الجريمة الإلكترونية

اعداد
نور سليمان

مقدمة

دخلت خدمة الإنترنت مصر عام ١٩٩٣ علي يد مركز المعلومات ودعم اتخاذ القرار بالتعاون مع شبكة الجامعات المصرية ومع بداية عام ١٩٩٧ بدأ المركز في خصخصة خدمات الإنترنت في مصر وكانت البداية من خلال ست عشرة شركة زادت إلى ثمانٍ وستين شركة في عام ٢٠٠٠ وانتهت إلى إحدى عشرة ومائتي شركة هي إجمالي الشركات التي تقدم خدماتها في مجال الإنترنت داخل مصر.

وكان **عدد مستخدمي الإنترنت في مصر في العام الأول لاستخدامه لم يتجاوز خمسة وسبعين ألف شخص ولكنه بعد تطبيق حملة حاسب لكل بيت وانخفاض أسعار خدمات الإنترنت السريع وصل عدد مستخدمي الإنترنت حاليا إلى أضعاف هذا الرقم يحصلون علي خدماتهم من خلال ٢١١ شركة تعمل في هذا المجال داخل حدود مصر.**

على الرغم من هذا الانتشار الرهيب للإنترنت في مصر والجهود المبذولة من جانب الحكومة المصرية لجذب الاستثمارات في مجال التكنولوجيا إلا أن هناك فراغا تشريعيا في هذا المجال خاصة في قضايا النشر الإلكتروني وقوانين جرائم الإنترنت الخاصة باقتحام النظم وغيرها.

في عام ٢٠٠٢ أنشئت ادارة مكافحة جرائم الحاسب الالي وشبكة المعلومات. ومهمة هذه الادارة رصد ومتابعة جرائم التطور التكنولوجي وتتبع مرتكبيها من خلال أحدث النظم الفنية والتقنية الحديثة ويتم تقنين الإجراءات بعد عملية التتبع الفني وضبط القائم بارتكاب الجريمة التي يكون تكييفها القانوني من خلال قانون العقوبات المصري.

وشهد عام ٢٠٠٥ صدور أول حكم لجرائم التشهير عبر الانترنت عندما قضت محكمة جنح مستأنف النزهة بمعاقبة المتهم بالحبس لمدة ستة أشهر لإدانته بنشر صور إباحية ومعلومات خاصة عن فتاة خليجية علي شبكة الإنترنت وبدأت القضية ببلاغ من الفتاة لمباحث المصنفات الفنية.

ولقد نتج عن الثورة التكنولوجية تلك ظهور نوع جديد من المعاملات يسمى المعاملات الإلكترونية تختلف عن المعاملات التقليدية التى نعرفها، من حيث البيئة التي تتم فيها هذه المعاملات.

ويقصد بالمعاملات الإلكترونية كل المعاملات التى تتم عبر تجهيزات إلكترونية مثل الهاتف، والفاكس، وأجهزة الحواسب، وشبكة الإنترنت، ومؤخراً عن طريق الهاتف المحمول .وتتكون تلك المعاملات من عدد من المكونات الأساسية.

وتتشابه الجريمة الإلكترونية مع الجريمة التقليدية في أطراف الجريمة من مجرم يرتكب الجريمة لدافع معين، ومجني عليه قد يكون شخصا طبيعيا أو شخصا اعتباريا، وأداة تستخدم في ارتكابها ومكان وقوع الجريمة. أما الاختلاف فيكمن في الأداة المستخدمة في ارتكاب الجريمة حيث تكون أداة ذات تقنية عالية في الجرائم المعلوماتية أو الإلكترونية، وأيضا مكان الجريمة حيث في أغلب الأحوال ترتكب الجريمة المعلوماتية عن بعد بسبب وسائل وشبكات الاتصال بين الجاني ومكان الجريمة.

لقد تباينت الصور الإجرامية لظاهرة الجريمة المعلوماتية وتشعبت أنواعها فلم تعد تهدد العديد من الصالح التقليدية التي تحميها القوانين والتشريعات منذ عصور قديمة، بل أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بثورتي الاتصالات والمعلومات .

فبعد أن كان الاعتداء على الاموال يتم بواسطة السرقة التقليدية أو النصب،و كانت الثقة في المحررات الورقية يعتدى عليها بواسطة التزوير، أصبحت هذه الأموال يعتدي عليها عن طريق اختراق الشبكات المعلوماتية واجراء التحويلات الالكترونية من اقصى مشارق الأرض الى مغاربها في لحظات معدودة، كما اصبحت تلك الحقوق الثابتة في الاوعية الورقية يتم الاعتداء عليها في اوعيتها الالكترونية المستحدثة عن طريق اختراق الشبكات والانظمة المعلوماتية دون الحاجة الى المساس باي وثائق أو محررات ورقية.

وبعد ان كانت الحياة الخاصة للإنسان تواجه الاعتداء باستراق السمع أو الصورة الفوتوغرافية، أصبحت هذه الخصوصية تنتهك بواسطة اختراق، البريد الالكتروني والحواسب الشخصية، وقواعد البيانات الخاصة بالتأمين الصحي والمستشفيات ومؤسسات الائتمان والتأمين الاجتماعي. وبالتالي أصبحت الجريمة المعلوماتية ، من أكبر التحديات التي نواجهها في عالمنا المعاصر، إن لم تكن أكبرها على الإطلاق.

أما المصالح المستحدثة، فتتمثل في استحداث مراكز قانونية أفرزتها الحياة الرقمية الجديدة مثل حقوق الملكية الفكرية على تصميم البرامج المعلوماتية، بالإضافة الى حقوق الملكية الصناعية، والاسم التجاري للمواقع الإليكترونية المختلفة، والحقوق الناتجة عن تشغيلها والخدمات التي تقدمها للعملاء.

أهمية البحث:

ترجع أهمية موضوع الجرائم المعلوماتية إلى انتشار استخدامها على الصعيد الدولي والإقليمي والوطني؛ فلم يعد هناك مجال اقتصادي أو اجتماعي أو إداري، إلا وتباشر فيه الحاسبات وتقنية المعلومات دوراً رئيسياً في أدائه وتطويره كالبنوك والمؤسسات الحكومية.

كما أنه لا شك في أن الجريمة المعلوماتية أصبحت مُتلازمة مع الطفرة الهائلة في مجال تكنولوجيا الاتصالات والمعلومات، فمع التقدم المُذهل في استخدامات شبكة المعلومات الدولية (الإنترنت)، طفت الجرائم المعلوماتية بصورها المُختلفة، بالشكل الذي أصبح فيه الأمن المعلوماتي مُهدداً بأساليب إجرامية لم يعرفها القانون من قبل مثل مُحاولات التسلل في وسائل مُعالجة المعلومات وتخزينها واسترجاعها ونقلها بقصد التعديل أو التبديل فيها أو تعطيلها حتى أصبح هناك مجال خصب للإجرام، والاعتداء علي الحقوق المُرتبطة بها ولذلك هناك العديد من التحديات والمخاطر التي تقع على عاتق الأجهزة الأمنية في مواجهة هذه الطائفة من الجرائم.

أضف إلى ذلك ما ترتب على ظاهرة العولمة وثورة الاتصالات والمعلومات من ظهور مفهوم الجريمة العابرة للحدود، والتي أضحت ظاهرة دولية يتعدى خطرها وضررها نطاق الدولة الواحدة.

وكل ذلك أدى إلى ظهور أنواع مختلفة من الجرائم سواء فيما يتعلق بالاعتداء على الأشخاص أو الأموال أو حتى المساس بأمن الدولة، حيث صاحب هذه التقنية جرائم الاعتداء على الشرف والاعتبار والجرائم الأخلاقية والسرقة وغسل الأموال والاعتداء على حقوق الملكية الفكرية، وغيرها.

إشكالية البحث:

واجه القضاء مشكلات في تطبيق أحكام القوانين العقابية التقليدية على الجرائم المعلوماتية، تمثلت في صعوبات فيما يتعلق بأركان هذه الجرائم وارتباطها بشكل أو بآخر بالقسم العام لقانون العقوبات، مما يتعين تطوير أحكام القسم العام في قوانين العقوبات التقليدية لتستجيب لطبيعة الجرائم المعلوماتية ، وهو ماغفلت عنه كثير من الدول مكتفية باصدار تشريعات جديدة (خاصة) تحكم الجرائم المعلوماتية.

ومن هذه الصعوبات وجود عقبات في تطبيق أحكام جريمة السرقة على الأفعال غير المشروعة المرتكبة في الفضاء الافتراضي بسبب صعوبة انطباق الركن المادي للجريمة على الجرائم المرتكبة في العالم الرقمي. واذا كان قسماً من الأفعال غير الشرعية ، في مجال الجريمة المعلوماتية ، يمكن أن يقع تحت أقسام قانون العقوبات التقليدي ، فهناك قسماً يخرج عن إطارها، مما يستدعي إعادة النظر في مجمل قانون العقوبات لكي يتلاءم مع ما تتطلبه المعلومات بوجه صحيح.

كما أن الإجرام المعلوماتي له طبيعة خاصة نظراً لجسامة أخطاره وفداحة خسائره، وتزايد أعدادها، وسهولة ارتكابه، فضلاً عن المُشكلات القانونية الموضوعية والإجرائية التي تثيرها هذه الطائفة من الجرائم.

وأضف إلى ذلك الصعوبات الخاصة بمُكافحة هذه الطائفة من الجرائم، ومنها صعوبة السيطرة على شبكة الإنترنت، وعلى الجرائم التي ترتكب عليها، بل وصعوبة اكتشافها واكتشاف هوية مرتكبيها أو أماكن ارتكابها أو تحديد مصدرها أو إيقافها بالنظر إلى سرعة نشر المعلومات وتسجيلها على أجهزة الحاسبات الخادمة في الخارج.

فهناك فراغ تشريعي في الدول التي تطبق أحكام قانون العقوبات التقليدية على الجرائم المستجدة لعدم إمكان انطباق الركن المادي لجريمة السرقة مثلا على هذه الجرائم؛ لأن المفهوم التقليدي للركن المادي يعني بروز نشاط يرتبط بأشياء مادية ذات وجود محسوس، وأن هذا السلوك المادي أو النشاط المحسوس الذي يستلزمه الفقه والقضاء لتحقق الركن المادي للجرائم المعلوماتية يصعب تحققه في الجرائم المعلوماتية؛ لأن العمليات التي تجري من خلال الحاسوب تجري في فضاء افتراضي غير محسوس.

منهج البحث:

لعل من المناسب استخدام المنهج الوصفي التحليلي في وصف وتحليل وتشخيص موضوع البحث من مُختلف جوانبه وأبعاده، بهدف التوصل إلى نظرة واضحة عن الآليات الملائمة لمكافحة هذه الظاهرة الإجرامية المستحدثة، كما نستخدم المنهج المقارن، لنرى ما وصلت إليه بعض التشريعات العربية أو الأجنبية بهدف تحديد موقف هذه التشريعات من مُكافحة هذه الطائفة من الجرائم.

الباب الأول

الأحكام العامة للجرائم المعلوماتية

تمهيد وتقسيم:

بلغ انتشار استخدامات الحاسب الآلي عبر شبكة المعلومات الدولية؛ ذروته هذه الآونة وهو ما استتبع تدخل القانون كعادته لتنظيم ما يجد من أمور ولبسط حكم القانون على هذه الأنشطة المعلوماتية بالشكل الذي يحمي حقوق المواطنين، حيث أصبحت تجار المعلومات تمثل نسبة ملحوظة من قيمة التجارة الدولية العالمية.

فقد ترك الحاسب الآلي بصمات واضحة في تطوير عدد كبير من الأنشطة اليومية سواء من حيث المضمون أو الشكل أو الزمن أو المسافة. (1)

وبالرغم من أن شبكة المعلومات الدولية "الإنترنت" يمتد نشاطها عبر جميع دول العالم، إلا أنها لا تخضع لهيمنة منظمة أو هيئة أو مؤسسة حكومية أو غير حكومية، ولا توجد إدارة مركزية لها.

---

(1) De Shutter (B) : A propose de la fraude informatique, Revue de droit pénal et criminelle, Avril 1985 , p. 383.

ويرجع سبب ذلك إلى أن شبكة الإنترنت قامت في الأصل على مبدأ الاستعانة بشبكات قائمة وموجودة، فهي في الواقع عبارة عن اتحاد فيما بين شبكات اتصال قائمة تغطي كامل الكرة الأرضية تقريبا. (١)

وهذا الطابع الدولي أو العالمي لشبكة الإنترنت يضع ما يقرب من مائتي دولة في حالة اتصال دائم، وتنتشر المعلومات والبيانات التي يتم إدخالها وتحميلها عبر الشبكة، في ثوان معدودة، في كل الدول المرتبطة بها، وتكون متاحة أمام أي مستخدم في تلك الدول. (٢)

وقد اعتبر البعض(٣) أن اكتشاف المعلوماتية في تاريخ الإنسانية، يمثل أهمية قصوى تفوق اكتشاف الطباعة، خاصة وأن برامج الحاسب الآلي تلعب دوراً مهما في المجال الاقتصادي، حيث إن تكاليف ابتكارها قد يصل إلي الملايين من الدولارات.

وقد تنوعت الجرائم المعلوماتية التي ترتكب بصورة يومية وشملت شتى مجالات النشاط الإنساني، عبر دول العالم بأسرها، وصارت تهدد أمن وسلامة الأفراد والمؤسسات، على حد سواء. ومع تزايد المعلومات واستخدام شبكة الإنترنت في تبادل المعلومات وزيادة أعمال التجارة الالكترونية وغيرها من الأنشطة تزايدت صور الاعتداءات والتهديدات، وظهر العديد من أنماط الجرائم، وهو الأمر الذي تطلب ضرورة التصدي لهذه الطائفة من الجرائم بالشكل الذي يُحقق فاعلية في مواجهتها.

وبات واضحاً أن الحدود الدولية لأي دولة، لم تعد تقف حائلا دون اختراق نظم معلوماتها من خارج حدودها، سواء للحصول بغير حق على هذه المعلومات أو تدميرها ، أو لبث معلومات أخرى إليها، أو حتى لتعطيل كل هذه النظم (٤) .

ولم يعد نطاق الإجرام المعلوماتي قاصرا على المجال الاقتصادي، بل لم لم تسلم منه حرمة الحياة الخاصة للأفراد، واعتبارا من عام ١٩٧٨ بدأت جرائم الفيروسات تلوح في الآفاق، باعتبارها إحدى صور الجرائم المعلوماتية، وهذه الجرائم من شأنه أن تقوض النظام المعلوماتي وتجعله والعدم سواء. (٥)

---

(١) انظر:
Holtgen (D.); internet pour tous, les éditions du téléphone, 2ème éd. 1996.

(٢) انظر:
P.Y. Gautier Suite de la promenade à travers un site immatériel : des condamnations de justice en nature sur Internet Dalloz 1997 chronique p. 176.

(3) G. BRAIBANY, La protection des droits individuels au regard du développement de l'informatique, RIDC, 1971, P. 749.

(٤) د. عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، دراسة تحليلية نقدية لنصوص التشريع المصري مقارنة بالتشريع الفرنسي ، الطبعة الثانية ١٩٩٥م ص ١٣٣ .
Rapport du conseil d 'Etat, Internet et les reseaux - numeriques, la documentation fram sais , Paris 1998, P .202

(٥) انظر:

وتقتضي مكافحة الجرائم المعلوماتية عابرة الحدود توحيد التشريعات المختلفة من ناحية، وأن يكون نظام الإثبات بالدليل الالكتروني (prevue informatique) واحداً بين الدولة التي وقعت فيها الجريمة من ناحية والدولة التي يقيم فيها المتهم، وتتولى المحاكمة عنها من ناحية أخرى، وهذا أمر يستحيل تحقيقه. ولذلك لابد أن يكون هناك تعاون دولي يتفق مع طبيعة الجرائم المعلوماتية عابرة الحدود ، والتي تتميز بطابع خاص يقتضي التصدي له دوليا ([1]) .

نتناول في هذا الباب الأحكام العامة للجرائم المعلوماتية، فنبين مفهوم الجرائم المعلوماتية في فصل أول.

الفصل الأول

مفهوم الجرائم المعلوماتية

تقسيم:

يعيش العالم في الوقت الحاضر وسط أكبر عمليات النهضة العلمية وخصيصاً في مجال تقنية المعلومات الناتجة من الثورة التكنولوجية الهائلة في المعلومات والأنظمة الإلكترونية التقنية، ونتج عن الثورة المعلوماتية ظهور صناعة جديدة وهي صناعة المعلومات بظهور مؤسسات وشركات تهتم بصناعة الأجهزة الإلكترونية وإنتاج البرامج الإلكترونية المسخرة لتشغيل الأجهزة، وهذا ما ظهر فيما يسمى بالحاسوب وبرامجه**([2])**، حيث إن الحاسوب ليس مجرد جهاز ولكنه نظام كامل متكامل يتكون من مجموعة من الأجهزة والتعليمات المخزنة وتكون مداخلات هذا النظام البيانات التي يقوم بمعالجتها وتخزينها في حين تتمثل مخرجاته بالمعلومات أو النتائج، فالحاسوب يدخل في جميع مجالات الحياة اليومية وذلك لتمتعه بالقدرة الفائقة على تخزين قدر كبير من المعلومات ويقوم بتصنيفها وترتيبها بحيث يمكن البحث عنها والحصول عليها بسهولة ويسر بوقت سريع**([3])**.

حيث إن استعمال الحاسوب والشبكات الإلكترونية المتصلة فيه لم ينحصر فقط في عمل الهيئات الإدارية العامة أو الخاصة فقط وإنما امتد استعماله للأفراد ، ولم يعد استعمال الحاسوب قاصراً على الميادين العلمية أو الحسابية البحتة، بل امتد عمل الحاسوب وتقنياته الحديثة حتى اصبح عنصراً أساساً في جميع الأعمال والمعاملات والأنشطة التي يقوم بها الإنسان وتمس حياة الفرد اليومية، حيث أصبح الحاسوب والإنترنت يستخدم في الأعمال الإدارية والحكومية والأعمال التجارية والأمور العسكرية

Sieber (Ulrich); Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique, Rev. Int. Dr. Pén. 1993.vol. 64. p. 53 et s.

([1]) NOVARD (Pierre) ,La procedure penale en matiere in formatique, Bulletins 'actualite, Decembre 1995.

([2]) د. محمد الهيني – التكنولوجيا الحديثة والقانون الجنائي – دار الثقافة لنشر، الأردن ٢٠٠٨، ص ١٥١.

([3]) د. جميل عبد الباقي الصغير –القانون الجنائي والتكنولوجيا الحديثة – دار النهضة العربية، القاهرة ١٩٩٢، ص٩.

والحربية وكذلك في الأعمال الطبية والصناعية والحسابية والهندسية والتعليمية، حيث أصبح استخدام الحاسوب والإنترنت يشمل جميع مجالات الحياة التي تهم الإنسان([1]).

ونتيجة لثورة المعلومات والتكنولوجيا الهائلة في الأنظمة والبرامج الإلكترونية والمعلوماتي والتي أدت إلى فتح الأبواب على مصراعيها لظهور صور من السلوك الجرمي المنحرف والغير ممكن توقعه([2])، حيث أدى الاستخدام المستمر للأنظمة الحاسوبية والمعلوماتية إلى ظهور أساليب جرمية حديثة تسمى جرائم الحاسوب أو جرائم الإنترنت أو الجرائم المعلوماتية، حيث تم استخدام التقنية الحديثة في ارتكاب أعمال جرمية، حيث إن بعض الجرائم قد ترتكب على الحاسوب والأنظمة المعلوماتية، و تكون المعلومات الهدف أو الغاية التي يسعى إليها الجاني([3])، ولهذا سوف نتحدث في هذا الفصل عن مفهوم الجرائم المعلوماتية من حيث التعريف والخصائص وذلك في المبحثين التاليين كما يلي:

المبحث الأول

تعريف الجريمة المعلوماتية

إن الجريمة في نطاق القانون الجنائي تعرف بأنها عبارة عن عمل أو امتناع يرتب القانون على ارتكابه عقوبة([4])، وكذلك تعرف بأنها السلوك الإنساني المحظور الذي يخل بأمن المجتمع وسلامته، أو كل تصرف أو ترك حرمه المشرع وقرر له العقوبة المناسبة أو التدابير الاحترازية([5])، وعرفت الجريمة أيضاً بأنها كل عمل أو امتناع بجرمه النظام القانوني ويقرر له جنائياً هو العقوبة التي توقعها الدولة عن طريق الإجراءات الأصول التي رسمها المشرع([6])، أما تعرفنا للجريمة فهو كل أمر يحظره المشرع عن طريق العقاب الجنائي بالقيام بعمل أو الامتناع عن عمل إذا لم يقع استعمالاً لحق أو أداء لواجب.

ومن خلال التعريفات السابقة للجريمة يتبين لنا أن هناك أربعة عناصر لا بد من تحققها للقول بأن هناك جريمة وهذه العناصر هي:

- وجود سلوك أو تصرف قد يكون في صورة عمل أو الامتناع عن عمل يلزم القانون القيام به.
- تعتبر الجريمة فعل غير مشروع إذا وجد نص في قانون العقوبات أو القوانين العقابية الأخرى الملحقة به أو المكملة له تجرم هذا الفعل وأن لا يكون هناك سبب من أسباب التدبير والإباحة.

([1]) د. محمد الأمين البشري – التحقيق في الجرائم المستحدثة – منشورات جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٤، ص ٨٥.

([2]) د. عبدالعال الدربي ومحمد إسماعيل – الجرائم الإلكترونية – المركز القومي للإصدارات القانونية، القاهرة ٢٠١٢، ص ٣٩.

([3]) محمد علي سالم وحسون هجيج – الجريمة المعلوماتية – بحث منشور في مجلة بابل، العدد ٢ سنة ٢٠٠٧، ص ٨٥.

([4]) د. محمد علي عياد – شرح قانون العقوبات، القسم العام – دار الثقافة للنشر، الأردن ١٩٩٧، ص ٩٣.

([5]) د. محمود محمود مصطفى - شرح قانون العقوبات – دار النهضة العربية – القاهرة ١٩٨٠ – ص ٣٣.

([6]) سيد أنور سالم وآمال عثمان – علم الإجرام وعلم العقاب – دار النهضة العربية – القاهرة ١٩٨٠، ص ٦٦.

- أن يكون الفعل غير المشروع قد صدر من الجاني عن إرادة جنائية وتمتعه بالوعي والإدراك، لأنه إذا انتفت الإرادة الجنائية فإن الأمر يصبح من موانع العقاب.
- وجود جزاء جنائي يقرره المشرع على هذه الأفعال وتطبقه المحاكم في القضاء التي تعرض عليها(١).

أما تعريف الجرائم المعلوماتية فقد عرف الفقه القانوني والدارسون هذه الجريمة بعدة تعريفات تتمايز وتتباين تبعاً لموضوع العلم المنتمية إليه وتبعاً لمعيار التعريف ذاته، فاختلفت تلك التعريفات وفقاً لما يأتي:

١– معيار موضوع الجريمة

٢– معيار آليات ارتكاب الجريمة

ولهذه سوف نتناول تعريف الجريمة الإلكترونية في هذا المبحث وبيان ذلك في المطالب التالية:

المطلب الأول

تعريف الجريمة المعلوماتية وفق معيار موضوع الجريمة

هناك مجموعة من التعريفات استندت إلى معيار موضوع الجريمة(٢) وإلى أنماط السلوك محل التجريم ، فأنصار المعيار الموضوعي يستندون في تعريفهم بالجريمة المعلوماتية أن يكون الحاسوب والمعلومات هي محل الجريمة، فيجب أن يتم الاعتداء على الحاسوب أو على نظامه المعلوماتي، وكذلك يستندون إلى معيار شخصي يستوجب أن يكون الجاني ملماً بتقنية المعلومات واستخدام الحاسوب لإمكانية اعتبارها من جرائم تقنية المعلومات الإلكترونية(٣).

والجريمة المعلوماتية عرفت من قبل أنصار المعيار الموضوعي بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه"(٤)، وعرفها الأستاذ (Artarso Lerz) بأنها " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطاً بتقنية المعلومات"(٥)، ويلاحظ على تعريف الأستاذ (Artarso) أنه يتطلب الفعل مما يقع ضمن نطاق قانون العقوبات، وفي هذا الافتراض مسبق على شمول نصوص قانون العقوبات لأنماط السلوك الإجرامي فمن جرائم الحاسوب وهي مسألة لا تراعي الجدل الذي لم ينتهي حول مدى انطباق قواعد التجريم التقليدية على هذه الأفعال، والذي حسم تقريباً لجهة عدم انطباق نصوص القانون القائمة والحاجة إلى

(١) د. عبد الرحمن توفيق أحمد – شرح قانون العقوبات، القسم العام – دار الثقافة للنشر، الأردن ٢٠١١، ص ٣٧.

(2) Cybercriminalité: enjeux, sources de données et faisabilité de recueillir des données auprès de la police, Centre canadien de la statistique juridique, p6.

(٣) محمود عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر، الأردن، ٢٠٠٥، ص ١٦.

(4) Michel Alexander, computer crime –uglg secret for business, computer world, vol,Xx iv, No 11, 1990, PP. 104.

(٥) خالد عياد الحلبي – إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت – دار الثقافة للنشر، الأردن ٢٠١١، ص ٢٨.

نصوص خاصة تراعي العناصر المميزة للجريمة المعلوماتية عن غيرها من الجرائم التي عرفها قانون العقوبات(١).

كما عرفها(مكتب المحاسبة العامة للولايات المتحدة الأمريكية) بأنها "الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة وإساءة استخدام المخرجات، وإضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيداً من الناحية التقنية مثل تعديل الحاسوب وبرامجه ومعلوماته" (٢)، وكذلك عرفت بأنها كل سلوك غير مشروع أو غير مسموح به يتعلق بالمعالجة الآلية للبيانات والمعلومات أو نقل هذه البيانات أو المعلومات"(٣)، وعرف الفقيه (Merwe) الجريمة المعلوماتية بأنها الفعل غير المشروع الذي يتورط في ارتكابه الحاسوب أو هو الفعل الإجرامي الذي يستخدم في اقترفاه الحاسوب كأداة رئيسية"، حيث إن تعريف (Merwe) جاء مقصوراً على الإحاطة بأوجه الظاهرة الإجرامية(٤).

ويعرف Tiedmann الجريمة المعلوماتية بأنها " كل جريمة ترتكب ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات"، أو هي "كل أشكال السلوك غير المشروع (أو الضار بالمجتمع) التي ترتكب باستخدام الحاسب".(٥)

ويعرفها الأستاذ (Mass) فقد عرف جرائم المعلوماتية بأنها "الاعتداء القانوني الذي يرتكب بواسطة المعلومات الحاسوبية بغرض تحقيق الربح"(٦)، حيث إن الأستاذ (Mass) قد ربط الجريمة بتحقيق الربح، أي ربط القاعدة الجزائية بالغاية من الفعل فالأصل أن الغاية لا تعتبر ركن من أركان التجريم وبالتالي لا علاقة لها بالتجريم وهي ليست عنصراً فيه بغض النظر عن طبيعتها مشروع في ذاتها أم لا، ولذا فيقتصر مفهومه لجرائم المعلوماتية على الحالات التي يقصد فيها المجرم تحقيق الربح، وهذا الأمر غير منطقي وغير مقبول حيث يمكن أن ترتكب الجرائم المعلوماتية لغير تحقيق الربح(٧).

وكذلك عرفت الجريمة المعلوماتية بأنها "السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإغلاق المعلومات أو إساءة استخدامها مما يتسبب أو يحاول التسبب إما في إلحاق الضرر بالضحية أو حصول الجاني على فوائد لا يستحقها(٨)، ونجد بأن هذا التعريف قد ربط الجريمة المعلوماتية بإلحاق

---

(١) د. يونس عرب – دليل أمن المعلومات والخصوصية - ج١، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، ط١، الأردن ٢٠٠٢، ص ٢١٤.

(٢) مشار إليه لدى د. علي القهوجي – الحماية الجنائية لبرامج الحاسوب- الدار الجامعية للنشر، الإسكندرية ١٩٩٧، ص ٢.

(٣) د. هدى قشقوش – جرائم الحاسب الإلكتروني – دار النهضة العربية، القاهرة ١٩٩٢، ص ١٨.

(٤) د. عبدالعال الدربي ومحمد إسماعيل – الجرائم الإلكترونية – المركز القومي للإصدارات القانونية، القاهرة ٢٠١٢، ص ٤١.

(5) Tiedmann (K.): Fraude et autres délits d'affaires commise l'aide d'ordinateurs électroniques. Revu. dr. pén. crim. 1984. P. 612.

(6) Masse (M.): L'utilasation abusive de D.A. B. Rev. Experts des systet d'information, novembre 1981, p. 6.

(٧) أسامة المناعسة وجلال الزعبي – جرائم الحاسب الآلي – دار وائل للنشر، الأردن ٢٠٠١، ص ٧٥.

(٨) المهندس حسن داود – جرائم نظم المعلومات – أكاديمية نايف العربية للعلوم الأمنية، الرياض ٢٠٠٠، ص ٢٣.

الضرر بالمجني عليه أو محاولة التسبيب بالضرر له، حيث إن القاعدة العامة في القانون الجنائي لا ترتب العقاب والتجريم على حصول الضرر أم لا سواء أكان متعمد أم غير متعمد فقد تكون نتجية الجريمة تامة إذا حصلت النتجية كما هي الحال في جرائم القتل و السرقة و الأغتصاب حيث تسمى هذه الجرائم (جرائم الضرر) وفي بعض الجرائم تكون النتجية محتملة لحدوث الضرر دون وقوعه فعلاً كما في جرائم حمل السلاح من غير الترخيص و المؤامرة و التحريض على أرتكاب الجرائم ويدعى هذا النوع من الجرائم ب (جرائم التعريض للخطر) وقد يكون جرائم لها وجود مادي محسوس ومنها له وجود معنوي غير محسوس، فالقاعدة العامة الجنائية تعاقب على القيام بالفعل الجرمي سواء تحققت النتيجة أم لا، لأنه إذا لم تتحقق النتيجة فإن الجاني يعاقب على الشروع فيها، ونجد أن الجاني ما دام قد قام بالفعل سواء كان بهدف إلحاق الضرر بالغير أو عدم الإضرار به فإن الركن المادي للجريمة يكون متوافرا، ولهذا فإنني لا أتفق مع هذا التعريف.

وكذلك تعرف الجريمة المعلوماتية بأنها "غش المعلوماتية وهي كل سلوك غير مشروع يتعلق بالمعلومات المعالجة نقلها" حيث إن محل الجريمة المعلوماتية يتصور من زاويتين، الزاوية الأولى إذا كانت المعلومات جانية، فتكون المعلوماتية أداة أو الاعتداء، حيث إن الجاني يستخدم التقنية المعلوماتية في تنفيذ جرائمه الإلكترونية سواء أكانت الجريمة موجهة ضد الأشخاص أو الأموال، أما الزاوية الثانية وهي محل الاعتداء فالجاني يتجه قصده الجرمي إلى الاعتداء على الشيء أو المال المعلوماتي ذاته، فهذا الشيء أو المال المعلوماتي هنا قد يكون الحاسوب بجميع مكوناته المادية والمعنوية أو الشبكات أو البرامج أو المعطيات(١). والغش المعلوماتي هو "الاعتداء غير المشروع الذي يرتكب عن طريق نظم المعلومات بغرض تحقيق ربح"(٢)، أو هو "مجموعة الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب".(٣)

كما تم تعريفها على أنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة، عن الاستخدام غير المشروع لتقنية المعلومات".(٤)

وأيضاً عرفت الجريمة المعلوماتية وفقاً للمعيار الموضوعي على أنها "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كانت مرتبطة بتقنية المعلومات"(٥)، وأرى بأن هذا التعريف قد ربط الجريمة المعلوماتية فقط بالأنماط المعروفة في قانون العقوبات أي بالأنماط المعروفة بالجريمة التقليدية، وهذا مفهوم ضيق بحيث لا يتسع للأنماط الحديثة التي سوف تظهر في المستقبل نتيجة التطور العلمي الهائل

---

(١) د.علي القهوجي – الحماية الجنائية البيانات المعالجة إلكترونية – ورقة عمل قدمت إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، الإمارات مايو ٢٠٠٠، ص ٥٦١.

(2) Masse (M.): L'utilasation abusive de D.A. B. Rev. Experts des systet d'information, novembre 1981, p. 6.

(3) Vivant et Le Stanc, Lamy droit de l'informatique, 1989, no. 2323. p.1540.

(4) Bart De Schutter; La criminalité liée à l'informatique, Rev. dr. Pen.Cr. No 1. 1985. p.390.

(٥) د. هشام محمد رستم – قانون العقوبات ومخاطر تقنية المعلومات – مكتبة الآلات الحديثة، أسيوط ١٩٩٢، ص ٣١.

في مجال المعالجة الآلية والإلكترونية للمعلومات، فقد يظهر في المستقبل أنماط وصور جديد للجريمة المعلوماتية لم تكن معروفة.

وكذلك عرفت وفقاً للمرجع العالمي ويكيبيديا (wikipedia) بأنها "نشاط جرمي مصدره الحاسوب أو الشبكة المعلوماتية وهي قد تكون أداة ارتكابه أو هدفه أو مكان ارتكابه، وهذا التعريف يركز على أهم الوسائط الإلكترونية الحديثة بصفتها موضوعاً للجريمة المعلوماتية(١).

وما من شك في أن معيار موضوع الجريمة كأساس للتعريف، معيار من أهم المعايير وأكثرها قدرة على إيضاح طبيعة ومفهوم الجريمة في مجمل التعريف، على أن لا يغرق في وصف الأفعال، إذ قد لا يحيط بها، وإذا سمى الإحاطة بها فإنه سيغرق بالتفصيل الذي لا يستقيم بغرض وشكل التعريف، و هذا بالإضافة إلى عدم وجود اتفاق حتى الآن على الأفعال المنطوية تحت وصف جرائم الحاسوب(٢).

المطلب الثاني

تعريف الجريمة المعلوماتية وفق معيار آليات ارتكاب الجريمة

لقد تناولنا في المطلب السابق عن تعريف الجريمة المعلوماتية وفق المعيار الموضوعي المستند إلى محل الجريمة وهي المعلومات الإلكترونية، أما في هذا المطلب سوف نتطرق إلى تعريف الجريمة المعلوماتية إلى آليات ارتكاب الجريمة، حيث إن هذه التعريفات المستندة إلى وسيلة ارتكاب الجريمة المعلوماتية ، وهي تلك التي يتوجب أن يكون لمقترفها معرفة تقنية كافية بالحاسوب والأنظمة المعلوماتية الإلكترونية وكذلك بالشبكات.

ويستند أنصار التعريف وفق آليات ارتكاب الجريمة المعلوماتية إلى وسيلة ارتكاب الجريمة المعلوماتية الإلكترونية، حيث يشترطون وجوب ارتكابها بواسطة النظام المعلوماتي الإلكتروني، أي أن هذا الاتجاه جعل الوسيلة الإلكترونية شرطاً في قيام الجريمة المعلوماتية(٣)، حيث إن هذه الجرائم لا تقع على الحاسوب أو على المعلومات أو على البرامج المعلوماتية فقط، ولكنها تقع باستخدام الأنظمة المعلوماتية الإلكترونية كوسيلة لتنفيذها، فلا يكون النظام المعلوماتي الإلكتروني أو الحاسوب هو محل الحماية الجنائية، بل أن أموال الغير هي التي يجب أن تحظى بهذه الحماية وذلك بإتقاء مخاطر الأنظمة الإلكترونية

(١) د.عادل سقف الحيط- جرائم الذم والقدح والتحقير المرتكبة عب الوسائط الإلكترونية – دار الثقافة للنشر، الأردن ٢٠١٥، ص ٣٨.
(٢) خالد عياد الحلبي – إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت – دار الثقافة للنشر، الأردن ٢٠١١، ص ٢٩.
(٣) د. يوسف العفيفي – الجرائم الإلكترونية في التشريع الفلسطيني – رسالة ماجستير، الجامعة الإسلامية بغزة – فلسطين ٢٠١٣، ص ١٠.

والحاسوب، والفاعل في هذه الجريمة هو مستخدم النظام الإلكتروني أو الحاسوبي، أما الجهاز فليس إلا الوسيلة المستخدمة في ارتكاب الجريمة التي يتمثل محلها في الحق الذي تم المساس به([1]).

وهناك عدة تعريفات انطلقت مستندة إلى وسيلة وآلية ارتكاب الجريمة، فقد عرفها الأستاذ (جون فورستر) بأنها "فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"، وكذلك عرفها الأستاذ تاديمان (Tredmann) بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"([2])، وأرى أن هذين التعريفين قاصران لأنهما جعلا الوسيلة الوحيدة في ارتكاب الجريمة المعلوماتية الإلكترونية فقط من خلال جهاز الحاسوب، وأرى أن هذه الجريمة قد تقع من أي جهاز يعتمد على النظام المعلوماتي الإلكتروني مثل جهاز الهاتف النقال خصوصاً الأجهزة الذكية الحديثة وكان عليهما أن يستبدلا كلمة حاسوب بجهاز إلكتروني أو معلوماتي.

وكذلك انتُقِد هذان التعريفان لأنهما يستدعيان الرجوع إلى العمل الأساسي المكون لها وليس فقط للوسائل المستخدمة لتحقيق الجريمة([3]).

وكذلك عرفت بأنها "كل سلوك سلبي أو إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأي صورة كانت"، وأيضاً عرفت من قبل خبراء المنظمة الأوروبية للتعاون الاقتصادي بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو ينقلها"([4]).

وعرفت الجريمة المعلوماتية على أنها "الجرائم الناتجة عن استخدام المعلوماتية والتقنية الحديثة المتمثلة بالحاسوب والإنترنت في أعمال وأنشطة إجرامية بهدف أن تحقق عوائد مالية ضخمة يعاد ضخها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الإلكترونية وممارسة الأنشطة التجارية عبر هذه الشبكة"([5])، ونجد من هذا التعريف أنه جعل محل الجريمة المعلوماتية هي التي تقع على أموال بطرق إلكترونية دون التطرق إلى الجرائم الأخرى مثل جريمة الاختراق للمواقع دون سلب النقود أو جريمة إتلاف المواقع والمعلومات، ولهذا أرى أن هذا التعريف قاصراً على إعطاء المعني الوافي للجريمة المعلوماتية.

وأيضاً عرفها الفقيهان الفرنسيين فيفنت وليستتك (Lestanc & Vivant)

بأنها "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب"([6])، ومن هذا التعريف نجد بأنه مستند على معيارية احتمال جدارة الفعل بالعقاب، وهو معيار غير منضبط البنية، ولا يستقيم كتعريف قانوني وإن كان يصلح لتعريف في نطاق علوم الاجتماع أو غيرها([1]).

([1]) د. جميل عبد الباقي الصفير –القانون الجنائي والتكنولوجيا الحديثة – دار النهضة العربية،القاهرة ١٩٩٢، ص ١٥.
([2]) خالد عياد الحلبي – إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت – دار الثقافة للنشر، الأردن ٢٠١١، ص ٢٩.
([3]) د. يونس عرب – دليل أمن المعلومات والخصوصية - ج١، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، ط١، الأردن ٢٠٠٢، ص ٢١٤.
([4]) حمزة بن عفون – السلوك الإجرامي للجرم المعلوماتي - رسالة ماجستير، جامعة الحاج الخضر ، الجزائر ٢٠١٢، ص ١٥.
([5]) عبدالله عبد الكريم عبدالله – جرائم المعلوماتية والإنترنت – منشورات الحلبي الحقوقية،بيروت ٢٠٠٧، ص ١٥.
([6]) د. محمد الشوا - ثورة المعلومات وانعكاسها على قانون العقوبات- دار النهضة العربية - القاهرة ١٩٩٤، ص٦.

وكذلك عرف خبراء متخصصون من بلجيكا للجريمة المعلوماتية في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية ((OECD)) بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"(٢)، إن هذه التعريف متبني من قبل العديد من الفقهاء ويعتبر لديهم أنه من أفضل التعريفات لأنه واسع يتيح الإحاطة الشاملة قدر الإمكان بظاهرة جرائم تقنية المعلومات وكذلك لأنه يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها وكذلك يتيح إمكانية التعامل مع التطورات المستقبلية للتقنية المعلوماتية(٣).

ونجد من التعريف السابق بأنه يشير إلى إمكانية وقوع الجريمة المعلوماتية بالسلوك السلبي أي الامتناع وكذلك أحاط هذا التعريف وقوع الجريمة بطريقة مباشرة وغير مباشرة الحق المعتدي عليه، ولذلك أتسم بالشمول.

كما عرف الجريمة المعلوماتية الأستاذ شولدن هاشت (Sheldon J Hecht) بأنها "واقعة تتضمن تقنية الحاسوب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمداً ويمكنه الحصول على مكسب"(٤)، وكذلك يوجد تعريف قريب منه هو تعريف الأستاذ باركر (Parker) الذي يعرف الجريمة المعلوماتية بأنها "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتي ،ينشأ عنه خسارة تلحق بالمجني عليه و كسب يحققه الفاعل "(٥)، ونجد من هذين التعريفين أنهما تعريفين وصفيين للجريمة ولا يقوما على تحديد ماهيتها، وكذلك يعتمدان على معيار تحقق أو احتمال تحقق خسارة المجني عليه وهذا المعيار لا يتضمن نطاقه حالات اختراق النظام المعلوماتي الإلكتروني والبقاء فيه دون أي مسلك آخر من شأنه تحقيق أو احتمال تحقيق خسارة ، وكذلك اعتمد على أن الجاني قد يكون غايته الحصول على مكسب، حيث تكون غاية الجاني في بعض الحالات ليس الحصول على أي مكسب، وكذلك نجد بأن التعريفين تضمنا حصول هذه الجريمة بشكل مقصود حيث يمكن أن تقع هذه الجريمة بشكل غير مقصود نتيجة الخطأ أو بالتالي يتوجب على الشخص الذي قام بهذه الجريمة بشكل غير مقصود أن يتلقى عقابا لكنه أخف من الجريمة المقصودة.

وأيضاً عرفت بأنها "جرمية تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات و يطال اعتداءاها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات"(٦)، ونجد بأن هذا التعريف قد جاء بدون أن يذكر أن النظام المعلوماتي وسيلة في ارتكاب الجريمة وإنما قد اعتمد على أن المعلومات والنظام المعلوماتي هي محل الجريمة المرتكبة.

---

(١) د. يونس عرب – دليل أمن المعلومات والخصوصية - ج١، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، ط١، الأردن ٢٠٠٢، ص ٢١٩.

(2)Bart de Schutter, La Criminalite Liee a Linfprmatlque, R.D.P/C, No 1, 1986, P.390.

(٣) د. هشام محمد رستم – قانون العقوبات ومخاطر تقنية المعلومات – مكتبة الآلات الحديثة، أسيوط ١٩٩٢ ص ٣٥.

(٤) د. يونس عرب – دليل أمن المعلومات والخصوصية - ج١، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، ط١، الأردن ٢٠٠٢، ص ٢١٦.

(٥) رصاع فتيحة – الحماية الجنائية للمعلومات على شبكة الإنترنت – رسالة ماجستير، جامعة أبي بكر بلقايد، الجزائر ٢٠١٢، ص ٤٠.

(٦) د. عبد الله محمود – إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات – بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية – دبي ٢٠٠٣، ص ٥٨٩.

أما المؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في النمسا سنة ٢٠٠٠ قام بتعريف الجريمة المعلوماتية من ضمن توصيات المؤتمر بأنها " يقصد بالجريمة المعلوماتية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وهذا الجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"([1]).

وكذلك عرفت الجريمة المعلوماتية بأنها "هي الجرائم التي يكون فيها الحاسوب وسيلة ارتكاب فعل غير مشروع أو محل لوقوع الفعل غير المشروع وذلك بالقيام بعمل أو الامتناع عن أدائه، من شأنه الاعتداء على الأموال المادية أو المعنوية،حيث شرط أن يكون مرتكبها على معرفة تقنية في استخدام الحاسوب والتعامل بمعطياته"([2])، ونجد بأن هذين التعريفين جاءا شاملين ووافيين في تعريف الجريمة المعلوماتية عندما بينا أن الجريمة قد تقع بواسطة النظام المعلوماتي الإلكتروني أو أن يكون هذا النظام محلا للجريمة بأي فعل جرمي إيجابي أو سلبي ويشمل جميع أنواع هذه الجريمة، ولكن نجد أن التعريف الثاني للأستاذ الحلبي بأنه حدد وسيلة ارتكاب الجريمة بواسطة الحاسوب، حيث أنه في هذا الوقت الحاضر يمكن ارتكب هذه الجريمة بواسطة أجهزة إلكترونية أخرى مثل الهاتف المحمول، وعلما أنه يقصد من مصطلح الحاسوب أي جهاز إلكتروني معلوماتي تتم بواسطته ارتكاب الجريمة المعلوماتية.

ونجد بعض الآراء الفقهية قد انتقدت الجريمة المرتكبة بواسطة النظام المعلوماتي الإلكتروني على اعتمادها على الوسيلة المستخدمة في الارتكاب ، وأنه يجب الرجوع إلى الفعل والأساس المكون لها و إلى الوسائل المستخدمة لتنفيذها في الجريمة لذلك يتعين أن نعتبرها من الجرائم المعلوماتية ، حيث لا يمكن الاعتماد على الوسيلة المستخدمة في الجريمة دون الرجوع إلى العمل الأساسي المكون لها([3]).

ونجد كذلك جانباً من الفقه يحلل الجريمة المعلوماتية من خلال العلاقة أو الصلة بين النظام الإلكتروني وارتكاب بعض الجرائم، وذلك نتيجة طبيعية للتطور التكنولوجي الحالي، سواء كان استخدام النظام المعلوماتي الإلكتروني كمحل للجريمة أو كان وسيلة للجريمة، وأصبح انتشار الوسائل المعلوماتية يزيد من فرص انتشار هذا النوع الجديد من الجرائم أو الأفعال غير المشروعة المتعلقة بالمعلوماتية المعالجة إلكترونياً([4]).

ولقد عرفت الجريمة المعلوماتية من وجهة نظري بأنها "هي الفعل غير المشروع التي يكون فيها النظام المعلوماتي الإلكتروني أداة لتنفيذ العمل الجرمي المراد تحقيقه أو الفعل الموجه ضد النظام المعلوماتي أو المعلومات المخزنة في الأنظمة أو على الشبكات الإلكترونية بأفعال مجرمة سواء كانت الجريمة إيجابية أو سلبية من شخص على دراية كافية مع التعامل مع التقنية الإلكترونية للمعلومات وبشكل مقصود ومتعمد".

([1]) أسامة المناعسة وجلال الزعبي – جرائم الحاسب الآلي – دار وائل للنشر، الأردن ٢٠٠١، ص ٧٨.

([2]) خالد عياد الحلبي – إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت – دار الثقافة للنشر، الأردن ٢٠١١، ص ٣١.

([3]) محمد الكعبي – الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت – دار النهضة العربية، القاهرة، ص ٣٤.

([4]) د. هدى قشقوش – الإتلاف لعمدي لبرامج وبيانات الحاسب الإلكتروني – بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات ٢٠٠٠، ص ٤.

والغاية من اختياري لهذا التعريف للجريمة المعلوماتية يرجع لاستناد هذا التعريف إلى أكثر من معيار لتحديد ماهية الجريمة المعلوماتية، **فالمعيار الأول** يستند إلى وسيلة الجريمة المرتكبة بواسطة الأنظمة المعلوماتية الإلكترونية **والمعيار الثاني** يتمثل في طبيعة محل الجريمة بالاعتداء على النظام المعلوماتي الإلكتروني أو على المعلومات أما **المعيار الثالث** المستند على السلوك الجرمي بصورته الإيجابية أو السلبية والتعمد في تنفيذ الجريمة.

ولعل سبب اختلاف التعريفات المتعلقة بالجرائم المعلوماتية هو أن لكل باحث مشهود له بالخبرة في هذا المجال تعريفا خاصا للجريمة المعلوماتية، يحدد مدلول لها ومنه ينطلق في بحثها. **(١)**

المبحث الثاني

خصائص الجريمة المعلوماتية وطبيعتها

إن الجرائم العادية التقليدية لها خصائص وسمات تتصف وكذلك لها طبيعة قانونية تخص كل جريمة عن الأخرى، والجرائم المعلوماتية التي تزهر في عصر التطور العلمي والثورة الهائلة في مجال التكنولوجيا الرقمية وكون هذه الجرائم حديثة ومتطورة فإن لها خصائص منفردة تتميز بها عن غيرها من الجرائم التقليدية وكذلك لها طبيعة قانونية تميزها عن غيرها، ولهذا سوف نتناول في هذه المبحث هذه الخصائص والطبيعة ذلك في المطلبين التاليين على النحو الآتي:

المطلب الأول

خصائص الجريمة المعلوماتية

أنشئت شبكة المعلومات والاتصالات الدولية المعروفة بشبكة الإنترنت من قبل الولايات المتحدة الأمريكية في الستينيات من القرن العشرين بهدف خدمة التأهب السريع للقوات المسلحة حال نشوب حرب نووية أو أي هجوم نووي عليها. وبعد زوال التهديد النووي بانهيار الاتحاد السوفيتي في بداية التسعينيات من القرن الماضي، انتفى التهديد العسكري لهذه الشبكة، وتحولت لخدمة أغراض أخرى مدنية، وشارك في الاستفادة منها العديد من الشركات والجامعات والمؤسسات الخاصة. **(٢)**

إن انتشار شبكة المعلومات الدولية "الإنترنت" أدى إلى التغير التقني المتزايد والمتعاظم في هذا المجال وإلى سهولة تداول المعلومات ، ومن ثم ساعد على ارتكاب الجريمة المعلوماتية عن طريق الحاسوب أو أي نظام إلكتروني، ولهذا فإن السياسة الجنائية الحديثة تستدعي المحاولة في حصر الخصائص التي تتميز بها الجرائم المعلوماتية عن غيرها من الجرائم العادية ذلك من أجل مكافحة هذا النوع من الجرائم المستحدثة التي رافقت التطور التقني الذي يمر به عالمنا المعاصر بفضل التطور التكنولوجي الهائل وثورة المعلومات، فهذه الجرائم أصبح لها شكل آخر عن الجرائم التقليدية بأسلوب وطريقة مختلفة ، ولهذا سوف

([1]) Bart De Schutter; ibid. p.389.

([2]) Tortelo (N.) et Liontier (R.): internet pour les jurists, Paris.Dalloz. 1996. P. 2.

نتناول في هذا المطلب بعض الخصائص التي جعلتها ظاهرة إجرامية جديدة لم يعرفها العالم من قبل، واختلافها عن الجرائم التقليدية التي ترتكب في العالم المادي، وذلك على النحو التالي:

أولاً: الجريمة المعلوماتية جريمة عابرة للحدود

أخذت تكنولوجيا المعلومات تلعب دوراً بالغ الأهمية في العالم المعاصر، فغزت الأسواق سواء الخاصة بالدول المتقدمة صناعياً أو دول العالم الثالث، فالدول المتقدمة صناعياً تقوم بتصنيع أجهزة الحاسب الآلي وابتكار برامج ومصنفات لتحقيق الربح المادي، وتقوم دول العالم الثالث باستقبال هذه المبتكرات وتستخدمها على نطاق واسع لصغر حجمها وقلة كلفتها وتزايد الحاجة إليها، وهذا التطور التكنولوجي في مجال الأنظمة المعلوماتية الإلكترونية والبرامج وخاصة الشبكة الدولية للمعلومات الإنترنت (Internet)، وجعل الإنتاج الذهني يتصف بالعالمية، لأنه لا يقتصر على دولة دون أخرى، فالبشرية كلها شريكة في الاستفادة من هذا الإنتاج الأدبي والفني([1]).

ففي عصر الحاسوب والأنظمة المعلوماتية الإلكترونية ومع انتشار الشبكة الدولة للمعلومات الإنترنت وأمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، حيث أصبح أمر التنقل والاتصال بينها أمراً سهلاً، طالما حدد اسم الموقع المراد أو الذي تم العثور عليه من خلال مواقع البحث الإلكتروني أو عند تحديد العنوان الإلكتروني للمرسل إليه أو عند معرفة كلمة السر للدخول([2])، حيث إن ربط عدد مهول من الأجهزة الإلكترونية عبر شبكة الإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمراً ممكنا وشائعاً لا يعترف بالحدود الإقليمية للدول ولا بالمكان ولا بالزمان وأصبحت ساحتها العالم أجمع([3]).

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([4]).

فالسهولة في حركة المعلومات عبر أنظمة الحديثة جعل بالإمكان ارتكاب الجريمة عن طريق جهاز الكتروني موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى، وذلك راجع إلى أن مجتمع

([1]) محمود عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر، الأردن، ٢٠٠٥، ص ٣٤.
([2]) أسامة المناعسة وجلال الزعبي – جرائم الحاسب الآلي – دار وائل للنشر، الأردن ٢٠٠١، ص ١٠٥.
([3]) د. عبدالعال الدربي ومحمد إسماعيل – الجرائم الإلكترونية – المركز القومي للإصدارات القانونية، القاهرة ٢٠١٢، ص ٢٥.
([4]) Mascala Coeinne "Criminalité et contrat électronique ll. IN: Le contrat électronique, Travaux de l'association Capitant Henri, Journées National, Paris, 2000, p. 119.

المعلومات لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود([1]).

ففي مجتمع المعلومات تذوب الحدود الجغرافية بين الدول، لارتباط العالم بشبكة واحدة، حيث إن أغلب الجرائم المرتكبة عبر شبكة الإنترنت، يكون الجاني فيها في دولة ما والمجني عليه في دولة أخرى، وقد يكون الضرر المترتب عن الجريمة ليس واقعاً على المجني عليه داخل إقليم دولة الجاني، وتعارض المواد المعروضة مع الثقافات المتلقية لها خاصة إذا كانت تتعارض في الدين والعرف والنظام الاجتماعي والأخلاقي والسياسي للدولة([2]).

ونرى بأن السهولة في حركة المعلومات عبر أنظمة وبرامج التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طرق النظام الإلكتروني موجود بدولة معينة بينما يتحقق الفعل الجرمي والنتيجة في دولة أخرى.

وهذا يرجع للطبيعة التي تتميز بها الجريمة المعلوماتية بأنها جريمة لا حدود لها ، مما يسبب العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب تطبيقه، بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام([3]).

ونجد بأن الجريمة المعلوماتية هي نوع من الجرائم التي يتم ارتكابها عبر المسافات، حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد وهو يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة، بحيث يتباعد المسافات بين الفعل الذي يتم من خلال جهاز الفاعل وبين النتيجة أي المعطيات وهي محل الاعتداء، وبالتالي لا تقف الجريمة المعلوماتية عند الحدود الإقليمية لدولة معينة بل تمتد إلى الحدود لدولة أخرى مما يزيد من صعوبة اكتشافها.

فالتحقيق في الجرائم المعلوماتية يتطلب القيام بإجراءات وأعمال للتحقيق خارج حدود الدولة، مثل تفتيش المواقع الإلكترونية أو تفتيش الأجهزة الإلكترونية – المادية – للعثور على البيانات أو المعلومات، أو إلقاء القبض على المطلوبين، أو معاينة مسرح الجريمة، وكل ذلك يحتاج إلى تعاون دولي ملموس على أرض الواقع([4]).

وأرى بأنه إذا لم يوجد تعاون دولي في إجراءات التحقيق يثير إشكالية أخرى تتعلق بالتعارض مع سيادة الدولة وهذا التعارض يعقد من إمكانية القيام بعمل دولي مشترك للحد من الجرائم المعلوماتية بحيث يدفع بتلك الجهود إلى التركيز في الإطار القانوني لكل دولة على حده.

([1]) نهلا المومني – الجرائم المعلوماتية – دار الثقافة للنشر – الأردن ٢٠٠٨، ص ٥١.

([2]) د. عبدالعال الدربي ومحمد إسماعيل – الجرائم الإلكترونية – المركز القومي للإصدارات القانونية، القاهرة ٢٠١٢، ص ٥٦.

([3]) GRAVE-RAULIN Laurent, règles de confitis de jurisdictions et règles de confits de lois appliqués aus cybers, délit mémoire de master 2 professionnel droit de l'internet publique, université Paris 2-Panthéon Sorbonne, 2008, P 6.

([4]) د. يوسف العفيفي – الجرائم الإلكترونية في التشريع الفلسطيني – رسالة ماجستير، الجامعة الإسلامية بغزة ، فلسطين ٢٠١٣ ، ص ٦٦.

وهذا التباعد أدى إلى أن تتشتت الجهود في مواجهة هذا النوع من الإجرام، فوجود الجاني على سبيل المثال في أوروبا والمتضرر في أمريكا يجعل التصدي لهذا النوع من الإجرام أمراً عسيراً، وذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق، الأمر الذي حدا بالبعض للقول بأن أبرز المجتمعات المعاصرة في ظل التقنية الحديثة، واقتصاداً بلا حدود وثقافة بلا حدود، عن جريمة منظمة بلا حدود حيث تم استغلال الحاسب فيها أسوأ استغلال، فعن طريق الإنترنت يتم تحويل الأموال إلكترونيا وغسلها([1]).

وكما حصل في الحقيقة في قضية معروفة باسم مرض نقص المناعة المكتسب (الأيدز) التي تؤكد الخصائص الخاصة والطبيعة الصعبة للجريمة المعلوماتية فهي من القضايا التي لفتت النظر الى البعد الدولي للجرائم المعلوماتي ، وتتلخص هذه القضية التي حدثت عام ١٩٨٩ بقيام المتهم جوزيف بوب القاطن في أوهايو بالولايات المتحدة الأمريكية بتوزيع عدد كبير من النسخ الخاصة بأحد البرنامج الذي هدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة ، لا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة) ، إذا كان يترتب عن 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 المضاد للفيروس وفي الثالث من فبراير من عام ١٩٩٠ تم القاء القبض على المتهم في مكان سكنه، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي ، حيث إن ارسال هذا البرنامج قد تم من داخل المملكة المتحدة وبفعل وافق القضاء الأمريكي على تسليم المتهم ،وتم توجيه إحدى عشرة تهمة ابتزاز إليه ووقعت معظمها في دول مختلفة إلا ان اجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية ،ومهما كان الإمر فإن لهذه القضية أهميتها من ناحيتين :

الأولى: أنها المرة الأولى التي يتم فيها تسليم متهم في جريمة معلوماتية.

الثانية: أنها المرة الأولى التي يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث (فيروس).

ولهذا تظهر الحاجة الملحة للتعاون الدولي في مجال مكافحة هذه الجرائم وضبط فاعليها، وتجدر الإشارة هنا إلى جهود الإنتربول في هذا المجال، من خلال ضابط الارتباط المنتشرين في كافة الدول عبر العالم، والمكلفين بتوفير قاعدة بيانات ضخمة يمكن أن تشكل نقطة انطلاق للمكافحة والتصدي لهذه الجرائم([2])، وكذلك بشأن القبض المجرمين وتسليمهم إلى الجهات المختصة وتسهيل مهام مأموري الضبط القضائي بشأن إجراءات الضبط والتفتيش وجمع الاستدلالات، ولذلك يجب عقد المؤتمرات الدولية للخروج منها باتفاقيات دولية تعالج مشكلة مكافحة الجرائم المعلوماتية والقضاء عليها([3]).

وتكمن أهم المشاكل المتعلقة بالتعاون الدولي حول الجريمة المعلوماتية، في أنه لا يوجد هناك مفهوم عام، مشترك بين الدول حول صور النشاط المؤدي أو المكون لهذه الجريمة، بالإضافة إلى نقص

([1]) محمود عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر، الأردن، ٢٠٠٥، ص ٣٥.
([2]) أسامة المناعسة وجلال الزعبي – جرائم الحاسب الآلي – دار وائل للنشر، الأردن ٢٠٠١ ، ص ١٠٦.
([3]) د. يوسف العفيفي – الجرائم الإلكترونية في التشريع الفلسطيني – رسالة ماجستير، الجامعة الإسلامية بغزة ، فلسطين ٢٠١٣ ، ص ١٦.

الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتفكيك وتحليل عناصر الجريمة إن وجدت، وجمعها للإدانة، فكل هذا يشكل عائقاً كبيراً أمام التعاون في مجال مكافحة هذا النوع من الجرائم(١).

ومما سبق يتوجب من الدول العمل على التصدي للجرائم المعلوماتية أن تقوم بذلك من خلال عملين هما:

الأول: جهود داخلية تقوم بها جميع الدول بسن القوانين الملائمة لمكافحة الجرائم المعلوماتية.

الثاني: جهود دولية عن طريق عقد المعاهدات الدولية لمكافحة هذه الجريمة حتى لا يستفيد جناة هذا الجرائم من عجز التشريعات الداخلية من توجيه العقاب عليهم وكذلك من أجل تطوير التعاون الدولي في شأن التحري والتحقيق في هذه الجرائم.

ثانيا: جرائم صعبة الإثبات والاكتشاف

تحدث في البند السابق أن من خصائص الجريمة المعلوماتية أنها عابر للحدود، حيث إن الجريمة ترتكب في دولة ما في حين يتحقق النتيجة الجرمية في دولة أخرى، فالجريمة المعلوماتية لا تحدها حدود ولا تعترف بعنصر المكان أو الحدود الجغرافية، وتتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ومن الوجهة التقنية الفنية بين النظام الإلكتروني (أداة الجريمة) وبين المعلومات الإلكترونية (محل الجريمة المستهدفة بالاعتداء).

وتكمن الصعوبة في هذه الحالة بسبب التباعد الجغرافي بين الفعل وتحقيق النتيجة من أكثر المسائل التي تثير إشكالات في مجال الجرائم المعلوماتية وبشكل خاص الإجراءات الجنائية المتبعة والاختصاص القضائي والقانون الواجب التطبيق على هذه الجريمة، وهذا السبب الذي دعا إلى تظافر الجهود الدولية لمكافحة الجريمة المعلوماتية والتي باتت واحدة من أهم سمات العصر وظواهره(٢).

فالجريمة المعلوماتية تتميز بطابع خاص، حيث إن إثباتها يحيط به الكثير من الصعوبات والتي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثراً خارجياً، فلا يوجد جثث لقتلى ولا آثار للدماء وإذا اكتشفت يكون ذلك بمحض الصدفة.

حيث تفتقر جرائم المعلومات للآثار التقليدية للجريمة مثل البصمات والسلاح والآثار المادية، بالإضافة إلى سهولة محو الدليل الجرمي الناشئ عنها والتخلص منه في ثوان معدودة(٣)، فالجرائم المعلوماتية لا تحتاج إلى أي عنف أو سفك للدماء، أو آثار اقتحام لسرقة الأموال وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة النظام المعلوماتي الإلكتروني(١)، ونجد بأن الجاني يستخدم

---

(١) محمد محي الدين عوض – مشكلات السياسة الجنائية المعاصر في جرائم نظم المعلومات – ورقة عمل مقدمة إلى مؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ١٩٩٣، ص ٣٥.

(٢) د. جميل عبد الباقي الصغير –القانون الجنائي والتكنولوجيا الحديثة – دار النهضة العربية،القاهرة ١٩٩٢، ص ١٧.

(٣) محسن الخليفة – جرائم الحاسب الآلي وعقوباتها في الفقه والنظام – رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٣، ص ٤٥.

(١) رصاع فتيحة – الحماية الجنائية للمعلومات على شبكة الإنترنت – رسالة ماجستير، جامعة أبي بكر بلقايد، الجزائر ٢٠١٢، ص ٤٤.

فيها وسائل فنية وتقنية عالية ومعقدة وسلوكه الإجرامي يتمثل بعمل سريع لا يستغرق بضع ثواني وإنها تفتقر للدليل المادي الذي يثبت تورط الجاني بالجريمة.

ومما يزيد في صعوبة إثبات واكتشاف الجريمة المعلوماتية عدم وجود خبرة لدى أفراد الضابطة العدلية (رجال الشرطة) في مثل هذه الجرائم من ناحية التحقيق والبحث على الأدلة والتحفظ عليها، وكذلك من الصعوبات التي تواجه إثبات هذه الجرائم عدم اقتناع القضاة بكثير من الجرائم المستحدثة في هذا المجال وعدم فهمهم لمكنون وماهية الجرائم المعلوماتية بجميع صورها([1]).

ونرى بأن الجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه، ولا يدري حتى بوقوعها، والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أمر ليس بالعسير في الكثير من الأحيان بحكم المعرفة والخبرة في مجال الحاسبات غالباً لدى مرتكبيها.

ويكون للمجني عليه دور أساسي كذلك في صعوبة اكتشاف وتحديد نوع الجريمة المعلوماتية، حيث تحرص أغلب الجهات التي تتعرض أنظمتها المعلوماتية للقرصنة والانتهاك على عدم الكشف حتى بين موظفيها عما تعرضت له، وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنه للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها([2])، وتشير بعض التقديرات إلى أن ما يتراوح بين ٢٠% و ٢٥% من جرائم الحسابات لا يتم الإبلاغ عنها مطلقاً، خشية الإساءة إلى سمعة المؤسسة أو المصنع، ويرى البعض أن للمجني عليه كذلك دوراً مثيراً للريبة في بعض الأحيان، فهو قد يشارك بطريقة غير مباشرة في ارتكاب الفعل، وذلك بسبب وجود ظروف تجعل تعرضه للجريمة المعلوماتية أمراً مرتفعاً بشكل كبير، ويرجع ذلك بشكل أساس إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية([3]).

ويبدو أن إحجام المجني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية أكثر وضوحاً في المؤسسات للمالية مثل البنوك والمؤسسات الادخارية ومؤسسات الاقتراض والسمسرة، حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم، أو اتخاذ الإجراءات القضائية حيالها، إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث إن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه. وهذا ما يؤثر بدوره على السياسة التي يمكن أن توضع لمكافحتها، وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم، وبالتالي حجم الإجرام المعلوماتي الخفي، ومن بين الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم الحاسبات التزاماً على عاتق موظفي الجهة

([1]) د. يوسف العفيفي – الجرائم الإلكترونية في التشريع الفلسطيني – رسالة ماجستير، الجامعة الإسلامية بغزة، فلسطين، ٢٠١٣، ص ١٦.

([2]) Tiedmann (K.): Fraud et autres délits d'affaires commise à l'aid d'ordinateurs électroniques. Rev. dr. pén. crim. 1984. p. 613; Jean Pradel et Christian Feuillard, les infractions commis au moyen de l'ordinateur. Rev. Dr. Pen. Cr. 1985. p. 307.

([3]) نهلا المومني – الجرائم المعلوماتية – دار الثقافة للنشر – الأردن ٢٠٠٨، ص ٢٥.

المجني عليها بالإبلاغ عما يصل عملهم به من جرائم في هذا المجال، مع تقرير خبراء على الإخلال بمبدأ الالتزام، غير أن هذا الاقتراح لقي رفضاً، لأنه ليس من المقبول تحويل المجني إلى مرتكب للجريمة([1]).

الدليل الجنائي لإثبات الجريمة المعلوماتية يختلف تماماً عن الدليل الجنائي في الجريمة التقليدية، وذلك من حيث البيانات والمعلومات المدونة في جهاز الحساب وكيفية إثباتها، سواء من حيث وسيلة الإثبات أو القائم به، وما إذا كانت تتوافر لديه الخبرة الكافية أم لا، سيما وأن أجهزة العدالة الجنائية خصوصاً العربية غير مؤهلة لهذا الدور وهي بحق ثغرة يعتمد عليها المجرم المعلوماتي الذي يتسم بأنه مجرم ذكي في ذاته يعكس أعلى درجات المهارة في فنون التعامل مع الحاسب الآلي، ويكفي للتدليل على خطورة هذا الأمر أن بعضهم يتعامل مع هذا النوع من الجرائم بوصفه يمارس هواية ولا حرفة، فالصعوبات التي تعترض تحصيل الدليل الجنائي في هذه الجرام كثيرة ومتنوعة منها ما يتعلق بالدليل الجنائي ذاته، ومنها ما يتعلق بموضوع الجريمة، والآخر يتعلق بجهات الضبط القضائي أو الجنائي في هذه الجرائم، على أنه يمكن القول استحصال الدليل الجنائي في هذه الجرائم محكوم بضابطين:

الأول: ضرورة وجود قاعدة قانونية تقرر الإجراء القانوني الواجب إتباعه في مثل هذه الجرائم مع مراعاة طبيعتها الخاصة.

الثاني: ضرورة المعرفة الفنية والتأهيل المهني والتقني لرجال الضبط والتحقيق الجنائي([2]).

وتجدر الإشارة إلى أن وسائل المعاينة طرقها التقليدية لا تفلح في غالب الأحيان في إثبات هذه الجريمة نظراً لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث، حيث تخلف آثار 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 ويتلاشي دوره في إظهار الحقائق المؤدية للأدلة والبراهين المطلوبة، ويرجع ذلك لسببين اثنين هما:

الأول: الجريمة المعلوماتية لا تخلف آثاراً مادية.

الثاني: إن كثيراً من الأشخاص يتعاقبون على مسرح الجريمة خلال الفترة من زمان ووقوع الجريمة وحتى اكتشافها أو التحقيق فيها، وهي مدة طويلة نسبياً، الأمر الذي يعطي مجالاً واسعاً للجاني أو لآخرين أن يعيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت، الأمر الذي يرث الشك في دلالة المستقاة من المعاينة في الجريمة المعلوماتية([3]).

وأرى بأنه يمكن إجمال صعوبة إثبات واكتشاف الجريمة المعلوماتية كما يلي:

([1]) حمزة بن عفون – السلوك الإجرامي للجرم المعلوماتي - رسالة ماجستير، جامعة الحاج الخضر ، الجزائر ٢٠١٢، ص ٢٢.

([2]) د. محروس نصار غالب – الجريمة المعلوماتية – بحث منشور في مجلة التقني الصادرة عن هيئة التعليم التقني ، المجلد ٢٤ ، العراق ٢٠١١ ، ص٥.

([3]) د. عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دار الكتب القانونية، القاهرة ٢٠٠٢، ص ٢٨.

الأول: ضرورة وجود قاعدة قانونية تقرر الإجراء القانوني الواجب إتباعه في مثل هذه الجرائم مع مراعاة طبيعتها الخاصة.

الثاني: ضرورة المعرفة الفنية والتأهيل المهني والتقني لرجال الضبط والتحقيق الجنائي(١).

في خمسة أسباب هي:

١. أنها جريمة لا تترك أثر.
٢. إنها جريمة يصعب فنياً الاحتفاظ بآثارها، إن تركت أثراً.
٣. إنها جريمة يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية، وما تخلفه من آثار غير مرئية.
٤. إنها جريمة تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها.
٥. إنها جريمة تعتمد على قمة الذكاء في ارتكابها.

ثالثاً: خطورة الجرائم المعلوماتية

إن الجرائم المعلوماتية تتسم بالخطورة البالغة بسبب مساسها بالإنسان في فكرة وخصوصياته وأموال وآمنة، كما أن الخسائر الناشئة عنها لا تحصى لكثرتها قياساً عن الجرائم التقليدية والخاصة في جرائم الأموال، فتنطوي على سلوكيات غير مألوفة تمس المؤسسات في اقتصادها وكذلك تمس الدولة في أمنها القومي والسياسي والاقتصادي(٢).

وتكمن خطورة هذه الجرائم في أنها تقع على المعطيات الإلكترونية من معلومات وبرامج وبيانات والتي لها قيمة اقتصادية وتسبب خسائر باهظة في الأموال والأقتصاد ، سواء بالنسبة للبرامج المعتدي عليها أم بالنسبة للمعلومات التي يتم الاعتداء عليها التي قد يستخدمها الجناة للابتزاز أو لتحقيق منافسة غير مشروعة بتصنيع منتوج صناعي أو تجاري تحتكر إحدى الشركات أو الأفراد صناعته وإنتاجه، بل مخاطرها تتعدى ذلك إذ يكفي أن يتاح الوقت الكافي للص ذو دراية وخبرة في أنظمة المعلومات الإلكترونية لأن يقضي على مؤسسة اقتصادية عملاقة بمجرد أن يعرف رقم حسابها أو الرقم السري الذي تحتفظ بأسرارها سواء فيما يتعلق بأسلوب إدارتها أو فيما يتعلق بأسرار صناعتها تحته وهو ليس بالأمر المستحيل على شخص صاحب خبرة إذ يستطيع وخلال لحظات أن يدمر كل المعلومات والبيانات والبرامج السرية لتلك المؤسسة أو أن يفشي سر صناعتها بوضعه على شبكة المعلومات بحيث يكون في متناول كل من هب ودب(٣).

ومن أجل التذليل على خطورة الجرائم المعلوماتية يمكن القول بأنه وأمام الانتشار الواسع والكبير في استخدام النظام المعلوماتي الإلكتروني الذي لم يظل مقتصراً استخدامه على الشركات أو المؤسسات المالية والاقتصادية والتجارية ... إلخ، بل أصبح متناول الأفراد حتى في مدارسهم ومنازلهم مما يتيح للجميع

---

(١) د. محروس نصار غالب – الجريمة المعلوماتية – بحث منشور في مجلة التقني الصادرة عن هيئة التعليم التقني ، المجلد ٢٤ ، العراق ٢٠١١ ، ص٥.
(٢) عبير النجار، جرائم الحاسب الآلي في الفقه الإسلامي، رسالة ماجستير، الجامعة الإسلامية بغزة، فلسطين ٢٠٠٩، ص ١٧.
(٣) د. محمد الهيتي – مرجع سابق – ص ١٥٦.

الاتصال به بصورة أو بأخرى فإنه لا شك في مضار هذا الاتصال الذي كما يكون مشروعاً يمكن أن غير مشروع، وهذا الاتصال وعلى وجه الخصوص الاتصال غير المشروع لا شك في نتائجه الضارة والدليل على ذلك يتضح من خلال الوقائع التي سنذكرها على سبيل المثال لا الحصر ففي عام ١٩٧٧ تمكن أحد تلاميذ المدارس الثانوية من اختراق نظام المعلومات لجامعة (البرتا) عن طريق أحد المحطات الطرفية المثبتة على سور الجامعة مما أسفر عن إصابة نظم معلومات الجامعة بالعطب الكلي، وحيث إن الطالب المذكور غير مصرح باستعمال الجهاز، لذلك أدين عن جريمة الاستعمال غير المشروع لمنشآت الاتصال، وفي عام ١٩٨٠ قامت مجموعة من التلاميذ بإحدى مدارس نيويورك ومن خلال إحدى وعشرون محاولة باختراق نظامين لمؤسستين كبيرتين في كندا عن طريق الهاتف الملحق بالكمبيوتر التعليمي للمدرسة، وتبين أن بنكي المعلومات لهاتين لمؤسستين أصابهما تدمير جزئي نتيجة عبث هؤلاء التلاميذ(١). وقد حدث أيضاً أن أحد الهواة في أوروبا تمكن من حل شفرة أحد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية) وأصبح السبيل أمامه مفتوحاً للعبث في بيانات هذه المركز(٢).

فعلى سبيل المثال: حصدت فرنسا عام ١٩٨٦م وفقاً لإحصاء الجمعية العمومية لشركات التأمين ضد الحرائق والمختلفة ٧,٣ مليار فرنك فرنسي، والمملكة المتحدة اختلفت التقديرات بشأن خسائرها؛ حيث تراوحت من ٥٠٠ مليون جنية إلى ٢ بليون جنيه في السنة، ووجدت دراسة تبنتها الحكومة في ١٩٨٦م أن ٤٠ % من شركات المملكة المتحدة قد عانت على الأقل من نصب رئيسي في الحاسوب خلال السنوات الأخيرة(٣).

ففي الولايات المتحدة الأمريكية يشير التقرير الذي قدمته نقابة المحامين الأمريكيين في عام ١٩٨٤م على الحجم الهائل في الخسائر لحقت بحوالي ثلاثمائة من أكبر الشركات هناك، إذ يشير التقرير إلى أن معدل الخسارات السنوية لتلك الشركات يتراوح ما بين ٢ -١٥ مليون دولار سنوياً- وتعتبر البنوك هي الهدف لرئيس للنسل الجديد من مجرمي التقنية العالية، ذلك لأنها تعتمد اعتماداً كلياً ورئيسياً على أنظمة نقل التمويل إلكترونيا، فبنوك نيويورك وحدها تتناقل ٢٠٠ بليون دولار يومياً فما الذي سيكون عليه الحال إذا ما استطاعت الأيدي المنحرفة على الحصول على رموز التحويل الإلكترونية المستخدمة وكم من الأموال يمكن نقلها وبثوان معدودة إلى خارج البلد(٤).

إضافة لهذا النوع فإن هناك أنواعاً؛ كالقروض الوهمية، وفتح اعتمادات، وأشكال أخرى من التلاعب، كما تطال هذه الجرام بخطورتها الحياة الخاصة للأفراد، إضافة لتهديدها للأمن القومي للدول، وفقد الثقة بالتقنية، وتهدد الملكية الفكرية وقتل روح الإبداع الإنساني(١).

لذلك فإن جرائم المعلوماتية تشكل خطورتها من حيث المصالح التي ينالها الاعتداء فالنظام الإلكتروني لم يعد جهازاً لإجراء العمليات الرياضية المعقدة بل أصبح مستودعاً لأسرار الشركات والأشخاص على حد سواء بل حتى الدول لذلك فإن اختراق أنظمة المعلومات، فإفشاء الأسرار الخاصة

---

(١) د. عمر الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسوب - بدون ناشر، القاهرة ١٩٩٥، ص ٦.
(٢) د. جميل عبد الباقي الصغير –القانون الجنائي والتكنولوجيا الحديثة – دار النهضة العربية،القاهرة ١٩٩٢، ص١٧.
(٣) عبير النجار – جرائم الحاسب الآلي في الفقه الإسلامي – رسالة ماجستير، الجامعة الإسلامية بغزة، فلسطين ٢٠٠٩، ص ١٧.
(٤) محمود عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر، الأردن، ٢٠٠٥، ص ٣٣.
(١) د. جميل عبد الباقي الصغير –القانون الجنائي والتكنولوجيا الحديثة – دار النهضة العربية،القاهرة ١٩٩٢، ص ١٧.

بالأفراد صيداً ثميناً لقراصنة المعلومات، فإفشاء الأسرار الخاصة بالأفراد أو الشركات أو الدول وانتهاك حرمة الحياة الخاصة وإفشاء أسرار الدولة كلها مصالح دخل إليها النظام الإلكتروني الذي لم يعد في وقتنا الحاضر مستودعاً للسر فقط بل أنه أضحى يُعتمد عليه حتى في التبضع بل أنه أصبح ينافس الإنسان حتى في عمله([1]).

ونجد أن حداثة جرائم المعلومات تشكل الوجه الآخر لخطورتها إذ أنها لا زالت جرائم خافية المعالم على الكثيرين كما أنها خافية في أبعادها وآثارها عنهم أنها خافية حتى على الجهات التي تتولى تحديد معالمها وآثارها وأقصد بذلك السلطتين التشريعية والقضائية إذ أنها حديثة على الجهات المتخصصة في فض المنازعات (القضاء) كما هي خافية أو غير واضحة المعالم على الجهة المسؤولة عن سن القوانين، ولا سيما في بلداننا النامية، فيكف سيكون الأمر بالنسبة للجهة الأخيرة التي تريد أن ترسم معالمها وتحدد أركانها وهي لا زالت في طور التكوين والنشوء.

وما زاد من خطورة جرائم المعلومات هو أن هذه الجرائم أخذت طابعاً دولياً حيث لم تعد مقتصرة على النطاق الوطني، وذلك بسبب سهولة الاتصال بين دول العالم اليوم حيث جعلت أنظمة المعلومات اليوم العالم قرية صغيرة لا يعترف فيها بحدود لا طبيعية ولا سياسية، غير أن انسياب هذه المعلومات متجاوزة بذلك الحدود الدولية للدول تثير الكثير من المشاكل القانونية، فلا تقتصر كما يذهب البعض على مدى مشروعية هذه المعلومات وانسيابها، ومنها ما يتعلق بشروط المعلومات التي يجوز بثها عن هذا الطريق، إن كان لا ينكر هذا الجانب، بل أن لها مخاطر تتعلق بالمبادئ الراسخة في القانون الجنائي، وعلى وجه الخصوص فيما يتعلق بمبدأ الإقليمية، ويزداد الأمر خطورة إذا علمنا كثيراً من بلدان العالم لا تعرف تجريم التصرفات التي تنال من برامج الحاسب الآلي كجرائم مستقلة في تشريعاتها([2]).

رابعاً: الجرائم المعلوماتية جرائم ناعمة

إن الجرائم المعلوماتية تتصف بأنها ناعمة ولا تتطلب عنفاً لتنفيذها أو مجهوداً كبيراً، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعاً من المجهود العضلي الذي يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو السطو المسلح أو الاغتصاب.

فالجريمة المعلوماتية لا تحتاج إلى مجهود عضلي بل تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على المعرفة بتقنيات الأنظمة المعلوماتية، حيث لا يوجد في واقع الأمر شعور بعدم الأمان تجاه المجرمين في مجال المعالجة الآلية للمعلومات باعتبار أن مرتكبيها ليسوا من محترفي الإجرام بصيغته المتعارف عليها([1]).

فالجريمة المعلوماتية تتميز بأنها جرائم هادئة لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع النظام المعلوماتي بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة، وتحتاج فقط إلى مجرم لديه الخبرة والتقنية الفنية على التعامل مع النظام لارتكاب جريمته([2])، فيقوم الجاني بتنفيذ

([1]) محمد الهيتي – مرجع سابق – ص ١٥٧.
([2]) د. عمر الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسوب – بدون ناشر، القاهرة ١٩٩٥ ، ص ص ١٦.
([1]) محمد علي سالم وحسون هجيج – الجريمة المعلوماتية – بحث منشور في مجلة بابل، العدد ٢ سنة ٢٠٠٧، ص ٩٢.
([2]) صغير يوسف – مرجع سابق – ص ١٦.

جريمته عن بعد دون التواجد في مسرح الجريمة ولا يتطلب لتنفيذها سوى الضغط على مفتاح معين لإتمام الجريمة بدون استخدام أي عنف بدني([1]).

خامساً: الجرائم المعلوماتية جرائم قائمة على التقنية الإلكترونية

إن الجرائم التقليدية تتطلب نوعاً من الجهد العضلي والقوة والعنف في تنفيذها وبعضها تحتاج إلى دهاء وأسلوب معين مثل النصب، حيث لا تعتمد على التقنية الإلكترونية، أما الجريمة المعلوماتية فهي جرائم ناعمة لا تحتاج إلى الجهد العضلي أو العنف وإنما الإلكتروني في ارتكاب وتنفيذ الجريمة، حيث أنها تحتاج إلى معرفة تنقية من الفاعل وتوفر الجهاز الإلكتروني – مهما كان مسماة وإلى شبكة الإنترنت.

ويرتبط هذا النوع من الجرائم ارتباطاً وثيقاً بالتطور السريع الذي تشهده اليوم في تكنولوجيا الاتصالات، مما يؤثر على مرتكب الجريمة المعلوماتية وأسلوب ارتكابه من خلال تبادل الأفكار، والخبرات الهدامة، مع العديد من المجرمين من حول العالم عبر الشبكة الإلكترونية، وتطور التقنيات المستخدمة([2]).

وتتميز الجريمة المعلوماتية عن غيرها أن الجهاز الإلكتروني هو أداة الجريمة ووسيلة تنفيذها، أو موضوع الجريمة كإتلاف أو سرقة البيانات والمعلومات وهنا تثور المشكلة، أما لو كان موضوع الاعتداء هو الجهاز نفسه أو شاشته أو الكيانات المادية للجهاز فهنا تطفي نصوص التجريم التقليدية، ويطبق قانون العقوبات على موضوع الجريمة، فبدون الجهاز الإلكتروني تنتفي الجريمة المعلوماتية وتتطلب هذه دراية كافية وخبرة فائقة بالنظام الإلكتروني والإنترنت في بعض الجرائم، أو معرفة بسلوكيات الفعل المرتكب في الجرائم البسيطة منها، كما أنها لا تمتاز بالعنف، وأغلب الجرائم الإلكترونية ترتكب عبر الإنترنت([3]).

والجريمة المعلوماتية، جرائم فنية تقنية في الغالب الأعم، والأشخاص الذين يقومون بارتكابها عادة يكونون من ذوي الاختصاص ف مجال تقنية المعلومات، أو على الأقل شخص لديه حد أدنى من المعرفة والقدرة على استعمال الجهاز الإلكتروني والتعامل مع شبكة الإنترنت، ومثال على ذلك فإن الجرائم المعلوماتية ذات الطابع الاقتصادي مثل التحويل الإلكتروني غير المشرع للأموال يتطلب مهارة وقدرة فنية وتقنية عالية جداً من قبل مرتكبيها([1]).

ولذلك فإن ما يميز الجريمة المعلوماتية عن غيرها من الجرائم، أنها تتطلب وجود علم كافي بالجوانب الفنية والتقنية لاستخدام الحاسوب والإنترنت، وتعتبر العلاقة بين مدى الدراية بالجوانب الفنية

([1]) د. يوسف العفيفي – الجرائم الإلكترونية في التشريع الفلسطيني – رسالة ماجستير، الجامعة الإسلامية بغزة ، فلسطين ٢٠١٣ ، ص ١٧.

([2]) عبير النجار – جرائم الحاسب الآلي في الفقه الإسلامي – رسالة ماجستير، الجامعة الإسلامية بغزة، فلسطين ٢٠٠٩، ص١٩.

([3]) د. يوسف العفيفي – الجرائم الإلكترونية في التشريع الفلسطيني – رسالة ماجستير، الجامعة الإسلامية بغزة ، فلسطين ٢٠١٣ ، ص ١٤.

([1]) حمزة بن عفون – السلوك الإجرامي للجرم المعلوماتي - رسالة ماجستير، جامعة الحاج الخضر ، الجزائر ٢٠١٢، ص ٢٦.

والتقنية الحاسوب وبين الجريمة المعلوماتية علاقة طردية، فكلما زادت الخبرة لدى الأفراد بمعرة تقنية الحاسوب، زاد احتمال استخدام خبرتهم بشكل غير مشروع([1]).

وكذلك ما يميز هذه الجريمة أن موضوع الاعتداء يقع على المعلومات والبيانات والمعطيات المخزنة على النظام الإلكتروني، فهذه المعلومات والتي هي موضوع الجريمة يمكن تخزينها ونقلها من جهاز لآخر عبر الوسائط الصلبة أو المرنة أو عبر البريد الإلكتروني، ولذلك فهي تعتبر مكونات معنوية تقبل الحيازة والنقل ويقع عليها فعل السرقة والإتلاف ولذلك يجب أن يكون هذا المال محل حماية من قبل القانون الجنائي([2]).

وأجد من الواقع العملي أن الجرائم المعلوماتية قد ترتكب من خلال الهواتف المحمولة، خاصة بعد ظهور أجهزة الهاتف الذكية والتي هي في الحقيقة عبارة عن أجهزة حاسوب صغيرة، والتي من خلالها يتم الاتصال بشبكة الإنترنت، ويسهل تخزين ونقل المعلومات من خلالها، وليس كما ذكر بعض الباحثين أن الحاسوب هو الأداة الوحيدة في ارتكاب الجريمة المعلوماتية ففي أيامنا هذه أرى أنه يمكن تصنيف هواتف المحمول الذكية ضمن أجهزة الحاسوب، ذلك لأنه لا يختلف عن الحاسوب سوى الحجم بل أن الهواتف الذكية يمكن من خلالها الاتصال المباشر بخلاف الحاسوب، أما بالنسبة للوظائف الأخرى فتتم ممارسة جميع وظائف الحاسوب من خلال الهاتف الذكي.

وأرى أنه يشترط لتوافر هذه الخاصية للجريمة المعلوماتية توافر شروط معينة وهي:

١. يجب توافر جهاز إلكتروني مهما كانت تسميته سواء أكان حاسوب أم هاتف ذكي كأداة لتنفيذ الجريمة.
٢. يجب ربط الجهاز لإلكتروني بشبكة الإنترنت كوسيلة للاتصال ما بين الأنظمة الأخرى لتنفيذ الجريمة.
٣. يجب أن يكون الجاني ذو خبرة فائقة في مجال الأنظمة المعلوماتية الإلكترونية وشبكة الإنترنت وذو دراية كبيرة في استخدامها لتنفيذ جريمته.

([1]) محمود عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر، الأردن، ٢٠٠٥، ص ٣٣. ص ٣٦.
([1]) خالد عياد الحلبي – إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت – دار الثقافة للنشر، الأردن ٢٠١١، ص ٥٥.

الخاتمة

بعد أن انتهينا من دراسة الجرائم المعلوماتية وبينا الأحكام العامة لها من حيث مفهوم الجرائم المعلوماتية وخصائصها و طبيتها نستنتج ما يلي :-

أولا: النتائج:

- لم يعد نطاق الإجرام المعلوماتي قاصرا على المجال الاقتصادي، بل لم لم تسلم منه حرمة الحياة الخاصة للأفراد، واعتبارا من عام ١٩٧٨ بدأت جرائم الفيروسات تلوح في الآفاق، باعتبارها إحدى صور الجرائم المعلوماتية، وهذه الجرائم من شأنه أن تقوض النظام المعلوماتي وتجعله والعدم سواء.
- يتم تعريف الجرائم المعلوماتية بعدة تعريفات تتمايز وتتباين تبعاً لموضوع العلم المنتمية إليه وتبعاً لمعيار التعريف ذاته، فاختلفت تلك التعريفات وفقاً لمعيار موضوع الجريمة، ومعيار آليات ارتكاب الجريمة

. أن التعريف المقترح للجريمة المعلوماتية هو "هي الفعل غير المشروع التي يكون فيها النظام المعلوماتي الإلكتروني أداة لتنفيذ العمل الجرمي المراد تحقيقه أو الفعل الموجه ضد النظام المعلوماتي أو المعلومات المخزنة في الأنظمة أو على الشبكات الإلكترونية بأفعال مجرمة سواء كانت الجريمة إيجابية أو سلبية من شخص على دراية كافية مع التعامل مع التقنية الإلكترونية للمعلومات وبشكل مقصود ومتعمد".

- من خصائص الجريمة المعلوماتية أنها جريمة عابرة للحدود وصعبة الإثبات والاكتشاف وعلى قدر كبير من الخطورة نظرا لأنها من الجرائم الناعمة التي لا تتطلب عنفا في ارتكابها.

- أن المجرم المعلوماتي يتسم بالذكاء والمهارة، يتمتع بالسلطة، ويخاف من كشف جريمته، يتسم بالتخطيط والتنظيم . ويمكن تصنيف مرتكبي الجرائم المعلوماتية إلى مجموعة من الفئات والطوائف، ولا يعني بطبيعة الحال أن كل مجرم يندرج ضمن طائفة محددة دون غيرها، بل يمكن أن يكون المجرم الواحد مزيجاً من أكثر من طائفة أو فئة.

- محل الجرائم المعلوماتية قد يكون الأشخاص أو الأموال أو المساس بأمن الدولة.

التوصيات:

- نوصي المشرع بسرعة إصدار قانون الجريمة الإلكترونية خلال الدورة البرلمانية الحالية وعدم الإبطاء في إصداره نظرا لأهميته القصوى لمعالجة ومكافحة الجرائم المعلوماتية المختلفة.

- وضع تشريع عربي موحد ليكون نموذجا تسترشد به كل دولة عند وضع التشريعات الخاصة في كل دولة، على أن يشمل الجانب الموضوعي سواء من حيث بيان أركان الجرائم المعلوماتية أو الجانب الإجرائي وما يتضمنه من إجراءات منذ وقوع الجريمة واكتشافها أو الإبلاغ عنها وحتى المحاكمة.

- نأمل أن يكون هناك تعاون دولي يتفق مع طبيعة الجرائم المعلوماتية عابرة الحدود، والتي تتميز بطابع خاص يقتضي التصدي له دوليا، بأن يكون نظام الإثبات بالدليل الالكتروني واحداً بين الدولة التي وقعت فيها الجريمة من ناحية والدولة التي يقيم فيها المتهم.

- عمل دورات تأهيلية في هذا المجال سواء لرجال الشرطة أو القضاة أو أعضاء النيابة العامة لتبصيرهم بما يستجد في هذا المجال مع الاستعانة بخبرات الدول المتقدمة في هذا المجال، من أجل توفير ضمانات أكثر وحماية فعالة ضد هذه الجرائم.

- إبرام الاتفاقيات الدولية من أجل تيسير تنفيذ إجراءات الإنابات القضائية ولإزالة العقبات التي تؤدى إلى تأخيرها، وذلك عن طريق تداول هذه الإنابات من السلطة القضائية مباشرة أو عن طريق التصوير عن بعد، في حالة الاستعجال فمثل هذه الإجراءات من شأنها تحسين التعاون القضائي.

المراجع :

المراجع العربي:-

١- د. عمر الفاروق الحسيني ، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية ، دراسة تحليلية نقدية لنصوص التشريع المصري مقارنة بالتشريع الفرنسي ، الطبعة الثانية ١٩٩٥م .
٢- د. محمد الهيتي – التكنولوجيا الحديثة والقانون الجنائي – دار الثقافة لنشر، الأردن ٢٠٠٨.
٣- د. جميل عبد الباقي الصغير –القانون الجنائي والتكنولوجيا الحديثة – دار النهضة العربية، القاهرة ١٩٩٢.
٤- د. محمد الأمين البشري – التحقيق في الجرائم المستحدثة – منشورات جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٤.
٥- د. عبدالعال الدربي ومحمد إسماعيل – الجرائم الإلكترونية – المركز القومي للإصدارات القانونية، القاهرة ٢٠١٢.
٦- محمد علي سالم وحسون هجيج – الجريمة المعلوماتية – بحث منشور في مجلة بابل، العدد ٢ سنة ٢٠٠٧.
٥- د. محمد علي عياد – شرح قانون العقوبات، القسم العام – دار الثقافة للنشر، الأردن ١٩٩٧.
٦- د. محمود محمود مصطفى - شرح قانون العقوبات – دار النهضة العربية – القاهرة ١٩٨٠ .
٧- سيد أنور سالم وآمال عثمان – علم الإجرام وعلم العقاب – دار النهضة العربية – القاهرة ١٩٨٠، ص ٦٦.
٨- د. عبد الرحمن توفيق أحمد – شرح قانون العقوبات، القسم العام – دار الثقافة للنشر، الأردن ٢٠١١.
١٠- محمود عبابنة – جرائم الحاسوب وأبعادها الدولية – دار الثقافة للنشر، الأردن، ٢٠٠٥.
١١- خالد عياد الحلبي – إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت – دار الثقافة للنشر، الأردن ٢٠١١.
١٢- د. يونس عرب – دليل أمن المعلومات والخصوصية - ج١، جرائم الكمبيوتر والإنترنت، اتحاد المصارف العربية، ط١، الأردن ٢٠٠٢.
١٣- د. علي القهوجي – الحماية الجنائية لبرامج الحاسوب- الدار الجامعية للنشر، الإسكندرية ١٩٩٧.
١٤- د. هدى قشقوش – جرائم الحاسب الإلكتروني – دار النهضة العربية، القاهرة ١٩٩٢.
١٥- أسامة المناعسة وجلال الزعبي – جرائم الحاسب الآلي – دار وائل للنشر، الأردن ٢٠٠١.
١٦- المهندس حسن داود – جرائم نظم المعلومات – أكاديمية نايف العربية للعلوم الأمنية، الرياض ٢٠٠٠.
١٧- د.علي القهوجي – الحماية الجنائية البيانات المعالجة إلكترونية – ورقة عمل قدمت إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، الإمارات مايو ٢٠٠٠.

١٨- د. هشام محمد رستم – قانون العقوبات ومخاطر تقنية المعلومات – مكتبة الآلات الحديثة، أسيوط ١٩٩٢.
١٩- د.عادل سقف الحيط- جرائم الذم والقدح والتحقير المرتكبة عب الوسائط الإلكترونية – دار الثقافة للنشر، الأردن ٢٠١٥.
٢٠- د. يوسف العفيفي – الجرائم الإلكترونية في التشريع الفلسطيني – رسالة ماجستير، الجامعة الإسلامية بغزة – فلسطين ٢٠١٣.
٢١- حمزة بن عفون – السلوك الإجرامي للجرم المعلوماتي - رسالة ماجستير، جامعة الحاج الخضر ، الجزائر ٢٠١٢.
٢٢- عبدالله عبد الكريم عبدالله – جرائم المعلوماتية والإنترنت – منشورات الحلبي الحقوقية،بيروت ٢٠٠٧.
٢٣- د. محمد الشوا - ثورة المعلومات وانعكاسها على قانون العقوبات- دار النهضة العربية - القاهرة ١٩٩٤.
٢٤- رصاع فتيحة – الحماية الجنائية للمعلومات على شبكة الإنترنت – رسالة ماجستير، جامعة أبي بكر بلقايد، الجزائر ٢٠١٢.
٢٥- د. عبد الله محمود – إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات – بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية – دبي ٢٠٠٣.
٢٦- محمد الكعبي – الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت – دار النهضة العربية، القاهرة.
٢٧- د. هدى قشقوش – الإتلاف لعمدي لبرامج وبيانات الحاسب الإلكتروني – بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات ٢٠٠٠.
٢٨- نهلا المومني – الجرائم المعلوماتية – دار الثقافة للنشر – الأردن ٢٠٠٨.
٢٩- محمد محي الدين عوض – مشكلات السياسة الجنائية المعاصر في جرائم نظم المعلومات – ورقة عمل مقدمة إلى مؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ١٩٩٣.
٣٠- محسن الخليفة – جرائم الحاسب الآلي وعقوباتها في الفقه والنظام – رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض ٢٠٠٣.
٣١- د. محروس نصار غالب – الجريمة المعلوماتية – بحث منشور في مجلة التقني الصادرة عن هيئة التعليم التقني ، المجلد ٢٤ ، العراق ٢٠١١.
٣١- د. عبد الفتاح بيومي حجازي – الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت – دار الكتب القانونية، القاهرة ٢٠٠٢.
٣٢- عبير النجار، جرائم الحاسب الآلي في الفقه الإسلامي، رسالة ماجستير، الجامعة الإسلامية بغزة، فلسطين ٢٠٠٩.
٣٣- د. عمر الحسيني – المشكلات الهامة في الجرائم المتصلة بالحاسوب - القاهرة ١٩٩٥.

المراجع الانجليزية :-

1- Michel Alexander, computer crime –uglg secret for business, computer world, vol,Xx iv, No 11, 1990.

المراجع الفرنسية :-

1- De Shutter (B) : A propose de la fraude informatique, Revue de droit pénal et criminelle, Avril 1985 .

2- Holtgen (D.); internet pour tous, les éditions du téléphone, 2ème éd. 1996.

3- P.Y. Gautier Suite de la promenade à travers un site immatériel : des condamnations de justice en nature sur Internet Dalloz 1997 chronique.

4- G. BRAIBANY, La protection des droits individuels au regard du développement de l'informatique, RIDC, 1971.
5- Rapport du conseil d 'Etat, Internet et les reseaux - numeriques, la documentation fram sais , Paris 1998.
6- Sieber (Ulrich); Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique, Rev. Int. Dr. Pén. 1993.
7- NOVARD (Pierre) ,La procedure penale en matiere in formatique, Bulletins 'actualite, Decembre 1995.
8- Cybercriminalité: enjeux, sources de données et faisabilité de recueillir des données auprès de la police, Centre canadien de la statistique juridique.
9- Tiedmann (K.): Fraude et autres délits d'affaires commise l'aide d'ordinateurs électroniques. Revu. dr. pén. crim. 1984.
10- Masse (M.): L'utilasation abusive de D.A. B. Rev. Experts des systet d'information, novembre 1981.
11- Vivant et Le Stanc, Lamy droit de l'informatique, 1989, no. 2323.
12- Bart De Schutter; La criminalité liée à l'informatique, Rev. dr. Pen.Cr. No 1. 1985.
13- Tortelo (N.) et Liontier (R.): internet pour les jurists, Paris.Dalloz. 1996.
14- Mascala Coeinne "Criminalité et contrat électronique ll. IN: Le contrat électronique, Travaux de l'association Capitant Henri, Journées National, Paris, 2000.

15-GRAVE-RAULIN Laurent, règles de confitis de jurisdictions et règles de confits de lois appliqués aus cybers, délit mémoire de master 2 professionnel droit de l'internet publique, université Paris 2-Panthéon Sorbonne, 2008 .

16-Tiedmann (K.): Fraud et autres délits d'affaires commise à l'aid d'ordinateurs électroniques. Rev. dr. pén. crim. 1984. p. 613; Jean Pradel et Christian Feuillard, les infractions commis au moyen de l'ordinateur. Rev. Dr. Pen. Cr. 1985. p. 307.