عنـــوان المحاضـــرة

جرائـــم المعلومـــاتيـــة

ألقيـت مـــن طـــــــــرف :

بـــورزام أحمـــــد

وكيـل الجمهوريـــــة , لـــدى محكمـــة باتنـــة

بالمجلس القضائي بباتنـــة

يوم : 06 /06/20 .

الخطـــــــــة

المبحث الأول : نبذة تاريخية عن تطور جرائم المعلوماتية : ــ

ــ خلال الستينيات وبدايـــة السبعينيات .
ــ أواخـــــــر السبعينيـــــــات .
ــ خلال الثمانينـــــــــــــــــات .
ــ خـــلال التسعينيـــــــــــــــات .

تعريـــف جرائـــم المعلومـــاتيـــة :

ــ تعريف يستنـــد على محـــــل الجريمـــــة .
ــ تعريف يستند على الوسيلة المستعملة في إرتكاب الجريمة.
ــ تعريف يستند على السمـــات الشخصية لمرتكب الجريمة.
ــ تعريف يستند على الهدف من إرتكاب الجريمة .
ــ تعريف خبراء منظمة التعاون الإقتصادي والتنمية .

المبحث الثانـــي : أنواع جرائم المعلوماتيـــــة :

ــ الكومبيوتر كهدف للجريمة .
ــ الكومبيوتر كأداة لإرتكاب الجريمة .
ــ الكومبيوتر كبيئة لإرتكاب الجريمة .
ــ جرائم متصلة بالتطور التكنولوجي وإنتشار إستخدام الكومبيوتر.

المبحث الثالـــث : نماذج من بعض التشريعات في مجال جرائـــم المعلوماتية : ــ

ــ التشريع الأمريكي .
ــ التشريع الفرنســـي .
ــ التشريع الجزائري .

المبحث الرابع : أهم المخاطر الأمنية التي تتعرض لها نظم المعلوماتية : ــ

ــ الفايروسات .
ــ التجسس الاليكتروني .
ــ الارهاب الاليكتروني .
ــ القرصنة .
ــ تبييض الأمـــــوال .
ــ تزوير البيانـــات وإستعمالها .
ــ تهديد التجارة الإليكترونيـــــة .
ــ الإغراق بالرسائل الإليكترونيـــة .

المبحث الخامس : التحديات الإجرائية لجرائم المعلوماتية :

ــ عدم ترك أثر مادي وراءها .
ــ مسألة التفتيش .
ــ مسألة الحجز والتحريز .
ــ مسألة أدلـــة الإثبـــــات .
ــ مسألة الإختصاص القضائي .

المبحـــث الأول

جرائـــم المعلوماتيـــة

نبذة تاريخية عن تطور جرائم المعلوماتية :

ـ إن ظاهرة جرائم الكومبيوتر والإنترنت تعد ظاهرة إجرامية مستجدة نسبيا وهي تدق أجراس الخطر لتنبيه مجتمعات العصر الراهن إلى حجم المخاطر والخسائر الناتجة عنها باعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة (بيانات ، معلومات ، برامج بكافة أنواعها ...) يرتكبها أشخاص أذكياء يمتلكون أدوات المعرفة التقنية التي يستخدمونها في الاعتداء على الحق في خصوصية المعلومات ، على معطيات الكومبيوتر المخزنة وعلى المعلومات المنقولة عبر نظم وشبكات الإنترنت .

ـ إن ذلك يظهر مدى خطورة مثل تلك الجرائم التي تطال الحياة الخاصة للأفراد ، تهدد الأمن القومي والسيادة الوطنية وتنشر فقدان الثقة بالتقنية العصرية المتطورة وكما تهدد إبداع العقل البشري .

ـ لذا فإن إدراك ماهية جرائم المعلوماتية وتحديد موضوعها ، خصائصها ومخاطرها ، حجم الخسائر الناتجة عنها ، سمات مرتكبيها ودوافعهم يفرض على الدول إعطاء أهمية استثنائية للتعامل مع هذه الظاهرة ومع نطاق مخاطرها الاقتصادية ، الأمنية ، الاجتماعية والثقافية .

ـ من خلال ذلك يمكن أن نقول بأن أكثر مسائل ظاهرة جرائم المعلوماتية إثارة للجدل والنقاش من طرف فقهاء علم الإجرام في مختلف النظم القانونية اللاتينية ،الجرمانية و الانجلوساكسونية هي مسألة تحديد قائمة جرائم المعلوماتية وتحديد أنماط السلوك الإجرامي والأفعال المكونة له مع تحديد الضوابط القانونية التي تحكم تلك الجرائم .

ـ إن هذه المسائلة أفرزت خلافا موضوعيا لدى علماء الإجرام حول مدى انطباق النصوص القانونية التقليدية على تلك السلوكات .

ـ وقد حسم الجدل بترجيح الرأي القائل بعجز وعدم كفاية وعدم تطابق النصوص القانونية التقليدية على الأنماط الجديدة من جرائم المعلوماتية .

ـ إن مفهوم جرائم المعلوماتية ارتبط تاريخيا بتطور التقنية العلمية واستخداماتها:

- **إذ في المرحلة الأولى :**

من شيوع استخدام الكومبيوتر في الستينيات ثم في السبعينيات ظهر أول اهتمام بما يسمى بجرائم المعلوماتية لكن ذلك الاهتمام اقتصر على نشر مقالات صحفية يناقش فيها التلاعب بالبيانات المخزنة ، تدمير أنظمة الكومبيوتر ، التجسس المعلوماتي و الاستخدام غير المشروع للبيانات المخزنة في نظم الكومبيوتر .

مما أدى إلى طرح سؤال حول ما إذا كانت تلك السلوكات مجرد تصرف عابر أم ظاهرة إجرامية مستجدة ؟

بل توسع ذلك الجدل إلى التساؤل حول ما إذا كانت تلك السلوكات تشكل فعلا جرائم بالمفهوم القانوني أم هي مجرد سلوكات غير أخلاقية تقع وترتكب في بيئة الكومبيوتر .

لكن في الأخير فإن التعامل مع تلك الظاهرة بقي أقرب إلى النطاق الأخلاقي منه إلى النطاق القانوني .

إلا أنه ومع تزايد استخدام الكومبيوتر في **منتصف السبعينات** ، بدأ الحديث عن اعتبار تلك السلوكات بوصفها كظاهرة إجرامية وليست مجرد سلوكات غير أخلاقية .

أما في الثمانينات ، فقد ظهر مفهوم جديد لجرائم المعلوماتية ارتبط بعمليات اقتحام نظم الكومبيوتر عن بعد كأنشطة نشر وزرع الفايروسات الإلكترونية التي تقوم بتدمير الملفات والبرامج بواسطة مقتحمي النظم (Hackers) .

أما من حيث الدوافع لارتكاب مثل تلك السلوكات فقد ظل في البداية محصورا في رغبة المحترفين في تجاوز إجراءات أمن المعلومات وفي إظهار تفوقهم التقني ، كما تم حصر مرتكبوا تلك الأفعال في الأولاد القصر المتفوقين الراغبين في التحدي والمغامرة ، مما أدى إلى إنشاء تنظيم خاص بـ : Hackers للمطالبة بوقف تشويه حقيقتهم ، مع إصرارهم على أنهم يؤدون خدمة في التوعية لأهمية معايير أمن النظم والمعطيات , لكن في الحقيقة ، فإن معظم أولئك(المغامرين)أصبحوا فيما بعد مجرمين حقيقيين ، مما أدى إلى إعادة النظر في سمات مرتكبو جرائم المعلوماتية وطوائفهم بعدما ظهر ما يسمى بالمجرم المعلوماتي المدفوع

بنوايا إجرامية خطيرة تستهدف الإستيلاء على أموال الغير والتجسس قصد الإستيلاء على المعطيات السرية سواء كانت اقتصادية أو أمنية أو شخصية.

ـ أما فترة التسعينيات فقد شهدت تطورا هائلا في حقل جرائم المعلوماتية بعد أن تغير نطاقها ومفهومها وذلك بفعل ما أحدثته شبكات الإنترنت من تسهيل لعمليات الدخول إلى الأنظمة واقتحام شبكات المعطيات مما أدى إلى ظهور أنماط جديدة للإجرام كأنشطة إنكار الخدمة التي تقوم بتعطيل نظام تقني ومنعه من القيام بعمله المعتاد ، وكثيرا ما مورست مثل تلك الأنشطة على مواقع الإنترنت المختصة بتسويق منتجات معينة هامة والتي يؤدي انقطاعها عن الخدمة لساعات معينة إلى خسائر مالية تقدر بالملايين من الدولارات .

ـ كما نشطت بقوة جرائم نشر وزرع الفايروسات عبر مواقع الإنترنت التي تسهل من انتقالها إلى ملايين المستخدمين في نفس الوقت ، وظهرت أيضا أنشطة الرسائل الإلكترونية الماسة بكرامة واعتبار الأشخاص .

تعريف جرائم المعلوماتية

إن الجريمة ، بصفة عامة ، تعرف بأنها **" كل فعل غير مشروع صادر عن إرادة إجرامية يقرر له القانون إما عقوبة أو تدبيرا من تدابير الأمن "**

ـ أما بالنسبة لجريمة المعلوماتية ، فقد اختلف الباحثون حول تحديد مفهوم تلك الجريمة .

ـ وعليه يمكن حصر وتصنيف التعريفات المختلفة لجريمة المعلوماتية في صنفين أساسيين هما :

الصنف الأول : ويشمل التعريفات القائمة على معيار قانوني وبالتالي يعرف هذه الجرائم بالنظر إلى موضوع الجريمة (السلوك محل التجريم والوسيلة المستخدمة في ارتكاب الجريمة مع اشتراط توفر المعرفة والدراية التقنية لدى شخص مرتكبها)

الصنف الثاني : ويشمل التعريفات القائمة على تعدد المعايير بالإعتماد أساسا على موضوع الجريمة وأنماطها وعلى العناصر المتصلة بآليات ارتكابها وعلى البيئة التي ارتكبت فيها وعلى سمات مرتكبيها.

- وسنقتصر على ابرز وأهم التعريفات :

تعريف يستند على محل الجريمة : (أنماط السلوك محل الجريمة)

- يعرف جريمة المعلوماتية بأنها : كل نشاط غير مشروع موجه إما لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الأنظمة أو المحمولة أو المتبادلة عن طريقها .

بمعنى أنها كل سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات أو بتحويلها.

تعريف يستند على الوسيلة المستعملة في ارتكاب الجريمة :

ويعرفها بأنها : كل فعل إجرامي يستخدم الكومبيوتر في ارتكابه كأداة رئيسية .

تعريف يستند على سمات شخصية لدى مرتكب الجريمة :

وتنحصر تلك السمات أساسا في الدراية والمعرفة التقنية .

- وتعرفها وزارة العدل الأمريكية بأنها : **" كل جريمة تكون لمرتكبها معرفة فنية بالكومبيوتر تمكنه من ارتكابها " .**

تعريف يستند على الهدف من الجريمة :

ويعرفها بأنها : كل فعل متعمد مرتبط بأي وجه من أوجه استعمالات الكومبيوتر يتسبب في إلحاق أو إمكانية إلحاق خسارة بالمجني عليه أو حصول أو إمكانية حصول مرتكبها على مكسب.

تعريف خبراء منظمة التعاون الاقتصادي والتنمية :

ويعرفونها بأنها : كل سلوك غير مشروع أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها .

- من خلال جميع التعريفات المشار إليها أعلاه .

يمكن أن نستخلص بأن جريمة المعلوماتية تتميز عن باقي الجرائم التقليدية من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها والأنماط المختلفة للسلوك الإجرامي المجسد للركن المادي لكل جريمة على حدة وكذلك من حيث الهدف المراد تحقيقه من ارتكاب جريمة من جرائم المعلوماتية.

المبحـــث الثانـــي :

أنــواع جـرائم المعلوماتيـــة

- إن أجهزة وتقنيات المعلوماتية تلعب ثلاثة أدوار أساسية في ميدان ارتكاب جرائم المعلوماتية ودور آخر رئيسيا في اكتشاف مثل تلك الجرائم :
- ويمكن حصر دور الكومبيوتر في ارتكاب الجريمة في الآتي :

1- الكومبيوتر كهدف للجريمة

- إن أوضح مثال عن ذلك ، هو عندما تكون السرية ، الأمن ، التكامل والوفرة في تدفق المعلومات هي الهدف من الاعتداء ، بمعنى أن الاعتداء يشمل المعلومات وخدمات الكومبيوتر قصد المساس بالسرية وبأمن النظم ، المحتوى والتكامل أو تعطيل قدرة النظم لمنعها من القيام بأعمالها .
- وذلك عن طريق الدخول غير المرخص به إلى أنظمة المعلومات أو زرع الفايروسات قصد تدمير المعطيات والملفات المخزنة أو المنقولة أو تعديلها أو حذفها أو الإستيلاء عليها .

2- الكومبيوتر كأداة لارتكاب الجرائم :

- ويكون الكومبيوتر كأداة لارتكاب الجريمة في حالة إساءة استخدامه من أجل الإستيلاء على أموال الغير عن طريق التحويلات غير المشروعة أو في التزوير والتزييف أو في الحصول على أرقام بطاقات الائتمان وإعادة استعمالها في الإستيلاء على أموال الغير أو في جرائم القتل عن طريق الدخول إلى قواعد البيانات الصحية والعلاجية وإدخال تغييرات عليها أو على عمل الأجهزة الطبية والمخبرية .

3- الكومبيوتر كبيئة لارتكاب الجريمة :

- وذلك كما هو الحال في قرصنة البرامج ثم إعادة تخزينها واستغلالها واستعمال الكومبيوتر كوسيلة لنشر مواضيع غير مشروعة كترويج المخدرات والأفعال الإباحية.

4- جرائم متصلة بالتطور التكنولوجي وانتشار استخدام الكومبيوتر :

- إن التطور التكنولوجي في مجال المعلوماتية وانتشار استخدام الكومبيوتر في جميع مجالات الحياة المختلفة ساعد بشكل كبير في ظهور جرائم جديدة ، مثل جريمة سرقة البرامج والتسويق غير الشرعي لتلك البرامج ، التقليد والمساس بحق الملكية الفكرية الشيء الذي يترتب عليه إلحاق أضرار جسيمة بالشركة الأم صاحبة الأجهزة أو البرامج .

- وقد عبر عن ذلك الرئيس المدير العام لشركة **BUSINESS SOFT WARE.** من خلال جريدة الشروق اليومية الصادرة بتاريخ : 2006/02/22 الذي حدد بأن نسبة 83% من البرامج في الجزائر متحصلة عن طريق القرصنة .

ولذا فإنه يرى لو تقلصت نسبة القرصنة على مستوى منطقة الشرق الأوسط وشمال افريقيا خلال 2005 -2009 بنسبة 10 نقاط مئوية ، سيصبح رقم أعمال قطاع تكنولوجيات الإعلام 27.5 مليار دولار تقابله زيادة في المداخيل الجبائية بنحو 669 مليون دولار ، في حين أن رقم الأعمال حاليا لا يتجاوز 17 مليار دولار تقابله 6.6 مليون دولار فقط كمداخيل جبائية .

- وقد ورد أيضا في جريدة المحقق الأسبوعي العدد رقم 11 من 28 ماي إلى 03 جوان 2006 مقال تحت عنوان : قرصنة الإنتاج الفني تتحول إلى تجارة منظمة وقد حددت قيمة سوق الأشرطة والأقراص المقلدة المتعلقة بالسمعي البصري وبرامج الأعلام الآلي في الجزائر بـ : 1.5 مليار دولار .

دور الكومبيوتر في اكتشاف الجريمة :

- إن الكومبيوتر يستخدم بشكل واسع في مجال التحريات عن كافة جرائم الكومبيوتر ، وذلك بعد تزايد نطاق هذه الجرائم واعتماد مرتكبيها على الوسائل التقنية المتجددة والمتطورة ، مما استلزم استخدام نفس وسائل الجريمة المتطورة للكشف عنها ، ومن ثم أصبح الكومبيوتر يلعب دورا أساسيا في الكشف عن مثل هذه الجرائم وتتبع مرتكبيها وإبطال أثر الهجمات التدميرية لمخترقي النظم ولا سيما هجمات الفايروسات وإنكار الخدمة وقرصنة البرامج .

- وعليه يمكن تصنيف جرائم المعلوماتية حسب الآتي :

1- تصنيفها حسب نوع المعطيات محل الجريمة :

- الجريمة الماسة بقيمة المعطيات :

كإتلاف وتشويه البيانات والبرامج باستخدام الفايروسات مثلا أو تزوير المستندات المعالجة آليا واستعمالها في أغراض غير مشروعة.

الجريمة الماسة بالمعطيات الشخصية :

كالاعتداء على المعطيات الشخصية المتصلة بالحياة الخاصة للأشخاص السرية أو المحمية بعد الوصول إليها بطريقة غير مشروعة والتلاعب بها باستعمالها في التشهير بأصحابها ...

الجريمة الماسة بحقوق الملكية الفكرية للبرامج (القرصنة) :

كحالة نسخ وتقليد البرامج وإعادة إنتاجها وصنعها وتسويقها بدون ترخيص من أصحابها ، وذلك يشكل اعتداء على العلامة التجارية وبراءة الاختراع .

2- تصنيفها حسب دور الكومبيوتر في ارتكابها :

- وقد تبنت هذا التصنيف القائم على اعتبار الكومبيوتر إما كهدف للجريمة أو كوسيلة لارتكابها أو كبيئة أو محتوى للجرائم معظم التشريعات العالمية ، خاصة منها الأوربية ، الأمريكية ، الكندية والأسترالية .
- وضمن هذا المنظور فإن الإتفاقية الأوربية لجرائم الكومبيوتر لسنة 2001 تقسم جرائم الكومبيوتر حسب الأصناف الأتية بالإضافة إلى جرائم الخصوصية التي نظمتها إتفاقية أوروبية أخرى مستقلة والمبرمة سنة 1981 .

*** الصنف الأول :** ويشمل الجرائم التي تستهدف النظم والمعطيات خاصة منها : السرية ،الأمن, الوفرة في تدفق المعلومات والتكامل .

- **وتضـم :** - الدخول غير المرخص به .
- تدمير المعطيات .
- الإعتراض غير القانوني للنظم .

*** الصنف الثاني :** ويشمل الجرائم المرتبطة بالكومبيوتر .
ويضـم : - التزوير واستعمال المزور .
- النصب والاحتيال .

*** الصنف الثالث :** ويشمل الجرائم المرتبطة بالمحتوى ويضم طائفة واحدة فقط ، وهي المتعلقة بالأفعال الإباحية واللاخلاقية.

*** الصنف الرابع :** ويشمل الجرائم المتعلقة بانتهاك حقوق الملكية الفكرية (القرصنة) .

3 - تصنيفها حسب مساسها بالأشخاص والأموال :

- وهو التصنيف الشائع بالولايات المتحدة الأمريكية والذي تبناه القانون النموذجي لجرائم الكومبيوتر والإنترنت لسنة 1998 ، الذي صنف وقسم تلك الجرائم إلى الجرائم الماسة بشرف وخصوصية الأشخاص والواقعة على الأموال كالسرقات ، التزوير واستعمال المزور ، المقامرة وجرائم الآداب العامة والجرائم المرتكبة ضد المصالح الحكومية .
- ويلاحظ من خلال هذا التصنيف أنه يقوم على فكرة الهدف النهائي الذي يستهدفه الاعتداء .

المبحـــث الثالـث :

نماذج من بعض التشريعات

في مجـال جرائـم المعلوماتيــة

نتيجـة الاعتمـاد والارتبـاط الكبيـر لمعظـم القطاعـات الحيويـة والحساسة في معظم دول العالم ، خاصة المتطورة منها بنظم المعلوماتية ، ونتيجـة أيـضا المخـاطر والأضـرار الجـسيمة التـي ألحقت بالعديـد مـن تلـك الدول ، بسبب الاستخدام غير المشروع للكومبيوتر ، شرعت تلك الدول ، أولا في إعداد قواعد الحماية لأجهزتها وبرامجها ثم ثانيا في سن القوانين الردعية إنطلاقا من المبدأ العام القائل"إن الضرورة تولد القاعدة القانونية".

أ- التشريع الأمريكي :

فـي الولايـات المتحـدة الأمريكيـة ، ومنـذ الخمـسينات بـدأ العمـل بالإعلام الآلي وتطويره إلى أن تم اكتشاف أول كومبيوتر شخصي في بداية الثمانيات ، الذي عرف بدوره تطويرا من حيث الشكل والبرامج .

- وأن أول تشريع في مجال نظم المعلوماتية ظهر سنة 1958 بولاية فلوريدا الأمريكية ، ثم تلاه تشريع فيديرالي سنة 1984 والذي عدل سنة 1986 ثم سنة 1990 ثم سنة 1994 ، ثم سنة 1996 ثم سنة 2001 .
- ويتميـز التـشريع الأمريكـي بتمييـزه بـين نـوعين مـن جـرائم المعلوماتية وهي :

1- جريمة الدخول بدون إذن إلى نظم المعلوماتية :

- وتطبق هذه الجريمة على جميع الأشخاص مهما كانوا .

2- جريمة تجاوز الصلاحية في الدخول إلى أنظمة المعلوماتية :

- ويقصد بهذه الجريمة بأن الدخول إلى أنظمة المعلوماتية يكون مرخص به في مجال ونطاق معين فقط ، لكن ، فإن المستخدم للكومبيوتر يتجاوز ذلك النطاق والصلاحية ويدخل إلى مجالات أخرى محمية وسرية .

ب – التشريع الفرنسي :

-إن حتمية حماية الاقتصاد والأمن الوطني وكذلك حماية المعطيات الشخصية ، دفعت بفرنسا في سنة 1979 إلى إصدار أول تشريع لحماية الحريات والمعطيات ، ثم تلاه قانون 1985 الذي ينظم ويحكم جرائم المعلوماتية .
- وكذلك وبناء على توجيهات اللجنة الأوربية المقدمة سنة 2000 حول التجارة الرقمية مابين دول الاتحاد الأوربي أصدرت فرنسا قانون 2004 المتعلق بالإقتصاد الرقمي .
- إن التشريع الفرنسي بدوره يميز ما بين نوعين من جرائم المعلوماتية وهما :

1- جريمة المساس بنظام المعالجة الآلية للمعطيات :

- ويتفرع عن هذه الجريمة ، الجرائم الثلاثة الآتية :
أ – جريمة الدخول غير المرخص به إلى الأنظمة المعلوماتية .
ب – جريمة عرقلة السير الحسن لنظام المعالجة الآلية للمعطيات.
ج – جريمة إدخال أو تعديل أو حذف معطيات مخزنة بداخل الأنظمة المعلوماتية.

2 - جريمة المساس بحقوق الأشخاص :

- ويتفرع عن هذه الجريمة الجرائم الآتية :
أ – جريمة عدم إتخاد الإحتياطات الكافية لحماية المعطيات الشخصية .
ب- جريمة الاعتداء على الحياة الشخصية للأفراد .
ج – جريمة مسك معلومات شخصية والاحتفاظ بها خارج المدة القانونية المحددة لها .

د – جريمة تحويل المعلومات الشخصية المتبادلة عن طريق النظم بمناسبة إما تسجيلها أو حفظها .

ج – التشريع الجزائري :

- تماشيا مع التطور التكنولوجي في مجال الاتصالات وانتشار استخدام النظم المعلوماتية ، فقد استحدث المشرع الجزائري نصوص قانونية بموجب القانون رقم 15/04 الصادر بتاريخ : 2004/11/10 تحت عنوان : **جرائم المساس بأنظمة المعالجة الآلية للمعطيات** ، محددا بذلك الأفعال والسلوكات التي تدخل ضمن مجال هذا النوع الجديد من الجرائم والتي يمكن حصرها في الآتي :

1- جريمة الدخول أو البقاء في المنظومة عن طريق الغش المادة 394 مكرر من قانون العقوبات :

– وتقوم هذه الجريمة بمجرد ما يتم الدخول غير المرخص به وعن طريق الغش الى المنظومة المعلوماتية ، سواء مس ذلك الدخول أو البقاء كامل المنظومة أو جزء منها فقط .

ويكفي أيضا إثبات المحاولة على تحقيق ذلك لتطبيق أحكام هذه المادة .

هذا ولا يشترط لقيام هذه الجريمة إلحاق أضرار بالمنظومة المعلوماتية ، كما أنه ليس من الضروري أن تكون المنظومة محمية أم لا لتقوم الجريمة .

اجتهاد القضاء الفرنسي :

بعدما تم الدخول غير المرخص به إلى منظومة شركة TATIالفرنسية عدة مرات من طرف شركة أخرى ، قامت شركة TATI بمقاضاة تلك الشركة عن طريق الدخول غير المرخص به فإحتجت تلك الشركة بأن موقع TATI لم يكن محميا ، وبالتالي ، ليس لهذه الأخيرة (TATI) الحق في الاحتجاج على الدخول إلى موقعها ، فقضى القضاء الفرنسي ، بأنه ليس من الضروري أن تكون الأنظمة محمية .

2- جريمة إدخال معطيات في منظومة المعالجة الآلية أو إزالة أو حذف أو تعديل معطيات منظومة المعالجة الآلية عن طريق الغش – المادة 394 مكرر ، ف 1 من قانون العقوبات :

وتقوم هذه الجريمة بمجرد ارتكاب أحد الأفعال المذكورة أعلاه بغض النظر عن المجال المستهدف ، سواء كانت البرامج أو المعطيات أو ...

3 – **جريمة القيام عمدا أو عن طريق الغش بتصميم ، توفير ، نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية أخرى .**

- أو حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم المعلوماتية ، (المادة 394 مكرر ف 3 من قانون العقوبات).

- ويلاحظ ، بأن كل هذه الجرائم هي جرائم عمدية وترتكب عن طريق الغش ونتيجة إساءة استخدام الكومبيوتر .

4 - **جريمة المشاركة ضمن جماعة أو في اتفاق لغرض ارتكاب إحدى جرائم المعلوماتية : المادة 394 مكرر ف 5 من قانون العقوبات .**

- وتقوم هذه الجريمة إما على الانتماء أو الاشتراك إما في جماعة أو اتفاق الغرض منه التحضير والإعداد لارتكاب جريمة أو أكثر من جرائم المعلوماتية .

- ويشترط في ذلك التحضير والإعداد أن يكون مجسدا في فعل أو عدة أفعال مادية .

5 – **جريمة الشروع في ارتكاب إحدى جرائم المعلوماتية : المادة 394 مكرر ف 7 من قانون العقوبات :**

- وتكون العقوبة المقررة عن الشروع ، بطبيعة الحال هي نفس العقوبة المقررة للجريمة التامة المزمع ارتكابها .

*** المصـــادرة :**

- بعد الاحتفاظ بحق الغير الحسن النية ، فإن المحكمة بعدما تقضي بالإدانة عن ارتكاب إحدى جرائم المعلوماتية المذكورة أعلاه ، فإنها تقضي أيضا بمصادرة الأجهزة ، البرامج والوسائل المستخدمة في ارتكاب الجريمة وبإغلاق المواقع التي تكون وتشكل محلا للجريمة وبإغلاق المحل أو مكان الاستغلال الذي ارتكبت به الجريمة بعلم مالكه .

المبحـث الرابــع

أهم المخاطر الأمنية التي تتعرض لها نظم المعلوماتية

مقدمـــة :

- إن أول مرة يطلق فيها هذا المصطلح كان خلال انعقاد مؤتمر جرائم المعلوماتية بأستراليا خلال يومي 16 و 17 من شهر فبراير من سنة 1998 .
- وقد خلصت دراسة أجرتها منظمة الأمم المتحدة حول جرائم المعلوماتيـة إلـى أن مـابين 24 – 42 % مـن القطـاع العـام والقطـاع الخاص كان ضحية لهذه الجرائم .
- حسب دراسة أجراها معهد أمن الكومبيوتر بأمريكا سنة 1999 فإن خسائر 163 شركة من جرائم المعلوماتية بلغت أكثر من 123 مليون دولار أمريكي .
- في حين أظهرت دراسة أحرى لنفس المعهد أجريت خلال سنة 2000 ارتفاع عدد الشركات المتضررة من تلك الجرائم ، إذ وصل إلى 273 شركة ، بلغ مجموع خسائرها أكثر من 256 مليون دولار أمريكي .
- وقد قدرت الجمعية الأمريكية للأمن الصناعي بأن الخسائر السنوية التي تتكبدها الشركات نتيجة إساءة استخدام الكومبيوتر تبلغ 555 مليون دولار أمريكي .
- بالإضافة إلى هذه الأضرار الجسيمة التي تتكبدها "القطاعات" العامة والخاصة ، فإن هذه الأخيرة أيضا تتعرض إلى أضرار وخسائر جسيمة تتسبب فيها الفايروسات المختلفة .

فمثـلا : بلغت الخسائر التي تسبب فيها فايروس RED CODE مليارين دولار أمريكي ، في حين بلغت خسائر فايروس I LOVE YOU 8.7 مليار دولار أمريكي .

- وبالرغم من هذه الخطورة الجسيمة ، فإن متابعة وملاحقة جرائم المعلوماتية والكشف عنها أمر صعب للغاية ، لكون هذه الجرائم لا تترك أثرا ماديا وراءها .
- وعليه ، فإن معظم هذه الجرائم تم اكتشافها عن طريق الصدفة وبعد مرور وقت طويل من ارتكابها وبالتالي ، فإن الجرائم التي لم يتم اكتشافها تكون أكثر من التي تم اكتشافها .

تعريف الفيروس :

– وهو عبارة عن برنامج مثل أي برنامج آخر ، لكنه يتسم بالقدرة التدميرية والوظائف التخريبية كالإتلاف ، الحذف ، التعديل والنسخ ... وهو يهدف إلى إحداث أكبر ضرر بالنظام المعلوماتي الذي تم زرعه فيه وبأي نظام آخر متصل به في أي مكان في العالم ..

خصائص الفيروس :

– يتميز الفيروس بعدة خصائص أهمها :

1- **العدوى :** فهو برنامج يتم تسجيله أو زرعه على الأقراص الصلبة أو الأسطوانات الخاصة بالكومبيوتر وبمجرد تشغيل البرنامج ينتقل الفيروس من جهاز إلى آخر وبسرعة فائقة حتى يصل إلى الذاكرة فينتشر بداخلها ويشرع في نسخ نفسه بسرعة غير عادية .

2- **الإختفاء :** يتميز الفيروس بقدرة التمويه والاختفاء بداخل ملفات مخفية أو بموقع الذاكرة ويظل هناك حتى يحين توقيت معين أو تعطى له إشارة معينة ، فيقوم بتشغيل نفسه ويمارس نشاطه التدميري .

3 – الاختراق : للفيروس القدرة الفائقة على الدخول إلى الأنظمة المعلوماتية والتسلل إليها واختراق كل إجراءات الحماية .

4 – التدمير : إن أهم أعراض الإصابة بالفيروس هو بطء تشغيل النظام المعلوماتي ، بعد ما يصيب الفيروس عامل السرعة الذي يعد أهم ميزة في النظام ، ثم يشرع الفيروس في مسح البيانات المخزنة على وسائط التخزين ثم شغل واحتلال ذاكرة النظام بطريقة يتعذر معها التعامل مع البيانات والمعلومات فتتوقف الاستجابة لنظام التشغيل ، كما يقوم الفيروس بالتشويش على المعلومات وإدخال معلومات أخرى خاطئة .

* أغراض الفيروس :

- يتم استخدام الفيروسات من أجل تحقيق عدة أهداف أهمها :

1 – لضمان حماية النسخ الأصلية للبرامج من مخاطر النسخ غير المصرح به ، إذ ينشط الفيروس بمجرد البدء في عملية ذلك النسخ .

2 – لضمان جبر الزبون على الوفاء بإلتزاماته التعاقدية في الوقت المحدد :

- إذ من أجل تحقيق ذلك ، يقوم المنتج بوضع وزرع الفيروس على البرنامج الذي يبيعه إلى الزبون لتنشط قوته التدميرية في وقت محدد لتدمير كامل البرنامج وذاكرة الجهاز ، إذا لم يف الزبون بالتزاماته التعاقدية في المواعيد المحددة مسبقا ، وفي حالة الوفاء بتلك الالتزامات في المواعيد المحددة ، يسلم المنتج إلى الزبون الوسيلة المناسبة لوقف الفيروس وتدميره.

3 – لاثبات الذات أو لمجرد التدمير وإلحاق الضرر بالغير من طرف بعض الخبراء المحترفين الذين يهدفون من وراء زرع الفايروسات واستخدامها إلى إثبات الذات أو مجرد إلحاق الأذى بالغير .

4 – لإضعاف إمكانيات المنافس وتكبيده خسائر معتبرة .

- يستخدم الفيروس أحيانا لتحقيق أهداف عدوانية للاطلاع على امكانيات المنافس والعمل على اضعافها بغرض تكبيده خسائر ضخمة ، سواء كان ذلك من أجل تحقيق أغراض سياسية أو عسكرية أو إقتصادية أو ...

5 – الحصول على مكاسب شخصية :

- أحيانا يستخدم الفيروس بغرض الابتزاز من أجل الحصول على مكاسب شخصية ، مثل ما يحدث كثيرا مع الشركات الكبرى والبنوك .

* أنواع الفيروسات :

- توجد أنواع كثيرة من الفيروسات وهي دائما في تطور مستمر ، سواء من حيث ابتكار أنواع جديدة أو بتطوير الفيروسات الجديدة وذلك تماشيا مع تطور نظم المعلوماتية .

- إن الفيروسات تتفاوت من حيث القوة والهدف وتوقيت نشاطها .

1- **فهناك فيروسات عامة** ، تنتقل إلى أي جهاز أو برنامج أو ملف وتمارس نشاطها التدميري . – وهناك فيروسات محددة : تستهدف نوعا معينا من النظم لمهاجمته وتدميره ، فهي لا تعطل البرامج ، بل تغير الهدف منها ، كإحداث تلاعب مالي أو تعديل وتغيير مثلا في أهداف عسكرية معينة ، ومن بين هذه الفيروسات فيروس : NASA المناهض للأسلحة النووية .
وأن هذا النوع من الفيروسات يحتاج إلى مهارة ودقة عالية .

2 – ان الفيروسات تختلف بحسب مكان تواجدها ، فهناك مثلا :
* فيروسات تتولى تدمير البرامج واتلافها ، مثلا القنبلة المعلوماتية .
* فيروس السرطان الذي يمسح أجزاء من الشاشة بصورة تدريجية حتى يأتي عليها كلها .
* فيروس الدودة المعلوماتية ، الذي يعمل على ايقاف وتعطيل النظام المعلوماتي كليا .
* فيروس المخ الذي يعمل على غزو ذاكرة الجهاز فيسبب أضرار بالغة بالقرص الصلب ، بعد أن يتم زرعه بجهاز بدء التشغيل ثم يتسلل حتى يصل إلى جدول تجزئة القرص .
* فيروس " مايكل أنجلو " الذي يتلف جهاز بدء التشغيل ثم القرص الصلب .
* فيروس " الشلال " الذي يعمل على اسقاط وحذف بعض الحروف من النصوص المخزنة داخل الجهاز .
* فيروس " كريسماس " الذي يتمثل في رسالة بريد اليكتروني تعرض بطاقة تهنئة على الشاشة ، لكنه في تلك الأثناء يقوم بقراءة الملفات المخزنة تم يرسل نسخ من نفسه إليها .

*** الحماية من الفيروسات** :

- نظرا لخطورة الفيروسات الجسيمة وآثارها المدمرة على النشاط المعلوماتي والتجارة الإلكترونية ، ظهرت حملة قوية لمقاومتها من خلال أساليب الوقاية والأمن ، المتمثلة في :
1 - اتخاذ الإجراءات الاحتياطية لمنع الإصابة بالفيروس أو لانتشاره .
2 – مراجعة نظام التشغيل والملفات بشكل دوري ومستمر بحثا عن الفيروسات .

3 – استعمال برامج الحماية من الفيروسات مثل :
- VACCINE الذي يعمل على الكشف عن الفيروسات.
- DISK WATCHER " مراقب القرص " المخصص لمقاومة الفيروس .
- GAURD DOG " كلب الحراسة " الذي يمنع أي شخص أجنبي من التعامل مع الملفات ، بل ويصدر صوتا تحذيريا مميزا عند حدوث ذلك.
- ANTIVIRUS الذي يقوم بالمسح الدوري للقرص الصلب .
- أجهزة HARD WARE التي تزود بأقراص مخصصة للكتابة فقط عليها ثم تخزين البرامج بصفة مستديمة ، ومن ثم تصبح تلك الأقراص صالحة للقراءة فقط دون الكتابة عليها مرة أخرى .

* أسباب صعوبة إثبات جرائم المعلوماتية :

1- إن تلك الجرائم لا تترك أثرا ماديا لها بعد ارتكابها .
2 – إنها تحتاج إلى خبرة فنية دقيقة وعالية ومتخصصة إذ يصعب ، بل يستحيل على المحقق التقليدي التعامل معها .
3 – أنها تعتمد على الخداع في ارتكابها وعلى التضليل في التعرف على مرتكبيها .
4 – إنها تعتمد على قمة الذكاء في ارتكابها .
- وأمام خطورة هذه الجرائم وصعوبة متابعتها والكشف عنها والتعرف على مرتكبيها ، فإن أول خطوة في مكافحة هذه الجرائم تبدأ من تحديد هذه الجرائم ، ثم تحديد الجهة التي يجب التعامل معها ، ثم تكوين وتدريب إطارات تكوينا فنيا متخصصا يتناسب مع طبيعة هذه الجرائم ، ثم وضع آليات وإجراءات لمكافحتها والتعامل معها وتحديد العقوبات القمعية .
- وإن كل ذلك لا يمكن تحقيقه إلا عن طريق التعاون الدولي .

* فئات مرتكبوا جرائم المعلوماتية :

- ويمكن بصفة عامة حصر أولئك الجناة في الفئات الأربعة الآتية :

- **الفئة الأولى :** وتنحصر في المستخدمين لأجهزة الكومبوتر في منازلهم ، نظرا لسهولة استخدامهم لتلك الأجهزة واتصالاتهم بأجهزة الكومبيوتر الأخرى دون التقيد بوقت أو بنظام معين .

ـ الفئـــة الثانيـــة : وهـــي الموظفـون الـساخطون الغاضـبون علـى قطاعاتهم التـي يعملـون بهـا ، الـذين يرجعـون إلـى أمـاكن عملهـم بعـد انتهـاء فترة العمل الرسمية ويقومون بتخريب واتلاف مثلا المعطـيات والبرامج ... إلخ .

ـ الفئـــة الثالثـــة : وهـــي فئـــة العـــابثين أو مـــا يعرفـــون بمـــصطلح HACKERS " المتسللون / المقتحمون "

- وينقـسمون إلـى قـسمين ، فمـنهم العـابثون قـصد التـسلية فقـط ، ومـنهم العـابثون المحترفـون الـذين يتـسللون ويقتحمـون نظـم المعلوماتيـة معينـة ومختارة بكل عناية ثم يعبثون أو يتلفون أو يسرقون محتويات تلك الأنظمة

ـ الفئـة الرابعة : وهم العاملون في الجريمة المنظمة المتخصصة .

* أهـم المخاطـر الأمنية :

- إن مجال المعلوماتية معرض لعدة مخاطر أمنية ، أهمها ما يلي :

1 – خطر التجسس الإليكتروني :

- إن عصر المعلوماتية وما صاحبه من تكنولوجية وتقنيات عالية التطور جعل حدود الدول مستباحة بأقمار التجسس والبث الفضائي .

-وبـذلك تحولـت وسـائل التجـسس مـن الطـرق التقليديـة إلـى الطـرق الإليكترونية ، خاصة بعد انتشار استخدام شبكات الإنترنت .

إن الخطورة لا تكمن في استخدام الإنترنت ، ولكن في ضعف الوسائل الأمنيـة المـستخدمة فـي حمايـة الـشبكات القطاعيـة الخاصـة بالمؤسـسات والهيئات الحكومية .

– ومـن هنـا لا يمكـن حتمـا الإعتمـاد كليـا علـى بـرامج ووسـائل الحمايـة التـي تنتجهـا الـشركات الأجنبيـة لكـون تلـك البـرامج والوسـائل ليست في مأمن ولا محل ثقة كاملة .

– ومن أمثلة ذلك التجسس الخطير ، هو التجسس الذي تقوم بـه أجهزة الاستخبارات الأجنبية بغرض الحصول على أسرار دولـة معينـة ثم إفشائها لدولة أخرى معادية أو لاستغلالها بما يضر المصلحة الوطنية

لتلك الدولة ، مستعملة في ذلك مثلا التجسس الإليكتروني على المكالمات الهاتفية ، رسائل الفاكس والبريد الإليكتروني و ... إلخ .

2 – خطر القرصنة :

- ويقصد بالقرصنة الاستخدام أو النسخ غير المشروع أما لنظم التشغيل أو لبرامج الكومبيوتر في مجال المعلوماتية .
-وقد أدت القرصنة إلى خسائر باهضة جدا ، بلغت مثلا في سنة 1988 (11 مليار) دولار أمريكي في مجال البرامج وحده فقط .

3- خطر الإرهاب الاليكتروني :

- لقد تنبهت الدول الغربية ، وخاصة الولايات المتحدة الأمريكية إلى خطر الإرهاب الإليكتروني ، ذلك مما جعل مثلا الرئيس الأمريكي بيل كلينتون يشكل لجنة خاصة اسند إليها مهمة حماية البنية التحتية الأساسية في أمريكا .
- فكان أول عمل قامت به تلك اللجنة هو تحديد الأهداف المحتمل استهدافها من طرف الإرهابيين ، مثل مصادر الطاقة الكهربائية ، قطاع الاتصالات ، شبكات الكومبيوتر ، خاصة القطاعية منها .
- ثم قامت بانشاء مراكز خاصة في كل ولاية للتعامل مع احتمالات وقوع أي هجوم إرهابي إليكتروني عليها .
- وبدورها قامت أجهزة الاستخبارات المركزية الأمريكية (C. I . A) بإنشاء مركز حروب المعلوماتية ووظفت به ألف (1000) إطار من خبراء أمن المعلومات .
- وقد اتخذت نفس الإجراءات وتدابير الحماية من طرف الأجهزة الحكومية الأخرى كالمباحث الفيدرالية FBI والقوات الجوية الأمريكية .
- وقد جاء في إحدى التقارير المعدة من طرف وزارة الدفاع الأمريكية بأن شبكة الاتصالات ، مصادر الطاقة الكهربائية ، البنوك وقطاعات النقل في أمريكا معرضة للهجوم من قبل أي جهة تسعى إلى محاربة أمريكا بدون أن تواجه قواتها المسلحة .

4 – تزوير البيانات :

- إن تزوير البيانات يعتبر من أكبر جرائم نظم المعلوماتية انتشارا وتتم عملية التزوير عن طريق الدخول إلى قاعدة البيانات ثم العمل على تعديل تلك البيانات أو إضافة معلومات خاطئة بهدف الاستفادة غير المشروعة من وراء ذلك .

5 – تبييض الأموال :

- إن أول ما استعمل هذا المصطلح كان في الولايات المتحدة الأمريكية سنة 1931 ، نسبة إلى شركة الغسل التي تمتلكها المافيا ، وذلك خلال محاكمة أحد زعماء تلك المافيا .
- وقد شملت تلك المحاكمة مصادرة جميع الأموال التي ثبت بأنها متأتية من التجارة غير المشروعة في المخدرات .
- واشمل تعريف لمصطلح تبييض الأموال (غسل الأموال) هو : كل عملية من شأنها تخفى المصدر غير المشروع الذي اكتسبت منه الأموال .
- وقد استفادت المافيا الدولية من التقنية الحديثة المتطورة في مجال المعلوماتية ووظفتها في أنشطتها الإجرامية ، ومنها بالطبع طرق تبييض الأموال فلجأت إلى إنشاء مواقع لها عبر شبكات الإنترنت متخصصة في عمليات تبييض الأموال كموقع مثلا : LAUNDRY MAN بالإضافة إلى مواقع أخرى تستخدم كستائر لعمليات تبييض الأموال ، كالمواقع الافتراضية المخصصة لنوادي القمار التي لاحقتها المباحث الفيدرالية الأمريكية واعتقلت العديد من مدراء تلك المواقع وتمت متابعتهم قضائيا .
- إن استخدام شبكات الإنترنت جعل عمليات تبييض الأموال تتم بسرعة لانعدام الحواجز الحدودية بين الدول ، وبدون ترك أي أثر مادي ، في الغالب ، وراءها .

ويقدر المتخصصون المبالغ المالية التي يتم تبييضها سنويا بحوالي (400) مليار دولار أمريكي من مجموع (600) مليار دولار التي تنفق سنويا من طرف الأمريكيين وحدهم في عمليات القمار .

6 – تهديدات التجارة الإليكترونية :

- بدأت التجارة الإليكترونية تنتشر خلال السبعينيات بسبب ما توفره من سهولة في الاتصال ما بين الأطراف واختزال العمليات الورقية والبشرية ، فضلا عن السرعة في إرسال البيانات وانخفاض كلفة التشغيل .
- لكن ،فإن هذه المزايا التي شجعت شركات الأعمال على التحول نحو إستخدام الإنترنت للإستفادة أكثر من مزايا التجارة الإليكترونية ، إرتبطت بها مخاطر عديدة كالسرقات والنصب والاحتيال والتزوير واستعمال المزور وانتحال صفة الغير... إلخ .

فمثلا : أصبح الاستيلاء على أرقام بطاقات الائتمان عبر شبكات الإنترنت أمرا سهلا للغاية ، إذ أصبح بإمكان لصوص هذه البطاقات أن يسرقوا مئات الآلاف من أرقام تلك البطاقات في يوم واحد فقط ، ثم يقومون ببيع تلك الأرقام إلى آخرين لإستعمالها في عمليات سلب أموال أصحاب تلك البطاقات .

- **قضيـــــــة :** -

قام شخصان خلال سنة 1994 بإنشاء موقع إليكتروني خصص لعروض بيع سلع معينة ، على أن يتم إرسال تلك السلع إلى أصحابها فور تسديدهم لقيمتها إليكترونيا ، لكن اتضح فيما بعد بأن تلك السلع لم ترسل إلى أصحابها على الإطلاق كما تبين بأن ذلك الموقع كان موقعا وهميا ، القصد منه النصب والاحتيال ، وقد تم التعرف على أصحاب ذلك الموقع والقاء القبض عليهم .

- **قضيـــــة أخرى : -**

لقد استطاع شخص من اقتحام نظام الكومبيوتر الذي يتحكم في تدفق معظم الطاقة الكهربائية الموجهة إلى تزويد مختلف أنحاء ولاية كاليفورنيا الأمريكية ، وبالرغم من أن الخسائر كانت محدودة ، إلا أن ذلك الاقتحام كشف عن وجود ثغرات أمنية في نظام الكومبيوتر الخاص بشركة الكهرباء .

7 - الإغراق بالرسائل الإليكترونية :

- ويقصد به إرسال الرسائل إلى البريد الإليكتروني لشخص معين أو لمقدم الخدمة (PROVIDER) قصد الاضرار به ، إذ يؤدي ذلك إلى تعطيل الشبكة وعدم امكانية استقبال أي رسائل ، فضلا عن امكانية انقطاع الخدمة تماما ، وذلك بعد تسبب تلك الطريقة في ملء جميع منافذ الاتصال COMMUNICATION – PORTS : وكذلك قوائم الانتظار .
- وبالتالي فإن الجهة المستهدفة ستتكبد خسائر مادية ومعنوية غير محدودة من جراء ذلك التعطيل أو انقطاع الخدمة تماما .
- ولتجنب الوقوع في مثل تلك المخاطر ، فقد لجأت بعض الشركات إلى تطوير برامج تسمح باستقبال جزء محدود فقط من الرسائل في حالة تدفق عدد كبير منها.

المبحث الخامس

التحديات الإجرائية لجرائم المعلوماتية

إن أنشطة مكافحة جرائم المعلوماتية أظهرت تحديات ومشاكل كثيرة تختلف في جوانب كثيرة عن التحديات والمشاكل التي ترتبط بالجرائم التقليدية الأخرى .

منها مـــثلا :

1 – إن جرائم الكومبيوتر والإنترنت لا تترك أثرا ماديا وراءها بمسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية ، كما أن مرتكبيها يملكون القدرة على اتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة جدا مما يخلق تحديات كبيرة في مجال ضبط مثل هذه الجرائم وجمع الأدلة عنها والتعرف على مرتكبيها .

2 – إن التفتيش في مثل هذا النوع من الجرائم يتم عادة على نظم الكومبيوتر والإنترنت وقواعد البيانات وشبكات المعلوماتية المحلية،الإقليمية والدولية ، مما يجعل هذا الإمتداد والتوسع في التفتيش يخلق تحديات كبيرة حول مدي شرعية هذا الإجراء ومدى مساسه بحقوق الخصوصية المعلوماتية الخاصة بأصحاب النظم التي يشملها التفتيش.

- وعملا بمبدأ مشروعية الدليل وسلامة مصدره فإن هذا النوع من التفتيش يتطلب اصدار مذكرة قضائية تجيز تفتيش أنظمة كمبيوتر معينة ، لأن المشروعية الإجرائية تفرض تحقيق أقصى الضمانات للمشتبه فيه تتفق ومقتضيات قرينة البراءة .

- كما يستوجب أن يجري هذا النوع من التفتيش من طرف من تتوفر لديهم الخبرات الفنية الكفيلة بتحقيق الغرض من التفتيش .

- إن مسألة حاجة أنشطة التفتيش للسرعة من جهة ومسألة قدرة الجناة على إخفاء الدليل من جهة أخرى ، تستوجب التفكير في آلية إستصدار أوامر الحجز المستعجلة للنظم المشتبه فيها ، مع أمر أصحابها بالكف عن استخدام النظام فورا بمجرد البدء في اجراءات التفتيش، مع امكانية أيضا ، إرسال مثل تلك الأوامر المستعجلة إلى الجهات التي قد تتوفر لديها البيانات المرتبطة بنشاط النظام المشتبه فيه .

3 – إن الحجز و التحريز ينصبان أساسا على المعطيات والبيانات والبرامج المخزنة في النظام المشتبه فيه أو في النظم المرتبطة به بمعنى أن الحجز والتحريز ينصبان على أشياء ذات طبيعة معنوية ، معرضة بكل سهولة للتغيير والاتلاف ، مما يخلق مشاكل حول تحديد المعايير المقبولة ، قانونا وتقنيا لتنظيم عمليتي الحجز والتحريز المعلوماتي .

فضلا عن ذلك ، فإن هذا النوع من الحجز قد يمس بخصوصية صاحب النظام وإن كان مشتبه فيه ، خاصة عندما تمتد إجراءات الحجز إلى كل محتويات النظام ، التي قد تضم وتشمل معلومات وبيانات قد يحرص عل سريتها أو أن تكون محل حماية قانونية أو بحكم طبيعتها أو لتعلقها وارتباطها بجهات أخرى.

4 – إن أدلة الإثبات (أدلة الإدانة) في مثل هذا النوع من الجرائم هي ذات نوعية مختلفة ، فهي معنوية الطبيعة ، مثل : معلومات الدخول والبرامج / مما أثار مشاكل كثيرة أمام القضاء من حيث مدى قبولها وحجيتها ومن حيث أيضا ، تحديد المعايير الواجب توفرها في تلك الأدلة حتى تكون لها حجية الإثبات ، مثل قواعد الإثبات التقليدية .

5 – **إن الإختصاص القضائي :** (المحلي أو القانون الواجب التطبيق)
يتسم بقصور وبفراغ قانوني في مجال هذا النوع من الجرائم ، التي في الغالب ما ترتكب من طرف أشخاص من خارج الحدود أو أنها تمر عبر شبكات معلومات تقع بخارج البلاد أيضا ، وهذا من شأنه يطرح تحدي تحديد قواعد الاختصاص والقانون الواجب التطبيق حتى يمكن معالجة مشاكل امتداد أنشطة الملاحقة والتحري والحجز والتفتيش خارج الحدود الوطنية .
- وكل ذلك لا يمكن تحقيقه إلا عن طريق تعاون دولي شامل يقوم على الموازنة ما بين متطلبات مكافحة جرائم المعلوماتية ووجوب حماية السيادة الوطنية وحقوق وحريات الأفراد وحماية خصوصياتهم .

- إنتهـــــــــــــــى -