المحور الخامس : أساليب و تقنيات إرتكاب الجرائم المعلوماتية

يحتاج مرتكب الجريمة سواء كانت تقليدية أو معلوماتية إلى إستخدام وسائل و أساليب غير مشروعة لتحقيق أغراضه ، إلا أن الجريمة المعلوماتية تتميز بكونها تنصب حول التأثير سلبا عل الحاسب الآلي و إتلاف و تدمير أنظمته المعلوماتية .

فالمجرم المعلوماتي يحتاج إلى الإستعانة بأدوات معينة يفرض وجودها هذا النوع من الجرائم ، و بسبب إعتبار الجريمة جريمة تقنية ترتكب بوسائل فنية و تقنية تتناسب و طبيعة المعلومات محل الجريمة المعلوماتية ، فإنها بالضرورة تجعل مرتكبها يلجأ في تنفيذ جرائمه إلى إستعمال تقنيات مختلفة تتميز بالتغير و التطور المستمر ، و لذا فرغم محاولة حصرها فإنه بالمقابل لا يمكن التنبؤ بالوسائل الفنية و التقنية التي قد أستحدثت في مجال تكنولوجيا المعلومات.

و لعل من أهم هذه التقنيات ما يسمى بالإختراق و إستعمال البرامج الخبيثة و التي سنتناولها من خلال مايلي:

أولا : أدوات الجرائم المعلوماتية

حتى يتمكن الجاني من تنفيذ جريمته المعلوماتية يستلزم توفر أدوات لذلك و من أبرزها مايلي:

- الإتصال بشبكة الإنترنت بإعتبارها أداة رئيسية لتنفيذ الجريمة.
- توفير برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب.
- وسائل التجسس و منها ربط الكاميرات بخطوط الإتصال الهاتفي .
- توفير ما يسمى بالباركود و هي عبارة عن أدوات تستخدم لمسح الترميز الرقمي و فك تشفيرة الرموز.
- توفير طابعات .
- أجهزة الهاتف النقال و الهواتف الرقمية الثابتة.

ثانيا : الإختراق (Haking)

عبارة عن تقنية يتم بها الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، كونه يمثل القدرة على الوصول إلى هدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام

الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير قانونية.

و قد عرفه القانون العربي النموذجي الموحد في جرائم إساءة إستخدام تقنية المعلومات بأنه : " الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات و ذلك عن طريق إنتهاك الإجراءات الأمنية."

و عملية الإختراق الإلكتروني تتم عن طريق تسريب البيانات الرئيسية و الرموز الخاصة ببرامج شبكة الإنترنت من أي مكان في العالم ، بحيث لا أهمية للبعد الجغرافي في الحد من الإختراقات المعلوماتية التي لا تزال نسبتها كبيرة ، و منها لم تكتشف بعد بسبب تعقيد نظم تشغيل الحاسبات الإلكترونية و الشبكات المعلوماتية.

1/أنواع الإختراق:

لهذا الأسلوب التقني الإجرامي أنواع تتمثل في :

أ-إختراق مزودات الخدمة أو الأجهزة الرئيسية للشركات أو المؤسسات أو الجهات الحكومية ، عن طريق إختراق الجدران النارية الموضوعة لحمايتها و الذي غالبا ما يتم بإستخدام المحاكاة الممثلة لمصطلح يطلق على إنتحال شخصية للدخول إلى النظام.

ب-التعرض للبيانات أثناء إنتقالها و التعرف على شفرتها من أجل كشف كل من بطاقات الإئتمان و الأرقام السرية للبطاقات البنكية.

ج-إختراق الأجهزة الشخصية و هي الطريقة الأكثر شيوعا ، نظرا لتوفر العديد من برامج الإختراق سهلة الإستخدام.

2/وسائل الإختراق :

يتم إختراق جهاز الضحية دون علمه عن طريق عدة أدوات ووسائل منها:

أ-الإختراق بإستعمال نظم التشغيل المليئة بالثغرات من خلال البروتوكولات التي يستخدمها نظام التعامل مع شبكة الإنترنت ، فيقوم المخترق بالبحث عن ضحية من خلال معرفة رقم IP (Internet Protocol) الخاص به.

ب- الإختراق بإستخدام البرامج و هي الطريقة التي تتطلب وجود برنامجين ، حيث الأول يسمى برنامج الخادم Server الموجود في جهاز الضحية و الثاني يسمى بالبرنامج المستفيد العميل Client الموجود بجهاز المخترق ، و من أخطرها برنامج حصان طروادة المتميز

بالقدرة على الإختراق دون إمكانية كشفه و لا تتبعه و حذفه من البرنامج المصاب ، الذي بمجرد عمله لمرة واحدة يسهل له القيام بمهامه و يمكن إرساله للضحية عن طريق الرسائل الإلكترونية و إستخدام برامج الدردشة.

ج–الإختراق بإستخدام أسلوب التفتيش عن مخالفات التقنية ، بالبحث في مخالفات الحواسب من قمامات و مواد متروكة عل مستوى الجهاز تسهل إختراق النظام مثل البرامج المدون عليها كلمة السر أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة.

د– الإختراق بإستعمال أسلوب المحاكاة بواسطة التخفي بإنتحال شخصية و صلاحيات شخص يمكنه الدخول إلى نظم المعلوماتية بإستخدامه وسائل التعريف الخاصة به.

هـ–الإختراق باللجوء إلى إنتحال شخصية الموقع عن طريق قيام المخترق بوضع نفسه في موقع بيني، بين البرنامج المستعرض للحاسب الخاص بأحد مستخدمي الإنترنت و بين الموقع (WEB) ، و به يتمكن من خلال جهاز حاسوبه مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع و بين الموقع نفسه ، و بالتالي سرقتها أو تغييرها.

و– الإختراق بواسطة تشمم كلمات السر و جمعها و إلتقاطها، عن طريق إستخدام برمجيات يمكنها تشمم أو إلتقاط كلمات السر خلال تجوالها في جزء من الشبكة أو أحد عناصرها و مراقبتها و متابعتها لحركة الإتصال على الشبكة.

ن–الإختراق بواسطة المسح و النسخ الذي هو عبارة عن أسلوب يستخدم فيه برنامج الماسح ، و هو برنامج إحتمالات يقوم على فكرة تغيير التركيب أو تبديل إحتمالات المعلومة المتعلقة بكلمة السر أو رقم هاتف الموزع .

فقد تستخدم قائمة الإحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصول إلى ما يستخدمه الموزع ، أو إجراء مسح لإحتمالات عديدة لكلمة السر للوصول للكلمة الصحيحة التي تمكن المخترق من الدخول للنظام.

ر–الإختراق بواسطة هجومات إستغلال المزايا الإضافية و التي هي عبارة عن أسلوب لا يمكن مخترق النظام من تدمير معطيات المستخدم و التلاعب بها فقط ، و إنما يسهل له تدمير مختلف ملفات النظام حتى الغير متصلة بالمدخل الذي دخل منه، لأنه إستثمر المزايا الإضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله.

ز-الإختراق عن طريق إستراق الأمواج و الهندسة الإجتماعية ، حيث يتم إستراق الأمواج بإستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم المختلفة ، كالتقاط كل من موجات شاشات الكمبيوتر الضوئية أو الموجات الصوتية من أجهزة الإتصال.

أما الهندسة الإجتماعية فهي تسمية لأسلوب شخصي في الحصول على معلومة الإختراق ، و ليس لها أي أبعاد تقنية حيث يلجأ المخترق فيها لإستعمال أسلوب الكذب و الخداع للحصول على معلومات ذات طابع تقني ، مثل الحصول على كلمة المرور أو سر النظام عن طريق إيهام الضحية بأنه شخص مساعد له تابع مثلا لقسم الصيانة أو قسم التطوير، و يحتاج هذه المعلومات التي تمكنه من إرتكاب جريمته.

3/الحماية الفنية من الإختراق :

لكي يتم الحد من عملية الإختراق و ما يترتب عليها من آثار فإنه يتوجب إتباع الطرق المتمثلة في :

أ- إتباع إجراءات وقائية: كإخفاء الملفات المهمة و إغلاقها بكلمات سرية و عدم تركها على الجهاز، بل تحفظ في إسطوانة و تشغل عند الحاجة ، مع ملاحظة أنها إجراءات غير كافية لأنها تجرد المستخدم من منافع الحاسب الآلي.

ب-تثبيت برامج حماية على الحاسب : بحيث تنقسم إلى نوعين الأولى برامج مضادات للفيروسات و الثانية الجدران النارية ، بحيث تقوم الأولى بمراقبة أي ملف يقوم المستخدم بإستخدامه للتأكد من خلوه من الفيروسات مثل فيروس أحصنة طروادة ، أما الثانية فهي برامج صغيرة تثبت داخل النظام من أجل مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الإنترنت ، بحيث تقوم بالسماح أو الإعتراض على دخول هذه البيانات أو خروجها و تنبيه المستخدم بذالك ليقوم بالسماح بذالك أو عدمه.

ج-الإستعانة بخبرات محترفي التسلل : عملية يقم بها المسؤولين عن أمن الحاسبات الآلية و شبكات الإنترنت و كذلك رجال الأمن ، من أجل تطوير نظم الحماية ضد المتسللين لأجهزة الحاسوب و معطياتهم و الذين يملكون مهارات متقدمة و يطورون تقنياتهم للإختراق بشكل مستمر.

ثالثا : الفيروسات (البرامج الخبيثة المدمرة):

ترتكب الجريمة المعلوماتية المتسببة في إتلاف البيانات و البرامج عن طريق برامج مدمرة تقوم بخداع مستخدم الحاسب ، حيث تظهر على شكل برامج مفيدة و آمنة فيؤدي تشغيلها إلى تعطيل الحاسب المصاب و تدمير برامجه .

فهي برمجيات ماكرة يمكن تصنيفها إلى أربعة أنواع رئيسية هي الفيروسات و الدود و أحصنة طروادة و برامج الإنزال إضافة لبرامج القنبلة المعلوماتية ، و هي أنواع يتفق الفقهاء في كل من إنجلترا و الولايات المتحدة على أن المشاكل الناشئة عنها واحدة.

1-الفيروسات :

فيروسات الحواسب موجودة منذ أواخر الثمانينات و يزداد عددها و تأثيرها بإستمرار، و أصلها عبارة عن برامج أعدها شخص أو أشخاص بهدف تخريب و شطب البيانات من ذاكرة الحاسوب ، و هي مبرمجة على أن تعمل من خلال برامج أو برنامج آخر و لها القدرة عل نسخ ذاتها ، و أبرز طرق إنتشارها البريد الإلكتروني أو البرامج المحملة من الإنترنت.

و يمكن تعمد أشخاص معينون نشرها بإضافتها مع ملفات ترسل بالبريد الإلكتروني الذي بمجرد فتحه من المرسل إليه تفتح هذه الملفات و ينتشر الفيروس و يبدأ عمله في التخريب.

أ-تعريفها و خصائصها : الفيروسات هي برامج يتم إنتاجها خصيصا لكي تلحق نفسها ببعض البرامج المشهورة عن طريق تزييف أو تعديل بسيط للتوقيع الخاص بالبرنامج الأصلي المتمثل في مجموعة الأرقام الثنائية ، و تتمكن هذه البرامج من تدمير البرامج و المعلومات أو إصابة الأجهزة بالخلل بعدة طرق ، فمنها ما يبدأ بالعمل مباشرة عند الإصابة ، و بعضها عند تنفيذ بعض الأوامر، متميزة بقدرتها عل التكاثر و الإنتقال من جهاز إلى آخر عن طريق الملفات المتبادلة بين المستخدمين.

و فيروسات الحاسب الآلي عبارة عن برامج خبيئة تسلسل إلى البرمجيات بحيث تدخل إليها و تنسخ نفسها على برامج أخرى وهذا من أجل التخريب وبالتالي الحصول على منافع شخصية، و تكون هذه الفيروسات مخزنة على البرامج التطبيقية و برامج التشغيل و تنشط في حالة نسخ البرامج من جهاز إلى أخر و عن طريق شبكة الانترنت انطلاقا من رسائل البريد الالكتروني و الوثائق و المعلومات التجارية و المالية المنقولة عبر شبكة الانترنت.

و عند الحديث عن الفيروس المعلوماتي فإننا نقصد الفيروس المتعلق بالحاسب الآلي و المتعلق بالإنترنت المختلفين عن بعضهما من حيث الإنتشار و الدور، بحيث يتميز فيروس

الإنترنت بإنتشاره الكبير و المستمر رغم إغلاق الحاسب أو النظام كله ، كما أنه يقوم بدور المخرب و المختلس للمعلومات خلافا لفيروس الحاسب الآلي الذي يقتصر دوره على التخريب فقط ، كما أن له قدرة أكبر من قدرة الحاسب الآلي بحيث يقوم بدوره طالما كانت شبكة الإنترنت تعمل و لو تم إغلاق أجهزة الحاسب ، بعكس فيروس الحاسب الذي يبقى في الجهاز المصاب به و لا ينتقل إلى الجهاز الآخر إلا بالعدوى عن طريق ملف أو برنامج من الجهاز المصاب أو عن طريق القرص المرن أو الصلب أو القرص المنضغط أو جهاز USB.

و يتميز الفيروس المعلوماتي بعدد من الخصائص التقنية ، و المتمثلة في كونه عبارة عن برنامج صغير يختفي بسهولة في النظام المعلوماتي و بالتالي يصعب على البرامج المضادة للفيروسات العثور عليه، إضافة لقدرته الهائلة على مهاجمة المكونات المعنوية لجهاز الحاسب الآلي و الشبكات المعلوماتية التي تربطها فيما بينها مما يزيد في قدرته على الإنتشار و السرعة في تنفيذ أهدافه.

ب-أنواع الفيروسات : تتميز الفيروسات بكثرة العدد و التنوع ،لذا لقد حدد الفقه العديد من الفيروسات المختلفة إعتمادا على كل من تكوينها و أهدافها و كذا شكلها و مكانها كالتالي:

1/أنواع فيروسات الحاسب الآلي من حيث تكوينها وأهدافها :

1-فيروس عام العدوى : ينتقل إلى أي برنامج أو ملف بهدف تعطيل نظام التشغيل بكامله.

2-فيروس محدود العدوى : يستهدف مهاجمة نوع معين من النظام و يتميز ببطء الانتشار و صعوبة الاكتشاف.

3-فيروس عام الهدف : يتميز بسهولة إعداده و اتساع مدى تدميره و تندرج تحته أغلب الفيروسات .

4-فيروس محدد الهدف : يقوم بتغيير هدف البرامج دون تعطيلها، و يحتاج إلى مهارة عالية بالتطبيق المستهدف .

2/ أنواع الفيروسات حسب شكلها و مكانها :

1-الفيروس المتعدد الأجزاء: يقوم بإصابة الملفات مع قطاع الإقلاع في نفس الوقت و يكون مدمرا في الكثير من الأحيان إذا لم يتم الوقاية منه.

2-الفيروس المتطور: يتميز بكونه يغير الشفرة كلما إنتقل من جهاز لآخر، و بتطور مضادات الفيروسات يتناقص خطره.

3- الفيروس المختفي : هو فيروس يخفي نفسه بحيث يجعل الملف المصاب سليما لخداع مضادات الفيروسات ، التي أصبح من السهل عليها كشف هذا النوع من الفيروسات.

4- فيروس بدء التشغيل : هو فيروس يصيب قطاع الإقلاع في الجهاز ، مما قد يمنع المستخدم من إقلاع الجهاز و كذا الوصول إلى النظام.

5- فيروس الملفات : هو فيروس عامة ما يصيب البرامج ، و ينتشر بين الملفات الأخرى و البرامج الأخرى عند تشغيله.

3/أنواع أخرى من الفيروسات حسب كثرة عددها المتسارع:

إضافة لأنواع الفيروسات السالفة الذكر فقد أكد البعض بأن الفيروسات كثيرة جدا و لا يمكن حصرها ، إذ أنها آخذة في التزايد بشكل متسارع و أهمها : الفيروسات المقيمة ، الفيروسات النائمة ، الفيروسات الإستعراجية ، فيروسات الثغرات...

ج/ كيفية الإصابة بالفيروسات و الآثار المترتبة على ذلك:

عندما بقوم الفيروس بإصابة برنامج معين فإنه يقوم بربط نفسه في بداية البرنامج أو في منتصفه أو في نهايته ، بحيث يبدأ عمله بإنطلاق عمل البرنامج .

و من الآثار التي يخلفها الفيروس و التي تختلف حسب نوعه ما يلي:

-البطء الشديد في الحاسب مما يجعل التعامل معه مستحيلا.

-عدم القدرة على تشغيل معظم التطبيقات و ظهور رسالة خطأ كلما تمت محاولة تشغيلها.

-إمتلاء القرص بما لا يتناسب مع عدد و حجم الملفات الموجودة عليه.

-مسح الملفات التنفيذية و كذا حذف جميع المعطيات الموجودة داخل القرص الصلب.

-ظهور مربعات حوار غريبة أثناء العمل على الجهاز.

-إضاءة لمبة القرص الصلب أو القرص المرن دون أن تقوم بعملية فتح أو حفظ ملف.

-إصابة أحد أجزاء المكونات الصلبة ، مثل ما يحدث مع فيروس "تشير نوبل" الذي يصيب نظم الإدخال و الإخراج الأساسية مما يؤدي إلى توقف الحاسب بالكامل.

د/الحماية من الفيروسات :

مادامت الفيروسات عبارة عن وسيلة تستخدم لتدمير المعلومات و البيانات و البرامج و تعطيل شبكة المعلومات ، فإنه يتوجب على صاحب الحاسب الآلي و مستعمل الإنترنت سواء كان شخصا طبيعيا أو معنويا ، و خاصة إذا كان معتادا على تبادل الأقراص المرنة و الملفات عبر الإنترنت ، أن يلتزم بإتباع خطوات الحماية المتمثلة فيما يلي :

-توفير برنامج حماية من الفيروسات في جهاز الحاسب الآلي مع ضرورة تحديثه بشكل دوري.

-عدم فتح المرفقات في أي إيميل مجهول المرسل أو في إيميلات أصدقائك إذا كانت تنتهي ب exe أو bat أو أي إمتداد لا تعرفه.

-عدم قبول ملف من شخص مجهول بعكس الشخص المعروف لديك، ففي حالة قبولك ملف منه فافحصه ببرنامج الحماية لأنه قد يكون هو أيضا ضحية للفيروسات.

-وجوب فحص جميع البرامج المنزلة من الإنترنت أو تم تشغيلها من قرص مرن أو CD قبل التشغيل.

-ضرورة الأخذ بالاعتبار كون أن النظام الوحيد الآمن تماما هو المكتوب باليد أو المحفوظ ، لذا من الضروري مراعاة عملية الإحتفاظ دائما بنسخ بديلة للمعلومات المهمة تفعيلا لفكرة الوقاية خير من العلاج.

2- برامج الدودة :

أطلقت سنة 1988 عبر شبكة الانترنت الولايات المتحدة الأمريكية برنامج يعرف بالدودة، و الذي يسبب لأجهزة الحاسب الآلي خلال الشبكة انهيار في قيادة و توجيه الجامعات و المعاهد العسكرية و منشآت الأبحاث الطبية.

و يقوم برنامج الدودة باستغلال أي فجوة في نظام التشغيل كي ينتقل من حاسوب لآخر أو من شبكة لأخرى عبر الوصلات الرابطة بينها، حيث تتكاثر أثناء انتقالها بإنتاج نسخ منها وتسبب بالتخريب الفعلي للملفات و البرامج و نظام التشغيل .

و قد أطلقت هذه الدودة من طرف طالب أمريكي يسمى روبرت موريس بقسم علوم الكمبيوتر بجامعة كورنيل بولاية نيوروك ، حيث قام ببث الدودة لإثبات عدم ملائمة أساليب و وسائل الأمان في شبكات الكمبيوتر ، ولكنه تسبب في تدمير الآلاف من شبكات الحاسب الآلي

المنتشرة في الولايات المتحدة و إعاقة طريق و مسلك الشبكات إضافة لخسائر مالية كبيرة لمواجهة دودة الإنترنت ، لذا أدين بإنتهاك قانون الإحتيال و إساءة إستخدام الكمبيوتر و حكم عليه بالحبس لمدة ثلاث سنوات و بالعمل أربعمائة ساعة في الخدمة الإجتماعية و غرامة مالية تقدر بعشرة آلاف و خمسين دولارا أمريكيا إضافة لتكاليف المراقبة.

و من المهم الإشارة إلى أن الديدان التي تنتشر عن طريق الإيميل ، فإنه يرفق بالرسالة ملفا يحتوي على دودة ، و عندما يشغله المرسل إليه تقوم الدودة بنشر نفسها إلى جميع الإيميلات الموجودة في دفتر عناوين الضحية.

3- حصان طروادة :

جاءت تسميته تأثرا بتلك الأحصنة التي إستعملتها الجنود اليونانية عندما حاصرت مدينة طروادة ، حيث تخفوا داخل أحصنة خشبية عندما أدخلت إلى داخل المدينة فقفزوا منها و تمكنوا من مهاجمة و هزيمة عدوهم .

و بنفس الطريقة يعمل برنامج حصان طروادة ، بحيث يختفي هذا البرنامج داخل برنامج حاسوبي عادي و لكن عند تنفيذه يتسبب في الكثير من المشاكل الناتجة عن نشاطه التدميري و المتمثلة في تعديل البرامج و تزوير المعلومات و محو بعضها .

و مما يميز حصان طروادة كونه يقوم بالتخفي داخل الملفات العادية ، و يحدث ثغرة أمنية في الجهاز المصاب تسهل دخول المخترقين إليه و العبث بمحتوياته ، عن طريق نقل أو محو الهام منها أو إستخدام هوية هذا الجهاز في الهجوم على أجهزة أخرى.

4- برامج الإنزال :

هي برامج صممت لمراوغة مكافحة الفيروسات ، و تعتمد على التشفير غالبا لمنع إكتشافها.

ووظيفة هذه البرامج عادة نقل وتركيب الفيروسات ، فهي تنتظر لحظة حدوث أمر معين على الحاسب الآلي لكي تنطلق و تلوثه بالفيروس المحمول في طياتها.

5- <u>القنبلة المعلوماتية :</u> و تنقسم إلى قسمين الأولى منطقية و الثانية زمنية .

<u>أ/ القنبلة المنطقية :</u> عبارة عن برامج صغيرة يتم إدخالها بطرق غير مشروعة و مخفية مع برامج أخرى ، بهدف تدمير و تغيير برامج و معلومات النظام في لحظة محددة أو في فترة زمنية منظمة عند انجاز أمر معين .

و للقنابل المنطقية فيروس يعمل كالقنبلة إذ يظل في حالة سكون حتى يتم تفجيره في الوقت المناسب ، إذ يظل البرنامج موجودا و لا تأثير له حتى يجد بيانات مخزنة في مكان محدد لها قيمة معينة أو بعد تشغيل البرنامج لعدة مرات معينة و في المرة التالية يبدأ الفيروس في العمل.

و مثالها زرع القنبلة المنطقية التي سوف تعمل عند إضافة سجل موظف بحيث تنفجر لتمحو سجلات الموظفين الموجودة أصلا في المنشأة .

ففي ولاية لوس أنجلس بالولايات المتحدة الأمريكية تمكن أحد العاملين بإدارة المياه و الطاقة من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها ، مما أدى إلى تخريب هذا النظام عدة مرات.

ب/ القنبلة الزمنية : سميت كذلك لقيامها بالعمل التخريبي في وقت محدد سلفا، بحيث تختلف عن القنبلة المنطقية المرتبطة بالقيام بنشاط معين ، أم الزمنية فهي مرتبطة بلحظة زمنية محددة بالساعة و اليوم و السنة.

و مثالها يمكن للمخرب كتابة برنامج وظيفته مسح الكشوفات التي تحمل أسماء الموظفين و بياناتهم اللازمة لدفع رواتبهم قبل إستلام رواتبهم بساعة ، مما يؤدي إلى تأخير عملية الدفع و إرباك أعمال الشركة و الإساءة لسمعتها .

و من أمثلتها الواقعية قيام محاسب خبير في نظم المعلومات بدافع الإنتقام بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة التي يعمل بها و قامت بفصله ، حيث إنفجرت بعد ستة أشهر من رحيله من المنشأة و رتبت إتلاف كل البيانات المتعلقة بها.

المحور السادس: الجهود الدولية و الإقليمية المبذولة لمكافحة الجريمة المعلوماتية:

لقد أثر كل من تطور التكنولوجيا و ثورة المعلومات على كل جوانب الحياة سواء الإقتصادية أو الإجتماعية أو الثقافية أو السياسية بشكل إيجابي رتب التطور و السرعة و قلة التكاليف في كل المجالات ، إلا أنه في نفس الوقت أدى إلى ظهور نتائج سلبية بإستغلال هذه التطورات فيما هو ضار مثل تسهيل إرتكاب الجرائم المعلوماتية.

فبظهور الإنترنت إزدادت الإعتداءات على كل ما يطاله إستخدام الحاسوب من حياة خاصة و أموال و أمن الدولة و إقتصادها ، إضافة للإعتدءات التي طالت الحاسوب نفسه و برامجه التي تم تغييرها و تعديلها و التلاعب بها بأشكال مختلفة.

و هذا ما إستدعى تدخل المشرع لوضع حد لهذا التنامي الخطير في ميدان الإجرام المعلوماتي عن طريق وضع نصوص قانونية موضوعية تجرم و تعاقب على الأفعال التي تشكل إعتداء أو تهديد للأمن المعلوماتي.

و تظهر مكافحة الجريمة المعلوماتية من الناحية الموضوعية و الإجرائية في مختلف الإتفاقيات الدولية التي تم إبرامها في هذا المجال و المقسمة لكل من :

أولا: الجهود الدولية المبذولة لمكافحة الجريمة المعلوماتية.

ثانيا: الجهود الإقليمية المبذولة لمكافحة الجريمة المعلوماتية.

أولا : الجهود الدولية المبذولة لمكافحة الجريمة المعلوماتية.

أولت كل من الأمم المتحدة و أغلب المنظمات الدولية اهتماما خاصا بموضوع الجريمة المعلوماتية تجلى من خلال ما توصلت إليه من إتفاقيات دولية تخص هذا المجال و المتمثلة في كل من اتفاقية برن و معاهدة الويبو و اتفاقية تريبس .

1/ الإتفاقيات الدولية:

❶ **<u>إتفافية برن :</u>** تعتبر إتفاقية برن الموقعة بتاريخ 1971 في سويسرا حجر الأساس في مجال الحماية الدولية لحق المؤلف و وقعت عليها 120 دولة ، بحيث تم تعديلها سنة 1979 و إرتفع عدد الدول فيها إلى 140دولة في 1999 .

و تمنح هذه الإتفاقية صاحب حق المؤلف حق استئثاري في التصريح بعمل نسخ من المصنفات بأي طريقة و بأي شكل كان ، كما تمنحه الحق في أن يرخص أو يمنح أي

ترجمة أو إقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه ، كما تلزم بتوقيع جزاءات سواء كان المؤلف المعتدى عليه وطنيا أو أجنبيا.

و بموجب هذه الإتفاقية تتمتع برامج الحاسب الآلي "الكمبيوتر" سواء كانت بلغة المصدر أو بلغة الآلة بالحماية بإعتبارها أعمالا أدبية وفقا لما جاء فيها.

و تهدف هذه الإتفاقية إلى حماية حقوق المؤلفين على مصنفاتهم الأدبية و الفنية ، التي لها أحكاما خاصة لتحديدها مع توضيح شروط حمايتها.

-المبادئ الأساسية لإتفاقية برن:

و تقوم هذه الإتفاقية الدولية على مجموعة من المبادئ الأساسية التي تحدد نطاق الحماية الواجبة و أسلوب تطبيقها و المتمثلة في :

أ-مبدأ المعاملة الوطنية: أي تمتع كافة المصنفات الخاضعة لحماية الإتفاقية في إقليم دولة عضو بنفس الحماية المتمتعة بها المصنفات الوطنية لدى الدولة الأخرى الطرف في هذه الإتفاقية.

ب-الحد الأدنى للحماية: مبدأ هدفه مواجهة التفاوت التشريعي بين مستويات الحماية في الأنظمة القانونية المختلفة ، و بمقتضاه يتمتع المؤلفون بحقوق مادية و أدبية إنطلاقا من تطبيق المساواة بين الوطني و الأجنبي ، زيادة على وضع حد أدنى يتعين أن لا تقل عنه الحماية التي تلقاها أي من المصنفات المتمتعة بحماية إتفاقية برن.

❷ **معاهدة الويبو :** لتوفير الحماية للملكية الفكرية تم تشكيل المنظمة العالمية للملكية الفكرية "ويبو" التي تعتبر منظمة دولية غير حكومية و إحدى الوكالات المتخصصة التابعة لمنظمة الأمم المتحدة ، مقرها جنيف تأسست بموجب اتفاقية ستوكهولم المبرمة سنة 1967 و دخلت حيز التطبيق 1970 و بلغ عدد الدول الأعضاء فيها سنة 1999 170 دولة .

و تهدف هذه المنظمة لدعم الملكية الفكرية في جميع أنحاء العالم و حماية الملكية الصناعية و كذا حماية المصنفات الأدبية و الفنية .

و تنقسم معاهدة الويبو إلى ثلاث معاهدات الأولى بشأن حق المؤلف و الثانية بشأن الأداء و التسجيل الصوتي و الثالثة بشأن الحماية الدولية لحق المؤلف و الحقوق المجاورة.

وتهدف منظمة الويبو العالمية للملكية الفكرية إلى :

أ–تدعيم إتخاذ الإجراءات التي تهدف إلى تسيير الحماية الفاعلة للملكية الفكرية في جميع أنحاء العالم.

ب–تنسيق التشريعات الوطنية للدول الأعضاء في إطار الحماية الفاعلة للملكية الفكرية على الصعيد العالمي.

ج–تقديم الخدمات الفنية و القانونية و التدريجية في مجال العمل على الحماية الدولية للملكية الفكرية.

د–النهوض بأعباء التسجيل في مجال الحماية الدولية للملكية الفكرية ، و أن تنشر البيانات الخاصة بالتسجيلات حيثما كان ذلك ملائما.

مع ملاحظة أنه لمعاهدة الويبو الخاصة بحماية حق المؤلف دور هام في حماية البرمجيات ، إنطلاقا من مادتها الرابعة التي نصت على تمتع برامج الكمبيوتر بالحماية بإعتبارها مصنفات أدبية بالمعنى الوارد في المادة الثانية من إتفاقية برن.

❸ **<u>إتفاقية تريبس:</u>** هي إتفاقية مجالها حماية الملكية الفكرية من عمليات السطو الإلكتروني على الأعمال الفنية و تم التوقيع عليها من قبل الدول الأعضاء سنة 1994 .

لقد تناولت هذه الإتفاقية تحرير التجارة العالمية مع الأخذ في الإعتبار بأمرين هامين :

–**الأمر الأول:** ضرورة توفير جزاءات و تدابير لإنقاذ حقوق الملكية الفكرية دون أن تقف عائقا أمام التجارة الدولية المشروعة.

–**الأمر الثاني:** العمل على تشجيع الحماية الفاعلة في مجال حقوق الملكية الفكرية بجميع فروعها .

و قد نصت هذه الإتفاقية على مكافحة الجريمة المعلوماتية بالنص من خلال مادتها العاشرة في فقرتها الأولى على أنه تتمتع برامج الحاسب الآلي أو الكمبيوتر سواء كانت بلغة المصدر أو بلغة الآلة بالحماية بإعتبارها أعمال أدبية بموجب معاهدة برن لسنة 1971.

كما نصت ذات المادة العاشرة في فقرتها الثانية على حماية البيانات المجمعة أو المواد الأخرى بشروط معينة.

و لفاعلية هذه المكافحة إشترطت مواد الإتفاقية على الدول الأعضاء لحماية حقوق الملكية :

المادة 41: إتخاذ إجراءات سريعة لمنع التعديلات و الإنتهاكات الحالة.

المادة 42: ضرورة توافر إجراءات قضائية و مدنية إلى جانب إجراءات إدارية أخرى.

المادة 09: على الدول الأعضاء الإلتزام بأحكام المواد من 01 إلى 21 من معاهدة برن لسنة 1971 ، مع مراعاة سريان الحماية على المنتوج و ليس على مجرد الأفكار أو الإجراءات أو أساليب العمل و الحماية الزمنية لعديد المصنفات المحددة بطول حياة المؤلف بالإضافة إلى مدة خمسين عاما بعد وفاته.

-المبادئ الأساسية لإتفاقية تريبس:

و تقوم هذه الإتفافية على عدة مبادئ تتمثل في :

أولا : مبدأ المعاملة الوطنية: ألزمت المادة الثالثة من الإتفاقية كل دولة عضو بأن تمنح الأجانب المنتمين إلى دولة أخرى من الدول الأعضاء معاملة لا تقل عن تلك الممنوحة لمواطنيها في شأن حماية الملكية الفكرية.

ثانيا: مبدأ الدولة الأولى بالرعاية: أوجبت المادة الرابعة من الإتفاقية على الدول الأعضاء أن تمنح المنتمين إلى كافة الدول فورا و بدون أية شروط ،أية مزايا ، أو حصانات أو معاملة تفضيلية تمنحها للمتمين إلى أي دولة أخرى متعلقة بحماية حقوق الملكية الفكرية .

ثالثا:وضع حد أدنى من الحماية القانونية: مكنت الإتفاقية أي دولة عضو من تقديم حماية قانونية تفوق الحماية المقدرة في إتفاقية تريبس ، و لكن لا يجوز لها أن تقرر حماية أدنى مما قررته الإتفافية.

رابعا: وقت إنفاذ إتفاقية تريبس : بسبب كون الدول الصناعية المتقدمة المتضررة الأولى من قرصنة الملكية الفكرية ، فقد حاولت إجبار العديد من الدول النامية لتطبيق الإتفاقيات و الحد من القرصنة و التزوير و التقليد ، و لكنها لم تتوصل إلى عقد إتفاقية تريبس بسبب ما يتطلبه الأمر من مرونة في إلزام الدول بأحكامها التي يتطلب تطبيقها فترات زمنية إنتقالية.

خامسا : المعاملة التفضيلية للدول النامية : أرادت إتفاقية تريبس من خلالها تمكين الدول النامية من إنشاء قاعدة تكنولوجية متطورة تخدم مصالحها الإقتصادية و تمكنها من اللحاق بعجلة التجارة الدولية.

2/عمل المنظمات الدولية في مكافحة الجريمة المعلوماتية:

لقد تمت مكافحة الجريمة المعلوماتية من خلال دور الإتفاقيات الدولية على المستوى الدولية، إضافة لدور المنظمات العالمية في مكافحتها مثل منظمة الأمم المتحدة في جهودها المبذولة مثل:

-تقرير لها بعنوان " إقتراحات المواجهة الدولية تجاه صور تطور الجريمة سنة 1987.
-إجتماعها عام 1990 لمناقشة مشروع لحلول مشكلة الجريمة المرتبطة بالحاسب الآلي ، مركزة على أهمية جهود الدول الأعضاء لضبط جرائم المعلوماتية لما لها من آثار سلبية و ضيقة على الأفراد و المجتمع.
-مؤتمر " ريودي جانيرو" الدولي الخامس عشر للجمعية الدولية لقانون العقوبات المنعقد بتاريخ 1994/09/04 الذي أرسى جانبا هاما من المبادئ العامة المتعلقة بالقانون الإجرائي الخاص بالجرائم المعلوماتية.

ثانيا : الجهود الإقليمية المبذولة لمكافحة الجريمة المعلوماتية:

تبرز هذه الجهود الإقليمية من خلال مساعي المجلس الأوروبي الذي برز دوره لمكافحة هذه الجريمة في الحفاظ على كل ما يتعلق بالحياة الخاصة ، إضافة لجهود جامعة الدول العربية من خلال إعتمادها على قانون الإمارات العربي الإسترشادي لمكافحة جرائم تقنية المعلومات و الإتفافية العربية لمكافحة الجريمة المعلوماتية.

1/معاهدة بوادست (معاهدة اقليمية) :

شهدت العاصمة المجرية بودابست في أواخر عام 2001 أولى المعاهدات الدولية التي تكافح الجرائم الإنترنت و تبلور التضامن و التعاون الدولي في محاربتها، و محاولة الحد منها خاصة و أن هذه الجرائم أصبحت تهدد الأملاك و الأشخاص.

و قد قام بصياغتها عدد كبير من الخبراء القانونيين في مجلس أوروبا بمساعدة دول أخرى، لاسيما الولايات المتحدة الأمريكية بعد مشاورات عديدة بين الحكومات و أجهزة الشرطة و قطاع الكمبيوتر على مستوى العالم، وصولا في النهاية للتوقيع عليها من قبل 30 دولة بتاريخ 2001/11/23 لمواجهة ما يسمى بالجرائم المعلوماتية.

و رغم أن هذه المعاهدة أوروبية الميلاد إلا أنه تم التوقيع عليها من قبل دول لا تعتبر أعضاء في مجلس أوروبا مثل كندا و اليابان و الولايات المتحدة الأمريكية و جنوب إفريقيا. تكونت هذه الاتفافية من 48 مادة تؤكد من خلالها على ضرورة اتخاذ تدابير تشريعية لمكافحة جرائم الحاسوب و مخاطرها على الدول، كما تضمنت العديد من التوصيات للدول الأعضاء من أجل محاربة الجريمة المعلوماتية بإعتبارها مرجعا في ميدان محاربة الإجرام

السيبيري ، سواء بالنسبة للإتفاقيات اللاحقة ذات الصلة بها أو بالنسبة للتشريعات الداخلية لبعض الدول.

-العناصر الأساسية لاتفاقية بودابست :

1/ أهمية التدابير التشريعية الموضوعية أي نصوص التجريم الموضوعة لهذا المجال

2/ أهمية التدابير التشريعية الإجرائية المتلائمة مع طبيعة الجرائم الإلكترونية.

3/أهمية تدابير التعاون الدولي و الإقليمي في مجال مكافحة هذه الجرائم و الانطلاق مما أنجز من جهود دولية و إقليمية في هذا المجال .

-فصول اتفاقية بودابست :

الفصل الأول : تضمنت مواده تعريف للمصطلحات الأساسية .

الفصل الثاني : عنوانه الخطوات الواجب اتخاذها على الصعيد الوطني و يضم ثلاثة أقسام

القسم الأول : يتضمن المواد من 2 إلى 13 و التي تعالج النصوص الموضوعية لجرائم الحاسوب .

القسم الثاني : يتكون من المواد 14 إلى 21 و التي تتعلق بالقواعد الاجرائية .

القسم الثالث : يتكون من المادة 22 و يتعلق بالاختصاص .

الفصل الثالث : عنوانه التعاون الدولي و يضم المواد من 23 إلى 35

الفصل الرابع : يتضمن الأحكام الختامية و يضم المواد من 36 إلى 48 .

-تصنيف الجرائم المعلوماتية في الاتفاقية: تم من خلال 5 عناوين في قسمها الأول تتمثل في:

الطائفة الأولى: الجرائم التي تستهدف عناصر أمن المعلومات :

تضم جوهر جرائم الحاسوب والتي تعرف بالجرائم ضد سرية البيانات وسلامتها و سلامة النظام و إتاحة البيانات و النظم .

الطائفة الثانية:الجرائم المرتبطة بالكمبيوتر:

تضم الانتهاكات الممارسة بواسطة الحاسب الآلي التي تمس بعض المصالح القانونية التي تحميها قوانين العقوبات، و تضم أيضا جرائم الغش المعلوماتي و التزوير المعلوماتي .

الطائفة الثالثة:الجرائم المرتبطة بالمحتوى:

تشمل الإنتهاكات و الجرائم المرتبطة بالمحتوى و التي تخص الإنتاج و النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية .

الطائفة الرابعة: الجرائم المرتبطة بحق المؤلف و الحقوق المجاورة :

تشمل الجرائم الجنائية التي تعد إعتداء على المصنفات المحمية بحق المؤلف و الحقوق المجاورة.

الطائفة الخامسة: المساهمة الجرمية و العقوبة :

بها أحكام إضافية تخص عملية الشروع و الاشتراك في هذه الجرائم و كذا الجزاءات و التدابير طبقا للمعايير الدولية الحديثة بالنسبة لمسؤولية الأشخاص المعنوية .

-أنواع الجرائم الإلكترونية التي تضمنتها تصنيفات إتفاقية بودابست:

أوجبت الإتفاقية نوع جديد من التقسيمات بشأن جرائم الكمبيوتر المختلفة و أحكامها (القواعد الموضوعية)، بحيث تتضمن أربع طوائف رئيسية لجرائم الكمبيوتر و أخرى خامسة تتعلق بأحكام المساهمة و العقوبات لهذه الجرائم الأربعة، بحيث تقسم هذه الطوائف إلى تسع جرائم في ميدان الجرائم المعلوماتية تلزم الإتفاقية الدول الأعضاء فيها و أي دولة توقع عليها أو تريد الإنضمام إليها بإتخاذ الإجراءات و التدابير التشريعية الملائمة بتجريمها.

الطائفة الأولى: الجرائم التي تستهدف عناصر أمن المعلومات: و تشمل على:

1/جريمة الدخول غير القانوني المتعمد: مصطلح إستعملته الإتفاقية في حين أن غالبية التشريعات الوطنية تستخدم تعبير الدخول غير المصرح به ، و ذلك بالدخول المتعمد إلى نظام كمبيوتر أو جزء منه دون حق أو إذن سواء كان بنية إنتهاك وسائل الأمن أو بنية الحصول على معطيات الكمبيوتر أو لأية نية غير مشروعة.

2/جريمة الإعتراض غير القانوني : المتعمد و دون حق بواسطة وسائل تكنولوجية للبيانات المرسلة غير العامة إلى أو من نظام كمبيوتر، و كذلك إعتراض الإشعاعات الكهرومغناطيسية المنبعثة من أي نظام كمبيوتر تحمل هذه المعطيات.

3/جريمة التدخل المتعمد أو الإرادي في المعطيات: بالتدمير أو الحذف أو التشويه و الإفساد أو تبديلها أو تغييرها أو تعديلها أو تعطيلها أو كبتها أو إخمادها.

4/جريمة التدخل المتعمد في نظم الحاسوب: عن طريق إرسال ذات الأفعال المشار إليها في المادة الرابعة من الإتفاقية و المتعلقة بالتدخل في المعطيات من أجل تعطيل أداء و عمل الأنظمة بالتدمير و الحذف و التعديل و التعطيل.

5/جريمة إساءة إستخدام الأجهزة : و هي جريمة تحتوي نوعين من الأفعال ،النوع الأول يتعلق بالأفعال المنصوص عليها في الفقرة الأولى من المادة السادسة، و تشمل الإنتاج المتعمد أو بيع أو شراء أو إستخدام أو إستيراد أو توزيع أو غير ذلك أدوات ووسائل توفير الأجهزة بما فيها برامج الكمبيوتر لإرتكاب أي جريمة من المذكورة في المواد من 2 إلى 5 السالفة الذكر، و كذلك كلمات السر و رموز الدخول أو أية برامج مشابهة تتيح إختراق نظام الكمبيوتر و الدخول إليه أو أي جزء منه بنية إرتكاب أي جرم من الجرائم المذكورة في المواد من 2 إلى 5 السالفة الذكر.

كما تشمل هذه الجريمة وفق الفقرة الثانية من المادة السادسة الحيازة و التملك لأي عنصر أو أداة لإرتكاب أي من الأفعال المشار إليها في المواد من 2 إلى 5 من الإتفاقية.

الطائفة الثانية: الجرائم المرتبطة بالكمبيوتر: و تشمل على:

1/جريمة التزوير المتعمد بإستخدام جهاز الكمبيوتر: عن طريق إدخال أو تعديل أو حذف أو إخفاء بيانات الكمبيوتر على نحو يظهر بيانات غير أصلية و كأنها أصلية و قانونية بغض النظر عن كونها مقروءة أو غير مقروءة.

2/جريمة الإحتيال المتعمد بإستخدام الكمبيوتر: بدون حق و على نحو يسبب خسارة الغير لممتلكاته عن طريق إدخال أو حذف أو تعديل أو كتم بيانات الكمبيوتر، أو من خلال التنقل بعمليات نظام الكمبيوتر أو برامجه بنية الحصول على منفعة إقتصادية لنفسه أو لغيره.

الطائفة الثالثة: الجرائم المرتبطة بالمحتوى: و تشمل على:

-**الجرائم المرتبطة بدعارة الأطفال:** و هي جرائم كثيرة المحتوى ترتكز على ضرورة تجريم أي شخص و بشكل عمدي عرض أو توزيع أو نقل أو غير ذلك من الأفعال التي توفر أو تتيح توفير المواد الإباحية المتعلقة بالأطفال.

الطائفة الرابعة : الجرائم المرتبطة بحق المؤلف و الحقوق المجاورة: و تشمل على:

-**الجرائم المرتبطة بحق المؤلف:** تناولت الإتفاقية وجوب إتخاذ الدول المنظمة لها تدابير تشريعية تجرم الإخلال أو الإعتداء على حق المؤلف أو الحقوق المجاورة وفقا لمدة تحددها

القوانين الوطنية للدول الأعضاء المتوافقة مع إتفاقية برن لحماية المصنفات الأدبية و الفنية، و إتفاقية تريبس و إتفاقية الويبو لحق المؤلف و إتفاقية الأداء و المنفوغرامات ، بشرط أن تكون هذه الأفعال قد ارتكبت عمدا و بغرض تجاري و بإستخدام نظام الكمبيوتر.

الطائفة الخامسة : المساهمة الجرمية و العقوبة: ويعالج هذا الجزء كل من :

1/الشروع و المساعدة و التحريض: أوجبت الإتفاقية على الدول الأعضاء إتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع و التدخل و التحريض في إرتكاب هذه الجرائم و ما تتخذه من إجراءات ردعية.

2/ مسؤولية الأشخاص المعنوية: نصت الإتفاقية على مسؤولية الأشخاص المعنوية على الأفعال التي ترتكب لمصلحة الشخص المعنوي ، من قبل أي شخص الذي يتصرف لمصلحته سواء كان إستنادا إلى تمثيل قانوني أو بإعتباره مناطا به إتخاذ القرار عن الشخص القانوني ، أو لأنه خاضع لسلطته بما في ذلك أفعال التحريض و التدخل و المساعدة الجنائية.

3/ معايير العقاب: أوجبت الإتفافية على الدول الأعضاء فيها إقرار العقوبات الملائمة و الفعالة لهذه الجرائم ، بما فيها العقوبات المانعة للحرية بالنسبة للأشخاص الطبيعيين مثل ماهو الحال في القانون الأمريكي و الغرامات المالية للأشخاص المعنوية.

-الشروط الواجب توفرها في الأفعال لكي تأخذ وصف الجريمة المعلوماتية :

1/ أن ترتكب الجرائم المذكورة في الاتفاقية دون وجه حق .

2/ أن ترتكب الجرائم المذكورة بطريقة عمدية من أجل إقرار المسؤولية الجنائية .

-الإلتزامات المفروضة من قبل إتفاقية بودابست على الدول الأعضاء :

أكدت الاتفاقية على الدول عند وضعها لتشريعاتها الداخلية الخاصة بالجرائم المعلوماتية مراعاة الاتفاقيات الدولية لحقوق الإنسان، مثل الاتفاقية الأوروبية لحماية حقوق الإنسان و الحريات الأساسية لعام 1950، و الميثاق الدولي للحقوق المدنية و السياسية لسنة 1966، و كذلك الاعتماد على معايير معينة لتقرير الاختصاص القضائي حول الجرائم المقررة في هذه الاتفاقية و المتمثلة في مبدأ الإقليمية و مبدأ نسبية الاختصاص المكاني و مبدأ الجنسية.

-أهداف اتفاقية بودابست :

1/السعي لتحقيق وحدة التدابير التشريعية بين دول الأوروبية و دول المنظمة لهذه الاتفاقية من غير الدول الأوروبية.

2/ التأكيد على أهمية التعاون الدولي و الإقليمي في ميدان مكافحة الجرائم الالكترونية، و إيجاد مرجعية و دليل إرشادي للتدابير التشريعية الوطنية في ميدان مكافحة الإجرام الإلكتروني.

3/ ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية و سلامة و توفر المعلومات و أنظمة الكمبيوتر و شبكاته، و أنشطة إساءة استخدامها بما في ذلك تحديد الإطار الموضوعي لهذه الأنشطة و الإطار الإجرائي لها.

4/ تحقيق التوازن بين حماية حقوق الإنسان الأساسية المعترف بها بموجب اتفاقية مجلس أوروبا لحماية حقوق الإنسان و حرياته لعام 1950 والعهد الدولي للحقوق المدنية و السياسية لعام 1966، و الاتفاقيات الأخرى الدولية الخاصة بالحقوق المتصلة بالرأي و حرية الوصول إلى المعلومات و حرية البحث و التلقي و النقل للمعلومات والأفكار،و مراعاة الحق في الخصوصية و حيازة المعلومات و الاستفادة من عناصر الملكية الفكرية.

فهي معاهدة تسعى لإحترام حقوق الإنسان و الحد من تعرضه لجرائم الإنترنت.

-<u>الاجراءات الجنائية الجديدة لمكافحة الجريمة الالكترونية في اتفاقية بودابست :</u>

وضعت هذه الاتفاقية مجموعة من الإجراءات الجديدة التي تقوم على مبدأ أساسي يتمثل في التزام الدول الأعضاء بإقرار الإجراءات التشريعية، و إجراءات أخرى عند الضرورة بما بتناسب مع قوانينها الداخلية و مجالها القضائي و المتمثلة خاصة فيما يلي :

1/**<u>الحفظ السريع للمعطيات المخزنة :</u>** إجراء نصت عليه المواد 16 و 17 من الاتفاقية، و يقصد به الاحتفاظ بالمعلومات السابقة و تخزينها مع حمايتها مما يفسدها أو يتلف نوعيتها و هو إجراء قانوني جديد لكشف الجريمة المعلوماتية و المرتكبة بواسطة شبكة الانترنت.

وسبب إستحداث هذا الإجراء الجديد هو سرعة تغير البيانات المعلوماتية و فاعليتها للتلاشي و التلاعب بها بمحوها أو تدميرها، فيسهل فقدان أدلة إرتكاب الجريمة المعلوماتية ، لذا أكدت المادة 16 من الاتفاقية على تمكين السلطات الوطنية المختصة من إصدار أمر بحفظ البيانات عن طريق أمر قضائي أو أمر إداري أو أي طريق مماثل للتفتيش أو إصدار أمر بالاطلاع .

2/ تجميع المعلومات الخاصة بالمشتركين : نصت هذه الاتفاقية على أهمية المعلومات الخاصة بالمشتركين لتحديد هوية الفاعل في الجريمة المعلوماتية، بحيث تتضمن هذه المعلومات حفظ رقم الهاتف أو عنوان البريد الالكتروني أو عنوان الموقع أو .. الخ .

3/ التفتيش المعلوماتي : و قد نصت عليه المادة رقم 19 من الاتفاقية التي بينت أنه يجب توفر شرط الحصول على إذن رسمي للتفتيش، بعد الإعتماد بتوفر بيانات في مكان محدد يساعد على إثبات وقوع جريمة معلوماتية محددة بمقتضى القوانين الداخلية، و تفتيش البيانات المعلوماتية و المعطيات المجمعة بعد الحصول على الإذن الرسمي للتفتيش .

كما نصت المادة رقم 31 على وجوب وجود أحكام إجرائية إضافية لضمان الحصول على البيانات المراد إستعمالها كدليل.

4/ اجراءات التنصت : هو إجراء جديد في إطار المكافحة الإجرائية للجريمة المعلوماتية، و يتميز بأنه خاص قد يمس بحقوق الأفراد الخاصة لذا لا يعتد به كإجراء قانوني إلا إذا اتخذ بموافقة السلطات القضائية ، و مفاده اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية كالخطوط الهاتفية مثلا، و وضع الترتيبات التقنية بدون موافقة المعنيين من أجل التقاط اتصالات و تسجيلات كلامية لشخص أو عدة أشخاص في أماكن عمومية أو خاصة أو التقاط صور لشخص أو عدة أشخاص يتواجدون في أماكن خاصة ، وذلك كله من أجل التحري و الوصول إلى أدلة تثبت قيام جريمة معلوماتية .

5/ التعاون الدولي : لتفعيل الإجراءات السابقة نصت الاتفاقية في مادتها 23 على ضرورة تعاون الدول فيما بينها في أوسع نطاق ممكن لكشف هذا النوع من الجرائم مع مراعاة تقليل الصعوبات التي تواجه تبادل المعلومات و الأدلة حتى تتم بصورة سريعة على المستوى الدولي .

كما قامت هذه الاتفاقية بتحديد المفهوم العام لإلتزام التعاون الدولي في مجال الجرائم المعلوماتية، و كذا الأحكام الخاصة بتسليم المجرمين و أحكام خاصة و شروط أخرى في حالات جرائم معلوماتية معينة .

6/**الطابع التوجيهي الملزم لهذه الاتفاقية** : نصت عليه المادة 2 منها و التي أقرت أنه يلتزم كل عضو فيها بإصدار تشريع و اتخاذ الإجراءات الضرورية لكشف الجريمة و تطبيق الجزاءات المقررة قانونا في حالة الارتكاب المعدي لها .

7/التأكيد على التحديد الدقيق للمصطلحات الجديدة : أثارت هذه الاتفاقية مشكلة تحديد المصطلحات القانونية المستعملة في مجال المكافحة الإجرائية للجريمة المعلوماتية، من حيث كونها تستعمل المصطلحات المستعملة في الجرائم التقليدية كمصطلح التفتيش و الضبط أو تستخدم مصطلحات جديدة تتماشى مع ما يحدث من تطور تكنولوجي.

وكنتيجة تعد اتفاقية بودابست المنعقدة سنة 2001 بمثابة إرساء لإتفاق دولي يمثل رؤية موحدة للإجرام التقني أو المعلوماتي و إحاطته بسياج قانوني يسمح بالتعامل معه و مواجهته.

2/ إتفافية المجلس الأوروبي لسنة 2004:

تعد إتفافية الجرائم المعلوماتية للمجلس الأوروبي من أحدث الإتفاقيات لمكافحة الجريمة المعلوماتية على المستوى الدولي، و التي صدرت عن المجلس الأوروبي بعد أن وقعت عليها 32 دولة و دخلت حيز التطبيق بتاريخ 2004/07/01.

-**الجرائم المتناولة من خلال هذه الإتفاقية :** نصت على الجرائم الماسة بالنظام المعلوماتي مبينة أساليب التحقيق فيها ، و المتمثلة في كل من الجرائم المرتكبة ضد سرية و تكامل و توافر البيانات أو نظم الحاسبات كجرائم التدخل و الإختراق عل أجهزة الحاسبات الآلية ، و الجرائم المتصلة بالمحتوى و المتعلقة بالجرائم الخاصة بالإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية ، و الجرائم المتضمنة إنتهاكا لحقوق الملكية الفكرية.

-**الأساليب الإجرائية في هذه الإتفاقية:** تتمثل في :

1-إرساء كل من إجراء التفتيش و ضبط أنظمة الحاسبات الآلية.

2-إجراء الحفظ السريع لبيانات الحاسب المخزونة التي تم جمعها و حفظها فعليا بمعرفة حائز البيانات.

3-إجراء الأمر بإصدار نسخة من البيانات و الذي يمكن السلطات من إجبار الشخص على تقديم بيانات الحاسب المخزنة أو أحد عناوين ISP (Internet Service Provider) المعنية و التي تساهم في التوصل إلى معلومات حول المشترك.

4-إجراء إعتراض بيانات المحتوى و التي تعني إعتراض محتوى الإتصال سواء كان رسالة أو معلومة منقولة.

5-المساهمة في إنشاء وحدة (EUROJUT) و التي مهمتها التعاون بين دول الإتحاد الأوروبي، المجسد بتعاون السلطات القضائية في مكافحة الجريمة المعلوماتية بإصدار إجراء جديد جماعي يتمثل في أمر القبض الأوروبي Mandat d'arrêt Européen الذي يسمح بتسليم المجرم المعلوماتي بسرعة في أي دولة من دول الإتحاد الأوروبي.

3/القانون العربي النموذجي الإسترشادي لمكافحة الجريمة المعلوماتية:

يعد هذا القانون خطوة فعالة في مجال مكافحة الجريمة المعلوماتية خاصة في المجتمعات العربية التي عرفت كغيرها من الدول إنتشار هذه الجريمة العابرة للحدود.

و قد كان هذا القانون ثمرة عمل مشترك قدم بشكل مشروع لمكافحة الجريمة المعلوماتية من قبل كل من مجلس وزراء الداخلية العرب و مجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية.

و قد تم إعتماد هذا القانون النموذجي من قبل مجلس وزراء العدل العرب في دورته 19 بالقرار رقم 495-د-19-2003/10/08 ، و مجلس وزراء الداخلية العرب في دورته 21 بالقرار رقم 417-د-2004/21 .

و يعتبر بمثابة قرار بشأن مشروع قانون عربي إسترشادي لمكافحة جرائم تقنية أنظمة المعلومات و ما في حكمها و يتكون من 27 مادة.

-**الجرائم المدرجة ضمن القانون العربي النموذجي:** تتمثل في :

أولا : جريمة غسل الأموال عبر الوسائط الإلكتروني.

تنص المادة رقم 19 من القانون العربي النموذجي لمكافحة الجريمة المعلوماتية على أنه : " كل من قام بتحويل الأموال غير المشروعة أو نقلها أو تمويه للمصدر غير المشروع لها أو إخفائه أرقام بإستخدام أو إكتساب أو حيازة للأموال ، مع العلم بأنها مستمدة من مصدر غير مشروع أو بتحويل الموارد أو الممتلكات مع العلم بمصدرها غير المشروع و ذلك عن طريق إستخدام الحاسب الإلكتروني أو شبكة المعلومات الدولية بقصد إضفاء الصفة المشروعة على نلك الأموال يعاقب ، و تترك العقوبة وفقا لتقدير كل دولة.

ثانيا: جريمة التزوير المعلوماتي.

نصت المادة رقم 04 من القانون العربي النموذجي الموحد بشأن مكافحة الجريمة المعلوماتية في فقرتها الأولى على أنه : " كل من زور المستندات المعالجة آليا أو البيانات المخزنة في

ذاكرة الحاسوب أو على شريط أو إسطوانة ممغنطة أو غيرها من الوسائط يعاقب ، و تترك العقوبة وفقا لتقدير الدولة..."

كما تضيف ذات المادة في فقرتها الثانية على أنه كل من استخدم المستندات المعالجة آليا مع علمه بتزويرها يعاقب بنفس عقوبة فعل التزوير.

ثالثا : جريمة إختراق النظم المعلوماتية.

تنص المادة رقم 03 من القانون العربي النموذجي الموحد لمكافحة الجريمة المعلوماتية عل أنه : " كل من توصل بطريقة التحايل لإختراق نظم المعالجة الآلية للبيانات يعاقب بالحبس و الغرامة (تترك العقوبة لتقدير كل دولة) ، و إذا نتج عن هذا الفعل محو أو تعديل للبيانات المخزنة بالحبس أو تعطيل تشغيل النظام بسبب تسريب للفيروسات أو غيرها من الأساليب المعلوماتية ، تكون العقوبة الحبس و الغرامة المالية."

و تتحقق جريمة إختراق النظم المعلوماتية بإرتكاب :

أ-كل من جريمة أو البقاء غير المشروع في النظام المعلوماتي بأي وسيلة تقنية كإنتهاك كلمة السر الحقيقية أو عن طريق إستخدام برنامج أو شفرة خاصة.

ب-فعل إعاقة تشغيل نظم معالجة البيانات بفعل التعطيل بأي وسيلة كانت كتسريب الفيروسات.

ج-المحو بإزالة جزء من المعطيات المسجلة على الدعامة الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل أو تخزين المعطيات إلى المنطقة الخاصة بالذاكرة.

د-التعديل و المتمثل في تغيير المعطيات الموجودة داخل النظام و إستبدالها بمعطيات أخرى ، و يتم التلاعب في المعطيات عن طريق إستبدالها أو التلاعب في البرنامج أو إعداده بمعطيات مغايرة تؤدي إلى نتائج غير التي صمم لها البرنامج.

رابعا: السرقة العلمية.

نصت المادة رقم 14 من ذات القانون النموذجي على سرقة المعلومات بتجريم كل من عمليات نسخ و نشر المصنفات الفكرية أو الأدبية أو الأبحاث العلمية أو ما في حكمها إذا ما أرتكب دون وجه حق ، و الحكم بعقوبة الحبس التي يترك تقديرها وفقا لقانون كل دولة و دون الإخلال بالنصوص الخاصة بالملكية الفكرية لكل بلد .

كما حدد هذا القانون النموذجي الإطار التجريمي و العقابي للأفعال التي من شأنها أن تشكل خطرا على المنظومة المعلوماتية أو سلامة نقل البيانات عبر شبكة الإنترنت.

رابعا:الإتفاقية العربية لمكافحة الجريمة الإلكترونية لسنة 2010.

جاءت هذه الإتفاقية العربية التي وافق عليها مجلسي وزراء الداخلية و العدل العرب في إجتماعهما المشترك المنعقد بمقر الأمانة العامة بجامعة الدول العربية بتاريخ 2010/12/21 ، كمبادرة عربية لمكافحة الجرائم الإلكترونية و ذلك في إطار مواكبة الجهود المبذولة على المستوى الدولي ، بهدف تعزيز التعاون بين الدول العربية و تدعيمه في مجال مكافحة جريمة تقنية المعلومات.

و قد أدت هذه الإتفاقية لميلاد قوانين عديدة لمكافحة ما يسمى بالجرائم الإلكترونية في السعودية و الأردن و قطر و الإمارات و العراق و سلطنة عمان ...

و جاءت مضامين الإتفاقية العربية مطابقة لأحكام إتفاقية بودابست خاصة على مستوى القواعد الإجرائية، التي أوجبت على الدول الأطراف ملاءمتها مع قوانينها الوطنية فيما يخص الأبحاث الجنائية لتدابير التحفظ على بيانات الكمبيوتر المخزنة و كشفها و إصدار أوامر.

-الجرائم المدرجة ضمن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

لقد ألزمت هذه الإتفاقية كل دولة طرف بتجريم الأفعال المبينة في الفصل الثاني منها المعنون بالتجريم ، و ذلك وفقا لتشريعاتها و أنظمتها الداخلية على النحو التالي:

1/جريمة الدخول غير المشروع:

1-الدخول أو البقاء و كل إتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الإستمرار به.

2-شدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الإتصال أو الإستمرار أو بهذا الإتصال:

أ-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة و للأجهزة و الأنظمة الإلكترونية و شبكات الإتصال و إلحاق الضرر بالمستخدمين و المستفيدين .

ب-الحصول على معلومات حكومية سرية.

2/جريمة الإعتراض غير المشروع:

الإعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية و قطع بث أوإستقبال بيانات تقنية المعلومات.

3/جريمة الإعتداء على سلامة البيانات:

1-تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا و بدون وجه حق.

2-للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في القرة(1) من هذه المادة أن تتسبب بضرر جسيم.

4/جريمة إساءة إستخدام وسائل تقنية المعلومات:

1-إنتاج أو بيع أو شراء أو إستيراد أو توزيع أو توفير :

أ-أية أدوات أو برامج مصممة أو مكيفة لغايات إرتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب-كلمة سر نظام معلومات أو شيفرة دخول أو معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد إستخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

2-حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد إستخدامها لغايات إرتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

5/ جريمة التزوير:

إستخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، و بنية إستعمالها لبيانات صحيحة.

6/جريمة الإحتيال:

التسبب بإلحاق الضرر بالمستفيدين و المستخدمين عن قصد و بدون وجه حق بنية الإحتيال لتحقيق المصالح و المنافع بطريقة غير مشروعة ، للفاعل أو للغير ، عن طريق:

1-إدخال أو تعديل أو محو أو حجب المعلومات و البيانات.

2-التدخل في وظيفة أنظمة التشغيل و أنظمة الإتصالات أو محاولة تعطيلها أو تغييرها.

3-تعطيل الأجهزة و البرامج و المواقع الإلكترونية.

7/جريمة الإباحية:

1-إنتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو إستيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.

2-شدد العقوبة على الجرائم المتعلقة بإباحية الأطفال و القصر.

3-يشمل التشديد الوارد في الفقرة(2) من هذه المادة ، حيازة مواد إباحية الأطفال و القصر أو مواد مخلة بالحياء للأطفال و القصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

8/الجرائم الأخرى المرتبطة بالإباحية:

المقامرة و الإستغلال الجنسي.

9/جريمة الإعتداء على حرمة الحياة الخاصة:

الإعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.

10/ الجرائم المتعلقة بالإرهاب و المرتكبة بواسطة تقنية المعلومات:

1-نشر أفكار و مبادئ جماعات إرهابية و الدعوة لها.

2-تمويل العمليات الإرهابية و التدريب عليها و تسهيل الإتصالات بين التنظيمات الإرهابية.

3-نشر طرق صناعة المتفجرات و التي تستخدم خاصة في عمليات إرهابية.

4-نشر النعرات و الفتن و الإعتداء على الأديان و المعتقدات.

11/الجرائم المتعلقة بالجرائم المنظمة و المرتكبة بواسطة تقنية المعلومات:

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

2-الترويج للمخدرات و المؤثرات العقلية أو الإتجار بها.

3-الإتجار بالأشخاص.

4-الإتجار بالأعضاء البشرية.

5-الإتجار غير المشروع بالأسلحة.

12/الجرائم المتعلقة بإنتهاك حق المؤلف و الحقوق المجاورة:

إتنهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف ، و ذلك إذا ارتكب الفعل عن قصد و لغير الإستعمال الشخصي ، و إنتهاك الحقوق المجاورة لحق المؤلف ذات

الصلة كما هي معرفة حسب قانون الدولة الطرف ، و ذلك إذا ارتكب الفعل عن قصد و لغير الإستعمال الشخصي.

13/جريمة الإستخدام غير المشروع لأدوات الدفع الإلكترونية:

1-كل من زور أو إصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الإلكترونية بأي وسيلة كانت.

2-كل من استولى على بيانات أي أداة من أدوات الدفع و استعملها أو قدمها للغير أو سهل للغير الحصول عليها.

3-كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.

4-كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

14/الشروع و الإشتراك في إرتكاب الجرائم :

1-الإشتراك في إرتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية إرتكاب الجريمة في قانون الدولة الطرف.

2-الشروع في إرتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الإتفاقية .

3-يجوز لأي دولة طرف الإحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كليا أو جزئيا.

15/المسؤولية الجنائية للأشخاص الطبيعية و المعنوية:

تلتزم كل دولة طرف مع مراعاة قانونها الداخلي ، بترتيب المسؤولية الجزائية للأشخاص الإعتبارية عن الجرائم التي يرتكبها ممثلوها بإسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصيا.

16/تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات:

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال إرتكابها بواسطة تقنية المعلومات.

المحور السابع : الجهود المبذولة لمكافحة الجريمة المعلوماتية في ظل القانون الجزائري:

نظرا لكون الجريمة المعلوماتية جريمة مستحدثة لم تتناولها النصوص التقليدية للجريمة ، فقد إستقر الفقه على إخضاعها لقوانين الملكية الفكرية لما توفره من حماية جنائية ضد أي تقليد لبرامج الحاسب الآلي بسبب كونها نتاجا ذهنيا و فكريا يخول لصاحبه حقوقا لا يجوز للغير المساس بها.

كما تناولها المشرع الجزائري من خلال تعديل قانون العقوبات الجزائري بموجب القانون رقم 15/04 الذي أدمج في الباب الثاني في الفصل الثالث من الكتاب الثالث قسما سابعا مكرر عنوانه " المساس بأنظمة المعالجة الآلية للمعطيات" ، إضافة لقوانين أخرى لها علاقة بالمعلوماتية.

لذا سنتناول مكافحة المشرع الجزائري للجريمة المعلوماتية في نصوص كل من الملكية الفكرية و نصوص قانون العقوبات و كذا نصوص أخرى على النحو التالي:

أولا: مكافحة الجريمة المعلوماتية في إطار نصوص الملكية الفكرية.

لقد كفل الدستور الجزائري لسنة 1996 و كذا تعديله لسنة 2016 الحقوق الأساسية و الحريات الفردية مع ضمان عدم إنتهاك حرمة الإنسان من خلال العديد من المواد منها المادة رقم 44 التي تنص على :" حرية الإبتكار الفكري و الفني و العلمي مضمونة للمواطن و حقوق المؤلف يضمنها القانون.

لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ و الإعلام إلا بمقتضى أمر قضائي..."

و عند الحديث عن مكافحة الجريمة المعلوماتية في إطار نصوص حق المؤلف نلاحظ على المشرع الجزائري بأنه لم يدرج صراحة برامج الكمبيوتر ضمن المصنفات الخاضعة لحماية حق المؤلف ، إلا أنه أورده على سبيل المثال لا الحصر إنطلاقا من الأمر رقم 17/73 المتعلق بحقوق المؤلف المعدل بموجب الأمر رقم 10/97 المعدل و المتمم بدوره من قبل الأمر رقم 05/03 المتعلق بحق المؤلف و الحقوق المجاورة ، الذي وضع فيه المشرع قائمة المؤلفات المحمية ، حيث أدمج تطبيق الإعلام الآلي ضمن المصنفات الأصلية من خلال مادته رقم 04 التي تنص على أنه : " تعتبر على الخصوص كمصنفات أدبية أو محمية ما يأتي : المصنفات الأدبية المكتوبة مثل :.....و برامج الحاسوب..."

و الملاحظ أن أغلب التشريعات قد أدرجت برامج الكمبيوتر تحت نطاق المصنفات المحمية بحق المؤلف، أي أنها تخضع لنفس الشروط التي تخضع لها المصنفات الأدبية و لذل يجب توفر شرط موضوعي فيها و جوهري هو شرط الإبتكار و آخر شكلي هو الوجود أو التعبير عن البرنامج بواسطة تسميته بالدعامة.

شدد المشرع على العقوبات الناجمة على المساس بحقوق المؤلف لا سيما مؤلفي المصنفات المعلوماتية إنطلاقا من رقم 153 من الأمر رقم 05/03 المتعلق بحق المؤلف و الحقوق المجاورة، و هي عقوبات موجودة في سياق تجريم الإعتداءات على الملكية الفكرية و التي تناولتها المواد من 390 إلى 394 من قانون العقوبات ثم تم نقلها إلى الأمر رقم 10/97 الخاص بحقوق المؤلف.

-الجرائم الواقعة على البرامج في نطاق حق المؤلف:

لقد نص المشرع الجزائري من خلال الأمر رقم 05/03 على جريمة التقليد المتمثلة في نقل مصنف لم يسقط في الملك العام من غير إذن مؤلفه، و التي لم تعرفها قوانين حق المؤلف و إنما إكتفت بتعداد الأفعال المشكلة للتقليد.

فقد عدد المشرع مجموعة من الأفعال الماسة بالمصنفات و حقوق مؤلفيها و جرمها ، و هي الأفعال المكونة لجريمة التقليد و الجرائم الملحقة بها و التي تناولتها المادة رقم 151 التي تنص على وجود جنحة التقليد في الحالات التالية:

1-الكشف غير المشروع عن مصنف أو أداء فني.

2-المساس بسلامة مصنف أو أداء فني.

3-إستنساخ مصنف أو أداء فني بأي أسلوب من الأساليب في شكل نسخ مقلدة أو مزورة.

4-إستيراد نسخ مقلدة أو تصديرها.

5-بيع نسخ مزورة من مصنف أو أداء فني.

6-تأجير مصنف أو أداء فني أو عرضه للتداول.

-العقوبات المقررة لجريمة التقليد:

تضمنتها العديد من المواد التي قسمتها إلى قسمين من العقوبات :

1/عقوبات أصلية : تنقسم بدورها إلى :

أ-العقوبات البسيطة : أوردت المادتان رقم 151 و 152 من الأمر رقم 05/03 لمرتكب جنحة التقليد لمصنف أو أداء فني عقوبة تتمثل في الحبس من ستة أشهر إلى ثلاثة سنوات، و بغرامة من خمسة مائة ألف إلى مليون دينار جزائري سواء كان النشر قد حصل في الجزائر أو خارجها طبقا للمادة رقم 153 من نفس الأمر.

كما نصت المادة رقم 154 على معاقبة الشريك في إرتكاب جريمة التقليد سواء بأعماله أو بوسائله بنفس عقوبة المادة رقم 153.

و تضمنت المادة رقم 156 نفس العقوبة المقررة في المادة رقم 153 لكل من يمتنع عن دفع المكافأة المستحقة للمؤلف.

ب-العقوبة المشددة: شدد المشرع العقوبة في حالة العود إلى ضعف العقوبة المقررة في المادة رقم 153.

2/ عقوبات تكميلية : تتم عن طريق كل من :

أ-الغلق المؤقت: لمدة لا تتعدى ستة أشهر لمؤسسة يستغلها المقلد أو شريكه ، و أن يكون نهائي عند الإقتضاء من طرف محكمة الموضوع.

ب-المصادرة: سواء للمبالغ التي تمثل الإيرادات الناتجة عن الإستغلال غير الشرعي لمصنف أو أداء محمي أو إتلاف العتاد.

و هي مصادرة وجوبية بحيث تؤول الأموال و الوسائل المصدرة للمؤلف أو مالك الحقوق أو ذوي حقوقهما كتعويض عن ما لحقهم من ضرر.

ج-نشر ملحق الحكم : أي التشهير بالمحكوم عليه و التأثير على شخصيته الأدبية و المالية.

و ما يتم مصادرته من نسخ و إيرادات و أقساط تأمر الجهة القضائية المختصة بتسليمها للمؤلف أو لأي مالك للحقوق أو ذويهم ، و ذلك بموجب شكوى لدى الجهة القضائية المختصة من طرف مالك الحقوق أو من يمثله قانونا طبقا للمادة رقم 160 من الأمر رقم 05/03.

ثانيا : مكافحة الجريمة المعلوماتية في إطار نصوص قانون العقوبات و ما عرفه من تعديلات:

تناول المشرع الجرائم الخاصة بأنظمة الحاسوب الآلي إنطلاقا من الأمر رقم 156/66 المتضمن قانون العقوبات المعدل بموجب القانون رقم 04/ 15 المؤرخ في 2004/11/10 المتضمن قسم تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" و المكون من 08 مواد حيث تبدأ من المادة رقم 394 مكرر إلى المادة رقم 394 مكرر07.

و في عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب القانون رقم 23/06 المؤرخ في 2006/12/20 ، حيث مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، و هذا بتشديد العقوبة على هذه الأفعال فقط دون المساس بنصوص القانون رقم 15/04 ، و هذا بسبب الإنتشار الواسع لهذه الجرائم المؤثرة على الإقتصاد الوطني.

كما عرف قانون العقوبات في العام الحالي 2020 تعديل آخر بموجب القانون رقم 06/20 المؤرخ في 2020/04/28 الذي مس العديد من الفصول التي ستوضح لاحقا

إضافة لما عرفته هذه السنة من ظهور للقانون رقم 05/20 المؤرخ في 2020/04/28 و الذي يتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتها و المتضمن إلغاء عدد من مواد الأمر رقم 156/66 المتضمن قانون العقوبات المعدل و المتمم و الذي سنتناوله لاحقا

-أنواع الجرائم الإلكترونية في قانون العقوبات الجزائري:

تناولها القانون رقم 15/04 من خلال القسم السابع مكرر 1 تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات و المتمثلة في:

1-الغش أو الشروع فيه في كل أو جزء من منظومة المعالجة الآلية للمعطيات.

2-حذف أو تغيير للمعطيات المنظمة.

3-إدخال أو تعديل في نظام المعطيات.

4-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار بالمعلومات المخزنة.

5-حيازة أو إفشاء أو نشر أو إستعمال المعطيات.

و هي أفعال مجرمة ضد أموال الغير و مضرة بالمجتمع ، و تعتبر من ضمن جرائم الإختلاس و النصب و خيانة الأمانة.

-العقوبات المقررة لهذه الجرائم : لقد قسمها قانون العقوبات كالتالي:

1/العقوبات الأصلية: و تأخذ بدورها عدة صور تتمثل في:

أ-عقوبة جريمة الدخول أو البقاء داخل النظام : تأخذ صورتين تتمثل في :

*-**الصورة البسيطة للعقوبة:** تناولتها المادة رقم 394 مكرر في فقرتها 01 التي بينت بأنه يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50.000 د ج إلى 100.000 د ج كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

*-**الصورة المشددة للعقوبة:**تناولتها المادة رقم 394 مكرر في فقرتها 02 و 03 التي بينت أنه تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام إشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50.000 د ج إلى 150.000 د ج .

كما بينت المادة رقم 394 مكرر3 بأنه تضاعف العقوبات المنصوص عليها في هذا القسم ، إذا إستهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام ، دون الإخلال بتطبيق عقوبات أشد.

ب-عقوبة جريمة الإعتداء العمدي على المعطيات:

تناولتها المادة رقم 394 مكرر01 التي بينت بأنه يعاقب من ستة أشهر إلى ثلاث سنوات و بغرامة من 500.000 د ج إلى 2.000.000 د ج ، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.

ثم أضافت المادة رقم 394 مكرر 02 بأنه يعاقب من شهرين إلى ثلاث سنوات و بغرامة من 1.000.000 د ج إلى 5.000.000 د ج ، كل من يقوم عمدا و عن طريق الغش بما يأتي:

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

ج-عقوبة الإشتراك في الجريمة: حسب المادة رقم 394 مكرر05 فإن كل من شارك في مجموعة أو في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها

في هذا القسم و كان هذا التحضير مجسدا بفعل أو عدة أفعال مادية ، يعاقب بالعقوبات المقررة للجريمة ذاتها.

د-عقوبة الشروع في الجريمة: حسب المادة رقم 394 مكرر07 فإنه يعاقب على الشروع في إرتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.

2/ العقوبات التكميلية: تناولنها المادة رقم 394 مكرر 06 التي نصت بأنه مع الإحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم ، علاوة على إغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

3/عقوبة الشخص المعنوي: حسب المادة رقم 394 مكرر 04 فإنه يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

-القانون رقم 06/20 المعدل و المتمم لقانون العقوبات :

لقد صدر القانون رقم 06/20 بتاريخ 2020 /04/28 ليعدل و يتمم الأمر رقم 156/66 المؤرخ في 1966/07/08 و المتضمن قانون العقوبات إنطلاقا من عدة مواد تخص كل من :

-الفصل السادس مكرر المتعلق ب: نشر و ترويج أخبار أو أنباء تمس بالنظام و الأمن العموميين.

-الفصل الثامن المعاق ب : التزوير للحصول على الإعانات و المساعدات العمومية و الإعفاءات الإجتماعية.

-الفصل التاسع المتعلق ب: المساس بنزاهة الإمتحانات و المسابقات.

القسم الثالث المتعلق ب: القتل الخطأ و الجرح الخطأ و تعريض حياة الغير و سلامته الجسدية للخطر.

-القانون رقم 05/20 المتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتها:

لقد صدر القانون رقم 05/20 بتاريخ 2020/04/28 بهدف الوقاية من التمييز و خطاب الكراهية و مكافحتها ، و هذا بإلغائه لعدد من مواد الأمر رقم 156/66 المتضمن قانون العقوبات المعدل و المتمم و تناوله لأفعال مجرمة و عقوباتها على النحو التالي:

1/جديد و مصطلحات قانون التمييز و خطاب الكراهية رقم 05/20: و التي جسدتها المادة الثانية منه و المتمثلة في كل من :

-**خطاب الكراهية:** المتمثل في جميع أشكال التعبير التي تنشر و تشجع التمييز المتضمن العداء و الإهانة الموجهة للشخص أو عدة أشخاص عل أساس الجنس أو العرق أو اللون أو النسب....

-**التمييز:** المتمثل في كل تفرقة أو إستثناء أو تفضيل يقوم على أساس الجنس أو العرق أو اللون أو النسب.. بهدف تعطيل و عرقلة الإعتراف بحقوق الإنسان و الحريات الأساسية و التمتع بها على قدم المساواة في كل مجالات الحياة العامة.

-**أشكال التعبير:**القول أو الكتابة أو الرسم أو الإشارة أو التصوير أو الغناء أو التمثيل أو أي شكل آخر من أشكال التعبير مهما كانت الوسيلة المستعملة.

و إستعمال عبارة مهما كانت الوسيلة المستعملة دلالة على إستعمال كل الوسائل بما فيها الوسائل ذات الطبيعة الإلكترونية.

-**الإنتماء الجغرافي:** أي الإنتماء إلى منطقة أو جهة محددة من الإقليم الوطني.

2/حماية ضحايا التمييز و خطاب الكراهية:

لقد أكد القانون إنطلاقا من مادته رقم 16بأن الدولة تضمن للضحايا المنصوص عليهم في هذا القانون التكفل الصحي و النفسي و الإجتماعي بما يضمن أمنهم و سلامتهم و حرمتهم الجسدية و النفسية و كرامتهم ، إنطلاقا من إتباع الجهات القضائية المختصة مجموعة من القواعد الإجرائية و كذا توقيع الأحكام الجزائية المحددة بهذا القانون على النحو التالي:

أ-العقوبات الموقعة على مستعملي الوسائل الإلكترونية في جريمة التمييز و خطاب الكراهية: لقد تناول القانون رقم 05/20 هذه العقوبات إنطلاقا من المواد التالية:

المادة رقم 31: " يعاقب على التمييز و خطاب الكراهية بالحبس من سنتين إلى خمس سنوات و بغرامة من 200.000 د ج إلى 500.000 د ج :.....

-إذا أرتكبت الجريمة بإستعمال تكنولوجيات الإعلام و الإتصال."

المادة رقم 34: " دون الإخلال بالعقوبات الأشد ، يعاقب بالحبس من خمس سنوات إلى عشر سنوات و بغرامة من 5.000.000 د ج إلى 10.000.000 د ج كل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني يخصص لنشر معلومات للترويج

لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز و الكراهية في المجتمع."

المادة رقم 35 :"يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة من 200.000 د ج إلى 500.000 د ج ،كل من أنتج أو صنع أو باع أو عرض للبيع أو للتداول منتجات أو بضائع أو مطبوعات أو تسجيلات أو أفلام أو أشرطة أو إسطوانات أو برامج للإعلام الآلي أو أي وسيلة أخرى تحمل أي شكل من أشكال التعبير التي من شأنها أو تؤدي إلى إرتكاب الجرائم المنصوص عليها في هذا القانون."

ب-العقوبات التكميلية لمستعملي الوسائل الإلكترونية في جريمة التمييز و خطاب الكراهية:

إنطلاقا من المادة رقم 37 فإنه مع الإحتفاظ بحقوق الغير حسن النية فإنه يحكم بكل من :

-مصادرة الأجهزة و البرامج و الوسائل المستخدمة في إرتكاب أو أكثر من الجرائم المنصوص عليها في القانون و الأموال المتحصل عليها.

-إغلاق الموقع الإلكتروني أو الحساب الإلكتروني الذي أرتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن.

-إغلاق محل أو مكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه.

ج-عقوبة الإشتراك أو الشروع في جريمة التمييز و خطاب الكراهية:

حسب كل من المادتين رقم 36 و 39 فإن كل من إشترك أو شرع في هذه الجريمة يعاقب بالعقوبات المقررة للجريمة ذاتها المنصوص عليها في هذا القانون .

د-عقوبة الشخص المعنوي:

حسب المادة 38 فإنه توقع على الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القانون بالعقوبات المنصوص عليها في قانون العقوبات.

ثالثا: مكافحة الجريمة المعلوماتية في إطار القوانين الخاصة:

دائما في إطار الحد من إنتشار الجريمة المعلوماتية المرتكبة من طرف الشخص الطبيعي و كذا الشخص المعنوي ، فإضافة لما أصدره المشرع الجزائري من القوانين العامة السالفة الذكر فإنه قام بإصدار قوانين خاصة في نفس المجال تتمثل فيما يلي:

1/ القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها:

أصدر المشرع الجزائري القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها بتاريخ 2009/08/05 ، من أجل تدارك الفراغ التشريعي في مجال مكافحة الجريمة المعلوماتية من خلال فصوله المبينة للإجراءات المطبقة في محاربة الجريمة المعلوماتية و الوقاية منها ، و هذا من خلال إجراءات التحري التي قسمها إلى :

أولا: مراقبة الإتصالات الإلكترونية:

نصت المادة الرابعة من هذا القانون على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية و هي على النحو التالي:

1-الرقابة على الأفعال الموصوفة بجرائم الإرهاب أو التخريب و الجرائم الماسة بأمن الدولة.

2-حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

3-لمقتضيات التحريات و التحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

4- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .

لا يتم هذا الإجراء إلا بإذن مكتوب من السلطة القضائية المختصة.

عندما يتعلق الأمر بالحالة الأولى من المادة الرابعة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية التابعين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ، إذنا لمدة 6 أشهر قابلة للتجديد و ذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها.

ثانيا: تفتيش المنظومة المعلوماتية:

لقد أجاز هذا القانون من خلال مادته الخامسة للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية في الحالات الضرورية المنصوص عليها سابقا، الدخول بغرض التفتيش و لو عن بعد إلى منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها و منظومة تخزين معلوماتية.

كما بين القانون بأنه يجوز تمديد التفتيش بسرعة إلى المنظومة المعلوماتية أو جزء منها إذا كانت هناك أسباب تدعو للإعتقاد بأنه يمكن الدخول إليها، و هذا بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

و أضاف القانون بأنه في حالة ما إذا كانت المعطيات المبحوث عنها يمكن الدخول إليها إنطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني ، يكون الحصول عليها بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

كما أجاز القانون لسلطات التفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها ، قصد مساعدتها و تزويدها بكل المعلومات الضرورية لعملها.

ثالثا: حجز المعطيات المعلوماتية:

حسب هذا القانون إنطلاقا من مادته رقم 06 يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية، تكون قابلة للحجز و الوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

و يجوز إستعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للإستغلال لأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات.

كما نص القانون من خلال مادته رقم 08 على إمكانية الحجز عن طريق منع الوصول إلى المعطيات و ذلك بأمر من السلطة التي تباشر التفتيش عن طريق تكليف أي شخص مؤهل مع إستعمال وسائل تقنية مناسبة لذلك.

رابعا: حفظ المعطيات المتعلقة بحركة السير:

ألزم ذات القانون من خلال مواده رقم 10 و 11 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها.

و هذا بوضع المعطيات التي يتعين عليها حفظها تحت تصرف السلطات المذكورة مع كتمان سرية هذه العمليات ،إذ يقوم مقدموا الخدمات بحفظ مايلي:

1-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

2-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.
3-الخصائص التقنية و كذا تاريخ و وقت و مدة كل إتصال.
4-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.
5-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال ، و كذا عناوين المواقع المطلع عليها.

تحدد مدة هذه المعطيات بسنة واحدة إبتداء من تاريخ التسجيل ، مع الإشارة إلى قيام المسؤولية الجزائية للأشخاص الطبيعيين و المعنويين عند عدم إحترامهم للإلتزامات المنصوص عليها قانونا مما يؤدي إلى عرقلة حسن سير التحريات القضائية، إذ يعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات و بغرامة من 50.000 د ج إلى 500.000 د ج ، أما الشخص المعنوي فيعاقب بالغرامة المحددة وفقا للقواعد المقررة في قانون العقوبات.

كما ألزم القانون إنطلاقا من المادة رقم 12 مقدمي خدمات الإنترنت بالقيام بما يلي:
1-التدخل الفوري لسحب المحتويات التي يسمح الإطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن.
2-وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة و إخبار المشتركين لديهم بوجودها.

ثانيا: قانون البريد و الإتصالات السلكية و اللاسلكية:

مواكبة للتطورات التكنولوجية تناول القانون رقم 03/2000 المؤرخ في 2000/08/05 المتعلق بالبريد و الإتصالات السلكية و اللاسلكية الأفعال الإلكترونية من خلال مجموعة من المواد والتي أكدت على كل من :

-إجراء التحويلات المالية عن الطريق الإلكتروني بنصها من خلال مادته رقم 87 على أنه : " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن طريق المتعامل و المحولة بالبريد أو البرق أو عن الطريق الإلكتروني."

-إستعمال حوالات دفع عادية أو إلكترونية أو برقية بنصها إنطلاقا من مادته رقم 84 على أنه : " تطبق أحكام المادة 89 من هذا القانون عند إستعمال حوالات دفع عادية أو إلكترونية أو برقية."

وحول سرية المراسلات و إحترامها فإنه تأكيدا من هذا القانون لما نص عليه الدستور الجزائري في مادته رقم 46 بأن : " لا يجوز إنتهاك حرمة حياة المواطن الخاصة ، و حرمة شرفه و يحميهما القانون.

سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة.

لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية و يعاقب القانون على إنتهاك هذا الحكم...."

فقد نص بدوره من خلال مادته رقم 105 على أنه :" لا يمكن في أي حال من الأحوال إنتهاك حرمة المراسلات."

ثم قام بتحديد جزاء كل موظف أو مستخدم أو مندوب عن مصلحة البريد يقوم بفتح أو تحويل أو تخريب البريد ، إنطلاقا من نص مادته رقم 127 على أنه : " كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم بإختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو إختلاسها أو إتلافها يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات و بغرامة من 30.000 د ج إلى 500.000 د ج و يعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق أو يختلس أو يتلف برقية أو يذيع محتواها ، و يعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات."

ثالثا: قانون التأمينات:

لقد تطرق القانون رقم 01/08 المؤرخ في 2008/01/23 المعدل و المتمم للقانون رقم 83/01 المتعلق بالتأمينات لتنظيم الجريمة الإلكترونية من خلال هيئات الضمان الإجتماعي في نصوص عديدة تخص كل من :

-البطاقة الإلكترونية التي تسلم للمؤمن له إجتماعيا مجانا بسبب العلاج و هي صالحة في كل التراب الوطني.

-الجزاءات المقررة في حالة الإستعمال غير المشروع الذي يتم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية، أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له إجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية.

و التي حددها القانون بنصه من خلال مادته رقم 93 على أنه : " دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به ، يعاقب بالحبس من سنتين إلى خمس سنوات و بغرامة من 100.000 د ج إلى 200.000 د ج كل من يسلم أو يستلم بهدف الإستعمال غير المشروع البطاقة الإلكترونية للمؤمن له إجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهن الصحة."

الخاتمة:

لقد شهد العالم تطورا تكنولوجيا و ثورة للمعلومات رتبت نوعين من النتائج و الآثار، الأولى إيجابية تمثلت في تسهيل الإتصال بين البشر و سرعة نقل المعلومات بينهم ، و الثانية سلبية تمثلت في توفيرها للمجال الخصب لإرتكاب سلوكات إجرامية تسمى بالجرائم الإلكترونية أو المعلوماتية، التي عرفت إنتشارا واسعا في إرتكابها من قبل الشخص الطبيعي و كذا الشخص المعنوي بإستعمال الحاسب الآلي و شبكة الإنترنت ، مما أدى بجميع الدول التي تضررت من نتائج هذه الجرائم العابرة للحدود بالبحث عن القوانين العامة الموضوعية و القواعد الإجرائية المطبقة على هذا النوع من الجرائم ، و التي تجسدت في مجموع الإتفاقيات الدولية و الإقليمية السالفة الذكر.

و رغم صعوبة هذا النوع من الجرائم فقد حاول المشرع الجزائري التصدي لهذا النوع من الجرائم متأثرا بالقوانين الدولية و العربية الموضوعة لمكافحة جريمة الإنترنت، عن طريق إصدار مجموعة من القوانين العامة و القوانين الخاصة للحد من إنتشار هذه الجريمة الحديثة و التقليل من آثارها الضارة بكل أفراد المجتمع و مؤسسات الدولة و إقتصادها.