بسم الله الرحمن الرحيم

جرائم المعلوماتية

مقدمة :

أصبح إستخدام البيئة الرقمية في كافة المجالات والمعاملات في إزدياد مضطرد مما يستدعي المواكبة البحثية والقانونية للتعامل مع قوانين هذه البيئة المستحدثة وإيجاد الحلول اللازمة أمام مشكلاتها ، فأصبحت الضرورة ملحة لأن تواكب قواعد النظام القانوني هذه المتغيرات ، وبإجازة قانون مكافحة جرائم المعلوماتية في السودان في عام 2007 صار لازماً التبحر في هذا المجال بدراسة البيئة الرقمية والمعلوماتية وإبراز تجارب الدول الأخرى للمقارنة والإستفادة منها وإشاعة نوع من الثقافة يعين على الإدراك العميق تجاه المتغيرات العصرية المستمرة في بيئة المعلوماتية ، مما يدعو لإتباع الطرق العلمية في التحقيق والإثبات والمواجهة لهذا النوع من الجرائم في البيئة الرقمية ، والجرائم المعلوماتية هي ثمرة من ثمار التقدم السريع في شتى المجالات التي يتميز بها عصرنا الحاضر وقد صاحب هذا التقدم في مجال العلوم والتقنية وإستخداماتها لخير البشرية تقدم مواز في مجال الجريمة .

تعريف الجرائم المعلوماتية :-

وصفت هذه الجريمة بأنها جريمة تقاوم التعريف resists definitionلكثرة ما تناولته الكتابات عنها شرحا وتوضيحا .

هناك تعريفات متعددة لجرائم المعلوماتية وتعددت نسبة للنظر اليها من عدة زوايا فمنهم من نظر اليها من خلال وسيلة إرتكابها ومنهم من نظر اليها من خلال موضوعها ومنهم من نظر اليها من خلال توافر المعرفة بتقنية المعلومات ومنهم من نظر اليها نظرة مختلفة .

ومن التعريفات الجامعة للجرائم المعلوماتية :

التعريف البلجيكي الذي ورد في الإجابة البلجيكية على الإستبيان الذي أجرته منظمة التعاون الإقتصادي والتنمية ((OCDEحول الغش المعلوماتي عام 1982 حيث ورد تعريف للجريمة المعلوماتية مقتضاه انها ((كل فعل أو إمتناع من شأنه الإعتداء على الأموال المادية او المعنوية يكون ناتجاً ، بطريقة مباشرة أو غير مباشرة عن الإستخدام غير المشروع لتقنية المعلومات)) ويلاحظ ان هذا التعريف يعتبر تعريفاً واسعاً للجريمة المعلوماتية يعبر عن طابعها التقني الخاص أو المميز وتنطوي تحته أبرز صورها ويشمل تحديده لركنها المعنوي (القصد الجنائي) ويمكن من خلال هذا التعريف التعامل مع التطورات المستقبلية للتقنية .

التعريف في القانون السوداني :-

صور جرائم المعلوماتية :-

1.الجرائم المتعلقة بالأموال :-

جرائم التقنية ذات الصبغة المالية من أكثر أنواع جرائم نظم المعلومات وأعظمها أثراً لتعلقها بصورة مباشرة بالأصول المالية ، سواء تلك الخاصة بالأفراد ، أو المؤسسات الإقتصادية العامة منها والخاصة وهي على النحو التالي :-

- جريمة إساءة الإئتمان .
- جريمة إتلاف النظم .
- جريمة السرقة المعلوماتية .
- جريمة التزوير المعلوماتي .
- جريمة غسيل الأموال .
- جريمة الإعتداء على برامج الحاسب الألي .

2.جرائم تقنية الإتصالات :-

الحديث عن جرائم تقنية الإتصالات لا ينقطع فمع كل تأخر في سن التشريعات الجديدة اللازمة لمواجهة هذه الجريمة ومكافحتها ، تزداد خطورة الظاهرة ، وتتسع الأثار السلبية لثورة تقنية نظم المعلومات ، ويزداد الجناة إجراماً، فيما تتعاظم خسائر المجني عليهم افراداً أو مؤسسات ، الأمر الذي يدفع بمزيد من الجهد لمكافحة هذه الظاهرة وملاحقة الجناة فيها وشكلها على النحو التالي :-

- جرائم الإعتداء على حرمة الحياة الخاصة .
- جرائم الإنترنت المتعلقة بالقاصرين .
- جرائم نظم الإتصالات .
- جرائم التجسس الإلكتروني .
- جرائم المواقع الاباحية .
- جرائم الإرهاب .
- جرائم القذف الإلكتروني [الذم – القدح – التحقير- إشانة السمعة]

خصائص جرائم المعلوماتية :

تتميز جرائم التقنية بخصائص تختلف إلى حد ما عن الجريمة العادية نذكرها على النحو التالي:-

أولاً: جرائم عابرة للدول :

إن تعبير "جرائم عابرة للدول" أو جرائم عبر وطنية هي تلك الجرائم التي تقع بين أكثر من دولة ، بمعنى أنها لا تعترف بالحدود الجغرافية للدول كجرائم غسيل الأموال ، والمخدرات وغيرها .

وفي عصر الحاسب الآلي ومع انتشار شبكة الإتصالات العالمية (الإنترنت) أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة بحيث يغدو أمراً سهلاً ، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر ، وسواء تم ذلك بطرق مشروعة أو غير مشروعة .

في هذه البيئة يمكن أن توصف الجريمة التقنية بأنها جرائم عابرة للدول ، إذ غالباً مايكون الجاني في بلد ، والمجني عليه في بلد آخر ، كما قد يكون الضرر المتحصل في بلد ثالث في نفس الوقت ، وعليه تعتبر جرائم التقنية شكلاً جديداً من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية.

ثانياً : جرائم صعبة الإثبات :

يستخدم الجاني فيها وسائل فنية تقنية معقدة في كثير من الأحيان كما يتمثل السلوك المجرّم المكون للركن المادي فيها من عمل سريع ، قد لا يستغرق أكثر من بضع ثواني ، بالإضافة الى سهولة محو الدليل، والتلاعب فيه [. Tomeson Case]
مما يزيد الأمر صعوبة ضعف خبرة الشرطة ومعرفتهم الفنية بأمور الحاسب الآلي سواء تمثل الضعف في تحديد الدليل المعتبر ، أم في إنتشال ذلك الدليل والمحافظة عليه .

بالإضافة إلى عدم تقبل القضاء لغاية الآن لكثير من صور الجريمة الحاسوبية وأمكانية إثباتها بطرق جديدة ، ولا تزال جرائم التقنية تعامل وفق المفهوم التقليدي للجريمة العادية .

ثالثاً : جرائم مغرية للمجرمين :

لما كانت جرائم التقنية جرائم سريعة التنفيذ إذ غالباً ما يتمثل الركن المادي فية بضغط كبسة معينة في الجهاز ، مع إمكانية تنفيذ ذلك عن بعد ، دون إشتراط التواجد في مسرح الجريمة .

رابعاً : جرائم سهلة الإرتكاب :

تمتاز جرايم التقنية بأنها جرائم ناعمة أو كما يطلق عليها بعض الفقه مصطلح " جرائم ذوي الياقات البيضاء" كناية على أنها لا تحتاج الى إلى أدني مجهود عضلي ولا تحتاج إلى سلوكيات مادية فيزيائية متعددة لتحقيق النتيجة فيها "فطالما توافرت لدى الفاعل التقنية اللازمة والوسيلة المناسبة أصبح إرتكاب الجريمة من السهولة بمكان لا يحتاج إلى وقت ولا على جهد .

الإثبات وجمع الأدلة في البيئة الرقمية :

مع السرعة المذهلة والمتزايدة في التقدم التقني والانفجار المعلوماتي ينهض الان الدليل الافتراضي (الرقمي) الذي يحتاج الي مزيد من البحث والتكييف ففي الغالب
الاعم هو دليل غير ملموس يعتمد علي معادلات رياضية معقدة وخوارزميات ترتكز علي (0) zeroوالرقم (1) . one
وعلي مدي التاريخ الادلة التي تعاملت معها أجهزة العدالة أدلة لها اشكال وطرق محددة الا أن الجرائم التي ترتكب في بيئة المعلوماتية شكلت تجدياً قانونياً جديداً يصعب علي أهل العدالة الخوض فيه دون التزود بالمعرفة الجديدة المتعلقة بعالم المعلوماتية وتقنياته .

طبيعة الادلة الرقمية :

الادلة الرقمية تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة ولا يدركها الرجل العادي بالحواس الطبيعية للإنسان [معادلات رياضية] .

وتتسم الجرائم في البيئة الرقمية أو بيئة المعلوماتية بصعوبة تتعلق بالإثبات والتحقيق إذ ان نوع هذه الجرائم التي تقع على الحاسبات والشبكات أو بواسطتها ، مستتره في الغالب .

مفهوم الدليل الرقمي :

أحدث تعريف للدليل الرقمي هو ماعرفة (Eoghan casey)بأن الادلة الرقمية تشمل جميع البيانات التي يمكن أن تثبت ان هنالك جريمة قد ارتكبت ، أو توجد علاقة بين الجريمة والمتضرر منها ، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة ، الرسومات ، الخرائط ، الصوت أو الصورة .

إذاً الأدلة الجنائية الرقمية هي معلومات يقبلها المنطق والعقل ويعتمدها العلم ، يتم الحصول عليها بإجراءت قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الاتصال ، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل او شئ أو شخص له علاقة بجريمة أو جاني أو مجني عليه .

الأدلة الرقمية والأدلة المادية :

يري البعض أن الادلة الجنائية الرقمية ماهي الا مرحلة متقدمة من الادلة المادية الملموسة التي يمكن ادراكها باحدي الحواس الطبيعية للانسان الي الاستعانة بجميع مايبتكره العلم من اجهزة مخبرية ووسائل التقنية العالية ومنها الحاسوب محور الأدلة الرقمية ، فالأدلة الجنائية الرقمية في منظور أنصار هذا الاتجاه لاتختلف عن اثار الاسلحة والبصمات أو البصمة الوراثية D.N.A..

ولكن الحقيقة ، الأمر غير ذلك فإن الادلة الرقمية هي نوع متميز من وسائل الاثبات ولها من الخصائص العلمية والمواصفات القانونية مايؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية .

خصائص الأدلة الرقمية :

1.الأدلة الرقمية تتكون من دوائر وحقول مغناطيسية ونبضات كهربائية غير ملموسة ولا يدركها الرجل العادي بالحواس الطبيعية للإنسان .

2.الادلة الرقمية ليست كما يقول البعض ، أقل مادية من الادلة المادية فحسب بل تصل الي درجة التخيلية في شكلها وحجمها ومكان وجودها غير المعين .

3.يمكن استخراج نسخ من الادلة الجنائية الرقمية مطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية الشئ الذي لا يتوفر في انواع الادلة الأخري .

4.يمكن التعرف علي الادلة الرقمية المزورة أو التي جري تحريفها بمضاهاتها مع الأدلة الأصلية بالقدر الذي لا يدع مجالاً للشك

5.من الصعب الإتلاف أو القضاء علي الأدلة الجنائية الرقمية التي يمكن استرجاعها من الحاسوب بعد محوها .

6.علاوة علي وجود الادلة الرقمية في مسرح الجريمة التقليدي يمكن وجودها أيضاً في مسرح أو مكان افتراضي Virtual Scene of Crime .

7.تتميز الادلة الجنائية الرقمية عن غيرها من انواع الادلة بسرعة حركتها عبر شبكات الاتصالات .

وقد قضت المحاكم بإمكانية اعتماد مثل تلك الأدلة غير الملموسة لأنها تتميز عن غيرها من أنواع الأدلة المادية الأخري بمايلي: -

1.يمكن استخراج نسخ منها مماثلة ومطابقة للأصول ولها ذات الحجية .

2.يمكن بالأساليب العلمية الملائمة تحديد وتأكيد ما إذا كانت الأدلة الرقمية قد تعرضت اتعديل أو تحريف .

3.من الصعب إتلاف الأدلة الجنائية الرقمية ، وفي حالة محوها أو إتلافها يمكن استرجاعها من ذاكرة الحاسوب .

4.إذا حاول المتهمون إتلاف الأدلة الرقمية يمكن الاحتفاظ بنسخ منها في أماكن آمنة ، علماً بأن للنسخ قيمة الأصل .

المواجهة التشريعية والاجرائية لجرائم المعلوماتية :

ما مدى ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم المعلوماتية؟

1.إن القواعد التقليدية في قانون العقوبات غير ملاءمة لمواجهة جرائم السرقة والنصب وخيانة الأمانة وإخفاء الأشياء المتحصلة من الجريمة إذا وقعت تلك الجرائم على معلومات.

2.يرجع السبب في عدم الملاءمة سابقة الذكر إلى الطبيعة الخاصة للمعلومات إذا ما قورنت بغيرها من منقولات . ذلك أن المعلومات لها طابع معنوي .

3.إن القضاء الفرسي إجتهد في تحديد مفهوم جديد للإختلاس يتماشى مع ما للمعلومات من طبيعة خاصة على ما سلف بيانه .

4.إن أحكام القضاء الفرنسي إستقرت على أن المعلومات لا تكتسب صفة المال المنقول الذي تحمية جرائم الأموال إلا إذا كانت مدونة على دعامة مادية .

5.إن إنطباق وصف تزوير المحررات على تغير البيانات الواردة في النظام (الكمبيوتر) لم ينل إجماعا في الرأي . ومن المناسب التدخل التشريعي في تحديد مفهوم التزوير بحيث يشمل تغير الحقيقة في بيان مكتوب أو في معلومات مبرمجة ، على غرار ما فعله المشرع الفرنسي.

6.لو إنتهينا إلى توفر وصف التزوير على تغير الحقيقة في المعلومات المدونة على دعامة مادية ، فإن ذلك لا يكفي لتوفير حماية جنائية لتلك المعلومات ، ما لم يعد للاحتجاج به في إثبات حق أو مصلحة قانونية على ما سلف بيانه .

7.أن النصوص التقليدية في خصوص السرقة والنصب وخيانة الأمانة وإخفاء الأشياء المسروقة غير كافية لتوفير الحماية للمعلومات داخل النظام (الكمبيوتر) . ويحتاج الأمر إلى نصوص خاصة لتجريم التداخل في نظام الكمبيوتر وتغيير البيانات الواردة فيه والتحايل للإستفادة بخدمات (وقت) أو برامج يقدمها نظام الكمبيوتر . وقد تدخل المشروع في قوانين أوربية وأمريكية بالتجريم في هذا المجال .

قوانين مكافحة جرائم المعلوماتية العالمية :

تعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والإنترنت ، حيث صدر قانون البيانات السويدي عام (1973) الذي عالج قضايا الإحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسوبية أو تزويرها أو تحويلها أو الحصول غير المشروع عليها .

وتبعت الولايات الأمريكية السويد حيث شرعت قانوناً خاص بحماية الحاسب الآلي (1976-1985) وفي عام (1985) حدد معهد العدالة القومي خمسة أنواع رئيسية للجرائم المعلوماتية وهي :

1.جرائم الحاسب الآلي الداخلية .
2.جرائم الإستخدام غير المشروع عن بعد .
3.جرائم التلاعب بالحاسب الآلي .
4.دعم التعاملات الإجرامية .
5.سرقة البرامج الجاهزة والمكونات المادية للحاسب .

وتاتي بريطانيا كثالث دولة تسن قوانين خاصة بجرايم الحاسب الآلي حيث أقرت قانون مكافحة التزوير والتزييف عام (1981) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإلكترونية أو باي طريقة أخرى .

وتطبق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والإنترنت حيث عدلت في عام (1985) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والإنترنت ، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسوبية ، وجرائم التدمير ، أو الدخول غير المشروع لانظمة الحاسب الآلي .

وفي عام (1985) سنت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والإنترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو اي كسب غير مشروع سواء للجاني أو طرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الإستفادة منها .

وكانت فرنسا من الدول التي إهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988) القانون رقم (19-88) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها ،كما تم عام (1994) تعديل قانون العقوبات لديها ليشمل مجموعة من القواعد القانونية الخاصة بالجرائم المعلوماتية وأوكل على النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريات وسماع الاقوال .

أما في هولندا فلقاضي التحقيق الحق بإصدار أمر بالتنصت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة ، كما يجيز القانون الفنلندي لمأمور الضبط القضائي التنصت على المكالمات الخاصة بشبكات الحاسب الآلي ، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة إتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاث أيام .

وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت ونصت تلك القوانين على انه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمة السر التي يستخدمها إذا ما كان سيؤدي الى إدانته .

كما يوجد في المجر وبولندا قوانين خاصة بجرائم الحاسب الآلي والإنترنت وتوضح كيفية التعامل مع تلك الجرائم ومع المهتمين فيها .

التشريعات والقوانين المتعلقة بجرائم المعلوماتية في الدول العربية :

يمكن تلخيصا كما يلي :

1. في نطاق التجارة الإلكترونية تم إقرار عدد من التشريعات في الأردن وتونس ومصر والبحرين والسودان .
2. في نطاق حماية المصنفات الرقمية تم توفير الحماية للبرمجيات وقواعد البيانات في مختلف الدول العربية ، وثمة توفير حماية لطوبغرافيا الدوائر المتكاملة في الأردن وتونس .
3. على صعيد قوانين جرائم الكمبيوتر تم إقرار مودا معدلة في قانون الجزاء العماني جرمت عدد من صور جرائم الكمبيوتر وصدر قانون أردني
4. وعماني في ذات الحقل ونفس الخطوة تمت في الامارات العربية المتحدة والسودان ومصر إضافة إلى أن هناك مشروع قانون نموذجي وضعته جامعة الدول العربية.
5. ليس ثمة أي قانون في حقل الخصوصية وحماية البيانات الشخصية.
6. أما على صعيد الإثبات فثمة تعديل لقانون البيانات الأردنية وهناك مشروع قانون معدل للقانون اللبناني في حجية البريد الالكتروني ومستخرجات الحاسوب.
7. على صعيد معايير المقاييس التقنية لم يوضع الى حد الان أي تشريعات تضبط مستويات إلتزامات جهات خدمات الانترنت , وثمة جملة من التعليمات المنظمة لبعض الخدمات العامة للإنترنت كمقاهي الإنترنت , لكنها تعليمات إدارية لا تتصل بالجوانب التقنية
8. على مستوى أجهزة الشرطة تم إستحداث قسم جرائم الكمبيوتر في الأردن والسودان والسعودية والإمارات وتونس ومصر والبحرين .
9. لم يجر أي تدخل في تشريعات الأصول الجزائية والعقوبات بشأن تنظيم عمليات ضبط وتفتيش نظم المعلومات وقواعد البيانات
10. ليس ثمة أي إتفاقية تعاون أو تنظيم للإختصاص أو القانون الواجب التطبيق أو نقل التحقيق خارج الحدود بالنسبة لمسائل وقضايا الإنترنت بين الدول العربية أو بينها وبين دول العالم .

إضاءة حول قانون جرائم المعلوماتية السوداني لسنة 2007

صدر في السودان من التشريعات التي تحمي المتعاملين مع الشبكة الإلكترونية أو جهاز الحاسب الألي ومنها تشريعات تحرم تلك الأفعال غير المشروعة أسوة بالدول المتقدمة وتنفيذاً لقرار مجلس وزراء العدل العرب مما حث الدول الأعضاء في إصدار قانون لمكافحة جرائم المعلوماتية وفيما يلي نورد السمات الأساسية لفروع القانون :-

يشتمل القانون على ثمانية فصول

الفصل الأول : يتضمن الأحكام التمهيدية من إسم القانون وبدء العمل به على نطاق تطبيق القانون على عدد من التفاسير المتفق عليها في الدول التابعة لجامعة العربية .

الفصل الثاني : جرائم نظم ووسائط وشبكات المعلومات :

أفرد لعدد من الجرائم المعلوماتية كما اشتملت نصوص تلك المواد على العقوبات الواجب تطبيقها , هذا وقد أفرد المشرع نص خاص بإرتكاب تلك الجريمة بواسطة الموظف العام , ونص على جريمة التنصت وإلتقاط أو إعتراض الرسائل . وأشار على جريمة دخول المواقع عمداً بقصد الحصول على بيانات أو معلومات أمنية كما نص على جريمة إيقاف أو تعطيل أو إتلاف البرامج أو البيانات أو المعلومات

وتتحدث عن إعادة أو تشويش أو تعطيل الشبكة المعلوماتية أو أحد أجهزة الحاسب الألي أو دخول المواقع الخاصة بدون وجه حق.

الفصل الثالث : الجرائم الواقعة علي الاموال والبيانات والاتصالات :

إشتمل على ثلاث مواد أفردت للجرائم الواقعة على الأموال والبيانات والإتصالات وإشتملت تلك الاموال على التهديد والإبتزاز وانتحال الشحصية أو صيغة غير صحيحة بغرض الحصول على مال أو سند كما تضمن هذا الفصل الحصول على أرقام أو بيانات البطاقات الإئتمانية وما في حكمها دون وجه حق كما شمل ذلك الفصل الجرائم الخاصة بالإنتفاع دون وجه حق بخدمات الإتصالات .

الفصل الرابع : جرائم نظام العام والاداب :

أفراد للجرائم الخاصة بجرائم النظام العام والأداب وذلك من حيث إنشاء أو نشر المواقع بقصد ترويج أفكار وبرامج مخالفة للنظام والآداب . كما تضمن هذا المشروع جريمة الإعتداء على المبادئ والقيم الدينية أو الحرمات .

الفصل الخامس : جرائم الارهاب والملكية الفكرية :
خصص لجرائم الإرهاب والمعلومات الأمنية والملكية الفكرية وذلك من حيث إنشاء أو نشر المواقع للجماعات الإرهابية ومن تلك الجرائم دخول المواقع عمدا دون وجه حق بغرض الحصول على بيانات أو معلومات أمنية .
هذا وقد نصت المادة 19 من ذات الفصل على جريمة نشر أو نسخ المصنفات الفكرية أو الأدبية أو الأبحاث العلمية دون وجه حق .

الفصل السادس : جرائم الاتجار في الجنس البشري والمخدرات وغسل الاموال :
أفرد لجرائم الإتجار في الجنس البشري والمخدرات والأموال القذرة .

الفصل السابع: أحكام عامـــة :
إشتمل على أحكام وقد تضمن نص خاص بتعريف التحريض أو الإتفاق وعقوبتهما كما أفرد نص لتعريف الشروع وعقوبته وأشار الفصل لابعاد الاجنبي في حالة الجرائم المنصوص عليها في المواد (7/15/16/18/20/21/22) اذا كان مداناً .
هذا وقد إشتمل هذا الفصل أيضاً على وجوب مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في إرتكاب تلك الجرائم .

الفصل الثامن : إجراءات تنفيذ القانون :
وبما أن هذا القانون ينطبق على المواطن السوداني والأجنبي على حد سواء عليه رأى المشرع على إبعاد الأجنبي شريطة مراعاة نصوص الاتفاقيات الدولية . وذلك في حالة إرتكاب مواد معينة وهي المادة 15 , 16 , 17 , 18 , 20 , 21 , 22 .
الاتجاهات المستقبلية للجريمة المعلوماتية - أهم التوقعات :
يكاد ينعقد الإتفاق بين الباحثين المعنيين بإستشراف ملامح مجتمع المستقبل على أن المشكلات الناجمة عن الجريمة في مجال المعالجة الآلية للبيانات وشبكات المعلومات ستشهد تفاقما حادا فيما يأتي من السنين.

ازدياد حجم الجريمة :
ستزداد معدلات هذه النوعية من الجرائم وترتفع خسائرها نتيجة تعميم المعلومات في سائر المجالات , لاسيما في مجال التعاملات المالية والإدارية وقطاع الأعمال الحكومي والخاص , وذيوع التعامل عبر شبكة المعلومات العالمية (الإنترنت) التي تربط بين المراكز الإتصالية والمعلوماتية حول الكرة الأرضية , فضلاً عن أن تدني أسعار بعض الأجهزة والمعدات الحديثة التي تباع في الأسواق سيفتح باباً واسعاً لإرتكاب تلك الجرائم عن طريق وسائل الإتصال .

تطور نوع الجريمة :

سيؤدي تيسير الإتصال عن بعد بأنظمة المعالجة الآلية للبيانات وشبكات المعلومات وشبكات المعلومات العالمية الى ظهور أنماط مستحدثة غير معروفة بعد , مما سيساهم في ذلك أن تطور الرقابة الأمنية لنظم الحاسبات والشبكات كما سيؤدي بالإضافة الى الحد من التلاعب التقني التقليدي والبسيط قي نظم المعلومات الى إبتكار أساليب خداعية جديدة لإرتكاب الجرائم المعلوماتية وإثارة التحدي الذهني لدى المجرمين وزيادة عدد الجرائم التي تقع بالتواطؤ والتعاون مع عدة مجرمين .

تعقيدات الجريمة كجريمة عابرة للحدود :

فإن تزايد إستخدام شبكات المعلومات العالمية وتنوع أشكالها وتعاظم الطلب على إستخدامها سيتيح إنتقال الجريمة المعلوماتية عبر الحدود الجغرافية للدول . وإذا لم يتم , على المستوى الدولى تنسيق عمليات وإجراءات مكافحتها على النحو الذي أسلفنا بيانه فإن بعض الدول ستكون ملاذا أو ملجأ لإرتكابها .

وبالإضافة الى ما تقدم , يجب أن يكون متوقعا كذلك أن تستخدم الحكومات وعصابات الجريمة المنظمة والجماعات الإرهابية إمكانات الجريمة المعلوماتية

لتحقيق أغراضها. ومن المتوقع أيضاً أن تحدث تغيرات في نوعية المجني عليهم في هذه الجرائم. ففي معظم الحالات التي وقعت حتى الآن تمثل المجني عليهم في الشركات التي تملك أنظمة معلوماتية , أما في المستقبل فسيزيد عدد المجني عليهم والمتضررين من هذه الجرائم مع التزايد المطرد في عدد مستخدمي الحاسبات وشبكة المعلومات العالمية (الإنترنت) , وسيندرج بينهم مستخدمي بطاقات الإئتمان ومستخدمي شبكات المعلومات ومستخدمي الحاسبات الشخصية بصورة أوسع وأكبر , إضافة الى أنظمة المعلومات والشبكات الخاصة بالدول التي ستسعى لأسباب سياسية أو إقتصادية أو عسكرية , لممارسة التجسس الإلكتروني والتنصت على الشفرة التي يستخدمها أعداءها في حماية معلوماتهم وإتصالاتهم أو الى تدمير البنية التحتية للمعلوماتية من مراكز إتصالات وشبكات وإفساد قواعد البيانات والمعلومات المخزنة فيها في إدارتها لصراعها مع أعدائها .

وفي ضوء ما تقدم يمكن القول بأن مواجهة الجرائم المعلوماتية والوقاية منها وحشد الجهود للتغلب على صعوبة إكتشافها سيكون من المسائل التي ستحظى بأهمية بالغة في السنوات المقبلة .

وبالله التوفيق