جامعة دمشق
كلية الحقوق
قسم القانون الدولي

مكافحة الجرائم الالكترونية في القانون الدولي

رسالة أُعدت لنيل درجة الماجستير في القانون الدولي

إعداد الطالب

علاء المرعي

بإشراف الدكتور

ماهر ملندي

الأستاذ المساعد في قسم القانون الدولي

١٤٣٧هـ / ٢٠١٦م

بسم الله الرحمن الرحيم

وقل رب زدني علماً

لجنة مناقشة الرسالة والحكم عليها :

الدكتور ماهر ملندي

أستاذ مساعد في قسم القانون الدولي – كلية الحقوق - جامعة دمشق

عضواً مشرفاً

الدكتورة أمل يازجي

أستاذ مساعد في قسم القانون الدولي – كلية الحقوق - جامعة دمشق

عضواً

الدكتور عيسى المخول

أستاذ مساعد في قسم القانون الجزائي – كلية الحقوق - جامعة دمشق

عضواً

الإهداء

إلى من أخذا بيدي وأنا طفل ... ومنحاني القوة والثقة لأصل إلى حيث أنا ...

إلى من منحاني عمرهما عُمراً من السعادة والأمل ...

إلى والديَّ أطال الله في عُمرهما ...

إلى الورود التي تحيط بي وتبعث في نفسي الأمل ...

إلى من أتمنى لهم أكثر مما أتمناه لنفسي ...

أخي وعائلته

إلى رفيقتي وشريكتي وحبيبتي ومن سنتقاسم العمر معاً ....

حبيبتي لين

إلى رمز الإخلاص والوفاء ...

إلى الكنز الذي لا يقدر بثمن ...

إلى من أحببتهم وأحبوني ...

أصدقائي

شكر وتقدير

أتوجه بعميق الشكر والامتنان إلى أستاذي الفاضل

الدكتور ماهر ملندي

الذي تفضل بقبول الإشراف على هذه الرسالة ومنحني الكثير من وقته ، فكان لنصائحه وتوجيهاته الأثر الأهم في إنجاز هذا البحث .

كما أتقدم بوافر الشكر إلى السادة أعضاء لجنة المناقشة لقبولهم الحكم على هذه الرسالة .

فلا شك أن ملاحظاتهم ونقدهم سيغني هذا البحث .

- **الدكتورة أمل اليازجي**
- **الدكتور عيسى المخول**

مخطط البحـث

مقدمــة

الفصل الأول : مفهوم الجرائم الالكترونية وسبل مكافحتها .

المبحث الأول : مفهوم الجريمة الالكترونية

المطلب الأول : تعريف الجريمة الالكترونية

أولاً : مدلول الجريمة الالكترونية.

ثانياً :الجريمة الالكترونية كإحدى صور الجرائم المنظمة .

المطلب الثاني : أنواع الجريمة الالكترونية

أولاً : جرائم الإضرار بالبيانات .

ثانياً : جرائم الاعتداء على الاشخاص .

ثالثاً :جرائم تصميم البرمجيات الخبيثة وتطورها (الفيروسات)

رابعاً : جرائم الأضرار بالمصالح العامة والخاصة.

خامساً : جرائم الاعتداء على الأموال .

المطلب الثالث: الصفة الدولية للجريمة الالكترونية .

أولا : الجرائم الالكترونية كونها من الجرائم العابرة للحدود .

ثانياً : أهمية مكافحة الجريمة الالكترونية على الصعيد الدولي .

ثالثاً : أهم الصعوبات التي تواجه قمع الجرائم الالكترونية .

المبحث الثاني : مكافحة الجرائم الالكترونية في القوانين الوطنية

المطلب الأول : التشريعات الأجنبية لمكافحة الجرائم الالكترونية.

المطلب الثاني : التشريعات العربية لمكافحة الجرائم الالكترونية.

المطلب الثالث: التشريعات السورية لمكافحة الجرائم الالكترونية

الفصل الثانى: فاعلية القانون الدولى فى مكافحة الجرائم الالكترونية

المبحث الأول: مكافحة الجرائم الالكترونية من قبل المنظمات والمؤتمرات الدولية

المطلب الأول: مكافحة الجرائم الإلكترونية من قبل المنظمات الدولية

أولاً- منظمة الأمم المتحدة .

ثانياً- المنظمة الدولية للشرطة الجنائية . (انتربول).

ثالثاً- المنظمات الإقليمية .

المطلب الثاني: مكافحة الجرائم الإلكترونية من قبل المؤتمرات الدولية

أولاً- مؤتمر الأمم المتحدة السابع حول منع الجريمة لعام ١٩٨٥م .

ثانياً- مؤتمر الأمم المتحدة الثامن حول منع الجريمة لعام ١٩٩٠م .

ثالثاً- مؤتمر الأمم المتحدة العاشر حول منع الجريمة لعام ٢٠٠٠م.

رابعاً- مؤتمر الأمم المتحدة الحادي عشر حول منع الجريمة لعام ٢٠٠٥ م .

خامساً- مؤتمر الأمم المتحدة الثاني عشر حول منع الجريمة لعام ٢٠١٠ م .

المبحث الثاني: مكافحة الجرائم الالكترونية في الاتفاقيات الدولية .

المطلب الأول: الاتفاقات الأوربية حول مكافحة الجرائم الالكترونية .

أولاً: الاتفاقية الأوربية الخاصة بحماية الأفراد من معالجة المعلومات الخاصة بهم لعام ١٩٨١ م.

ثانياً: الاتفاقية الأوربية حول الجريمة الافتراضية لعام ٢٠٠١ م.

المطلب الثاني: الاتفاقيات العربية حول مكافحة الجرائم الالكترونية.

أولاً: القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها .

ثانياً: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .

الخـــاتمة

مُقَدِّمَة

أصبح تناقل الخبر أسرع وأقل كلفة من أي وقت مضى في تاريخ الاتصالات ويعود ذلك إلى ظهور منظومة الانترنت التي أدت إلى حدوث تغيرات جذرية لدى جميع شرائح المجتمع الإنساني ولا سيما على القطاع الإعلامي حيث دخلت في حالة تنافس مع المصادر التقليدية للإعلام مثل الراديو والتلفزيون كما أن بعض الصحف قد قامت بإلغاء طبعته الورقية لتستبدلها بطبعة على شبكة الانترنت.

كما وتتبع أهمية إدخال الانترنت إلى أي بلد من حقيقة أساسية وهي أن شبكة الانترنت تتحدى الحدود والرقابة الحكومية والتقليدية على وسائل الإعلام، وتوفر صوتاً بديلاً عن وسائل الإعلام التقليدية أي أنها تؤمن تدفق المعلومات من دون وجود حدود فعلية، وبالتالي يوفر فرصاً لا تقدر بثمن لتحريك المستخدمين لعبور الحدود الوطنية .

وبين تطور الاتصالات عن بعد وظهور المعلوماتية التي جعلت العالم كله وحدة سكنية واحدة فتطور وسائل الاتصال والمعلوماتية، قد ترتب عليه اكتشاف أنظمة تكنولوجية جديدة أدت إلى ظهور استخدامات جديدة لوسائل الاتصالات عن بعد وتعد العمليات الالكترونية إحدى التجليات الرئيسة لتكنولوجيا المعلومات عن بعد، فهذه الأعمال قد أثرت تأثيراً كبير على البنيان الإداري والاقتصادي من خلال استخدام تقنيات العمل بالانترنت والشبكات لتطوير أنشطة الأعمال الحالية وخلق أنشطة أعمال افتراضية جديدة .

وإن التسارع والتقدم التقني والتكنولوجي الهائل الـذي لحـق بوسـائل الاتصالات الحديثة كالفكس والانترنت وسائر صور الاتصال الالكتروني عبـر الأقمار الصناعية كل ذلك دفع مرتكبي الجرائم الالكترونية لاستغلاله في تنفيـذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الـدول، وهي جرائم مبتكرة ومستحدثة تمثل ضرباً من ضروب الذكاء الإجرامي، حيث استعصى بداية إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجزائية بسبب قصور أنظمة الملاحقة الإجرائية التي تبدو عاجزة على اسـتيعاب هـذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائيـة فـي إطـار القوانين الوطنية أو على صعيد الملاحقة الجنائية الدولية ، مما أوجب تطـوير البنية التشريعية الجنائية لكافة دول العالم لمواجهة هذا الخطر ولا يمكن التوصل إلى ذلك إلا من خلال عقد المؤتمرات الدولية الفاعلة في توحيد الجهود الدوليـة لمواجهة الجرائم الالكترونية وعقد الاتفاقيات والمعاهدات الدولية التي تتكامـل بدورها مع التشريعات الوطنية في سبيل ملاحقة ومكافحة مرتكبي هذه الجـرائم الدولية .

وبالتالي فإن الاتصالات وسرعتها الكبيرة التي لم يعرفها تاريخ الإنسانية من قبل أثرت تأثيراً مباشراً على الدول ولاسيما علـى المسـتويات السياسـية والثقافية والاجتماعية ولذلك من المهم جداً معالجة مشكلة اختراق شبكة الانترنت من قبل العابثين بالأمن المعلوماتي، ولا يمكن تحقيق ذلك دون تعـاون دولـي وثيق يسعى لمكافحة هذه الجرائم العابرة للحدود .

والاشكالية تكمن بأن الجرائم الالكترونية تتسم بحداثة أساليب ارتكابهـا وسرعة تنفيذها وسهولة إخفاء معالمها ودقة وسرعة محو آثارها ، فقد نتج عن ذلك جملة من الصعوبات والاشكاليات العملية التي تعرقل وتقف كحجر عـائق

أمام أجهزة العدالة في مواجهتهم لهذه الطائفة من الجرائم ولاسيما أجهزة البحث والتحري والتي تعمل من أجل استيفاء الدليل الالكتروني ، إذ أصبحت هذه الأخيرة تواجه مشاكل وصعوبات اجرائية أثناء مباشرة مهامها للكشف عن هذا النوع من الجرائم وملاحقة مرتكبيها وتقديمهم للعدالة.

وأمام هذا الوضع ثار السؤال حول ما إذا كان بالإمكان الاكتفاء بالقواعد الإجرائية العادية للبحث عن الجريمة الالكترونية، أم أن الأمر يتطلب وضع قواعد إجرائية خاصة بها تنسجم مع خصوصيتها وطبيعتها؟

وقد جاء هذا البحث بهدف الوقوف على هذه المشكلة وتسليط الضوء على أبعادها القانونية والاجتماعية وعلى التطورات التي لحقت الواقع التشريعي لمكافحة الجرائم الالكترونية على مستوى الدول الأجنبية والعربية، ويهدف إلى تقصي ما أقرته هذه الدول من تشريعات جديدة أو ما تنوي وضعه في تشريعات لا تزال في طور التشريع، وما حقيقته بشأن إنفاذ القائم من هذه التشريعات المتعلقة بمكافحة الجرائم الالكترونية .

كما يسعى البحث إلى تقييم مدى توافق ما أنجز مع الهدف الأساسي وهو إيجاد البيئة التشريعية الملائمة للعصر الرقمي وتطبيقاته، وتحديد مواطن القصور والنقص التي لا تزال قائمة وتحديد السبل والطرق المناسبة لمواجهة هذا الخطر الذي يلاحق الاستقرار المعلوماتي ويحاول ضرب الثقة باستخدام الحاسوب في حياتنا .

الفصل الأول

مفهوم الجريمة الالكترونية وسبل مكافحتها

المبحث الأول

مفهوم الجريمة الإلكترونية

نظراً لظهور الحاسوب والإنترنت في جوانب حياتنا كافة، بدأت تبرز أنواعاً جديدة من الجرائم تسمى الجرائم الإلكترونية، وبالتالي أصبح هناك حاجة لتعريف هذه الجريمة. كما انصب اهتمام المجتمع على التعاون في سبيل مكافحتها وسن القوانين والتشريعات للتعامل مع هذا النوع من الجرائم المستحدثة والعابرة للحدود، آخذين بالحسبان ما تسببه هذه الجرائم من خسائر مادية ومعنوية كبيرة على صعيد الدول والأفراد والمؤسسات.

المطلب الأول : تعريف الجريمة الإلكترونية

تُعرّف الجريمة الإلكترونية بأنها الجريمة الناتجة عن استخدام الإنترنت والتقنية الحديثة والكومبيوتر في أعمال وأنشطة إجرامية، وعادة ما ترتكب بهدف تحقيق عوائد مالية ضخمة جَّراء أعمال غير شرعية، ويعاد ضخها عبر شبكة الإنترنت باستخدام النقود الإلكترونية أو بطاقات السحب التي تحمل أرقاماً سرية أو بتداول الأسهم وممارسة الأنشطة التجارية .

وتعِّرف المنظمة الأوربية للتعاون الاقتصادي الجريمة الإلكترونية "بأنها كل سلوك غير مشروع أو منافٍ للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها ".[1]

---

[1] د. عبد الله عبد الكريم عبد الله ، جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية) ، الطبعة الأولى، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٧ ، ص١٥-١٦.

ويُعّرف المجرم المعلوماتي، بأنه ذاك الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسوب الإلكتروني، والقادر على استخدام هذا التكتيك لاختراق الرقم السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه .

وفي الاصطلاح الإلكتروني، يطلق خبراء أمن المعلومات الإلكترونية مصطلح هاكرز "Hackers" وهي جمع لكلمة (هاكر)، وهو الإنسان الذي يقوم بعمليات الاختراق والتخريب عبر شبكة الإنترنت، كما يطلقون مصطلح "كراكرز" "Crackers" على المتخصصين بفك شفرات البرامج وليس تخريب الشبكات ، فهم نوع من الهاكرز المتخصص .

كما أن المجرم الالكتروني هو الشخص الذي يملك قدرات تقنية خاصة تمّكنه من ارتكاب الجريمة الإلكترونية عن طريق استخدام الكومبيوتر وشبكة الإنترنت، مما يؤدي لإحداث اضطرابات في المجتمع الدولي، نظراً لمخالفته قواعد الأمن الالكتروني العالمية.

أولاً : مدلول الجريمة الإلكترونية :

تنطوي الجريمة الإلكترونية الخالصة على ست خطوات أساسية ، يتمّ تنفيذها آلياً بواسطة برنامج محدد أو عدة برامج، ويمكن تحديد هذه الخطوات:

١. البحث عن نظام الحاسب الآلي الذي يحتوي على المعلومات أو البرامج المطلوبة .
٢. الوصول إلى نقاط الضعف في النظام الذي يحتوي على هذه المعلومات أو البرامج .

٣. الاستفادة من نقاط الضعف التي تعتري النظام للدخول إليه ثم التحكم فيه.
٤. تنفيذ السلوك الإجرامي الذي تمّ تحديده مسبقاً .
٥. تحويل هذا السلوك إلى ربح غير مشروع يحصل عليه الفاعل، أو إلى خسارة تلحق بالمجني عليه .
٦. إخفاء جميع الأدلة تجنباً لكشف الفاعل وسلوكه الإجرامي .[١]

وتختلف التسميات التي تطلق على الجريمة الإلكترونية من حيث اتساع مدلولها، فقد تسمى (الجريمة التقنية)، حيث يتسع مدلولها لكي يشمل كل الجرائم التي يتمّ ارتكابها بوسائل تكنولوجية ، ويشمل ذلك بطبيعة الحال جرائم الحاسوب والإنترنت، وكل ما يعتمد على التقنية كما هو الشأن في استخدام تقنية الهاتف النقال أو المحمول لارتكاب جرائم القدح والقذف أو البلاغ الكاذب والتهديد وكذلك استخدام تقنية الحاسوب في حفظ سجلات الاتجار غير المشروع بالمخدرات والمؤثرات العقلية والرقيق الأبيض والتجارة بأعضاء البشر والأطفال .[٢]

وقد تسمى الجريمة الإلكترونية بمصطلح "جرائم المعلوماتية" ، وهذا النوع من الجرائم ليس حديثاً على النحو الذي يستشعر حداثته بعض الفقه المقارن . فالجريمة المعلوماتية لها جذور في قانون العقوبات المقارن ، فهي تحتوي على مجموعة من الجرائم محلها المعلومات ، كجرائم التجسس والتخابر والحصول على وثائق وأسرار الدفاع عن البلاد والاكتشافات والاختراعات العلمية

---

[١] د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية ، بيروت ٢٠٠٤ ، ص٣٦.

[٢] د. عمر محمد أبو بكر بن يونس ، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية) ، دار النهضة العربية ، القاهرة ، ٢٠٠٤ ، ص٢١٩ .

والابتكارات الصناعية التي يلزم بقاؤها سرية . فالجريمة المعلوماتية ذات جذور في قانون العقوبات إلا أن الجديد هنا هو ما استحدثته ثورة المعلومات المعاصرة في تطوير الدور الايجابي لمبدأ الحق في المعرفة الذي يعد الأساس الذي تقوم عليه ثورة المعلومات المعاصرة.

إلاَّ إن مصطلح "الجريمة المعلوماتية" يستخدم للدلالة على الجرائم الناشئة عن استخدام الإنترنت ، وهو استخدام ناقص لكونه في الحقيقة يعبر عن نوعية محددة من جرائم الإنترنت ،وهي الاستيلاء على المعلومات عبر الإنترنت ، كما هو الشأن في جرائم التجسس الاقتصادي عبر الإنترنت في التشريع الأمريكي .[1]

ولابد من تحديد مفهوم الإنترنت باعتبارها الأداة أو الوسيلة التي ترتكب عن طريقها الجريمة الإلكترونية (فمصطلح الإنترنت) مشتق من لفظين أثنين هما لفظ (دولي) ولفظ (شبكة عمل) ويطلق بعض الاختصاصين في هذا المجال على الشبكة المذكورة مصطلّح (الشبكة العالمية) [2]

والإنترنت من الناحية القانونية ، نظام اتصالات عامة لا تمتلكه أي مؤسسة . ويمكن الوصول إليه دولياً، فهو شبكة دولية لحسابات تتصل ببعضها البعض عبر خطوط الهاتف أو عبر أسلاك معينة.

ونلاحظ بأن هذه المصطلحات التي تدل على الجريمة الإلكترونية تتشارك بمعيار مهم وهو الطابع الدولي أو العالمي الذي لا يعترف بحدود، وهو

---

[1] المرجع السابق ، ص٢٢٠ .

[2] د. سليم عبد الله الجبوري ، الحماية القانونية لمعلومات شبكة الإنترنت ، الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت، ٢٠١١ ، ص ٢٢ .

المقياس الحقيقي للجريمة الإلكترونية. كما يوجد مقياس أخـــر هـــو المصـــلحة المعتدى عليها، ومقدار الضرر الذي يتعرض له المجتمع الدولي ، والتأثير على الثقة الدولية المعتمدة بين دول العالم .

ثانياً : الجريمة الإلكترونية كإحدى صور الجرائم المنظمة

عـــرَّفت الأمم المتحدة الجريمة المنظمة في اتفاقيـــة الأمـــم المتحـــدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٢ المادة /٢/ فقرة /أ/، بأنهـــا جماعة ذات هيكل تنظيمي ، مؤلفة من ثلاثة أشخاص أو أكثر ، موجودة لفتـــرة من الزمن وتعمل بصورة متضافرة بهدف ارتكاب واحدة أو أكثر من الجـــرائم الخطيرة أو الأفعال المجرمة من أجل الحصول ، بشكل مباشر أو غير مباشـــر، على منفعة مالية أو منافع مادية أخرى .[١]

كما تُعرف الجريمة المنظمة بأنها " تلك النوعية من الأنشطة الجماعيـــة ذات التشعب الواضح المعالم من حيث النطاق الشخصي والموضوعي."

ويتمّثل الجانب الشخصي للجريمة الإلكترونية، بارتكابها من قبل شخص واحد أو أكثر، فهنالك غالباً مجموعة أشخاص مرتبطين ببعضهم بكيان إجرامي وبنطاق إلكتروني، يستخدمون شبكة الإنترنت لتحقيق فكرة التنظيم العصـــابي الالكتروني المناهض لفكرة نظام اجتمّاعي أو اقتصادي قائم في دولة ما أو دول متعددة .أما من الناحية الموضوعية فالجريمة الإلكترونية قد تكون كجرائم غسيل الأموال عبر الإنترنت ، أو جرائم واقعة علـــى الملكيـــة الفكريـــة، أو انتحـــال

---

[١] الاتفاقية منشورة علـــى الموقـــع الإلكترونـــي: http://www1.umn.deu/humanats/arab/corgcrim e.htm/

الشخصية، أو جرائم إتلاف المعلومات المتعلقة بالمصارف والبنوك والشـــركات الكبرى، أو كالجرائم الإباحية وغير الأخلاقية والجنسية.

وتهدف الجريمة المنظمة في الأساس إلى الإفادة المادية وتحقيق الأرباح غير المشروعة ، من خلال مواصلة العمل بوسائل إجراميـــة، فكمـــا تســـتعين الشركات العادية بشبكة الإنترنت بحثاً عن فرص جديدة لتحقيق الأرباح ، كذلك تفعل المنظمات الإجرامية .

فالجرائم المالية تسود بدرجة أكبر مع النشاطات المرتبطة بالإنترنت . فالتلاعب في أسعار أسهم الشركات المرتبط بالإنترنـــت يولـــد خســـائر تقـــدر بعشرات آلاف الملايين من الدولارات في السنة للمستثمرين ، فهي توفر مجالاً واسعاً لأرباح الجريمة المنظمة . فمن وجهة نظر جماعات الجريمة المنظمة ، توفر شبكة الإنترنت، نمواً للتجارة الإلكترونية ومجموعة من الأهداف للتغلغـــل وممارسة النفوذ ، وهو احتمال يشير إلى وجوب أن تكون تكنولوجيا الإنترنـــت وشركات خدمات الإنترنت حذرة بصورة خاصة حـــول الشـــركاء المحتمّلـــين والداعمين الماليين لها ، وخضوعها وملكيتها للرقابة الحكومية .

وفي هذا السياق توفر شبكة الإنترنت مجالات هائلـــة جديـــدة وســـهلة لتحقيق أرباح غير مشروعة، وذلك عبر أنشطة تتخذ من الشبكة والكومبيـــوتر أداة للجريمة .فخلال السنوات القليلة الماضية ، بدأت بعض المجموعات التـــي تتعاطى الجريمة المنظمة كحرفة لها ببناء قاعدة لدى بعض الدول التي تؤمن لها ملاذاً آمناً تستطيع من خلاله ممارسة عملياتها العابرة للأوطان .

مع العلم بأن ساحة الجريمة في هذا العالم الافتراضـــي أي فـــي عـــالم الشبكات الإلكترونية ، لا توجد له أي حدود ، ويشكل ذلك مزية تجعل النشـــاط الإجرامي عملاً سهلاً للغاية مقارنة بالواقع التقليدي للجريمة .

وعندما تحاول السلطات المختصة مراقبة هذا العالم الافتراضي المتمّثل بشبكة الإنترنت تبدو أمامها حدود البلدان ومناطق الصلاحيات واسعة جداً، مما يجعل التحقيق في الجرائم الإلكترونية ومحاولة مكافحتها تحدياً صعباً .

وهكذا نجد بأن الترابط بين الجريمة المنظمة وشبكة الإنترنت ليس طبيعياً فقط ، ولكنه ترابط من المرجح له أن يزدهر وأن يتطور إلى حد أبعد في المستقبل. فشبكة الإنترنت تؤمن الطرق والوسائل لتحقيق أرباح كبيرة بأقل قدر ممكن من المخاطر. وجماعات الجريمة المنظمة لا تريد أكثر من ذلك. ولهذا كان من الضروري إظهار العلاقة بين الجريمة المنظمة والجريمة الإلكترونية من أجل بيان سبل مكافحة هذه الجريمة على الصعيد الدولي .

المطلب الثاني : أنواع الجريمة الإلكترونية

تصنف الجرائم الإلكترونية ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، فهنالك جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته ، وهنالك فئات تختلف فيما بينها حسب الأسلوب المتبع في الجريمة أو الباعث أو الدافع لارتكاب الجريمة أو تعدد محل الاعتداء.

ولا نبالغ إذا قلنا إنه ثمة نظريات ومعايير عدة لتصنيف مختلف الجرائم الإلكترونية ، ومع هذا سنحاول أن نقف على أبرز التصنيفات وأهمها الآتي:

أولا: جرائم الإضرار بالبيانات

تعد هذه الفئة من الجرائم الإلكترونية الأشد خطورةً وتـأثيراً وأكثرهـا حدوثاً. وتشمل هذه الفئة على كل الأنشطة من تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل للمعلومات وقواعد البيانـات الموجـودة بصـورة الكترونيـة (Digital form) على الحواسيب الآلية المنظمة أو غيـر المنظمـة بشـبكات المعلومات، أو مجرد محاولة الدخول بطريقة غير مشروعة عليهـا ، وبمعنـى أخر وصول شخص غير مصرح له وإمكانية دخوله إلـى حجـرة الحواسـيب المركزية بالمؤسسة ثم خروجه دون إحداث أي أضرار ، ويعُـد ذلـك خرقـاً لسياسة وإجراءات أمن المعلومات بتلك المؤسسة .

وبالتالي فإن استخدام شبكة الإنترنت يؤدي للدخول إلى قواعد البيانات أو مواقع الإنترنت والحصول على معلومات غير مسموح بهـا، أو إمكانيـة السيطرة التامة على تلك الأنظمة بالرغم من وجود إجـراءات حمايـة متعـددة الدرجات وأنظمة كشف ومنع الاختراق والدخول إلى أنظمة المعلومات، وبالتالي يعطي المؤشر أو الإنذار لهذه المؤسسة لتغير نظام الحماية الموجود لها، والقيام بتحديث دوري لأنظمة أمن المعلومات لمواكبة التطور الدائم بأساليب الاختراق .

أما بالنسبة إلى تعديل أو محو أو سرقة أو إتلاف أو تعطيل العمل لنظم المعلومات ، فإن تلك الأنشطة تتمّ بواسطة أفرادٍ هواة أو محترفين يطلق عليهم الهاكر (Hackers)، وهم الذين يقومون بهذه الأعمال بغرض الاستفادة المادية أو المعنوية من البيانات أو المعلومات التي يقومـون بالاسـتيلاء عليهـا ، أو بغرض الاضرار بالجهة صاحبة تلك الأنظمة لوجود كره شخصي مثل موظف في إحدى المؤسسات يرغب بالانتقام من هذه المؤسسة أو حقد سياسي أودينـي للقيام بهذا العمل .

ويعتمد هذا النوع من الجريمة الإلكترونية على إغراق أجهزة الخـــوادم بآلاف أو ملايين الطلبات للحصول على معلومات، الأمر الذي قـــد لا تحتملـــه قدرة المكونات المادية، أو نظم قواعد البيانات والتطبيقات والبرامج الموجـــودة على تلك الخوادم، والتي قد تصاب بالشلل التام لعدم قدرتها على تلبية هذا الكـــم الهائل من الطلبات والتعامل معها .

ويحتاج الأمر إلى ساعات عديدة حتى يتمّكن مديرو النظم والشبكات من التعرف على مصادر الهجوم، وعيوب النظم لديهم واستعادة العمـــل بصـــورة طبيعية، وبالطبع فإن هذه الساعات من الاســـتخدام التـــي يكـــون فيهـــا نظـــام المعلومات مُعطلاً، تكبد المؤسسة خسائر مادية جسيمة فضلاً عن تعطيل مصالح المتعاملين مع تلك الأنظمة وفقدانهم الثقة في تلك المؤسسة، وهـــروب العمـــلاء منها إلى مؤسسات منافسة كلما أمكن ذلك.

ومثال ذلك، حادث "أوميغا"، حيث أقدم مصمم ومبرمج شبكات كومبيوتر ورئيس سابق لشركة (omega) من مدينة "Delaware " ويدعى "Timothy" على إطلاق قنبلة إلكترونية في عام١٩٩٦بعد ٢٠ يوماً من فصله من العمل، فاستطاع أن يلغي جميع تصاميم وبرامج الإنتاج لإحدى كبرى مصانع التقنية العالية فـــي نيوجرسي، والمرتبطة والمؤثرة على نظم تحكم مستخدمة في "nasal" والبحرية الأمريكية ، ملحقاً خسائر بلغت ١٠ مليون دولار، وتعد هذه الحادثة مثالاً حيـــاً على مخاطر جرائم الإضرار بالبيانات المخزنة على الكومبيوتر ، بل اعتبـــرت أنها أكثر جرائم تخريب الكومبيوتر خطورةً.[١]

---

[١] عبد الصبور عبد القوي علي مصري ، الجريمة الإلكترونية ، ، دار العلوم للنشر والتوزيع، مصر ، ٢٠٠٨، ص٣٤.

ثانياً: جرائم الاعتداء على الأشخاص

يقصد بالاعتداء على الأشخاص ، أفعال القدح و القــذف و التشـــهير، وبث أفكار وأخبار من شأنها الإضرار الأدبي أو المعنوي بالشخص أو الجهــة المقصودة . وتتنوع طرق هذا الاعتداء على الموقع الشخصي للشخص المشهر به وتغيير محتوياته. ويندرج هذا النوع من الاعتداء ضمن مصطلح الجرائم التي تتمّ ضد الحواسب والشبكات كنشر أخبار و معلومات غير صحيحة على موقــع الشخص المعتدى عليه.

وتعد جرائم القذف والقدح من أكثر الجرائم التـــي تقــع عــن طريــق الإنترنت، فنجد بعض المتعاملين بشبكة المعلومات العالمية يستســهل الرمـــي بالقذف والقدح للآخرين عبر الإنترنت لأسباب عدة أهمها :

- إن من يرتكب هذه الجرائم يختفي وراء أسماء وهمية فيأمن بــذلك العقوبة.
- إن المتعاملين بالإنترنت لا تحدهم حدود جغرافية ، فتجد القاذف أو الشاتم من بلد والمقذوف أو المسبوب من بلد آخر ، الأمر الذي يأمن معه من الملاحقة القضائية.

وتظهر هذه الجريمة أيضاً في أفعال الاعتداء على حقوق الملكية الفكرية و أسماء مواقع الإنترنت (Damain Names). فالقاعدة العالمية في تســجيل أسماء النطاقات على شبكة الإنترنت، أن التسجيل بالأســبقية ولــيس بالأحقيــة (First come Firstserved)، الأمر الذي أحدث الكثير من المخالفات التي تتمّ على صعيد القضاء.

ومن الجرائم الأخرى المتعلقة بأسماء النطاقات على شبكة الإنترنت ما يعرف بإعادة التوجيه (Redinection)، مثلما حدث لموقع شركة Nike في شهر حزيران عام ٢٠٠٠، حيث قامت جماعة من المحترفين بالدخول على موقع شركة تسجيل النطاقات الشهيرة والمعروفة باسم (Network solutions) ، ومن ثم تغيير بيانات النطاق لضعف إجراءات أمن المعلومات بالشركة في ذلك الحين، وبذلك تمّت إعادة توجيه مستخدمي إنترنت إلى موقع لشركة انترنت في اسكوتلاندا[١].

ثالثاً : جرائم تصميم البرمجيات الخبيثة (الفيروسات) وتطورها

يعرف البرنامج الخبيث بأنه برنامج مكتوب بإحدى لغات البرمجة ، حيث يتمّ إدخاله بواسطة أحد المخربين بهدف إحداث الضرر بنظام الحاسوب . ويمثل فيروس الحاسوب نوعاً من أنواع جرائم التعدي على النظم الإلكترونية .[٢]

وقد استمّرت الفيروسات في التطور و الانتشار ، حتى بات يظهر ما يقارب المئتين فيروس جديد شهرياً. والتي تعددت خصائصها وأضرارها. فالبعض ينشط في تاريخ معين والبعض الأخر يأتي ملتصقاً بملفات عادية، و عند تشغيلها فإن الفيروس ينشط و يبدأ في العمل الذي يختلف من فيروس لأخر وقد يقوم الفيروس بإتلاف الملفات الموجودة على القرص، الصلب أو إتلاف

---

[١] مقالة بعنوان أنواع جرائم الكمبيوتر والأنترنيت منشورة على الموقع الالكتروني www.lawjo.net

[٢] أ.أسامة فتحي ، فيروسات الحاسب ، بحث منشور على الموقع –http://www.kutub.info 2494.pdf ، ص٣ .

القرص الصلب ذاته، أو إرسال الملفات الهامة بالبريد الالكتروني و نشرها عبر شبكة الإنترنت.

وقد ظهرت مؤخراً نسخاً مطورة من الفيروسات تسمى (الديدان) التي لديها القدرة على العمل والانتشار من حاسب لأخر من خلال شبكات المعلومات بسرعة رهيبة، و تقوم بتعطيل عمل الخوادم المركزية والإقلال من كفاءة وسرعة شبكات المعلومات أو إصابتها بالشلل التام . وهنالك نوع أخر يدعى حصان طروادة (Trojan Horse) يقوم بالتخفي داخل الملفات العادية ، ويحدث ثغرة أمنية في الجهاز المصاب تمّكن المخترقين من الدخول بسهولة على ذلك الجهاز، و العبث بمحتوياته ، و نقل أو محو ما هو مهم منها، أو استخدام هوية هذا الجهاز في الهجوم على أجهزة أخرى ، والذي يتمّ من خلال الحصول على عنوان الإنترنت الخاص بجهاز الضحية، و منه يتمّ الهجوم على أجهزة أخرى. [1]

ومثال على ذلك قضية موريس، وهي إحدى أولى الهجمات الكبيرة والخطرة في بيئة الشبكات. ففي شهر تشرين الثاني عام ١٩٨٨ تمّكن طالب يبلغ من العمر ٢٣ عاماً ويدعى "روبير موريس" من إطلاق فيروس عرف باسم (دورة موريس) عبر الإنترنت ، أدى إلى إصابة ٦ ألاف جهاز يرتبط معها حوالي ٦٠٠٠٠ نظام عبر الإنترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مئة مليون دولار، إضافة إلى مبالغ أكثر من ذلك تمّثل الخسائر

[1] مقالة منشورة بعنوان أنواع جرائم الكمبيوتر والانترنت على الموقع الالكتروني www.lawjo.net

الغير مباشرة الناجمة عن تعطيل هذه الأنظمة، وقد حكم على "موريس" بالسجن لمدة ٣ أعوام وعشرة آلاف دولار غرامة .[١]

رابعاً : جرائم الأضرار بالمصالح العامة والخاصة

تندرج ضمن طائفة هذا النوع من الجرائم الالكترونية باستخدام الحواسب الآلية و الشبكات للتشهير بالأشخاص المعنويين أو الحقيقيين، ومنها بث أفكار ومعلومات، وأحياناً أخبار و فضائح ملفقة من خلال بناء مواقع على شبكة الإنترنت تحتوي على كافة البيانات الشخصية، مع العديد من الأخبار والموضوعات التي من شأنها الإضرار الأدبي و المعنوي بالمصالح الخاصة والمادية للشخص أو الجهة المقصودة.

ويتمّ أيضاً استخدام الحواسب الآلية و شبكة الإنترنت في انتهاك حقوق الملكية الفكرية لبرامج الحاسب، و المصنفات الفنية المسموعة و المرئية، و نشرها و تداولها عبر شبكات الإنترنت فيما يعرف بالقرصنة، الأمر الذي يلحق الضرر المادي والمعنوي بمصالح الأشخاص أو الجهة المالكة لتلك المواد.

ويتمّ استخدام الحاسب لنسخ جميع المصنفات المسموعة و المرئية، و توزيعها بصورة غير مشروعة سواء من خلال الاسطوانات الممغنطة، أو من خلال مواقع الإنترنت التي انتشرت انتشاراً كبيراً في الآونة الأخيرة. وأيضا انتشرت برامج تبادل الملفات بين مستخدمي الإنترنت التي يتمّ استخدامها في تبادل الأغاني والأفلام و البرامج غير المرخصة.

---

[١] المرجع سابق.

ومن أشكال هذه الجريمة هي التخابر أو الاتصال بين أفراد منظمة اجرامية ، أو نشاط يهدد أمن و استقرار الدولة أو نشاط محرم قانوناً مثل شبكات الدعارة التي باتت وسيلة الاتصال الرئيسة التي لها حجرات الدردشة (Chatting Rooms)منتشرة عبر شبكة الإنترنت .

ومثال على ذلك قضية الجحيم العالمي، حيث تعامل مكتب التحقيقات الفدرالية مع قضية أطلق عليها اسم مجموعة الجحيم العالمي (GLOBAL HELL) . فقد تمّكنت هذه المجموعة من اختراق مواقع البيت الأبيض ووزارة الداخلية الأميركية، وقد أدين اثنين من هذه المجموعة جرّاء تحقيقات الجهات الداخلية في الولايات المتحدة ، وقد تبين من خلال التحقيقات أن هذه المجموعة تسعى إلى الاختراق أكثر من التدمير أو التقاط المعلومات الحساسة. وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها ، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة.[1]

وكذلك حادثة المواقع الاستراتيجية التي حصلت في ١٩ تشرين الثاني ١٩٩٩، فقد تمّت إدانة شخص أميركي يدعى (Eric burns) من قبل محكمة فيرجينيا الغربية بالحبس لمدة خمسة عشرة شهراً، والبقاء تحت المراقبة السلوكية لمدة ٣سنوات، بعد أن أقر بأنه قام وبشكل متعمدٍ باختراق كومبيوترات محمية، الحق فيها ضرراً بالغاً في كل من ولايات فيرجينيا وواشنطن إضافة إلى مدينة لندن في بريطانيا ، وقد تضمن هجومه الاعتداء على مواقع لحلف الأطلسي، إضافة إلى الاعتداء على موقع نائب رئيس الولايات المتحدة، كما اعترف بأنه قد اطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق

[1] عبد الصبور عبد القوي علي مصري ، مرجع سابق ، ص ٣١- ٣٢ .

كومبيوترات البيت الأبيض ، وقد قام (Eric) بتصميم برنامج أطلق عليه (webbandit) ليقوم بعملية تحديد الكومبيوترات المرتبطة بشبكة الإنترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها ، وباستخدام هذا البرنامج اكتشف أن الخادم الموجود في فيرجينيا، والذي يستضيف مواقع حكومية وإستراتيجية، منها موقع نائب الرئيس، يتوفر فيه نقاط ضعف تمّكن من الاختراق ، فقام في الفترة مابين آب ١٩٩٨ وحتى كانون الثاني ١٩٩٩ باختراق هذا النظام أربع مرات، وآثر نشاطه على العديد من المواقع الحكومية التي تعتمّد على نظام وموقع (USIA) للمعلومات ، وفي إحدى المرات تمّكن من جعل آلاف الصفحات من المعلومات متوفرة، مما أدى إلى إغلاق هذا الموقع لثمانية أيام ، كما قام بالهجوم على مواقع لثمانين مؤسسة إعمال يستضيفها خادم الشبكة (LASER.NET) في منطقة فيرجينيا والعديد من المؤسسات العاملة في واشنطن، إضافة إلى جامعة واشنطن، والمجلس الأعلى للتعليم في فيرجينيا (رتشموند)، ومزود خدمات إنترنت في لندن ، وكان يستبدل صفحات المواقع بصفحات خاصة به تحت اسم (ZYKLON) أو باسم الامرأة التي يحبها (CRYSTAL) .[١]

خامساً: جرائم الاعتداء على الأموال

مع اعتماد المؤسسات المصرفية والمالية على تكنولوجيا المعلومات و الاتصالات والتحول التدريجي في جميع أنحاء العالم نحو ما يطلق عليه تسمية البنوك والمصارف والمؤسسات المالية الإلكترونية، شهد هذا التطور ظهور عدد كبير من الجرائم الإلكترونية.فعلى مستوى البنوك و المؤسسات المالية، تمّت أتمتة نظم الإدارة و المحاسبة، و ربط الأفرع المختلفة لتلك المؤسسات بعضها

[١] عبد الصبور عبد القوي ، مرجع سابق ، ص٣٣ .

ببعض من خلال شبكات المعلومات لضمان سهولة و يسر إدارة العمليات المالية داخلها. و تمّ تحقيق تعامل المؤسسات مع العملاء عن بعد عن طريق الاتصال المباشر من خلال شبكات المعلومات الخاصة غير المتاحة لمستخدمي الإنترنت (Private Networks)التي كان لها بعض القيود المكانية للاتصال، أو من خلال شبكة الإنترنت التي تشكل واجهة لتلك التعاملات .(Web Interface) ، وتمّ أيضاً استخدام بطاقات الائتمان و الدفع الالكتروني (Credit Cards) بأنواعها المختلفة لتسهيل المعاملات و التوجه للإقلال من التعاملات بالنقد المباشر في إطار التحول إلى المجتمّع اللانقدي (Cash–less Society) دون الخوض في تفاصيل فوائد وأهمية مثل هذا النوع من التعامل المالي و آثاره الايجابية على كفاءة البنوك في القيام بدورها، وأيضا آثاره على الاقتصاد ككل، فان ذلك النوع من التعاملات قد أصبح أمراً واقعاً يتزايد الاعتماد عليه خصوصاً بعد تنامي حجم الأعمال التي تتمّ من خلال التجارة الإلكترونية Electronic) (Commerce وظهور الأسواق الإلكترونية (Electronic Marketplace) لتسويق وبيع السلع والخدمات. وظهر نتيجة ذلك خدمات كثيرة مثل الاشتراك في النوادي الخاصة، أو الاشتراك في مسابقات على الشبكة أو لعب القمار أو ألعاب أخرى لقاء أجور محددة. ففي دولة مثل الولايات المتحدة الأميركية فإنه يوجد بها حوالي ١٨٥ مليون بطاقة بنسبة ٦٣ % من إجمالي عدد السكان.أما بالنسبة للصين، فان حجم التعاملات المالية باستخدام بطاقات الائتمان قد تعدى ال ١٦٩ مليار دولار أميركى في عام ٢٠٠١.[١]

ومن أشهر جرائم سرقة الأموال و التي جرت أحداثها في إمارة دبي بدولة الإمارات العربية المتحدة في أواخر عام ٢٠٠١ ما قام به مهندس حاسوب

---

[١] مقالة منشورة على الموقع الإلكترونية بعنوان أنواع جرائم الكمبيوتر والأنترنيت www.lawjo.net

آسيوي يبلغ من العمر ٣١ عاماً، و تمّ نشر وقائع الجريمة في نيسان من عـــام ٢٠٠٣، حيث قام بالعديد من السرقات المالية لحسابات عملاء في ١٣ بنكاً محلياً و عالمياً، وباختلاس الأموال من الحسابات الشخصية، و تحويل تلك الأموال إلى حسابات وهمية ، كما قام أيضا بشراء العديد من السلع و الخدمات عبر شـــبكة الإنترنت مستخدماً بيانات بطاقات الائتمّان والحسابات الشخصية لعدد كبير من الضحايا. كُلّ ذلك تمّ من خلال الدخول للشبكة من خلال إحدى مقاهي الإنترنت العامة المنتشرة في دبي، و قد بلغت قيمة الاختلاسات حوالي ٣٠٠ ألف درهـــم من البنوك المحلية بالإمارات فقط.

وكما حدثت جريمة أخرى لدى أحد فروع سيتي بنك بالولايـــات المتحـــدة الأميركية عام ١٩٩٤، حيث استطاع مواطن روسي الجنسية الاستيلاء على ما يقارب ٤٠٠ ألف دولار أميركي.[١]

ومن الطرق التي يستخدمها لصوص بطاقات الائتمان نشر مواقع وهميـــة لبنوك أو مؤسسات لتقديم الخدمات، و توريد السلع يكون الغرض الرئيسي منها الحصول على بيانات تلك البطاقات.

وقد قام المركز القومي لمعلومات جـــرائم الســـرقات بالولايـــات المتحـــدة الإميركية The National Fraud Information Center (NFIC) الذي تـــمّ إنشاؤه عام 1992 بالتعرف على أوجه الحماية من الجرائم الإلكترونية وآثارها السلبية، ويقوم الزبائن بالشراء الشراء عن طريق الإنترنت عبر الاتصال علـــى الرقم الساخن لهذا المركز، أو عن طريق البريد الالكتروني المخصص له على

---

[١] المرجع السابق .

شبكة الإنترنت ، والإبلاغ عن أية مخالفات أو سرقات تمّت لهم من خلال بطاقات الائتمان. [١]

وتعد ظاهرة غسل الأموال الحاصلة من أنشطة غير مشروعة من أبرز الأنماط الإجرامية المستحدثة التي تقوم بها شبكات منظمة تمّتهن الإجرام، حيث تأخذ درجات عالية من التنسيق والتخطيط والانتشار في أنحاء العالم كافة. وتشير إحصائيات الأمم المتحدة وصندوق النقد الدولي إلى أن أكثر من ٣٠ مليار دولار أمريكي من الأموال القذرة تغسل سنوياً عبر الإنترنت مخترقة حدود ٦٧ دولة في العالم [٢].

ومثال على ذلك قضية العملة الرقمية لشركة (E-Gold) . فمنذ البدايات الأولى للانترنت، ظهر العديد من البدائل للعملات الورقية التقليدية كان أخرها ما بادرت إليه شركة أمريكية تسمى (E-Gold) حيث تقدم للمتسوقين وأصحاب الأنشطة التجارية بديلاً فريداً للمعاملات التجارية عبر الإنترنت. وتقدم (E-Gold) لعملائها عملة رقمية تطلق عليها الذهب الإلكتروني، ولا يحتاج فتح حساب لدى موقع الشركة إلا بضع نقرات على الماوس .ويمكن للعملاء أن يستخدموا أسماء وهمية لأنه لا توجد جهة تراقب أنشطة الشركة . وعن طريق بطاقة ائتمان أو تحويل الكتروني يشتري العميل وحدات من الذهب الالكتروني يمكن نقلها ببساطة لأي عميل أخر لديه حساب لدى الشركة. وبالنسبة لمتلقي الأموال تتمّ عملية تحويل وحدات الذهب الالكتروني إلى أموال تقليدية بنفس السهولة دون الحاجة للكشف عن هويته الحقيقية. وتجتذب فكرة الذهب الالكتروني الأشخاص الذين يفضلون الاستثمار في الذهب ، ويعتقدون أن

---

[١] المرجع السابق .

[٢] المرجع السابق.

الأموال يجب أن ترتبط به. وتتباهى شركة (E-Gold) بأن عملتها الافتراضية مدعومة باحتياطي ذهبي مخزن في لندن ودبي .

ولكن الفكرة تجتذب أيضاً المجرمين الذين يريدون نقل الأموال بسرعة ودون أن يكتشفهم أحد. في حين تخضع المصارف الأميركية وشركات تحويل الأموال التقليدية مثل "western union" لالتزامات قانونية بمراقبة عملائها وإبلاغ السلطات عن أي تحويلات مريبة، لا تواجه (E-Gold) هذه المشكلة، فالشركة تمارس أنشطتها من ولاية فلوريدا الأمريكية لكنها مسجلة في جزيرة (نيفس) بالبحر الكاريبي، حيث القوانين المالية متساهلة للغاية .

ففي ١٩ كانون الأول ٢٠٠٥ قام عملاء من مكتب التحقيقات الفيدرالي (FBI) بتفتيش مقر شركة "gold and silver reserve" الشركة الأم لشركة "E-Gold " في مدينة "ميلبورن" بولاية فلوريدا الأمريكية ومنزل مؤسس الشركة "douglas Jackson'، وقاموا بنسخ وثائق وملفات الكومبيوتر. ويؤكد المحققون في هذه الجرائم أن عملات رقمية أخرى يتمّ استخدامها بنفس الطريقة لخدمة أغراض غير قانونية، وتوجد مجموعة من هذه الخدمات على الأقل في مناطق مثل روسيا وبنما، وتزعم ثمانية منها على الأقل بما في ذلك (E-Gold) إن سبائك ذهب حقيقية تغطى المعاملات المالية التي تنفذها هذه الشركات، وتحقق (E-Gold) ومنافسوها أرباحاً من خلال تحصيل نسبة صغيرة من الرسوم على تلك التحويلات .[١]

ويتبين مما سبق بأن جرائم الحاسوب في نطاق الظاهرة الإجرامية المستحدثة، جرائم تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج)

---

[١] د. عبد الله عبد الكريم عبد الله ، مرجع سابق ، ص٥٠-٥١ .

وتطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب، وأن الجرائم التي تنصب على الكيانات المادية تدخل في نطاق الجرائم التقليدية، ولا تندرج ضمن الظاهرة المستجدة لجرائم الحاسوب.

المطلب الثالث: الصفة الدولية للجريمة الإلكترونية

فقدت الحدود الجغرافية كل أثر لها في الفضاء الشبكي أو الآلي. حيث يتمّ تبادل البيانات في شكل حزم الكترونية توجه إلى عنوان افتراضي ليس له صلة بالمكان الجغرافي ، فهو فضاء ذو طبيعة لا مركزية، و يمكن إجمال أهم خصائصه في عدم التبعية لأي سلطة حاكمة .فالفضاء الآلي هو نظام الكتروني معقد لأنه عبارة عن شبكة اتصال لا متناهية غير مجسدة و غير مرئية، متاحة لأي شخص حول العالم و غير تابعة لأي سلطة حاكمة، فالسلوك المرتكب فيها يتجاوز الأماكن بمعناه التقليدي، الذي له وجود حقيقي وواقعي.[1]

أولاً : الجرائم الإلكترونية جرائم عابرة للحدود

تتجاوز الجريمة الإلكترونية حدود الدول وهذا ما يجعل منها جريمة ذات طبيعة دولية وتتصف بخصوصية معينة تجعل الدول تسارع لمكافحة هذا النوع من الجرائم ، فالاعتداءات التي تقع على مصالح الدول من الجرائم الإلكترونية تهم الجماعة الدولية ككل ، والتي قررت حمايتها بقواعد القانون الدولي . فهذه الاعتداءات تكسب الجريمة الإلكترونية الصفة الدولية ، حيث تعد المصلحة المعتدى عليها معيار مهم لإصباغ الصفة الدولية على الجريمة الإلكترونية.

---

[1] رحاب عميش – الجريمة المعلوماتية، مقالة منشورة على الموقع الالكتروني: www.docstoc.com/docs/145259921

ويرى بعض الباحثين بأن الجريمة الإلكترونية صورة من صور العولمة ، فمن حيث المكان يمكن ارتكاب هذه الجرائم عن بعد، وقد يتعدد هذا المكان بين أكثر من دولة . ومن حيث الزمان تختلف الأوقات بين الدول .فالجريمة الإلكترونية قد ترتكب عن طريق حاسب آلي في دولة ما، في حين يتحقق الفعل الإجرامي في دولة أخرى، فجرائم الكومبيوتر والإنترنت لاتحدها حدود ولا تعترف بعنصر المكان أو الحدود الجغرافية ، وكما أنها تتميّز بالتباعد الجغرافي بين الفاعل والمجني عليه ، ومن الوجهة التقنية ما بين الحاسوب أداة الجريمة ، وبين المعطيات أو البيانات محل الجريمة في نظام الحاسوب المستهدف بالاعتداء . وهذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكنه وبفعل تقنيات الشبكات النظم والمعلومات ، امتد خارج هذه الحدود – دون تغيير في الاحتياجات التقنية ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزن فيه المعطيات محل الاعتداء.

والحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقق النتيجة من أكثر المسائل التي تثير إشكالات في مجال الجرائم الإلكترونية وبشكل خاص الإجراءات الجنائية والاختصاص والقانون الواجب التطبيق، فأثارت الطبيعة الدولية للجرائم الإلكترونية تساؤلاً مهماً يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي أم تلك التي توجد بها البيانات محل الجريمة أم تلك الدولة التي أضر بها النشاط الإجرامي .

كما أن التوسع الكبير في إجراء المعاملات البنكية عبر شبكة الإنترنت منح البعد الدولي للجريمة الإلكترونية. فربط وسائل الاتصالات بالكومبيوتر

ضاعف من المعاملات المالية الدولية التي تتمّ بالوسائل الإلكترونيـــة، وبصـــفة خاصة من خلال التحويل الالكتروني للمعلومات والتبادل الالكتروني للبيانات .[1]

ولابد من الإشارة إلى أن هذه الطبيعة الدولية للجريمة الإلكترونية لفتـــت نظر المجتمع الدولي إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجرائم الإلكترونية، والعمل على التوفيق بين التشريعات الوطنية التي تتناول هذه الجرائم .

ثانياً : أهمية مكافحة الجريمة الإلكترونية على الصعيد الدولي

تعد شبكة الإنترنت أحدث أدوات العالم لربط كافة الدول ببعضها عـــن طريق شبكة عنكبوتية معقدة .والجريمة الإلكترونية هي صراع بين التقدم التقاني وحماية أمن الخصوصية. ومن الملاحظ أن التقدم الهائل فـــي قطـــاع تقنيـــات الاتصال الحديثة، قد صاحبه أيضاً زيادة في الجرائم الإلكترونية، فعمليات الغش المصرفي التي تتمّ عبر الإنترنت نتيجة سرقة المعلومات الشخصـــية للأفـــراد عندما يقومون بإرسالها عبر الإنترنت ، يهدد بتقليل حجم التعاملات من خـــلال التجارة الإلكترونية، وبخاصة مع اتجاه أغلب الدول الآن لاســـتخدام البطاقـــات الإلكترونية الذكية سواء في بطاقات الهوية أو المبادلات الاقتصادية، مما يتسبب في خسائر فادحة لاقتصاد هذه الدول. كما أن هناك مخاوف من التهديدات التي تتعرض لها الهواتف المحمولة، وبخاصة مع الخدمات الجديدة التي تقدمها مثـــل إتاحة القيام بالأعمال المصرفية، ومنها التعرف على الحســـاب البنكـــي ودفـــع الفواتير وتحويل الأموال وغيرها من الخدمات الجديدة الواعدة، وأيضاً جـــرائم كاميرا الهواتف المحمولة، كما أن هناك مخاوف من بطاقات الائتمان المـــزودة

[1] د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية، مرجع سابق ، ص٥٢ .

بتقنية التعريف اللاسلكية Radio Frequency dentification (RFID) ، والتي تستخدم حالياً وتؤدي لسرعة وسهولة العديد من الأعمال والخدمات، حيث تتيح للأفراد تمّريرها عبر أجهزة القراءة من دون إدخالها، إذ هناك مخاوف من أن هذه البطاقات ستقوم ببث اسم ورقم بطاقة ائتمان الفرد وتاريخ انتهائها إلى أي شخص آخر يقترب منه حاملاً جهاز مسح إلكتروني.

هذا بالإضافة إلى التهديدات السلبية، الثقافية والاجتمّاعية والنفسية ، والتي تؤثر على سلوكيات وقيم وأفكار الأفراد، وبخاصة عند دخول الأبناء في غياب الآباء إلى مواقع محظورة عليهم على شبكة الإنترنت .

ونجد بأن أهمية ملاحقة الجريمة الإلكترونية تتعلق بخطورة النتائج التي تترتب على ارتكابها ولاسيما النتائج الاقتصادية .حيث توصلت دراسة أعدتها الشركة العالمية لأمن المعلومات (kaspersky) من خلال نتائج أراء خبراء في أمن تقنية المعلومات من جميع أنحاء العالم حول القضايا الكبرى المتعلقة بمجال عملهم ، أن التهديدات الإلكترونية أصبحت أكثر تنوعاً وتقع بشكل متكرر ، كما تشكل خطراً أكبر من ذي قبل على المؤسسات في العالم أجمع. ويرى نحو نصف الخبراء المشاركين في الدراسة أن الجريمة الإلكترونية بأشكالها المختلفة هي ثاني أكبر خطر يهدد المشاريع ، إذ إنَّ شركاتهم عادة ما تواجه البرمجيات الخبيثة ، والرسائل المزعجة والمحاولات الغير مشروعة للدخول إلى أنظمة الشركة.كما أعدت دراسة شركة (HP) والتي أظهرت أن معدل التكلفة السنوية للجرائم الإلكترونية ، والتي تكبدتها مجموعة منتقاة من أكبر الشركات الأمريكية، بلغ حوالي ثمانية ملايين دولار [1].

[1] مقالة منشورة على موقع الاقتصادية الالكتروني www.aleqtisadiah.com

وإن أهمية مكافحة الجريمة الإلكترونية تظهر بنتائجها الكارثية على قطاع البنوك ، وذلك عندما بدأت البنوك والمؤسسات المالية في استخدام التكنولوجيا في المعاملات المالية . ومع ظهور الإنترنت أصبح من الممكن إجراء العديد من المعاملات البنكية من خلال هذه الشبكة، والتي يطلق عليها مصطلح البنوك الإلكترونية .

فالكثير من الأفعال الغير مشروعة قد ارتبطت بالبنوك الإلكترونية أو بالمعاملات المالية التي تتمّ من خلال شبكة الإنترنت بصفة عامة . فعلى الرغم من الإجراءات الأمنية المتبعة في محيط البنوك الإلكترونية ، والتي تتمثّل بصفة رئيسة فيما يعرف بالتوقيع الإلكتروني ، بالإضافة إلى أنظمة الرقابة الداخلية وغيرها من الإجراءات الأمنية ، إلا أن بعض الجرائم قد وجدت في البنوك الإلكترونية مسرحاً لها .ولاسيما جريمة غسيل الأموال ، حيث يتمّ نقل الأموال أحياناً دون وساطة أية مؤسسة مالية تحتفظ بالوثائق المتعلقة بهذه المعاملات . وبالإضافة إلى ما سبق ، فإن الطبيعة المجهولة للأموال الإلكترونية ، فضلاً عن صعوبة الكشف عنها وسهولة نقلها إلى أي مكان في العالم ، كل ذلك دفع مجرمي غسيل الأموال إلى استخدام شبكة الإنترنت بوصفها الوسيلة المثلى لارتكاب أفعالهم الغير مشروعة .[1]

فأهمية ملاحقة هذه الجرائم تنبع من ضرورة التقليل من الخسائر التي تتعرض لها الدول على الصعيد الاقتصادي ولم تقتصر هذه الخسائر على الجانب البنكي، إنما أيضاً جريمة التهرب الضريبي الالكتروني التي أسهمت المعاملات المالية التي تتمّ من خلال شبكات المعلومات بظهورها ، والتي تحقق خسائر كبير لخزينة الدولة نتيجة التهرب من دفع الضرائب.

---

[1] د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية مرجع سابق ، ص٤٢-٤٣ .

ثالثاً : أهم الصعوبات التي تواجه قمع الجرائم الإلكترونية

تتمثّل صعوبة ملاحقة الجرائم الإلكترونية بالخصائص التي تتميّز بها هذه الجريمة عن غيرها من الجرائم التقليدية ، فهي جريمة عابرة للحدود وترتبط بآخر ما توصلت إليه التقنيات الحديثة في مجال الحواسب والمعلوماتية ، وترتكب من قبل أشخاص أذكياء أو كما يطلق عليها (جريمة الأذكياء) ، بالإضافة إلى صعوبات تنطلق من مفاهيم دولية أو أسس لا تتنازل عنها الدول، وأهمها مبدأ السيادة القومية . وإنَّ عدم وجود مفهوم محدد للجريمة الإلكترونية متفق عليه بين الدول ، بالإضافة إلى تحديات أخرى تعاني منه الدول نجم عنه صعوبات عدة في مجال مكافحة هذا النوع من الجرائم المستحدثة والعابرة للحدود ، وأهم هذه الصعوبات مايلي:

١- الطبيعة غير المادية (الافتراضية) للجرائم الإلكترونية

إن الجريمة الكترونية تتمّ ببيئة لا علاقة لها بالورق أو المحررات ، فيصعب استخلاص الدليل المادي لهذه الجريمة، لأنه في عالم غير واقعي . وإن هذه الخصوصية للجريمة الإلكترونية تولد عدداً كبيراً من الصعوبات والتحديات في مجال مكافحاتها ، كصعوبة كشفها لأنه لا يشوب ارتكابها أي عمل من أعمال العنف ، كما أنها لا تترك آثاراً، إنما يتمّثل مظهرها في تغيير أو محو الأرقام والبيانات الموجودة بأنظمة الحاسبات الآلية .[١] فصعوبة اكتشافها وإثباتها

---

[١] د. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مصر، مكتبة الآلات الحديثة، ١٩٩٢ ، ص٤١.

تعود إلى عدة أسباب من بينها وسيلة تنفيذها التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد .[1]

ومن أهم الأسباب التقنية التي تكسب الجرائم الإلكترونية صعوبة الاكتشاف ،هي عمليات التخفي (Proxys) أثناء التجوال على الشبكة والتي تؤمنها بعض المواقع على الشبكة. حيث تسمح هذه العملية لمستخدمها بالانطلاق إلى أي موقع على شبكة الإنترنت دون أن يكتشف ذلك الموقع شخصية الزائر. وعلى الرغم من أهمية (proxys) والهدف الذي صممت من أجله لتأمين الشبكات والمواقع ضد عمليات الاختراق، إلا أنها استغلت استغلالاً سيئاً من قبل قراصنة الإنترنت ، فمرتكب الجريمة الذي يستخدم هذه المواقع يصعب الوصول إليه . كما أن الأمر لم يقف عند هذا الحد، بل قام مصممو الفيروسات المدمرة من خلال استخدامهم لتلك المواقع، في إطلاق فيروساتهم إلى العالم الأمر الذي بات يشكل ظاهرة خطيرة في المجتمّعات الدولية لصعوبة التوصل لشخصية مرتكب الفعل.[2]

كما تؤدي الطبيعة الافتراضية إلى صعوبات تتعلق بإجراءات تعقب الجريمة الإلكترونية وضبطها ، فالتفتيش في هذا النمط من الجرائم يتمّ عادة على نظم الكومبيوتر وقواعد البيانات وشبكات المعلومات ، ويتجاوز النظام المشتبه به إلى أنظمة أخرى مرتبطة ، وهذا الوضع الغالب في ظل شيوع الشبكات بين الحواسيب، وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول ، وامتداد التفتيش إلى نظم غير النظام محل الاشتباه ، خلق تحديات كبيرة أولها مدى قانونية هذا

---

[1] د. نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، مرجع سابق ، ص٤٩ .

[2] د. علاء الدين شحاته – التعاون الدولي في مجال مكافحة الجريمة، القاهرة ، ٢٠٠٠م ص ٢٥.

الإجراء، ومدى مساسه بحقوق الخصوصية المعلوماتية لأصحاب الـنظم التـي يمتد إليها التفتيش .

كما إن ضبط الجرائم الإلكترونيـة لا يتوقـف علـى تحريـز جهـاز الكومبيوتر، بل قد يشمل ضبط المكونات المادية إلى مختلف أجزاء النظام التي تزداد يوماً بعد يوم، والأهم أن الضبط ينصب على المعطيات والبيانات والبرامج المخزنة في النظام ، أو النظم المرتبطة بالنظام محل الاشتباه، أي على أشـياء ذات الطبيعية المعنوية المعرضة بسهولة للتغيير والإتلاف، وهذه الحقائق تثيـر مشكلات متعددة، منها المعايير المقبولة للضبط المعلوماتي، ومعايير التحريـز إضافة إلى مدى مساس إجراءات ضبط محتويات نظام ما بخصوصية صـاحبه وإن كان المشتبه به. وعندما تتعدى أنشطة الضبط إلى كل محتويات النظام التي تضم عادة معلومات وبيانات يحرص على سرِّيتها، أو أن تكون محـل حمايـة بحكم القانون، أو لطبيعتها، أو تعلقها بجهات أخرى.

وأدلة الإدانة في هذا النوع من الجرائم ذات نوعية مختلفة، فهي ذات طبيعة معنوية كسجلات الكومبيوتر ومعلومات الـدخول والاشـتراك والنفـاذ والبرمجيات. وقد أثارت مثل هذه الأدلة مشكلات جمة من حيث مدى قبولها لدى القضاء وحجيتها والمعايير المتطلبة لتكون كذلك خاصة في ظل قواعد الإثبـات التقليدية .

وما يزيد صعوبة اكتشاف الجريمة الإلكترونية الإحجام عن الإبلاغ عنها في حال اكتشافها لخشية المجني عليهم، ولأسباب تتعلق بسمعة المؤسسة التـي تتأثر إذا ما وصل إلى علم المتعاملين معها تعرض أنظمة المعلومات الخاصـة

بها إلى التلاعب . فضلاً عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة .[١]

وإن الأثر الرادع الذي يحققه التشريع في الجرائم التقليدية ليس له هذا الأثر في الجرائم الإلكترونية ، فلا يوجد شعور عام بعدم أخلاقية الفعل أو بمساسه بمصالح أو قيم يحرص المجتمّع على حمايتها ، بل إنَّ الكثير من العاملين في المجال المعلوماتي لا يجدون أي خطأ في استعمال الشفرات السرية الخاصة بالدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة أو في نسخ البرامج بدلاً من شرائها واستعمال الحاسبات الآلية للمؤسسات التابعين لها لأغراض شخصية .[٢]

٢ ــ تنازع الاختصاص القضائي في الجرائم الإلكترونية

يقصد بالاختصاص " السلطة التي يقررها المُشرِّع للقضاء لأن ينظر في دعاوى معينة حددها القانون"[٣] وإنَّ أهم المشكلات والصعوبات التي تعترض المجتمّع الدولي في ملاحقة الجرائم الإلكترونية تتمّثل في تحديد الاختصاص القضائي المرتبط بتحديد القانون الواجب التطبيق على هذه الجريمة ، فقواعد الاختصاص القضائي التقليدية صيغت كي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني للجريمة ، وهي قواعد ترتكز على مبدأ الإقليمية، ما يرتبط بسيادة الدولة على أقليمها ، فلا يكون الخروج عليه بقبول اختصاص قضائي أجنبي إلا في حالات استثنائية يجب النص عليها صراحة. وهنا تثور أمامنا

---

[١] د. هشام محمد فريد رستمّ ، مرجع سابق ، ص٤٢ .

[٢] د. نائلة عادل محمد فريد قورة ، مرجع سابق ، ص٥١ .

[٣] د. محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، الطبعة الثانية ، دار النهضة العربية ، القاهرة ، ١٩٨٨ ، ص٣٥٩ .

مدى إمكانية الاعتمّاد على هذه القواعد لتحديد الاختصاص القضـــائي لجريمـــة ترتكب في مجال تنعدم فيه الحدود الجغرافية ، وكثيراً مايكون مُركبوها في بلاد مختلفة و من جنسيات متعددة، وكثيراً أيضاً ما يتعلق السلوك الإجرامي بـــأكثر من دولة : الدولة التي ارتكب فيها السلوك والدولة التي تمّ فيها القـــبض علـــى الجاني ، و تلك التي حدثت فيها النتيجة الإجرامية .

فالجرائم الإلكترونية لا تعرف حدوداً جغرافية ، بالإضافة إلى أن الإنترنت ليست ملكاً لأحد ، ولا تخضع لسيطرة دولة معينة . لذلك تتعدد الدول المختصة بملاحقة هذه الجرائم لكون الإنترنت شبكة عالمية تتجاوز حدود الدول المعروفة والمحددة عالمياً .

وإن اختصاص القضاء بنظر الجرائم الإلكترونيـــة والقـــانون المتعـــين تطبيقه على الفعل لا يحظى دائماً بالوضوح أو القبول أمام حقيقة هي أن غالبية هذه الأفعال ترتكب من قبل أشخاص من خارج الحدود أو تمّرُّ عبـــر شـــبكات معلومات وأنظمة خارج الحدود حتى عندما يرتكبها شخص من داخـــل الدولـــة على نظام في الدولة نفسها ، وهو ما يبرز أهمية امتحان قواعـــد الاختصـــاص والقانون الواجب التطبيق وما إذا كانت النظريات والقواعد القائمة في هذا الحقل تطال هذه الجرائم أم يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها ومـــا تثيره من مشكلات في حقل الاختصاص القضائي . ويرتبط بمشكلة الاختصاص والقانون الواجب التطبيق مشكلات امتداد أنشطة الملاحقة والتحـــري والضـــبط والتفتيش خارج الحدود، وما يحتاجه ذلك إلى تعاون دولي شامل للموازنة بـــين موجبات المكافحة ووجوب حماية السيادة الوطنية .

٣- مبدأ السيادة الوطنية والاختصاص الداخلي للدول

غالباً ما تتعارض الجهود الدولية في سبيل مكافحة الجرائم الإلكترونية مع سيادة الدولة على أراضيها ، فالدولة تتمّتع بالسيادة، ولهذه السيادة مظهران: داخلي يتجلى في بسط سلطان الدولة على الإقليم ومن فيه، والقيام بمهمات التشريع والتنفيذ والقضاء بحيث يكون جميع أفراد الدولة خاضعين لقوانينها وأنظمتها . ومظهر خارجي يتجلى في تنظيم علاقات الدولة بالدول الأخرى على أساس من الاستقلال الذي لا تبعية فيه لأية قوة خارجية .[١]

ولكن سيادة الدولة ليست مطلقة، فهي مقيدة بعدد من الالتزامات أو المعاهدات الدولية التي تتمّ بإرادة الدولة ذاتها ، وأحياناً لأسباب يحتمّها التطور التكنولوجي .[٢]

وإن التطور التكنولوجي يقودنا إلى لفت النظر للعلاقة بين السيادة والعولمة . "فالعولمة هي مجموعة عمليات تغطي أنحاء العالم".[٣] ومن إحدى هذه العمليات قطاع الاتصالات والمعلومات ، فأهم العوامل التي تعطي القوة التأثيرية الهائلة للعولمة على السيادة الوطنية للدول هي شبكة الإنترنت ، والثورة في وسائل الاتصال فالعولمة تهدف إلى وضع الشيء على مستوى عالمي ، أي نقله من المحدود (بحدود الدولة القومية) إلى فضاء اللامحدود (تجاوز حدود الدولة القومية).

كما أن ملاحقة الجرائم الإلكترونية تتطلب نظاماً خاصاً بالتفتيش والملاحقة وجمع الأدلة. ولتحقيق هذا الهدف المتمّثل بالحصول على المعلومات

---

[١] د. محمد المجذوب ، القانون الدولي العام ، الطبعة السادسة ، منشورات الحلبي الحقوقية ، بيروت ، ٢٠٠٧ ، ص٩١ .

[٢] د. محمد المجذوب ، المرجع السابق ، ص٩٢ .

[٣] المرجع السابق ، ص٩٢-٩٤ .

والبيانات المتعلقة بالجرائم الإلكترونية، لابد من وجود نظام تعاون على الصعيد الدولي يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع أدلة معينة أو معلومات مهمة ، فعدم وجود مثل هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالباً ما تكون مفيدة في التصدي للجرائم الإلكترونية .

وترفض بعض الدول التعاون لكون ذلك يشكل انتهاكاً للسيادة الوطنية للدولة المطلوب منها البيانات والمعلومات . فهنالك العديد من القضايا المرتبطة بالاقتصاد التي كانت تحسم في إطار الاختصاص الداخلي لكل دولة أو حتى في الإطار الإقليمي ضمن سيادة الدولة الواحدة ، ولكن أهم تلك القضايا التي تتجاوز حدود الدول هي الجرائم الإلكترونية . فتوحيد الجهود بشأن هذه القضايا ومثيلاتها أصبح يفترض اتخاذ تدابير لن تكون فعالة إلا إذا اتخذت بشكل جماعي .

ونجد بأن تمّسك الدولة بالسيادة الوطنية بشكلها المطلق يمكن أن يمثل عائقاً في سبيل قيام العلاقات التعاونية بين الدول من أجل مكافحة هذه الظاهرة الخطرة على استقرار المجتمّع الدولي وأمنه .[1]

٤- اختلاف محل التجريم في التشريعات الوطنية

للحكومات مناهج مختلفة بشأن التشريعات الخاصة بالإنترنت. فمعظم دول العالم تنظّم الإنترنت ضمن حدود قيمها السياسية والقانونية والأخلاقية والثقافية. لكن تطوّر تكنولوجيا الاتصالات والمعلومات يجري على مستوى دولي خارج عن نطاق سيطرة الدول، فاعتماد تشريعات فعَّالة وتنفيذها لمكافحة

[1] د. علاء الدين شحاتة ، التعاون الدولي في مجال مكافحة الجريمة ، ايتراك للنشر والتوزيع ، القاهرة ، ٢٠٠٠ ، ص٤٠.

جرائم الإنترنت يشكّل تحديًا كبيرًا للحكومات. وبالتالي فإن جـرائم الإنترنـت تمثّل تحديثاً كبيراً للأجهزة القانونية سواء في البلدان المتقدمة أو النامية.

فاكتشاف محتوى المخالفات في التكنولوجيا الجديدة، وإيجاد الثغرات في التشريعات المقننة لمعالجتها، واعتماد قوانين جديدة تجرِّم التعـديات المتعلقـة بالكومبيوتر، يزيد من التأخير في عملية مكافحة الجرائم الإلكترونية، إضافة إلى الحاجة لمعدات وتقنيات قد لا تكون متوافرة للتحقيق في الأعمـال الإجراميـة المحتملة . فالتعامل بالأدلة الرقمية يترافق مع تحديات كبيرة، ويتطلّب إجراءات محدّدة للحفاظ على سلامة المعلومات، وتجنّب تعديل الأدلة أو حذفها، أو التعدي على حقوق مستخدمي الإنترنت.

وكما أسلفنا الذكر ، فالطبيعة الخاصة للجريمـة الإلكترونيـة تتطلـب إجراءات مختلفة تماماً عن الأساليب المتبعة في ملاحقة الجرائم التقليدية ، وإن هذه الإجراءات لا تكون فاعلة إلا إذا اقترنت بتعاون دولي من قبل الدول المعنية بملاحقة هذه الجرائم ، ويتطلب ذلك توافق تشـريعي ولاسـيما مـن الناحيـة الإجرائية ، إلا أن الواقع ينطوي على تنوع واختلاف فـي الـنظم الإجرائيـة القانونية المتبعة.

حيث نجد طرق التحري و التحقيق و المحاكمـة التـي تثبـت فائـدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قـد لا يسـمح بإجرائها . كما هو الحال بالنسبة للمراقبة الإلكترونية ، والعمليات المستترة على شبكة الإنترنت وغيرها من الإجراءات الشبيهة. فإذا اعتبرت طريقة مـا مـن طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة ، قد تكـون ذات الطريقة غير مشروعة في دولة أخرى ، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة السلطات من إنفاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعّالة ، بالإضافة إلى أن السلطات القضائية لدى الدولـة

الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة ، حتى وإن كان هذا الدليل قد تــمّ الحصــول عليــه بموجب الاختصاص القضائي أو بشكل مشروع.[1]

ويرى البعض أن طرق الاتصال بين الدول تتمّ عادة باستخدام القنــوات الدبلوماسية، وقد لوحظ في كثير من الأحيان أن الاتصالات الشرطية تحتاج إلى اتصالات خاصة تحقق لها السرعة المناسبة من أجل تحقيق الغاية المرجوة من الاتصال .[2]

ونجد أن عدم وجود نموذج موحد للمكافحة بين تشريعات الدول يقتضي توحيد النظم القانونية للدول. ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفــق مــع طبيعــة هــذا النــوع المستحدث من الجرائم، ويخفف من الفوارق الكبيرة بين الأنظمة العقابية الداخلية ، وتتمّثل هذه الوسيلة في تحــديث التشــريعات المحليــة المعنيــة بــالجرائم الإلكترونية، و إبرام اتفاقيات خاصة لمكافحة هذا النوع من الجرائم المعاصرة .

---

[1] د. حسين بن سعيد بن سيف الغافري ، محاضرة ألقيت أمام مجلس إدارة الاتحاد العربي للتحكــيم الإلكتروني ، ٢٠٠٧، ص٥٣ .

[2] د. علاء الدين شحاتة ، مرجع سابق ، ص١١١ .

المبحث الثاني

مكافحة الجرائم الإلكترونية في القوانين الوطنية

تعد الدول المتقدمة تكنولوجياً سباقة لمواجهة الجرائم الإلكترونية ، وذلك من خلال سن التشريعات الخاصة بمكافحة الجرائم الإلكترونية أو تعديل القوانين القائمة للتلائم مع هذا النوع من الإجرام، كما أن الدول العربية لم تغفل عن سن التشريعات في محاولة منها للحدِّ من هذا الاجرام المستحدث، وبناءً على ذلك سوف نلقي الضوء في المطلب الاول على الأحكام التشريعية لبعض الدول غير العربية ، وفي المطلب الثاني على النصوص التشريعية لبعض الدول العربية.

المطلب الأول: التشريعات الأجنبية لمكافحة الجرائم الإلكترونية

اتجهت كافة الدول الأوروبية والمتقدمة تقنياً إلى إيجاد القوانين الجديدة القادرة على مواكبة الجرائم الالكترونية والإحاطة بملاحقتها والحد من وقوعها وتلافي القصور الحاصل بالقوانين التعليمية القديمة وعليه فقد وجدت هذه الدول قوانين جديدة لمكافحة الجرائم الالكترونية، ومن هذه الدول:

أولاً- السويد: و من أوائل الدول التي اتجهت إلى سن التشريعات الخاصة بمكافحه الجرائم الإلكترونية والإنترنت ، وقد صدر أول قانون خاص بها سمي بقانون البيانات عام ١٩٧٣م ، ويتضمن هذا القانون مكافحة جريمة الاحتيال عبر الإنترنت، بالاضافه إلى عدد من الجرائم الإلكترونية قبل الدخول غير المشروع إلى البيانات المحمية، أو تزوير المعلومات الإلكترونية.[١]

---

[١] منير محمد الجنبهي، وممدوح محمد الجنبهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية ٢٠٠٥ ص١٨٦-١٨٧ .

ثانياً- الولايات المتحدة الأمريكية : يُعد قانون (فلوريدا) لجرائم الحاسوب الصادر في عام ١٩٧٨ م أول قانون في الولايات المتحدة الامريكية من أجل مكافحة الجرائم الإلكترونية ، حيث يعتبر هذا القانون أنَّ كل دخول غير مشروع إلى الحاسوب هو بمثابة جريمة ، حتى لو لم تتوفر النية الجرمية من هذا الدخول.[١]

أما القانون الوطني في الولايات المتحدة الصادر في ٢٦ /٢٠٠١/١٠ والمعدل للقانون الصادر عام ١٩٨٤ الخاص بالاحتيال وسوء استخدام الكومبيوتر.[٢] ، فقد عاقب كل من يقوم عمداً بالدخول إلى حاسوب مشمول بالحماية ، دون أن يكون مصَّرحاً له بذلك ، أو يكون متجاوزاً للتصريح الممنوح له، إذا كان الغرض والأثر المترتب على هذا الدخول هو الحصول على شيء ذي قيمة عن طريق الاحتيال ، ويدخل وقت الحاسوب الذي يقدر بخمسه آلاف دولار أمريكي خلال سنة واحدة في عداد الأشياء ذات القيمة[٣]. كما توجد القوانين الأمريكية الفيدرالية الإجرائية ، من أجل مكافحة الجرائم الإلكترونية والمعاقبة على الدخول غير المشروع للحصول على البيانات المحمية.[٤] وخولت وزارة العدل الأمريكية في العام ٢٠٠٠ م خمس جهات حكومية للتعامل مع الجرائم الإلكترونية منها مكتب التحقيقات الفيدرالية "FBI" .[٥]

---

[١] د. محمد طارق الخن ، جريمة الاحتيال عبر الإنترنت، رسالة دكتوراه، جامعة دمشق، كلية الحقوق، ٢٠١٠، ص١٦١

[٢] THE USA PATRIOTACT هو القانون الوطني الأمريكي الصادر في ٢٠٠١/١٠/٢٦، وقد تناول تعديل حوالي ١٥ قانوناً.

[٣] د. محمد طارق الخن، مرجع سابق ، ص١٦٢ .

[٤] USA computer crime sprocdural acts، القوانين الأمريكية الفيدرالية الإجرائية بشأن جرائم الكومبيوتر المنصوص عليها في الباب ١٨ للقانون الفيدرالي.

[٥] الجنبهي، مرجع السابق، ص ١٨٨.

وثمة جهود تشريعية واسعة في حقل حماية المعلومات والخصوصية معروضة على المؤسسات التشريعية في معظم الولايات المتحدة الأمريكية، ففي ولاية (Arezona) هناك مشروع قانون لحظر توفير البيانات الشخصية الخاصة بأي موظف حكومي على شبكة الإنترنت أو أي موقع معلوماتي أو حيازة أي معلومات شخصية تهدد بالخطر سلامة أي موظف حكومي أو سلامة عائلته أو حصول تهديد يظهر أنه نتيجة المعلومات الشخصية .[١]

ثالثاً– بريطانيا: اشتمل قانون مكافحة التزوير والتزييف لعام ١٩٨١ م على تعريف للمصطلحات وأدوات التزوير ووسائل التخزين الإلكترونية المتنوعة .[٢] كما قام المُشرِّع البريطاني في عام ١٩٩٠ بإصدار قانون إساءة استخدام الكومبيوتر يتضمن في قسمه الأول تجريم الدخول غير مشروع إلى النظام المعلوماتي (القرصنة) ، أما القسم الثاني فقد تضمن تجريم الدخول غير المشروع مع عنصر إضافي وهو النية لارتكاب أو تسهيل ارتكاب الجرائم، أما القسم الثالث فيقمع تجريم أي تعديل لمحتوى الحاسوب.[٣]

رابعاً– فرنسا: اهتمّت الدولة الفرنسية بتطوير القوانين الخاصة بها للتناسب مع الجرائم الإلكترونية المستحدثة، حيث قامت بتعديل قوانينها الجنائية للتلاؤم مع التطورات الإجرامية. وقد أصدرت أول قانون خاص بها في ١٩٨٨ م رقم / ١٩ /، والذي أضاف إلى قانون العقوبات الجنائي الفرنسي جرائم الحاسب الآلي والعقوبات المقررة لتلك الجرائم. [٤] كما تمّ في عام ١٩٩٤ م تعديل قانون

---

[١] مقالة منشورة على الموقع www.ituarabic.org/coe/2006/Ecrime بعنوان الاتجاهات التشريعي للجرائم الإلكترونية للمحامي الدكتور يونس عرب – عمان ، الأردن.

[٢] الجنبهي، مرجع سابق ، ص ١٨٨ .

[٣] د. غسان رباح: الوجيز في قضايا حماية الملكية الفكرية والفنية مع دراسة مقارنة حول جرائم المعلوماتية، الطبعة الأولى ، منشورات الحلبي الحقوقية، بيروت عام ٢٠٠٨ ، ص١٥١.

[٤] د. محمد طارق الخن، مرجع سابق ، ص ١٦٥ .

العقوبات الفرنسي ليشمل مجموعة جديدة من القواعد القانونية الخاصة بالجرائم الإلكترونية، حيث أوكل هذا القانون في مواده للنيابة العامة سلطة التحقيق فيها بما في ذلك طلب عمل التحريات وسماع الأقوال والشهود.[١]

وجَّرم القانون الدخول بشكل احتيالي أو البقاء بشكل غير مشروع في نظام المعالجة الآلية للبيانات أو في جزء منه. وتشدد العقوبة لهذه الجريمة إذا كان الدخول غير المشروع أدى إلى محو أو تعديل البيانات. وجُرِمت هذه المواد التعطيل أو التدخل في عمل نظام المعالجة الآلية للبيانات، بالإضافة لتجريم إتلاف أو تعديل البيانات في نظام المعالجة الآلية، كما عاقب القانون على الشروع في ارتكاب هذه الجرائم.[٢]

خامساً – ألمانيا: صدر في عام ١٩٨٦ القانون الثاني لمكافحة الجريمة الاقتصادية، حيث جرم وعاقب على إتلاف أو محو أو تغيير أو تزوير البيانات المعالجة آلياً، وشدد العقوبة بالنسبة للبيانات ذات الأهمية الأساسية لقطاع الأعمال أو السلطة الإدارية لتصل إلى حدِّ السجن لمدة خمس سنوات والغرامة، وكذلك جَرَّم هذا القانون غش الحاسوب أو الاحتيال بواسطة الحاسوب وعاقب عليه بذات العقوبة المذكورة، وعاقب على الحصول دون تصريح من قبل الفاعل لنفسه أو لغيره على بيانات غير معدة أو مخصصة له ومحمية بوجه خاص ضد الوصول غير المصرح به.[٣] كما أصبح للقاضي الحق بموجب هذا القانون إصدار أوامره بمراقبه اتصالات الحاسب الآلي وتسجيلها والتعامل معها، إلا أن

---

[١] الجنبهي، مرجع سابق، ص ١٨٩ .

[٢] قانون العقوبات الفرنسي لعام ١٩٩٢ باللغة الانكليزية على موقع القوانين الفرنسية على الإنترنت www.legifrance.gouv.fr .

[٣] مقالة منشورة على الموقع www.ituarabic.org/coe/2006/Ecrime بعنوان الاتجاهات التشريعي للجرائم الإلكترونية للمحامي الدكتور يونس عرب – عمان ، الأردن.

القانون قد أعطى ذلك الحق للمحقق بشرط مدة أقصاها ثلاثة أيام.[1]

ونجد بأن التجربة الأوربية الأكثر نضجاً في مجال مكافحة الجرائم الإلكترونية ، فعلى المستوى الوطني تعد التشريعات الأوربية، ولا سيما التشريع السويدي والبريطاني والأمريكي من أوائل الدول التي تعاملت مع الظاهرة تعاملاً واقعياً من خلال سن التشريعات الخاصة بمكافحة هذه الجرائم المستحدثة والمبنية على دراسات معمقة للواقع وللطبيعة الخاصة لنوع هذه الجرائم، بالإضافة إلى وضع المشكلات والحلول والتدابير الأفضل للحدّ منها.

فإدراك الدول الأوربية لظاهرة الجرائم الإلكترونية وأهمية التعاون بمكافحتها، جعل الاتجاهات التشريعية الأوربية متمّاثلة تقريباً أو متقاربة بشأن التعامل مع ظاهرة الجرائم الإلكترونية.

المطلب الثاني : التشريعات العربية لمكافحة الجرائم الإلكترونية

تعدُّ محاولات المُشرِّع العربي خجولة نوعاً ما أو حديثة نسبياً، ويمكن التمييز من خلال هذه الدراسة بين نوعين أو اتجاهين اتبعا في الدول العربية .

الاتجاه الأول : الدول العربية التي سنت قانوناً خاصاً بمكافحة الجرائم الإلكترونية ومنها:

أولاً- سلطنة عُمان : أصدرَ المُشرِّع العماني المرسوم السلطاني رقم ٢٠٠١\٧٢ ، والمتضمن تعديل بعض أحكام القانون الجنائي العماني ليشمل الجرائم الإلكترونية، وتُعد سلطة عُمان الدولة العربية الأولى التي تصدت للجرائم المعلوماتية .[2]

---

[1] الجنبهي – المرجع السابق ، ص ١٩٠ .

[2] د. محمد طارق الخن – مرجع سابق، ص ١٧٠.

حيث عاقبت المادة (٢٧٦) من المرسوم المذكور كل من تعمد استخدام الحاسب الآلي في ارتكاب أحد الأفعال الآتية:

- الالتقاط غير المشروع للمعلومات أو البيانات.
- الدخول غير المشروع على أنظمة الحاسب الآلي .
- التجسس والتنصت على البيانات والمعلومات .
- انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم .
- تزوير بيانات أو وثائق برمجية أياً كان شكلها .
- إتلاف وتغيير ومحو البيانات والمعلومات .
- جمع المعلومات والبيانات وإعادة استخدامها .
- تسريب المعلومات والبيانات .
- التعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع.
- نشر واستخدام لبرامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية .

بالإضافة إلى المعاقبة على القيام بتزوير أو تقليد بطاقة من بطاقات الوفاء أو السحب واستعمالها [١] .

ولكن المُشرِّع العماني لم يكتفِ بهذا المرسوم السلطاني، إنما أضاف فصل في الباب السابع من قانون الجزاء العماني تحت عنوان (جرائم الحاسب الالي). وكذلك أضيفت مواد إلى قانون تنظيم الاتصالات العماني الصادر بالمرسوم السلطاني رقم (٣٠) لسنة ٢٠٠٢ تُحرم تبادل رسائل التحرش والحياء العام، وتحرم استخدام أجهزة الاتصالات للإهانة، أو الحصول على معلومات سرية، أو إفشاء الأسرار، أو إرسال رسائل تهديد ، وأسست السلطنة قانوناً ينظم

[١] قانون الجزاء العماني المنشور على الموقع www.rop.gov.com / Arabic/ poprules/

المعاملات الحكومية الإلكترونية والتوقيع الالكتروني وحوادث اختراق الأنظمة.[1]

ثانياً- المملكة العربية السعودية : أصدرت المملكة في ٣١ آذار عام ٢٠٠٧ نظام لمكافحة الجرائم الإلكترونية بما في ذلك الجرائم التي ترتكب عن طريق الهاتف المحمول، وتمّت المصادقة عليها بموجب المرسوم الملكي رقم م/١٧ ، ويتألف هذا النظام من ١٩ مادة ، للحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها ، وبما يؤدي إلى المساعدة على تحقيق الأمن المعلوماتي، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، وحماية المصلحة العامة والأخلاق والآداب العامة وحماية الاقتصاد الوطني . وعاقب المُشرِّع السعودي على عدد من الجرائم الإلكترونية كالتنصت على ما هو مرسل عن طريق شبكة الإنترنت أو أحد أجهزة الحاسب الآلي بطريقة غير شرعية، أو الدخول غير المشروع لتهديد شخص أو ابتزازه ، لحمله على القيام بفعل أو الامتناع عنه مشروعاً ، والدخول غير المشروع إلى الموقع الالكتروني ، أو الدخول إلى موقع الكتروني لتغير تصاميم هذا الموقع، أو إتلافه أو تعديله، أو شغل عنوانه، بالإضافة إلى المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا ،أو ما في حكمها والتشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة. كما عاقب المُشرِّع على الشروع بهذه الجرائم المنصوص عليها في النظام.[2] وهدف المُشرِّع السعودي من إصدار هذا النظام إلى إضفاء الثقة في صحة المعاملات والتوقيعات والسجلات الإلكترونية وسلامتها وتيسير استخدام التعاملات والتوقيعات الإلكترونية على الصعيدين

---

[1] قانون تنظيم الاتصالات العماني المنشور على الموقع wwww.mola.gov.om

[2] القانون السعودي لمكافحة الجرائم المعلوماتية منشور على الموقع www.aecert.ae/ uaelaw-ar.html

المحلي والدولي للاستفادة منها في جميع المجالات ، كـالإجراءات الحكوميـة والتجارة والطب والتعليم والدفع المالي الالكتروني، وإزالة العوائق أمام استخدام التعاملات والتوقيعات الإلكترونية، ومنع إسـاءة الاسـتخدام والاحتيـال فـي التعاملات والتوقيعات الإلكترونية.[١]

ثالثاً- الإمارات العربية المتحدة : أصـدرت دولـة الإمـارات بتـاريخ ٢٠٠٦/١/٣١ القانون الاتحادي رقم /٢/ الخاص بمكافحة الجرائم الإلكترونية، ويعد من القوانين الرائدة في العالم العربي الذي تضمن تفاصيل كثيرة ، فهو من جانب قد وضح معاني المصطلحات المستعملة وذات الدلالة القانونيـة، وهـي المعلومات الإلكترونية والبرنامج المعلوماتي ، ونظام المعلومات الالكترونـي، والشبكة المعلوماتية، والمستند الالكتروني، والموقع وغيرها من المصطلحات في المادة الأولى [٢] .

وقد عاقب المُشرِّع الإماراتي على كل فعل مقصود يتوصل فيه بغيـر وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو يتجاوز مدخلاً مصرحاً به ، وعاقب على تزوير مستند من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفاً به قانونـاً في نظام معلوماتي، وكذلك نص على تجريم تعطيل الوصول إلى الوسـائل أو البرامج أو المعلومات أو الشبكات المتعلقة بتقنيات المعلومات وكـذلك العبـث بالشبكة المعلوماتية، وبالفحوص الطبية باستخدام الإنترنت أو الإساءة إلى أحـد المقدسات أو الشعائر الإسلامية، بالإضافة إلى عدد من الجرائم الأخرى، ولكـن

---

[١] بحث منشور على الموقـع –http: //facults.ksa.edu.syl shaima atalla/ pages/ crifor asp

[٣] القانون الاتحادي لدولـة الإمـارات العربيـة المتحـدة – منشـور علـى الموقـع الالكترونـي www.emiatesid.gov.ae/assets/945lnas7g6n.

يؤخذ على القانون الاتحادي بأنه غيَّب الجانب الإجرائي اللازم لمكافحة هذا النوع من الجرائم، والذي يتطلب إجراءات خاصة مختلفة عن ملاحقة الجرائم التقليدية.

الاتجاه الثاني : الدول التي تسعى إلى سن تشريع خاص بالمعاملات والتجارة الإلكترونية، ومنها:

أولاً- تونس: وتعد من الدول المتأخرة بإصدار تشريع خاص بالجرائم الإلكترونية، فقد اكتفت بإصدار مجموعة من القوانين الخاصة بالتجارة الإلكترونية مثل قانون رقم /٨٣/ لسنة ٢٠٠٠ المتعلق بالمبادلات والتجارة الإلكترونية، وقانون رقم/٥٧/ لسنة ٢٠٠٠ المتعلق بالمصادقة الإلكترونية والمعترف بالوثيقة الإلكترونية ومجموعة القرارات المكملة لها. [١] وقد نص القانون رقم /٨٣/ الصادر سنة ٢٠٠٠ المتعلق بالتجارة الإلكترونية والمبادلات في الباب السابع الفصل /٤٣/ على المخالفات والعقوبات المترتبة على مخالفة أحكام هذا القانون، حيث تتمّ معاينة المخالفات لأحكامه من قبل أعوان الضابطة العدلية، والأعوان المحلفين للوزارة المكلفة بالاتصالات، والوكالة الوطنية للمصادقة الإلكترونية، وأعوان المراقبة الاقتصادية . ويتمّ سحب الترخيص من مزودي خدمات المصادقة الإلكترونية ويتمّ إيقاف نشاطهم، إذا أخلوا بواجباتهم المنصوص عليها بهذا القانون أو بنصوصه التطبيقية [٢] .

ثانياً- مصر: إن استجابة المُشرِّع المصري لمكافحة الجرائم الإلكترونية متأخرة فلم يعمل المُشرِّع على سن قوانين جديدة خاصة بها ولم يقم حتى بتعديل ما لديه

---

[١] تقرير بعنوان الإنترنت والحكومات العربية الصادرة عن الشبكة العربية لحقوق الإنسان يوم /١٣/ ديسمبر ٢٠٠٦ المنشور على الموقع www.liqaa.net/fip.php.article190

[٢] قانون رقم /٨٣/ لسنة /٢٠٠٠/ التونسي المتعلق بالمبادرات والتجارة الإلكترونية المنشورة على موقع نقابة المحامين في سورية www.syrianbar.org

من قوانين ، وقد تمّ الاكتفاء بتطبيق قواعد القانون الجنائي التقليدي على الجرائم الإلكترونية. على سبيل المثال لا الحصر، يُعد المُشرِّع المصري قانون براءات الاختراع منطبقاً على الجانب المادي من نظام المعالجة الآلية للبيانات الإلكترونية، وكما يعدُّ نصوص قانون حماية الحياة الخاصة، وقانون تجريم إفشاء الأسرار قابلة للتطبيق على مكافحة بعض الجرائم الإلكترونية [١]، وحالياً يتمّ إعداد مشروع قانون من مكافحة جرائم الإنترنت، ويتكون المشروع من /١٣/ مادة تفرض عقوبات رادعة على المشاركين أو الفاعلين لهذا النوع من الجرائم، حيث سيعاقب (hackers) بالحبس لمدة عام وغرامة لا تتجاوز ١٥٠٠٠ جنيه، وسيعاقب كل من تعمد الاستيلاء على بيانات بنكية أو ائتمّانية أو ملكية الأوراق المالية، أو استغلالها للحصول على الأموال وللابتزاز [٢].

وفي جميع الأحوال لا تكون العقوبات المنصوص عليها في هذا النص القانوني تتناسب وحجم الخسائر والنتائج المترتبة على ارتكاب الجريمة الإلكترونية، وبالتالي فإن إدراج هذه الأفعال (الجرائم الإلكترونية) تحت قانون غير مناسب لها سيجعل العقوبة غير مناسبة أو محققة النتيجة التشريعية في سبيل مكافحة هذه الجرائم المستحدثة، فهي ذات طبيعة خاصة كما أشرنا سابقاً [٣] كما أصدر المُشرِّع المصري قانون التوقيع الالكتروني في مصر رقم /١٥/ لعام ٢٠٠٤[٤].

ثالثاً- الأردن: أصدر المُشرِّع الأردني قانوناً خاصاً بالمعاملات الإلكترونية رقم /٨٥/ لسنة ٢٠٠١، ويهدف هذا القانون إلى تسهيل استعمال الوسائل الإلكترونية في إجراء المعاملات مع مراعاة أحكام أي قوانين أخرى دون تعديل

---

[١] الجنبهي ، مرجع سابق ، ص ١٩٢ .

[٢] مقالة منشورة على الموقع www.soum7.com / news.asp?news sid=663483 .

[٣] المحاميان الجنبهي مرجع سابق ، ص ١٩٢ .

[٤] قانون التوقيع الالكتروني المصري موجود على الموقع الالكتروني: mrwsa.arabblogs.com

أو إلغاء لأي من هذه الأحكام، مع الأخذ بعين الاعتبار لدى تطبيق هذه الأحكام قواعد العرف التجاري الدولي ذات العلاقة بالمعاملات الإلكترونية ودرجة التقدم في تقنية تبادلها[1]. كما شمل هذا القانون التوقيع الالكتروني، حيث أكدت المادة (١٠) من قانون المعاملات الإلكترونية الأردني على أن التوقيع الالكتروني يفي بمتطلبات التشريع الذي يستوجب توقيعاً على المستند، كما رتب أثراً على خلوه من التوقيع، وهذا تكريس لمبدأ أن التوقيع الالكتروني حقق المقصود من التوقيع الخطي، لكن إيفاء التوقيع الالكتروني بوظيفة التوقيع العادي رهن بالثقة بصحة هذا التوقيع [2]. كما أصدر المُشرِّع الأردني في العام ٢٠١٠ " قانون جرائم أنظمة المعلومات" ، حيث عاقب كل من دخل قصداً إلى موقع الكتروني أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، وكل من دخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام المعلومات، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نسخ أو التقاط أو تمكين الآخرين من الإطلاع على البيانات أو المعلومات وكل من استخدم نظام المعلومات، أو الشبكة المعلوماتية أو أنشأ موقعاً الكترونياً لتسهيل القيام بأعمال إرهابية أو دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لإتباع أفكارها بالإضافة إلى عدد من الجرائم الإلكترونية [3].

---

[1] قانون المعاملات الإلكترونية الأردنية رقم ٨٥ لعام ٢٠٠١ .

[2] بحث بعنوان (حجية التوقيع الالكتروني في الأردن مقدم من السيدة أحلام الجمبرجي ، عام ٢٠٠٨، منشور على الموقع الالكتروني www.free-zones.gov.jo .

[3] قانون الاردني للجرائم جرائم أنظمة المعلومات لعام ٢٠١٠ .

المطلب الثالث: التشريعات السورية لمكافحة الجرائم الإلكترونية

أصدر المُشرِّع السوري القانون رقم /١٧/ لعام ٢٠١٢ المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية. ولقد صدر هذا القانون بعد دراسة طويلة من قبل لجنة من المختصين والتقنيين والقانونين لإعداد مشروع قانون مكافحة الجريمة الإلكترونية، وقد ارتكزت هذه اللجنة في دراستها على القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات، وعلى التجارب التي تمّت الإشارة إليها على الصعيدين العربي والأجنبي، بالإضافة إلى الاتفاقية الأوربية لمكافحة الجريمة الافتراضية لعام ٢٠٠١ [١]. ويتألف هذا القانون من خمسة فصول و ٣٦ مادة حدد فيها المُشرِّع الأفعال التي تشكل جرائم الكترونية، والعقوبات المحددة لها، حيث تضمنت المادة الأولى تفسير بعض المصطلحات اللازمة للعمل بأحكام القانون كالمعلومات والجهاز الحاسوبي وبرمجيات حاسوبية والشبكة والموقع الالكتروني والتواصل على الشبكة بالإضافة إلى عدد من المصطلحات الأخرى . كما حدد القانون السبل والإجراءات المتوجبة على المتضرر إتباعها في حال تعرضه لعمل غير مشروع على الشبكة. وعاقب أيضاً على إفشاء البيانات والمعلومات في المادة /٩/ من قبل مقدم الخدمات على الشبكة بإفشاء المحتوى أو البيانات أو المعلومات المخزنة لديه مخالفاً بذلك التزامات المحافظة على المهنة. وقد راعى هذا القانون تطبيق أحكام قانون التجارة بالإضافة إلى مراعاة حقوق المؤلف والملكية ، حيث أشار في المادة /١٤/ بأن يطبق على أي محتوى يوضع على الشبكة القوانين النافذة المتعلقة بحماية حقوق المؤلف والحقوق المجاورة وحماية

---

[١] كتاب وزير الاتصال والتقانة رقم (٢٨/٣٠٠٠) تاريخ ٢٠٠٨/٩/٩ الموجه إلى وزارة العدل، وقرار السيد وزير العدل رقم /١٣١١٣/ تاريخ ٢٠٠٨/٩/١٥ حول تشكيل لجنة لإعداد مشروع قانون مكافحة الجريمة الإلكترونية.

حقوق الملكية الفكرية والتجارية والصناعية وبراءات الاختراع. أما الفصل الثالث فقد خصص لمكافحة الجريمة المعلوماتية فعاقب على الدخول غير المشروع إلى المنظومة المعلوماتية وعاقب على شغل اسم موقع الكتروني أو إعاقة الوصول إلى الخدمة واعتراض المعلومات، بالإضافة إلى تصميم البرمجيات الخبيثة واستخدامها والاحتيال عن طريق الشبكة وانتهاك حرمة الحياة الخاصة والاستخدام الغير مشروع لبطاقة الدفع. وقد أشار القانون إلى إحداث ضابطة عدلية مختصة تحدث في وزارة الداخلية تكلف باستقصاء الجرائم المعلوماتية وجمع أدلتها الرقمية والقبض على فاعلها وإحالتهم إلى المحاكم الموكل إليها أمر معاقبتهم، وأثار القانون نقطة هامة تتعلق بمدى حجية الدليل الرقمي، حيث يعود للمحكمة تقدير قيمة الدليل الرقمي ولكن بوجود شرطين:

١- أن تكون الأجهزة الإلكترونية أو المنظومات المعلوماتية المستمد منها هذا الدليل تعمل على نحو سليم.

٢- أن لا يطرأ على الدليل المقدم إلى المحكمة أي تغيير خلال مدة حفظه .

وقد اعتبر المُشرِّع السوري الشبكة وسيلة من وسائل العلنية المنصوص عليها في قانون العقوبات والقوانين الجزائية النافذة في سورية [١]. ولا بد من الإشارة إلى أنه في فترة الإعداد لقانون مكافحة الجرائم الإلكترونية، أصدر المُشرِّع السوري قانون التوقيع الالكتروني رقم /٤/ تاريخ ٢٠٠٩/٢/٢٥ . وقد تضمن هذا القانون فصلاً خاصاً يتعلق بالجرائم المرتبطة بالتوقيع الالكتروني، كتزويره أو استعمال التوقيع المزور ، أو تقديم المعلومات غير الصحيحة للحصول على شهادة المصادقة على التوقيع الالكتروني، وغير

[١] قانون مكافحة الجرائم الإلكترونية في سورية الصادر بالمرسوم رقم /١٧/ لعام ٢٠١٢.

ذلك من الجرائم [1].

وهكذا نجد بأن المُشرِّع السوري أدرك أهمية ملاحقة هذا النوع من الجرائم والنتائج والخسائر الاقتصادية الكبيرة المترتبة على وقوعها، وفي محاولة منه لمواكبة الدول المتقدمة أصدر قانوناً خاصاً لمكافحة هذه الجرائم ولم يكتفِ بعطف هذه الأفعال على قانون العقوبات التقليدي كما فعل المُشرِّع المصري.

[1] د. محمد طارق الخن، مرجع سابق، ص ١٧٣.

الفصل الثاني

فاعلية القانون الدولي في مكافحة الجرائم الالكترونية

المبحث الأول

مكافحة الجرائم الإلكترونية من قبل المنظمات والمؤتمرات الدولية

بما أن الجرائم الالكترونية تتمتع بطبيعة خاصة وهي جريمة عابرة للحدود، فإن مكافحتها الفعّالة لا تتحقق إلا بوجود تعاون متكامل من المجتمّع الدولي على المستويات كافة. فالتمّسك بمبدأ السيادة ومشاكل الحدود تشكل عقبة كبيرة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، حيث يستحيل على دولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لذلك أصبحت الحاجة ماسة لإنشاء منظمات دولية معنية بمكافحة هذا النوع من الجرائم. فقد لعبت المنظمات الدولية وعلى رأسها منظمة الأمم المتحدة دوراً مهماً في المحافظة على الأمن والاستقرار، وخاصة في مجال مواجهة الجريمة .

المطلب الأول: مكافحة الجرائم الإلكترونية من قبل المنظمات الدولية

سنتعرض في هذا المطلب إلى دور منظمة الأمم المتحدة في مكافحة الجرائم الإلكترونية، بالإضافة إلى دور المنظمة الدولية للشرطة الجنائية (الإنتربول)، ودور المنظمات الإقليمية مثل الاتحاد الأوروبي وجامعة الدول العربية.

أولاً- منظمة الأمم المتحدة

ترجع أهمية دور منظمة الأمم المتحدة في مكافحة الجرائم إلى طبيعة عمل المنظمة، وإلى عالميتها باعتبارها المنظمة الأم لباقي المنظمات الدولية، كما أن أهم أهدافها تتمّثل في الحفاظ على السلم والأمن الدوليين، وتنمية العلاقة

الودية بين الدول، وتحقيق التعاون الأمني في مواجهة الجرائم ذات البعد الدولي وفي مقدمتها الجرائم الإلكترونية.

بالإضافة إلى أنها تؤدي دوراً فعّالاً في وضع نظام يكفل التعاون والتنسيق بين المنظمات الدولية من خلال وضع نظام متبادل يقوم على حلٍّ المشكلات بين الدول، وإحداث تقاربٍ فيما بينهما من أجل التعاون في سبيل الخير المشترك للجماعة الدولية.

وعلى الرغم من أن القرارات التي تصدر عن المنظمة بشأن مكافحة الجرائم وملاحقتها والقضاء عليها ليس لها طابع إلزام، فإنها تتمتّع بقيمة أخلاقية أو أدبية كبيرة تجعلها ترقى إلى حدِّ الإلزام، ويعود ذلك لكونها تصدر عن منظمة دولية تضم في عضويتها معظم دول العالم، وبالتالي فإن هذه القرارات والتوصيات تصدر بناءً على موافقة عدد كبير من دول العالم، وبالتالي فإنها تعُّد تعبيراً عن رأي أو إرادة المجتمع الدولي، مما يجعل الدولة المخالفة لهذه القرارات في موقف استنكار من أعضاء المجتمّع الدولي الذي يمنحها نوعاً من الإلزام [1] .

وتقوم الأمم المتحدة بممارسة دورها في مكافحة الجريمة من خلال المجلس الاقتصادي والاجتماعي الذي يتولى الإشراف بصفة عامة على كل أجهزة المنظمة المختصة بمكافحة الجريمة، فيقوم هذا المجلس باعتماد قراراتها وينظم أعمالها، ثم يقوم بعرض القرارات التي تحتاج إلى تصديق على الجمعية العامة للأمم المتحدة. وقد ركز المجلس الاقتصادي والاجتمّاعي في برنامجه المتعلق بمكافحة الجريمة على هدفين، الأول وهو الحد من الخسارة المادية التي تنتج عن وقوع الجرائم، والثاني العمل على توفير المناخ الدولي المناسب وعلى

---

[1] د. محمد الشناوي، مرجع سابق، ص ٢٧٥ .

أعلى المستويات لتحقيق العدالة الجنائية سواء على نطاق ما يعدُّ جريمة وما لا يعد جريمة، وتقدير العقوبات المناسبة لكل جريمة، والعمل على إيجاد أسس أو قواعد تعتمد في وضع التشريعات الوطنية في سبيل مكافحة ومنع الجـــرائم ذات البعد الدولي[١] .

كما تمارس الأمم المتحدة دورها في مكافحة الجرائم من خـــلال عقـــد المؤتمرات الدولية التي تبحث من خلالها عن إيجاد الحلول الملائمة والفعَّالة في سبيل الحدِّ من هذه الجرائم، ووضع سياسات وبرامج وخطط موحدة بين أعضاء المجتمع الدولي من أجل تحقيق فاعلية المكافحة.

لذلك تعقد مؤتمرات دورية كل خمس سنوات، وذلـــك بهـــدف تعزيـــز وتبادل المعارف والخبرات بين الاختصاصين في مختلف الدول من أجل تدعيم التعاون الدولي والإقليمي في مجال مكافحة الجريمة، ويعُّد مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تمّ انعقاده في مدينة ميلانو بإيطاليا سنة ١٩٨٥م، حيث نتج عن هذا المؤتمر مجموعة من القواعد التوجيهية، والتي تُوِجت بالمصادقة على هذه المبادئ في مؤتمر هافانا "كوبا" عام ١٩٩٠م [٢].

كما أكد هذا المؤتمر على وجوب تطبيق التطورات الجديدة في مجـــال العلم والتكنولوجيا في كل مكان لصالح المجتمع الدولي، وبالتالي لمنع الجريمـــة على نحو فعِّال كما أكد على ضرورة اتخاذ تدابير ملائمة ضد حـــالات إســـاءة استعمال التكنولوجيا، كما أشار إلى مسألة الخصوصية التي يمكن أن تخترق عن

---

[١] المرجع السابق ص.٢٧٥

[٢] محمد الأمين ومحسن عبد الحميد أحمد، معايير الأمم المتحدة في مجـــال العدالـــة الجنائيـــة ومنـــع الجريمة أكاديمية نايف للعلوم الأمنية، الرياض ، الطبعة الأولى، ١٩٩٨ ، ص ١٩.

طريق الاطلاع على البيانات الشخصية المخزنة داخل نظم الحاسبات الآلية، والتي تشكل انتهاكاً لحقوق الإنسان واعتداءً على حرمة الحياة الخاصة.

كما واصلت الأمم المتحدة جهودها في مكافحة الجريمة عبر عقد عدة مؤتمرات كل خمس سنوات أهمها "المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين"، والذي عقد في القاهرة عام ١٩٩٥ ، وكان من أهم توصياته العمل من أجل حماية حياة الإنسان الخاصة وملكيته الفكرية في مواجهة مخاطر التكنولوجيا، والعمل على التنسيق وتعزيز التعاون بين أعضاء المجتمّع الدولي لاتخاذ الإجراءات المناسبة للحدّ منها [١] .

ولكن تبقى العقبة الأهم في وجه الدول مدى فاعلية القواعد والمبادئ التي تُقرها المؤتمرات الدولية ، والتوصيات والإرشادات التي تصدرها، فإن تنفيذ التوصيات التي تصدر عن هذه المؤتمرات تصب في مصلحة جميع أعضاء المجتمّع الدولي، كما أن مواطني الدول يتأثرون بهذه القرارات والتوصيات ومن هنا تأتي أهمية تنفيذ هذه القرارات والتوصيات. كما تتمثّل جهود الأمم المتحدة في منع الجريمة من خلال الاتفاقيات الدولية ذات الصلة بالموضوع، ومن أهم هذه الاتفاقيات "المعاهدة العالمية لحق المؤلف"، وقد انبثقت هذه المعاهدة عن منظمة اليونيسكو ١٩٥٢ [٢] ، وإن الهدف من هذه الاتفاقية هو تسهيل انتشار نتاج العقل البشري وتعزيز التفاهم الدولي [٣].

---

[١] الموقع الالكتروني: www.nauss.edu.sa/A/00archve/s/fm-dar5-3-nerprls02-p11
راجع أيضاً د.محمد الشناوي ، مرجع سابق ، ص٢٧٦

[٢] تعُّد اليونيسكو منظمة دولية متخصصة ترتبط بالأمم المتحدة حسب الشروط والتي نصت عليها المادتان ٥٧ و ٦٣ من ميثاق الأمم المتحدة والمؤتمر العام لمنظمة اليونيسكو في ١٤ ديسمبر ١٩٤٦ .

[٣] محمد الأزهر، حقوق المؤلف في القانون المغربي دراسة مقارنة في الملكية الأدبية والفنية، دار النشر المغربية، ١٩٤٤ ص٦١-٦٢ .

وعلى الرغم من أن حماية البرامج المعلوماتية والحاسب الآلي لـــم تكـــن موضوعاً مباشراً لهذه الاتفاقية، وربما يرجع السبب في ذلك إلى أن القرصـــنة والاعتداءات الإلكترونية لم تكن قد وصلت إلى هذا الحد، إلا أن هذه الاتفاقيـــة مهدت إلى المرحلة التي عرفتها مفاوضات جولة (الأورجواي)، والتي تميّـــزت بإعلان صريح عن موضوع الحماية للبرامج وذلك ضمن نصوص الاتفاقية التي تُعنى بالجوانب المتصلة بالملكية الفكرية.

وهكذا نجد بأن الاتفاقيات الدولية من شأنها أن تؤدي إلى تطويـــق هـــذه الجريمة والحد من مخاطرها على المجتمع الدولي بأسره، ويتوجب على الـــدول أن تتكاتف جميعها في وضع هذه الاتفاقيات الدولية موضع التنفيـــذ، وأن تقـــوم بتضمين تلك القواعد والاتفاقيات في تشريعاتها ولوائحها الداخلية من أجـــل أن تكون لها القوة الإلزامية في تنفيذها شأنها في ذلك شأن القوانين الداخلية .

ثانياً- المنظمة الدولية للشرطة الجنائية (الإنتربول)

انعقد المؤتمر الأول للشرطة الجنائية الدولية في موناكو عـــام ١٩١٤، وقد هدف المؤتمرون إلى إيجاد صيغة دولية معينة للتعاون في ســـبيل مكافحـــة الجرائم الدولية وقد كان عدد المجتمعين أربعة عشر دولة [١]، و ذلـــك لمناقشـــة ووضع أسس للتعاون الدولي في بعض المسائل الشرطية، وخاصةً فيما يتعلـــق بمدى إمكانية إنشاء مكتب دولي للتسجيل الجنائي وتنســـيق إجـــراءات تســـليم المجرمين، إلا أنه ونتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية تذكر [٢].

---

[١] منشور على موقع المنظمة الجنائية الدولية : www.interpol.net

[٢] د. محمد منصور الصاوي، أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات، دار المطبوعات الجامعية، ص ٦٤٨ .

وبنهاية عام ١٩٢٣ تمّ عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية، وضم مندوبي تسعة عشر دولة، ونتج عن هذا المؤتمر إنشاء اللجنة الدولية للشرطة الجنائية، وتعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة[١] .

وبعد اندلاع الحرب العالمية الثانية عقد في بروكسل "بلجيكا" عام ١٩٤٦ مؤتمر دولي يهدف إلى إحياء مبادئ التعاون الأمني ووضعها موضع التنفيذ، وانتهى الاجتماع إلى إحياء اللجنة الدولية للشرطة الجنائية بعد توقفها على أثر اندلاع الحرب ونقل مقرها إلى باريس بفرنسا، وتمّ تغيير اسمها ليصبح المنظمة الدولية للشرطة الجنائية [٢].

وتعد اليوم المنظمة الدولية للشرطة الجنائية من أهم المنظمات الدولية الناشطة في مجال مكافحة الجريمة نظراً لما تقدمه من إمكانية تعقبٍ وضبطٍ لمرتكبي الجرائم على اختلاف أنواعها أينما وجدوا، وتسليمهم إلى الهيئات المختصة بغية محاكمتهم وتوقيع العقوبة المناسبة عليهم، وتضم حالياً مئة وتسعين بلداً عضواً فيها، ويعمل لديها خمسمئة وواحد وأربعون موظفاً من تسعة وسبعون جنسيةً مختلفَّة ، وتباشر مهامها بأربع لغات رسمية (الانكليزية ، الفرنسية، الإسبانية والعربية) ، أما مقرها الحالي فيوجد بمدينة ليون الفرنسية [٣] .

---

[١] علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، ايتراك للنشر والتوزيع، ٢٠٠٠ ، ص ١٧٤-١٧٦.

[٢] د. خالد ممدوح ابراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية ، الطبعة الأولى ، ٢٠٠٩ ، ص٣٩٩-٤٠٠ .

[٣] مقالة منشور على الموقع الالكتروني: www.algeriepolice.dz/? .

وتعد منظمة الإنتربول ذات طبيعة اجتماعية بحتة، فتنص المادة الثالثة من دستور المنظمة أنه "ممنوع على المنظمة أن تقوم بأي تدخل أو نشاط له طابع سياسي أو عسكري أو ديني أو عنصري"، وإنما تنحصر أهداف المنظمة وفقاً لما بينته المادة الثانية من الدستور على تأكيد وتشجيع التعاون المتبادل بين سلطات الشرطة الجنائية للدول الأعضاء في المنظمة في حدود القوانين القائمة وبروح الإعلان العالمي لحقوق الإنسان، وإقامة وتنمية النظم التي من شأنها أن تسهم على نحو فعَّال في منع ومكافحة الجرائم وتتبع مرتكبيها [١] .

وقد نص ميثاق المنظمة الدولية للشرطة الجنائية على إنشاء مكاتب مركزية في إقليم الدولة العضو في الإنتربول، حتى يكون هذا المكتب وسيلة الاتصال وأداة التنسيق بين الشرطة المحلية من جانب وأجهزة المنظمة الدولية للشرطة الجنائية والمكاتب الوطنية المماثلة في الدول الأعضاء من جانب آخر[٢]، وأشار الميثاق إلى ثلاث وظائف أساسية تركز عليها جهوده وموارده وهي:

١- العمل على قيام تعاون شرطي عالمي ، ويقصد من ذلك بأن يكون بوسع موظفي المنظمة الاتصال فيما بينهم في مختلف أنحاء العالم، لذلك أقام الإنتربول منظومة اتصالات عالمية شرطية توصل معظم البلدان الأعضاء بهذه المنظومة.

٢- حفظ مجموعة أو قاعدة كبيرة من البيانات الميدانية وقواعد بيانات شرطية حتى تتمّكن الشرطة من الاتصال فيما بينها عبر الحدود، فهي بحاجة إلى معلومات تساعدها في التحقيقات ولمنع وقوع الجرائم، وتشتمل هذه البيانات على أسماء الأفراد والبصمات والصور ووثائق وجوازات السفر المسروقة أو المفقودة والمطلوبين، بالإضافة إلى معلومات ذات أهمية بالنسبة للانتربول.

---

[١] د. محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، مصر ، ٢٠٠٨ ، ص ٢٧٩.

[٢] المرجع السابق، ص ٢٨٠ .

٣- جهود الإنتربول حالياً تشمل عدد من المجالات وهي: المجرمون والفارون والأمن العام والإرهاب، والمخدرات والإجرام المنظم، والإتجار في البشر والإجرام المالي المرتبط بالتكنولوجيا المتقدمة مثل جرائم النصب والاحتيال والجريمة المعلوماتية ومجالات اهتمام أخرى [١] .

وقد استحدث الإنتربول عدداً من فِرق العمل التي تضم خبراء من شتى أنحاء العالم المتخصصين في الإرهاب البيولوجي والاتجار في البشر وجرائم تكنولوجيا المعلومات، وتجتمّع هذه الفرق بانتظام لتطوير وتشجيع الممارسات السليمة والتدريب على التحقيق والتحليل في مجالات إجرامية معينة.

وأن من أهم مهام الإنتربول مواجهة الاحتيال والنصب، والمقصود بالاحتيال هو الاحتيال الدولي، فنجد أن الإنتربول يسهم بدور بارز في مكافحة جرائم النصب عبر الإنترنت ، حيث إنها جرائم دولية ترتكب عبر الحدود في أكثر من دولة.

وقد أعلنت مؤخراً منظمة الإنتربول عن مساعيها إلى تنسيق القوانين والأحكام في مختلف بلدان العالم، والعمل مع الشركات المتخصصة بأمن الإنترنت بهدف إنشاء منظومة دولية من أجل مكافحة الجرائم الإلكترونية .[٢]

كما أكدت المنظمة على أن الجهود المبذولة عالمياً لمكافحة الجرائم الإلكترونية، وتعزيز الأمن الالكتروني بحاجة إلى تطبيق قانوني، وإلى العمل المباشر مع شركات القطاع الخاص التي تعمل في مجال أمن الإنترنت .

---

[١] المرجع السابق، ص ٢٨٠-٢٨١ .

[2] Malcom Anderson :" policing the world : Interpol the politics of International police co-operation ", claren press oxford, 1989.p168-185

بالإضافة إلى تنسيق القوانين والأحكام حول هذا الشأن في مختلف البلدان، وإن الإنتربول يعمل على توحيد الجهود مع جميع الدول، وذلك لتحسين الإجراءات القانونية التي تسمح بسرعة الاستجابة للتهديدات الإلكترونية.

وأشارت المنظمة خلال مؤتمر التعاون الدولي لمكافحة الجرائم الإلكترونية إلى أن الضباط المختصين في التحقيق بالجرائم الإلكترونية يتعرضون غالباً لتعقيدات القوانين والأحكام واختلافها بين الدول، إضافة إلى أن المجرمين وقراصنة الإنترنت يستغلون بذكاء هذه الثغرات القانونية المتمثلة بالاختلافات الإجرائية والقانونية بين البلدان فيما يتعلق بالجرائم الإلكترونية [1] .

ونظراً لما تنطوي عليه هذه الجرائم من مخاطر تهدد الاقتصاد الوطني والدولي تمّ عقد المؤتمر الدولي السادس بمعرفة المنظمة الدولية للشرطة الجنائية، وذلك عام ٢٠٠٥، وكان من أبرز القضايا المطروحة التهديدات التي تنتج عن إساءة استعمال التكنولوجيا الحديثة، بالنسبة للبنية التحتية الوطنية للدول الأعضاء، بالإضافة إلى التهديدات المتنامية بسبب إساءة استعمال المجموعات الإجرامية المنظمة للتكنولوجيا الحديثة وتهديد الإرهاب الذي تطرحه إساءة استعمال المجموعات الإرهابية للتكنولوجيا الحديثة، واستخدامها للاتصالات والدعاية والاعتداءات، وقد أكد المؤتمر على ضرورة التدريب وتوحيد المعايير القانونية والإجرائية على الصعيد العالمي لمواجهة جرائم الإنترنت والحاسبات الآلية.

وأكدت المنظمة على أهمية جمع المعلومات عن الجرائم الإلكترونية في قواعد بيانات الإنتربول وتعميمها على الدول الأعضاء، واستحداث فرق عمل

---

[1] مقالة منشور على الموقع الالكتروني: (الإنتربول – قوانين – صارمة – بين البلدان) www.algadidah.com/2013/.4/

إنتربول خاصة بجرائم تكنولوجيا المعلومات في جميع الأقاليم التي لا يوجد فيها فرق من هذا النوع[1].

ونلاحظ بأن أهم المزايا التي حققتها المنظمة الدولية للشرطة الجنائية هي تفعيل التعاون الدولي في تبادل المعلومات بين الدول الأعضاء في سبيل تحقيق المكافحة الفعَّالة للجريمة الإلكترونية وذلك طبعاً من خلال قاعدة البيانات التي قامت المنظمة الدولية للشرطة الجنائية بإنشائها، فهي تعتمد على شبكة الإنترنت لربط جميع الدول الأعضاء فيما بينهم من خلال المنظمة، مما يساعد على سرعة تبادل الرسائل والمعلومات، وإن هذه الشبكة مؤمنة تأمينات عالمية بشكل عالٍ ضد الاختراق .

وعلى الرغم من أن المنظمة الدولية للشرطة الجنائية تعُّد من أهم المنظمات الدولية المعنية بمكافحة الجرائم الدولية، إلا أنه يؤخذ عليها عدم التنسيق الكامل بين المنظمة والمكاتب الإقليمية الموجودة في الدول الأعضاء، وبطء بعض الإجراءات التي تؤدي إلى فرار بعض المطلوبين من يد العدالة.

بالإضافة إلى عدم التزام بعض الدول بالقرارات التي تصدر عن الدولة الأم، أي الدولة التي ينتمّي إليها المطلوب محاكمته، واستمّرار التعميم عن المطلوب على الرغم من صدور قرار بكف البحث عنه أمام قضاء بلده.

وهكذا نجد بأن للمنظمات الدولية دوراً فعالاً في مكافحة الجرائم الإلكترونية، وذلك يعود إلى تعدد الدول الأعضاء، وإمكانية تقديم التسهيلات اللازمة لملاحقة هذه الجرائم المستحدثة ذات الطبيعة الخاصة من سرعة التحقيق، وتوفر قاعدة البيانات اللازمة، وتحقيق التعاون بين الدول من ناحية

[1] د. محمد الشناوي، مرجع سابق، ص ٢٨٣ وما بعدها .

الاتصالات وشبكة الإنترنت بهدف التقليل من هذه الجرائم التي تسبب خسائر مادية فادحة لدول العالم.

ثالثاً- المنظمات الإقليمية

برزت على المستوى الإقليمي جهود متعددة لمكافحة الجرائم الإلكترونية، ومن أهمها جهود الاتحاد الأوروبي الذي يحاول تكريس التعاون بين أعضاء الاتحاد لمواجهة هذا النمط المستحدث من الإجرام سواء فيما بينهم أو بالتنسيق مع هيئات ومنظمات دولية أخرى [1]، وبالإضافة إلى ذلك، نجد جهوداً مبذولة على المستوى العربي من خلال الجامعة العربية بواسطة مجلس وزراء العدل العرب.

١- **الاتحاد الأوروبي:** ظهر التعاون الأمني الأوروبي بصورة شاملة ومنتظمة بعد توقيع هذه الدول على معاهدة الوحدة الأوربية المعروفة بمعاهدة "ماسترخ" لعام ١٩٩٢، وقد عملت هذه الاتفاقية على تسهيل حركة رأس المال والسلع والخدمات والأشخاص عبر حدود الدول الأعضاء، مما دفع المنظمات الإجرامية إلى توسيع نطاق أنشطتها، واتخاذ كافة السبل للحصول على الأموال من خلال ارتكاب كافة أشكال الإجرام، ومن أهمها الجرائم الإلكترونية، فامتد نشاط هذه المنظمات الإجرامية إلى مختلف الدول الأعضاء في الاتحاد، مستغلةً بذلك الفجوات الموجودة في تشريعات الدول الأعضاء من جهة، والتقدم التكنولوجي وسهولة حركة الأموال من جهة أخرى.

وقد اتخذ الاتحاد الأوروبي عدداً من الإجراءات في سبيل مكافحة الجريمة الإلكترونية وخصوصاً في مجال حماية الحياة الخاصة للإنسان من

---

[1] محمد أمين الشوابكة، (جرائم الحاسوب والإنترنت الجريمة المعلوماتية) ، دار الثقافة والنشر والتوزيع، الطبعة الأولى، الإصدار الثاني ٢٠٠٧ ص ٧٣ ؟

مخاطر المعالجة الأولية للبيانات ذات الطبيعة الشخصية، حيث بـــرزت جهـــود المجلس الأوروبي والسوق الأوربية المشتركة بعقد معاهـــدة مجلـــس أوروبـــا الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات، وقد وضعت في العام ١٩٨١، وكان كل ذلك الجهد نتيجة اهتمّام لجنة الـــوزراء فـــي المجلـــس بمسألة الخصوصية السرية منذ عام ١٩٦٨، والتي انطوت على توجيهات تهدف لوجوب توفير قواعد تكمل حماية البيانات الشخصية مـــن مخـــاطر المعالجـــة الآلية[١].

إن المبادئ والأسس التي تقوم عليها اتفاقية المجلس الأوروبي لا تختلف عن توصيات مجلس منظمة التعاون الاقتصادي والتنمية عام ١٩٨٠ ، وإن كان الاختلاف يكمن في عنصر الإلزام الذي تتمّيز به اتفاقية المجلـــس الأوروبـــي باعتبارها اتفاقية قانونية تلزم الدول الأطراف فيها.

وحديثاً أعلنت الدول الأعضاء في الاتحاد الأوروبي عن افتتاح المركز الأوروبي للجريمة الإلكترونية، والذي يقع على عاتقه معالجة الجرائم الخطيرة والمنظمة على الإنترنت، وتمّ افتتاح هذا المركز في هولندا التي تعد مقراً لـــه، ويتألف من طاقم كبير يعمل على دعم جهود مكافحة الجريمة الإلكترونية فـــي دول الاتحاد الأوروبي.

ويتم تمويل هذا المركز من قبل وكالة الشرطة الأوربية التي تتخذ من لاهـــاي مقراً لها، وقد وضع المركز مجموعة من الأهداف يقوم بالتركيز عليها، وهـــي

---

[١] وقعت على هذه الاتفاقية كل من النمسا – بليجكا – الدنمارك – ألمانيا – إيطاليا – لوكسمبورغ – النرويج – البرتغال – السويد – تركيا – المملكة المتحدة، وقد صدقت عليها كل مـــن فرنســـا – ألمانيا – النرويج – اسبانيا – السويد.

الاحتيال المصرفي عبر الإنترنت، والاعتداء على الأطفال، والجرائم التي تستهدف نظم تقنية المعلومات التابعة للاتحاد الأوروبي .

ويعمل المركز على تزويد الشرطة ووكالات إنفاذ القانون في الدول الأعضاء، بالمعلومات حول اتجاهات الجرائم الإلكترونية الجارية، بالإضافة إلى تفاصيل عن التهديدات الناشئة عن ارتكاب هذه الجرائم.[١]

٢- **جامعة الدول العربية :** إن أبرز الجهود العربية المبذولة من أجل مكافحة الجرائم الإلكترونية هي اعتماد مجلس وزراء العدل العرب للقانون الجنائي العربي الموحد كقانون نموذجي بموجب القرار رقم /٣٣٩/ لسنة ١٩٩٦، وهو خطوة مهمة على الصعيد العربي في مجال محاربة القرصنة وجرائم معطيات الحاسوب، فعاقب في المادة /٤٦٤/ منه على الدخول بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة وتغيير المعلومات داخل النظام وتزوير الوثائق المعالجة آلياً وسرقة المعلومات [٢] .

ويظهر أيضاً دور جامعة الدول العربية في مجال مكافحة الجرائم الإلكترونية من خلال حماية الملكية الفكرية وحق المؤلف خصوصاً في إبرام الاتفاقية العربية لحماية حقوق المؤلف التي أوصى مؤتمر الوزراء العرب المسؤولين عن الشؤون الثقافية المنعقد في بغداد في عام ١٩٨١ م بإبرامها، وقد جاء في ديباجة الاتفاقية أن الدول العربية إذ تحذوها الرغبة على حدٍّ سواء في حماية حقوق المؤلفين على المصنفات الأدبية والفنية بطريقة فعَّالة وموحدة [٣]،

---

[١] منشور على الموقع الألكتروني: /WWW.AITNEWS.COM/2013/01/10

[٢] القانون الجنائي العربي الموحد منشور على الموقع الالكتروني: WWW.cargg.org/sites/default/files/uniles/united/arab-crimmd

[٣] للاطلاع على الاتفاقية منشورة على الموقع: /www.aipit.org.eglarabic/pdf .

وفي هذا السياق قامت المنظمة العربية للتربية والثقافة والفنون أيضاً بعقد الاتفاقية العربية لتسيير انتقال الإنتاج الثقافي العربي في العام ١٩٨٧[١] .

وتعد هاتان الاتفاقيتان مثالاً واضحاً على جهود الجامعة العربية والمنظمات المتخصصة التابعة لها في مجال تنظيم حقوق المؤلف، وإن كان يعدُّ جهداً متواضعاً، نظراً لما تمّثله حماية حق المؤلف، باعتبارها اتجاهاً واحداً من اتجاهات مكافحة الجرائم الإلكترونية.

المطلب الثاني : مكافحة الجرائم الإلكترونية من قبل المؤتمرات الدولية

نظراً للطبيعة الخاصة للجرائم الإلكترونية لابد من تحرك المجتمع الدولي لمكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه، بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات.

فقد رأت الدول في عقد المؤتمرات الدولية ضرورة للحد من الصعوبات التي تواجهها في مكافحة هذه الجرائم فعمدت إلى عقد عدد من المؤتمرات التي تهدف إلى مكافحة الجريمة بشكل عام والجرائم الإلكترونية بشكل خاص ، وسوف نتعرض إلى عدد من هذه المؤتمرات ومنها:

---

[١] للاطلاع على الاتفاقية العربية لتسير انتقال الإنتاج الثقافي العربي مراجعة الموقع : www.almeezan.qa/agrteementspage.aspx

أولاً- مؤتمر الأمم المتحدة السابع حول منع الجريمة لعام ١٩٨٥م

تعقد الأمم المتحدة مؤتمرات لمنع الجريمة ومعاملة المذنبين كل خمس سنوات بناء على قرار المجلس الاقتصادي والاجتمّاعي وتحت إشراف فرع منع الجريمة والعدالة الجنائية [١] الذي تتخذ له مقراً في فينا، حيث تم عقد المؤتمر السابع لمنع الجريمة ومعاملة المذنبين في ميلانو بإيطاليا في الفترة ما بين ٢٦ أب - ٦ أيلول لعام ١٩٨٥، واشترك في هذا المؤتمر ١٢٥ دولة من جميع أنحاء العالم، ومنها سورية.

واشتركت العديد من المنظمات الدولية والإقليمية، ومن بينها المركز العربي للدراسات الأمنية والتدريب، ومجلس وزراء الداخلية العرب، ومجلس وزراء العدل العرب، وجامعة الدول العربية، والمنظمة العربية للدفاع الاجتماعي.

وسبق انعقاد المؤتمر عدة اجتماعات تحضيرية إقليمية في عام ١٩٨٣م، وذلك بالتعاون مع اللجنة الاقتصادية والاجتمّاعية لاسيا والمحيط الهندي، ومعهد أميركا اللاتينية لمنع الجريمة ومعاملة المذنبين، واللجنة الاقتصادية لأميركا اللاتينية، والجمعية الاقتصادية لغرب أسيا.[٢].

---

[١] مقالة منشورة على الموقع الالكتروني: www.nauss.edu.sa/A/00archve/s/fm-dar5-3-nerprls02-p11

[٢] مقالة منشورة على الموقع الالكتروني: www.nauss.edu.sa/A/00archve/s/fm-dar5-3-nerprls02-p11

ومن أهم المواضيع الأساسية التي تناولها المؤتمر حول الجريمة:

١- الأبعاد الجديدة للإجرام ومنع الجريمة في سياق التنمية وتحديات المستقبل.

٢- إجراءات العدالة الجنائية وآفاقها في عالم متغير .

٣- ضحايا الجريمة.

٤- وضع وتطبيق معايير وقواعد الأمم المتحدة في مجال العدالة الجنائية.

٥- الشباب والجريمة والعدالة.

وأشارت التقارير التي تمّ إعدادها من قبل سكرتارية فرع منع الجريمة والعدالة الجنائية في الأمم المتحدة إلى نقطتين رئيستين في مكافحة ومنع الجريمة وهي :

١- الأبعاد الجديدة للظاهرة الإجرامية

أشار التقرير إلى توسع نطاق الظاهرة الإجرامية في الظروف الراهنة، واستراتيجيات منع الجريمة والتخطيط لها، والتعاون المحلي والدولي ودور الأمم المتحدة، وتحديات المستقبل بالنسبة لمنع الظاهرة الإجرامية، وقد أشار إلى اعتراف الأمم المتحدة بصعوبة حصر النماذج، والأنواع الجديدة للظاهرة الإجرامية ويعود ذلك إلى تعقد المضامين الاجتماعية التي تنشأ فيها هذه الأنماط والنماذج، ومن أهم هذه النماذج جرائم الكومبيوتر والإنترنت .

كما أن اتجاهات الجريمة تتأثر بصورة كبيرة بسوء الحالة الاقتصادية التي يعيشها الأفراد في الدول المتخلفة، وإلى سوء الأوضاع والاستقرار الداخلي والوحدة والتناسق، حيث تبين أن الدول التي تعيش استقراراً داخلياً قد ظهرت فيها معدلات منخفضة للظاهرة الإجرامية، في حين أن الدول التي ظهرت فيها الاضطرابات الداخلية والأزمات الاقتصادية وارتفاع الهجرة الداخلية والبطالة قد سجلت مستوى مرتفع من الجرائم. [1]

وقد أشار التقرير إلى مجموعة من المبادئ والقواعد التي يجب على الدول إدخالها في نظمها التشريعية الهادفة إلى منع الجريمة ومكافحة الظاهرة الإجرامية، وهي قواعد تتعلق بمنع الجريمة والنظام الاقتصادي الدولي، والتنمية القومية ومنع الجريمة ومكافحتها ، وقواعد التعاون الدولي في منع الجريمة والعدالة الجنائية.

٢- تنظيم العدالة الجنائية وأفاقها في عالم متغير

تبين بأن النمو الاقتصادي السريع وخاصة في الدول النامية، قد أثرت على متطلبات العدالة الجنائية، وأصبح من الضروري إعادة النظر في تلك الظروف التي تعمل فيها أجهزة العدالة الجنائية من حيث التخطيط والإدارة، وقد تبين بأن أجهزة تنظيم العدالة الجنائية تتأثر بصورة مباشرة وغير مباشرة بالوسط الاجتمّاعي الذي تعمل فيه، وبالقيم والإيدولوجيات السائدة في المجتمّع، وتقف أجهزة تنظيم العدالة الجنائية عاجزة عن توفير محاكمة إنسانية عادلة سريعة.

---

[1] مقالة منشورة على الموقع الالكتروني: www.nauss.edu.sa/A/00archve/s/fm-dar5-3-nerprls02-p11

وفيما يتعلق بأفاق العدالة الجنائية في عالم متغير فهي تتمثّل في وضع خطة تنظيمية متكاملة ترمي إلى إدخال التعديلات المناسبة على جهاز العدالة الجنائية، وتوفير التشريعات الضرورية لتحقيق الأهداف المرجوة، وإعادة تنظيم أجهزة العدالة الجنائية، والاعتماد على البحث العلمي، واستخدام التكنولوجيا الحديثة في مجال تنظيم العدالة الجنائية[1] .

وقصد التقرير بشأن التعديلات التشريعية إلى ضرورة رفع الصفة التجريمية عن بعض الأفعال التي تعدُّ جريمة، من أجل تخفيف الضغط على الأجهزة المختصة بتطبيق العدالة الجنائية. وفي مجال البحث العلمي أشار التقرير إلى ضرورة استخدام الكومبيوتر، وإيجاد ظروف التجربة وآلياتها للقيام بعملية التقييم والتقدير، وقياس فعالية أجهزة العدالة الجنائية.

وإن من أهم القرارات التي صدرت عن مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين لعام ١٩٨٥ القرار رقم (٩)، والذي يدعو الدول الأعضاء إلى تطوير المعلومات والنظم الإحصائية باتخاذ التدابير اللازمة لنقل المعلومات داخل النظام القضائي، ويحثهم على حماية حقوق المواطنين ومصالحهم المشروعة وخاصة سرقة البيانات، ويطالب الأمين العام بتدعيم الجهود الرامية إلى إنشاء وتطوير الاحصائيات القومية، ويوصي لجنة منع الجريمة ومكافحتها باستعراض

[1] مقالة منشورة على الموقع الالكتروني: www.nauss.edu.sa/A/00archve/s/fm-dar5-3-nerprls02-p11

الدراسات التي قامت بها الأمم المتحدة عن اتجاهات الجريمة، وسير نظم العدالة الجنائية، واستراتيجيات منع الجريمة[1].

ثانياً- مؤتمر الأمم المتحدة الثامن حول منع الجريمة لعام ١٩٩٠م

عقد مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين في هافانا من ٢٧ أب إلى ١٧ أيلول من عام ١٩٩٠ انطلاقاً من الإعلان العالمي لحقوق الإنسان الذي يجسد مبادئ المساواة أمام القانون وافتراض البراءة والحق في محاكمة عادلة وعلنية أمام محكمة مستقلة ومحايدة، ورغبة من الدول في التعاون الدولي من أجل مكافحة الجرائم ذات الطابع الدولي والتي تتطلب تكاتفاً من الدول من أجل الحد من الظواهر الإجرامية الحديثة منها الجرائم الإلكترونية وشبكة الإنترنت، فقد تمَّ عقد مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين .

حيث ركز المؤتمر على دور القائمين بتنفيذ العدالة، وحدد المبادئ التوجيهية لعمل أعضاء النيابة العامة والمحامين وانطلاقاً من أن أعضاء النيابة العامة والمحامين يضطلعون بدور حاسم في إقامة العدل ، وأن القواعد المتعلقة بأدائهم لمسؤولياتهم الهامة ينبغي أن تعزز احترامهم للمبادئ الأنفة الذكر والتزامهم بمبادئ القانون، بحيث تسهم في إقامة عدالة جنائية منصفة وفي وقاية المواطنين من الجريمة بصورة فعَّالة، فالهدف الجوهري هو تأمين حصول أعضاء النيابة العامة على

---

[1] للاطلاع على القرار مراجعة الموقع: www.nauss.edu.sa/A/00archve/s/fm-dar5-3-nerprls02-p11

المؤهلات المهنية اللازمة للاطلاع بوظائفهم، عن طريق تحسين أساليب تعيينهم وتدريبهم القانوني والمهني، ومن خلال تهيئة كافة الوسائل التي تلزمهم لأداء دورهم بطريقة سليمة في مكافحة الإجرام ، وبصفة خاصة في أشكاله وأبعاده الجديدة المتمّثلة بالجرائم الحديثة (الإلكترونية) [1] .

ثالثاً- مؤتمر الأمم المتحدة حول منع الجريمة لعام ٢٠٠٠م

عقد المؤتمر في فيينا عام ٢٠٠٠ في سبيل مواجهة تحديات الجريمة عبر الوطنية وتعزيز سيادة القانون وتدعيم نظام العدالة الجنائية والتعاون الدولي في مكافحة الجريمة عبر الوطنية ومنع الجريمة منعاً فعَّالاً من خلال مواكبة التطورات الجديدة، وذلك يعود إلى أن الجماعات الإجرامية تستغل ظواهر عصرية مثل العولمة، وتزايد انفتاح الحدود بين بلدان العالم والتقدم التكنولوجي.

وهذه المشاكل الحديثة النشوء لا يمكن للحكومات أن تتصدى لها على نحو فعال بمفردها أو من خلال الأشكال التقليدية للتعاون الدولي في مجال مكافحة الجريمة، لذلك كان من الضروري عقد هذا المؤتمر .

وتأتي أيضاً أهمية المؤتمر العاشر لمنع الجريمة ومعاملة المجرمين أنه انعقد على أعتاب ألفية جديدة، فكان ملتقى عالمياً وغير مسبوق لتبادل وتعزيز أفكار ابتكارية من ميدان الجريمة ولاسيما الجرائم المستحدثة نتيجة للتطور التقني كالجرائم الإلكترونية [2] وصدر

---

[1] مبادئ توجيهية للمؤتمر الثامن منشورة على الموقع الالكتروني:
http://www.hrea.ogr/index.php

[2] منشورة على الموقع الالكتروني:
www.on.ogr/arbic/events/conferences/cnime/conferrnce.htm

عن هذا المؤتمر "إعلان فيينا" بشأن أولويات العدالة ومواجهة تحديات القرن الحادي والعشرين، وقد أكد هذا الإعلان على ضرورة توفير التنسيق والتعاون بين الدول في مكافحة مشكلة الجريمة العالمية، واتخاذ التدابير اللازمة، والحاجة إلى تطوير وتعزيز أنشطة التعاون التقني بغية مساعدة البلدان فيما تبذله من جهود لتدعيم نظمها المحلية في مجال العدالة الجنائية وقدرتها على التعاون الدولي.

وأكد الإعلان في البند السابع عشر منه على توصيات عملية بشأن منع ومكافحة الجريمة المتعلقة بالحواسيب، ودعوة لجنة منع الجريمة والعدالة الجنائية إلى الاطلاع بالعمل في هذا الشأن، آخذة بعين الاعتبار الأعمال الجارية في محافل أخرى.

والتأكيد على الالتزام بالعمل من أجل تعزيز القدرات على منع الجريمة المرتبطة بالتكنولوجيا الراقية والحواسيب والتحري عن تلك الجرائم وملاحقتها [1] .

رابعاً- مؤتمر الأمم المتحدة حول منع الجريمة لعام ٢٠٠٥م

عُقد المؤتمر الحادي عشر في بانكوك عام ٢٠٠٥، وعالج عدد من المواضيع المهمة في مجال مكافحة الجريمة أهمها:

١- تعزيز التعاون الدولي في إنفاذ القانون، بما في ذلك تدابير تسليم المجرمين.

٢- تعزيز إصلاح العدالة الجنائية، بما في ذلك العدالة التصالحية.

---

[1] نص منشور على الموقع: http: //www1.umn.edu/hnmanrtss/arab/vi2000.html

٣- استراتيجيات لمنع الجريمة وأفضل الممارسات ، وخاصة فيما يتعلق بجرائم المناطق المتضررة والشباب المعرضين للخطر .

٤- تدابير مكافحة الإرهاب، فيما يتعلق بالاتفاقيات والبروتوكولات الدولية ذات الصلة.

٥- تدابير مكافحة الجريمة الاقتصادية، بما في ذلك غسل الأموال.

٦- تدابير مكافحة الجرائم ذات الصلة بالحاسوب.

هذا وقد دعت الجمعية العامة في قرارها ١٢١/٥٦ الدول الأعضاء عند وضع القوانين الخاصة بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، أن تأخذ في اعتبارها أعمال وإنجازات لجنة منع الجريمة والعدالة الجنائية والمنظمات الدولية والإقليمية الأخرى، وفي قرارها ٢٦١/٥٦ أحاطت الجمعية العامة علماً بخطط العمل لتنفيذ "إعلان فينا" المشار إليه سابقاً، حيث تسعى الدول من أجل متابعتها إلى دعم عدد من الإجراءات، ومن بينها تجريم إساءة استعمال تكنولوجيا المعلومات، ووضع وتنفيذ قواعد وإجراءات تضمن تحري الجرائم ذات الصلة بالحاسوب والاتصالات على نحو فعّال، وضمان تدريب العاملين في إنفاذ القانون وتزويدهم بالمعدات اللازمة لتمكينهم من الاستجابة على نحو فعّال لطلبات المساعدة في تعقب الاتصالات وغير ذلك من التدابير اللازمة لكشف وتحري الجرائم عبر الوطنية المتصلة بالتكنولوجيا الرفيعة والحاسوب، والشروع في مناقشات بشأن إجراءات لمكافحة الجرائم المتصلة بالتكنولوجيا ، وآثار التغير التكنولوجي مع الصناعات العاملة في تطوير الحاسوب ونشره، ومعدات الاتصالات، وبرمجيات ومعدات الشبكات، وخلاف ذلك.

وعلاوة على ذلك، أحاطت الجمعية العامة علماً في قرارها ٢٣٩/٥٧، بالعناصر المرفقة بالقرار بهدف إنشاء ثقافة عالمية لأمن الفضاء الحاسوبي، ودعت الدول الأعضاء وجميع المنظمات الدولية ذات الصلة أن تضع هذه العناصر في اعتبارها، وفي قرارها ١٩٩/٥٨ شجعت الجمعية العامة الدول الأعضاء والمنظمات الإقليمية والدولية ذات الصلة التي وضعت استراتيجيات للتصدي لأمن الفضاء الحاسوبي، وحماية الهياكل الأساسية الحيوية للمعلومات على تبادل أفضل الممارسات[١].

خامساً- مؤتمر الأمم المتحدة الثاني عشر حول منع الجريمة لعام ٢٠١٠م

رَّكز المؤتمر في جدول أعماله على مواضيع تتعلق بالأطفال والشباب والجريمة، وإعمال مبادئ الأمم المتحدة التوجيهية في مجال منع الجريمة، وتقديم المساعدة التقنية لتيسير التصديق على الصكوك الدولية المتصلة بمنع الإرهاب وقمعه وتنفيذ تلك الصكوك، واتخاذ التدابير في مجال العدالة الجنائية للتصدي لتهريب المهاجرين والاتجار بالأشخاص، والصلات بالجريمة المنظمة العابرة للحدود الوطنية، واتخاذ التدابير في مجال منع الجريمة والعدالة الجنائية للتصدي للعنف ضد المهاجرين وأسرهم، والتعاون الدولي لمكافحة غسيل الأموال استناداً إلى صكوك الأمم المتحدة وسائر الصكوك ذات الصلة، والنهج العلمي لتعزيز التعاون الدولي في مجال مكافحة الجريمة والمشاكل المتعلقة بها،

---

[١] أعمال المؤتمر منشورة على الموقع: www.un.org/arabic/events/11thcongress/docs/programme v0581638.pdf

بالإضافة إلى التطورات الأخيرة والتي ركز عليها المؤتمر في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة، بما ذلك الجرائم الإلكترونية[1] .

و عقدت حلقات عمل أثناء المؤتمر بشأن التثقيف في مجال العدالة الجنائية على الصعيد الدولي من أجل تحقيق سيادة القانون واستقصاء أفضل الممارسات المعتمدة في مجال معاملة السجناء في نظام العدالة الجنائية، وبشأن النهج العملي لمنع الجريمة في المدن، وحلقة عمل بشأن الصلات القائمة بين الاتجار بالمخدرات وسائر أشكال الجريمة المنظمة، وبشأن الاستراتيجيات وأفضل الممارسات من أجل الحيلولة دون اكتظاظ السجون.

وأهم مقررات مؤتمر البرازيل هو إعلانه بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية وأهمها تطور تكنولوجيا المعلومات والاتصالات وزيادة استخدام الإنترنت مما يجعل الفرصة مناسبة أمام المجرمين لتوسيع النطاق الإجرامي[2].

وأشار المؤتمر إلى أهم صعوبات وتحديات الجريمة الالكترونية وهي:

١-عدم اليقين: إن طبيعة الجرائم الالكترونية المتطورة بشكل سريع يجعل من الصعب الحصول على أرقام إحصائية دقيقة، وحول حجم الخسائر المالية وعدد الجرائم التي يرتكبها الجناة في الفضاء

---

[1] مقررات المؤتمر وثيقة منشورة على الموقع : www.unodc.org/documents/crime-cogress/ crime /v10538262.pdf

[2] وثيقة منشورة على الموقع : www.unodc.org/documents/crime-cogress/ crime /v10538262.pdf

الالكتروني، ولا يقتصر تطبيق هذا النقد المنهجي على الخسائر، وإنما ينطبق أيضاً على الجرائم المعترف بها، كما إنه من غير المؤكد مدى إبلاغ الضحايا عن الجرائم الإلكترونية، فعلى الرغم من أن السلطات المعنية بمكافحة الجرائم الإلكترونية تشجع الضحايا على الإبلاغ عن تلك الجرائم. فما زال العديد من الضحايا الذين يقومون بالإبلاغ عن وقوع تلك الجرائم قليل نسبياً وخصوصاً في القطاع المالي (البنوك) خوفاً من أن يسيء الإعلان السلبي إلى سمعة أولئك الضحايا. كما أكد المؤتمر على أنَّه غالباً ما يتمّ اقتباس معلومات غير موثوقة وغير قابلة للتحقيق من مصادرها أو تحديد الجهات التي تقوم بعملية الإحصاء.

٢-**البعد الدولي:** إن الجريمة الإلكترونية ذات بعد دولي وعابرة للحدود نظراً لارتباطها بشبكة الإنترنت التي صممت أصلاً لتكون شبكة عسكرية تقوم على بنية شبكة لا مركزية، وإن صفتها الدولية ناجمة عن توفيرها للخدمات والتحديثات التي تصل إلى كل أنحاء العالم في لحظات وهذا ما يفرض صعوبة التحقيق في الجريمة الالكترونية بالإضافة لمبدأ السيادة الوطنية الأساسي، الذي بمقتضاه لا يمكن إجراء تحقيقات في أقاليم أجنبية، دون إذن السلطات المحلية [١] .

والتحدي الرئيسي الآخر يتعلق بالوقت القصير المتاح لإجراء التحقيقات في الجرائم الإلكترونية، والتي يمكن أن يستغرق وصولها إلى مقصدها أسابيع، في حين يمكن إيصال الرسائل الإلكترونية في ثوانٍ، كما يمكن تنزيل ملفات كبرى في دقائق.

---

[١] وثيقة منشورة على الموقع : www.unodc.org/documents/crime-cogress/ crime /v10538262.pdf

كما أشار المؤتمر إلى ضرورة التعاون الأمني والفعَّال بين السلطات في مختلف البلدان وفي جميع المجالات، ففي قضايا الجريمة الإلكترونية، تحذف الأدلة غالباً بشكل تلقائي وضمن أطر زمنية قصيرة، ويمكن للإجراءات الرسمية المطولة أن تعيق التحقيقات إعاقة خطيرة.

٣ــ الاختلافات في النهج القانونية الوطنية: يرى المؤتمر إنَّ لمسألة التقارب بين النُظم التشريعية أهمية كبيرة ، لأن العديد من البلدان تستند في نظام مساعداتها القانونية المتبادلة إلى مبدأ ازدواجية التجريم، الذي بمقتضاه يجب اعتبار الاعتداء جريمة في الدولة التي تطلب المساعدة والدولة التي تقّدمها، وقد حدد المؤتمر أهم التدابير اللازمة للتصدي للجريمة الإلكترونية والمتمّثلة بواجب الدول وضع تشريعات للجرائم الإلكترونية على الصعيدين الوطني والإقليمي، والعمل على بذل الجهود على الصعيد العالمي لتنسيق التشريعات بشأن الجريمة الإلكترونية وإنفاذ القانون الذي يعتمّد بقدر كبير، على توافر أدوات التحقيق ومنها؛ البرامج الجنائية (لجمع الأدلة ورصد لوحة المفاتيح واستكشاف أو استرداد الملفات المحذوفة) وبرامج إدارة التحقيق ، وما إلى ذلك من أدوات ضرورية لإنفاذ القوانين المتعلقة بمكافحة الجرائم الإلكترونية. ودعا المؤتمر إلى ضرورة بناء القدرات والإمكانات، فالجريمة الإلكترونية مسألة لا تعني البلدان المتقدمة فحسب، ولكنها تعني البلدان النامية أيضاً. وبما أن التحقيق في الجرائم الإلكترونية ومقاضاة الضالعين في ارتكابها ينطوي على تحديات فريدة، فمن المهم توفير التدريب لضباط إنفاذ القانون والمدعين العامين والقضاة[١].

[١] وثيقة تتعلق بمقررات المؤتمر الثاني عشر لمنع الجريمة منشورة على الموقع : www.unodc.org/documents/crime-cogress/ crime /v10538262.pdf

ونلاحظ أن نيل الجريمة الإلكترونية موقعاً بارزاً في جدول أعمال مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، مما يؤكد أهميتها التامة والتحديات الخطيرة التي تطرحها، على الرغم من أن مناقشة المسألة ما زالت متواصلة نحو نصف قرن من خلال المؤتمرات السابقة ، ويبقى الموضوع مثيراً للجدل، لأن التكنولوجيا ما انفكت تتطور، ولأن الأساليب المستخدمة في ارتكاب الجرائم الإلكترونية تتغير أيضاً.

المبحث الثاني

مكافحة الجرائم الالكترونية في الاتفاقيات الدولية

الجريمة ظاهرة اجتماعية تمثل إحدى المشكلات الكبرى في العالم وتشكل إحدى القضايا الرئيسة التي تأخذ حيزاً لا بأس به في مجالات عمل الأمم المتحدة.

وسنتحدث في المطلب الأول عن المعاهدات والاتفاقية الأجنبية حول مكافحة الجرائم الالكترونية، وفي المطلب الثاني عن المعاهدات والاتفاقيات العربية حول مكافحة الجرائم الالكترونية .

المطلب الأول : الاتفاقيات الأوربية حول مكافحة الجرائم الالكترونية

تقوم الدول عند تلاقي وجهات النظر حول مكافحة الجرائم الالكترونية بصياغة ذلك بموجب معاهدة أو اتفاق دولي يحدد سبل التعاون فيما بين الأطراف الموقعة وطرق الواجب اتباعها لتحقيق الغاية من هذه المعاهدة .

وغالباً ما تشتمل مثل هذه الوثائق الموقعة على ما يفيد رغبة الأطراف في دعم التعاون وتوثيق الروابط بعينها والانتقال إلى صورة أو شكل جديد من الأشكال التعاونية الأكثر تأثيراً كتبادل المساعدة في التحقيقات، أو تبادل المساعدة القضائية والشرطية والمنح الفنية أو التدريبية [1].

---

1 Pem laa jimene 2 : 'international securithies en for emcnet cooperation Act and Memora of understanding , In harvard intirational law journal , winter 1990 , vol , 31 , No, Harvard law school, cambrige , massachustts, p.295-311 .

ومن أهم مزايا مثل هذه الوثائق أنها يمكن أن ترسم بوضوح كافة الإجراءات التفصيلية التي تحكم بحال الاهتمام المشترك بين أطراف التعاون وأن تنشئ جدول زمني يسهل في التعامل ومن أهم الاتفاقيات الدولية التي تم إنشائها في سبيل مكافحة الجرائم الالكترونية[1] .

أولاً- الاتفاقية الأوربية الخاصة بحماية الأفراد من معالجة المعلومات الخاصة بهم لعام ١٩٨١ م

تعد هذه الاتفاقية من أهم أعمال المجلس الأوروبي وهي الاتفاقية المسماة باتفاقية (١٠٨) والخاصة بحماية الأفراد من معالجة المعلومات الخاصة بهم والموقعة بتاريخ ١٩٨١/١/٢٨ وجاءت مقسمة إلى سبعة فصول تضمنت التوصيات العامة، الأسس المبدئية لحماية المعلومة، انتقال المعلومة خارج حدود البلد، التعاون المتبادل بين الدول، اللجنة الاستشارية، التعديلات الجائز اقتراحها من الأعضاء ، البنود الختامية. فالمادة الأولى منها عرفت الهدف من الاتفاقية هو حماية الأفراد وحماية حياتهم الخاصة فيما يتعلق بالمعالجة الآلية للمعلومات بغض النظر عن أصولهم أو جنسياتهم، وقد أوضحت المادة الثانية معاني المصطلحات المستعملة في الاتفاقية مثل المعلومة الشخصية بأنها تلك المعلومة المتعلقة بفرد بعينه – محدد – ويقصد بملفات المعلومات أي مجموعة من المعلومات تعالج ألياً بالحاسوب، ويقصد بالمعالجة الآلية تخزين المعلومة في الحاسوب ونقل وتبادل البرامج أو تغيير المعلومة أو مسحها، أو توزيعها كذلك ، وقامت الاتفاقية بتحديد من يطلق عليهم مراقب الملفات أو المسؤول عنها بكونه

[1] hardishon piit & Shapiro: "proplems of en forcement in the 435 maltintioanl securities market, 9u. pa.j.int lbus. G 1987

كل شخص طبيعي أو قانوني أو سلطة عامة أو وكالة أو أية جهة مصرح لها وفقاً لقانون البلد بتحديد الهدف من جمع المعلومات وكيفية أو هدف معالجتها [1].

كما أصدر المجلس الأوروبي التوصية المرقمة (٤٦/٩٥) المتعلقة بحماية الأفراد فيما يخص المعلومات المتعلقة بهم وعملية تناقلها والصادرة في ١٩٩٥/١٠/٢٤ وتتكون هذه التوصية من (٣٤) مادة يسبقها مقدمة من (٧٢) مادة تحظى بأهمية خاصة كونها دليل لفهم مضمون التوصيات، وأهم ما تضمنته هذه التوصية الترخيص بالتنقل الحر دون أدنى قيود للمعلومات الفردية عبر الملفات التقليدية (الورقية) ما كان منها مكتوباً أو مخزناً في ذاكرة الحاسب الألي والمتنقل عبر شبكات المعلوماتية للدول المؤلف منها السوق الأوربية المشتركة حيث أن هذه المعلومات أصبحت ذات قيمة اقتصادية تستوجب حمايتها إضافة لقيمتها الإنسانية، وهذا استتبع توحيد أساليب التظلم القانونية المكرسة لحماية الأفراد في الدول الأعضاء في السوق الأوربية وذلك من أجل تأمين الحد الأدنى من الحماية لتلك المعلومات عند انتقالها عبر الحدود، وبموجب هذه التوصية يحق لأي فرد أوروبي أن يلزم القضاء المحلي في أي من دول السوق الأوربية باحترام هذه التوصية وأخذاً بالأولوية من حيث التطبيق على القانون المحلي خصوصاً ما تعلق منها بالجانب الجزائي [2].

وهكذا نجد بأن الدول الأوربية كانت السباقة في مجال عقد الاتفاقيات والمعاهدات اللازمة لمكافحة الجرائم الالكترونية وقد سخرت العدد الكبير من الاختصاصيين والقانونيين والفنين في سبيل مكافحة هذا الخطر الذي يسبب الخسائر المادية والمعنوية للمؤسسات والبنوك وكافة الأشخاص الخاضعة للقانون الدولي في تعاملاتها التجارية الدولية ولعل السبب في ذلك يعود إلى أن الدول

---

[1] الاتفاقية موجودة على الموقع الالكتروني: www.metment.gov.com

[2] التوصية رقم (٤٦/٩٥) موجودة على الموقع: http:www.stanford.edu.html.p52-39

الأوربية هي الدول الأكثر تقدماً علمياً وتقنياً الأمر الذي دفعها لوضع التوصيات وعقد الاتفاقيات التي تحتاجها تشريعاتها الداخلية لمكافحة هذا النوع المستحدث من الإجرام وملاحقة القائمين بارتكاب هذه الأعمال.

ثانياً- الاتفاقية الأوربية حول الجريمة الافتراضية لعام ٢٠٠١م

تؤدي الاتفاقات والمعاهدات الدولية دوراً فعالاً في إنشاء المنظمات والكيانات الدولية لإدارة التعاون الدولي في سبيل مكافحة الجريمة ، وقد أسهمت في تطوير أوجه التعاون المختلفة في مكافحة الجريمة بالإضافة إلى كون المعاهدات تعد من أهم مصادر القانون الدولي المكتوب.

فبعد جهود بذلها الاتحاد الأوروبي سعياً لإيجاد وسيلة لمكافحة الجرائم المرتكبة عبر الإنترنت، تم إبرام هذه الاتفاقية في العاصمة المجرية بودابست بتاريخ ٢٠٠١/١١/٢٣ وتعد هذه الاتفاقية من أهم الاتفاقيات الأوربية في سبيل مكافحة الجرائم الالكترونية والإنترنت، وتضم العديد من النصوص التجريمية والإجرائية الخاصة بمكافحة الجريمة المعلوماتية[١].

وقد كانت هذه الاتفاقية الخطوة الأولى والعملية في مجال مكافحة الجرائم المرتكبة عبر الإنترنت وخاصة بعد أن وصلت الجرائم إلى حد خطير يهدد الأشخاص والشركات والبنوك[٢].

تتلخص أهم أهداف الاتفاقية في السعي لتحقيق وحدة التدابير الشتريعية بين الدول الأوربية والدول المنضمة للاتفاقية من غير الدول الأوربية والتأكيد على

---

[١] د. هلالى عبد اللاه أحمد، الجوانب الموضوعة والإجرائية لجرائم المعلوماتية، ط١ ، ٢٠٠٢، ص ١٠٧.

[٢] منير محمد الجيهي، ممدوح محمد الجنينيهي ، مرجع سابق، ص ١٨ .

أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الإنترنت، وتحقيق التوازن بين حقوق الإنسان والإجراءات المتخذة لمواجهة الجرائم الالكترونية ، حيث تقدم هذه الاتفاقية الخاصة بجرائم الإنترنت دليلاً إرشادياً لتطوير التشريعات الوطنية لمكافحة الجرائم الالكترونية [١].

وتقوم هذه الاتفاقية بتعريف وتحديد العقوبات المترتبة على ارتكاب جرائم الإنترنت في إطار قوانينهم المحلية، وبالاطلاع على هذه الاتفاقية نجد في مقدمتها الكثير من الجرائم المرتكبة عبر الإنترنت، منها المتعلقة بالبيانات الشخصية في مجال الخدمات المتعلقة بالاتصالات السلكية واللاسلكية [٢].

وقد استغرقت المفاوضات بين الدول الموقعة على هذه الاتفاقية أربعة أعوام حتى تم التوصل إلى الصيغة النهائية المناسبة، حيث قامت أربع دول من غير الأعضاء في المجلس الأوروبي بالمشاركة في إعداد هذه الاتفاقية والتوقيع عليها، وهي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية[٣].

تتألف هذه الاتفاقية من /٤٨/ مادة موزعة على أربعة فصول وهي:

الفصل الأول: يتضمن تعريفاً للمصطلحات الأساسية .

الفصل الثاني: يتضمن الخطوات الواجب اتخاذها على الصعيد الوطني من أجل مكافحة الجرائم الالكترونية وهو يتألف من ثلاث أقسام يتضمن القسم الأول المواد التي تعالج الأحكام الموضوعية لجرائم الإنترنت، والثاني يتضمن المواد

---

[١] الاتفاقية منشور على الموقع الالكتروني eonvenwtions.c.int

[٢] واقد يوسف، النظام القانوني للدفع الالكتروني، رسالة لنيل درجة الماجستير، جامعة مولود معمري، كلية الحقوق، الجزائر ص١٨٥ .

[٣] هذه الاتفاقية متوفرة على الموقع الالكتروني euripeconvutiononsber-crimeconventions .co.int

التي تتعلق بالأحكام الإجرائية والأساليب اللازم اتباعها لمواجهة هذا الخطـــر، والثالث يعالج موضوع الاختصاص .

الفصل الثالث: ويتعلق بالتعاون الدولي بين الأطراف الموقعة من أجل مكافحـــة جرائم الإنترنت.

الفصل الرابع: يشتمل على الأحكام الختامية التي تم الاتفاق عليها بـــين الـــدول الأعضاء [١].

وقد نصت المادة الثانية من الاتفاقية على تجريم الدخول غير المشروع إلى المواقع الالكترونية، حيث أنه ((يجب على كل طرف أن يتبنـــى التـــدابير التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقاً لقانونه الداخلي الولوج العمدية لكل أو لجزء من جهـــاز الحاســـب بدون حق، كما يمكن أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجراميـــة أخـــرى، أو أن ترتكب الجريمة في حاسب ألي يكون متصلاً عن بعد بحاسب آخر)) [٢].

ومن خلال ذلك نجد بأن الاتفاقية قد تضمنت أحكاماً إجرائيـــة تتعلـــق بجريمة الدخول (الولوج) غير المشروع التي تنطوي على تهديد وتعدي علـــى النظام المعلوماتي المتبع في منشأ أو مؤسسة معينة، إذ أن هناك ضرورة لتوفير ممارسة ملائمة لمصالح المنظمات والمؤسسات وإتاحة الفرصة لرجـــال الإدارة في هذه المؤسسات أن يديروا ويستثمروا ويتحكموا في نظمهم بدون تشويش أو عقبة من أي نوع .

---

[١] الاتفاقية منشورة على الموقع السابق .

[٢] انظر المادة الثانية من الاتفاقية .

فاعتبرت الاتفاقية إن مجرد التدخل غير المصرح به بمعنى القرصنة أو السطو أو الدخول غير المشروع في النظام المعلوماتي، كل أولئك يجب أن يعتبر غير قانوني في حد ذاته كمبدأ عام، وذلك على أساس أن هذه الأفعال يمكن أن تخلق عقبات أمام المستخدمين القانونيين للنظم والبيانات، كما يمكن أن تؤدي إلى إتلاف أو تدمير باهظ التكلفة في حالة إعادة البناء كما أن هذا التدخل يمكن أن يترتب عليه الوصول إلى بيانات سرية، مثال ذلك كلمات المرور أو معلومات عن النظام المستهدف أو أسرار تسمح باستخدام النظام مجاناً، بل وتشجع القراصنة على ارتكاب أنواع أكثر خطورة من الجرائم المتعلقة بالحاسب مثال ذلك الغش المعلوماتي أو التزوير المعلوماتي.

ويشمل الدخول غير المشروع أو المصرح به بموجب الاتفاقية الاختراق الذي يحدث للنظام بأكمله أو لجزء منه أياً كان، إذا يستوي أن جزءاً مادياً أو برامج جزئية أو بيانات مخزنة في النظام المعلوماتي أو ملفات أو بيانات تتعلق بالمرور والمحتوى الحاسوبي، ويعد أيضاً دخولاً غير مشروع الاختراق الذي يحدث لنظام معلوماتي متصل بشبكات اتصال عامة أو لنظام معلوماتي متصل بنفس الشبكة أو بأي شبكة محلية أو إنترنت أو بأي شبكة خاصة للشركة وفي كل الحالات فإن طريق الاتصال سواء أكانت عن بعد بما في ذلك الاتصال اللاسلكي، أم كانت على نطاق قريب لا تدخل في الاعتبار [1].

وقد اشترطت المذكرة التفسيرية لاتفاقية بودابست أن يحدث فعل الاختراق أو الدخول غير المشروع دون حق يعني أنه لا عقاب في حال الدخول المصرح به من مالك النظام أو مالك جزء منه أو صاحب الحق فيه كما يحدث

---

[1] Explanatry note in English of the 2001. European convention on Virtual crime.

في حالة الاختبار أو الحماية المصرح بها للنظام محل الشأن كذلك لا يكون هناك تجريم في حالة ما إذا كان الدخول إلى النظام بالمجان ومتاحاً للجميع ففي مثل تلك الحالة يصبح الدخول إلى النظام حقاً من الحقوق .

وقد أشارت المذكرة التفسيرية للاتفاقية إلى أن العديد من التشريعات الداخلية سبق وأن تضمنت نصوصاً تتعلق بالجرائم المرتبطة بالقرصنة لكن نطاقها والعناصر المكونة لها متنوعة أو متباينة للغاية، كما أن المدخل العام للعقاب في العبارة الأولى من المادة الثانية من الاتفاقية لا يخلو من اختلاف وعادة ما ينشأ الخلاف من المواقف التي لا يترتب على مجرد التدخل فيها مخاطر أو حينما تؤدي أفعال القرصنة إلى اكتشاف تصدعات أو نقاط ضعف في أمن النظم .

كما جاء في المادة الثالثة من الاتفاقية أنه يتوجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقاً لقانونها الداخلي، واقعة الاعتراض غير المشروع ودون حق من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب في مكان الوصول، أو في داخل النظام المعلوماتي، بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية (بقصد الغش) وأن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحساب أخر [1].

وقد جاء في المذكرة التفسيرية أن الهدف من نص المادة الثالثة هو حماية الحق في احترام نقل البيانات وأن هذه الجريمة تمثل انتهاك للحق في احترام الاتصالات مثل التنصت والتسجيل التقليدي للمحادثات التليفونية بين

---

[1] راجع المادة الثالثة من اتفاقية بودابست لمكافحة جرائم الإنترنت لعام ٢٠٠١ .

الأشخاص، كما أن الحق في احترام المراسلات مكفول عن طريق المادة الثامنة من الاتفاقية الأوربية لحقوق الإنسان، والمادة الثالثة من اتفاقية بودابست تطبق هذا المبدأ على كل أشكال النقل الالكتروني للبيانات سواء تم هذا النقل عن طريق التليفون أو الفاكس أو البريد الالكتروني .

كما أشارت المذكرة الإيضاحية للاتفاقية إلى المصدر الذي أخذت عنه المادة الثالثة بأن نص هذه المادة اشتق بشكل أساسي من جريمة الاعتراض غير المصرح به المنصوص عليها في التوصية رقم (٩/٨٩) ، وفي الاتفاقية الحالية تم توضيح أن مفهوم الاتصالات يمتد ليشمل وسائل نقل بيانات الحاسب، وكذلك انبعاثات الإشعاعات الكهرومغناطيسية ويتم الاعتراض باستخدام وسائل فنية تتعلق بالتنصت أو التحكم أو مراقبة محتوى الاتصال والحصول على المحتوى بطريقة مباشرة من خلال طريقة الدخول إلى داخل النظام المعلوماتي واستخدامه، أو بشكل غير مباشرة عن طريق استخدام أجهزة التنصت، كذلك يمكن أن تشتمل وسائل الاعتراض على تسجيل البيانات، وكذلك نطاق الوسائل الفنية يجب أن يمتد ليشمل الأجهزة الفنية المتصلة بخطوط النقل أو الاتصال مثل أجهزة تجميع وتسجيل الاتصالات اللاسلكية، كما يمكن أن يشمل الكيانات المنطقية وكلمات المرور والشفرات. ومن الجدير بالذكر أن اشتراط استخدام وسائل فنية يعد شرطاً مقيد لتجنب عقبة العقاب المبالغ فيه .

وجريمة الاعتراض غير المشروع تنطبق على وسائل النقل غير العلنية للبيانات الحاسب وأن مصطلح غير العلنية صفة تتبع طبيعة وسائل النقل والاتصال، وليس طبيعة البيانات المرسلة فالبيانات المرسلة من الممكن أن تكون مهيأة لكل الناس لكن هم يرغبون بنقلها أو إرسالها بطريقة سرية، حيث يمكن الاحتفاظ بالبيانات بطريقة سرية لأغراض تجارية حتى يتم دفع مقابل للخدمة، كما في حال التيلفون بالاشتراك، وعلى ذلك فإن مصطلح غير العلنية لا يستبعد

الاتصالات في حد ذاتها عبر الشبكات العامة، فاتصالات العاملين سواء أكان لأغراض العمل أم لا، والتي تشمل وسائل النقل غير العلنية لبيانات الحاسب وهي أيضاً محمية ضد الاعتراض غير المشروع بمقتضى المادة الثالثة من الاتفاقية [١].

وقد نصت المادة الرابعة من الاتفاقية على جريمة التدخل أو التشويش على البيانات ((١-يجب على كل عضو أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم ، تبعاً لتشريعية الداخلي، إذا حدث ذلك عمداً ، ودون حق، أي أضراراً، أو محو، أو تعطيل، أو إتلاف ، أو طمس لبيانات الحاسب .

٢- يمكن لأي طرف أن يحتفظ بحق اشتراط أن يكون السلوك المنصوص عليه في الفقرة الأولى يؤدي إلى أضرار جسيمة)) [٢].

ووفقاً لما جاء في المذكرة التفسيرية إن الهدف من تقرير هذا النص هو أن تكون البيانات وبرامج الحاسب مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمداً، والمصالح القانونية المحمية بهذه المادة هي سلامة وحسن تشغيل أو حسن استخدام البيانات أو برامج الحاسب المسجلة .

ونلاحظ بأنه قد ورد بالفقرة الأولى من المادة الرابعة مصطلح الإضرار، ومصطلح التعطيل، وهي من الأفعال المرتكبة التي تتصل على وجه الخصوص بالإتلاف لمحتوى البيانات والبرامج من معلومات، كما ورد بالفقرة أيضاً مصطلح محو البيانات، وهذا المصطلح يعادل مصطلح تدمير الأشياء في

---

[١] المذكرة التفسيرية لاتفاقية بودابست لعام ٢٠٠١ .

[٢] انظر المادة (١) /٣ من ميثاق الأمم المتحدة .

مجال تدمير الأشياء المادية، فهو يهدمها ويجعلها في حالة لا يمكن التعرف عليها، واستخدم النص مصطلح طمس البيانات المعلوماتية، وهذا المصطلح يمتد ليشمل كل تصرف من شأنه أن يجعل هذه البيانات غير موجودة أو غير متاحة للشخص الذي له الحق الدخول إلى داخل الحاسب أو الاعتماد على تلك البيانات التي كانت مخزنة، واستخدم النص مصطلح الإتلاف يعني تغيير البيانات الموجودة، وكذلك إدخال شيفرات عدوانية، مثال ذلك الفيروسات أو حصان طروادة ، والتي من شأنها تغيير البيانات التي تنتج عن هذا التصرف .

وقد أعطت الاتفاقية للدول الأعضاء الحق في اشتراط أن يترتب على السلوك الإجرامي وفقاً للمادة الرابعة ضرر جسيم ، وتفسير الضرر الجسيم يخضع للتشريع الوطني للدولة العضو في الاتفاقية .

ونلاحظ بأن الاتفاقية لم تحدد نوع معين من المعلومات والبيانات التي يحميها النص القانوني إذ أن كل الأنواع من المعلومات تكون محمية بالنص القانوني سواء في ذلك المؤمنة منها أو غير المأمنة وذلك لأن القصد هو حماية سلامة وإتاحة المعلومات للجميع أثناء تعاملاتهم الالكترونية ونصت المادة الخامسة من الاتفاقية على جريمة إتلاف أو تعديل نظام الحاسب ((يجب على كل عضو أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية لتجريم ، تبعاً لتشريعين الداخلي، الإعاقة الخطيرة، إذا حدث ذلك عمداً ، ودون حق، لوظيفة نظام الحاسب، عن طريق إدخال، أو نقل، أو الإضرار ، أو محو ، أو تعطيل ، أو إتلاف ، أو طمس البيانات المعلوماتية)) [1].

[1] انظر المادة الخامسة في اتفاقية بودابست .

ووفقاً لما جاء في المذكرة التفسيرية [1]. أن التوصية رقم ٩٨/٩ أشارت إلى هذا العنوان تحت مسمى تخريب نظام الحاسب، ويهدف هذا النص إلى تجريم الإعاقة العمدية للاستخدام أو التأثير على بيانات الحاسب والمصالح القانونية المحمية هي مصلحة مشغلي، ومستخدمي نظام الحاسب، أو نظام الاتصالات في القيام بأعماله بدقة وحماية جميع أنواع الوظائف ومصطلح الإعاقة يرتبط بالأفعال التي تمثل اعتداء على حسن تشغيل النظام، وهذه الإعاقة يجب أن تكون ناجمة عن الإدخال، أو النقل، أو الإضرار ، أو محو ، أو الإتلاف، أو طمس البيانات المعلوماتية، ويجب أن تكون الإعاقة جسيمة حتى يترتب عليها جزاء جنائياً، ويجب على كل دولة أن تحدد الشروط الواجب توافرها حتى تتحقق الإعاقة المجرمة بنص القانون.

وتعتبر الإعاقة جسيمة وفقاً للاتفاقية عندما تكون البيانات المرسلة من الحجم أو التواتر بما يحمل ضرراً جسيماً لقدرة المالك أو المشغل بالنسبة لاستخدام الجهاز أو الاتصال بالأجهزة الأخرى، كالفيروسات التي تمنع أو تبطئ بشكل ملموس عمل الجهاز أو البرامج التي ترسل مقداراً هائلاً من البريد الالكتروني إلى مرسل إليه من أجل شل وظائف اتصال نظام الحاسب.

وفي جميع الحالات يجب أن تكون الإعاقة دون حق فالأنشطة الشائعة المتضمنة في تصميم الشبكات، أو الممارسات الخاصة بالتشغيل أو التجارة ، كل ذلك يكون بحق، إذ أن الأمر يتعلق على وجه الخصوص، بأنشطة اختبار أمن

---

[1] انظر Pem laa jimene 2 : 'international securithies en for emcnet cooperation Act and Memora of understanding , In harvard intirational law journal , winter 1990 , vol , 31 , No, Harvard law school, cambrige , massachustts, p.295-311 .

نظام الحاسب أو حماية النظام والمصرح بها من قبل المالك للنظام أو القائم على تشغيله، أو عند إعادة تنظيم نظام التشغيل للحاسب، والذي يحدث عندما يقتني مشغل النظام كياناً منطقياً جديداً، كما في حالة تشغيل كيانات منطقية للدخول عبر الإنترنت ، كل تلك الأنشطة تعتبر شرعية ، وبالتالي لا يتم العقاب عليها بواسطة هذه المادة .

وفيما يتعلق بإرسال رسائل الكترونية لأغراض تجارية أو لأغراض أخرى لمرسل إليه لم يطلب استقبالها، وتسبب له مضايقات ، وبالأخص تلك الرسائل التي يتم إرسالها غالباً وبكميات ضخمة وكبيرة، كما هو الحال في تجارة البريد الالكتروني .

ومع ذلك يكون للدول الأعضاء الحق في اعتبار بعض أنواع التداخلات ضمن مفهوم الإعاقة وفق قانونهم الوطني والمعاقبة عليها إدارياً أو إعطائها جزاء بطريقة أخرى، ويترك النص للدول تحديد في أي الأحوال يعد النظام قد تمت إعاقته عن العمل جزئياً أو كلياً وفق قانونهم الوطني وتحديد تلك الحالات التي يكون فيها العقاب إدارياً وتلك التي يكون فيها العقاب جنائياً بشرط أن يكون الفعل قد تم بطريق العمد وبأن تكون لدى الجاني نية إحداث الإعاقة الجسيمة.

كما نصت الاتفاقية في المادة السادسة منها على إساءة استخدام الحاسب لتعديل المعلومات وإتلافها، وأشارت في المادة السابعة من الاتفاقية إلى جرائم التزوير المرتبطة في الحاسوب.

أما في المادة الثامنة من الاتفاقية والتي جاءت بعنوان (الاحتيال المرتبط بالحاسوب) فقد اعتبرت هذه المادة أن جريمة الاحتيال تقع (عندما يقوم شخص عند قصد، وبدون وجه حق، وعلى نحو يسبب خسارة في ممتلكات الغير بمايلي:

أ) أي إدخال أو تعديل أو حذف أو كتم لبيانات الحاسوب.

ب) أي تدخل في وظائف نظام الحاسوب.

وبنية احتيالية أو غير شريفة بغرض الحصول دون وجه حق على منفعة اقتصادية لنفسه أو لغيره) [١].

وحسب ما جاء في المذكرة التفسيرية لهذه الاتفاقية ، فإن هذا النص يغطي جميع أشكال الاحتيال المرتبط بالحاسوب.

ويشترط لتطبيق هذا النص أن يرتكب الجاني أحد الأفعال المذكورة في الفقرتين /أ–ب/ دون وجه حق، وأن تلحق خسارة اقتصادية في ملكية الغير، وأن يحصل الجاني لنفسه أو لغيره على منفعة اقتصادية نتيجة ارتكابه لهذه الجريمة [٢].

وقد نصت الاتفاقية على الأحكام الإجرائية الواجب على الدول الموقعة إتباعها عند وضع قوانينها الخاصة بمكافحة الجرائم الالكترونية بالمواد من (١٤ حتى ٢١) من الاتفاقية الأوربية، وقد تضمنت هذه المواد إلزام كل طرف في هذه الاتفاقية بتهيئة تشريعاته الداخلية لتقرير وتحديد السلطات والإجراءات اللازمة في مجال التحقيق بالجرائم المنصوص عليها في الاتفاقية كما الزمت هذه الاتفاقية الدول الأطراف عند سن تشريعها الداخلي أن تراعي الاتفاقيات الدولية لحقوق الإنسان، مثل : الاتفاقية الأوربية لحماية حقوق الإنسان والحريات

---

[١] انظر المادة /٨/ من الاتفاقية الأوربية لمكافحة جرائم الإنترنت بودابست .

[٢] د. عمر بن يونس، الاتفاقية الأوربية حول الجريمة الافتراضية (المذكرة التفسيرية) ، الطبعة الثانية، مؤسسة آدم للنشر والتوزيع – مالطا ، عام ٢٠٠٨ ص ٨٩– ٩٠ .

الأساسية لعام ١٩٥٠ ، والميثاق الدولي حول الحقوق المدنية والسياسية لعام ١٩٦٦[١].

وقد أشارت المادة /١٩/ من الاتفاقية ، على ضرورة أن يكون هناك نصوص تشريعية داخلية لدى الدول الأطراف تسمح بما يلي:

- تفتيش نظام الحاسوب أو جزء منه والبيانات المخزنة فيه .
- تفتيش معالج تخزين البيانات في الحاسوب الذي يحوي على بيانات معينة.

وتسمح الفقرتين /٢-٣/ من المادة /١٩/ بمد التفتيش إلى نظام حاسوب أخر أو جزء منه، إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المطلوبة قد تم تخزينها في نظام الحاسوب الأخر، ويشترط أن يكون هذا الحاسوب ضمن النطاق الإقليمي، وتسمح بضبط القطع الصلبة للحاسوب ووسيط التخزين، مع اتخاذ الإجراءات اللازمة للمحافظة على سلامة هذه البيانات [٢].

كما أشارت المادة /٢٠/ من الاتفاقية إلى ضرورة اتخاذ إجراءات تشريعية لإلزام فردي الخدمة بمساعدة الجهات المختصة لمعرفة حركة البيانات وتجميعها [٣].

أما المادة /٢١/ فقد أشارت إلى إمكانية مراقبة محتوى البيانات أثناء عملية التراسل ، وذلك من أجل تجميع الدليل ذي الطبيعة الجنائية [٤].

---

[١] د. عمر بن يونس، الاتفاقية الأوربية حول الجريمة الافتراضية، المرجع السابق ص ١١٣ و ١٢٠.

[٢] المرجع السابق ، ص١٥٤-١٥٦

[٣] المرجع السابق، ص ١٦٩ .

[٤] المرجع السابق، ص ١٧٨ .

وقد أشارت المادة /٢٢/ من الاتفاقية إلى مسألة الاختصاص والمعايير التي يجب على الدول الأطراف اعتمادها لتقرير الاختصاص القضائي حول الجرائم المقررة في هذه الاتفاقية والتي تم الإشارة إليها سابقاً ومعايير الاختصاص التي أخذت بها هذه الاتفاقية هي[١]:

١- مبدأ الإقليمية .

٢- مبدأ نسبية الاختصاص المكاني، أو ما يعرف بالإقليم الاعتباري، أي الجرائم المرتكبة على السفن التي ترفع علم الدولة أو الطائرات المسجلة وفقاً للقانون فيها.

٣- مبدأ الجنسية .

ولابد من الإشارة إلى الخلاف الوحيد الذي قام بين الدول الموقعة على الاتفاقية خلال فترة المفاوضات هو مجال محاربة العنصرية، حيث أن الدول الأوربية اعتبرت أن التحريض على الكراهية العنصرية هي جريمة بحد ذاتها. ومن المعلوم أن هذه الجريمة يعاقب عليها القانون الدولي. فشجعت الدول الأوربية على أن تنص الاتفاقية على لزوم إزالة المواقع التي تدعو إلى أفكار التحريض على الكراهية العنصرية وملاحقة القائمين على هذه المواقع باعتبارهم يرتكبون جريمة يعاقب عليه القانون الدولي، بينما الولايات المتحدة الأمريكية تختلف بوجهة نظرها مع الدول الأوربية فهي ترى عدم الحاجة إلى ضرورة أن تحتوي الاتفاقية على مواد لإزالة المواقع التي تدعو إلى التحريض العنصري على أساس أن الدستور الأمريكي لا يعتبر مثل هذه المواقع جريمة يعاقب عليه القانون بل أنها تعبير عن الرأي، وهو ما يكفله الدستور الأمريكي. وسعياً من الدول الموقعة على الاتفاقية في تقليل حدة الخلافات فيما بين الدول المتفاوضة

[١] د. عمر بن يونس: الاتفاقية الأوربية حول جريمة الافتراضية، المرجع السابق ، ص ١٨١-١٨٥.

تم الاتفاق على عدم تضمين الاتفاقية ذلك الموضوع، وذلك بشرط أن يتم دراسة الأمر من كافة الجوانب لاحقاً والوصول إلى نقطة اتفاق يوافق عليها جميع الأطراف[1].

وهكذا نجد بأن الدول بمفردها لا تستطيع مواجهة تلك الجرائم التي ترتكب عبر الإنترنت مهما سنت من قوانين داخلية نظراً لكون تلك الجرائم ذات طبيعة خاصة فهي جرائم دولية (عابرة للحدود) لا يقف أمامها أي عائق جغرافي وبالتالي فإن هذه الدول يفضل الانضمام إلى المعاهدات والاتفاقيات الدولية التي تبرم في مجال مكافحة الجرائم الالكترونية نظراً لكبر حجم الأضرار والخسائر التي تصيبها المادية والمعنوية منها ولأن العديد من الدول حتى المتقدمة منها عاجزة عن مواجهتها بمفردها دون وجود تعاون وتضامن دولي في سبيل مكافحتها .

المطلب الثاني: الاتفاقيات العربية حول مكافحة الجرائم الالكترونية .

حاولت الدول العربية مواكبة التطور في مجال مكافحة الجرائم الالكترونية وسعت لتعزيز التعاون بين الدول العربية حفاظاً منها على أمنها ومصالحها واقتناعاً منها بضرورة الحاجة إلى وجود سياسة مشتركة لمواجهة هذا الخطر الذي يتهدد كافة المجتمعات فقد أثمرت الجهود العربية إلى إيجاد القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية المعلومات وما في حكمها والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٢ والتي سنتناول كل منهما في الفرعين التالين :

---

[1] م. منير محمد الجنيهي، وممدوح محمد الجنيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، مرجع سابق، ص١٨٣ .

أولاً- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها [1]:

صدر القانون العربي النموذجي أو الاسترشادي في شأن مكافحة جرائم تقنية المعلومات كثمرة عمل مشترك بين مجلس الوزراء الداخلية العرب ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية، بعد أن تبين أن كليهما قدم مشروعاً في هذا الخصوص وتم اجتماعهما المشترك في ٢١-٢٠٠٣/٥/٢٢ حيث تم النظر في المشروعين اللذين تم إعدادهما في نطاق المجلسين .

وقد سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة. حيث تم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم (٤٩٥-١٩٥-٢٠٠٣/١٠/٨) ، كما اعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (٤١٧، د ٢٠٠٤/٢١) .

ويتكون هذا القانون من /٢٧/ مادة، وهي على النحو التالي:

المادة الأولى حيث تناولت تعريف عدة مفاهيم، كالبيانات والبرنامج المعلوماتي والنظام المعلوماتي والشبكة المعلوماتية والموقع والالتقاط حيث

[1] تم إعداد هذا القانون الاسترشادي من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لمؤتمر وزراء الداخلية العرب في نطاق الأمانة العامة لجامعة الدول العربية وتم إقراره عام ٢٠٠٣ هذا القانون متوفر على موقع جامعة الدول العربية www.arableagueonline.org

عرفت البيانات بأنها ((كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الألي، كالأرقام والحروف والرموز وما إليها...)).

نجد بأن المادة الأولى قد جعلت مفهوم البيانات مفتوحاً وشاملاً حيث ختمت التعريف بكلمة (وما إليها .. محاولة منها لجعل نطاق العبارة واسعاً شاملاً نوعاً ما).

وقد عرف القانون البرنامج المعلوماتي بأنه ((مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام الحاسب الألي ومعدة لإنجاز مهمة ما)).

كما عرف النظام المعلوماتي في محاولة من القانون للتمييز بين البرنامج والنظام بأنه ((مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات)) .

أما الشبكة المعلوماتية فهي ((ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها)).

كما تعرف المادة الأولى الموقع بأنه ((مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد)).

أما الالتقاط فهو ((مشاهدة البيانات أو المعلومات أو الحصول عليها)).

نلاحظ بأن القانون قد حدد بشكل واضح معاني المصطلحات والكلمات في المادة الأولى منعاً للغموض والوقوع في الاختلاف حول المقصود من المفاهيم والمعاني المستخدمة في نصوص المواد .

أما المادة الثانية فقد جاءت مشددة للعقوبة على ارتكاب جرائم الانترنت حيث أشارت إلى عدم الإخلال بالعقوبة الأشد في حال وجود نص عقابي أخـــر يعاقب على الأفعال المجرمة في هذا القانون .

وقد حدد هذا القانون الجرائم المعاقب عليها في المواد من (٣ إلى ٢٢) وهي على النحو التالي:

المادة الثالثة نصت على جريمة الدخول بغير حق إلى موقـــع أو نظـــام معلوماتي، مع تشديد العقوبة إذا كان الدخول بقصد إلغاء أو إتلاف أو إعادة نشر بيانات أو معلومات شخصية.

أما المادة الرابعة فقد نصت على جرمية تزوير المستندات المعالجة في نظام معلوماتي أو استعمال السند المعالج المزور .

حيث نصت المادة على ((كل من ارتكب تزويراً في أحد المستندات المعالجة في نظام معلوماتي يعاقب بالحبس مدة لا تقل عن ... ويعاقب بذات العقوبة كل من استعمل المستند المزور مع علمه بالتزوير)).

نلاحظ بأن القانون العربي الاسترشادي قد ساوى فـــي العقوبـــة بـــين تزويـــر المستندات المعالجة في نظام معلوماتي، وجريمة استعمال المستند المزور بشرط علمه بالتزوير .

وقد نصت المادة الخامسة من القانون على الظـــروف المشـــددة علـــى جريمة الدخول بغير حق إلى موقع أو نظام معلوماتي المنصوص عليهـــا فـــي المادة الثالث من نص القانون.

وقد عاقبت المادة السادسة من القانون كل من أدخل عن طريق الشـــبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، أي شيء مـــن شـــأنه

إيقاف عمل الحاسب أو تعطيله، وقد قصد القانون (الفيروسات) وقد عاقب على مجرد القيام بعملية الإدخال دون تحقق الغرض، وقد جعل العقوبة مشددة في حال تحقق الغاية من الإدخال .

أما المادة السابعة من القانون فقد عاقبت على التشويش أو الإعاقة أو التعطيل عمداً وبأية وسيلة الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات .

بينما المادة الثامنة من القانون فقد عاقبت كل من تنصت أو اعترض أو التقط بدون وجه حق ما هو مرسل عن طريق الشبكة المعلوماتية .

نلاحظ بأن المشرع قد جاء بمفهوم جديد بموجب هذه المادة وهو مصطلح الالتقاط حيث عرفت المادة الأولى هذا المفهوم ((الالتقاط : مشاهدة البيانات أو المعلومات أو الحصول عليها)) .

أما المادة التاسعة فقد أشارت إلى جريمة التهديد والابتزاز عن طريق الشبكة المعلوماتية.

وقد عاقبت المادة العاشرة على جريمة الاحتيال عبر استخدام الشبكة المعلوماتية أو أحد أجهزة الحاسب الألي، أو اتخاذ أي أسلوب من شأنه خداع المجنى عليه .

وقد أشارت المادة الحادية عشرة من القانون على جريمة الحصول بدون وجه حق على أرقام وبيانات بطاقة الائتمان .

بينما المادة الثانية عشرة فقد عاقبت على جريمة الانتفاع بدون وجه حق بخدمات الاتصالات.

ونصت المادة الثالثة عشرة على الجرائم المخلة بالأداب العامة والمخالفة للنظام العام التي تتم عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي .

بينما المواد (١٤ إلى ٢٢) فقد عاقبت على الجرائم المتعلقة بحماية حقوق الملكية الفكرية، والجرائم المتعلقة بالاعتداء على تصاميم المواقع، وجرائم الاعتداء على المبادئ الدينية أو حرمة الحياة الخاصة، وجرائم الاتجار بالجنس البشري والجرائم المتعلقة بالإتجار وترويج وتعاطي المخدرات أو المؤشرات العقلية، وجرائم غسيل الأموال، والجرائم المتعلقة بتسهيل وترويج البرامج والأفكار المخالفة للنظام العام، والجرائم المتعلقة بإنشاء المواقع العائدة للجماعات الإرهابية والترويج لأفكارها، وجرائم الحصول على معلومات تمس الأمن، الأمن الداخلي أو الخارجي أو الاقتصاد الوطني .

وقد نصت المواد (٢٣ إلى المادة ٢٧) على الأحكام العامة الواجب تطبيقها على ارتكاب الجرائم المنصوص عليه بموجب هذا القانون .

حيث نصت المادة الثالثة والعشرون على عقوبة المحرض أو المساعد أو المتفق مع الغير على ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون.

أما المادة الرابعة والعشرون فقد عاقبت على الشروع في الجرائم المنصوص عليها.

أما المادة الخامسة والعشرون فقد حددت التدابير الاحترازية الواجب اتباعها والإجراءات الواجب القيام بها من أجل التعامل مع الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون، وهي مصادرة هذه الأجهزة والوسائل مع عدم الإخلال بحقوق الغير حسني النية .

أما المادة السادسة والعشرون وتتعلق بالاختصاص ، حيث نص القانون على مايلي: ((تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه حتى ولو ارتكبت كلياً أو جزئياً خارج إقليم الدولة، متى أضرت بأحد مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة عليها)) .

نلاحظ بأن القانون قد عالج موضوع الاختصاص بمعيار المصلحة المعتدى عليها فجعل اختصاص الدولة قائماً حتى أضرت الجريمة المرتكبة بمصلحة الدولة، ويقوم اختصاصها حتى لو ارتكبت هذه الجريمة كلياً أو جزئياً خارج إقليم الدولة .

أما المادة السابعة والعشرون فقد تضمنت وجوب إبعاد الأجنبي المحكوم عليه وفقاً للمواد (١٦وحتى ٢٢) ولابد من الإشارة بأن هذا القانون قد وضع القواعد الأساسية التي تعيين على المشرع العربي اللجوء إليها عند سن قانون وطني لمكافحة هذه الجرائم سواء أكان القانون الوطني مستقلاً لمكافحة هذه الجرائم المستحدثة أم كان تعديلاً لقانون العقوبات المطبق بالفعل في أي دولة عربية .

وقد أشار هذا القانون لأنواع الجرائم التي تقع على الكمبيوتر والانترنت بصفة عامة ومحدداً عقوبتها وأحال إلى التشريع الوطني كل ما يتعلق بأركان هذه الجرائم وكذلك العقوبات التي تطبق عليها .

وأخيراً نجد بأن القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، كان موفقاً إلى حد ما فيما يتعلق بوضع مصطلحات ومفاهيم شاملة نوعاً ما إلى كافة الجرائم المعلوماتية التي يمكن أن ترتكب عن طريق الحاسوب أو عبر الانترنت، إلا أنه يؤخذ عليه أنه أغفل عرض سبل

المكافحة والوسائل اللازمة للتعاون بين الدول العربية من أجل الحد من هذا الخطر الذي يتهدد المجتمعات العربية .

ثانياً- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات [1]:

رغبة من الدول العربية في تعزيز التعاون فيما بينها لمكافحة الجرائم الالكترونية التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات .

قامت الدول العربية بعقد هذه الاتفاقية بمدينة القاهرة بتاريخ ٢٠١٠/١٢/٢١ وتم إيداعها في الأمانة العامة لجامعة الدول العربية .

وتتألف هذه الاتفاقية من (٤٣) مادة وخمس فصول حيث يتناول الفصل الأول أحكام عامة حول جرائم الانترنت .

أما الفصل الثاني فيتناول الأفعال التي تستوجب التجريم بينما يحتوي الفصل الثالث على الأحكام الإجرائية .

أما الفصل الرابع فيتناول التعاون القانوني والقضائي في سبيل مكافحة الجرائم الالكترونية.

أما الفصل الخامس فيحتوي على الأحكام الختامية وسنتناول هذه الفصول بشيء من التفصيل:

تناولت المادة الأولى من الاتفاقية الهدف منها حيث نصت: ((تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم

---

[1] الاتفاقية موجودة على الموقع الالكتروني: www.lawjo.net26439-2012

تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها)).

أما المادة الثانية من الاتفاقية فقد بينت المقصود من المصطلحات، والمفاهيم الواردة بمضمون الاتفاقية ومن هذه المصطلحات :

١- " **تقنية المعلومات:** أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكية أو لاسلكياً في نظام أو شبكة .

٢- **مزود الخدمة:** أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها .

٣- **البيانات :** كل ما يمكن تخزين ومعالجة وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها ....إلخ" [١].

وقد أشارت المادة الثالثة إلى مجالات تطبيق الاتفاقية حيث تنطبق على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها وذلك في الحالات الآتية:

١- ارتكبت في أكثر من دولة.

---

[١] المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

٢- ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى .

٣- ارتكبت في دولة وظلت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.

٤- ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى [١].

أما المادة الرابعة من الاتفاقية فقد أكدت على صون مبدأ السيادة حيث يتم تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى .

حدد الفصل الثاني من الاتفاقية الأفعال التي يتوجب على الدول الأطراف تجريمها وفقاً لتشريعاتها وأنظمتها الداخلية .

فقد نصت المادة السادسة على جريمة الدخول غير المشروع وعاقبت على كل محو أو تعديل أو تدمير لبيانات محفوظة على الأجهزة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين، بالإضافة إلى الحصول على معلومات حكومية سرية .

أما المادة السابعة فقد أشارت إلى جريمة الاعتراض غير المشروع حيث نصت : ((الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات))[٢].

بينما المادة الثامنة فقد عاقبت على جريمة الاعتداء على سلامة البيانات سواء بالتدمير أو محو أو إعاقة أو تعديلها أو حجب البيانات بدون وجه حق .

---

[١] المادة الثالثة من الاتفاقية .

[٢] المادة السابعة من الاتفاقية .

أما المادة التاسعة فتجرم إساءة استخدام وسائل تقنية المعلومات، حيث تعتبر الاتفاقية أن "إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة" [1].

نجد بأن هذا التجريم واسع جداً، ويمكن أن يشمل العديد من التطبيقات والبرمجيات التي يتم استخدامها في اختبارات أمن وحماية الشبكات والبرمجيات والأنظمة المعلوماتية وتستخدم بالأساس لكشف الثغرات الأمنية للأنظمة وشبكات الاتصالات والبرمجيات .

وقد أشارت كل من المادتين العاشرة والحادية عشر إلى جرائم التزوير والاحتيال ، وقد عاقبت على كل فعل من شأنه إلحاق الضرر بوسائل، وبيانات تقنية المعلومات.

أما المادة الثانية عشر تتناول "جريمة الإباحية" حيث تشدد المادة العقوبة في الجرائم المتعلقة بإباحية الأطفال والقصر ويشمل هذا التشديد حيازة مواد إباحية الأطفال والقصر أو مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات، ورغم أهمية هذه المادة وتناسبها مع الأعراف الإنسانية، إلا أنها تترك الباب مفتوحاً أمام الحكومات العربية لتفسيرها طبقاً لمعايير غير معروفة وليس محددة في الإنقاص .

حيث ينص البند الأول من المادة على تجريم (إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات) [2]، ولا يوجد أي تعريف واضح لماهية المواد "المخلة

---

[1] المادة التاسعة من الاتفاقية .

[2] المادة الثانية عشرة من الاتفاقية .

بالحياء" وعليه فإنه يمكن استخدامها فعلياً لتجريم العديد من أنـــواع المحتـــوى المنشور على الانترنت سواء كانت نصوصاً أدبية أو أعمال فنيـــة أو أي مـــن أنشطة النشر على الرقمي.

أما المواد الثالثة عشرة والرابعة عشرة فقد أشارت إلى الجرائم الأخرى المرتبطة بالإباحية كالمقامرة والاستغلال الجنسي، وجريمة الاعتداء على حرمة الحياة الخاصة .

بينما المادة الخامسة عشرة تتناول الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، وتنص في الفقرة الرابعة منها على تجـــريم "نشـــر النعـــرات والفتن والاعتداء على الأديان والمعتقدات" [١].

ولكن يؤخذ على هذه المادة أنه يمكن استخدامها لتجريم أي رأي أو تعبيـــر يمكن أن يشكل اختلافاً مع المعتقدات الدينية والاجتماعية السائدة، وقد أشـــارت المادة السادسة عشرة إلى تجريم الأفعال المتعلقة بالجرائم المنظمـــة والمرتكبـــة بواسطة تقنية المعلومات ومن هذه الأفعال:

١- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيـــام بغسل الأموال.

٢- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها .

٣- الاتجار بالأشخاص .

٤- الاتجار بالأعضاء البشرية .

٥- الاتجار غير المشروع بالأسلحة .

---

[١] فقرة (٤) من المادة الخامسة عشرة من الاتفاقية .

وقد نصت كل من المادتين السابعة عشرة والثامنة عشرة على الجرائم المتعلقة بانتهاء حق المؤلف والحقوق المجاورة، وجريمة الاستخدام غير المشروع لأدوات الدفع الالكترونية.

أما المادة التاسعة عشرة من الاتفاقية فقد نصت على تجريم الشروع والاشتراك في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية، ولا بد من الإشارة أن هذه المادة قد تركت للأطراف حرية الاحتفاظ بحقهم في عدم تطبيق تجريم الشروع على الجرائم المنصوص عليها في الاتفاقية كلياً أو جزئياً .

وقد أشارت المادة العشرون إلى المسؤولية الجنائية للأشخاص الطبيعية والمعنوية حيث نصت المادة :

"تلتزم كل دولة طرف مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بغرض العقوبة على الشخص الذي يرتكب الجريمة شخصياً" [1].

نجد بأن الاتفاقية قد ساوت في المسؤولية بين الشركات والمؤسسات التي تمتلك الشخصية المعنوية وبين المسؤولية الجزائية للأشخاص الذين يقومون بإدارتها .

أما المادة الحادية والعشرون تشدد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات، حيث ألزمت هذه الاتفاقية الدول الأطراف على تشديد العقوبة على الجرائم التقليدية المرتكبة عن طريق الانترنت أو الحاسوب.

---

[1] المادة العشرون من الاتفاقية.

ينص الفصل الثالث من الاتفاقية على الأحكام الإجرائية التي يتوجب على الدول الأطراف الالتزام بها من خلال قوانينها الداخلية وتشريعاتها واتخاذ كافة الإجراءات الضرورية اللازمة من الاتفاقية لتطبيق هذه الأحكام الإجرائية وهذا ما أكدت عليه المادة الثانية والعشرون .

أما المادة الثالثة والعشرون من الاتفاقية تلزم كل دولة بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر، أو الحصول على الحفظ العاجل للمعلومات المخزنة لمدة أقصاها ٩٠ يوماً قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي.

أما المادتين الرابعة والعشرون والخامسة والعشرون فتلزم الدول الأطراف باتخاذ الإجراءات الضرورية فيما يتعلق بالتحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين، بالإضافة إلى أمر تسليم المعلومات معينة في حيازة شخص على إقليم دولة إلى الدولة الطالبة للمعلومات.

وقد أكدت المادتين السادسة والعشرون والسابعة والعشرون على واجب الدول الأطراف الاتخاذ الإجراءات الضرورية لضبط وتفتيش المعلومات المخزنة من قبل الجهات المختصة في الدولة المعنية.

حيث نص الفقرة الثانية في المادة السابعة والعشرون أن كل دولة يجب أن تبين (الإجراءات الضرورية) لتمكين السلطات المختصة من إصدار الأوامر إلى "أي شخص لديه معرفة بوظيفة تقنية المعلومات" لتقديم المعلومات الضرورية لإتمام إجراءات نسخ معلومات تقنية المعلومات والاحتفاظ بها والحفاظ على سلامتها وإزالة أو منع الوصول لها، مما يعني أن المادة تجيز للسلطات المختصة الاستعانة بعناصر من خارج القطاعات الحكومية .

وقد تناولت المادة الثامنة والعشرون الجمع الفوري للمعلومات تبين المستخدمين وتلتزم الدول بتبني الإجراءات الضرورية" لتمكن السلطات المختصة من جمع أو تسجيل المعلومات، وتعطي للحكومات إمكانية "تبني إجراءات أخرى بالشكل الضروري لضمان الجمع، أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية.

أما المادة التاسعة والعشرون فتوسع في إجازة تبني إجراءات الضرورية لجمع وتسجيل المعلومات، إذا لم تستطيع الدولة الطرف بسبب نظامها القانوني الداخلي من اتخاذ إجراءات الجمع والتسجيل للمعلومات، المُعترضة، وأشارت المادة لهذه الإجراءات بجملة "تبين إجراءات أخرى" .

ينظم الفصل الرابع من الاتفاقية التعاون القانوني والقضائي بين الدول الأطراف، حيث تلزم المادة ثلاثون كل دولة تبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني (فصل الجرائم) وذلك إذا ارتكبت الجريمة وكانت "الجريمة تمس أحد المصالح العليا للدولة".

إلا أنه يؤخذ على الاتفاقية عدم تحديد مفهوم "المصالح العليا للدولة" حيث لم يتم تحديد أو تعريف المصطلح في أي من نصوص الاتفاقية، ما يعطي الدول الأعضاء صلاحية لتفسيره طبقاً لرؤيتهم أو مصالحهم والتي ربما يروا فيها "المصالح العليا للدولة".

وقد أشارت كل من المادتين الحادية والثلاثون والثانية والثلاثون إلى موضوع تسليم المجرمين والشروط والإجراءات اللازم على الدول الأعضاء الالتزام بها، وطرق تقديم المساعدات المتبادلة من أجل تحقيق غايات التحقيقات

المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلـــة الالكترونيـــة فـــي الجرائم.

وتتناول المادة الثالثة والثلاثون "المعلومات العرضية المتلقـــاة" والتـــي تجيز للدولة مشاركة المعلومات التي تم الحصول عليها من خلال تحقيقاتها مـــع دول أخرى، دون طلب مسبق، إذا كانت هذه المعلومات "يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيـــام بتحقيقـــات فـــي الجـــرائم المنصوص عليها في هذه الاتفاقية" وتجيز الفقرة الثانية من نفس المادة للدولـــة المزودة بالمعلومات أن " تطلب الحفاظ على سرية المعلومات، وإذا لم تســـتطيع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولـــة الطـــرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات" [1].

وقد حددت المادة الرابعة والثلاثون الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة التي يتوجب على الدول الأطراف الالتزام بها مـــن خـــلال وضع التشريعات الداخلية واتخاذ الإجراءات الضرورية فـــي ســـبيل مكافحـــة الجرائم المذكورة في الاتفاقية .

وقد أشارت المادة الخامسة والثلاثون إلى إمكانية رفض المساعدة من قبـــل الدولة الطرف المطلوب منها المساعدة وذلك بشرطين إذا :

١- كان الطلب متعلق بجريمة يعتبرها قانون الدولة الطرف المطلـــوب منها المساعدة جريمة سياسية .

٢- اعتبر أن تنفيذ الطلب يمكن أن يشكل انتهاكاً لســـيادته أو أمنـــه أو نظامه أو مصالحه الأساسية .

---

[1] المادة الثالثة والثلاثون من الاتفاقية .

وقد حددت المادة السادسة والثلاثون شروط السرية وحدود الاستخدام للمعلومات المقدمة من قبل الدولة المطلوب منها.

حيث يجوز للدولة الطرف المطلوب منها توفير المعلومات أو المواد الموجودة في الطلب بشرط [1]:

أ) الحفاظ على عنصرية السرية للدولة الطرف الطالبة للمساعدة ولا يتم الالتزام بالطلب في غياب هذا العنصر.

ب) عدم استخدام المعلومات في تحقيقات أخرى غير الواردة في الطلب.

بينما تناولت المادة السابعة والثلاثون لحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات، وأعطت الحق لأي دولة طرف أن تطلب من أي دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات التي تقع ضمن إقليمها بخصوص ما تود الدولة الطرف المطالبة للمساعدة أن تقدم طلباً بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات، ثم نصت المادة في فقرتها السادسة على أن أي حفظ يجب ((أن يكون لفترة لا تقل عن ٦٠ يوم من أجل تمكين الدولة الطرف الطالبة من تسليم البحث أو الوصول أو الضبط أو التأمين أو الكشف للمعلومات، وبعد استلام مثل هذا الطلب يجب الاستمرار بحفظ المعلومات حسب القرار الخاص بالطلب)).

وقد نصت المادة الثامنة والثلاثون على الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة حيث يتوجب على الدولة الطرف المطلوب منها أن تكشف للدولة الطرف الطالبة قدراً كافياً من معلومات تتبع المستخدمين من أجل تحديد مزود الخدمة ومسار بث الاتصالات .

---

[1] الفقرة الثانية من المادة السادسة الثلاثون من الاتفاقية.

أما المادة التاسعة والثلاثون، فقد حددت سبل التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة حيث تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الاتفاقية .

وقد أجازت المادة الأربعون من الاتفاقية لأي دولة طرف الوصول إلى معلومات تقنية المعلومات عبر الحدود، وبدون الحصول على تفويض من دولة طرف أخرى .

أما المادية الحادية والأربعون فقد أشارت إلى التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينة في أقاليمها، ويتوجب على كل دولة طرف توفير تلك المساعدة في الجمع الفوري لمعلومات تتبع المستخدمين.

أما المادة الثانية والأربعون فتلزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينة تبث بواسطة تقنية المعلومات.

بينما المادة الأخيرة من الاتفاقية الثالثة والأربعون فتلزم الدول الأطراف، ووفقاً للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات، وقد حددت المادة الهيكلية والتشكيل اللازم لقيام هذا الجهاز المتخصص .

وقد اشتمل الفصل الخامس من الاتفاقية على الأحكام الختامية الناظمة لهذه الاتفاقية .

وهكذا نجد بأن هذه الاتفاقية تحتوي على نصوص وقواعد أشـــمل مـــن القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، وقد تلاقت هذه الاتفاقية الكثير من عيوب هذا القانون إلا أنه يؤخذ عليها استخدامها لمجموعة من المصطلحات والألفاظ، التي تم تكرارها في أكثر من موضـــوع، دون وجود تعريف محكم ومنضبط لها في أي مكان بالاتفاقية.

ولم يتم وضع أطر قانونية محددة على الإجراءات المتبعة لجمع البيانات والمعلومات في فصل الإجراءات .

ونلاحظ بأن التجربة العربية في مكافحة الجرائم الالكترونية ما تزال في مراحلها الأولى وذلك يعود إلى أن الاعتماد على تطبيقات الحاسب الآلـــي فـــي البلدان العربية قد بدأ منذ نهاية العقد الأخير من القرن الماضي، وبـــدأت معـــه وتيرة الحركة التشريعية لضبط ومكافحة الجرائم الالكترونية .

خاتمة

تبين لنا من خلال هذه الدراسة أن الجريمة الالكترونية تستخدم الوسائل والتقنيات الحديثة ليس للاتصال بين المجرمين أو شبكات الفساد فقط، وإنما أصبحت هذه الوسائل الحديثة تستخدم بذاتها كأداة للجريمة ووسيلة لتنفيذها بشكل مباشر .

ولقد أصبحت الجريمة الالكترونية بأبعادها ومظاهرها الحديثة، تمثل تهديداً مباشراً للأمن والاستقرار والسلام في العالم، وعائقاً يحول دون إتمام عمليات التطوير والتنمية، ولم تعد عواقبها قاصرة على بعض الدول، بل امتدت أثارها لتهدد المجتمع الدولي برمته، بما يؤكد على الحاجة إلى التعاون والتنسيق الدوليين من أجل مجابهة شاملة لتلك الأبعاد الخطيرة.

فعلى الرغم مما ترتبه شبكة الانترنت من مزايا في شتى مجالات الحياة إلا أنه كما هو شأن كل اكتشاف أو اختراع جديد، أدى إلى ظهور مشاكل قانونية، دعت الدول إلى البحث عما إذا كانت القوانين القائمة تكفي لمواجهة بعض الاستخدامات غير المأمونة للانترنت، أم أنه يتعين مواجهة هذه الأعمال بنصوص تجريمية جديدة .

وفي هذا الإطار، فقد حاولت السياسة الأمنية المعاصرة من إنجاز منظومة أمنية، أخذت بفعالية الوسائل والتقنيات الحديثة، سواء على صعيد الإجراءات الأمنية الوقائية، أو في مواجهة الجرائم الالكترونية ، على نحو أتاح لها تطوير قدراتها في مواجهة التحديات والتعامل معها بأسلوب علمي مخطط لتحقيق أهدافها في مكافحة الجرائم الالكترونية.

وقد تمثلت هذه السياسية الأمنية، في مواكبة أحدث الاتجاهات العلمية والنظرية، ومحاكاة التقدم التقني والتكنولوجي، وتطور قدرات العنصر البشري، وتحديث الأجهزة والآليات الأمنية، في إطار من التعاون المتبادل والبناء بين أعضاء المجتمع الدولي، بما يكفل تفاعل وتبادل المفاهيم والأفكار الأمنية القادرة على مواجهة الإجرام الالكتروني .

ونحن نرى بأن التوصيات المقترحة لمكافحة الجرائم الالكترونية يمكن أن تكون على النحو التالي:

١- ضرورة التنسيق والتعاون الدولي قضائياً وإجرائياً في مجال مكافحة الجرائم الالكترونية، وتعزيز التعاون والتنسيق مع المؤسسات والمنظمات الدولية المعنية بمكافحة الجرائم الالكترونية، وخصوصاً منظمة الانتربول الدولية، يتوجب على دول العالم كافة الانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الانترنت وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والانترنت والعمل على دراسة ومتابعة التطورات التقنية والالكترونية في كافة المجالات .

٢- يتعين تدريب وتحديث الضابطة الشرطية بشأن التعامل مع أجهزة الكمبيوتر والانترنت، وذلك بعقد دورات تدريبية لرجال الشرطة والمختصين بمكافحة الجريمة الالكترونية، وذلك بهدف تبادل الخبرات اللازمة لملاحقة هذا النوع من الجرائم.

٣- ضرورة سن التشريعات لمكافحة الجرائم الالكترونية، وذلك بإدخال كافة صور السلوك الضار والحظر على المجتمع التي يستخدم فيها الانترنت، وتشجيع كافة أفراد المجتمعات والمؤسسات العاملة في مجالات الاقتصاد والبنوك على الإبلاغ عن هذه الجرائم .

٤- إنشاء قسم جديدة بكليات الحقوق والقانون لدراسة قانون المعلوماتية والانترنت، وسبل مكافحة الجرائم المرتكبة في هذا المجال .

٥- ينبغي وضع قواعد تسمح للسلطات القائمة بالضبط والتحقيق بتفتيش البريد الالكتروني وأية تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل، والكشف عن الحقيقة ، وأن تتم إجراءات التفتيش إلى أي نظام حاسب آلي، يمكن أن يكون ذا صلة بالنظام محل التفتيش وضبط ما به من معلومات .

المراجع

المراجع باللغة العربية:

١ـ الكتب :

١. د. خالد ممدوح إبراهيم، الجرائم المعلوماتيـــة، دار الفكـــر الجـــامعي، الاسكندرية، الطبعة الأولى، ٢٠٠٩.

٢. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شـــبكة الانترنـــت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، ٢٠١١.

٣. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنـــت (الجـــرائم الالكترونية) الطبعة الأولى، منشورات الحلبـــي الحقوقيـــة، بيـــروت، ٢٠٠٧.

٤. عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنـــت (الأحكام الموضوعية والجوانب الإجرائيـــة)، دار النهضـــة العربيـــة، القاهرة، ٢٠٠٤.

٥. عبد الصبور عبد القوي علي مصري، الجريمة الالكترونية، دار العلوم للنشر والتوزيع، مصر ٢٠٠٨.

٦. د. علاء الدين شحاته، التعاون الدولي في مجـــال مكافحـــة الجريمـــة، القاهرة ٢٠٠٠م.

٧. د. عمر بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، الطبعة الثانية، مؤسسة آدم للنشر والتوزيع – مالطا ٢٠٠٨.

٨. د. غسان رباح، الوجيز في قضايا حماية الملكية الفكرية والفنية مع دراسة مقارنة حول جرائم المعلوماتية، الطبقة الأولى، منشورات الحلبي الحقوقية، بيروت عام ٢٠٠٨م.

٩. د. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة ١٩٨٨.

١٠. د. محمد المجذوب، القانون الدولي العام، الطبعة السادسة، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٧.

١١. منير محمد الجنبهي وممدوح محمد الجنبهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفر الجامعي، الاسكندرية، ٢٠٠٥.

١٢. محمد الأمين ومحسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدل الجنائية ومنع الجريمة أكاديمة نايف للعلوم الأمنية، الرياض، الطبعة الأولى، ١٩٩٨.

١٣. محمد الأزهر، حقوق المؤلف في القانون المغربي دراسة مقارنة في الملكية الأدبية والفنية، دار النشر المغربية، ١٩٤٤.

١٤. د. محمد منصور الصاوي، أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات، دار المطبوعات الجامعية.الاسكندرية ، مصر ١٩٨٩.

١٥. د. محمد الشناوي، جرائم النصب المستحدثة، دار الكتب القانونية، مصر، ٢٠٠٨.

١٦. محمد أمين الشوابكة، (جرائم الحاسوب والانترنت، الجريمة المعلوماتية). دار الثقافة والنشر والتوزيع، الطبعة الأولى، ٢٠٠٧.

١٧. د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت ٢٠٠٤.

١٨. د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مصر، مكتبة الآلات الحديثة،١٩٩٢.

١٩. د. هلال عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلومات، ط١، ٢٠٠٢.

٢ـ رسائل ومحاضرات :

١- د. حسين بن سعيد سيف الغامري، محاضرة أُلقيت أمام مجلس إدارة الاتحاد العربي للتحكيم الإلكتروني، ٢٠٠٧.

٢- د. محمد طارق الخن، جريمة الاحتيال عبر الانترنت، رسالة دكتوراه، جامعة دمشق، كلية الحقوق، ٢٠١٠.

٣- واقد يوسف. النظام القانوني للدفع الالكتروني – رسالة لنيل درجة الماجستير – جامعة مولود معمري، كلية الحقوق، الجزائر.

٣ ـ القوانين والاتفاقيات:

١- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام ٢٠٠٢ الاتفاقية منشورة على الموقع الإلكتروني :

www. Umn.deu / humanats / apab/corgcpiwe.htm

٢- القانون الوطني الأمريكي الصادر في ٢٠٠١/١٠/٢٦ وقد تناول تعديل حوالي ١٥ قانوناً .

٣- القوانين الأمريكية الفيدرالية الإجرائية بشأن جرائم الكمبيوتر المنصوص عليها في الباب ١٨ للقانون الفيدرالي.

٤- قانون العقوبات التونسي لعام ١٩٩٢ باللغة الانكليزية على موقع القوانين التونسية على الانترنت: www.egifrance.gouv.fr .

٥- قانون الجزاء العماني المنشور على الموقع : www.rg.gov.com/Avabic/

٦- قانون تنظيم الاتصالات العماني المنشور على موقع : www.mola.gov.om.

٧- القانون السعودي لمكافحة الجرائم المعلوماتية منشور على الموقع : www.aecert.ae/uaelw.ar.htm/

٨- القانون الاتحادي لدولة الامارات العربية المتحدة منشور على الموقع الالكتروني :www.emiatesid.gov.ae/assets/9454057964

٩- قانون رقم /٨٣/ لسنة /٢٠٠٠/ التونسي المتعلق بالمبادرات والتجارة الإلكترونية المنشورة على موقع نقابة المحامين في سورية www.syria.var.org

١٠- قانون التوقيع الالكتروني المصري موجود على الموقع الالكتروني :Mrwsa.arbb/ogs.com

١١- قانون المعاملات الالكترونية الاردنية رقم /٨٥/ لعام ٢٠٠١.

١٢- قانون الأوربيين لجرائم أنظمة المعلومات لعام ٢٠١٣ .

١٣- كتاب وزير الاتصالات والتقانة .

١٤- قانون مكافحة الجرائم الالكترونية في سورية .

٤ ـ المقالات والأبحاث على الشبكة والتقارير :

١- مقالة بعنوان جرائم الكمبيوتر والأنترنيت منشورة على الموقع الالكتروني:

www.awjo.net

٢- أسامة فتحي، فيروسات الحاسب، بحث منشور على الموقع:

http :// www.Kutub.info – 2494 .pdf

٣- مقالة بعنوان الجريمة عبر الأنترنيت الركن المادي في جرائم الأنترنيت منشورة على الموقع الالكتروني: www.lawjo.ney المصدر شبكة قانونية الأردن.

٤- رحاب عميش – الجريمة المعلوماتيـــة، مقالـــة منشـــورة علـــى الموقـــع الالكتروني: www.docstoc.com/docs/145159921

٥- مقالة بعنوان مكافحة الجريمة الإلكترونية منشورة على موقع الاقتصـــادية الالكتروني: www.alojtisadiah.com

6- مقالة منشورة على الموقع www.ituarabic.org/coe/2006/Ecrime بعنوان الاتجاهات التشريعية للجرائم الإلكترونية للمحامي الدكتور يـــونس عرب، عمان – الاردن.

٧- تقرير بعنوان الانترنت والحكومات العربية الصادرة عن الشـــبكة العربيـــة لحقوق الإنسان يوم /١٣/ ديسمبر ٢٠٠٦ المنشور على الموقع:

www.ligqa.net/fip.php.article190

٨- مقالة منشورة على الموقع:

www.somn7.com/news.as?newssid.663483

٩- بحث بعنوان حجية التوقيع الالكتروني في الأردن مقدم من الســـيدة أحـــلام الجمبرجي، عام ٢٠٠٨، منشور على الموقع الالكتروني:

www.free-20nes-gov.jo

١٠- مقررات " المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين " المنعقد فـــي القاهرة ١٩٩٥ موجود على الموقع الإلكتروني:

www.neuss.edu.sa/a/ooarchve/S/fm-dar5-3ueloprlso2

١١- المؤتمر الأول للشرطة الجنائية الدولية في موناكو عـــام ١٩١٤ منشـــور على موقع المنظمة الجنائية الدولية:

www.interpil.net

١٢- مقالة منشورة على الموقع الالكتروني:

? www.algeriepolice.d2/

١٣- مقالة منشورة على الموقع الالكتروني: الانتربول – قوانين – مارقه – بين البلدان: www.algadidah.com/2013

١٤- مقالة منشورة على الموقع الالكتروني:

www.ALTNEWS.com/2013/01/10

١٥- مقالة منشورة على الموقع الالكتروني:

www.nauss.edu.sa/A/ooarchre/S/fm-dar.5-3nerpr/SD2

١٦- مبادئ توجيهية للمؤتمر الثامن منشورة على الموقع الإلكتروني:

Http;//www.hrea.ogr/index.pnp

١٧- وثيقة تتعلق بمقررات المؤتمر الثاني عشر لمنع الجريمة منشـــورة علـــى الموقع:

www.nucodc.orj/documents/cpime-cogress/crime/V10538262.pff

المراجع باللغة الانكليزية

1. Malcom Anderson : "policimg the world : Interpol the politics of International police Co-Operation", Claren don press. Oxford, 1989.
2. Pemlan jimene2: «international secur ithiesen for emcnef cooperation Act and Memora of understandine in Harvard intirational law journal, winter 1999 , vol, 31, No, Harvard law school, cambrige, massachustts , P.295 – 317.
3. hrdishon Piit & Shapiro : «Proplems of erforcement in the 435 mal tintioanl Securities market, 94 Pa.j.int lbus. G 1987.
4. Explanatorsote in English of the 2001 European Convention on Virtual crime.

الفهرس

الموضوع	الصفحة
مقدمــة	١
الفصل الأول : مفهوم الجرائم الالكترونية وسبل مكافحتها	٥
المبحث الأول : مفهوم الجريمة الالكترونية	٧
المطلب الأول : تعريف الجريمة الالكترونية	٧
أولاً : مدلول الجريمة الالكترونية	٨
ثانياً :الجريمة الالكترونية كإحدى صور الجرائم المنظمة .	١١
المطلب الثاني : أنواع الجريمة الالكترونية	١٣
أولاً : جرائم الإضرار بالبيانات .	١٤
ثانياً : جرائم الاعتداء على الاشخاص .	١٦
ثالثاً :جرائم تصميم البرمجيات الحديثة (الفيروسات)	١٧
رابعاً : جرائم الأضرار بالمصالح العامة والخاصة.	١٩
خامساً : جرائم الاعتداء على الأموال .	٢١
المطلب الثالث: الصفة الدولية للجريمة الالكترونية .	٢٦
أولا : الجرائم الالكترونية جرائم عابرة للحدود .	٢٦

ثانياً : أهمية مكافحة الجريمة الالكترونية على الصعيد الدولي	٢٨
ثالثاً : أهم الصعوبات التي تواجه قمع الجرائم الالكترونية .	٣١
المبحث الثاني : مكافحة الجرائم الالكترونية في القوانين الوطنية	٤١
المطلب الأول : التشريعات الأجنبية لمكافحة الجرائم الالكترونية.	٤١
المطلب الثاني : التشريعات العربية لمكافحة الجرائم الالكترونية.	٤٥
المطلب الثالث: التشريعات السورية لمكافحة الجرائم الالكترونية	٥٢
الفصل الثاني: فاعلية القانون الدولي في مكافحة الجرائم الالكترونية	٥٥
المبحث الأول: مكافحة الجرائم الالكترونية من قبل المنظمات والمؤتمرات الدولية	٥٧
المطلب الأول: مكافحة الجرائم الإلكترونية من قبل المنظمات الدولية	٥٧
أولاً- منظمة الأمم المتحدة .	٥٧
ثانياً- المنظمة الدولية للشرطة الجنائية . (انتربول).	٦١
ثالثاً- المنظمات الإقليمية .	٦٧
المطلب الثاني: مكافحة الجرائم الإلكترونية من قبل المؤتمرات الدولية	٧٠

أولاً- مؤتمر الأمم المتحدة السابع حول منع الجريمة لعام ١٩٨٥م .	٧١
ثانياً- مؤتمر الأمم المتحدة الثامن حول منع الجريمة لعام ١٩٩٠م .	٧٥
ثالثاً- مؤتمر الأمم المتحدة العاشر حول منع الجريمة لعام ٢٠٠٠م.	٧٦
رابعاً- مؤتمر الأمم المتحدة الحادي عشر حول منع الجريمة لعام ٢٠٠٥ م .	٧٧
خامساً- مؤتمر الأمم المتحدة الثاني عشر حول منع الجريمة لعام ٢٠١٠ م .	٧٩
المبحث الثاني: مكافحة الجرائم الالكترونية في الاتفاقيات الدولية .	٨٥
المطلب الأول: الاتفاقات الأوربية حول مكافحة الجرائم الالكترونية	٨٥
أولاً: الاتفاقية الأوربية الخاصة بحماية الأفراد من معالجة المعلومات الخاصة بهم لعام ١٩٨١ م.	٨٦
ثانياً: الاتفاقية الأوربية حول الجريمة الافتراضية لعام ٢٠٠١ م.	٨٨
المطلب الثاني: الاتفاقيات العربية حول مكافحة الجرائم الالكترونية.	١٠١
أولاً: القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها .	١٠٢
ثانياً: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .	١٠٨
الخـــاتمة	١٢١

المراجع	**١٢٥**
الفهرس	**١٣٣**