الأحكام العامة للجريمة المعلوماتية

د. محمد أحمد الشيشي

المستشار بهيئة قضايا الدولة المصرية

مدرس القانون الجنائي المنتدب بالجامعات المصرية

(ISSN: 2537 - 0758)

الأحكام العامة للجريمة المعلوماتية

د. محمد أحمد الشيشي

الملخص:

الجريمة المعلوماتية تتعلق بكل سلوك غير مشروع يقع على البيانات والمعلومات الموجودة على جهاز الحاسب الآلى أو أى نظام من أنظمة المعلومات. مادام أن هذا السلوك يشكل إعتداء على حقوق الغير أو أضرار بهم سواء وقع هذا الأضرار داخل الدولة أو خارجها فالبيانات سواء كانت فى مرحلة الإدخال إلى جهاز الحاسب، أو أثناء المعالجة الآلية لها أو فى مرحلة الإخراج فإنها تكون محلاً للجريمة المعلوماتية. ففى مرحلة الادخال من الممكن أن يتم إدخال بيانات غير صحيحة وفى مرحلة المعالجة قد يتم المحو أو التعديل أو التصحيح أما فى مرحلة الاخراج فقد يتم إتلاف الدعامة التى تحتوى هذه المعلومات؛ بالتالي فالمجرم المعلوماتى هو كل شخص يرتكب سلوك غير مشروع يتعلق هذا السلوك بالمعالجة الآلية للبيانات والمعلومات سواء كانت هذه البيانات، والمعلومات مخزنة على الحاسب الآلى؛ أو فى وسائط أخرى يتم تخزين البيانات عليها، وقد يتعلق هذا السلوك بمرحلة الادخال أو الاخراج؛ كما أنه يجب خضوع مرتكب مثل هذه الجريمة للعقاب بغض النظر عن البواعث أو الدوافع وراء ارتكابه لهذه الجريمة وبغض النظر عن عمره فلا عبرة بما إذا كان كبير أو صغير محترف أو متطفل فما دامت وقعت الجريمة فيجب وقوع العقاب مع مراعاة مبدأ التفريد العقابى.

الجريمة المعلوماتية – المجرم المعلوماتي.

Summary

Information crime relates to all illegal behavior that occurs on data and information on a computer or any information system. As long as this behavior constitutes an infringement of the rights of others or harm to them, whether this damage occurs inside or outside the country, the data, whether it is in the stage of entering the computer, or during the automated processing of it, or in the stage of output, it is the subject of information crime. In the input stage, incorrect data may be entered, and in the processing stage, erasure, modification, or correction may take place. As for the output stage, the support that contains this information may be destroyed; Therefore, the information criminal is every person who commits illegal behavior.

This behavior is related to the automated processing of data and information, whether this data or information is stored on the computer. or in other media on which data is stored, and this behavior may relate to the input or output phase; Also, the perpetrator of such a crime must be subject to punishment regardless of the motives or motives behind his commission of this crime and regardless of his age. It does not matter whether he is old or young, a professional or an intruder. As long as the crime occurred, the punishment must take place, taking into account the principle of punitive exclusivity.

Information crime - Information criminal

المقدمة

نظراً للتطور التكنولوجي الذى شهده العالم فى العقود الأخيرة، ولما كانت الجريمة قديمة قدم الانسان، وتطورت على مر العصور، فان ما شهده العالم من ثورة تقنية كان منطقياً معه أن تتطور الجرائم، بما يتلاءم مع هذا التطور التقني، وبالتالي فالجرائم المعلوماتية نتيجة منطقية لهذا التطور الحادث، الأمر الذى يتعين معه معرفة هذا النوع المستحدث من الجرائم حتى تتمكن الأنظمة القانونية مواجهة هذا النوع من الجرائم.

أسباب اختيار الموضوع

يكمن السبب فى اختيار الموضوع هو محاولة بيان مفهوم الجريمة المعلوماتية تمييزاً لها عن غيرها من الجرائم نظرا لحداثتها، ولتمكين الباحثين من الوقوف على العناصر الأساسية التى تميز هذا النوع من الجرائم.

أهمية البحث

تكمن اهمية البحث فى حل الإشكالات القانونية المترتبة على هذا النوع من الجرائم، وما تتطلبه من وجود تشريعات ملائمة بالجانب التقني لتلك الجرائم من خلال دراسة مفهوم تلك الجرائم.

مشكلة البحث

تتجلي مشكلة البحث فى التساؤل عن ماهية الجريمة المعلوماتية، وخصائصها التى تميزها عن غيرها من الجرائم، وماهية المجرم المعلوماتي، وسماته التى تميزه عن غيره.

منهجية البحث

انتهج الباحث للوصول للغاية من البحث الماثل المنهج التحليلي، للوقوف على ماهية الجريمة المعلوماتية، ومرتكبها، والخصائص المميزة لهما.

(ISSN: 2537 - 0758)

خطة البحث

فى ضوء ما تقدم فاننا نتعرض فى هذا البحث لماهية الجريمة المعلوماتية، وخصائصها، وماهية المجرم المعلوماتى، وخصائصه، وذلك فى مبحثين:

المبحث الأول: الجريمة المعلوماتية.

المبحث الثانى: المجرم المعلوماتى.

المبحث الأول
الجريمة المعلوماتية

نتعرض فى هذا المبحث لكلاً من ماهية الجريمة المعلوماتية، وخصائصها، وذلك فى مطلبين:

المطلب الأول: ماهية الجريمة المعلوماتية.

المطلب الثانى: خصائص الجريمة المعلوماتية.

المطلب الأول
ماهية الجريمة المعلوماتية

لإيضاح ماهية الجريمة المعلوماتية يتطلب منا الأمر إيضاح معنى كلاً من الجريمة، والمعلوماتية كلاً منهما على حدة.

الفرع الأول
الجريمة والمعلوماتية

الجريمة فى اللغة: مأخوذة من الجرم، وهو التعدى، والذنب؛ يقال جرم جرماً أى أذنب، ويقال جَرَم نفسه وقومه، وجَرَم عليهم وإليهم. أى جنى جناية، وأجرم أى ارتكب جُرماً، واجترم الذنب أى ارتكبه، والجمع جرائم[١].

أما الجريمة فى الاصطلاح فهى: أى تصرف يصدر من الشخص سواء كان بصورة إيجابية؛ أو سلبية يعاقب عليه القانون.

تعريف الجريمة فى القانون المصرى:

لم يضع المشرع المصرى شأنه شأن الكثير من التشريعات تعريفاً موحداً للجريمة، ولذا فقد حاول الشراح إيجاد تعريفاً للجريمة، وطبيعى أن تختلف هذه التعريفات تبعاً لاختلاف وجهات النظر، ولكن هذه التعريفات تدور حول معنى واحد وهو أن الجريمة هى كل سلوك غير مشروع سواء كان هذا السلوك تم بطريق إيجابى؛ أو سلبى يعاقب

[١] المعجم الوجيز، طبعة وزارة التربية والتعليم، ١٩٩٨، صت١٠١ وما بعدها.

عليه القانون بإحدى العقوبات المقررة فى قانون العقوبات سواء كانت عقوبة؛ أو تدبير إحترازى[٢].

أما المعلوماتية: فهى من المصطلحات المستحدثة، وقد أستخدمها لأول مرة مدير المعهد الإتحادى للمعلومات العلمية والتقنية بالإتحاد السوفيتى سابقاً صفة لعلم المعلومات العلمية، وهو يعنى إندماج المعلومات بأنواعها المختلفة مع النظم الألكترونية، والتعامل مع المعلومات بمعالجتها الكترونيا[٣].

ولإيضاح معنى المعلوماتية يقتضى منا الأمر التعرض أولاً لعناصرها، وهى المعلومات، والبيانات.

فالمعلومات جمع معلومة، وهى مشتقة من كلمة علم، والعلم هو إدراك الشئ بحقيقته. قال تعالى: "علم الإنسان ما لم يعلم"[٤].

ويمكن تعريف المعلومات، والبيانات من خلال العلاقة بينهما:

فالبيانات: هى عبارة عن مجموعة من الحقائق التى تعبر عن مواقف، وأفعال حدثت فى الماضى؛ أو فى الحاضر أو سوف تحدث فى المستقبل، وسواء كان التعبير بالكلمات؛ أو الأشكال؛ أو الرموز.

أما المعلومات فهى بيانات خضعت للتشغيل، والتحليل، والتفسير لتحقيق زيادة المعرفة لمستخدمى القرار، ومساعدتهم لتحقيق أغراض معينة، وتمكينهم من الحكم السديد على الظواهر والمشاهدات[٥].

ولذلك فالبيانات تكون فى حالة سكون أما المعلومات فهى فى حالة حركة، ونشاط. لذلك فإن البيانات تمثل حقائق، أو مشاهدات واقعية، أو قياسات تتم بطريقة منهجية يمكن لأحاد الناس قراءتها، وفهم دلالتها البسيطة دون دخول فى عمليات استنباطية؛ أو

---

[٢] فى هذا المعنى: د. محمود نجيب حسنى، شرح قانون العقوبات، القسم العام، طبعة ١٩٨٩، دار النهضة العربية، القاهرة، صـ٤٠؛ يراجع فى هذا المعنى أيضاً: د. محمود مصطفى، شرح قانون العقوبات، القسم العام، طبعة ١٩٨٣، صـ٣٥.

[٣] د. أيمن عبدالله فكرى، جرائم نظم المعلومات، رسالة دكتوراه، جامعة المنصورة، ٢٠٠٦، هامش صـ٤.

[٤] سورة القلم، الأية ٥.

[٥] د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعى، الاسكندرية، الطبعة الثانية، ٢٠٠٦، صـ٧٧.

(ISSN: 2537 - 0758)

استقرائية سواء من حيث استخلاص أى نتيجة مترتبة عليها، أو الربط فيما بين أكثر من بيان. فإن تم ذلك فإننا نكون بصدد دخول منطقة المعلومات[٦].

فالمعلومات هى كل نتيجة تترتب على تشغيل البيانات؛ أو تحليلها؛ أو استقراء دلالتها؛ أو استنباط ما يمكن استنباطه منها على نحو يفيد متخذى القرار؛ أو يسهم فى تطوير المعارف النظرية أو التطبيقية[٧].

هناك من عرفها بأنها: العلاقة بين المعلومات، وبين التقنية الحديثة التى تستخدم من أجل معالجة هذه البيانات[٨].

بالتالى يمكن تعريف المعلوماتية بأنها: البيانات؛ أو المعلومات؛ أو المعطيات التى يمكن معالجتها آلياً بواسطة الحاسب الآلى.

يرتبط بهذا التعريف العديد من المصطلحات الواردة بالمادة الأولى من القانون رقم ١٧٥ لسنة ٢٠١٨ فى شأن مكافحة جرائم تقنية المعلومات يتعين بيانها[٩].

البيانات والمعلومات الالكترونية: كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه، بواسطة تقنية المعلومات كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما فى حكمها.

المعالجة الالكترونية: أى عملية إلكترونية أو تقنية تتم كلياً أو جزئياً لكتابة أو تجميع أو تسجيل أو حفظ أو تخزين أو دمج أو عرض أو إرسال أو إستقبال أو تداول أو نشر أو محو أو تغيير أو تعديل أو استرجاع أو استنباط البيانات والمعلومات الالكترونية وذلك باستخدام أى وسيط من الوسائط أو الحاسبات أو الاجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى.

تقنية المعلومات: أى وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تستخدم لتخزين واسترجاع وترتيب وتنظيم ومعالجة وتطوير وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكياً أو لا سلكياً.

---

[٦] فى هذا المعنى: د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٢٣.

[٧] فى هذا المعنى: أ. محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلى، دار الجامعة الجديدة للنشر، ٢٠٠٠، صـ٣٢.

[٨] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، ٢٠٠٤، صـ٢٥.

[٩] الجريدة الرسمية – العدد ٣٢ مكرر (ج) فى ١٤ أغسطس سنة ٢٠١٨.

البرنامج المعلوماتى: مجموعة الأوامر والتعليمات المعبر عنها بأى لغة أو رمز أو إشارة والتى تتخذ أى شكل من الأشكال ويمكن استخدامها بطريق مباشر أو غير مباشر فى حاسب آلى لأداء وظيفة أو تحقق نتيجة سواء كانت هذه الأوامر والتعليمات فى شكلها الأصلى أو فى شكل آخر تظهر فيه من خلال حاسب آلى أو نظام معلوماتى.

النظام المعلوماتى: مجموعة برامج، وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية.

شبكة معلوماتية: مجموعة من الاجهزة أو نظم المعلومات تكون مرتبطة معاً، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية والتطبيقات المستخدمة عليها.

البريد الالكترونى: وسيلة لتبادل رسائل الكترونية على عنوان محدد بين أكثر من شخص طبيعى أو إعتبارى عبر شبكة معلوماتية أو غيرها من وسائل الربط الالكترونية من خلال أجهزة الحاسب الآلى وما فى حكمها.

دعامة الكترونية: أى وسيط مادى لحفظ وتداول البيانات والمعلومات الالكترونية ومنها الأقراص المدمجة والأقراص الضوئية والذاكرة الالكترونية وما فى حكمها.

الفرع الثانى
تعريف الجريمة المعلوماتية

نظراً لأن الجريمة المعلوماتية من الجرائم المستحدثة لذا نجد أن تعريف الجريمة المعلوماتية محل اختلاف بين الشراح فكلا منهم يعرف الجريمة المعلوماتية وفقاً لوجهة نظره الخاصة.

نتعرض أولاً لتعريف خبراء منظمة التعاون الاقتصادى والتنمية OECD[١٠] حيث تم تعريفها بأنها "كل سلوك غير مشروع؛ أو غير أخلاقى؛ أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات؛ أو نقلها"[١١].

كما تم تعريف الجريمة المعلوماتية فى المادة الأولى من القانون المصرى النموذجى الموحد فى شأن مكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات بأنها " كل فعل مؤثم يتم ارتكابه عبر أى وسيط الكترونى"[١٢].

---

[10] Orgnisation for Economic Co-operation and development, www.oecd.org

[١١] مشار إليه لدى: د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٦١.

(ISSN: 2537 - 0758)

لكن هذا التعريف يعيبه أنه متوسع إلى حد ما حيث أنه يمتد ليشمل أى فعل من الممكن أن يقع على جهاز الحاسب الآلى؛ أو بواسطته، وإنما الجريمة محل البحث إنما تتعلق بالبيانات والمعلومات الموجودة على الحاسب؛ أو على أى دعامة من الدعامات التى تستخدم لاستخراج البيانات الموجودة على الحاسب فمناط الجريمة التى نحن بصددها هى المعلومات أو البيانات.

التعريفات الفقهية للجريمة المعلوماتية:

هناك جانب من الفقه اعتمد على دور الحاسب الآلى، وهو بصدد تعريف الجريمة المعلوماتية فهذا الجانب يرى:

أن الجريمة المعلوماتية هى كل نشاط إجرامى يؤدى فيه نظام الحاسب الآلى دور لإتمامه على أن يكون هذا الدور على قدر من الأهمية، ولا يختلف الامر سواء أكان الحاسب الآلى آداة لإتمام النشاط الإجرامى أم كان محلاً له. ففى كلتا الحالتين ينبغى أن يكون لوجود الحاسب الآلى دور مؤثر فى إتمام النشاط الإجرامى[١٣].

وهناك جانب اخر يعتمد على محل الجريمة وهى المعطيات أو البيانات:

فيرى أن الجريمة المعلوماتية هى كل سلوك غير مشروع إيجابى أو سلبى من شأنه الاعتداء على المعلومات أو البيانات المخزنة داخل الحاسب أو داخل وسائط أخرى يتم تخزين البيانات عليها، ويترتب على ذلك ضرر بصاحب هذه البيانات[١٤].

وهناك من يرى بأن الجريمة المعلوماتية هى الجريمة التى تقع على نظم الحاسب والتلاعب، والافساد، والتخريب التى تقع على الحاسب الالكترونى، وبرامجه، وملحقاته، وبياناته[١٥].

---

[١٢] د. عبدالفتاح بيومى، مكافحة جرائم الكمبيوتر والانترنت فى القانون العربى النموذجى، دار الفكر الجامعى، الاسكندرية، الطبعة الأولى، ٢٠٠٦، صـ١٨.

[١٣] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، صـ٢٦؛ يراجع فى ذلك أيضاً:

.D.B. parker- combattre la crimpinalite in formatiqe- 1985-p-18, Vivant et lestanc- lamy in Droit de Linformatique- paris- 1989- p- 450, Klaus Tiedman, Fraude et autre délits d'affaires commis a l'aide d'ordinateur électronique ,Rev.D.P.C, N 1 , P612, Chernaouti-hell Slange, comment lutter la cypercriminalite?, revue la Science, n391, mais 2010, P24.

[١٤] فى هذا المعنى: أ. محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلى، مرجع سابق، صـ٣٥.

إلا أنه لا يمكن الأخذ بهذا التعريف لأنه يوسع من مفهوم الجريمة المعلوماتية فيمتد، ويشمل ملحقات الحاسب الالى؛ فى حين أنه يجب أن يقتصر التعريف السليم على المعطيات، والبيانات، وما يتعلق بهما.

لذلك نرى أن الجريمة المعلوماتية تتعلق بكل سلوك غير مشروع يرتكب فى إطار المعالجة الآلية للبيانات من خلال تجميعها، وتجهيزها لإدخالها إلى الحاسب بغرض الحصول على معلومات، وكذلك معالجة الكلمات أو النصوص. وهى طريقة آلية تمكن المستخدم من كتابة الوثائق مع إمكانية التصحيح، والتعديل ، والمحو، والتخزين، والاسترجاع، والطباعة. وهى عملية وثيقة الصلة بارتكاب الجرائم و لابد من فهمها للجانى كما فى حالة التزوير والتقليد، وقد تقع على مستخرجات الحاسب أى بعد الطباعة على الاوراق أو الدعامات المغناطيسية، ويكون الهدف من هذه المخرجات هى المعلومات الموجودة عليها.

بهذا يمكننا القول بأن الجريمة المعلوماتية هى كل سلوك غير مشروع يتعلق بالمعالجة الآلية للبيانات أو إدخالها إلى الحاسب أو استخراجها منه.

المطلب الثانى
خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بمجموعة من الخصائص التى تميزها عن غيرها من الجرائم وهى:

الحاسب الآلى هو أداة إرتكاب الجريمة المعلوماتية

الجريمة المعلوماتية لا تقع على جهاز الحاسب الآلى، وإنما تقع على أحد مكونات النظام المعلوماتى، وقد تقع من خلال استخدام هذا النظام، وغالباً ما يكون هدف الجانى هو الرغبة فى إجراء أى تعديل أو محو أو إضافة على البيانات الموجودة داخل جهاز الحاسب الآلى. سواء فى مرحلة الادخال أو المعالجة أو التشغيل ولا يتم ذلك إلا من

---

(١٥) د. علاء عبدالباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، ٢٠٠٢، صـ٤٩؛ يراجع فى ذلك أيضاً:

Michael D Rostoker and Robert H. Rines, Computer jurisprudence, legal responses to the information revulsion, ocoana publication, mc, 1986, P.333.

(ISSN: 2537 - 0758)

خلال استخدامها جهاز الحاسب الآلى وبالتالى فهو الوسيلة المستخدمة لارتكاب هذه الجريمة[١٦].

كما أن الامر لا يقتصر على المعلومات أو البيانات الموجودة على جهاز الحاسب وإنما من الممكن الوصول إلى أية معلومات موجودة على أى حاسب أخر باستخدام شبكة الانترنت، ولا يمكن الوصول إلى هذه الشبكة إلا باستخدام الحاسب الآلى، وبالتالى فهو أداة ارتكاب الجريمة حتى ولو كان محل الجريمة موجود فى مكان أخر.

ومن الممكن الوصول إلى شبكة الانترنت وارتكاب الجريمة المعلوماتية باستخدام الهاتف المحمول، خاصة وأن الولوج إلى شبكة الانترنت من الممكن أن يتم بواسطة هذه الهواتف إلا أن الاغلب الأعم فى هذه الجرائم هو ارتكابها بواسطة الحاسب الآلى[١٧].

الجريمة المعلوماتية ترتكب بواسطة الانترنت

يستطيع المجرم المعلوماتى من خلال استخدام الحاسب الالى الوصول إلى شبكة الانترنت، واستخدامها كأداة هامة لارتكاب الجريمة المعلوماتية، أو تسهيل إرتكابها حيث تعتبر هذه الشبكة هى حلقة الوصل بين كافة الاهداف المحتمل الوصول إليها كالبنوك، والشركات، والاشخاص.

لذلك نجد أن معظم هذه الأهداف عادة ما تلجأ إلى استخدام نظم الأمن الالكترونية لكى تحمى نفسها من تلك الجرائم أو على الاقل أن تحد من خسائرها عند وقوعها كضحية لهذه الجرائم[١٨].

بالتالى يتضح لنا دور شبكة الانترنت فى ارتكاب الجريمة المعلوماتية فمن خلالها يستطيع شخص وهو موجود فى منزله إرتكاب جريمة تترتب أثارها فى بلد أخر غير بلده مما يدل على خطورة هذه الجريمة، وخطورة الأداة التى تم استخدامها.

الجريمة المعلوماتية ليس لها حدود جغرافية

لا يقتصر إرتكاب الجريمة المعلوماتية داخل البلاد إضراراً بالشركات أو البنوك الوطنية أو الاشخاص داخل الدولة الواحدة وإنما يمكن إرتكاب الركن المادى لهذه

---

[١٦] فى هذا المعنى: أ. محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلى، مرجع سابق، صـ٧٦.

[١٧] فى هذا المعنى: د. حسين بن سعيد بن سيف الغافرى، السياسة الجنائية فى مواجهة جرائم الانترنت دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، ٢٠٠٧، صـ٤٠.

[١٨] فى هذا المعنى أ. منير محمد الجنيهى، جرائم الانترنت والحاسب الألى ووسائل مكافحتها، دار الفكر الجامعى، الاسكندرية، ٢٠٠٤، صـ١٤.

الجريمة فى دولة وتتحقق النتيجة فى دولة أخرى كل ذلك إنما يرجع إلى وجود شبكة الانترنت التى جعلت العالم كله بمثابة قرية صغيرة، ويمكن استخدامها فى ارتكاب هذه الجرائم.

فأهم ما يميز شبكة الانترنت هو عالميتها وكونها تربط بين كل القارات، وجميع دول العالم فلا تحدها حدود طبيعية، ولا حدود سياسية. كما أنها تسمح لمستخدميها بحرية التنقل بدون تعقيدات، أو صعوبات فهى عالم ضخم خالى من الحدود والعوائق لذا نجد أن الجريمة التى ترتكب من خلالها لا تعترف بعنصر المكان، ولا بعنصر الزمان. فالبعد الزمانى والمكانى والقانونى له دور فى تشتيت جهود البحث والتحرى لتعقب مثل هذه الجرائم فهى غير مقتصرة على دولة بعينها وإنما هى تمتد لتشمل العالم كله باعتباره مسرحاً للجريمة. حيث يمكن للفرد أن يرتكب جريمته فى أى مكان وفى أى زمان[١٩].

بالتالى نرى أن جريمة واحدة من شأنها التأثير على أكثر من دولة فى آن واحد، ويرجع ذلك إلى القدرة التى تتمتع بها الحاسبات الآلية فى نقل، وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، وتظهر هذه المشكلة بصفة خاصة فى مجال البنوك. حيث أدى التوسع الكبير فى إجراء المعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بُعد دولى للجرائم التى ترتكب إزاء هذه المعاملات البنكية. فالتحويل الالكترونى للأموال يمكن أن يتم من حساب فى بنك فى دولة معينة إلى حساب أخر فى بنك فى دولة أخرى[٢٠].

صعوبة التحرى والتحقيق والاكتشاف فى مجال الجريمة المعلوماتية

تتسم الجريمة المعلوماتية بالغموض بحيث يصعب إثباتها حيث أنها لا تترك أثار مادية تتخلف وراء ارتكابها لذا فالتحرى عنها، والتحقيق، والمقاضاة فى نطاقها ينطوى على العديد من المشكلات والتحديات الإدارية، والقانونية إبتداءاً من ملاحقة الجناة ثم

---

[١٩] فى هذا المعنى: د. حسين بن سعيد بن سيف الغافرى، السياسة الجنائية فى مواجهة جرائم الانترنت دراسة مقارنة، مرجع سابق، صـ٤١.

[٢٠] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، صـ٤٧؛ يراجع فى ذلك ايضاً:

Mascala Corinne, criminalite et contrat electronique, in: La contrat electronique, Travauxde l association Capitant Henri, journees national, Paris, 2000, P119.

(ISSN: 2537 - 0758)

إدانتهم، نظراً لأن إسناد الإدانة إلى الجناة أمر غير سهل، فمن الممكن إتلاف الأدلة من قبل الجناة أو إخفائها وصعوبة الوصول إلى الادلة، وحتى ولو تم إدانتهم فإنه تثور مشكلة التقاضى فى الجرائم العابرة للحدود فأى المحاكم تكون مختصة، وما هو القانون الواجب التطبيق وبالتالى فاكتشافها والمقاضاة عنها أمر غير ميسور[٢١].

كما أنه من الممكن القول بان هناك بعض السمات التى تؤكد صعوبة إكتشاف الجريمة المعلوماتية حيث أنها جريمة هادئة لا عنف فيها كما أنها جريمة فنية لا تترك أثراً كالاثار التى تتركها جريمة أخرى كالدم فى حالة وجود قتل أو أثار العنف فى حالة الاعتداء على الاشخاص، ونظراً لأن هذه الجريمة يتم التعامل فيها مع بيانات وأرقام، ومعلومات مخزنة الكترونياً.فتغير الارقام أو البيانات أو محوها من ذاكرة الحاسب هو ما يشكل الجريمة المعلوماتية، ولاشك أنه كلما تقدم الانسان، وأزداد فهمه للتقنيات الحديثة كلما استطاع أن يخفى جريمته عن طريق ارتكابها دون أثر يمكن الاهتداء اليه من خلاله. الامر الذى يتطلب وجود حماية جنائية كافية[٢٢].

وقد تكون صعوبة اكتشاف هذه الجريمة راجعاً إلى إحجام المجنى عليهم من الابلاغ عن وقوع هذه الجرائم حتى لا يفقدوا ثقة عملائهم. فضلاً عن إمكانية تدمير المعلومات التى يمكن أن تستخدم كدليل فى الاثبات فى مدة قد تقل عن الثانية الواحدة.

فعلى سبيل المثال: أحصت وزارة الداخلية الفرنسية عام ١٩٨٦ حوالى ١٢٠٠ جريمة معلوماتية فى حين كان هناك حوالى ٥٣٦٠٠ جريمة ضد الاشخاص، ١٨٩٠٠ جريمة تندرج تحت وصف جرائم الاداب، ٣ مليون جريمة ضد الأموال[٢٣].

وتفيد هذه الاحصائية قلة عدد الجرائم المعلوماتية، والذى غالباً ما يكون راجعاً إلى صعوبة إكتشاف هذه الجرائم أو إحجام المجنى عليه عن الابلاغ عن وقوع مثل هذه الجرائم ضده.

---

[٢١] فى هذا المعنى: د. حسين بن سعيد بن سيف الغافرى، السياسة الجنائية فى مواجهة جرائم الانترنت دراسة مقارنة، مرجع سابق، صـ٤٢؛ يراجع فى ذلك أيضاً:

Grave-raulin Laurent, regles de conflits de juridications et regles de conflits de lois appliquees aux cybers delit, memoire de master 2 professionnel-droit de l internt publique, Universite Paris 2- Pantheon Sorbonne, 2008, p6

[٢٢] فى هذا المعنى: أ. محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلى، مرجع سابق، صـ٩٧.

[٢٣] د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، صـ٤٤.

محل الجريمة المعلوماتية البيانات المعالجة آلياً

تقع الجريمة المعلوماتية فى بيئة المعالجة الآلية للبيانات حيث يستلزم لقيامها التعامل مع بيانات مجمعة، ومجهزة للدخول للنظام المعلوماتى بغرض معالجتها إلكترونياً بما يمكن المستخدم من إمكانية كتابتها من خلال العمليات المتبعة، والتى توافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها أو طباعتها وهذه العمليات هى وثيقة الصلة بارتكاب الجرائم. ولابد من فهم الجانى لها أثناء ارتكابها فى حالة التزوير والتقليد(٢٤).

بالتالى يتضح لنا أن البيانات سواء كانت فى مرحلة الإدخال إلى جهاز الحاسب، أو أثناء المعالجة الآلية لها أو فى مرحلة الإخراج فإنها تكون محلاً للجريمة المعلوماتية. ففى مرحلة الادخال من الممكن أن يتم إدخال بيانات غير صحيحة وفى مرحلة المعالجة قد يتم المحو أو التعديل أو التصحيح أما فى مرحلة الاخراج فقد يتم إتلاف الدعامة التى تحتوى هذه المعلومات.

المبحث الثانى
المجرم المعلوماتى

فى هذا المبحث نتعرض لدراسة المجرم المعلوماتى من ناحية ماهيته، والخصائص التى يتمتع بها هذا المجرم، وتمييزه عن غيره من المجرمين بالإضافة إلى دوافع ارتكابه لهذا النوع من الجرائم **وذلك فى مطلبين:**

المطلب الأول: ماهية المجرم المعلوماتى.

المطلب الثانى: سمات المجرم المعلوماتى ودوافع ارتكابه.

المطلب الأول
ماهية المجرم المعلوماتى

فكرة المجرم المعلوماتى هى فكرة جديدة فى مجال القانون الجنائى. فالمجرم المعلوماتى ليس بمجرم عادى وإنما هو مجرم ذو طبيعة خاصة حيث يتطلب أن يكون على درجة عالية من المهارة والخبرة والدراية بالتقنيات الحديثة، والحاسب الالى حتى يستطيع التعامل معه، ومع البيانات الموجودة عليه والتى غالباً ما تكون محلاً لجريمته.

---

(٢٤) د. أحمد خليفة الملط، الجرائم المعلوماتية، مرجع سابق، صـ٩٣؛ يراجع فى ذلك أيضاً:
Fauchoux Vincent- Deprez Pierre, Le droit de l internet (loi, contrat et usages), edition Llitec, Paris, 2008, P211.

(ISSN: 2537 - 0758)

لذلك لا يمكن القول بأن هذا المجرم مثل المجرم التقليدى وإنما هو مجرم ذو طبيعة خاصة يتسم بسمات خاصة تمكنه من ارتكاب الجريمة[٢٥].

وإذا كان الاصل أن يكون المجرم المعلوماتى على قدر من المهارة والدراية بالتقنيات الحديثة. إلا أن هذا الاصل يرد عليه استثناء وهو عدم معرفة المجرم المعلوماتى بما يتعلق بالتقنيات الحديثة للحاسب الآلى. وفى هذه الحالة من الممكن أن يستعين بمن هو له خبرة، ودراية بالتقنيات الحديثة، والذى يمكنه من الحصول على هدفه وهى المعلومة، ولا يمنع من أن يكون هذا التخصص مجرم معلوماتى، ولكن إذا وصل هذا المجرم إلى درجة عالية من البراعة فى تنفيذ الجرائم المعلوماتية فإنه يمكن أن يطلق عليه مصطلح المجرم التقنى، وبالتالى فإنه من الممكن أن يكون المجرم التقنى مجرم معلوماتى، وليس كل مجرم معلوماتى مجرم تقنى. فمصطلح المجرم التقنى أعم وأشمل من مصطلح المجرم المعلوماتى. فالإجرام التقنى يحتاج إلى مستوى فهم لتكنولوجيا المعلومات أعلى من فهم المجرم المعلوماتى[٢٦].

مما سبق يمكننا القول بأن المجرم المعلوماتى هو كل شخص يرتكب سلوك غير مشروع يتعلق هذا السلوك بالمعالجة الآلية للبيانات والمعلومات سواء كانت هذه البيانات، والمعلومات مخزنة على الحاسب الآلى؛ أو فى وسائط أخرى يتم تخزين البيانات عليها، وقد يتعلق هذا السلوك بمرحلة الادخال أو الاخراج.

تصنيفات المجرم المعلوماتى

يمكن تصنيف المجرم المعلوماتى لعدة أصناف: المخترقون أو المتطفلون، المحترفون، الحاقدون، صغار نوابغ المعلوماتية.

المخترقون أو المتطفلون

يتسم أفراد هذه الطائفة بأنهم يرتكبون الجرائم المعلوماتية بدافع التحدى الإبداعى، ويجدون أنفسهم متفقين إلى درجة أنهم ينصبون أنفسهم أوصياء على أمن نظم المعلومات فى المؤسسات المختلفة، والسمة الغالبة على أعضاء هذه الطائفة صغر

---

[٢٥] فى هذا المعنى: د. هدى حامد قشقوش، جرائم الحاسب الالكترونى فى التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢، صـ٢٧؛ يراجع فى ذلك أيضاً:

David Thampson ,Current trends in computer crime ,control computer quarterly , Vol , n1, 1991, P 2.

[٢٦] فى هذا المعنى: د. عمر محمد ابوبكر يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، عين شمس، ٢٠٠٤، صـ٢٢١.

السن، وقلة الخبرة، وعدم التمييز بين الأنظمة محل الاختراق، وبرغم هذه السمات فقد تمكن المجرمون من هذه الطائفة من اختراق مختلف أنواع نظم المعلومات التابعة للشركات المالية، والتقنية، والبنوك، ومصانع الالعاب، والمؤسسات الحكومية، ومؤسسات الخدمة العامة كما فى حالة اختراق أحد الصبية الذى يبلغ من العمر ١٤ عاماً نظام المعلومات العامة لوزارة الدفاع الامريكية[٢٧].

كما تتسم هذه الطائفة بتبادل المعلومات فيما بينهم، والتشارك فى وسائل الاختراق، وإطلاع بعضهم بعض على مواطن الضعف فى نظم المعلومات والشبكات. كما يقوم أطراف هذه الطائفة بعقد مؤتمرات لمخترقى نظم المعلومات يُدعى لها الخبراء من بينهم للتشاور حول وسائل الاختراق، وتنظيم عملهم فيما بينهم، ومن الممكن أن يتم استغلال هؤلاء الافراد من قبل منظمات وهيئات إجرامية تسعى للكسب المادى، ومن ناحية أخرى نجد أن العديد من هؤلاء المخترقين قد أسهموا فى تطوير نظم المعلومات والأمن فى عشرات المؤسسات والبنوك فى القطاعين العام والخاص حتى أن هناك العديد من الجهات التى تستعين بخبراتهم لفحص وتدقيق امن ونظم المعلومات[٢٨].

هذه الطائفة وإن كان اختراقهم لنظم المعلومات يعد دخول غير مشروع لأنه دخول غير مصرح به. إلا أن الحقيقة قد تكون غير ذلك لأن دافع هؤلاء غالباً ما يكون حب الاستطلاع، ومعرفة ما وراء هذه النظم الامنية. كما أن اغلبهم يتسم بالأخلاق ، فضلا عن أن منهم من نظم مواقع خاصة بهم لإيضاح حقيقة أمرهم وبالتالى حتى نستطيع أن نسبغ الصفة التجريمية على هؤلاء يقتضى منا أن نفرق بين من نشأ فى بيئة تتسم بالضوابط الأخلاقية وبين من تربوا فى أجواء التحدى والتفاخر بإختراقهم الانظمة المختلفة وبالتالى فإن مناط التجريم يكون هو ارتكاب الفعل المعاقب عليه وبالتالى فإذا ارتكب أحد أعضاء هذه الطائفة فعل مجرم فإنه يعاقب عليه.

المحترفون

هذه الطائفة لا ترتكب الجريمة المعلوماتية بدافع من التحدى الابداعى أو الاثارة، وإنما عادة ما يكون الدافع وراء ارتكاب مثل هذه الجرائم هو تحقيق المصالح الشخصية؛ أو المكاسب المادية.

---

[٢٧] مشار إليه لدى: د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٧٨.

[٢٨] فى هذا المعنى: د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٧٩.

(ISSN: 2537 - 0758)

فهذه الطائفة تتميز بالخبرة والادراك الواسع للمهارات التقنية، وتتمتع بالتنظيم، والتخطيط والاشتراك فى الانشطة، والجرائم التى يرتكبها أفرادها، ولذا فهى تعد اخطر طائفة من بين مجرمى التقنية. فالهدف الاساسى وراء ارتكاب افراد هذه الطائفة للجريمة المعلوماتية هو تحقيق الربح المادى سواء للمجرم المعلوماتى ذاته؛ أو للجهة التى سخرته لإجراء مثل هذه الجرائم. وبالرغم من وجود تخطيط، وتنظيم بين أفراد هذه الطائفة ولكنه لا يكون على المدى الواسع كما هو الحال بالنسبة للمتطفلين. فالمحترفون لا يقومون بعقد ندوات أو مؤتمرات للتعريف بهم أو لتبادل المعلومات كما هو الحال فى طائفة المتطفلين وقد أدى احتراف الجريمة المعلوماتية إلى وصول بعض المجرمين إلى مرحلة التخصص فهناك من يتخصص فى الاحتيال، والتزوير ويكون دافع هؤلاء غالباً هو الحصول على المال، وهناك من يوجه نشاطه إلى التجسس على نظم المعلومات التابعة للشركات الدولية بقصد الحصول على أسرار هذه الشركات إما لحساب أنفسهم؛ أو لحساب منافسين أخرين فى السوق وأحياناً لحساب مجموعات القرصنة الدولية[٢٩].

مما سبق يتضح لنا أن خطورة أفراد هذه الطائفة تكمن فى التقنية العالية التى يتمتع بها هؤلاء الافراد. حيث غالباً ما يكون هؤلاء الافراد من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة على تقنية الالكترونيات. كما يتمتعون بقدر عالى من الكفاءة والذكاء والتى تمكنهم من تحدى واختراق النظم المعلوماتية. دون أدنى إهتمام لأى قيمة من القيم التى يتم التعرض لها[٣٠].

الحاقدون

تختلف هذه الطائفة عن الطائفتين السابق ذكرهم فهى لا تهدف إلى إثبات الذات أو المقدرة الفنية، والتقنية أو التحدى الابداعى لنظم المعلومات. كما لا تهدف أيضاً إلى الحصول على مكاسب مادية أو سياسية ولكن هذه الطائفة إنما يكون غرضها الاساسى هو الانتقام أو الثأر من شخص بعينه أو من مؤسسة بعينها والمجرم فى هذه الحالة إما أن يكون مستخدم للنظام ومنتمى للطائفة التى يريد إضرارها بمعنى أن يقوم بإضرارها بحاسب من الحواسب المتعلقة بالمؤسسة أو الشخص المجنى عليه فى هذه الجريمة؛ وإما أن يكون غريب عن هذا النظام ولكن تتوافر لديه أسباب الانتقام[٣١].

---

[٢٩] هذا المعنى مشار إليه لدى: د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٨٠.

[٣٠] د. علاء عبدالباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، مرجع سابق، صـ٥٦.

[٣١] فى هذا المعنى: د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٨٠.

والامثلة على هذه الطائفة كثيرة منها: قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشآت التى يعمل بها بحيث بعد رحيله من المنشأة بعدة اشهر يتم تدمير البيانات الخاصة بحسابات، وديون المنشأة وقد تحقق ذلك[٣٢].

وجدير بالذكر أن أعضاء هذه الطائفة لا تتسم بالمعرفة التقنية الاحترافية ومع ذلك يكون لديه دافع رهيب فى سبيل الوصول إلى كافة العناصر المتعلقة بالفعل الذى ينوى إرتكابه على وجه الدقة، وتغلب على أنشطتهم من الناحية التقنية إستخدام تقنيات زراعة الفيروسات، والبرامج الضارة، وتخريب النظام، وإتلاف كل أو بعض المعطيات أو البيانات المراد إتلافها، وتعطيل النظام أو الموقع المستهدف إذا كان من مواقع الانترنت وبالرغم من أن سمات هذه الطائفة تضعها من حيث الخطورة فى مؤخرة الطوائف السابق ذكرها إذ هم أقل خطورة من غيرهم من مجرمى المعلوماتية. إلا أن ذلك لا يمنع أن تكون الاضرار التى تنجم عن أنشطة بعضهم جسيمة مما تكون سبباً فى إلحاق خسائر فادحة بالمؤسسات المستهدفة[٣٣].

صغار نوابغ المعلوماتية

يقصد بصغار نوابغ المعلوماتية الشباب البالغ المفتون بنظم المعلومات والحاسبات وغالباً ما ترتكب هذه الطائفة جريمتهم عن طريق حواسبهم الشخصية أو عن طريق الحواسب الموجودة داخل مدارسهم وهذه الطائفة عادة ما تكون بمثابة هواة، ولا يمكن ضمهم إلى الطوائف السابقة لأنه غالباً ما يكون الدافع وراء إرتكاب جريمتهم هو الميل للمغامرة، والتحدى، والرغبة فى الاكتشاف ونادراً ما تكون أفعالهم المحظورة غير شرعية وهذا النمط لا خوف منه ولكن يخشى التحول لأفراد هذه الطائفة من هاوٍ إلى محترف صغير للأفعال غير المشروعة كالاحتيال، والسلب وقد يمتد الأمر فيترتب عليه إحتضان مؤسسات إجرامية لهم وهنا تكمن الخطورة نظراً لأن مثل هؤلاء الافراد إذا ما ظهر عليهم النبوغ فى هذه السن الصغير فإن الامر يصبح جدى خطير إذا تم توجيه هذا النبوغ فى الإتجاه الخاطئ[٣٤].

---

[٣٢] مشار إليه لدى: د. أحمد خليفة الملط، الجرائم المعلوماتية، مرجع سابق، صـ٩٠.

[٣٣] هذا المعنى مشار إليه لدى: د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٨١.

[٣٤] د. علاء عبدالباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، مرجع سابق، صـ٥٤؛ يراجع فى ذلك أيضاً:

Agsous Naima, cybercriminalite: les reseaux informatiques, Revue de la gendarmerie, N29, novembre, 2008, P 19.

(ISSN: 2537 - 0758)

والامثلة على ذلك كثيرة ومنها: قيام طالب عمره ١٩ عاماً فى ألمانيا بنسخ وإفشاء بيانات حاسب آلى على نحو غير مصرح به مما أدى إلى خسارة الصناعة الالمانية بمبلغ ٢٣ ألف مارك[٣٥].

ونظراً لحداثة سن هذه الفئة فإن الامر يثير جدلاً كبيراً حول هذه الطائفة، ومدى إمكان تجريم فعلهم أو معاقبتهم الامر الذى يؤدى إلى وجود ثلاث اتجاهات[٣٦]:

الاتجاه الأول:

يدور أنصار هذا الاتجاه حول عدم إسباغ أى صفة تجريمية على أفراد هذه الطائفة ولا يجب إضافتهم ضمن أى طائفة من الطوائف الاجرامية لمجرمى الحاسبات إستناداً إلى أن صغار السن لهم ميل للمغامرة، والتحدى، والرغبة فى الاكتشاف، ونادراً ما تكون أهداف أفعالهم المحظورة غير شرعية إستناداً إلى أنهم لا يدركون، ولا يقدرون مطلقاً النتائج المحتملة التى يمكن أن تؤدى إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة.

الاتجاه الثانى:

أنصار هذا الاتجاه يعتبر أفراد هذه الطائفة ممن يقدمون خدمات جليلة لأمن المعلومات، ووسائل الحماية، ويصفهم بالاخيار، وأحياناً بالأبطال الشعبيين ويتمادى هذا الاتجاه فى تقديره لهذه الفئة بالمطالبة بمكافأتهم بإعتبارهم لا يسببون ضرراً للنظام المعلوماتى، وإليهم ينسب الفضل فى كشف الثغرات الأمنية فى تقنية المعلومات.

الإتجاه الثالث:

يرى أنصاره أن مرتكبى جرائم نظم المعلومات من هذه الطائفة يصنفون ضمن مجرمى الحاسب كغيرهم دون تمييز إستناداً إلى أن تحديد الحد الفاصل بين العبث فى الحاسبات وبين الجريمة أمر عسير من جهة ودونما أثر على وصف الفعل قانوناً من جهة أخرى. كما أن خطورة أفعالهم، والتى تتميز بانتهاك الانظمة، واختراق الحاسبات، وتجاوز إجراءات الامن. كل ذلك يعد من أخطر جرائم نظم المعلومات تعقيداً من الوجهة التقنية.

---

[٣٥] مشار إليه لدى د. عبدالفتاح بيومى، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، صـ٩٠.

[٣٦] عرض هذه الاتجاهات مشار إليها لدى د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٨١ وما بعدها.

ويدعم صحة هذا الاتجاه التخوفات التى يثيرها أصحاب الاتجاه الأول ذاتهم. إذ يخشون من الخطر الذى يواجه هذه الطائفة، والمتمثل فى احتمال تعرضهم لاحتضان المنظمات الاجرامية لهم وتحويلهم من مجرد هواة إلى مجرمين محترفين[٣٧].

الرأى الشخصى

إزاء الاتجاهات السابقة نستطيع أن نقول أن كافة هذه الاتجاهات يثيرها النقد، وذلك على النحو التالى:

فأصحاب الاتجاه الأول يرون عدم إسباغ أى صفة إجرامية على الفعل، وهذا أمر لا يمكن مسايرته لأن السلوك غير المشروع لا نستطيع أن نعفيه من الوصف الاجرامى.

أما أصحاب الاتجاه الثانى والذين يروا وجوب مكافئة هؤلاء النوابغ على ما أرتكبوه بحجة أنهم اكتشفوا ثغرات أمنية لا يمكن مسايرته لأن الاصل هو العقاب لأن دخولهم واكتشافهم لهذه الثغرات غير مصرح به وغير مشروع من البداية.

أما أصحاب الاتجاه الثالث والذين ذهبوا إلى وجوب معاقبتهم مثلهم مثل المحترفين فلا يمكن الاخذ بهذا القول لأنه يوجد به تطرف لأن ظروف أو سن هؤلاء الافراد تختلف عن ظروف المحترفين، وكذلك الاهداف. فأهداف صغار نوابغ المعلوماتية عادة ما يكون المغامرة أما المحترفين فهو الحصول على المال.

لذلك نرى أن الدخول غير المشروع لصغار نوابغ المعلوماتية، واختراق الانظمة الامنية للشركات، والمؤسسات هو فعل مجرم، ويستحق العقاب، ولكن فى حالة عقابهم لابد من وجود عقوبات مناسبة لهم تميزهم عن المحترفين نظراً لاختلاف الظروف التى تم ارتكاب الجريمة فيها وكذلك الاهداف التى يسعى كلا منهم إليها إعمالاً لمبدأ التفريد العقابى.

المطلب الثانى
سمات المجرم المعلوماتى ودوافع ارتكابه

نتعرض فى هذا المطلب للخصائص التى تميز المجرم المعلوماتى عن غيره، وكذلك دوافع إرتكابه لتلك الجريمة، **وذلك فى فرعين:**

الفرع الاول: سمات المجرم المعلوماتى.

الفرع الثانى: دوافع ارتكاب المجرم المعلوماتى لجريمته.

---

[٣٧] هذا المعنى مشار إليه لدى د. أيمن عبدالله فكرى، جرائم نظم المعلومات، مرجع سابق، صـ٨٣.

(ISSN: 2537 - 0758)

الفرع الأول
سمات المجرم المعلوماتى

يتسم المجرم المعلوماتى بعدة خصائص تميزه عن غيره من المجرمين نذكرها فيا يلى:

أولا: الذكاء

الاجرام المعلواتى يتطلب أن يكون المجرم على قدر عالى من الذكاء، وهذا هو أهم ما يميزها عن غيرها من الجرائم. فالاجرام المعلوماتى لا يتطلب أى قوة بدنية أو عضلية وإنما ترتكب الجريمة بصورة هادئة لا عنف فيها، ولا سفك دماء. فالإعتماد كله إنما يكون على الذكاء والتفكير وهما الاساس الذى عليه يتم ارتكاب الجريمة المعلوماتية. فهذا النوع من الاجرام ينتمى إلى جرائم الحيلة، ولذا يقال أن الاجرام المعلوماتى هو إجرام الاذكياء مقارنة بالجريمة التقليدية التى يتطلب فيها قدر من العنف(٣٨).

ثانيا: المهارة

يتميز المجرم المعلوماتى عن غيره بأنه يتطلب أن يكون لديه قدر من الخبرة، والمهارة التى تمكنه من ارتكاب جريمته.

فتنفيذ الجريمة المعلوماتية يتطلب قدر من الخبرة والمهارة والتى تكون قد تم اكتسابها عن طريق الدراسة المتخصصة أو الخبرة المكتسبة فى مجال تكنولوجيا المعلومات أو التفاعل الاجتماعى مع الاخرين ولكن هذا لا يعنى أنه يجب أن يكون على قدر من الخبرة الكافية ذلك أن هناك من مجرمى المعلوماتية من لم يتلقوا الخبرة الكافية أو المهارة اللازمة ومع ذلك فهم من أنجح مجرمى المعلوماتية(٣٩).

ونظراً للدقة التى تتطلبها الجريمة المعلوماتية حتى يتم ارتكابها فإن الامر لا يكون سهلاً على المبتدئ وإنما يتطلب قدر من الاحتراف حتى يستطيع تخطى العقبات التى أوجدها المتخصصون لحماية أنظمة الكمبيوتر كما يحدث فى البنوك فالمبتدئ وإن أمكن

---

(٣٨) د. محمد سامى الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، ١٩٩٨، صـ٣٤.

(٣٩) فى هذا المعنى: د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، صـ٥٢؛ يراجع فى ذلك أيضاً:
Mascala Corinne, Criminalite et contrat electronique, Op-cit, P118.

أن يرتكب الجريمة المعلوماتية إلا أنه لا يستطيع التوصل إلى نتائج سليمة سوى فى حالات قليلة[٤٠].

ثالثاً: المعرفة

الجناة عادة يمهدون لإرتكاب جرائمهم عن طريق التعرف على كافة الظروف التى تحيط بمحل جريمتهم، وهذا هو ما يتم فى إطار الجريمة المعلوماتية. فالتعرف على كافة الظروف التى تحيط بالجريمة المراد تنفيذها وإمكان نجاحها أو فشلها كل ذلك هو ما يقوم به الجناة قبل ارتكابهم لجريمتهم حتى لا يواجهون باشياء غير متوقعة من شأنها فشل مشروعهم الاجرامى أو الكشف عن مخططهم الاجرامى. ومن خلال المعرفة يستطيع المجرم المعلوماتى أن يُكون تصور كامل لكل ظروف الجريمة. ذلك أن مسرح الجريمة هو الحاسب الآلى وبالتالى يستطيع الجانى تنفيذ جريمته على أنظمة مماثلة لتلك التى يقوم باستهدافها وذلك قبل تنفيذ جريمته تمهيداً لا رتكابها والوصول إلى أعلى نسب النجاح وأقل نسب الفشل[٤١] وبالتالى يتضح لنا مدى أهمية العلم بظروف الجريمة وما له من دور هام فى نجاح المشروع الاجرامى.

رابعاً: السلطة

يقصد بها الحقوق والمزايا التى يتمتع بها المجرم المعلوماتى والتى تمكنه من ارتكاب جريمته، فكثير من مجرمى المعلوماتية لديهم سلطة مباشرة أو غير مباشرة فى مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة فى الشفرة الخاصة بالدخول إلى النظام الذى يحتوى على المعلومات والتى تعطى الفاعل مزايا متعددة لفتح الملفات، وقراءتها، وكتابتها، ومحو أو تعديل المعلومات التى تحتوى عليها وقد تتمثل هذه السلطة فى الحق فى استعمال الحاسب الآلى أو إجراء بعض التعاملات أو مجرد الدخول إلى الاماكن التى تحتوى على أنظمة الحاسب الآلية وقد تكون السلطة التى تتمتع بها الجانى غير حقيقية كما فى حالة استخدام شفرة الدخول الخاصة بشخص أخر[٤٢].

ومن هنا يتضح لنا أن مجرمى هذه الطائفة عادة ما ينتمون إلى الطبقة المتعلمة ومعظمهم من العاملين بالجهة محل الجريمة وعادة ما يكونوا محلاً للثقة ولا تشوب سمعتهم ولا نزاهتهم شائبة وكل ذلك هو ما يكون دافعاً لهم لارتكاب هذه الجرائم نتيجة

---

[٤٠] فى هذا المعنى: د. عبدالفتاح بيومى، مكافحة جرائم الكمبيوتر والانترنت، مرجع سابق، صـ٨٣.

[٤١] فى هذا المعنى: د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، صـ٥٣.

[٤٢] فى هذا المعنى: د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، صـ٥٣.

(ISSN: 2537 - 0758)

شعورهم بالأمن نظراً لجهل كبار الموظفين والمديرين بأنظمة المعلومات وتقنيات الحاسب والبرمجة ويظهر لديهم الإحساس بإمكانية إرتكاب الجريمة دون اكتشافهم[٤٣].

وبالتالى يتضح لنا دور السلطة فى ارتكاب الجريمة المعلوماتية بل يمتد الامر ويشمل دورها أيضاً فى إخفاء معالمها وصعوبة اكتشافها. ذلك أنه مادام هذا الموظف فى عمله فإنه يكون لديه الامكانية لإخفاء معالم جريمته والتى لن تظهر إلا بعد تركه لوظيفته أو قد لا تظهر بعد تركه وظيفته نتيجة لارتكابها بصورة متقنة.

الفرع الثانى
دوافع ارتكاب الجريمة المعلوماتية

الدافع لارتكاب الجريمة هو العامل المحرك للارادة وتوجيه السلوك الاجرامى لارتكاب الجريمة وتحقيق غاية معينة؛ فالجريمة المعلوماتية لا ترتكب إلا بوجود دوافع أو غاية يرمى إليها المجرم المعلوماتى شأنها فى ذلك شأن باقى الجرائم وهذه الدوافع او الغايات لا تخرج عن الدوافع الاتية:

أولاً: الدافع المادى

الدافع المادى هو الدافع الاساسى أو شبه الاساسى الذى يرمى إليه الجانى فى حالة ارتكابه أى جريمة وفى إطار الجريمة المعلوماتية فإن الامر لا يقتصر على الدافع المادى فقط وإنما يكون بجواره دافع أخر من الدوافع التى سيتم ذكرها. فتحقيق ربح هو دافع اساسى نظراً لأن تلك الجريمة سهلة على المتخصصين بالاضافة إلى صعوبة اكتشافها كما أن أرباحها تكون عالية جدا إذا ما قورنت بأى جريمة أخرى ولذا فهى وسيلة سريعة للثراء الفاحش.

ثانياً: الاستيلاء على المعلومات

قد يكون الغرض من ارتكاب الجريمة المعلوماتية هو الحصول على المعلومة والاستيلاء عليها باى وسيلة من وسائل الاستيلاء. سواء كانت هذه المعلومة محفوظة أو منقولة وسواء كان الاستيلاء عليها بالتغيير أو الحذف أو الالغاء نهائياً. فالجريمة المعلوماتية متعلقة بالبيانات والمعطيات الموجودة على الحاسب وبالتالى فهى الهدف الاول الذى يسعى إليه المجرم المعلوماتى سواء كان بقصد التنافس أو الابتزاز أو غيرها

---

[٤٣] فى هذا المعنى: د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالات الحديثة، أسيوط، ١٩٩٤، صـ٤٢.

من الدوافع وفى الاعم الاغلب يكون الهدف من الاستيلاء إقتصادى لتحقيق مكاسب إقتصادية. فالحصول على مزايا مادية والسعى وراء الربح هو من أهم الدوافع التى بسببها يتم الاستيلاء على المعلومة(٤٤).

وقد يكون الهدف هو الحصول على المعلومات فقط وتعلمها دون إستخدامها فى أى وسيلة غير مشروعة كالابتزاز وإن كان الامر فى ظاهره لا يشكل أى جريمة إلا إنه عند التأمل فيه نجد أن جمع المعلومات بطريقة غير مشروعة يندرج تحت جريمة الدخول غير المصرح به.

ويشير أحد الباحثين فى مجال قرصنة الانظمة وهو الاستاذ ليفى فى مؤلفه قراصنة الانظمة إلى أن اخلاقيات هؤلاء القراصنة ترتكز على مبدأين أساسيين هما: الاول: أن الدخول إلى أنظمة الحاسب الالى يمكن أن يعلمك كيف يسير العالم ، والثانى: أن جمع المعلومات يجب أن يكون غير خاضع للقيود هذا ودائما ما يعلن قراصنة الانظمة أن رغبتهم فى الوصول إلى مصادر المعلومات والحاسبات الالكترونية والشبكات تكون بهدف التعلم ليس إلا وكتب أحد القراصنة يقول " يكشف قراصنة الانظمة عن نقطة ضعف أمنية فيحاولون استغلالها لانها موجودة بهدف عدم تخريب المعلومات أو سرقتها وأعتقد أن ما يقوم به يشبه قيام شخص باكتشاف أساليب جديدة للحصول على المعلومات من المكتبة. فيصبح فى غاية الاثارة وينبغى ألا نستهين بكفاءة الشبكات التى يتعلم من خلالها القراصنة حرفتهم فهم يقومون بالفعل بالبحث من خلال الانظمة والعمل من خلال الجماعة وتعليم بعضهم البعض(٤٥).

وبالتالى يتضح لنا أن الاستيلاء على المعلومات لا يقتصر على استخدامها فى الابتزاز والوسائل غير المشروعة، وإنما من الممكن أن يكون الدافع على الاستيلاء هو الولع فى جمع المعلومات وتعلمها وليس الدافع المادى. فقد يعتبر البعض أن حصولهم على المعلومات من هذه الشبكات الأمنية كحصولهم على المعلومات من المكتبة، ولا يمنع ذلك من خضوع فعلهم للتجريم نظراً لأن دخولهم على هذه الشبكات دخول غير مشروع لانه غير مصرح به.

---

(٤٤) فى هذا المعنى: د. حسين بن سعيد بن سيف الغافرى، السياسة الجنائية فى مواجهة جرائم الانترنت دراسة مقارنة، مرجع سابق، صـ٤٤.

(٤٥) المرجع السابق، صـ٤٣.

(ISSN: 2537 - 0758)

ثالثا: الرغبة فى قهر النظام والتفوق على تعقيد الوسائل التقنية

قد يكون الدافع وراء ارتكاب الجريمة المعلوماتية هو الرغبة فى تحقيق الذات وتحقيق انتصار على نظم المعلومات وغالبا ما يتم ارتكاب ذلك دون أن يكون لدى الفرد أى نية للاجرام أو لارتكاب جريمة وعادة ما يكون ارتكاب مثل هذه الجرائم راجعاً إلى وجود عجز فى التقنية أو فى النظام الامنى للشبكات المعلوماتية والتى تترك الفرصة لهؤلاء الافراد إلى إرتكاب مثل هذه الجرائم[٤٦].

وعادة ما يكون مرتكبى هذا النوع من الجرائم هم صغار السن حيث يتوافر لديهم دافع التحدى والميل للمغامرة ومواجهة تقنيات الحاسب ومحاولة الانتصار على النظم الامنية فى الشبكات المعلوماتية دون أن يكون هناك أى دافع للربح المادى فالرغبة فى قهر النظام والتفوق على تعقيد الوسائل التقنية هو الدافع لارتكاب الجريمة لدى هذه الطائفة.

رابعاً: الانتقام من الجهات أو الاشخاص

الانتقام عادة ما يكون دافع له دور مؤثر فى ارتكاب الجريمة وفى الجريمة المعلوماتية قد يكون الدافع من وراء ارتكابها هو الانتقام من شخص بعينه أو من جهة بعينها لوجود خلافات سابقة بين الجانى وبين الشخص أو الجهة أو المؤسسة المجنى عليها.

وعادة ما يكون الانتقام فى صورة إلحاق أذى بالاخرين وفى هذه الحالة يتم ذلك عن طريق البيانات والمعلومات الموجودة على جهاز الحاسب، والتى يتم استخدامها فيما بعد أو فى الحال حتى يحقق الجانى هدفه فقد يقوم بتهديد المجنى عليه أو التشهير به أو الاساءة بسمعته وقد يصل الامر إلى حد الابتزاز لحصوله على أموال ليست من حقه وعادة ما يكون الجانى على علاقة سابقة بالمجنى عليه كأن يكون صديق لشخص المجنى عليه أو موظف داخل المؤسسة أو الجهة المجنى عليها ولكن تم إنهاء خدمته.

مثال ذلك: قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشئات بحيث إذا رحل من المنشأة يتم تدمير كافة البيانات الخاصة بحسابات وديون المنشاة وقد تحقق ذلك[٤٧].

---

[٤٦] فى هذا المعنى: د. أحمد خليفة الملط، الجرائم المعلوماتية، مرجع سابق، صـ٩٠.

[٤٧] مشار إليه لدى: المرجع السابق، صـ٩٠.

خامساً: التنافس

قد يكون التنافس هو الدافع وراء ارتكاب الجريمة المعلوماتية وعادة ما يتم ذلك بين زملاء داخل إحدى المؤسسات أو المنشئات ويريد كلا منهم أن يظهر براعته الفنية وقدراته فى التعامل مع أنظمة الحاسبات، ويظهر هذا بوضوح لدى مبرمجى المعلومات. فكلاً منهم يريد إثبات قدراته الفنية وقد يكون ذلك راجعاً لإندفاعه تحت تأثير رغبة قوية من أجل تأييد قدراته التقنية لإدارة المنشأة لإرتكاب فعل، وقد يعترف به حتى يثبت مدى قدرته على اختراق نظم المعلومات[٤٨].

سادساً: الدافع السياسى

قد يكون الدافع وراء ارتكاب الجريمة المعلوماتية هو دافع سياسى كتهديد الأمن القومى والعسكرى لدولة ما وظهور ما يعرف بحرب المعلومات والتجسس الالكترونى. فالدافع وراء ارتكاب هذه الجريمة هو دافع سياسى بحت يكون عادة إضرار بالمصالح المختلفة للبلاد الاخرى ويتم ذلك عن طريق الوصول إلى المعلومات السرية الموجودة لدى دولة ما ومحاولة تغييرها أو الدخول على النظام الامنى لإحدى الوزارات الهامة فى دولة ما كوزارة الدفاع ومحاولة تعديل بعض المعلومات أو محوها أو تخزين معلومات خاطئة كل ذلك من شأنه الاضرار بالأمن القومى للدولة محل الجريمة.

والحقيقة أنه أياً كان الباعث وراء ارتكاب الجريمة المعلوماتية فانه يوجد شعور دائم لدى مرتكب الجريمة بأن ما يقوم به لا يدخل فى عداد الجرائم وخاصة فى الحالات التى يمكن أن يقف فيها السلوك عند حد قهر نظام الحاسب الالى وتخطى الحماية المضروبة حوله. حيث يفرق هؤلاء الاشخاص بين الحماية المتعلقة بأحاد الافراد، وبين الحماية المتعلقة بالمؤسسات إعتقاداً منهم أن هذه المؤسسات لديها القدرة المالية على تحمل نتائج تلاعبهم[٤٩].

خلاصة القول: أن الجريمة المعلوماتية تتعلق بكل سلوك غير مشروع يقع على البيانات والمعلومات الموجودة على جهاز الحاسب الآلى أو أى نظام من أنظمة المعلومات. مادام أن هذا السلوك يشكل إعتداء على حقوق الغير أو أضرار بهم سواء وقع هذا الأضرار داخل الدولة أو خارجها كما أنه يجب خضوع مرتكب مثل هذه

---

[٤٨] فى هذا المعنى: د. محمد سامى الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، صـ٣٤.

[٤٩] فى هذا المعنى: د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، مرجع سابق، صـ٥٤.

(ISSN: 2537 - 0758)

الجريمة للعقاب بغض النظر عن البواعث أو الدوافع وراء ارتكابه لهذه الجريمة وبغض النظر عن سنه فلا عبرة بما إذا كان كبير أو صغير محترف أو متطفل فما دامت وقعت الجريمة فيجب وقوع العقاب مع مراعاة مبد التفريد العقابى.

الخاتمة

بذلك نكون قد انتهينا من هذا البحث المتواضع فى الجريمة المعلوماتية والذى **تناولناه فى مبحثين وتوصلنا فيه الي النتائج التالية:**

- الجريمة المعلوماتية تتعلق بكل سلوك غير مشروع يرتكب فى إطار المعالجة الآلية للبيانات من خلال تجميعها وتجهيزها لإدخالها إلى الحاسب بغرض الحصول على معلومات أو استخراج بيانات أو معلومات من الحاسب.
- الجريمة المعلوماتية لا تقع على جهاز الحاسب الآلى، وإنما تقع على أحد مكونات النظام المعلوماتى، وقد تقع من خلال استخدام هذا النظام.
- شبكة الانترنت أداة هامة لارتكاب الجريمة المعلوماتية، أو تسهيل إرتكابها حيث تعتبر هذه الشبكة هى حلقة الوصل بين كافة الاهداف المحتمل الوصول إليها.
- صعوبة إكتشاف الجريمة المعلوماتية حيث أنها جريمة هادئة لا عنف فيها كما أنها جريمة فنية لا تترك أثراً كالاثار التى تتركها جريمة أخرى.
- الجريمة المعلوماتية لا تعرف الحدود الجغرافية ويرجع ذلك إلى وجود شبكة الانترنت التى جعلت العالم كله بمثابة قرية صغيرة، ويتم استخدامها فى ارتكاب هذه الجرائم.
- المجرم المعلوماتي هو كل شخص يرتكب سلوك غير مشروع يتعلق هذا السلوك بالمعالجة الآلية للبيانات والمعلومات سواء كانت هذه البيانات والمعلومات مخزنة على الحاسب الآلى أو فى وسائط أخرى يتم تخزين البيانات عليها وقد يتعلق هذا السلوك بمرحلة الادخال أو الإخراج.
- الاجرام المعلوماتى يتطلب أن يكون المجرم على قدر عالى من الذكاء، وهذا هو أهم ما يميزها عن غيرها من الجرائم. فالاجرام المعلوماتى لا يتطلب أى قوة بدنية أو عضلية وإنما ترتكب الجريمة بصورة هادئة لا عنف فيها، ولا سفك دماء.
- تتعدد أغراض ارتكاب الجريمة المعلوماتية ويجمعها الحصول على المعلومة والاستيلاء عليها بأى وسيلة من وسائل الاستيلاء واستغلالها بصورة أو بأخري للاستفادة بها على نحو معين وتحقيق غرض معين.

وبهذا نكون قد انتهينا من بحثنا راجي المولى عزوجل أن يجعله فى ميزان حسناتنا وأن يوفقنا إلى ما يحبه ويرضاه.

المراجع

أولا: الرسائل

- د. أيمن عبدالله فكرى، جرائم نظم المعلومات، رسالة دكتوراه، جامعة المنصورة، ٢٠٠٦.
- د. حسين بن سعيد بن سيف الغافرى، السياسة الجنائية فى مواجهة جرائم الانترنت دراسة مقارنة، رسالة دكتوراه، جامعة عين شمس، ٢٠٠٧.
- د. عمر محمد ابوبكر يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، عين شمس، ٢٠٠٤.

ثانياً: المؤلفات

- د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعى، الاسكندرية، الطبعة الثانية، ٢٠٠٦.
- د. عبدالفتاح بيومى، مكافحة جرائم الكمبيوتر والانترنت فى القانون العربى النموذجى، دار الفكر الجامعى، الاسكندرية، الطبعة الأولى، ٢٠٠٦.
- د. علاء عبدالباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة.
- د. محمد سامى الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، ١٩٩٨.
- محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلى، دار الجامعة الجديدة للنشر، ٢٠٠٠.
- د. محمود مصطفى، شرح قانون العقوبات، القسم العام، طبعة ١٩٨٣.
- د. محمود نجيب حسنى، شرح قانون العقوبات، القسم العام، طبعة ١٩٨٩، دار النهضة العربية، القاهرة.
- منير محمد الجنيهى، جرائم الانترنت والحاسب الألى ووسائل مكافحتها، دار الفكر الجامعى، الاسكندرية، ٢٠٠٤.
- د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، ٢٠٠٤.
- د. هدى حامد قشقوش، جرائم الحاسب الالكترونى فى التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢.

(ISSN: 2537 - 0758)

- د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الالات الحديثة، أسيوط، ١٩٩٤.

ثالثا: المراجع الاجنبية

- Chernaouti-hell Slange, comment lutter la cypercriminalite?, revue la Science, n391, mais 2010.
- David Thampson ,Current trends in computer crime ,control computer quarterly , Vol , n1, 1991.
- .D.B. parker- combattre la crimpinalite in formatiqe- 1985-p-18.
- Fauchoux Vincent- Deprez Pierre, Le droit de l internet (loi, contrat et usages), edition Llitec, Paris, 2008.
- Grave-raulin Laurent, regles de conflits de juridications et regles de conflits de lois appliquees aux cybers delit, memoire de master 2 professionnel-droit de l internt publique, Universite Paris 2- Pantheon Sorbonne, 2008.
- Klaus Tiedman, Fraude et autre délits d'affaires commis a l'aide d'ordinateur électronique ,Rev.D.P.C, N 1.
- Mascala Corinne, criminalite et contrat electronique, in: La contrat electronique, Travauxde l association Capitant Henri, journees national, Paris, 2000.
- Michael D Rostoker and Robert H. Rines, Computer jurisprudence, legal responses to the information revulsion, ocoana publication, mc, 1986.
- Vivant et lestanc- lamy in Droit de Linformatique- paris- 1989.

رابعا: المواقع الالكترونية

- Orgnisation for Economic Co-operation and development, www.oecd.org