الجرائم المعلوماتية

م. عبدالنبي شنته فرج **م.م. طارق طه عبود**

المستخلص

يهدف البحث الى التعرف على الجرائم المعلوماتية التي اصبحت تشكل عقبه في ظل التطور التكنولوجي اضافه الى معرفه القوانين والتشريعات التي تتخذ ضد هذه الجرائم وايضا مرتكبوا هذه الجرائم اضافه الى خصائص هذه الجرائم ومدى تأثيرها على المجتمع التكنولوجي وخلص البحث الى الاستنتاجات الأتية :-

١- الجريمة المعلوماتية متعددة الحدود بحيث لا تقتصر على بلد معين.
٢- قانون ملائم لمكافحه هذه الجرائم .
٣- لا توجد اتفاقيات دوليه لحمايه المجتمع الدولي من نتائج واثار هذه الجريمة

Abstract

The research aims to identify information crimes that have become an obstacle in light of technological development in addition to knowledge of the laws and legislations that are taken against these crimes and also committed these crimes in addition to the characteristics of these crimes and the extent of their impact on the technological community. The research concluded the following conclusions

1- Information crime is multi-border so that it is not limited to - a specific country An appropriate law to combat these crimes .

2- There are no international agreements to protect the international community from the consequences and effects of this crime.

مشكله البحث:-

تكمن مشكلة البحث في الآتي:

١- هل الجريمة المعلوماتية متعديه الحدود ام في داخل الدولة الواحدة.

٢- هل هناك صعوبة في اكتشاف الجريمة المعلوماتية .

٣- هل توجد صعوبة في اثبات الجريمة المعلوماتية .

٤- ما اسلوب ارتكاب الجريمة المعلوماتية .

٥- هل الجريمة المعلوماتية تتم عادة بتعاون اكثر من شخص .

اهميه البحث:

تكمن اهميه البحث في تسليط الضوء على الجريمة المعلوماتي هل هناك تشابه بينها و بين الجريمة التقليدية اضافه الى ذلك تحتاج الجريمة المعلوماتية الى مسرح للجريمة ام انها تحصل بواسطه التقنيات ولا تحتاج الى فاعل اضافه الى وضع قانون يجرم هذه العملية وايضا ايجاد الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتشخيص عناصر الجريمة ان وجدت وجمع الأدلة عن الإدانة .

أهدف البحث:-

يهدف البحث الى :-

١- التعرف على ماهية الجرائم المعلوماتية

٢- التعرف على اهداف الجرائم المعلوماتية وما هو الغرض منها و هل لديها مسرح جريمة اسوة بالجريمة التقليدية.

٣- التعرف على وسائل الجرائم المعلوماتية وطرق الوقاية منها.

٤- التعرف على وسائل الجرائم المعلوماتية وطرق الوقاية منها.

المقدمـــة

لا جريمة ولا عقوبة الا بنص .. هل هناك نص يعاقب الأشباح القانون الجنائي وبصورة عامة مؤسس بصفه أساسية على مبدأ شرعية الجرائم والعقوبات ، لا جريمة ولا عقوبة الا بناء على قانون ويجب ان ينص على الجريمة والعقوبة بنصوص واضحة ، وهذا يعني (انه لا جريمة ولا عقوبة الا على الفعل الذي يعده القانون وقت اقترافه جريمة ولا يجوز تطبيق عقوبة اشد من العقوبة النافذة وقت ارتكاب الجريمة) كما ان (لا عقاب على فعل او امتناع الا بناء على قانون ينص على تجريمه وقت اقترافه ولا يجوز توقيع عقوبات او تدابير احترازية لم ينص عليها القانون)

وهذا يعني ان سريان القانون على الجرائم هو القانون النافذ وقت ارتكاب الجريمة ويرجع في تحديد وقت ارتكاب الجريمة الى الوقت الذي تمت فيه أفعال تنفيذها ...

ماذا عن جرائم المستقبل ؟

الجرائم التي تفرضها التكنولوجيا او ما يسمى الجانب المظلم للتكنولوجيا .. الجريمة المعلوماتية واحدة منها .

هنالك توصيف لجريمة المستقبل ، لكن هل هناك نصوص قانونية للعقاب ؟

أين القانون من جرائم المستقبل ؟

لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها: فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية

وهناك جانب يرى أن هذه الجريمة ناشئة أساساً من التقدم التكنولوجي، ومدى التطور الذي يطرأ عليه، وهو متجدد بصفة دائمة ومستمرة وخاصة في مجال تكنولوجيا المعلومات، ويفضل أن يطلق عليها اصطلاح " جرائم التكنولوجيا الحديثة "، فهي جرائم تكنولوجيا باعتبارها مرتبطة ارتباطاً وثيقاً بالتكنولوجيا التي تعتمد أساساً على الحواسيب وغيرها من أجهزة تقنية قد تظهر في المستقبل، وهي كذلك جرائم حديثة نظراً لحداثتها النسبية من ناحية ولارتباطها الوثيق بما قد يظهر من أجهزة حديثة تكون ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل.**(١)**

تعريف الجريمة المعلوماتية :-

اصطلاح الجريمة المعلوماتية يطلق على الجرائم المتعلقة بالحاسوب والإنترنت، فاصطلاح الجرائم المعلوماتية عام ويشمل التقنيات الحالية والمستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الإنترنت.

التكنولوجيا الحديثة تحديداً التكنولوجيا المتعلقة بتقنيات الحاسوب والإنترنت متطورة ومتسارعة النمو، الأمر الذي يجعل من الصعب حصر صور الجرائم المعلوماتية وأنواعها.

وفي هذا الإطار آثر المشرع الإنجليزي في قانون إساءة استخدام الحاسوب عام ١٩٩٠ عدم وضع تعريف محدد لجرائم الحاسوب؛ بغية عدم حصر

القاعدة التجريمية في إطار أفعال معينة، تحسباً للتطور العلمي والتقني في المستقبل .

في إطار تعريف الفقه للجريمة المعلوماتية نجد أن الاتجاهات تباينت في هذا السياق بين موسع لمفهوم الجريمة المعلوماتية وبين مضيق لمفهومها.

فمن التعريفات المضيقة لمفهوم الجريمة المعلوماتية تعريفها على أنها: كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازماً لارتكابه من ناحية لملاحقته وتحقيقه من ناحية أخرى.

وحسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية.

كذلك عرفت الجريمة المعلوماتية أنها: " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية

" الجريمة المعلوماتية تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات".

المقصود بالجريمة المعلوماتية: " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح او نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول أو التي تحول عن طريقه ، لكن ماذا عن الوسائط الاخرى مثل الهاتف الذكي او التي تحتوي على معالجات الكترونية ولا تصنف كحاسبات .

كما نلاحظ فإن هذا التعريف يضيق من مفهوم الجريمة المعلوماتية، إذ يخرج من نطاقها العديد من الأفعال غير المشروعة التي يستخدم الحاسب

أداة لارتكابها. في المقابل فإن هناك تعريفات حاولت التوسع في مفهوم الجريمة المعلوماتية، فعرفها أنها: " كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال المادية أو المعنوية" **(٢)**

وتم تعريفها كذلك أنها: " كل سلوك سلبي أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأية صورة كانت " .

وقد ذهبت مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في عام ١٩٨٣ إلى تعريف الجريمة المعلوماتية أنها: " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها " تغيير معطيات أو بيانات أو برامج الحاسوب أو محوها أو كتابتها أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها؛ وتبعاً لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية شخص آخر، أو بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص أخر ويتبنى الخبير الأمريكي

(Parker) مفهوماً واسعاً للجريمة المعلوماتية يشير إلى أنها: " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل". **(٣)**

الجريمة المعلوماتية " مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب"

ونحن من جانبنا نتفق مع هذا التعريف، إذ أنه تعريف حاول الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة المعلوماتية سواء التي قد تقع بواسطة النظام المعلوماتي أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما شمل التعريف جميع الجرائم التي من الممكن أن تقع في بيئة إلكترونية. فهذا التعريف لم يركز على فاعل الجريمة ومقدرته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية، بل إنه حاول عدم حصر الجريمة المعلوماتية في نطاق ضيق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب.**(٤)**

مفاهيم الجريمة المعلوماتية

أدت الحداثة التي تتميز بها الجريمة المعلوماتية واختلاف النظم القانونية والثقافية بين الدول إلى اختلاف في مفهوم الجريمة المعلوماتية فيما بينها حسب اللجنة الأوروبية فان مصطلح الجريمة المعلوماتية يضم كل المظاهر التقليدية للجريمة مثل الغش و تزييف المعلومات، و نشر مواد إلكترونية ذات محتوى مخل بالأخلاق أو دعوى لفتن طائفية. أدت الحداثة التي تتميز بها الجريمة المعلوماتية واختلاف النظم القانونية والثقافية بين الدول إلى اختلاف في مفهوم الجريمة المعلوماتية فيما بينها حسب اللجنة الأوروبية فان مصطلح الجريمة المعلوماتية يضم كل المظاهر التقليدية للجريمة مثل الغش و تزييف المعلومات، و نشر مواد إلكترونية ذات محتوى مخل بالأخلاق أو دعوى لفتن طائفية. حسب وزارة العدل في الولايات المتحدة الأمريكية التي عرفت الجريمة عبر الإنترنت بأنها "اي جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها". حسب منظمة التعاون الاقتصادي للجريمة المرتكبة عبر الإنترنت "هي كل سلوك غير مشروع أو غير اخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات ونقلها".**(٥)**

بعض تسميات الجرائم المعلوماتية

- جرائم الإنترنت Computer Crime
- جرائم التقنية العالية.Hi-tech Crime
- الجريمة السايبرية Cyber Crime

انواع الجرائم الإلكترونية

- الجرائم ضد الافراد: وتسمى بجرائم الإنترنت الشخصية تتمثل في سرقة الهوية ومنها البريد الإلكتروني، أو سرقة الاشتراك في موقع شبكة الإنترنت وانتحال شخصية أخرى بطريقة غير شرعية عبر الإنترنت بهدف الاستفادة من تلك الشخصية أو لإخفاء هوية المجرم لتسهيل عملية الإجرام.

- الجـرائم ضـد الملكيـة: تتمثـل فـي نقـل البرمجيـات الضـارة المضـمنة فـي بعـض البـرامج التطبيقيـة والخدميـة أو غيرهـا، بهـدف تـدمير الأجهـزة أو البـرامج المملوكـة للشـركات أو الأجهـزة الحكوميـة أو البنـوك أو حتـى الممتلكـات الشخصية.
- الجـرائم ضـد الحكومـات: مهاجمـة المواقـع الرسـمية وأنظمـة الشـبكات الحكوميـة والتـي تسـتخدم تلـك التطبيقـات علـى المسـتوى المحلـي والـدولي كالهجمـات الإرهابيـة علـى شـبكة الإنترنـت، وهـي تتركـز علـى تـدمير البنـى التحتية ومهاجمة شبكات الكمبيوتر وغالبا ما يكون هدفها سياسي.

- عبـارة عـن نبضـات إلكترونيـة غيـر مرئيـة ممـا يجعـل أمـر طمـس ومحـو الـدليل أمر سهل.**(٦)**

الجريمة وتقنية المعلومات

- التقنيات كهدف مثلا اختراق أنظمة البنوك والشركات.
- التقنيات كسلاح مثلا الترويج لأفكار هدامة ضارة بالمجتمع.
- التقنيات كمساعد مثلا استعمالها في التزوير والتزييف والاحتيال.

اهداف الجرائم المعلوماتية

- التمكـين مـن الوصـول إلـى المعلومـات بشـكل غيـر قـانوني كسـرقة المعلومـات أو حذفها والاطلاع عليها.

- الـتمكن مـن الوصـول بواسـطة الشـبكة العنكبوتيـة إلـى الاجهـزة الخادمـة المـوفرة للمعلومـات وتعطيلهـا أو التلاعـب بمعطياتهـا مثـل اداة المسـح (nc) وتـدعى سـكينة الجـيش السويسـري فـي مجموعـة ادوات الأمـن بحيـث تقـدم هـذه الاداة خدمـة مسـح قويـة للبروتوكـول الافتراضـي وتنفـذ بالشـكلnetcat وأيضـا البروتوكـول النقـلtcp ولمسـح هـذا البرتوكـول يجـب إضـافة المعامـل٢ u-

netcat اداة المسح (strobe) تستخدم لمسح منفذ بروتوكول النقل المضمون tcp.

- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالبنوك والمؤسسات والحكومات والأفراد والقيام بتهديدهم اما لتحقيق هدف مادي أو سياسي
- الكسب المادي أو المعنوي أو السياسي غير المشروع مثل تزوير بطاقات الائتمان وسرقة الحسابات المصرفية.

ادوات الجريمة المعلوماتية :-

- برامج نسخ المعلومات المخزنة في اجهزة الحاسب الالي.
- الإنترنت كوسيط لتنفيذ الجريمة.
- خطوط الاتصال الهاتفي التي تستخدم لربط الكمرات ووسائل التجسس.
- ادوات مسح الترميز الرقمي(البا ركو د)
- الطابعات.
- اجهزة الهاتف النقال والهواتف الرقمية الثابتة.
- برامج مدمرة: مثل برنامج حصان طروادة trojan horse بحيث يقوم بخداع المستخدم لتشغيله، حيث يظهر على شكل برنامج مفيد وامن ويؤدي تشغيله إلى تعطيل الحاسب المصاب و برنامج الدودة الذي يشبه الفيروس ولكنه يصيب اجهزة الحاسب دون الحاجة إلى اي فعل وغالبا يحدث عندما ترسل بريد إلكتروني إلى كل الأسماء الموجودة في سجل الأسماء.**(٧)**

مرتكبوا الجرائم المعلوماتية:-

١- طائفة القراصنة"

وهي بدورها تنقسم إلى:

أ- القراصنة الهواة Hackers : يقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الالية وبعضهم يطلق عليهم صغار نوابغ المعلوماتية واغلبهم من الطلبة. تضم هذه الطائفة الاشخاص الذين يستهدفون من الدخول إلى انظمة الحاسبات الالية غير المصرح لهم بالدخول اليها. كسر الحواجز الامنية الموضوعة لهذا الغرض وذلك بهدف الخبرة أو الفضول.

ب- القراصنة المحترفين Crackers : اعمارهم تتراوح ما بين ٢٥و٤٥ سنة اغلبهم انهم ذوي مكانة في المجتمع ودائمًا ما يكونوا من المختصين في مجال التقنية الإلكترونية. هم أكثر خطورة وعادة ما يعودون إلى ارتكاب الجريمة مرة اخرى.

٢- طائفة الحاقدين

يطلق عليهم المنتقمون لأنها تنطلق ضد اصحاب العمل والمنشئات التي كانوا يعملون بها وانتقاما من رب العمل وهم اقل خطورة، يرى الباحثون ان اهداف وأغراض الجريمة غير متوفرة لدى هذه الطائفة فهم لا يهدفون إلى اثبات قدراتهم التقنية ومهارتهم الفنية وليبغون تحقيق مكاسب مادية أو سياسية، بل يعمدون إلى اخفاء وإنكار افعالهم واغلب انشطتهم تتم باستخدام تقنيات زراعة الفيروسات والبرامج الضارة لتخريب الانظمة المعلوماتية.

٣- طائفة المتطرفين

الفكريين يعرف التطرف في هذا المجال بأنه عبارة عن انشطة توظف شبكة الإنترنت في نشر وبث واستقبال وإنشاء المواقع و الخدمات التي

تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري، مما دفع بعض المتشددين إلى سلوك الطريق الإجرامي وأصبح هناك ما يعرف بالمجرم المعلوماتي المتطرف الذي يستعمل بما في ذلك للشبكات الاعلامية الاخبارية التي تتبع نشطات الجماعية ونشر بيانات وتصريحات قادتها، وعادة ما يقوم هؤلاء بالاتصال من مقاهي ومكاتب الإنترنت يستعملون كافة المواقع الإلكترونية التي تسعى لتحقيق اغراض دعائية لصالحهم.

٤- طائفة المتجسسون

يقوم هؤلاء بالعبث أو الإتلاف محتويات الشبكة من جانب ومن جانب اخر وهو الأهم و الذي يشكل الخطر الحقيقي على تلك الواقع على سبيل المثال قد يتم تنزيل الاسرار الصناعية من كمبيوتر في احدى الشريكات و ارسالها بالبريد الإلكتروني مباشرة إلى منافستها، ومن أهم اهداف هذه الطائفة في استخدام الانظمة المعلوماتية هي الحصول على معلومات الاعداء والأصدقاء على حد سواء

٥- طائفة مخترقي الانظمة:

يتبادل افراد هذه الطائفة المعلومات فيما بينهم بغية اطلاع بعضهم على مواطن الضعف في الانظمة المعلوماتية وتجري عملية التبادل للمعلومات بينهم بواسطة النشرات الاعلامية الإلكترونية مثل: مجموعات الاخبار، بل ان افراد هذه الطائفة يتولون عقد المؤتمرات لكافة مخترقي الانظمة المعلوماتية بحيث يدعى اليها الخبراء من بينهم للتشاور حول وسائل الاختراق واليات نجاحها.**(٨)**

خصائص وسمات مرتكبو الجرائم :-

١- شخص ذو مهارات فنية عالية متخصص في الجرائم المعلوماتية يستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور و الشفرات ويسبح في عالم الشبكات، ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة في اجهزة الحواسيب من خلال الشبكات.

٢- شخص قادر على استخدام خبراته في الاختراق وتغيير المعلومات.

٣- شخص قادر على تقليد البرامج أو تحويل اموال.....

٤- شخص محترف في التعامل مع شبكات الحاسبة.

٥- شخص غير عنيف لأن تلك الجريمة لا تلجا للعنف في ارتكابها.

٦- شخص يتمتع بذكاء اذ يمكنه التغلب على كثير من العقبات التي تواجهه اثناء ارتكابه الجريمة، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الانظمة الامنية حتى لا تستطيع ان تلاحقه وتتبع اعماله الاجرامية من خلال الشبكات أو داخل اجهزة الحواسب فالإجرام المعلوماتي هو اجرام ذكاء.

٧- شخص اجتماعي له القدرة على التكيف مع الاخرين.

دوافع ارتكاب الجريمة المعلوماتية :-

١- **دوافع مادية** ويتمثل في: تحقيق الكسب المادي: تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الإنترنت. نظرا للربح الكبير، وغالبا ما يكون الدافع لارتكاب هذه الجريمة هو وقوع الجاني في مشاكل مادية مثال على ذلك تحويل حساب مالي إلى حسابه.

٢- **دوافع شخصية** وتتمثل في:

- الرغبة في التعلم يكرس مرتكبو هذه الجريمة وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الامنية للأنظمة الحاسوبية.
- دوافع ذهنية أو نمطية: غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الإنترنت هو الرغبة في اثبات الذات وتحقيق الانتصار على تقنية الانظمة المعلوماتية دون ان يكون لهم نوايا اثمة.
- دافع لانتقام تعد من اخطر الدوافع التي يمكن ان تنفع شخص يملك معلومات كبيرة عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته.
- دافع التسلية هي جريمة ترتكب من اجل التسلية لا يقصد من ورائها احداث جرائم.
- دافع سياسي يتم غالبا في المواقع السياسية المعادية للحكومة، ويتمثل في تلفيق الاخبار والمعلومات ولو زورا أو حتى الاستناد إلى جزء بسيط جدا من الحقيقة ومن ثم نسخ الاخبار الملفقة حولها، تعد الدوافع السياسية من ابرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم.**(٩)**

مكافحة الجرائم المعلوماتية :-

- محاربة الجريمة الإلكترونية تحتاج لوقفة طويلة وقوية من قبل الدول و الأفراد الكل مسؤول عن الإسهام قدر الإمكان لمحاربة و التصدي لها:
- تتجسد أول طرق مكافحة الجرائم الإلكترونية عبر الإنترنت في الاستدلال الذي يتضمن كل من التفتيش والمعاينة والخبرة والتي تعود إلى خصوصية الجريمة الإلكترونية عبر الإنترنت، اما الثاني سبل مكافحة الجريمة الإلكترونية هي تلك الجهود الدولية و الداخلية لتجسيد قانونية للوقاية من

هـذه الجريمـة المسـتحدثة، فأمـا الدوليـة فتتمثـل فـي جهـود الهيئـات والمنظمـات الدولية والتي تتمثل في:

- توعيـة النـاس لمفهـوم الجريمـة الإلكترونيـة وانـه الخطـر القـائم ويجـب مواجهتـه والحرص على ألا يقعوا ضحية له.
- ضـرورة التأكـد مـن العنـاوين الإلكترونيـة التـي تتطلـب معلومـات سـرية خاصـة كبطاقة ائتمانية أو حساب بنكي.
- عـدم الإفصـاح عـن كلمـة السـر لأي شـخص والحـرص علـى تحـديثها بشـكل دوري واختيار كلمات سر غير مألوفة.
- عدم حفظ الصور الشخصية في الكمبيوتر.
- عدم تنزيل اي ملف أو برنامج من مصادر غير معروفة.
- الحـرص علـى تحـديث انظمـة الحمايـة مثـل: اسـتخدام بـرامج الحمايـة مثـل نورتون norton، كاسبر سكي، مكافي .Mcafee...الخ.
- تكوين منظمة لمكافحة الجريمة الإلكترونية.
- ابلاغ الجهات المختصة في حال تعرض لجريمة إلكترونية.
- تتبـع تطـورات الجريمـة الإلكترونيـة وتطـوير الرسـائل والأجهـزة والتشـريعات لمكافحتها.
- تطـوير برمجيـات امنـة ونظـم تشـغيل قويـة التـي تحـد مـن الاختراقـات الإلكترونيـة وبرمجيـات الفيروسـات وبـرامج التجسـس مثـل مضـادات التجسـس وهـي بـرامج تقـوم بمسـح الحاسـب للبحـث عـن مكونـات التجسـس وإلغائهـا مثـل: lava soft

الهجمات المعلوماتية :-

وصلت الجرائم المعلوماتية إلى حد القتل ؛ففي شهر ٩ من عام ٢٠٢٠، توفيت امرأة في دوسلدورف في أحد المستشفيات الألمانية بعد تعطل نظام الحاسوب بسبب برنامج للقرصنة بواسطة الفدية، وهو برنامج خبيث يقيد الوصول إلى نظام الحاسوب الذي يصيبه. ويعكس هذا الهجوم الإلكتروني مدى هشاشة القطاع الصحي في مواجهة هذه الهجمات. وقال الكاتب أنوش سيدتا غيا في تقرير نشرته صحيفة لوتون (le temps) السويسرية، إنه لم يحدث أن سُجلت حالات وفاة نتيجة هجوم إلكتروني. ولكن تسبب هجوم سيبراني في وفاة مريضة في مستشفى بدوسلدورف نتيجة عدم تلقيها للعلاج. وأعلنت السلطات الألمانية عن العواقب المأساوية للهجوم السيبراني "الإلكتروني" الذي استهدف الشبكة الإلكترونية للمستشفى الجامعي في دوسلدورف ليصيب أنظمته بالشلل الجزئي منذ ٩ سبتمبر/أيلول.

وبرنامج الفدية المعروف باسم "را نسوم وير" هو برنامج ضار يستهدف نقاط الضعف في برامج معينة للسماح للمهاجمين بالتحكم عن بُعد في أنظمة الحاسوب. ومقابل إعادة الوصول إلى الملفات المحملة على أجهزة الحاسوب، عادة ما يطلب المخترق فدية تصل إلى عشرات أو حتى مئات الآلاف إن لم يرد خلاف ذلك.**(١٠)**

خصائص الجريمة المعلوماتية :

ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الإنترنت أضفى عليها مجموعة من الخصائص والسمات المميزة لهذه الجريمة عن الجرائم التقليدية هي:

أولاً : الجريمة المعلوماتية متعدية الحدود أو جريمة عبارة للدول:

المجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع

منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود. فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد. فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل الإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى.

هذه الطبيعة التي تتميز بها الجريمة المعلوماتية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد لقانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

كانت القضية المعروفة باسم مرض نقص المناعة المكتسبة (الايدز) من القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية، وتتلخص وقائع هذه القضية التي حدثت عام ١٩٨٩ في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأخذ البرامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طرواده)؛ إذ كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس؛

وف الثالث من فبراير من عام ١٩٩٠ تم إلقاء القبض على المتهم جوزيف بوب في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الإنجليزي، حيث أن إرسال هذا البرنامج قد تم من داخل المملكة المتحدة، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه إحدى عشرة تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية، ومهما كان الأمر فإن لهذه القضية أهميتها من ناحيتين:

ونتيجة لهذه الطبيعة الخاصة للجريمة المعلوماتية ونظراً للخطورة التي تشكلها على المستوى الدولي، والخسائر التي قد تتسبب بها؛ تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم .**(١١)**

والتعاون الدولي يتمثل في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء الأمر الذي يكفل الإيقاع بمجرمي المعلوماتية وتقديمهم للقضاء العادل.

تكمن أهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية في أنه لا يوجد هناك مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة. بالإضافة إلى أن نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة إن وجدت وجمع الأدلة عنها للإدانة فيها يشكل عائقاً كذلك أمام التعاون في مجال مكافحة هذا النوع من الجرائم .

وبالتالي من أجل التصدي للإجرام المعلوماتي لا بد أن تعمل الدول في اتجاهين:

الأول : داخلي حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة هذه الجرائم.

الثـاني : دولـي عـن طريـق عقـد اتفاقيـات الدوليـة، حتـى لا يسـتفيد مجرمـو المعلوماتيـة مـن عجـز التشـريعات الداخليـة مـن ناحيـة، وغيـاب الاتفاقيـات الدولية التي تتصدى لحماية المجتمع الدولي من نتائج وآثار هذه الجرائم

ثانياً : صعوبة اكتشاف الجريمة المعلوماتية

- تتميـز الجريمـة المعلوماتيـة بصـعوبة اكتشـافها وإذا اكتشـفت فـإن ذلـك يكـون بمحض الصدفة عادة

حيـث يبـدو مـن الواضـح أن عـدد الحـالات التـي تـم فيهـا اكتشـاف هـذه الجـرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية.

ويمكـن رد الأسـباب التـي تقـف وراء الصـعوبة فـي اكتشـاف الجريمـة المعلوماتيـة إلـى عـدم تـرك هـذه الجريمـة لأي أثـر خـارجي بصـورة مرئيـة. كمـا أن الجـاني يمكنـه ارتكـاب هـذه الجريمـة فـي دول وقـارات أخـرى، إذ أن الجريمـة المعلوماتيـة ريمـة عـابرة للـدول (دوليـة). وكـذلك فـإن قـدرة الجـاني علـى تـدمير دليـل الإدانـة فـي أقـل مـن الثانيـة الواحـدة شـكل عـاملاً إضـافياً فـي صعوبة اكتشاف هذا النوع من الجرائم.

فـالجرائم المعلوماتيـة فـي أكثـر صـورها خفيـة لا يلاحظهـا المجنـي عليـه أو لا يـدري حتـى بوقوعهـا والإمعـان فـي حجـب السـلوك المكـون لهـا وإخفائـه عـن طريـق التلاعـب غيـر المرئـي فـي النبضـات أو الذبـذبات الإلكترونيـة التـي تسـجل البيانـات عـن طريقهـا أمـراً لـيس عسـيراً فـي الكثيـر مـن الأحـوال بحكـم توافر المعرفة والخبرة في مجال الحاسبات غالباً لدى مرتكبها

كمـا أن المجنـي عليـه يعلـب دوراً رئيسـياً فـي صـعوبة اكتشـاف وقـوع الجريمـة المعلوماتيـة حيـث تحـرص أكثـر الجهـات التـي تتعـرض أنظمتهـا المعلوماتيـة للانتهـاك أو تمنـى بخسـائر فادحـة مـن جـراء ذلـك علـى عـدم الكشـف حتـى يـبن موظفيهـا عمـا تعرضـت لـه وتكتفـي عـادة باتخـاذ إجـراءات إداريـة داخليـة وأن

الإبـلاغ عنهـا للسـلطات المختصـة تجنبـاً للإضـرار بسـمعتها ومكانتهـا وهـز الثقة في كفاءتها .**(١٢)**

ويـرى الـبعض أن للمجنـي عليـه دوراً مثيـراً للريبـة فـي بعـض الأحيـان، فهـو قـد يشـارك بطريـق غيـر مباشـر فـي ارتكـاب الفعـل، وذلـك بسـبب وجـوده فـي ظـروف تجعـل تعرضـه للجريمـة المعلوماتيـة أمـراً مرتفعـاً بشـكل كبيـر، ويرجـع ذلـك بشـكل أساسـي إلـى القصـور الأمنـي الـذي يعتـري الأنظمـة المعلوماتيـة الـذي قـد يسـاعد علـى ارتكـاب الفعـل الإجرامـي، ويترتـب علـى ذلـك نتيجـة أخـرى تميـز الجريمـة المعلوماتيـة هـي أن هنـاك إمكانيـة الحيلولـة دون وقـوع هـذه الجريمـة مقارنـة بغيرهـا مـن الجـرائم، إذ يعتمـد ذلـك أساسـاً علـى تطوير نظم الأمن الخاصة بأنظمة الحاسبات وشبكاتها

وفـي لواقـع فـإن إحجـام المجنـي عليـه عـن الإبـلاغ عـن وقـوع الجـرائم المعلوماتيـة يبـدو أكثـر وضـوحاً فـي المؤسسـات الماليـة مثـل البنـوك والمؤسسـات الادخاريـة ومؤسسـات الإقـراض والسمسـرة، حيـث تخشـى مجـالس إدارتهـا مـن أن تـؤدي الدعايـة السـلبية التـي قـد تـنجم عـن كشـف هـذه الجـرائم أو اتخـاذ الإجـراءات القضـائية حيالهـا إلـى تضـاؤل الثقـة فيهـا مـن جانـب المتعـاملين معهـا. حيـث أن الجانـب الأكبـر مـن الجـرائم المعلوماتيـة لا يـتم الكشـف أو التبليـغ عنـه فـإن ذلـك يـؤثر سـلباً فـي السياسـة التـي يمكـن أن توضـع لمكافحتهـا، وقـد تـم طـرح عـدة اقتراحـات تكفـل تعـاون المجنـي عليـه فـي كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي

وإلـى جانـب ذلـك فـإن المجنـي عليـه يتـردد أحيانـاً فـي الإبـلاغ عـن هـذه الجـرائم خوفـاً مـن أن الكشـف عـن أسـلوب ارتكـاب هـذه الجـرائم قـد يـؤدي إلـى تكـرار وقوعهـا بنـاء علـى تقليـدها مـن قبـل الآخـرين كمـا أن الإعـلان عـن هـذه الجـرائم يـؤدي أحيانـاً إلـى الكشـف عـن مـواطن الضـعف فـي برنـامج المجنـي عليـه ونظامه المعلوماتي مما يسهل عملية اختراقه

ثالثاً : صعوبة إثبات الجريمة المعلوماتية

اكتشاف الجريمة المعلوماتية أمر – كما سبق وأشرنا – ليس بالسهل ولكن حتى في حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب.

فالجريمة المعلوماتي تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملوس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة. ففي هذه البيئة تكون البيانات و المعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كلياً من قبل الفاعل أمراً في غاية السهولة.**(١٣)**

ففي إحدى الحالات التي شهدتها ألمانيا أدخل أحد الجناة في نظام الحاسوب تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها من شأنها محو هذه البيانات بالكامل بواسطة مجال كهربائي وذلك إذا تم اختراقه من قبل الغير

وتجدر الإشارة إلى أن وسائل المعاينة وطرقها التقليدية لا تفلح غالباً في إثبات هذه الجريمة نظراً لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف آثاراً مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة المعلوماتية يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين

الأول : إن الجريمة المعلوماتية لا تخلف آثاراً مادية.

الثاني: إن كثيراً من الأشخاص يردون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها هي فترة طويلة نسبياً، الأمر الذي يعطي مجالاً للجاني أو للآخرين أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في دلالة الأدلة المستسقاة من المعاينة في الجريمة المعلوماتية.

بالإضافة إلى ذلك فإن نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء يشكل عائقاً أساسياً أمام إثبات الجريمة المعلوماتية ذلك أن هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والإنترنت. ونتيجة لنقص الخبرة والتدريب كثيراً ما تخفق أجهزة الشرطة في تقدير أهمية الجريمة المعلوماتية فلا تبذل لكشف غموضها وضبط مرتكبيها جهوداً تتناسب وهذه الأهمية. بل إن المحقق قد يدمر الدليل بمحوه محتويات الاسطوانة الصلبة عن خطأ منه أو إهمال أو بالتعامل بخشونة مع الأقراص المرنة

رابعاً : أسلوب ارتكاب الجريمة المعلوماتية

ذاتية الجرائم المعلوماتية تبرز بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها. فإذا كانت الجرائم التقليدية تتطلب نوعاً من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة ... فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها(soft crime) لا تحتاج إلى العنف، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة. وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الإنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة

للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو التغرير بالقاصرين كل ذلك دون حاجة لسفك الدماء.

خامساً : الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص

تتميز الجريمة المعلوماتية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها إضرار بالجهة المجني عليها، وغالباً ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه

والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود قد يكون اشتراكاً سلبياً وهو الذي يترجم بالصمت من جانب من يعلم بوقوع الجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكاً إيجابيا وهو غالباً كذلك يتمثل في مساعدة فنية أو مادية.

سادساً : خصوصية مجرمي المعلوماتية

المجرم الذي يقترف الجريمة المعلوماتية الذي يطلق عليه المجرم المعلوماتي يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية (المجرم التقليدي).

فإذا كانت الجرائم التقليدية لا أثر فيها للمستوى العلمي والمعرفي للمجرم في عملية ارتكابها – باعتبارها قاعدة عامة – فإن المر يختلف بالنسبة للجرائم المعلوماتية فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت.

فعلى سبيل المثال فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشروع للموال يتطلب مهارة وقدرة فنية تقنية عالية جداً من قبل مرتكبها.

كذلك فإن البواعث على ارتكاب المجرم المعلوماتي هذا النوع من الإجرام المعلوماتي قد يكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي. **(١٤)**

الاستنتاجات :-

١- الجريمة المعلوماتية متعددة الحدود حيث لا تقتصر على بلد معين.

٢- لا يوجد قانون ملائم لمكافحه هذه الجرائم .

٣ - لا يوجد اتفاقات دوليه لحمايه المجتمع الدولي من نتائج واثار هذه الجريمة.

٤- صعوبة اكتشاف هذه الجرائم لأنها لا تترك اثر مثل الجريمة التقليدية .

٥- صعوبة اثبات الجريمة المعلوماتية حتى لو تم اكتشافها

٦- نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء يشكل عائقا اساسيا امام اثبات الجريمة المعلوماتية .

٧- هذا النوع من الجرائم يتطلب تدريب وتأهيل هذه الجهات في مجال تقنيات المعلومات وكيفيه جمع الأدلة والتفتيش والملاحقة في بيئة الحاسوب والانترنت

٨- اسلوب ارتكاب الجريمة حيث الجريمة التقليدية تتطلب نوع من المجهود العضلي الذي قد يكون في ممارسه العنف والايذاء ام الجريمة المعلوماتية تكون هادئة بطبيعتها ولا تحتاج الى العنف

٩- الجريمة المعلوماتية تتميز عاده بتعاون اكثر من شخص على ارتكابها وغالبا ما يشترك في اخراجها الى حيز الوجود شخص متخصص في تقنية الحاسوب.

المراجع والمصادر حسب ورودها بالبحث

١- جميل عبدالباقي صفير . الجرائم الناشئة عن استخدام الحاسب الالي .- القاهرة: دار النهضة العربية ،٢٠١٠

٢- محمد عبدالله سلامه. موسوعة جرائم المعلوماتية.- الإسكندرية: المكتب العربي الحديث،٢٠٠٧.

٣- محمد شوابكه. جرائم الحاسوب والانترنت،٢٠٠٤.

٤- محمود احمد عباينه. جرائم الحاسوب وأبعادها الدولية .- عمان : دار الثقافة ،٢٠٠٥,

٥- احمد هلالي. الجوانب الموضوعية والإجرائية للجرائم المعلوماتية .- القاهرة :دار النهضة ،٢٠١٥

٦- عبدالله عبدالكريم عبدالله. جرائم المعلوماتية والانترنت الجرائم الإلكترونية .- بيروت : منشورات الحلي،٢٠١١

٧- محمد علي عليان. الجرائم المعلوماتية. الإسكندرية :دار الجامعة ،٢٠٠٩.-ط٢.-

٨- محمد الأمين بشري .التحقيق في جرائم الحاسوب الآلي .- القاهرة : دار الكتب القانونية ،٢٠٠٩.

٩- رستم هشام محمد. جرائم الحاسوب المستخدمة. القاهرة :دار الكتب ،٢٠٠٨ .

١٠- محمد امين رومي. جرائم الكمبيوتر والانترنت.- الإسكندرية: دار المطبوعات والنشر الجامعية ،٢٠٠٣.

١١- مدحت رمضان. جرائم الاعتداء على الأشخاص والانترنت .- القاهرة :دار النهضة ،٢٠١٠.

١٢- ابراهيم خالد ممدوح. الجرائم المعلوماتية .- الإسكندرية :دار الفكر،٢٠٠٩.

١٣- كامل سعيد .جرائم الكمبيوتر والجرائم الاخرى في مجال تكنلوجيا المعلومات .عمان : دار اليسير للنشر ،٢٠٠٢.

١٤- كامل عفيفي عفيفي. جرائم الكمبيوتر .القاهرة :دار النهضة ،٢٠١٠.