص15.

[17]. عبد الله عبد الكريم عبد الله ، المرجع السابق ، ص126

[18]. د. يونس عرب ، المرجع السابق، ص16

[19]. عماد مجدي عبد الملك ، جرائم الكمبيوتر و الأنترنت ، دار المطبوعات الجامعية، الإسكندرية، 2011، ص175

[20]. المجلس الأوروبي ، المذكرة التفسيرية لاتفاقية بودابست 2001 النسخة المترجمة بالعربية، 2014/05/12
http://conventions.coe.int/Default.asp?pg=Treaty/Translations/TranslationsChart_en.htm#185،

[21]. هلالي عبد اللاه أحمد ،جرائم المعلوماتية و أساليب المواجهة و فقاً لاتفاقية بودابست،ط1، دار النهضة، القاهرة، 2007، ص30

[22]. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، ص297

[23]. المرجع نفسه، ص302

[24]. هلالي عبد اللاه أحمد، المرجع السابق، ص 68

* فالقرصنة الإلكترونية أو المعلوماتيّة هي عمليّة اختراق لأنظمة الحاسوب.

[25]. المجلس الأوروبي ، المرجع السابق، ص21

[26]. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 319

[27]. عبد الله عبد الكريم عبد الله، المرجع السابق، ص 133

[28]. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 323

[29]. المجلس الأوروبي، المرجع السابق، ص66

[30]. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص496

[31]. المجلس الأوروبي، المرجع السابق، ص 68

[32]. الدليل الالكتروني هو كل البيانات التي يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسب من إنجاز مهمة ما، عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات، دار الجامعة الجديدة، الاسكندرية، 2010 ، ص53

[33]. علماً أن القانون المدني الجزائري قد انتبه إلى مسألة حجية الدليل الرقمي و التوقيعات الالكترونية و قبولها من طرف القاضي في مادتيه 1/223 و 327 من قانون 10/05 المتعلق بالمنافسة، محمد فولان، الحماية القانونية لتكنولوجيات الإعلام، مجلة المحكمة العليا، الجزائر، العدد01، 2010، ص 41

[34]. المجلس الأوروبي، المرجع السابق، ص69

[35]. فبالنسبة للنوع الأول فقد عرفها المشرع بموجب المادة 02 من قانون 04/09 المتعلق بقانون الوقاية من الجرائم المتصلة بتكنولوجيات العلوم و الاتصال، بأنها أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات توضح مصدر الاتصال، والوجهة المرسلة إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة أما النوع الثاني والمتعلقة بالمحتوى فلم يأت على تعريفها، وإن كانت تتعلق بمضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال.

[36]. الفرق بين حفظ البيانات و توثيق البيانات فالتعبيرين لهما معنى متقارب و لكنه يختلف في مجال المعلوماتية فالتوثيق عبارة عن عملية تخزين للبيانات و الاحتفاظ بها لفترة زمنية معينة، د طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 501

[37]. المجلس الأوروبي، المرجع السابق، ص71

[38]. طارق ابراهيم الدسوقي عطية، المرجع السابق، ص 504

[39]. و مثال ذلك ما جاء في القسم الثالث "في الانتقال و التفتيش و القبض " من الكتاب الأول من قانون 06 -22 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم للأمر55 -165 المؤرخ في 08 يونيو 1965 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 84، الجزائر، 24 ديسمبر 2006

[40]. نبيل صقر، المرجع السابق، ص 160

[41]. المجلس الاوروبي، المرجع السابق، ص95

[42]. Clément ENDRELIN , Les moyens juridiques de lutte contre la cybercriminalité , Diplôme universitaire sécurité intérieur/extérieur dans l'Union Européen , 2011 , p76

[43]. القانون رقم 575 لسنة 2004 في 21/06/ 2004 المتعلق بالثقة في الاقتصاد الرقمي

[44]. نعيم سعيداني ، المرجع نفسه ، ص 85