مدى الحماية الجنائية للمعلومات عبر الحاسوب والإنترنت

دراسة مقارنة

The Degree of Criminal Protection Of Information that is Technically Processed via Computer and the Internet: Acomparative Study

إعداد

منذر عبد الرزاق العمايره

إشراف الدكتورة

رنا إبراهيم العطور

قدمت هذه الأطروحة استكمالا لمتطلبات الحصول على درجة دكتوراه

فلسفة في القانون

كلية القانون

جامعة عمان العربية

عمان 2012

التفويض

أنا:منذر عبدالرزاق مصلح العمايره

أفوض جامعة عمان العربية بتزويد نسخ من أطروحتي للمكتبات أو المؤسسات أو الهيئات أو الأشخاص عند طلبهم حسب التعليمات النافذة للجامعة .

الإسم: منذر عبد الرزاق مصلح العمايره

التوقيع:

التاريخ: / / 2012

قرار لجنة المناقشة

نوقشت هذه الأطروحة بعنوان " مدى الحماية الجنائية للمعلومات عبر الحاسوب والإنترنت- دراسة مقارنة- " وأجيزت بتاريخ / / 2012

أعضاء لجنة المناقشة:		التوقيع
1- الأستاذ الدكتور علي جبار صالح	رئيساً	.....
2- الأستاذ الدكتور رياض الشلبي	عضواً	.....
3-الدكتورة رنا ابراهيم العطور	مشرفاً وعضواً	.....
4-الدكتور عماد عبيد	عضواً	.....

الإهــداء

إلى من كان رضاها سر نجـ احي وتوفيقي، وكان دعاؤها نوراً يضيء دربي ويؤنسني، إلى من سهرت الليالي لأنام، واسترسلت في دعائها كي لا أضام.

إلى والدتـي الغالية أطال الله في عمرها، وألبسها ثوب الصحة والعافية وأسعدها...

إلى رمز العزة والفخر، إلى القدوة الحسنة والمثل الأعلى الذي علمني المثابرة والعمل الدؤوب

والــدي العزيز أطال الله في عمره، وأدام عزه...

إلى من وقفت إلى جانبي وكانت مصدر إلهامي، رفيقة دربي ومفتاح قلبي لإخلاصها وتفانيها في العطاء بغير ملل، إلى من تحملت معي العبء والسهر والمشقة...

زوجتـي الغالية...حفظها الله ورعاها

إلى أختي الغاليه... وفقها الله وحماها، وأنار دربها بنوره الذي لا ينطفئ...

إلى اخواني ألأعزاء... أحاطهم الله بموفور الصحة والعافية

إلى أبنائـي، شموع دربي،،، ديانا... ليث... ليزا... فرح... عبود...

حماهم الله ...وأحاطهم برعايته

لهم جميعاً أهدي ثمرة هذا الجهد المتواضع

الباحث

شكر وتقدير

الحمد لله رب العالمين والصلاة والسلام على سيدنا محمد خاتم الأنبياء والمرسلين.

فبعد أن أكرمني الله بجزيل فضله وعظيم كرمه بإنهاء رسالتي العلمية فإن واجب الوفاء والعرفان بالجميل يقتضي أن أتقدم بعظيم الشكر وخالص التقدير لأستاذتي الفاضلة الدكتورة رنا إبراهيم العطور على تفضلها بقبول الإشراف على هذه الرسالة. وأدين لها بكل الإجلال والإحترام والتقدير على جهدها المتواصل في تقديم النصح والإرشاد والتوجيه، والتي لم تبخل عليّ يوماً بوقتها أو ثمرة علمها، وكانت لي خير المرشد والمعين الأمين على إنجاز هذا البحث وإظهاره في الصورة التي هو عليها، فلها مني جزيل الشكر والعرفان سائلاً المولى عز وجل أن ينعم عليها بدوام الصحة والعافية.

كما وأتقدم بالشكر والعرفان للأساتذة الأجلاء أعضاء لجنة المناقشة، الذين تفضلوا بقبول مناقشة هذه الأطروحة، متحملين عبء قراءتها بالرغم من ضيق الوقت وثقل الأعباء، وأثروا هذه الأطروحة بملاحظاتهم القيمة.

كما وأتقدم بالشكر والعرفان إلى جامعة عمان العربية بجميع كوادرها الأكاديمية والإدارية، لما قدموه لي طيلة فترة دراستي في الجامعه من عون ومساعدة، وأخص بالذكر أستاذي الفاضل الأستاذ الدكتور محمد سليم الغزوي عميد كلية القانون في الجامعة والذي أفاض علي من علمه وأحاطني برعايته.

وأخيراً أتقدم بالشكر والعرفان لكل من وقف إلى جانبي، وأعانني على إتمام هذه الدراسة، والله ولي التوفيق، هو نعم المولى ونعم النصير.

الباحث

فهرس المحتويات

الملخص باللغة العربية

مدى الحماية الجنائية للمعلومات المعالجة آلياً عبر الحاسوب والإنترنت

دراسة مقارنة

إعداد

منذر عبد الرزاق مصلح العمايرة

إشراف

الدكتورة رنا إبراهيم العطور

تناولت هذه الدراسة مدى الحماية الجنائية للمعلومات المعالجة آلياً والمخزنة في الحاسب الآلي أو المتداولة في طور التدفق أو الانتقال عبر شبكة الإنترنت من خطر الإجرام المعلوماتي الذي يرتكب بالوسائل التقنية والذي يطال المعلومات بالإعتداء، وذلك بهدف تحديد مدى كفاية التشريعات الأردنية لمعالجة الجرائم المستحدثة وحماية المعلومات المعالجة آلياً والتي هي دائماً محل هذه الجرائم، ولتحديد مدى الحاجة إلى نصوص قانونية خاصة لمعالجة هذا الموضوع، فالتطور التكنولوجي المعلوماتي ألقى مسؤولية كبيرة على عاتق المشرع الجنائي لمواجهة الجرائم المعلوماتية الناشئة عن استخدام الأنظمة المعلوماتية، وخاصةً في ظل قصور نصوص قوانين العقوبات التقليدية عن الإحاطة بهذه الجرائم، وسبب ذلك أن قواعد حماية الأموال من مخاطر الجريمة بوجه عام تأسست على حماية المال المادي المحسوس أي المال ذي الوجود المادي، وكذلك التعامل مع محل الجريمة الملموس ذي الطبيعة المادية، والتعامل مع سلوك جرمي ينتمي إلى عالم السلوكات المادية، الأمر الذي يتعذر معه حماية القيم غير المادية المتولدة عن المعلوماتية والمتمثلة في المعلومات المعالجة آلياً.

وقد تناول الباحث موضوع هذه الدراسة من خلال خمسة فصول، حيث خصص الفصل الأول منها للمقدمة ومشكلة الدراسة المتمثلة في تطوير التشريعات الخاصة في الحماية الجنائية للمعلومات في الجرائم التي ترتكب عبر شبكة الحاسوب والإنترنت، وبيان مدى كفاية القواعد القانونية الموضوعية في توفيرها، انطلاقاً من التشريعات الأردنية ومن ثم بعض التشريعات الأجنبية، وبين فيما بعد عناصر هذه المشكلة وأهمية الدراسة ومصطلحاتها وأهدافها، وأيضاً محددات هذه الدراسة والتي تقتصر على المقارنة بين القانون الأردني وقانون الولايات المتحدة الأمريكية بصورة أساسية

من حيث مدى الحماية التي وفرها كلٌ منهما للمعلومات المعالجة آلياً، مع الإشارة إلى موقف بعض التشريعات المقارنة الأخرى في بعض الأحيان، كما وبين الباحث أيضاً أن هذه الدراسة تقتصر على تناول موضوع الحماية الجنائية للمعلومات المعالجة آلياً والمخزنة في الحاسب الآلي أو المتدفقة عبر شبكة الإنترنت، والتي لا تنتمي إلى أي من المواد الأدبية أو الذهنية ولا تندرج حتماً في مجموعة القيم المحمية بموجب قوانين الملكية الفكرية، وقد انتهج الباحث خلال هذه الدراسة المنهج الوصفي والتحليلي والمقارن مع بيان ما سبق من دراسات قانونية لها صلة بموضوع هذه الدراسة.

أما الفصل الثاني فقد تناول الباحث فيه نبذة عن الجوانب التقنية والفنية للنظام المعلوماتي، ومن ثم مدلول المعلومات الإلكترونية والتمييز بينها وبين البيانات والبرامج، وشروطها وطبيعتها القانونية وأنواعها، حيث تبين أن هذه المعلومات ذات طبيعة خاصة معنوية بعيدة كل البعد عن الطبيعة المادية للأموال المحمية بموجب قوانين العقوبات التقليدية، ثم تناول الباحث تعريف الجريمة المعلوماتية والسمات الخاصة بها، ووجد بأنها جرائم عابرة للحدود ويصعب إكتشافها وإثباتها، كما وانها تتم بأسلوب لا يتسم بالعنف وتتم عادة بتعاون أكثر من شخص، ثم بحث بعد ذلك في محل هذه الجرائم وبين أنها دائماً تقع على المعلومات بمفهومها الواسع وهي المعطيات المعنوية للحاسوب، ومن ثم مخاطر هذه الجرائم وأركانها، حيث بين الباحث أن ركنها المادي يتمثل في ممارسة نشاط تقني رقمي محدد وهو استخدام الحاسوب والإنترنت، فهذه الجرائم ليست من جرائم الوسيلة، وإنما يدخل الحاسوب والإنترنت في النشاط الجرمي المكون لها.

وتعرض الباحث بعد ذلك إلى المجرم المعلوماتي، وبين سماته الشخصية وطوائفه ودوافعه وفئاته التي أبرزها على أساس معيار درجة الخطورة للفاعل.

وفي نهاية الفصل الثاني بين الباحث جهود المجتمع الدولي لمواجهة جرائم الحاسوب والإنترنت، ءمن خلال إلقاء الضوء على دور الأمم المتحدة على النطاق الدولي، ومن ثم دور المجلس الأوروبي، والذي أدى إلى خروج معاهدة بودابست لمكافحة جرائم الحاسوب لعام 2001 إلى حيز الوجود، ومن ثم بين الباحث الجهود العربية لمواجهة هذه الجرائم، والتي أثمرت عن صدور القانون العربي النموذجي والخاص بمكافحة جرائم الحاسب الآلي والإنترنت، والذي يعتبر قاعدة الأساس لخطوات تعاون مستقبلية على الصعيد العربي.

أما الفصل الثالث فقد تناول الباحث فيه الحماية الجنائية للمعلومات المعالجة آلياً وذلك في إطار نصوص جرائم الأموال، حيث تطرق تحديداً إلى جريمة سرقة المعلومات المعالجة آلياً، وجريمة إتلاف المعلومات المعالجة آلياً، وجريمة إعاقة عمل النظام المعلوماتي نظراً لتداخلها مع جريمة الإتلاف، وجريمة الاحتيال المعلوماتي، وبين صور هذه الجرائم ومحلها وهو الحق في المعلومات المعالجة آلياً، والوسائل التقنية المستخدمة في ارتكاب هذه الجرائم والمختلفة عن الأساليب التقليدية، وتوصل الباحث إلى نتيجة مؤداها أن نصوص قانون العقوبات الأردني قاصرة عن إحاطة محل هذه الجرائم، با لحماية الجنائية، وبين أيضاً موقف المشرعين الأردني والأمريكي والفرنسي- من هذه الجرائم وذلك من خلال الدراسة التحليلية لكافة النصوص والقواعد القانونية المتعلقة بهذه الجرائم.

أما الفصل الرابع فتناول الباحث فيه الحماية الجنائية للمعلومات من الجرائم التقنية المستحدثة في إطار المعالجة الآلية للبيانات، وتطرق إلى الجرائم الماسة بسرية المعلومات والبيانات المعالجة آلياً من ناحية، والتي منها جريمة الدخول غير المصرح به إلى النظام المعلوماتي، وجريمة البقاء غير المصرح به في النظام المعلوماتي، وجريمة الاعتراض غير القانوني لانتقال البيانات، ومن ناحية أخرى تطرق الباحث إلى الجرائم الماسة بسلامة المعلومات والبيانات المعالجة آلياً، والتي منها جريمة التزوير المعلوماتي، ومن ثمً تناول الباحث الجرائم الماسة بالمصالح القومية للدول والسلامة الشخصية للأفراد، والتي منها جريمة التجسس المعلوماتي وجريمة الاعتداء على الحياة الخاصة للأفراد (انتهاك الخصوصية)، وبين موقف المشرع الأردني والأمريكي والفرنسي- من كافة الجرائم سالفة الذكر، حيث وجد أن قانون العقوبات الأردني يخلو من أي نص يجرم أو يشير إلى فعل الدخول والبقاء غير المصرح بهما داخل النظام المعلوماتي، وفعل الاعتراض غير ال قانوني لانتقال البيانات والمعلومات المعالجة آلياً، أما باقي الجرائم فوجد الباحث أنه من الصعوبة بمكان أن تشملها النصوص التقليدية في قانون العقوبات الأردني، ومن خلال البحث في قانون جرائم أنظمة المعلومات الأردني المؤقت وجد الباحث أنه وفر جانباً من الحماية الجنائية للمعلومات المعالجة آلياً، إلا أن هذه الحماية لم تحط كافة أنواع المعلومات المعالجة آلياً والتي قد تجسد أو تمثل أموالاً أو أصولاً أو أسراراً أو بيانات شخصية أو لها قيمة بذاتها، ولم يستوعب كافة صور الجرائم المعلوماتية ، وأخيراً تناول الباحث في هذا الفصل موضوع الاشتراك الجرمي والعقوبات والمسؤولية الجزائية للأشخاص المعنوية.

أما الفصـل الخامس من هذه الدراسة فقد تناول الباحث فيه النتائج التي توصل إليها، والتوصيات، وتمنى على المشرع الأردني الأخذ بها في محاولة لتطوير التشريعات الجنائية الأردنية لمواكبة التطور الهائل في مجال تكنولوجيا المعلومات وجرائمها، وبين أخيراً في هذا الفصـل المراجع التي سـاهمت في مسـاندته وأنارت طريقه لإجراء هذه الدراسة المتواضعة.

Abstract

The Degree of Criminal Protection Of Information that is Technically Processed via Computer and the Internet: Acomparative Study

Prepared by

Monther Abd Al-Razaq Mesleh Al-Amaireh

Supervised by

Dr. Rana Ibrahim Al-Otoor

This study tackled the Degree of Criminal Protection of data, which is technically processed and stored in the computer or which circulated at the moving stage through the Internet, from data crimes risk committed by technical means which cause data offensive, the aim is to determine the adequacy of Jordanian legislation in treating the developed crimes and protect technically processed information which always replace these crimes, and to determine the need to special legal texts to treat this topic, specially under the inadequate texts of usual penalties related to these crimes. Such legal texts have been issued on the basis of protecting the sensible physical capital of physical nature, and dealing with criminal behavior which belongs to physical behaviors world. These legal acts could not protect the non-material values generated and presented in technically processed information.

The researcher tackled this study in five chapters. The first chapter consists the introduction and the study problem represented by developing the legislations concerning criminal protection for information committed via the computer and the internet, it also reports the adequacy of these legislations.

The researcher has also reviewed the elements of the problem and the importance of the study and its terms and aims, it also viewed the study determinants which restricted on comparing Jordan law and United States of America and some comparative legislations at some times.

The second chapter deals with a scrap about the technical and professional information system and then the electronic information, its denotations and legal nature. It was found that that the electronic data has aspecial significant nature different from the physical nature of protective capital under the provision of traditional penalty. The researcher also tackled the definition of cyber-crime, its characteristics and the information offender. At the end of this chapter, the researcher viewed the international community efforts in compacting the crimes of computer and internet.

In the third chapter, the researcher tackled the criminal protection for technically processed information in terms of the texts restricted for money crimes. Then, the researcher explored briefly theft, destruction and hindering information system work crime for its interfering with information destruction crime then fraud information crime. The researcher viewed that traditional penalty law cannot protect the cyber crimes by criminal protection.

The fourth chapter is about criminal protection of information from developed technical crimes in the frame of electronic processing for data and the researcher examined the crimes which affect information privacy such as login and unauthorized staying at the information system. The researcher also discussed the crimes that affect the safety of information and data which was technically processed such as fraud then about the national interests of the states and the personal safety for individuals (breach of privacy).

As for the fifth chapter, the researcher discussed the findings and investigations he found; he wishes that the Jordanian legislator will take these findings into account in attempt to develop the Jordanian criminal legitimates to keep pace with tremendous development in information technology and its crimes. In the last chapter, the researcher viewed the references which contributed to support and light his way to do this study.

الفصل الأول -

الإطار النظري والدراسات السابقة:

أولاً: المقدمة

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة سميت بالثورة المعلوماتية إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن، فقد أمست هذه المعلومات قوة لا يستهان بها في أيدي الدول والأفراد، وكان التطور الهائل الذي شهده قطاعا تكنولوجيا المعلومات والاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه هذه الثورة، ومما لا شك فيه أن الثورة المعلوماتية نتيجة للتقنيات العالية التي تقوم عليها والتي تتمثل في استخدام الحواسيب والشبكات المعلوماتية التي تربط بينها قد تركت أثاراً إيجابية، وشكلت قفزة حضارية نوعية في حياة الأفراد والدول. وجعلت القطاعات المختلفة في الوقت الراهن تعتمد في أداء عملها وبشكل أساسي على استخدام الأنظمة المعلوماتية نظراً لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها ومن ثم نقلها وتبادلها بين الأفراد والجهات والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول (المومني، 2008، 13).

وقد ترتب على ثورة المعلومات والاتصالات التي يحياها العالم الآن أن ظهرت أنماط من السلوك تشكل جرائم أو أفعالاً مخالفة ترتب المسؤولية الجزائية، إلا أن النصوص القانونية السارية عجزت عن أن تمد مظلتها إلى هذه الجرائم أو المخالفات كي تطالعها، وهو ما حدا بالمشرع إلى التدخل، وسن تشريعات تحكم الجريمة في ثوبها الجديد الذي يطلق عليه الجريمة المعلوماتية أو الجريمة بطريقة الكمبيوتر أو الإنترنت. وقد حدث هذا في معظم بلدان العالم المتقدم التي بادرت إلى وضع تشريعات تحكم أنظمة استخدام الحاسب الآلي وكذلك المعاملات عبر الانترنت، ومع ذلك فإن هذه التشريعات لن تتمكن أن تجاري هذه التقنيات، فالجريمة عبر شبكة الحاسوب والانترنت تسبق التشريعات التي تحكمها بمسافات طويلة، ولذلك لا عجب فيما يراه البعض من أن الآثار الاقتصادية والاجتماعية لثورة المعلوماتية في الوقت الحالي- تفوق الآثار الناتجة عن الثورة الصناعية (حجازي، 2009، 1).

وتأخذ الجريمة المعلوماتية صوراً متعددة تندرج تحتها جرائم غش الحاسب الآلي عن طريق اختراقه وسرقة المعلومات المخزنة فيه أو إتلافها وتدميرها، إلى جرائم أشد خطورة مثل التزوير المعلوماتي، وكذلك سرقة الأموال عن طريق الوسائط الإلكترونية، وأيضاً الجرائم الماسة بالعرض وجرائم الاتجار بالبشر، وغيرها من أصناف الجرائم المستحدثة التي يمكن اقترافها عن طريق هذه الوسائل المعلوماتية الحديثة (حجازي 2006، 10).

إن ظهور الإنترنت واستخدامه والاعتماد عليه بشكل مطلق، أدى إلى تغيير في شخصية ومواصفات مرتكب الجريمة، وبصفة خاصة جرائم الانترنت، فإن كانت جرائم الكمبيوتر في الماضي ترتكب من أشخاص على قدر كبير من الذكاء والحنكة، كالمبرمج والمستخدم المؤهل، فإن تطور نطاق استخدام الحاسب الآلي الشخصي وسهولة التعامل مع الانترنت أدى إلى التوسع في حجم ونطاق المتعاملين مع الحاسب الآلي، وبالتالي أدى إلى صعوبة الغوص في شخصية الجاني ومواصفاته، لكثرة مستخدمي هذه الشبكات وبشكل قد يعادل أو يفوق قدرة المبرمج أو المستخدم المؤهل في استخدام هذه الشبكات.

وقد أدى ظهور الإنسان المعلوماتي، وتكون المجتمع الإلكتروني، إلى تزايد انتهاك الحقوق الأساسية والحريات الفردية للأفراد التي كفلتها القوانين الدستورية، مما يدل على ارتباط الموضوع بالقانون الدستوري وارتباطه أيضاً بالقانون الإداري، خاصة مع ظهور ونمو الحكومات الإلكترونية، وأيضاً فإن ظهور العقود الإلكترونية، وإتمام عملية البيع والشراء عن بعد، تظهر ارتباط الموضوع بالقانون المدني، وبفروع القانون الخاص الداخلي والدولي، ولا سيما بظهور التحكيم عن بعد أو التحكيم الإلكتروني (الشوابكة، 2004، 11-12).

وقد أدى التزايد في عدد المجرمين الذين يعرفون كيفية التعامل مع الحاسبات الآلية وتقنياتها، إلى وضع هذا الاتجاه الإجرامي المتصاعد ، في موقع متقدم من اهتمام أجهزة العدالة الجنائية لضمان تنفيذ القوانين.

لذا بات من الضروري مواجهة هذا التيار الإجرامي المستحدث بمختلف الأساليب، سواء التشريعية، من خلال إقرار تشريع جديد ينص على عقوبة مرتكب تلك الجرائم، أم الفنية والأمنية من خلال وجود كوادر أمنية عالية التخصص في استخدام تكنولوجيا المعلومات (سليمان، لات، ب).

ومع التطور السريع الذي يمتاز به هذا النوع من الجرائم ، فقد برز الكثير من أوجه القصور الجزائي، سواء لجهة التجريم أم لجهة البحث والتحقيق، مما يتطلب مواكبة ذلك، والحقيقة أن المملكة الأردنية الهاشمية لم تكن بمعزل عن ثورة المعلومات وتداعياتها وآثارها الإيجابية والسلبية، إذ سارعت إلى تعديل تشريعاتها وأجهزتها الأمنية والقضائية المعنية بمكافحة جرائم الكمبيوتر والانترنت.

واعتمد المشرع الأردني سابقاً على قانون العقوبات الأردني التقليدي في معالجة بعض صور هذه الجرائم، وفي بعضها الآخر اعتمد على القوانين الخاصة ومنها: قانون الاتصالات الأردني رقم (13) لسنة 1995، وقانون حماية حق المؤلف رقم (22) لسنة 1992 (قانون الملكية الفكرية)، وقانون براءة الاختراع، وقانون المعاملات الإلكترونية المؤقت رقم 15 لسنة 2001، وقد حاول المشرع الأردني مواكبة التطور المعلوماتي الحاصل في العالم، والوقوف للحد من هذه الجرائم عابرة الحدود، والتي أصبحت تشكل خطورة كبيرة على أمن الأفراد وحرياتهم الشخصية وأيضاً أمن الدولة، ومع كل ذلك فإن هذه الجرائم من التطور السريع بحيث تجعل من الصعوبة على المشرع مواكبتها والسير جنباً إلى جنب مع تطورها، ومن هنا نجد أن الحكومة الأردنية قد أصدرت القانون المؤقت لجرائم أنظمة المعلومات لسنة 2010 في محاولة منها للإحاطة بهذه الجرائم وحماية أنظمة المعلومات، ولذلك تأتي هذه الدراسة لتحديد المقصود بجرائم أنظمة المعلومات، وتحديد عناصرها وخصائصها وطبيعتها القانونية، وبيان مدى الحماية الجنائية للمعلومات الإلكترونية في التشريعات الأردنية، ومدى كفاية النصوص الجنائية الحالية لمواجهة الجرائم المرتكبة عبر شبكة الإنترنت، وذلك من خلال البحث في القواعد الموضوعية دون الإجرائية، وفي حال عدم معالجة حالات معينة من هذه الجرائم هل يتم الرجوع إلى القواعد التقليدية العامة أم البحث في قوانين خاصة أخرى، ومد ى كفاية القواعد الموضوعية لذلك، خاصةً مع وجود عقبات تحول دون تطبيق النصوص الجزائية التقليدية على مثل هذا النوع من الجرائم، فابتداءً وجدت نصوص قانون العقوبات لحماية الأموال المادية ذات الكيان المادي الملموس، ولم تأتِ لحماية الأموال أو الأشياء المعنوية كالمعلومات، كما وأن مبدأ شرعية الجرائم والعقوبات يُعد عقبة أخرى حول إمكانية إدراج جرائم أنظمة المعلومات ضمن النصوص التقليدية في قانون العقوب ات الأردني، وتبحث هذه الدراسة أيضاً في مدى كفاية النصوص الجزائية الموضوعية في تحقيق غايتها، والمتمثلة في الحيلولة دون وقوع هذه الجرائم، أو الحد من ارتكابها وفي نفس الوقت ردع مرتكبيها، وهل جاءت كافيه وتفي بهذا الغرض أم أنها بحاجة إلى تعديل بما يتلاءم مع التطور التقني السريع لجرائم أنظمة المعلومات.

وإيماناً من الباحث بأهمية هذا الموضوع والذي ينطوي على خطورة كبيرة تمس الأفراد والدول معاً، فقد قرر بعد الاتكال على الله سبحانه وتعالى دراسته والبحث فيه، خاصة وأن هذا النمط من الجرائم المستحدثة قد غزا مجتمعات العالم بأكمله، على الرغم من الصعوبات التي قد تواجه الباحث والتي من أهمها أنه ليس من المختصين في مجال الحاسوب والإنترنت، كما وأن قلة وندرة التطبيقات القضائية ، وإجراءات التحقيق الابتدائي أمام الإدعاء العام والتحقيق الأولي أمام الضابطة العدلية يعتبر من أهم الصعوبات في هذا المجال ، داعياً الله تعالى أن تتحقق الفائدة من خلال هذه الدراسة، وحسبي في هذا أني قد اجتهدت وما توفيقي إلا بالله تعالى.

ثانياً: مشكلة الدراسة

تكمن مشكلة هذه الدراسة حول مدى الحماية الجنائية للمعلومات في الجرائم التي ترتكب عبر شبكة الحاسوب والإنترنت في التشريعات الأردنية، وبيان مدى كفاية القواعد القانونية الموضوعية في توفيرها، من خلال البحث في القوانين الخاصه بذلك والتي من أهمها – في هذا المجال- قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010، ومقارنة ذلك بالتشريعات الأجنبية.

ثالثاً: عناصر مشكلة الدراسة

تحاول هذه الدراسة الإجابة عن السؤال الرئيس التالي:

ما مدى الحماية الجنائية للمعلومات في الجرائم التي ترتكب عبر شبكة الحاسوب والانترنت في التشريعات الأردنية؟

ومن هذا السؤال تتفرع الأسئلة التالية:

1- ما المقصود بالجرائم المعلوماتية والسمات التي تتميز بها، ومدى خطورتها وأنماطها؟
2- ما هي صور الجرائم المعلوماتية ؟
3- ما هي جرائم أنظمة المعلومات التي وردت في القانون المؤقت الجديد لسنة 2010م؟
4- ما الدواعي التي تستوجب الحماية الجنائية للمعلومات من الجرائم التي قد تقع عليها؟
5- ما موقف المشرع الأردني من الحماية الجنائية للمعلومات عبر شبكة الحاسوب والانترنت؟

رابعاً: أهمية الدراسة

تتمثل أهمية الدراسة فيما يأتي:

1- تظهر أهمية الدراسة من خلال ارتباط معظم المصالح الفردية والعامة في الدول بنظم المعلومات والحاسبات الآلية وشبكة الإنترنت، للدرجة التي أصبح فيها النشاط الإنساني في وقتنا الراهن يعتمد بصورة أساسية على الحاسب الآلي في كافة معاملاته واستخداماته، الأمر الذي أدى إلى نشوء جرائم لم تكن مألوفة من قبل وهي الجرائم المرتكبة عبر شبكة الحاسوب والإنترنت.

2- إن التزايد في معدلات ارتكاب هذه الجرائم يرتبط بمدى التقدم في المجال المعلوماتي، وإدراك تأثيره في مصالح المجتمع، سواء من الناحية الأمنية أو الاقتصادية أو الثقافية.

3- كثر ارتكاب مثل هذه الجرائم، وتنوعت أساليبها، وتعددت اتجاهاتها، وزادت خسائرها، حتى أصبحت من مصادر التهديد البالغة للأمن القومي للدول، خاصة إذا تركت هذه الجرائم دون تدخل المشرع الوطني بإحاطة المعلومات وأنظمتها بحماية جنائية كافية، من خلال القوانين الخاصة التي تضم قواعد جامعة مانعه تحيط بكافة أساليب الحماية للمعلومات عبر شبكة الحاسوب والإنترنت.

4- كما وأن الحياة الخاصة للأفراد أضحت تعتمد في الكثير من مظاهرها على تقنية المعلومات المستحدثة، الأمر الذي أدى إلى تعرضها إلى انتهاكات خطيرة ، من الصعب السيطرة والإحاطة بها، ولذلك أتت هذه الدراسة لتوضح ماهية المعلومات الجديرة بالحماية الجنائية، وكيفية انتهاكها، وصور ارتكاب جرائمها، وتنوع أساليبها، وتعدد اتجاهاتها، وزيادة خسائره وأخطارها على الأفراد والمجتمعات والدول.

5- إن الدراسات ا لموجودة حالياً غير كافية، ولا تغطي كافة جوانب الموضوع، وإن وجدت فقد نظمت هذه الدراسات الجرائم المعلوماتية من حيث طبيعتها وسماتها، وكيفية ارتباطها وأساليبها، ولم تتطرق إلى الحماية الجنائية لأنظمة المعلومات في التشريعات الأردنية، وكان جل ارتكازها على القواعد التقليدية في قانون العقوبات الأردني ، أو على أحد القوانين الخاصة المساعدة في هذا الموضوع، كقانون الاتصالات، أو قانون الملكية الفكرية، أو قانون المعاملات الإلكترونية، أو قانون براءة الاختراع وغيرها. وذلك لعدم وجود تشريع خاص بالجرائم المعلوماتية، كالذي صدر عن المشرع الأردني عام 2010، وهو قانون جرائم أنظمة المعلومات المؤقت لسنة 2010.

6- إن هذه الدراسة تشكل إضافة أساسية حقيقية في موضوع الحماية الجنائية للمعلومات عبر شبكة الحاسوب والإنترنت في التشريعات الأردنية، من خلال تحليل كافة مواد القانون المؤقت الجديد، والقواعد التقليدية، والقوانين الخاصة الأخرى، وتحديد مدى الحماية التي وفرها المشرع الأردني لمثل هذا النوع من الجرائم الخطيرة في ظل تعدد التشريعات.

خامساً: التعريف بمصطلحات الدراسة

فيما يأتي عرض للتعريفات المفاهيمية والإجرائية للمصطلحات التي تتضمنها الدراسة، لتحقيق التوافق بين الباحث والقارئ، ولتجنب التكرار في توضيح المصطلحات، ولتدل أينما وردت في هذه الدراسة على المعاني المبينة إزائها :

1- **الحماية الجنائية**: وجود نصوص جزائية وقواعد عامة شكلية وموضوعية، تلزم الأفراد بالمحافظة على المصالح التي يحميها القانون، مع عدم الاعتداء عليها، وترتيب عقوبة جزائية أو تدابير إحترازية على من يخرق تلك القواعد، وذلك إنفاذاً لمبدأ الشرعية بأن لا جريمة ولا عقوبة ولا إجراء ولا تدبير إلا بنص.

2- **الحاسوب**: عبارة عن جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما، وذلك بتنفيذ ثلاث عمليات أساسية هي: استقبال البيانات المدخلة، ومعالجة البيانات إلى معلومات، وإظهار المعلومات المخرجة.

3- **الإنترنت**: هي كلمة إنجليزية مركبة مختصرة ومكونة من مقطعين (Inter) وهي اختصار للكلمة الإنجليزية (International) وتعني دولي و(Net) وهي اختصار لكلمة (Network) وتعني شبكة، والإنترنت هي الشبكة العالمية للمعلومات.

4- **الجرائم المعلوماتية**: وهي الجرائم التي يتم ارتكابها بواسطة نشاط تقني رقمي غير مشروع، يتمكن الفاعل من خلاله الاتصال بالحاسوب والإنترنت، وذلك من خلال تحويل كل فكرة أو مادة تقبل بطبيعتها التحول إلى مجموعة كبيرة من أرقام (0-1) (لغة الحاسوب)، ويؤدي إلى الاعتداء على مصلحة يحميها القانون، وهذه الجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

5- **المعلومات الإلكترونية**: هي البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك.

6- **البرامج الإلكترونية**: مجموعة من الأوامر والتعليمات المهيأة مسبقاً بشكل منسجم ومتناسق لتنفيذ وظيفة محددة عند استخدام أجهزة الحاسب الآلي.

سادساً: أهداف الدراسة

تهدف هذه الدراسة إلى ما يأتي:

1- بيان مدى خطورة ارتكاب جرائم أنظمة المعلومات، والتي تقع على المعلومات تحديداً بكافة صورها، عن طريق السرقة، أو الاستعمال غير المصرح به للنظام المعلوماتي، أو الإتلاف، أو التزوير، أو الدخول غير المصرح إلى النظام المعلوماتي، أو الاحتيال المعلوماتي، أو التجسس المعلوماتي، وغيرها من صور هذه الجريمة.

2- استعراض وتحديد موقف المشرع الأردني حول ذلك، من خلال القواعد الموضوعية، ومنهجه في حماية هذه المعلومات من الانتهاك عبر شبكة الانترنت، وتقييم هذا المنهج، وتقديم التوصيات اللازمة استناداً إلى النتائج التي تم التوصل إليها.

3- عرض الوسائل المختلفة لمواجهة مثل هذا النوع من الجرائم الخطيرة، سواء من الناحية التشريعية، أو من الناحية الأمنية، والوسائل الأخرى الكفيلة بإنجاح تلك المواجهة، وتوفير الحماية الجنائية اللازمة للمعلومات عبر شبكة الحاسوب والانترنت.

سابعاً: محددات الدراسة

تقتصر هذه الدراسة على البحث في القواعد الموضوعية دون الإجرائية من خلال المقارنة بين القانون الأردني والقانون الأمريكي بصورة أساسية، من حيث مدى الحماية الجنائية التي وفرها كل منهما للمعلومات عبر شبكة الحاسوب والإنترنت، ودون إغفال الإشارة في بعض الأحيان إلى التشريعات الأخرى المقارنة كالتشريع الفرنسي، كما وأن هذه الدراسة تقتصر على تناول موضوع الحماية الجنائية للمعلومات عبر شبكة الحاسوب والإنترنت، وفق مفهوم الجرائم الواقعة على المعلومات عبر هذه الشبكة، والتي تتعلق بالنشاط الإجرامي الذي يؤدي فيه نظام الحاسب الآلي دوراً هاماً لإتمامه، سواء أكان الحاسب الآلي أداة لإتمام النشاط الإجرامي أم كان محلاً له. وبالتالي تخرج عن نطاق هذه الدراسة بقية المعلومات غير المتعلقة بشبكة الحاسوب والإنترنت، كالمعلومات الورقية مثلاً.

وتـ خرج عن نطاق هذه الدراسة أيضاً المعلومات المتمثلة في المصنفات المبتكرة في الآداب والفنون والعلوم سواء الورقية أو المتمثلة في برامج حاسوب والمحمية بموجب قوانين الملكية الفكرية، وأيضاً تخرج عن نطاق هذه الدراسة بقية الموضوعات الأخرى المتعلقة بجرائم شبكة الحاسوب والإنترنت والتي لا تتعلق بأنظمة المعلومات، إلا بالقدر الضروري بما هو متعلق ومتصل بموضوع هذه الدراسة، وذلك بتسليط الضوء على العموميات دون الدخول في الجزئيات، وذلك لوضع الحلول القانونية المتعلقة بالقواعد الموضوعية.

ويقتصر موضوع هذه الدراسة أيضاً على الحماية الجنائية للمعلومات عبر شبكة الحاسوب والانترنت، وبالتالي تخرج عن نطاق هذه الدراسة الحماية المدنية لمثل هذا النوع من المعلومات.

ثامناً: منهج الدراسة

سيتبع الباحث بشكل أساسي المناهج التالية:

1- **المنهج الوصفي**: وذلك من خلال وصف الجرائم الواقعة على المعلومات عبر شبكة الحاسوب والإنترنت، وما قيل فيها من آراء فقهية ونظريات، مع أنها قليلة، وجمع الحقائق والبيانات عن حدوثها، وحصر العوامل المختلفة والمؤثرة فيها، كذلك وصف مفهوم أنظمة المعلومات الإلكترونية، وما يتعلق بحمايتها من خلال الحماية الجنائية لهذه المعلومات ، ومن خلال وصف موقف التشريعات من ذلك.

2- **المنهج التحليلي**: سيقوم الباحث بتحليل وتفسير النصوص والقواعد القانونية المتعلقة بأنظمة المعلومات عبر شبكة الإنترنت، ونصوص التشريعات ذات الصلة، لمعرفة أثرها في توفير الحماية الجنائية لهذه المعلومات.

3- **المنهج المقارن**: ويقوم هذا المنهج على المقارنة بين القانون الأردني والقانون الأمريكي، حول موضوع الدراسة، مع التعرض إلى التشريعات الأخرى في الحدود التي تخدم أهداف هذه الدراسة.

تاسعاً: الدراسات السابقة ذات الصلة

وجد الباحث بعض الدراسات التي تطرقت إلى بعض الجوانب والموضوعات التي سيتعرض لها الباحث في أطروحته على النحو الآتي:

1- المومني (2008)، الجرائم المعلوماتية:

هذه الدراسة رسالة ماجستير في القانون العام، نوقشت في الجامعة الأردنية، الأردن، وقد أشرفت عليها دكتورة وفقيهة القانون الجنائي رنا العطور، وقد تناولت هذه الدراسة الجانب الفني والتقني لجهاز الحاسوب والإنترنت، وماهية الجريمة المعلوماتية وسماتها العامة،

وأضرارها على الاقتصاد الوطني، والسمات الخاصة بالمجرم المعلوماتي والأسباب الدافعة إلى ارتكاب مثل هذه الجرائم، ثم تعرضت إلى صور الجرائم المعلوماتية الواقعة على النظام المعلوماتي والجرائم المعلوماتية الواقعة بواسطته، وكان محور هذه الدراسة الأساسي هو البحث فيما إذا كانت النصوص التقليدية في قانون العقوبات الأردني يمكن أن تمتد لتشمل في إطارها الجرائم المعلوماتية المستحدثة، واعتمدت هذه الدراسة على تحليل النصوص الجزائية الواردة في قانون العقوبات الأردني، وذلك لمعرفة مدى انطباقها على الجرائم المعلوماتية، وقد توصلت الباحثة إلى أن هناك عقبات تحول دون تطبيق هذه النصوص التقليدية على الجرائم المعلوماتية، ومنها أن نصوص قانون العقوبات وضعت ابتداءَ لحماية الأموال المادية ذات الكيان المادي الملموس، ولم توضع لحماية الأموال المعنوية كالمعلومات، حيث إن فكرة المال المعلوماتي لم تكن قد تبلورت لدى المشرع حين سن هذا القانون، وذلك لعدم اعتماد المجتمع على تكنولوجيا المعلومات في ذلك الوقت، أما هذه الدراسة فستقوم بتحليل ودراسة موقف المشرع الأردني من خلال قانون العقوبات التقليدي والقوانين الخاصة ، بما فيها قانون جرائم أنظمة المعلومات المؤقت لسنة 2010، في وقت يبدو فيه أن المشرع الأردني قد أدرك فكرة المال المعلوماتي، وبالتالي سوف يبين الباحث مدى كفاية التشريعات الأردنية في توفير الحماية الجنائية لأنظمة المعلومات عبر شبكة الحاسوب والإنترنت، من خلال النصوص التشريعية التي جاء بها المشرع الأردني لملاحقة التطور السريع لهذه الجرائم والسير خطوة بخطوة معها للإحاطة بكافة صور هذه الجرائم الخاصة بالمعلومات، وبالتالي فإن هذه الدراسة سوف تأتي بالجديد كقاعدة لدراسات مستقبلية.

2- **الشوابكة (2004)، جرائم الحاسوب والانترنت (الجريمة المعلوماتية):**

وقد تناول هذا المرجع مختلف جرائم الاعتداء الواقعة على الأشخاص عبر الإنترنت، مثل جرائم الذم والقدح والتحقير، وجرائم الاعتداء على حرمة الحياة الخاصة عبر الإنترنت، وجرائم الاستغلال الجنسي للأطفال، وتناول أيضاً جرائم الاعتداء على الأموال عبر الإنترنت، مثل سرقة المال المعلوماتي المعنوي، والتمويل الالكتروني غير المشروع للأموال، وجريمة إتلاف نظم المعلومات عبر الإنترنت.

وقد أنصب موضوع هذه الدراسة على فكرتين أساسيتين: تتعلق الأولى، فيما إذا كانت شبكة الإنترنت أداة إيجابية لارتكاب الجريمة، أي كوسيلة تسهل للمجرم المعلوماتي تحقيق غايته الجرمية، ورأى الباحث فيها أغلب صور جرائم الاعتداء على الأشخاص التي يتصور وقوعها عبر شبكة الانترنت.

والثانية، فيما إذا كانت شبكة الانترنت أداة سلبية لارتكاب الجريمة، أي محلاً لها، إذ يكون هدف المجرم البيانات والمعلومات المخزنة والمنقولة عبر قنوات الإنترنت المفتوحة (العامة) أو المغلقة (الخاصة)، ورأى فيها صور جرائم الاعتداء على الأموال، وقد توصل الباحث في هذه الدراسة إلى نتائج أهمها أن المشرعين الأردني والمصري، من خلال نصوصهما العقابية، يقصران نطاق الحماية على الأموال المادية الملموسة دون الأموال المعنوية، وتوصل إلى وجود قصور في النصوص الجنائية التقليدية سواء الموضوعية أم الإجرائية في مواجهة الإجرام المعلوماتي.

ومن هنا نجد أن هذه الدراسة جاءت على نحو كبير من العمومية والشمول في صور الجرائم، لتضم جرائم الاعتداء على الأشخاص والأموال عبر الإنترنت، ومقتصرة على تحليل القواعد الجنائية التقليدية دون القوانين الخاصة، إلا أن الباحث سوف تأتي دراسته وتنصب بشكل تفصيلي وأساسي على المعلومات دون غيرها، وسوف تبين مدى فعالية كافة التشريعات الأردنية في توفير الحماية الجنائية لأنظمة المعلومات دون أن تقتصر الدراسة على القواعد الجنائية التقليدية فقط.

3- **سلامة (2005)، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنه البرامج:**

وقد بين هذا المرجع أن من أهم المسائل القانونية التي أثارها استخدام الحاسب الآلي، هي تحديد ماهية برامج الحاسب الآلي، وطبيعتها القانونية، وهل هي مصنفات قابلة للحماية بموجب قانون حق المؤلف، أم أنها اختراعات يمكن حمايتها في إطار الملكية الصناعية، كالقوانين الخاصة ببراءات الاختراع و العلامات التجارية، وتناول هذا المرجع القواعد المقررة لحماية برامج الحاسب الآلي، حيث ركز على الحماية المقررة للملكية الفكرية للبرامج كالملكية الصناعية، والتجارية، والأدبية والفنية، وكل ذلك وفق قانون حماية حق المؤلف سواء أكانت هذه الحماية موضوعية أم إجرائية.

وقد جاء هذا المرجع كدراسة في القانون المدني، وركز على الحماية القانونية لبرامج الحاسب الآلي من الناحية المدنية وليست الجزائية، وتوصل في هذه الدراسة إلى نتائج أهمها: أن برنامج الحاسب الآلي يعتبر أحد المصنفات الأدبية والفنية المشمولة بالحماية سواء أكان بصورة برامج أم قواعد بيانات، وأن الحماية، لبرامج الحاسب الآلي تكفل للمؤلف حماية مدنية تتمثل في حقه في المطالبة بالتعويض، كما يكفل له حقه من خلال الحماية الجزائية التي بموجبها يتم إيقاع العقوبات الرادعة بحق المعتدي.

ومن هنا نجد أن هذا المرجع هو دراسة في القانون المدني، وركزت على الحماية القانونية لبرامج الحاسوب من خلال قانون حماية حق المؤلف، وتحدثت عن الملكية الفكرية والصناعية، والتجارية والأدبية والفنية، أما الباحث فسوف تنصب دراسته على الحماية القانونية الجنائية لأنظمة المعلومات عبر شبكة الإنترنت، وسوف يركز على الشق الجزائي منها من خلال البحث في الحماية الجنائية في القواعد التقليدية الجزائية والقوانين الخاصة وليست المدنية.

4- **سليمان، لات، إستراتيجية مكافحة الجرائم استخدام الحاسب الآلي:**

تناول هذا المرجع المواجهة التشريعية للجرائم الناشئة عن استخدام الحاسب الآلي، ومنها جرائم الأموال وصور ارتكابها، وجرائم النصب والسرقة وخيانة الأمانة، والجرائم المضرة بالثقة العامة، والماسة بالشرف والاعتبار، وجرائم الاعتداء على الحياة الخاصة وغيرها من الجرائم، مبيناً الآراء الفقهية التي قيلت حول تلك الجرائم، وقد أكد الباحث أن الدراسات السابقة التي تناولت هذا الموضوع من مختلف جوانبه، اعتمدت على المقارنة في التشريع الفرنسي- ولم تتناول التشريع الأمريكي، ولذلك فقد انصبت دراسته بشكل أساسي على المقارنة بين التشريع المصري والتشريع الأمريكي، أما هذه الدراسة فسوف ترتكز على المقارنة بين التشريع الأردني والتشريع الأمريكي، والوقوف على مدى الحماية الجنائية التي وفرها المشرع الأردني في مواجهه هذه الجرائم المرتكبة عبر شبكة الحاسوب والإنترنت.

5- **الهرش (2005)، الحماية الجزائية لبرامج الحاسوب، دراسة مقارنة:**

هذا المرجع أطروحة دكتوراه في القانون العام/ جامعة عمان العربية. حيث تناولت هذه الدراسة النظام القانوني لحماية برامج الحاسوب جزائياً، من حيث حماية برنامج الحاسوب في إطار قوانين الملكية الفكرية الأردنية، من خلال بيان ماهية المصنف، ومفهومه، وشروط الحماية، وبرنامج الحاسوب، وصفة المصنف، ومدى انطباق صفة المصنف ع لى برنامج الحاسوب، وتطرق أيضاً إلى حماية برنامج الحاسوب خارج نطاق قانون حماية حق المؤلف، من خلال قانون براءة الاختراع، وماهيته، ومدى انطباق صفة الاختراع على برنامج الحاسوب، وتناولت هذه الدراسة أيضاً حماية برنامج الحاسوب في إطار جرائم الأموال، من خلال مدى صلاحية برنامج الحاسوب لأن يكون محلاً لجرائم الأموال، ومدى انطباق صفة المال على هذا البرنامج، وتطرقت هذه الدراسة أيضاً إلى الحماية الجزائية لحقوق تأليف البرنامج، ولجريمة تقليد برنامج الحاسوب، وحدود التجريم والعقاب في نطاق حماية حقوق تأليف البرنامج. وكان محور الدارسة المقارنة بين القانون الأردني والقانون الأمريكي بصورة أساسية وفق قانون حماية حق المؤلف. وقد خرج الباحث بعدة نتائج منها: أن برنامج الحاسوب من المصنفات الفكري ة وفقاً لقانون حماية حق المؤلف الأردني والتشريعات المقارنة،

ويمكن كذلك حماية هذا البرنامج استناداً إلى قانون براءة الاختراع، وأنه لا يوجد مبرر لحماية برامج الحاسوب بقانون خاص، ولذلك نجد أن هذه الدراسة جاءت عامة على برامج الحاسوب دون تحديد، واقتصرت على حماية هذه البرامج وفق قانون حماية حق المؤلف تارة، وتارة أخرى وفق قانون براءة الاختراع فقط، إلا أن الباحث سيبين مدى الحماية الجنائية التي وفرتها كافة التشريعات الأردنية للمعلومات بشكل أساسي عبر شبكة الحاسوب والإنترنت، وبالتالي سيلقى الضوء على كافة التشريعات الأردنية وليس فقط قانون الملكية الفكرية وقانون براءة الاختراع.

6- ميلاد (2007)، جريمة إتلاف المعلومات، دارسة مقارنة:

هذه الدراســة هي أطروحة دكتوراه في القانون العام ، جامعة عمان العربية حيث تناولت ماهية نظم المعلومـات ومفهومهـا وطبيعتهـا القـانونيـة، ومـدى انطباق الصــفة المالية للمعلومات، ومدى كفاية النصـوص الجزائية، وبشـكل خاص القانون الليبي في الحماية من جرائم إتلاف المعلومات، وقد أدرجت هذه الدراسة الاتجاهات التشريعية والاتجاهات الفقهية حول ذلك، وبينت أركان هذه الجريمة، وكان الغرض من هذه الدراسة هو تحديد مدى كفاية نصوص قوانين العقوبات التقليدية في التشريع الليبي والمصري والأردني المتعلقة بإتلاف الأموال في حماية نظم المعلومات، ومدى الحاجة إلى نصـوص قانونية خاصـة تعالج مسـألة إتلاف نظم المعلومات.

وانصبت هذه الدراسـة بشـكل اقتصر على جريمة إتلاف نظم المعلومات فقط، وقد توصلت هذه الدراســة إلى نتائج أهمها: أن المعلومات المخزنة في جهاز الحاســوب تعتبر أموالاً مادية منقولة وبالتالي يمكن اعتبارها محلاً صالحاً لجريمة إتلاف الأموال المقررة في قانون العقوبات الليبي، إلا أن هذه النصوص التقليدية تبقى قاصرة عن حماية المعلومات، في مواجهة العديد من صور الإتلاف المستحدثة للمعلومات. وعلى الرغم من ذلك فإن هناك اعتبارات متعددة تسـتوجب تدخل المشـرع الليبي بالنص على تجريم إتلاف المعلومات من خلال نصـوص خاصـة، أما الباحث فسوف يدرس موضوع الحماية من ناحية التشريعات الأردنية مقارنة بالتشـريع الأمريكي وسـوف تأتي دراسـته بشـكل أوسـع من هذه الدراسـة السابقة، حيث ستبين مدى كفاية التشـريعات في توفير الحماية الجنائية للمعلومات بكافة صـور هذه الجرائم، ولن تقتصر فقط على جريمة إتلاف نظم المعلومات، وبالتالي سوف تأتي بإضافة جديدة إلى هذه الدراسة.

7- سلامة (2006)، جرائم الكمبيوتر والإنترنت:

وقد تناولت هذه الدراسة الجوانب الفنية للحاسب الآلي ومكوناته في فصلها التمهيدي، وتناولت جرائم الحاسب الآلي في فصلها الأول، من خلال التركيز على ماهية المعلومات وخصائص الجريمة المعلوماتية، وتقسيماتها، والآراء الفقهية حول تلك التقسيمات، والجهود الدولية التي بذلت لتقسيم هذه الجرائم، من خلال التقسيم الذي جاءت به منظمة التعاون الاقتصادي والتنمية، والتقسيم الذي جاء به المجلس الأوروبي لجرائم المعلوماتية، وقد ركزت هذه الدراسة بشكل مباشر على النظريات والآراء الفقهية حول تلك المواضع، أما الباحث فإن دراسته سوف تتطرق إضافة لذلك إلى النصوص القانونية الجنائية التقليدية والخاصة في التشريع الأردني مقارنة بالتشريع الأمريكي .

8- الطوالبة (2003)، التفتيش الجنائي على نظم الحاسوب والإنترنت، دراسة مقارنة:

هذا المرجع هو رسالة دكتوراه في القانون العام، جامعة عمان العربية، حيث سعى الباحث فيها إلى تطبيق النصوص التقليدية في قانون أصول المحاكمات الجزائية الأردني على موضوع التفتيش والضبط على نظم الحاسوب والإنترنت ومراقبة المشروعية، سيما وأن تطبيق هذه النصوص على الجرائم المتعلقة بالحاسوب والإنترنت يثير مشاكل عديدة في مسألة الإثبات، حيث يصعب في كثير من الأحيان العثور على أثر مادي للجريمة المعلوماتية، وفي أحيان أخرى سهولة محو الدليل في زمن قصير جداً، الأمر الذي يصعب عملية التفتيش على نظم الحاسوب والانترنت، وكان هدف الباحث في هذه الدراسة هو محاولة لسد الفراغ الحاصل في مثل هذا النوع من الجرائم، وقد توصل الباحث إلى عدة نتائج أهمها: إن التشريعات العربية لم تُعرف التفتيش الواقع على نظم الحاسوب والإنترنت ولم تحدد طبيعته القانونية.

وقد عرج الباحث على التوصية التي أصدرها المجلس الأوروبي لعام 1995م، والخاصة بمشاكل الإجراءات الجنائية الوطنية والتي من أهمها: أن توضح القوانين إجراءات تفتيش أجهزة الحاسوب، وضبط المعلومات التي تحويها، ومراقبة المعلومات أثناء انتقالها، وأن تسمح الإجراءات الجنائية للجهات القائمة على التفتيش بضبط برامج الحاسوب والمعلومات الموجودة في الأجهزة، ومن هنا نجد أن هذه الدراسة قد ركزت على الجانب الإجرائي لجرائم المعلومات، وبالأخص موضوع التفتيش والضبط لنظم الحاسوب والإنترنت، ولم تتطرق هذه الدراسة إلى الجانب الموضوعي، وباقي الإجراءات لمثل هذه الجرائم، أما الباحث فسوف يتطرق في دراسته إلى الجانب الموضوعي لمثل هذه الجرائم لمعرفة مدى الحماية التي وفرتها هذه القواعد الموضوعية الجنائية للمعلومات عبر الحاسوب والإنترنت.

الفصل الثاني-

ماهية نظم المعلومات والجرائم المعلوماتية والتعاون الدولي لمواجهتها:

كان للتقدم الإلكتروني في تكنولوجيا المعلومات والاتصالات الذي شهده العالم منذ منتصف القرن العشرين أثر كبير في انتشار التقنية العالية من حاسبات آلية، وبرامج متقدمة، وشبكات إتصال إلكترونية، قربت بين أفراد البشر في شتى أنحاء العالم على الرغم من بُعد المسافات فيما بينهم، حتى أصبحوا كخلية واحدة مترابطة، إلا أن هذه الثورة المعلوماتية والتقنية المتقدمة وعلى الرغم مما رتبته من مزايا في شتى مجالات الحياة، فقد رافقها تهديد مباشر للأمن والاستقرار والسلام في العالم، حيث ظهرت كثيراً من الخروقات القانونية والتعديات غير المتوقعة، وأصبحت في بعض الأحيان تحول دون إتمام عمليات التطوير والتنمية في الدول، ولم تعد عواقبها قاصرة على بعض الأفراد أو الجماعات، بل امتدت آثارها لتهدد دولاً برمتها، وقد أدى ذلك إلى تصدي الكثير من دول العالم عن طريق أجهزتها التشريعية للحد من هذه الخروقات القانونية، ولمواجهة الاستخدام غير القانوني لهذه التقنية الحديثة، ولوضع قواعد قانونية تنظم استخدام الشبكة الجديدة.

وقد كان مشرعو الدول في الماضي يستخدمون مصطلح الحاسب الآلي للدلالة على هذه التقنية، إلا أن هذا المصطلح كان قاصراً على جهاز الحاسوب بمكوناته المادية فقط من شاشة عرض ولوحة المفاتيح ووحدة التشغيل، إلا أنه في الوقت الراهن أصبح يتصل بمكونات أخرى كالطابعة والماسح الضوئي وشبكة الإنترنت، حيث أصبح يتكون من نظام معلوماتي متكامل وليس مجرد جهاز حاسوب، وللوقوف على ماهية نظم المعلومات والجرائم المعلوماتية والتعاون الدولي لمواجهتها، فقد تم تقسيم هذا الفصل وفقاً للمباحث التالية:

المبحث الأول: الجوانب التقنية والفنية للنظام المعلوماتي.

المبحث الثاني: المعلومات الإلكترونية، ماهيتها، الطبيعة القانونية لها، أنواعها وشروطها.

المبحث الثالث: الجرائم المعلوماتية والمجرم المعلوماتي.

المبحث الرابع: التعاون الدولي لمواجهة جرائم الحاسوب والإنترنت.

المبحث الاول: الجوانب التقنيه والفنية للنظام المعلوماتي:

إن دراسة موضوع الحماية الجنائية للمعلومات المتداولة عبر الحاسوب والإنترنت ، وموضوع الجرائم المعلوماتية الخاصة بالمعلومات المعالجة آلياً، يتطلب إلقاء الضوء على مفهوم النظام المعلوماتي ومكوناته ومفهوم الحاسب الآلي والإنترنت، لذلك سوف نتناول دراسة هذا المبحث وفقا للمطالب التالية:

المطلب الاول :المدلول العام للنظام المعلوماتي.

المطلب الثاني :مفهوم الحاسب الآلي وخصائصه.

المطلب الثالث : مفهوم الإنترنت وخصائصه.

المطلب الرابع :مكونات النظام المعلوماتي.

المطلب الأول : المدلول العام للنظام المعلوماتي وتطوره التاريخي:

وقد تم تقسيم هذا المطلب إلى فرعين الأول يتحدث عن التطور التاريخي للنظام المعلوماتي، والثاني يتعلق بمفهوم النظام المعلوماتي وذلك كما يلي:

الفرع الأول: التطور التاريخي للنظام المعلوماتي:

كان أول ظهور للحاسب الآلي سنة 1946 عندما قام باحثان أمريكيان في جامعة بنسلفانيا بتطوير أول جهاز في صورة أداة إلكترونية أو آلية للحساب، قابلة للبرمجة، وذلك اعتمادا على أفكار العالم الألماني المشهور (Jan Neumann) (عرجاوي، 2000، 364-365).

وقد تطورت صناعة الحاسبات الآلية وفقاً لخمسة أجيال نبرزها بشكل موجز كما يلي:

الجيل الأول- الفترة ما بين 1944 – 1959: كانت هذه الحاسبات تعمل باستخدام الصمامات المفرغة (Vacum type) كوسيلة لنقل وتخزين البيانات، وهي تمتاز بكبر حجمها وسرعتها البطيئة، وكان مخترع هذه الأجهزة هاوارد أيكن عام 1944 ، وقد استخدمت هذه الحاسبات لاحقاً في المجالات العسكرية (الملط، 2006، 21).

وفي مرحلة لاحقة تم تصنيع أجهزة الرادار التي استخدمت في الحرب العالمية، ثم ظهر الحاسب الآلي إنياك (ENIAC) على يد إيكارث وميكانيلي، في معهد الهندسة الإلكترونية في جامعة بنسلفانيا (الفيومي، 1998، 7-9).

ثم أبتكر بعد ذلك الحاسب الآلي إدفاك (EDVAC)، وهو أول حاسب ذي برامج تخزين، وفي عام 1948 استطاع فريق من العملاء في جامعة كامبردج من ابتكار جهاز سمي إدساك (EDSAC)، ثم ظهر الحاسب الآلي يونيفاك (UNIVAC) عام 1951، وفي عام 1954 ظهر الحاسب الآلي آي بي أم (I.B.M) وهو أشهر الحاسبات الإلكترونية ويعتبر أول حاسب يستخدم ذاكرة عبارة عن أسطوانة ممغنطة (عرجاوي، 2000، 365) (الملط، 2006، 21).

الجيل الثاني- الفترة ما بين 1960 وحتى 1965: وفقاً لهذا الجيل أصبحت الحاسبات الآلية تعمل بالترانزيستور وقادرة على تخزين كم هائل من البيانات وملائمة للتطبيقات التجارية والأغراض العلمية (الملط، 2006، 21).

الجيل الثالث: وفيه أستخدمت الدوائر المتكاملة بدلاً من الترانزيستور، وتمتاز بأنها أصغر حجماً وأقل كلفة، مما أدى إلى الحصول على حاسب ات آلية أكثر تعقيداً، وذات طاقة أكبر.

الجيل الرابع: ظهر هذا الجيل في أوائل السبعينات من القرن المنصرم، ويتمثل أساساً في استخدام الحاسبات الصغيرة، وهي لا تحتاج إلى تدريب خاص، أو إلى لغات معقدة لكتابة البرامج، كما شهد هذا الجيل زيادة في القدرة التخزينية للحاسبات الآلية.

الجيل الخامس: وقد ظهر في التسعينات في اليابان وأمريكيا، وتتصف الحاسبات في هذا الجيل بالذكاء الصناعي، بالإضافة إلى زيادة سعة الوحدات التخزينية، مع صغر حجم الحاسب الآلي نفسه (الفيومي، 1998، 8-9).

الفرع الثاني: مفهوم النظام المعلوماتي:

عرف الفقه النظام المعلوماتي بأنه "مجموعة من الأجزاء المترابطة التي تتفاعل مع البيئة، ومع بعضها بعضا لتحقيق هدف ما عن طريق قبول المدخلات وإنتاج المخرجات من خلال إجراء تحويلي منظم" (حجازي، 2009، 9).

أما الأنظمة القانونية فقد عرف المشرع الأردني النظام المعلوماتي في قانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001 بأنه "النظام الإلكتروني المستخدم لإنشاء رسائل البيانات، أو إرسالها أو استلامها أو معالجتها، أو تخزينها، أو لتجهيزها على أي وجه آخر".

وعرفه المشرع الأردني أيضاً في قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010 بأنه "مجموعة البرامج والأدوات المعدة لإنشاء البيانا ت أو المعلومات إلكترونياً، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها".

وقد عرفه القانون الاتحادي لدولة الإمارات رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات في المادة (1) بأنه "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الإلكترونية أو غير ذلك" (http://www.neuae.com/?p=25).

وقد عرفه نظام مكافحة جرائم المعلوماتية والتعاملات الإلكترونية السعودي الصادر في 1428/3/7هـ 2007/3/26 "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية" (htt//www.traidnt.net).

وعرفه قانون مملكة البحرين رقم 28 لسنة 2002 بشأن المعاملات الإلكترونية بأنه "نظام إلكتروني لإنشاء أو إرسال أو بث أو تسلم أو حفظ أو عرض أو تقديم المعلومات".

(http://www.ar.jurispedia.org.com)

وعرف قانون سلطنة عمان رقم 69 لسنة 2008 بشأن المعاملات الإلكترونية في المادة الأولى النظام المعلوماتي بأنه "نظام إلكتروني للتعامل مع المعلومات والبيانات بإجراء معالجة تلقائية لها، لإنشاء أو إرسال أو تسلم أو تخزين أو عرض أو برمجة أو تحليل تلك المعلومات والبيانات" (http://www.omanlegal.journal.com).

كما عرف قانون دبي للمعاملات والتجارة الإلكترونية رقم (2) لسنة 2002 النظام المعلوماتي بأنه "نظام إلكتروني لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونياً".

(http://www.helmylawyers.maktoobblog.com)

وقد جاء المشرع القطري وأدرج تعريفاً لنظام المعالجة الآلية للبيانات في المادة (370) من قانون العقوبات لدولة قطر رقم 11 لسنة 2004 بأنه "كل مجموعة من واحدة أو أكثر من وحدات المعالجة، سواء تمثلت في ذاكرة الحاسب الآلي، أو برامجه، أو وحدات الإدخال أو الإخراج، أو الاتصال التي تساهم في تحقيق نتيجة". (http://www.gcc-legal.org.com)

أما بالنسبة للمشرع المصري فلم يدرج تعريفاً للنظام المعلوماتي وفق قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 ، حيث صدر هذا القانون خالياً من أي تعريف للنظام المعلوماتي.(http://www.egy-law.com)

وفي الاتجاه الدولي فقد عرفت معاهدة بودابست الدولية لسنة 2001 بشأن مكافحة جرائم الفضاء الإلكتروني النظام المعلوماتي بأنه "كل جهاز بمفرده أو مع غيره من الأجهزة من الآلات

المتواصلة بينياً أو المتصلة، والتي يمكن أن يقوم واحد منها أو أ كثر تنفيذاً لبرنامج معين بأداء المعالجة الآلية للبيانات[1] (The Budapest International convention on cyber crime 2001 article 1A).

وقد نصت اتفاقية المجلس الأوروبي لعام 2000 والخاصه في الحماية من جرائم الحاسب الآلي في فصلها الأول والمخصص لضبط المصطلحات (Use of Terms) وجاء في المادة الأولى تعريف الحاسب الآلي "بأنه أي جزء من الأجزاء المترابطة التي تعالج البيانات وتشغل البرامج" .(http//convention.cone.Int/treaty/en/projectseybercrime.Httm1:page(1-17))

ويرتكز النظام المعلوماتي على ثلاثة أركان، الأول هو المدخلات (Input) وتتضمن البيانات المختلفة (Data)، والثاني المخرجات (Output) وهي نظم استدعاء هذه المعلومات بشكل منظم بحسب الحاجة إليها، إذ تعطي ميزة الإخراج استدعاء معلومة محددة ومطلوبة فلا تظهر المعلومات كلها مرة واحدة، والثالث المعالجة الآلية للبيانات المدرجة في النظام بحيث تتقبل المعالجة الاستفهام أو الاستدعاء وتجيب عليه، فنظام المعلومات هو عبارة عن آلية وإجراءات منظمة، تسمح بتجميع وتصنيف، وفرز البيانات Data ومعالجتها، ومن ثم تحويلها إلى معلومات (Information) يسترجعها الإنسان عند الحاجة، ليتمكن من إنجاز عمل أو اتخاذ قرار أو القيام بأية وظيفة عن طريق المعرفة التي سيحصل عليها من المعلومات المسترجعة من النظام (إبراهيم، 2009، 23).

أي أن نظام المعلومات (Information system) هو "مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها (Set of information component) والتي تعمل على جمع البيانات والمعلومات ومعالجتها وتخزينها وبثها وتوزيعها، بغرض دعم صناعة القرارات والتنسيق وتأمين السيطرة على المنظمة، إضافة إلى تحليل المشكلات، وتأمين المنظور المطلوب للموضوعات المعقدة".

---

[1] (Article 1-A "Computer System" Means any Device or a Group of Interconnected or Automatic Processing of Data).

ويشتمل نظام المعلومات على بيانات عن الأشخاص الأساسيين والأماكن والنشاطات والأمور الأخرى التي تخص المنظمة والبيئة المحيطة بها (إبراهيم، 2010، 18-19).

المطلب الثاني: مفهوم الحاسب الآلي وخصائصه:

وسيتم تقسيم هذا المطلب إلى ثلاثة فروع الأول منها يتعلق بتعريف الحاسب الآلي، والثاني حول مكونات الحاسب الآلي والثالث خصائص الحاسب الآلي.

الفرع الأول: تعريف الحاسب الآلي:

تعددت التعريفات التي أعطيت للحاسب الآلي على النحو التالي:

ذهب رأي إلى أن الحاسب "آلة تقوم بأداء العمليات الحسابية، واتخاذ القرارات المنطقية على البيانات الرقمية بوسائل إلكترونية، وذلك تحت تحكم البرامج المخزنة فيها (المناعسة، وآخرون، 2001، 58).

وذهب رأي آخر إلى القول بأنه: "مجموعة من الأجهزة المتكاملة تعمل مع بعضها بعضا بهدف تشغيل (Process) مجموعة من البيانات الداخلة(Input Data) وفقاً لبرنامج (Program) موضوع مسبقاً للحصول على نتائج معينة" (قشقوش، لات، 19).

وعرفه البعض بأنه "جهاز إلكتروني يتكون من مجموعة متداخلة من الأجزاء، تعمل فيما بينها بهدف مشترك، هو إخ راج العمليات الحسابية والمنطقية طبقاً لبرنامج يتم وصفه مسبقاً، من خلال عدة عمليات هي الإدخال والمعالجة والاسترجاع والإخراج" (إبراهيم، 2009، 17).

ويرى البعض بأن الحاسب الآلي هو جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعة كبيرة تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة وبدرجة عالية الدقة، وله القدرة على التعامل مع كم هائل من البيانات وكذلك تخزينها واسترجاعها عند الحاجة إليها" (لطفي، 1987، 6).

ويجد بعض الفقهاء المتخصصين في مجال الجرائم المعلوماتية ومنهم الدكتور/ خالد ممدوح إبراهيم أن أفضل تعريف للحاسب الآلي هو الذي ورد في الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، موسوعة دلتا كمبيوتر، وذلك لشموله جميع الوظائف التي يؤديها الحاسب الآلي في الحياة العملية والواقعية، حيث عرفت الحاسب الآلي بأنه: "جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال بيانات (Data Input)،

أو إخراج معلومات (Information Output)، وإجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج (Output Devices) أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الحاسب (Operator) عن طريق وحدات الإدخال، مثل وحدة المعالجة المركزية Central processing Unit (C.P.U) التي تقوم بإجراء العمليات الحسابية Arithmetic Operations، وكذلك العمليات المنطقية Logaic Operations، وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج (Output Devices)، مثل الطابعات Printers أو وسائط التخزين المختلفة Stoorage Units، وجميع العمليات التي يقوم بها الحاسب تتم بسرعة مذهلة تقترب في بعض الأحيان من سرعة الضوء" (فهمي وآخرون، 1991، 108).

ومن كل ما تقدم فإن الباحث يذهب مع التعريف الوارد في الموسوعة الشاملة لمصطلحات الحاسب الآلي موسوعة دلتا كمبيوتر، لأن دراسة الجوانب التقنية للحاسب الآلي يُحتم علينا الرجوع إلى المتخصصين في هذا المجال، ومن خلال الواقع العملي بمعرفة الشخص العادي في الحاسب الآلي، يبدو أن هذا التعريف الوارد في هذه الموسوعة هو شامل وجامع لكافة الوظائف الفنية والأدوار التي يؤديها الحاسب الآلي.

الفرع الثاني: مكونات الحاسب الآلي:

للحاسب الآلي مكونات مادية ومكونات منطقية وذلك كما يلي :

أولاً- المكونات المادية للحاسب الآلي:

تتألف المكونات المادية للحاسب الآلي من ثلاثة عناصر رئيسة وهي: وحدة تشغيل الحاسب، ووحدات الإدخال والإخراج، ووحدات التخزين، وسوف نتطرق إلى كل منها بإيجاز (سلامة، 2006، 36):

1- وحدة التشغيل:

تعتبر وحدة التشغيل الجزء الرئيس في جهاز الحاسب الآلي، ويطلق عليها البعض عقل الحاسب، حيث تتكون من الذاكرة الرئيسة Main memory، ووحدة الحساب والمنطق Arithmetic and logic unit، ووحدة التحكم Control Unit، ويطلق على وحدة الحساب والمنطق ووحدة التحكم معاً اسم وحدة التشغيل المعالجة المركزية Central Processing Unit (CP.U)، كما يطلق عليها أيضاً اسم وحدة المعالجة المركزية (طلبة وآخرون، 1992، 21-23).

(أ) الذاكرة الرئيسة Main memory:

تستخدم هذه الذاكرة لحفظ البيانات والمعلومات والبرامج المدخلة في الحاسب الآلي حفظاً دائماً أو م ؤقتاً، وتتكون هـذه الـذاكرة من جزأين هما: ذاكرة القراءة فقط، وذاكرة القراءة والكتـابة (أحمد، 1997، 20).

وسـميت ذاكرة القراءة بهذا الإسـم لأنه يمكن القراءة منها فقط دون أي اسـتخدام آخر، وتستخدم لتخزين البيـانـات والأوامر بهـا بصـــفـة دائمـة عند تصـــنيعها، لهذا فهي تســـمى أيضـــاً بالذاكرة الدائمة (Permanent memory)، ومن خصـائصـها أنها لا تكتب برامجها إلا بمعرفة الشركة المنتجة لها، ومن أمثلة هـذه البرامج (لغـة المترجم) Language interpreter، كما أنهـا تقوم بالاحتفاظ بالبيانات والأوامر المخزنة فيها في حالة انقطاع التيار الكهربائي، ولا يمكن لمستخدم الحاسب الآلي أن يسجل فيها أية معلومات (سلامة، 2006، 37).

أما ذاكرة القراءة والكتابة فهي تسـمى أيضـاً بالذاكرة العشـوائية، أو الذاكرة المؤقتة Temporary memory، أو الذاكرة المتطايرة Volatile Memory، أو ذاكرة العمل Working Memory.

وهـذه الـذاكرة يمكن من خلالهـا الوصـــول إلى عنوان فيهـا دون الحـاجـة إلى المرور على العناوين الأخرى، وهي تختلف عن ذاكرة القراءة فقط حيث إن الأخيرة غير قابلة للتعديل بواســطة المســتخدم، أما العشـــوائية فإن محتوياتها تتغير بحســـب البرامج التي يتم تحميلها بالحاســـب، كما أنها تفقد المعلومات والبيانات المخزنة بمجرد انقطاع التيار الكهربائي (محمود، 2002، 19).

(ب) وحدة الحساب والمنطق Arithmetic and Logic Unit:

وهـذه الوحـدة هي جزء من وحدة التشـــغيل أو المعالجة المركزية (CPU)، وهي مســـؤولة عن معالجة البيانات حسـابياً ومنطقياً، وتتكون من مجموعة من الدوائر الإلكترونية المنطقية التي يتم توظيفها لأداء العمليات ومجموعة من الســـجلات، وأهم وظائف هذه الوحدة، تأدية وإنجاز العمليات الحســـابية، Arithmetic Operation وإنجاز العمليات المنطقية Logical Operation (أحمد، 1997، 21).

(ج) وحدة التحكم Control Unit (CU):

وهي جزء من وحدة المعالجة المركزية (CPU)، وتقوم بالتنسيق والتحكم في البيانات الداخلة والخارجة من وإلى الذاكرة الرئيسة للحساب بتوجيهها إلى القنوات المختلفة، وهي تعمل كوسيلة اتصال من الذاكرة الرئيسة ووحدة الحساب والمنطق إلى باقي وحدات الحاسب، كما وأنها تحتوي على ساعة منطقية تقوم بالتحكم في توقيت العمليات المختلفة، وتحتوي على وحدات تخزين تسمى السجلات (registers) تؤدي مجموعة من الوظائف الأساسية مثل تخزين عنوان الأمر التالي المطلوب تنفيذه (محمود، 2002، 20).

2- وحدات الإدخال والإخراج Input / Output Unit:

وتستخدم في إدخال البيانات والمعلومات إلى وحدة التشغيل المركزية أو إخراجها لاستخدامها بواسطة المستخدم، وذلك بتوجيه من وحدة التحكم.

(أ) وحدات الإدخال Input Units:

وهي الوحدات المسؤولة عن إدخال المعلومات والبيانات إلى جهاز الحاسب الآلي، ومن أمثلتها لوحة المفاتيح Keyboard، الفأرة Mouse، الماسح (Scanner)، ماسح كود الأعمدة Barcode scanner، شاشات اللمس (Touch Screen)، وغيرها.

(ب) وحدات الإخراج Output Unit:

وهي الوحدات المسؤولة عن إخراج المعلومات بعد إدخال البيانات والتعليمات ومعالجتها عن طريق الحاسب الآلي، حيث يمكننا الحصول على هذه المعلومات بعد إدخال البيانات ومعالجتها، ومن ثم تخرج على شكل معلومات عبر وحدات الإخراج، ومن أمثلة هذه الوحدات شاشات العرض Monitor، الطابعة Printer، الراسم Plotter، الميكروفيلم Computer Output Microfilm (C.O.M).

3- وحدات التخزين Storage Disk Drive :وهي الوحدات المسؤولة عن تخزين البيانات والمعلومات، ومن أمثلتها وحدة الأقراص المرنة Floppy Disk Drive، ووحدة الأقراص الصلبة Hard Disk، والشريط المغناطيسي (Magnetice Tape).

ثانيا- المكونات المنطقية للحاسب الآلي (البرامج) Software:

يعرف البرنامج لغوياً بأنه مصطلح يستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسب الآلي، ويشـــمل ذلك برامج النظام وهي البرامج اللازمة لتشـــغيل الحاســـب (البرامج التشـــغيلية)وبرامج التطبيقات وهي البرامج الخاصة بمستخدم الحاسب (البرامج التطبيقية) (محمود، 2002، 31).

وعرفه البعض بـأنـه تعليمات مكتوبـة بلغـة مـا موجهـة إلى جهـاز تقني معتمد يســـمى بالنظام المعلوماتي بغرض الوصـــول إلى نتيجة معينة، أو مجموعة من التعليمات المتتابعة بصـــفة منطقية توجه إلى الكمبيوتر لأداء عمل أو أعمال معينة (الهادي، 1989، 110).

وقد عرفته المنظمة العالمية للملكية الفكرية المعروفة باسم "الويبو" بأنه: "مجموعة من التعليمات التي تســـمح بعـد نقلها على دعامة مقروئة من قبل الآلة ببيان أداء أو إنجاز أو وظيفة أو مهمة أو نتيجة معينة عن طريق آلة قادرة على معالجة المعلومات".

وقد عرف القانون الأمريكي الصـادر سـنة 1980 والخاص بحماية حق المؤلف البرنامج (Software) بأنه "مجموعة توجيهات أو تعليمات يمكن للنظام استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة" (الملط، 2006، 43).

أما بالنسـبة للمشرع الأردني فقد عرف البرنامج في المادة الثانية من قانون جرائم أنظمة المعلومات الأردني المؤقـت رقم (30) لســـنـة 2010 حيـث عرف البرامج بأنها "مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات".

وتقسم البرامج أو المكونات المنطقية للحاسب إلى نوعين:

الأول: برامج التطبيقات أو الكيانات المنطقية التطبيقية Applications Program/ Soft Ware.

وهي البرامج التي تصمم لتنفيذ وظائف محددة إدارية أو علمية أو غيرها، مثل الرواتب Payroll، والدراسـات الإحصائية Statistical Analysis، والمحاسبية Accounting، وغيرها من البرامج الأخرى (طلبة، وآخرون، 1992، 26).

والثاني: برامج النظام أو الكيانات المنطقية الأساسية: System Programs.

وهي برامج أكثر عمومية من برامج التطبيقات وتكون مســـتقلة عن أي تطبيق محدد، فهي تخدم برامج التطبيقات عن طريق أكبر إفادة ممكنة من مكونات الحاسـب، فمثلاً عند بدء تشـغيل الحاسب الآلي يقوم برنامج معين بتجهيز الأجهزة والمكونات للعمل، ومن أهم برامج النظام مترجمات ومفسرـات اللغات المختلفة، كذلك تدخل نظم التشغيل operating systems ضمن هذا التصنيف (محمود، 2002، 33).

وتقوم نظم التشغيل بالعديد من الوظائف والمهام تتخلص فيما يلي:

1- التحكم والسيطرة على مكونات النظام المعلوماتي.

2- أداء العمليات الأساسية التي تساعد المستخدم على التعامل مع مكونات النظام المعلوماتي مثل نسخ الملفات ومسحها.

3- التعامل مع برامج التطبيقات Applications Programs مثل الجداول الإلكترونية.

4- تنظيم الأعمال التي يقوم بها النظام المعلوماتي Job Control.

5- القدرة على أداء عدة وظائف في نفس الوقت Multitasking.

6- السماح لعدة مستخدمين بالتعامل مع النظام المعلوماتي في نفس الوقت Multi User.

7- القدرة على التعامل مع عدد كبير من الأنظمة المعلوماتية المصنعة بواسطة شركات مختلفة Portability.

8- القدرة على التعامل مع شبكات النظام المعلوماتي التي تستخدم وحدات طرفية بعيدة Remotes Terminal (الملط، 2006، 45-46).

ويرى الباحث أن المكونات المنطقية للحاسب الآلي (البرامج) تعتبر من المعطيات المعنوية والغير مادية للحاسب الآلي وهي تدخل في المعنى الواسع للمعلومات والتي تضم البيانات والمعلومات والكيانات المنطقية (البرامج).

الفرع الثالث: خصائص الحاسب الآلي:

يتميز الحاسب الآلي بعدة ميزات إضافةً إلى القدرات الهائلة في تخزين البيانات ومعالجتها واسترجاعها ومن هذه الميزات ما يلي:

1- إنه قابل للبرمجة أي يمكن تصميمه وتأهيله ليؤدي وظائف معينة عن طريق البرمجيات التي يمكن تطويرها وتحديثها لتؤدي وظائف لا حدود لها.

2- السرعة في معالجة البيانات مقارنة بسرعة البشر.

3- حفظ وتخزين البيانات في أضيق حيز ممكن عن طريق القرص الضوئي المدمج.

4- إمكانية الوصول إليه والتعامل معه واستخدامه من أي مكان في العالم عن طريق استخدام الشبكات (مراد، لات، 20-21).

ووفقاً لهذه الخصائص فإن الحاسب الآلي قادر على القيام بكثير من المهام منها:

1- أداء العمليات الحسابية الأربع بالإضافة إلى العمليات المنطقية (Logic).
2- يمكن للحاسب الآلي الاختيار بين البدائل بطريقة اتخاذ القرارات.
3- يمكن للحاسب الآلي أن يتذكر أو يستدعي معلومات سبق تخزينها فيه.
4- يمكن للحاسب الآلي الاتصال بحاسب آلي آخر، أو عدة حاسبات عن طريق شبكات الاتصال المحلية أو العالمية (www).

في حين لا يستطيع الحاسب الآلي القيام بأية مهام لا تندرج ضمن معطيات البرنامج المُغذى به على الإطلاق (المناعسة، وآخرون، 2001، 69).

المطلب الثالث: مفهوم الإنترنت وخصائصه:

وسنتناول في هذا المطلب تعريف الإنترنت في الفرع الأول وفي الثاني استخدامات شبكة الإنترنت وذلك كما يلي:

الفرع الأول: تعريف الإنترنت:

يعتبر اصطلاح الإنترنت اختصاراً لكلمتين انجليزيتين الأولى International والثانية Network، وتعني كلمة إنتر نت وفقاً لهذا الاصطلاح شبكة الا تصالات الدولية، وقد عرف كثيراً من الفقهاء مصطلح الإنترنت، وعرفته أيضاً بعض القوانين المتعلقة بالجرائم المعلوماتية سواء العربية أو الأجنبية.

وقد بدأ انتشار مصطلح الإنترنت في أوائل الثمانينات على أنه مجموعة من الشبكات المختلفة التي ترتبط فيما بينها بواسطة مجموعة بروتوكولات التحكم بالإرسال/ بروتوكولات الإنترنت وهي مجموعة بروتوكولات طورتها وزارة الدفاع الأمريكية لإتاحة الاتصالات عبر الشبكات المختلفة الأنواع (الجنبيهي، منير والجنبيهي، ممدوح، 2005، 8).

ومن أهم التعريفات التي قيلت عن شبكة الإنترنت "أنها مجموعة شبكات وأجهزة الحاسب الإلكتروني التي تتواجد في مختلف دول العالم والتي تتصل ببعضها، ويجمع بينها أنظمة الاتصالات الإلكترونية التي تستخدم لنقل البيانات أو ما يدعى بنظام Transmission Control Protocol Internet TCP/IP أي نظام نقل المعلومات، ويمكن لأي شخص لديه جهاز كمبيوتر شخصي PC، ولديه إشتراك على شبكة الإنترنت من قبل أحد مقدمي الخدمة المحلية، وجهاز المودم الخاص بالإنترنت، وخط تلفون سواء أرضي أو محمول الدخول على الإنترنت (إبراهيم، 2009، 37)، وقد عرفها البعض بأنها "شبكة دولية لمجموعة حواسيب مرتبطة ببعضها بعضا" (يونس، 2004، 395).

وعرفها البعض بأنها عبارة عن شبكة حاسوبية عملاقة تتكون من شبكات أصغر، بحيث يمكن لأي شخص متصل بالإنترنت أن يتجول في هذه الشبكة، وأن يحصل على جميع المعلومات فيها (إذا سمح له بذلك)، أو أن يتحدث مع شخص آخر في أي مكان من العالم (مصري، 2010، 17).

ويقول البعض أن الإنترنت عبارة عن استغلال متقدم للحاسب الآلي يقوم بربطه عبر الاتصالات الدولية المترابطة، مع وجوب توفر تقنية خاصة قوامها (Modem) وخط هاتف، ويتولى (Modem) تحويل البيانات الرقمية داخل جهاز الحاسب الآلي إلى إشارات صوتية بواسطة خطوط الهاتف التي تتولى بدورها نقل المعلومات عبر أكثر من (Modem) (المناعسة وآخرون، 2001، 60-61).

أما المشرع الأردني فقد أطلق عليها مُسمى الشبكة المعلوماتية في المادة الثانية الخاصة بالتعريفات من قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010، حيث عرف الشبكة المعلوماتية بأنها "ارتباط بين أكثر من نظام معلومات للحصول على البيانات والمعلومات وتبادلها".

ويرى الباحث أن معظم التعريفات الواردة في الفقه والقانون بخصوص شبكة الإنترنت متقاربة فيما بينها من حيث وصفها لهذه الشبكة بأنها ضخمة، وأنها تتكون من مجموعة كبيرة من الحاسبات للمشتركين في هذه الخدمة، والمنتشرين في شتى أنحاء العالم، لتبادل البيانات والمعلومات فيما بينهم كلما سمح لهم ذلك.

ونخلص من هنا إلى تعريف هذه الشبكة بأنها عبارة عن شبكة ضخمة وهائلة، تتكون من مجموعة كبيرة من الحاسبات الآلية، والمشتركين أصحابها في خدمة الإنترنت، والمنتشرة في معظم أنحاء العالم، وترتبط هذه الحاسبات ببعضها بعضا عن طريق خطوط الهاتف الأرضي أو الجوال، أو عن طريق الأقمار الصناعية بحيث يمكن لأصحابها تبادل المعلومات فيما بينهم عن طريق بروتوكول موحد يسمى بروتوكول تراسل الإنترنت (TCP/IP).

الفرع الثاني: استخدامات الإنترنت:

للإنترنت استخدامات وفوائد كثيرة في حياة كثير من البشر نوردها بشكل موجز كما يلي:

1- الشبكة العنكبوتية العالمية World Wide Web:

وهذه الشبكة يطلق عليها مصطلح الويب (Web أو www)، وتنشر من خلالها ملايين الوثائق والأبحاث والتقارير المختلفة المكتوبة والمصورة بمختلف اللغات ومن شتى المصادر المعلوماتية، فهي قاعدة بيانات هائلة تضم ملايين المعلومات ومعروضة في صورة قوائم منظمة يطلق عليها صفحات الويب (البشري، 2005، 45).

ويستطيع أي شخص طبيعي أو اعتباري لديه حاسوب مرتبط بالإنترنت نشر المعلومات على صفحة ويب (شبكة المعلومات الدولية World Wide)، وإذا كانت معظم صفحات الويب ذات صفة عامة يمكن لأي كان الدخول عليها، فإن هناك من الصفحات ما يتمتع بالخصوصية بحيث لا يستطيع أي كان الدخول إليها سوى باستخدام كلمة عبور (يونس، 2004، 408).

2- البريد الإلكتروني Electronic mail:

وهي عبارة عن الرسائل التي يتم تبادلها بين الأشخاص المستفيدين من الشبكه، وتعتبر وسيلة اتصال على درجة عالية من الكفاءة، للاتصال بالآخرين، وعقد الصفقات، والاستفسار عن البيانات والمعلومات ومن أي مكان على الأرض خلال ثوان معدودة (Edwards, and Waelde, 2000, P. 3).

3- بروتوكول نقل الملفات File Transfer Protocol (FTP):

ومن خلال برنامج (FTP) يمكن نقل أية كمية من الملفات أو البرامج من الكمبيوتر إلى أية شركة أو مؤسسة أعمال أو غيرهم، ووضعه على ذا كرة جهاز الكمبيوتر الخاص بالجهة الأخرى، وتتميز هذه الطريقة بسهولتها مقارنة بنقل الملفات عن طريق الأقراص والأشرطة المغنطة (إبراهيم، 2009، 39-40).

4- خدمة المعلومات والأخبار:

حيث يستطيع جميع الأشخاص المستفيدين من خدمة الإنترنت وفي شتى أنحاء العالم أينما وجدوا وفي أي وقت من الاطلاع على كم هائل من المعلومات والأخبار الشاملة والمتجددة باستمرار، والشاملة لجميع الميادين السياسية والاقتصادية والثقافية والاجتماعية والدينية وغيرها، وغالباً ما تكون هذه الخدمة مجانية.

5- التجارة الإلكترونية:

وتعرف التجارة الإلكترونية بأنها كل نشاط أياً كانت طبيعته، يتعلق بتبادل السلع أو الخدمات، متى كانت مباشرة هذا النشاط تحدث على شبكات الاتصال عن بعد، وكان النشاط يمثل قيمة مضافة للمشروع أو المورد أو العميل" (البشري، 2005، 47).

6-محركات البحث Search Engine:

ومحركات البحث هي أبواب الإنترنت، ولولاها لما انتشرت الإنترنت إلى هذا الحد، فمحركات البحث هي ممر إجباري لكل باحث عن المعلومات على الإنترنت، لأنها تفهرس ملايين الصفحات، وتسمح بالبحث في هذه الفهارس، للحصول على نتائج سريعة بدلاً من البحث يدوياً على كامل الشبكة.

7-قوائم البريد الإلكترونية Electronic Mailing List:

وتستخدم لتبادل الآراء والنقاش حول موضوع معين بين مجموعة من الأشخاص، وهي أشبه بنظام التخاطب عبر الإنترنت (التحاور) (إبراهيم، 2009، 41-43).

المطلب الرابع: مكونات النظام المعلوماتي:

يشتمل نظام المعلومات المعاصر على خمسة من العناصر الأساسية التي تشكل الموارد الضرورية، والتي هي العنصر البشري، والمكونات المادية، والكيانات المنطقية، والبيانات، والشبكات، وسوف نعرضها بإيجاز كما يلي:

الفرع الأول: العنصر البشري Human Ware:

يعتبر الأفراد عنصراً هاماً من عناصر النظام المعلومات، ولولاهم لما اكتملت عناصره، فهم متطلب ضروري لإجراء العمليات في نظم المعلومات، وقد يكون الأفراد مستخدمين نهائيين لهذا النظام End Users، أو فنيين Specialists IS وهم المسؤولون عن تشغيل وإدارة نظم المعلومات من الناحية الفنية Systems Specialists Information.

وقد يكونون محللي النظم System Analysts، أو مطوري البرمجيات Software Developers، وقد يكونون مشغلي النظام System Operators أو خبراء البرمجة Programmers، أو مهندسي الصيانة والاتصالات ومديري النظم (إبراهيم، 2010، 20-21).

الفرع الثاني: مكونات النظام المعلوماتي المادية Hardware:

وتشمل مكونات النظام المعلوماتي المادية الحاسبات، والمكونات الرئيسة، واستخدامات النظام، والتخزين الخارجي، والأجهزة الملحقة، وذلك كما يلي:

أولاً- الحاسبات Computers:

تعتبر الحسابات من المكونات المادية للنظام المعلوماتي، ويمكن تصنيفها على أساس طبيعة عملها إلى نوعين رئيسين هما:

(أ) حاسبات قياسية Analog Computers:

وهي الحاسبات التي تتلقى مدخلاتها في صورة قياسات من مختلف أجهزة القياس (ضغط جوي، حرارة، ضغط دم...إلخ)، وتستخدم في التطبيقات العسكرية، والمجالات الطبية، والأبحاث العلمية، والاختبارات الصناعية.

(ب)حاسبات رقمية Digital Computer:

وهي التي تتلقى مدخلاتها (حروف، أرقام، رموز، رسوم، صوت، صورة،... إلخ)، ويتم تحويل هذه المدخلات إلى أرقام الصفر والواحد، حيث يعمل هذا النوع بنظام الرقم الثنائي Binary System، ويستخدم هذا النوع في المجالات العلمية والتجارية والترفيهية (فضالة، 1999، 17 وما بعدها).

وتقسم الحاسبات الرقمية إلى أربعة أنواع كما يلي:

1- الحاسب الفائق (الخارق) Super Computer: ويستخدم هذا النوع في رحلات الفضاء وتطوير عمليات التصنيع المتقدمة.
2- الحاسب الكبير Main Frame: ويستخدم في الشركات العالمية متعددة الفروع في العالم.
3- الحاسب الصغير Mini Computers: ظهر في فترة الستينات وتستخدم الدوائر المتكاملة في صناعته بدلاً من الترانزستورات، ومازال مستخدماً حتى الآن في نطاق محدد.
4- الحاسب الدقيق Micro Computer: ظهر هذا النوع في منتصف السبعينات وكثر انتشاره في بداية الثمانينات، وهو يعتمد على شريحة واحدة صغيرة تسمى Microprocessor، وهو أكثر أنواع الحاسبات انتشاراً، ويوجد منه نوع أصغر يسمى الحاسب المحمول Portable Computer، ونوع آخر أصغر قليلاً يسمى الحاسب المفكرة Notebook Computer (الملط، 2006، 29-30).

ثانياً- المكونات الرئيسة Main Computers:

تقسم المكونات الرئيسة لأي نظام معلوماتي إلى ثلاثة أجزاء رئيسة وهي وحدات الإدخال، ووحدات التشغيل، ووحدات الإخراج.

ثالثاً- استخدامات النظام:

هناك استخدامات عديدة لأنظمة المعلومات، والتي تتمثل في أغراض كثيرة منها أنظمة عامة الغرض، وأنظمة محدودة الغرض، فالأولى هي التي يتم تصميمها لكثير من الاستخدامات العلمية والتجارية والاجتماعية، والثانية تستخدم لعملية معينة أو عدد قليل من العمليات (إبراهيم، 2009، 27).

رابعاً- التخزين الخارجي Xeternal Storage:

وهي وحدات تخزين إضافية أو ثانوية، بقصد التوسع في كافة وحدات التخزين الخارجية، وتقسم إلى نوعين:

الأول وحدات التخزين المباشرة، وتمثلها الأقراص الممغنطة Magnetic Disks كالقرص المرن Floppy Disk، والقرص الصلب Hard Disk، والثاني وحدات التخزين التتابعية، وهي التي يمكن الوصول إلى أي بيان مسجل عليها بقراءة الشريط من بدايته إلى المكان المطلوب (إبراهيم، 2010، 22).

خامساً- الأجهزة الملحقة Accessories:

هناك العديد من وحدات الإخراج الأخرى التي ترتبط ارتباطاً وثيقاً بالنظام المعلوماتي، وذلك في مجال الصناعة، وماكينات الخياطة، والتريكو، والمثاقب وغيرها، والتي يتم ربطها بالحاسب الآلي لتشغيلها آلياً وفقاً لبرامج معينة تعتمد على المنتج المطلوب إنتاجه (طلبه وآخرون، 1992، 103).

الفرع الثالث: الكيانات المنطقية (البرامج) Software:

يعرف البرنامج بأنه تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقني معقد تسمى النظام المعلوماتي بغرض الوصول إلى نتيجة معينة، أو مجموعة من التعليمات المتتابعة بصفة منطقية توجه إلى الحاسب الآتي لأداء عمل أو أعمال معينة (الهادي، 1989، 110).

الفرع الرابع: البيانات Data:

البيانات يمكن أن تكون بأي شكل، ومن ضمنها البيانات الألفبائية والرقمية التقليدية التي تمثل وتوصف المعاملات، وتعتبر البيانات ذات قيمة عالية، لذا فإنها يجب أن تستثمر وتدار بشكل فعال لكي تؤمن الفائدة للمستخدم النهائي (إبراهيم، 2010، 23).

الفرع الخامس: الشبكات Networks:

ويقصد بالشبكات اتصال جهازين أو أكثر من أجهزة النظام المعلوماتي اتصالاً سلكياً أو لا سلكياً، أو هي حزمة من أجهزة الحاسبات المتصلة معاً، وقد تكون الأجهزة موجودة في نفس الموقع فتسمى شبكة محلية (L.A.N) اختصاراً Local Area Network، ويمكن أن تكون موزعة في أماكن متفرقة ويتم ربطها عن طريق خطوط التلفون وتسمى في هذه الحالة (W.A.N) اختصاراً لـ Wide Area Network، أي شبكة واسعة النطاق أو ممتدة (أحمد، 1997، 37 وما بعدها).

المبحث الثاني: ماهية المعلومات الإلكترونية:

سنتناول في هذا المبحث مطلبين الأول مدلول المعلومات الإلكترونية والثاني الطبيعة القانونية لهذه المعلومات وذلك كما يأتي

المطلب الأول: مدلول المعلومات الإلكترونية:

وسيتم تقسيم هذا المطلب إلى ثلاثة فروع الأول منها سوف نتناول فيه مفهوم المعلومات والثاني التمييز بينها وبين البيانات والبرامج والثالث سوف نتناول فيه الشروط الواجب توافرها في المعلومات الإلكترونية وذلك كما يلي:

الفرع الأول: مفهوم المعلومات:

يطلق الكثير على هذا العصر "عصر المعلومات" نظراً لما يشهده من تقدم هائل في مجال التقنية والتطور التقني الذي أدى إلى انتشار الحاسب الآلي وبشكل واسع في شتى مناحي الحياة، وذلك نظراً لما تُتيحَه هذه الحواسيب من إمكانات عالية، وبناءً على ذلك فقد انتشر في هذه الأيام ما يسمى بمراكز المعلومات التي تعتمد نظم المعالجة الآلية للبيانات وتجميع أكبر قدر من مصادر مختلفة، ومن ثم تخزين هذه المعلومات في مكان واحد واسترجاعها في أقصر وقت ممكن، إضافة إلى القدرة على عمل فهارس وبطاقات للمعلومات وتنظيمها، بحيث تعطي في النهاية صورة متكاملة عن شخص ما، أو تمثل قيما مالية ذات قيمة اقتصادية عالية انطلاقاً من معلومات تبدو لأول وهلة تافهة وعديمة الأهمية.

ومن هنا فإن إمكانية محاولة البحث عن هذه المعلومات من قبل أشخاص غير مخولين بها، وإمكانية توصلهم واطلاعهم عليها والتي تدخل في خصوصية صاحبها أو تمثل له أموالاً أو قيماً أو أصولاً تكون واردة إلى حد كبير، وهنا تكمن الخطورة في استخدام الحاسبات الآلية.

فالمعلومات المختزنة في جهاز الحاسوب أو المتداولة عبر شبكة المعلومات الدولية (الإنترنت) قد تكون عرضة إلى الإختراق غير قانوني من أشخاص غير مخولين بالاطلاع عليها. لذا سوف نورد بعض التعريفات التي جاءت بها القوانين وأيضاً الفقه كما يلي:

عرف المشرع الأمريكي المعلومات في قانون المعاملات التجارية الإلكترونية لسنة 1999 في الفقرة العاشرة من المادة الثانية بأنها "تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر والبرامج الموضوعة على الأقراص المرنة وقواعد البيانات أو ما شابه ذلك" (إبراهيم، 2009، 50).

وبالاطلاع على هذا التعريف يرى الباحث أن المشرع الأمريكي قد توسع في تعريف المعلومات الإلكترونية، حيث صورها بأي شكل من الأشكال، كما وأنه في نهاية التعريف جاء بعبارة أو ما شابه ذلك وهنا ترك الأمر مطلقاً على إطلاقه، وذلك لأن الجرائم المعلوماتية هي من جرائم التقنية الحديثة سريعة التطور وباستمرار وفي وقت قصير، ومن الصعوبة على أي مشرع السيطرة عليها فجاء المشرع الأمريكي بهذه العبارة تحسباً من ظهور أشكال جديدة للمعلومات، لا ينطبق عليها التعريف الوارد في القانون، وبالتالي يؤدي إلى إفلات المعتدي من العقاب.

وفي فرنسا ووفقاً للقانون رقم 82-652 الصادر في عام 1982 عرف المعلومة بأنها "صوت أو صورة أو مستند أو معطيات أو خطابات أيا كانت طبيعتها" (إبراهيم، 2010، 26).

أما المشرع الأردني فقد أورد تعريفاً للمعلومات في قانون المعاملات الإلكترونية الأردنية رقم 85 لسنة 2001 (والمنشور على الصفحة 6010 عدد الجريدة الرسمية 4524 تاريخ 2001/12/34)، حيث عرفها في المادة الثانية من هذا القانون بأنها "البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب ما شابه ذلك".

وعرف أيضا رسالة المعلومات في نفس المادة بأنها "المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية أو بوسائل مشابهة ، بما في ذلك تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ الرقمي".

ويتبين من التعريف السابق أن المشرع الأردني سار على نَهْج المشرع الأمريكي، حيث إنه أعطى المعلومات مفهوماً موسعاً وشاملاً، وجعلها على أي شكل من الأشكال وجاء في نهاية التعريف بعبارة.. وما شابه ذلك تحسبا لما قد يظهر من أشكال جديدة للمعلومات، وحسنا فعل المشرع الأردني فبهذه العبارة ترك الأمر مطلقاً على إطلاقه في محاولة منه للسيطرة على كافة الصور التي قد تستجد للمعلومات في المستقبل.

ولم يعرف المشرع الأردني المعلومات وفقا لقانون الاتصالات الأردني رقم 13 لسنة 1995، ولا وفقا لقانون حماية حق المؤلف لسنة 1992، ولا وفقا لقانون براءات الاختراع لسنة 1999، على الرغم من أنه سابقاً كان يعالج معظم صور الجرائم المعلوماتية بموجب هذه القوانين والقواعد التقليدية في قانون العقوبات، وذلك قبل صدور قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010، (والمنشور في الجريدة الرسمية الصفحة (5334) العدد (5056) تاريخ 2010/9/16م).

كما وأن المشرع الأردني لم يورد في قانون المعاملات الإلكترونية تعريفاً للبيانات والتي يتبين أنها تختلف عن المعلومات من الناحية الفنية إلا أنه وبموجب القانون المؤقت الجديد تدارك هذا النقص الحاصل في التعريفات.

وقد عرف المشرع الأردني المعلومات بموجب قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010 في المادة الثانية بأنها "البيانات التي تمت معالجتها وأصبحت لها دلالة".

وعرف أيضاً البيانات في ذات المادة بأنها "الأرقام والحروف والرموز والأشكال والأصوات والصور التي ليست لها دلالة بذاتها".

ومن هنا نجد أن المشرع الأردني وبموجب القانون الجديد قد أعطى للمعلومات تعريفاً ضيقاً وأكثر وضوحاً من التعريف الوارد في قانون المعاملات الإلكترونية الأردني، حيث إنه اعتبر المعلومات عبارة عن بيانات ولكن بعد معالجتها آلياً وأن تصبح لها دلالة واضحة وليست مبهمة، وبالتالي فالمعلومات قد تكون أرقاماً أو حروفاً أو رموزاً أو أشكالاً أو أصواتاً أو صوراً ولكن بعد معالجتها آلياً حتى تصبح لها دلالة.

كما وأن المشرع الأردني في القانون الجديد قد أخرج (برامج الحاسوب) من مفهوم المعلومات ففي السابق وبموجب قانون المعاملات الإلكترونية تعتبر برامج الحاسوب معلومات، إلا أنه أخرجها من مفهوم المعلومات، حيث عرف المشرع الأردني في القانون الجديد البرامج بأنها: "مجموعة من الأوامر والتعليمات الفنية المعدة لإنجاز مهمة قابلة للتنفيذ باستخدام أنظمة المعلومات".

وبهذه التعريفات الواردة في قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010م نجد أن المشرع الأردني قد فرق وبشكل واضح لا يترك مجالاً للشك أو التأويل بين المعلومات والبيانات والبرامج وهذا يُحسب وبحق للمشرع الأردني بأن تدارك النقص الوارد في قانون المعاملات الإلكترونية الأردني.

ومن القوانين العربية التي عرفت المعلومات قانون إمارة دبي بشأن المعاملات والتجارة الإلكترونية رقم (2) لسنة (2002)، حيث عرف المعلومات الإلكترونية بأنها "معلومات ذات خصائص إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج حاسب آلي أو غيرها من قواعد البيانات" (http://www.helmylawyers.maktoobblog.com).

وعرف قانون البحرين رقم 28 لسنة 2002 بشأن المعاملات الإلكترونية المعلومات بأنها "البيانات والنصوص والصور والأصوات والرموز وبرامج الحاسوب والبرمجيات ويمكن أن تكون قواعد البيانات والكلام" (http://www.ar.jurispedia.org.com).

أما قانون الإمارات الاتحادي رقم (2) لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات، فقد عرف المعلومات الإلكترونية بأنها "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها" (http://www.neuae.com/?p=25).

أما بالنسبة للفقه فقد عرف البعض المعلومات بأنها "النقل المجرد لوقائع معينة تم الحصول عليها من مصادر متعددة" ويعرفها البعض الآخر "بأنها كل شكل أو حالة خاصة لمادة أو طاقة قابلة للإعلان أو الإبلاغ، ويعرفها البعض بأنها البيانات التي تمت معالجتها لترتيبها وتنظيمها وتحليلها بقصد الإفادة منها (علي، 2003، 9).

ويعرفها البعض الآخر بأنها "رسالة ما معبر عنها في شكل جعلها قابلة للنقل أو الإبلاغ للغير" ويعرفها البعض الآخر بأنها "رمز أو مجموعة رموز تنطوي على إمكانية الافضاء إلى معنى" (الملط، 2006، 74).

ويرى الباحث أن المعلومات الإلكترونية هي عبارة عن مجموعة من الأرقام والحروف والرموز والأشكال والأصوات والصور، التي تمت ترجمتها ومعالجتها آلياً عن طريق الحاسب الآلي، وأصبحت لها دلالة بذاتها بحيث تسمح بتكوين محتوى معرفي للمستخدمين، وبالتالي تصلح لأن تكون محلاً للإرسال والنقل والتبادل والاتصال، سواء أكان ذلك بواسطة الأفراد أو الأنظمة الإلكترونية".

وبمعنى آخر فالمعلومات هي عبارة عن الحقائق والمفاهيم التي يتناقلها ويتبادلتها الأفراد عبر وسائل الاتصال المختلفة.

فالمعلومة هي تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير، وتتطلب المعلومات بطبيعتها وجود وسط تخزن فيه، وتختلف وسائط تخزين المعلومات، فقد تكون أ حباراً أو ألواناً، وقد يكون الوسط ذبذبات كهربائية في الفضاء كموجات الراديو، أو قطع ووصل إلكتروني كالإشارات الرقمية في الحواسيب الآلية، ولا شك أن التلاعب الذي يقع على هذا الوسط من شأنه أن يعرض المعلومات إلى الخطر (إبراهيم، 2009، 53).

الفرع الثاني: التمييز بين المعلومات والبيانات والبرامج:

يذهب البعض إلى وجوب التفرقة بين المعلومات والبيانات، فالبيانات هي الأرقام أو الكلمات أو الرموز أو الحقائق أو الإحصاءات الخام التي لا علاقة بين بعضها بعضا، أما المعلومات فهي المعنى الذي يستخلص من هذه البيانات بعد معالجتها (رستم، 1992، 26).

فهناك تفرقة فنية بين اصطلاحي البيانات والمعلومات فالبيانات Data هي المدخلات (Input) إلى جهاز الحاسب الآلي بهدف تشغيلها Processing ومعالجتها داخل الجهاز والحصول على المخرجات (Output) في صورة المعلومات Information (إبراهيم، 2010، 29).

ويذهب بعض الفقه إلى تعريف البيانات بأنها عبارة عن كلمات وأرقام ورموز وحقائق وإحصاءات خام لا توجد أية صلات بينها، وهي صالحة لتكوين فكرة أو معرفة بواسطة الإنسان أو الأدوات والأجهزة التي يسخرها وهي ما تسمى بالمعالجة الآلية، وكثيراً ما تستخدم البيانات كمرادف للمعلومات رغم الاختلاف في المعنى والمفهوم والدلالة (الملط، 2006، 77).

ويقول البعض أن البيانات هي المعطيات المتصلة بجهة معينة، والمعلومات هي المعنى المستخلص منها بعد معالجتها، فالبيانات هي المدخلات للنظام المعلوماتي ومن قبيل ذلك تعرف البيانات بأنها "مجموعة من الحقائق تعبر عن مواقف وأفعال معينة حدثت في الماضي أو الحاضر أو ستحدث في المستقبل، سواء أكان التعبير بالكلمات أو الأرقام أو الأشكال أو الرموز".

أما المعلومات فهي "بيانات خضعت إلى التشغيل والتحليل والتفسير لتحقيق زيادة المعرفة لمتخذي القرارات، ومساعدتهم لتحقيق أغراض معينة، وتمكينهم من الحكم السديد على الظواهر والمشاهدات" (رستم، 1992، 26).

ونخلص مما سبق أن البيانات هي مجموعة المدخلات إلى جهاز الحاسوب، سواءَ أكانت رموزاً أم حروفاً أم أشكالاً أم أصواتاً أم صوراً أو غيرها، والتي ليس لها دلالة بذاتها، أما المعلومات فهي البيانات التي تمت معالجتها عن طريق الحاسب الآلي، وأصبحت قادرة على تكون المعرفة والحقائق والمفاهيم لدى المستخدمين، من أجل الإفادة منها فأصبحت لها دلالة.

أما البرامج فهي التعليمات الموجهة إلى جهاز الحاسب الآلي، بغرض الوصول إلى نتيجة معينة، أو مجموعة من التعليمات المتتابعة بصفة منطقية توجه إلى الحاسب الآلي لأداء عمل أو أعمال معينة (الهادي، 1989، 110)

الفرع الثالث: الشروط الواجب توافرها في المعلومات الإلكترونية للتمتع بالحماية القانونية (خصائصها):

تتحدد للمعلومات قيمة بوصفها ناتجة عن نشاط إنساني، ويجب أن تتوافر فيها بصفة عامة بعض الشروط والخصائص سواء أكانت مثبتة على وسيط مادي (دعامات) أم كانت بمعزل عن هذا الوسيط - حتى تتمتع بالحماية القانونية اللازمة، وبمعنى آخر أن هذه الخصائص إذا توافرت في المعلومة وتم الاعتداء عليها أو حيازتها والاستيلاء عليها بطريقة غير مشروعة من قبل الغير، فإن ذلك يشكل خرقاً للقانون، ويرتب المسؤولية الجزائية.

وتتمثل هذه الخصائص أو الشروط فيما يلي:

أولاً: التحديد والابتكار:

حتى تكون المعلومة موجبة للحماية القانونية يجب أن تكون محددة، وتعتبر هذه من الخصائص الأساسية لها، فصحيح أن المعلومة خاصة بصاحبها إلا أنه وفي بعض الأحيان قد يخصصها للإرسال ويبلغ بها الغير، فحتى تكون صالحة للتبليغ للغير والنقل والإرسال والتداول يجب أن تكون محددة وبشكل حقيقي، وبعكس ذلك فإنها تكون معلومة غير حقيقية وغير صالحة للتبليغ للغير عن طريق علامات أو إشارات مختارة، فالتبليغ الحقيقي يفترض أن تكون المعلومة محددة، وخاصة إذا كانت تتعلق بالمال، فالتحديد يصبح أكثر ضرورة م تى كان الاعتداء على الأموال التي تمثلها هذه المعلومة، فهذا الاعتداء يتطلب دائماً أن يقع على شيء محدد، وهو المعلومات المحددة التي تمثل المال (حسبو، 2000، 32).

أما بالنسبة للابتكار فحتى تنسب المعلومات إلى شخص معين أو أشخاص معينين بالذات، يجب أن ينسب ابتكارها له ابتداءَ ومن ثم تلتصق به وتصبح معلومة مُبتكرة من قبله وليست عامة شائعة للجميع، وبعكس ذلك تكون معلومة عامة غير مبتكرة وغير خاصة بشخص أو أشخاص معينين بالذات، وتكون شائعة وفي متناول الجميع (إبراهيم، 2010، 31).

ومن هنا يجد الباحث أن المعلومة يجب أن تكون محددة وخاصة وقاصرة على فرد أو أفراد معنيين بالذات دون غيرهم وتحمل ابتكاراً أو إضافة يكون هؤلاء الأفراد هم مصدرها. حتى ترتبط بهم فإذا كانت متاحة للكافة حتى لو كانت مهمة وليست مبتكرة من قبل أحد الأشخاص فإنها لا تكون محلاً للاعتداء وبالتالي ليست محلاً للحماية.

ثانياً: السرية و الاستئثار:

يجب أن تتصف المعلومات بالسرية، ومعنى السرية أن تقتصر هذه المعلومات على شخص معين أو أشخاص معينين، وأن تنحصر حركة الرسالة التي تحمل هذه المعلومات بين أشخاص محددين وليست للكافة، فالمعلومة غير السرية تكون متداولة بين الجميع وقابلة للنقل وبسهولة، ومثالها الأخبار المنشورة على المواقع الإخبارية في الإنترنت، والحقائق المنشورة على صفحات الإنترنت كدرجة الحرارة والضغط الجوي، أو تلك التي ترد على الزلازل والبراكين أو الفيضانات، فهذه جميعها معلومات ليست سرية وفي متناول الكافة، وغير مقتصرة على دائرة معينة من الأشخاص (الشوا، 1994، 175 وما بعدها).

وعندما تتصف المعلومة بطابع السرية فإنها تكون قابلة للحيازة من قبل صاحبها ومنحصرة في دائرة محددة من الأشخاص، ومن هنا يمكن القول بأنه لا يمكن تصور الجرائم الخاصة بالسرقة والاحتيال وإساءة الائتمان إذا انعدم هذا الحصر (قوره، 2005، 113-114).

ويمكن تحديد طابع السرية للمعلومة عن طريق ثلاثة معايير:

الأول: طبيعة المعلومة كاكتشاف شيء كان مجهولاً سابقاً.

الثاني: إرادة الشخص نفسه كاكتشاف مجال حديث للإدارة بواسطة رئيس شركة ما والاحتفاظ بسريته.

الثالث: وهما المعياران السابقا ن معاً كما هو الحال بالنسبة للرقم السري في البطاقات الائتمانية.

فالطابع السري وفقاً لهذه المعايير يقلل من تداول هذه المعلومات بين الكافة، ويقصره على دائرة محددة وهي دائرة المؤتمنين عليها فقط (الشوا، 1994، 176).

وتعتبر السرية من أهم الشروط والخصائص التي لابد من توافرها في المعلومات حتى تتم حمايتها قانونياً، ولكن لا يشترط أن تكون درجة السرية هذه مُطلقة، ومعنى ذلك أن المعلومات لا تفقد هذا الطابع وتبقى سرية حتى لو عرفها عدد غير محدود من الأشخاص، وذلك حسب طبيعة التعامل الذي قد يتطلب اطلاع البعض على سرية هذه المعلومات (إبراهيم، 2009، 57-58).

والمثال على ذلك إذا كانت المعلومات خاصة ومعروفة لمشروع استثماري معين كونها تدخل في حيازته، فإن اطلاع عدد محدد من المشاريع الأخرى المنافسة والتي تعمل في نفس المجال على هذه المعلومات لا يفقدها طابع السرية ولا تعتبر في هذه الحالة أنها معلومات متداولة لجميع الشركات، وإنما هي معلومات سرية للشركة الأم، إلا أن طبيعة النشاط الذي تعمل فيه يستوجب اطلاع عدد محدد من المشاريع المنافسة على هذه المعلومات وهنا تبقى المعلومات تتصف بطابع السرية (إبراهيم، 2010، 32).

ومن التطبيقات القضائية حول موضوع سرية المعلومات في إحدى القضايا التي نظرتها محكمة الاستئناف الفيدرالية في الولايات المتحدة الأمريكية وهي قضية (V. National Fund Raising Consultants, Inc):

وتتلخص وقائعها في أنه ثار نزاع بين طرفين بشأن تنفيذ عقد فرنشايز كان قد أبرم بينهما، ومن المعلوم أن عقود الفرنشايز هي من العقود التي تستوجب الترخيص باستغلال الإسم والعلامة التجارية، ويلتزم المرخص بموجب العقد بتزويد المرخص له بالمعرفة والخبرة الفنية اللازمة للإنتاج، وعند طرح القضية على محكمة الاستئناف الفيدرالية الأمريكية كان النزاع يدور حول مدى اعتبار المعلومات التي قدمت من الشركة المرخصة وهي شركة NFRC إلى المرخص له بمناسبة عقد الفرنشايز المبرم بينهما تعد من الأسرار التجارية، وبعد أن استعرضت المحكمة العناصر الواجب توفرها في الأسرار التجارية وفقاً للقسم 759 من مدونة القانون الأمريكي بشأن المسؤولية عن الفعل الضار لسنة 1939 Restatement of Torts، حيث استخلصت المحكمة أن الشركة المرخصة بذلت جهداً في تجميع المعلومات التي قدمتها للمرخص له، وقدمت له برامج تدريب من الصعب عليه الحصول عليها من مصادر أخرى، فقضت المحكمة في قرارها بتأمين قرار هيئة المحلفين من حيث وقوع اعتداء على الأسرار التجارية الخاصة بالشركة المرخصة (الصغير، 2007، 29).

أما بالنسبة للاستئثار فهو أمر ضروري للمعلومات حتى تتمتع بالحماية القانونية اللازمة، فالمشرع التقليدي يتطلب في الجرائم التقليدية وعندما يحدث اعتداء على القيم أو المال أو الأصول أن يكون الجاني قد استأثر بسلطة أو قيمة أو مال يخص الغير وعلى نحو مطلق، أما فيما يتعلق بالمعلومات فذكرنا ابتداءَ أن من صفات المعلومة السرية وأن تكون مقتصرة على دائرة أشخاص معينين، وبالتالي فإن الاستئثار في مجال المعلومات يمكن أن يرد عن طريق الدخول في هذه المعلومات والمخصصة لأشخاص معينين بالذات، وعندها يكون الاستئثار من حق صاحب المعلومة أو مؤلفها، وبهذا الاستئثار تتولد رابطة معينة بين المعلومة ومؤلفها أو صاحبها هذه الرابطة تسمى رابطة الأبوة (سلامة، 2006، 77).

ورابطة الأبوة هذه يمكن الاعتراف بها في حالتين هما:

الأولى- إذا وردت المعلومة على حقيقة أو حدث:

وهنا تكون معلومة عامة وشائعة للجميع وبإمكان أي كان أن يقوم بالاستيلاء عليها، أما إذا قام شخص بتجميع وحفظ هذه المعلومة فهنا يكون وكأنه أنشأ معلومة جديدة وتصبح في حيازته وتتولد رابطة الأبوة بينه وبين هذه المعلومة.

الثانية- إذا وردت المعلومة على فكرة أو عمل ذهني:

وفي هذه الحالة فإن صاحب هذه الفكرة أو العمل الذهني يكون مالكاً لها، وتتولد الرابطة المذكورة بينهما، فإذا قام الغير بالاستيلاء على هذه المعلومات دون وجه حق، فإن ذلك يُرتب المسؤولية الجزائية . (قورة، 2005، 114-115)

ويرى الباحث أنه وبعيداً عن المعلومات الوارده على شكل مصنفات أدبيه أو فكريه أوفنيه أو صناعيه والمحميه بموجب قوانين الملكيه الفكريه فحتى تتمتع المعلومات المعالجه آلياً بالحماية القانونية وترتب المسؤولية الجزائية في حال الاعتداء عليها من قبل الغير، فإنها يجب أن تتسم بطابع السرية بأن تكون مقتصرة على شخص معين أو أشخاص معينين، وأن تكون حركة الرسائل التي تتعلق بهذه المعلومات مقتصرة على هذه الدائرة فقط وليست مباحة للجميع، وأن تتسم أيضاً بطابع الاستئثار وتكون كذلك إذا كان الوصول إليها غير مصرح به إلا من قبل صاحبها أو أشخاص محددين، بحيث ترد رابطة بين المعلومات وصاحبها أشبه ما تكون برابطة الأبوة.

المطلب الثاني: الطبيعة القانونية للمعلومات:

وسوف نبحث هذا الموضوع من خلال دراسة الطبيعة القانونية للمعلومات الإلكترونية وأنواع هذه المعلومات وذلك كما يأتي:

الفرع الأول: الطبيعة القانونية للمعلومات:

ثار خلاف فقهي حول الطبيعة القانونية للمعلومات وذلك بالنظر إليها بعيداً عن الطبيعة المادية التي يمكن أن تندمج فيها(الدعامات الماديه) ، ووفقاً لهذا الموضوع فإنه يثور تساؤل هام هنا، هل المعلومات لها طبيعة مادية؟ وهل يمكن اعتبارها مالاً بالمفهوم التقليدي للمال والقابل للاستئثار؟ وهل يمكن أن تكون محلاً للاعتداء وبالتالي محلاً للحماية الجزائية؟ أم أن لها طبيعة من نوع خاص ولا يمكن اعتبارها من قبيل القيم أو المال التي يرد الاعتداء عليها في الجرائم التقليدية، وبالتالي لا تحميها قوانين العقوبات التقليدية، وبمعنى آخر إذا كانت المعلومات ذات طبيعة خاصة (معنوية) غير مادية وغير ملموسة، فكيف يمكن حمايتها جنائياً.

و بناءً على ذلك فقد انقسم الفقه إلى اتجاهين:

الأول: يرى أن المعلومة لها طبيعة من نوع خاص.

والثاني: يرى أن المعلومة ما هي إلا مجموعة مستحدثة من القيم (العريان، 2004، 49).

وسنبين ذلك بشيء من التفصيل كما يلي:

1- الاتجاه الأول التقليدي- للمعلومة طبيعة من نوع خاص (أو الطبيعة الذاتية للمعلومة):

يرى أصحاب هذا الاتجاه أن للمعلومة طبيعة من نوع خاص، نتيجة للفكر التقليدي الذي يعتمدونه في تحديد الجرائم، فالفكر التقليدي يقوم على توفير الحماية القانونية فقط للأشياء المادية الملموسة، ويعتبرها قيماً مادية يمكن حمايتها من الاعتداءات التي قد تقع عليها، وبمعنى آخر اعتبر أصحاب هذا الاتجاه أن الأشياء المادية الملموسة هي التي يمكن الاستئثار المادي بها وهي التي تعتبر قيماً وتكون محلاً للاعتداء، وبالتالي تستوجب الحماية الجزائية (ميلاد، 2007، 28-29).

أما المعلومات فقد اعتبرها أصحاب هذا الرأي ذات طبيعة معنوية غير ملموسة، وبالتالي لا يمكن اعتبارها مالاً أو قيماً فهي أشياء غير مادية وغير ملموسة. لا يمكن الاستئثار المادي بها أو الاستحواذ عليها أو حيازتها (السعدي، 2004، 26)، وعلى ذلك فإن المعلومات المختزنة في النظام المعلوماتي والتي لا تنتمي إلى أي من المواد الأدبية أو الذهنية أو الصناعية لا تندرج حتماً في مجموعة القيم المحمية قانونياً (سلامة، 2006، 88-89).

ومعنى ذلك أن المنهج التقليدي اشترط لاعتبار الأشياء من قبيل القيم أو الأموال أن تكون ذات طبيعة مادية وقابلة للتملك، وبالتالي فإن هذه الأشياء المادية تكون محلاً للحق الاستئثاري، وهذا لا ينطبق سوى على المال والقيم.

أما المعلومات فهي ذات طبيعة معنوية غير مادية وغير ملموسة، وبالتالي فهي أشياء معنوية لا يمكن تملكها، ولا تكون محلاً للحق الاستئثاري وفقاً لهذا الاتجاه التقليدي إلا إذا كانت من قبيل حقوق الملكية الأدبية أو الفنية أو الصناعية، غير أن المعلومات المختزنة في الحاسب الآلي أو المتدفقة برأيهم لا تنتمي إلى المواد الأدبية أو الذهنية أو الصناعية، ولذلك فهي مستبعدة من دائرة الأموال والقيم الجديرة بالحماية القانونية.

ومع ذلك فالأمر مستقر عند أصحاب هذا الرأي بالاعتراف بوجود خطأ قانوني في حالة الاستيلاء على معلومات الغير، وقد حاولوا حماية هذه المعلومات عن طريق دعوى المنافسة غير المشروعة، وذلك استناداً إلى حكم محكمة النقض الفرنسية "إن الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استئثاري (العريان، 2004، 49).

2- الاتجاه الثاني الحديث- المعلومة مجموعة مستحدثة من القيم (الأموال):

وقد جاء بهذا الاتجاه فقهاء متخصصون ومهتمون بموضوع الجرائم المعلوماتية وتكنولوجيا المعلومات، نتيجة للمشاكل الناشئة عن تزايد هذه الظاهرة الإجرامية، حيث حاول هؤلاء الفقهاء تطبيق النصوص التقليدية الواردة في قوانين العقوبات الوطنية على الاعتداءات والجرائم التي تقع على النظام المعلوماتي، وذلك بتطبيق وصف المال المادي والذي يكون محلاً للحق الاستئثاري على المعلومات الإلكترونية، ويرجع الفضل لأنصار هذا الاتجاه إلى كل من الأستاذين CATALA وVIVANT، على الرغم من اختلاف أسلوب كل منهما إلا أنهما يصبان في نفس النتيجة وهي توفير الحماية الجزائية للمعلومات الإلكترونية في النظام المعلوماتي (محمود، 2002، 167).

وتعتبر المعلومة وفقاً لمنهج الأستاذ CATALA واستقلالاً عن دعامتها المادية قيمة قابلة للاستحواذ، ويبرر ذلك بأن المعلومة عبارة عن سلعة أو منتج بصرف النظر عن دعامتها المادية، وهذه المعلومة تكون متداولة في السوق كالسلع والمنتجات المادية، وهي تقوم وفقاً لسعر السوق طالما أنها غير محظورة تجارياً، ويقول الأستاذ CATALA أيضاً أن هنالك علاقة قانونية تنشأ بين المعلومة وبين مؤلفها، وهذه العلاقة هي علاقة المالك بالشيء الذي يملكه، وهذه المعلومة خاصة بمؤلفها لوجود رابطة التبني التي تجمع بينهما (الشوا، 1994، 182-183).

وقد اعتمد هذا الرأي على حجتين لانطباق وصف القيمة على المعلومة.

الأولى: قيمتها الاقتصادية، ومفاد ذلك أن المعلومة كالسلعة أو المنتج لها قيمتها الاقتصادية، وتباع وتشترى وتستوجب الحماية القانونية.

والثانية: وجود علاقة تبني تجمع بين المعلومة ومؤلفها، وبالتالي فهي قابلة للحيازة والملكية من قبل صاحبها، وتستوجب الحماية الجزائية (العريان، 2004، 50).

أما الأستاذ Vinant فقد تبنى هذا الاتجاه واعتمد على حجتين هما:

الأولى: واستمدها من كل من الأستاذين (Piper & Palaniol) ومؤداها أن فكرة الشيء أو القيمة أو المال لها صورة معنوية، وأن نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات طابع اقتصادي، وأن تكون هذه القيمة جديرة بالحماية القانونية (سلامة، 2006، 92).

والثانية: يرى فيها أن كل الأشياء المملوكة ملكية معنوية والتي يعترف بها القانون، ترتكز على الإقرار بأن المعلومة قيمة عندما نكون بصدد براءة اختراع أو علامات أو رسومات أو من قبيل حق المؤلف، ومنشيء هذه المعلومة هو الذي يقدح ويكشف ويطلع الجماعة على شيء ما، بغض النظر عن الشكل أو الفكرة، فهو يقدم لهم المعلومة بمعنى واسع لكنها خاصة به، ويجب أن تعامل هذه المعلومة بوصفها مالاً وتصبح محلاً للحق، فلا يوجد ما يسمى بالملكية المعنوية بدون الاعتراف بالقيمة المعلوماتية (محمود، 2002، 171).

ومن وجهة نظر Vivant فإن المعلومة هي من قبيل المال بسبب قيمتها الاقتصادية، ويمكن أن تكون هذه المعلومة محلاً لعقد بيع طالما أن الإبداع يرتبط بصاحبه، ولصاحب هذه المعلومة أن يتنازل عنها بموجب عقد أو يقيد استخدامها أو أن يرفضه (الشوا، 1994، 186).

فالمعلومة وفقاً لأصحاب هذا الاتجاه هي قيمة بحد ذاتها وقابلة لأن تكون محلاً لعقد أو البيع أو التنازل وغيرها.

ويرى بعض الفقهاء أن المعلومات هي محل جرائم الحاسوب والإنترنت فهذه الجرائم إنما هي أنماط السلوك الإجرامي التي تطال المعلومات المخزنة أو المعالجة في نظام الحاسوب أو المتبادلة عبر الشبكات. وهي إما أن تُجسد أو تُمثل أموالاً أو أصولاً أو أسراراً أو بيانات شخصية أو لها قيمة بذاتها كالبرامج، فالجرائم المعلوماتية تستهدف الحق في المعلومات ويمتد تعبير الحق في المعلومات ليشمل الحق في انسيابها وتدفقها والحق بالمعلومات بذاتها أو بما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية (نبيه، 2008، 94-95).

ويرى البعض أن المعلومات تعد أموالاً منقولة مقومة بالمال وبالتالي يجوز أن يرد عليها جميع أنواع التعاملات التجارية وتتمتع بحماية القانون باعتبارها مال مقوم، ويستوي في ذلك أن تكون مبتكرة أو غير مبتكرة، فإذا كانت مبتكرة فهي محمية بتشريعات حماية حق المؤلف، وإن لم تكن مبتكرة فهي تعد محمية طبقاً للقواعد العامة في القانون المدني (إبراهيم، 2008، 24).

ومما تقدم فإن الباحث يذهب مع الاتجاه الحديث مع وجود بعض القيود، فصحيح أن للمعلومات طبيعة معنوية إلا أنه بتوافر صفات الذاتية والاستقلال لهذه المعلومات فإنها تعد قيمة بحد ذاتها دون ارتباطها بالوسائط المادية (الدعامات)، وهي تملك قيمة اقتصادية معينة وترتبط بمالكها برابطة المالك بالشيء الذي يملكه، إلا أن هذه الملكية معنوية وفقا للنظام المعلوماتي، وهذه المعلومات تختلف عن المعلومات التي تدخل في إطار الملكية الأدبية والفنية والصناعية والمحمية بموجب قوانين الملكية الفكرية، فهي معلومات معالجة آليا عن طريق النظام المعلوماتي والمخزنة في الحاسب الآلي أو متداولة عبر الشبكة، ولا تنتمي إلى المواد الأدبية أو الذهنية أو الصناعية، وبالتالي فإنها يمكن أن تكون محلاً للاعتداء ولابد من حمايتها الحماية القانونية اللازمة، وتماشياً مع مبدأ شرعية الجرائم والعقوبات، ومبدأ عدم جواز القياس في النصوص الجزائية، فإن الباحث يرى أن هذه المعلومات لا يمكن أن تكون محلاً للجرائم التقليدية المنصوص عليها في قوانين العقوبات التقليدية، لأن لها طبيعة من نوع خاص (معنوية) تختلف عن طبيعة المال المنقول (المادية) والمقصود في قوانين العقوبات، حتى مع الاعتراف بأن هذه المعلومات تشكل قيماً اقتصادية، وتتمتع بصفات الذاتية والاستقلال وإم كانية اعتبارها سلعاً تباع وتشترى كالمال، وإمكانية أن تكون محلاً للعقود شأنها شأن المال، إلا أن طبيعتها المعنوية غير المادية وغير المحسوسة تجعلها بعيدة كل البعد عن وصف المال المنقول المقصود في القوانين التقليدية في جرائم السرقة والإحتيال وغيرها ، فالباحث يتفق مع أصحاب الاتجاه الحديث بضرورة توفير الحماية الجنائية للمعلومات المخزنة في الحاسب الآلي أو المتداولة عبر الإنترنت، ويذهب مع أصحاب الاتجاه التقليدي في عدم إمكانية تطبيق النصوص التقليدية على الجرائم المعلوماتية، فهي بحاجة إلى نصوص تُراعى فيها الطبيعة المعنوية للمعلومات.

وفي أيامنا هذه أصبحت المعلومات الإلكترونية أحد المصالح الأساسية المستهدفة بعد النقود، وهي المنفذ إلى اقتصاد السوق، فقد تكون هذه المعلومات ذات قيم مالية خاصة بالأموال والاستثمارات للمنشآت العامة أو الخاصة، وقد تكون تجارية وصناعية تتعلق بالدراسات الخاصة بالأسواق

ومشروعات الاستثمار والتصنيع والإنتاج والتجارة والتوزيع والأبعاد ومراكز البيع والقطاع الصناعي للإنتاج، وقد تكون شخصية مخزنة في أنظمة الحواسيب الآلية وخاصة في البنوك وشركات التأمين ولدى المحامين والمستشفيات والأجهزة الأمنية والأحزاب والنقابات، وبالتالي فالاعتداء عليها يهدد المراكز المالية للشركات والأفراد وغيرهم ويهدد سرية الحياة الخاصة أو الحرية النقابية والسياسية وغيرها، وقد تكون هذه المعلومات عسكرية واقتصادية تتضمن أسرار الدولة ومشاريع الصناعات العسكرية الحديثة والمشاريع النووية والمشاريع الاقتصادية في الدولة، وبالتالي فالاعتداء عليها ينطوي على أخطار جسيمة تطال الدول، من هنا نجد أن المعلومات المخزنة في النظام المعلوماتي هي ذات أصول أو قيم اقتصادية أو سياسية أو مالية أو أدبية عالية على الرغم من طبيعتها المعنويه وبالتالي لابد من حمايتها من الاعتداء بطريقة قانونيه تتفق مع هذه الطبيعه .

الفرع الثاني: أنواع المعلومات:

تقسم المعلومات إلى ثلاث طوائف هي المعلومات الإسمية، والمعلومات الخاصة بالمصنفات الفكرية، والمعلومات المباحة (إبراهيم، 2009، 29).

وسوف نتناولها بشيء من التفصيل على النحو التالي:

الطائفة الأولى- المعلومات الاسمية: Information nominatives

ويقسم هذا النوع من المعلومات إلى مجموعتين وهما المعلومات الموضوعية والمعلومات الشخصية.

1- المعلومات الموضوعية: Information objectives

وهي تلك المعلومات المرتبطة بشخص المخاطب بها مثل اسمه، موطنه، حالته الاجتماعية، وهذه المعلومات غير متداولة، وغير شائعة للجميع، فلا يجوز الدخول إليها والاطلاع عليها إلاّ بموافقة صاحبها أو بأمر من السلطات المختصة (إبراهيم، 2010، 29).

2- المعلومات الشخصية:

يقصد بالمعلومات الشخصية المعلومات المنسوبة إلى الغير للإدلاء برأيه الشخصي فيها، ونجد أن هذه المعلومات تتفق مع المعلومات الموضوعية في أنها منسوبة إلى شخص معين في الذات، فالموضوعية منسوبة إلى الشخص المخاطب والشخصية منسوبة إلى الغير الذي أدلى برأيه فيها، وتختلف الشخصية في أنها موجهة إلى الغير وليست مرتبطة بشخصية صاحبها، ومثالها مقالات الصحف، الملفات الإدارية للعاملين لدى جهة معينة (إبراهيم، 2009، 55).

الطائفة الثانية- المعلومات الخاصة بالمصنفات الفكرية:

وهي عبارة عن المعلومات التي تكون على شـكل مصـنفات فكرية سـواء أكانت تتعلق بالملكية الأدبية الفنية أو الملكية الصـناعية، ونتيجة لذلك فإن رابطة الأبوة تنشـأ بين هذه المعلومات وبين مؤلفيها، ويكون لهم حق الاستئثار فيها، ولهم حقوق مالية وأدبية عليها (محمود، 2002، 161).

الطائفة الثالثة- المعلومات المباحة: Information Vacantes

ويقصـد بها تلك المعلومات التي تكون متداولة بين الكافة، ويسـتطيع أي كان الحصـول عليها دون إذن من صاحبها، ومثالها النشرات الجوية، وتقارير البورصة (مراد، لات، 50).

وإذا قام شـخص ما بجمع هذه المعلومات المباحة وصـياغتها بشـكل جديد فإنها تصـبح معلومات جديدة وخاصة بهذا الشخص وتنسب ملكيتها إليه، ويمكن القول إن هذه المعلومات إذا تم تجميعها بغرض معالجتها وتخزينها على جهاز الحاسب الآلي أو بقصد صياغة معلومات جديدة فإنها تقسم كما يلي:

أ- المعلومـات المعالجة: وهي المعلومات التي يقوم صـاحبها بجمعها وإدخالها إلى جهاز الحاسـب الآلي لمعالجتها آلياً بقصد تخزينها وحفظها فيه واسترجاعها وقت الحاجة.

ب- المعلومات المتحصـلة: ويقصد بها المعلومات التي يقوم صاحبها بجمعها ومعالجتها من معلومات أخرى ويتقرر له حق الملكية فيها طبقاً لقاعدة حيازة المال المنقول (إبراهيم، 2010، 30).

المبحث الثالث: الجريمة المعلوماتية والمجرم المعلوماتي:

وقد تم تقسـيم هذا المبحث إلى ثلاثة مطالب رئيسـه وذلك من خلال دراسـة مدلول الجريمة المعلوماتية وأركانها، والمجرم المعلوماتي كما يلي:

المطلب الأول: مدلول الجريمة المعلوماتية:

إن مفهوم الجريمـة المعلومـاتيـة يتسـع ليشـمـل مجموعـة من الجرائم والاعتداءات التي تطال المعطيـات المعنوية للحاسـب الآلي والنظام المعلوماتي، وتعتبر الجريمة المعلوماتية جريمة مسـتحدثة غزت العـالم منـذ منتصـف القرن العشـرين، حيـث جاءت هذه الجريمة الحديثة مرتبطة ارتباطاً مباشراً بتقنية التكنولوجيا والمعلومات والاتصـالات، ومنذ ظهور هذا النوع من الجرائم حاولت تشـريعات الدول وضـع قوانين تتناسـب وخطورة هذه الجرائم، للسـيطرة عليها ومحاولة الإلمام بكافة صورها وعدم ترك الفرصة لأي كان بأن يعبث في التقنيات الحديثة الخاصة بتكنولوجيا المعلومات،

وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض وعدم الوضـوح، ومما لا شـك فيه فقد حاول الفقه والدراســات القانونية في هذا المجال وضــع تعريف جامع مانع لهذه الجريمة، إلا أن الفقه لم يتفق على تعريف محـدد لهـا، وذلـك لأن هـذه الجرائم هي من صــنف جـديـد ارتبط بمعـالجـة البيانات والمعلومات والبرامج أي المكونات المعنوية للحاســب الآلي، وقد أدى ذلك إلى ظهور نوع جديد من المجرمين انتقل بالجريمة من صـورتها التقليدية إلى أخرى إلكترونية قد يصـعب التعامل والسيطرة عليها، وقد نتج عن ذلك تعذر إيجاد فهم مشـترك ومحدد لظاهرة الجريمة المعلوماتية، وما يستتبع ذلك من صعوبة مواجهتها – وتعذر إيجاد تشريعات جامعة ومانعة للسيطرة عليها ومنع اختراق النظام المعلوماتي.

وبناء على ما تقدم فإننا ســوف نحاول من خلال هذا المطلب الوصــول إلى تعريف محدد لظاهرة الجرائم المعلوماتية، بعد التطرق إلى الاتجاهات الفقهية المختلفة حول تعريفها، ثم بعد ذلك نبين خصائصها، ومحلها ومخاطرها.

الفرع الأول: تعريف الجريمة المعلوماتية:

اختلف الفقـه حول تعريف الجرائم المعلومـاتيـة، وقد بذلت محاولات عديدة تســعى إلى إيجاد تعريف مناسب لتلك الجرائم وإن كانت لا تخرج جميعها عن اتجاهين:

الأول: اتجاه يضـيق من مفهوم الجريمة المعلوماتية، بحيث تقل الحالات التي يمكن أن يتصـف فيها النشاط الإجرامي.

الثـاني: اتجـاه يوســع من مفهوم الجريمـة المعلوماتية، بحيث يوســع من الحالات التي تنطبق عليها هذه الجرائم إلى الحد الذي يدخل أفعالاً لا يمكن أن تعد من قبيل جرائم الحاسب الآلي (قوره، 2005، 28 وما بعدها).

وسوف نعرض كلاً من الاتجاهين على حدة كما يلي:

(1) الاتجاه الأول- الاتجاه الذي يضيق من مفهوم الجريمة المعلوماتية:

يذهب أنصـار هذا الاتجاه إلى تعريف الجريمة المعلوماتية بأنها "كل فعل غير مشروع يكون العلم بتكنولوجيـا الحاســبـات الآليـة بقـدر كبير لازماً لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى" (ســلامة، 2006، 11-12)، وقد عرفت وزارة العدل الأمريكية الجريمة المعلوماتية وذلك في دراســة وصــفها معهـد ســتـانفور للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفتها أنها "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها" (http/www.oecd.org.com).

ومن خلال البحث في معطيات هذه التعريفات فإنه حتى يكون الفعل المرتكب فعلاً جرمياً ويدخل ضمن دائرة الجرائم المعلوماتية، لابد أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من العلم بتكنولوجيا المعلومات والحاسب الآلي لارتكاب الجريمة وتحقيقها، ويذهب أنصار الاتجاه المضيق إلى أن الجرائم التي تفتقر إلى العلم بهذه التكنولوجيا وعلى قدر عال، فإنها ليست بحاجة إلى تشريعات خاصة تضبطها وتسيطر عليها، وإنما يمكن معالجتها بالنصوص التقليدية، وذلك على خلاف الجرائم التي تتوافر لها المعرفة العالية فهي تكون بحاجة إلى نصوص خاصة تتوافق مع طبيعتها المستحدثة والتقنية والمختلفة عن الجرائم التقليدية.

وقد عرف بعض أنصار هذا الاتجاه الجريمة المعلوماتية بأنها "كل نشاط غير مشروع، موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر، أو تلك التي يتم تحويلها عن طريقه" (إبراهيم، 2009، 74).

ومعنى ذلك أن الجرائم المعلوماتية وفقاً لرأيهم هي الجرائم التي ينصب فيها النشاط الإجرامي على الحاسب الآلي أو داخل نظامه. أي الكيانات المعنوية، وتخرج من نطاقها الجرائم التي يكون الحاسب الآلي أداة لارتكابها.

(2) الاتجاه الثاني- الاتجاه الموسع من مفهوم الجرائم المعلوماتية:

ذهب بعض أنصار هذا الاتجاه إلى تعريف الجريمة المعلوماتية بأنها "كل سلوك إجرامي يتم بمساعدة الكمبيوتر" وذهب البعض الآخر إلى تعريفها بأنها "كل جريمة تتم في محيط أجهزة الكمبيوتر" (إبراهيم، 2010، 42).

ويماثل هذا التعريف أيضاً ما ذهبت إليه مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية سنة 1983 عند تناولهم موضوع الجرائم المرتبطة بالمعلوماتية، حيث عرفوا الجريمة المعلوماتية بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها (htt/www.arab.elaw.com).

ومفاد هذه التعريفات السابقة أن النشاط أو الفعل حتى يكون جرمياً ويدخل ضمن دائرة الجريمة المعلوماتية، فإنه لابد أن يكون للحاسب الآلي دور لإتمامه، سواء أكان الحاسب الآلي أداة لإتمام الفعل الإجرامي، أم كان محلاً لها وذهب بعض أنصار هذا الاتجاه إلى تعريف الجرائم المعلوماتية بأنها "كل تلاعب بالحاسب الآلي ونظامه من أجل الحصول بطريقة غير مشروعة على مكسب للجاني أو إلحاق خسارة بالمجني عليه" (سلامة، 2006، 14).

وتجدر الإشارة هنا أن جانباً من الفقه يرى أنه عند وضع تعريف محدد للجريمة المعلوماتية تجب مراعاة عدة اعتبارات هامة وهي:

1- أن يكون هذا التعريف مقبولاً ومفهوماً على المستوى العالمي.

2- أن يراعي عند وضع التعريف التطور المتلاحق والسريع لتكنولوجيا المعلومات والحاسب الآلي.

3- أن يوضح التعريف خصوصية الجريمة المعلوماتية، بحيث يحدد الدور الذي يقوم به الحاسب الآلي في ارتكاب الجريمة (قورة، 2005، 32).

تقدير الاتجاهات السابقة:

أولاً- الانتقادات الموجهة إلى الاتجاه الأول: المضيق لمفهوم الجرائم المعلوماتية:

(1) أخذ على هذا الاتجاه أنه يضيق من مفهوم الجريمة المعلوماتية حتى أن البعض يرى أن الجريمة المعلوماتية من وجهة نظر هذا الاتجاه سوف تصبح أشبه بالخرافة، فهذا الاتجاه يجعل الجرائم المعلوماتية قاصرة فقط على الأشخاص ذوي الخبرة والكفاءة والقدرة العالية في استخدام تكنولوجيا المعلومات والحاسب الآلي، علماً بأن هناك بعض الجرائم المعلوماتية مثل إتلاف البيانات المخزنة في الحاسب الآلي، أو سرقة المعلومات الإلكترونية، لا تحتاج إلى هذا القدر العالي من الخبرة والكفاية في مجال الحاسب الآلي (سلامة، 2006، 12).

(2) يؤخذ على البعض من أنصار هذا الاتجاه والذين يقصرون الجرائم المعلوماتية في السلوك الإجرامي الذي يقع على الحاسب الآلي أو داخل نطاقه فقط، وبهذا فهم يضيقون من نطاق الجرائم المعلوماتية، بحيث ووفقاً لهذا التعريف تخرج كثير من الأفعال الجرمية من نطاق الجرائم المعلوماتية، هذه الأفعال التي ترتكب بواسطة الحاسب الآلي أي يكون أداة لارتكابها مثل جريمة التزوير المعلوماتي عن طريق الحاسب الآلي أي يكون أداة فيها.

ثانياً- الانتقادات الموجهة إلى الاتجاه الثاني: الموسع لمفهوم الجرائم المعلوماتية:

أخذ على هذا الاتجاه أنه يوسع كثيراً من مفهوم الجريمة المعلوماتية، حيث اعتبر أن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يضفي على هذا النشاط وصف الجريمة المعلوماتية، وهذا ينطوي على مغالطة جسيمة، فالحاسب قد يكون محلاً تقليدياً في بعض الجرائم مثل سرقة الحاسب الآلي نفسه (سلامة، 2006، 13).

ووفقاً لكل ما سبق يمكن للباحث القول بأن الثورة المعلوماتية المستحدثة والتي جاءت نتيجة التطور الهائل في قطاعي تكنولوجيا المعلومات والاتصالات، أدت إلى ظهور أنماط جديدة من السلوك تشكل جرائم أو أفعالاً جرميه تستوجب المسؤولية الجزائية، وأن ظهور الإنترنت وتعدد استخداماته والاعتماد عليه بشكل مطلق وفي شتى مجالات الحياة السياسية والاقتصادية والثقافية والاجتماعية وغيرها، أدى إلى تغيير في شخصية ومواصفات مرتكب الجريمة وبصفة خاصة جرائم الحاسوب والإنترنت، فإن كانت جرائم الحاسوب في الماضي ترتكب من قبل أشخاص على قدر عال من الذكاء والحنكة والكفاءة العالية والمتخصصين في مجال الحاسوب والتقنيات الفنية كالمبرمج، والمستخدم المؤهل والمهندس وغيرهم من المتخصصين في هذا المجال، إلا أنها وفي وقتنا الحاضر أصبحت ترتكب من الشخص العادي غير المتخصص والذي لا يتمتع بقدر عال من القدرة والكفاءة العالية والتخصصية في استخدام الحاسب الآلي (أي من غير المتخصصين)، وذلك نتيجة تطور استخدام الحاسب الآلي الشخصي وسهولة التعامل مع الإنترنت، حيث أدى ذلك إلى التوسع في حجم ونطاق المتعاملين مع الحاسب الآلي ، إلى الحد الذي أدى إلى وصول الحاسوب والإنترنت إلى كل منزل وكل مكان، كما وأنه ونتيجة لتخطي الدول لسنوات عديدة في مجال الجرائم المعلوماتية، فإنها أصبحت على الأغلب تحاول وضع تشريعات تُواجه هذا النوع من الجرائم في محاولة منها للسيطرة عليها ومجرميها، وأصبحت واعية في مجال سلطات التحقيق والقضاء من حيث تدريب الأشخاص المختصين لديها على هذا النوع من الجرائم، حتى يكونوا على درجة عالية من الكفاءة والخبرة في هذا المجال.

وبالنظر إلى التعريف الوارد في الاتجاه الأول والمضيق لمفهوم الجرائم المعلوماتية فإن الباحث يرى بأن هذا التعريف قد يصلح في فترة بداية ظهور هذا النوع من الجرائم عندما كانت ترتكب من قبل أشخاص متخصصين وذوي كفاءة عالية في مجال الحاسوب والإنترنت، أما في وقتنا الحاضر فقد اتسعت دائرة الأشخاص الذين يتعاملون بهذه التقنيات الحديثة، وبالتالي الذين يرتبكون مثل هذا النوع من الجرائم، كما وأن هناك كثيراً من الجرائم المعلوماتية ليست بحاجة إلى مقدرة وكفاءه عالية في مجال تكنولوجيا المعلومات مثل إتلاف البيانات المخزنة في الحاسب الآلي، وسرقة المعلومات المخزنة في الحاسب الآلي.

كما يرى الباحث أن بعض أنصار هذا الاتجاه المضيق قد قصروا الجرائم المعلوماتية على الأفعال الجرمية التي تقع على الحاسب الآلي أو داخل نطاقه، وهذا يؤدي إلى إخراج كثير من الأفعال الجرمية من دائرة الجرائم المعلوماتية، وبالتالي إفلات الفاعل من العقاب، مثل جريمة الاستغلال الجنسي للأطفال عبر شبكة الإنترنت، حيث ترتكب هذه الجريمة بواسطة الحاسب الآلي بحيث يكون الأخير أداة للجريمة.

أما فيما يتعلق بالاتجاه الموسع لمفهوم الجرائم المعلوماتية وخاصة الذين عرفوا الجريمة المعلوماتية بأنها "كل جريمة تتم في محيط الحاسبات الآلية"، فإن الباحث يرى أن هؤلاء الفقهاء قد تركوا المطلق على إطلاقه، ووفقاً لهذا التعريف فإن كل سلوك جرمي يرتكب ضمن دائرة ومحيط الحاسب الآلي يعتبر جريمة معلوماتية، فماذا لو كانت مكونات الحاسب الآلي المادية هي محل الجريمة، كجريمة سرقة الحاسب الآلي نفسه (المكونات المادية للحاسب الآلي)، الشاشة مثلاً أو لوحة المفاتيح، أو الكاميرا، أو الطابعة أو الأسطوانات الممغنطة أو غيرها من المكونات المادية للحاسب الآلي، والتي لا تدخل ضمن الكيانات المنطقية للحاسب الآلي أو معطياته (بيانات ومعلومات)، حيثُ تعتبر هذه جريمة سرقة تقليدية وتطبق عليها النصوص التقليدية في قوانين العقوبات، وبالتالي لا يمكن القول بأن النشاط الجرمي المرتكب في مثل هذه الجريمة نشاط يدخل ضمن دائرة الجرائم المعلوماتية.

أما بالنسبة للتعريف الآخر والذي جاء به بعض أنصار الاتجاه الموسع، والذي مفاده "أن جرائم المعلومات تعني "كل تلاعب بالحاسب الآلي ونظامه من أجل الحصول بطريقة غير مشروعة على مكسب للجاني أو إلحاق خسارة بالمجني عليه"، فإن الباحث يرى أنه ليس كل عبث أو تلاعب بالحاسب الآلي ونظامه يهدف الفاعل من ورائه الكسب المادي أو المعنوي أو إلحاق خسارة بالمجني عليه، حيث إن هناك كثيراً من الأفعال ترتكب من قبل أشخاص دون أن يتوافر لديهم القصد الجرمي بالحصول على كسب مادي أو معنوي أو إلحاق ضرر بالمجني عليهم، ومثال ذلك المخترقون فمنهم الهاكرز (HACKERS)، والكراكرز (CRACKARS) فالهاكرز هم الأشخاص الذين لديهم القدرة الفائقة على اختراق الأجهزة والشبكات أياً كانت إجراءات وبرامج وتدابير الحماية التي يتم اتخاذها، إلا أنهم لا يقومون بأي من الإجراءات التي تؤذي من تم اختراق جهازه أو شبكته (الجنيهي، منير والجنيهي، ممدوح، 2005، 28).

أما الكراكرز: ويطلق عليهم المخربين وهم يتشابهون مع الهاكرز في قدراتهم على الاختراق وتخطي إجراءات وبرامج الحماية، إلا أنهم يقومون بالعبث بالبيانات والمعلومات المخزنة على تلك الحاسبات والشبكات مع توافر نية التخريب لديهم (الجنبيهي، وآخرون، 2005، 28).

ومن هنا يجد الباحث أن التعريف السابق لبعض أنصار الاتجاه الموسع للجرائم المعلوماتية من شأنه أن يجعل الهاكرز لا يدخلون دائرة الجرائم المعلوماتية، وبالتالي إفلاتهم من العقاب.

وتجدر الإشارة هنا أن الأمم المتحدة قد أشارت في المدونة الصادرة عنها بشأن الجريمة المعلوماتية إلى الخلاف الواقع بين الخبراء حول ماهية العناصر المكونة لجرائم الحاسب الآلي أو حتى الجرائم المتعلقة بالحاسب الآلي ولعل هذا ما يفسر عدم التوصل إلى تعريف متفق عليه د ولياً للجرائم المعلوماتية (حجازي، 2004، 8). كما وأن المشرع الإنجليزي في قانون إساءة استخدام الحاسوب لعام 1990 آثر عدم وضع تعريف محدد لجرائم الحاسوب، بغية عدم حصر القاعدة التجريمية في إطار أفعال معينة، تحسباً للتطور العلمي والتقني في المستقبل (http/www.shabab20.net).

وبناء على ما تقدم يمكن للباحث أن يضع تعريفاً للجرائم المعلوماتية كما يلي "كل دخول مقصود وغير مصرح به إلى نظام الحاسب الآلي وكل نشاط تقني باستخدام الحاسب الآلي والإنترنت يؤدي إلى الاعتداء على معطياته المعنوية أو كياناته المنطقية أو أية مصلحة يحميها القانون وذلك بأية وسيلة تقنية".

الفرع الثاني: خصائص الجريمة المعلوماتية:

تتميز الجريمة المعلوماتية بخصائص تميزها عن الجريمة التقليدية ومن أهمها ما يلي:

أولاً: الجريمة المعلوماتية جريمة عابرة للحدود:

من أهم ما يميز شبكة الإنترنت أنها عالمية فهي لا تعرف حدوداً جغرافية سواء بالنسبة للمرسل أو المستقبل، إذ يستطيع كل مالك لحاسب آلي أن يرسل أو يستقبل المعلومات بدون أي اعتبار لحدود جغرافية مما جعلها ظاهرة عالمية، أو كما يعرفها البعض بأنها شبكة الشبكات (حسين، 2003-2004، 8).

لذلك تتسم الجريمة المعلوماتية غالباً بالطابع الدولي، فهي لا تعرف الحدود بين الدول والقارات، بل إنها تتخطى هذه الحدود، وتقرب المسافات بينها، وتجعلها وكأنها جميعها في حيز مادي واحد (مكان واحد)، فشبكة الإنترنت العالمية تجعل دول العالم والقارات في اتصال دائم على خط هذه الشبكة On line، وهذا يسهل ارتكاب الجريمة المعلوماتية من دولة إلى دولة أخرى، فيمكن من خلال هذه الشبكة والنظام المعلوماتي ونظام تكنولوجيا المعلومات ارتكاب كثيراً من الجرائم مثل جريمة القرصنة، وإتلاف نظم المعلومات، وتزوير وإتلاف المستندات، والاحتيال المعلوماتي وغيرها.

ولا يشترط لتحقيق الجريمة المعلوماتية أن يكون فاعلها متواجداً على مسرح الجريمة، فمعظم هذه الجرائم تتحقق نتائجها الجرمية عن طريق ارتكابها من قبل فاعلها عن بعد، فالفاعل يرتكب جريمته عن بعد وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة، ومن ثم تتباعد المسافة بين الفعل الذي يتم من خلال جهاز الحاسب الآلي للفاعل، وبين النتيجة أي المعطيات محل الاعتداء والمتواجدة في الحاسب الآلي للمجني عليه، ومن هنا فإن هذه الجريمة لا تقف عند الحدود الجغرافية والإقليمية لدولة معينة، بل تمتد إلى الحدود الإقليمية لدولة أخرى مما يزيد من صعوبة اكتشافها (محمود، 2002، 351).

وهذه الجرائم هي صورة من صور العولمة فمن الناحية المكانية يمكن ارتكابها عن بعد وبين أكثر من دولة، ومن الناحية الزمنية تختلف التوقيتات بين الدول، وهذا الأمر يثير تساؤلين الأول: حول تحديد القانون الواجب التطبيق على هذه الجريمة والإجراءات الجزائية، والثاني: أن هذا الأمر يؤدي إلى التعارض مع سيادة الدولة، وبالتالي قد يعقد من الاتفاقيات والأعمال الدولية المشتركة للحد من جرائم تقنية المعلومات (إبراهيم، 2009، 78-79).

ثانياً: الصعوبة في إثبات الجريمة المعلوماتية:

فالجرائم المعلوماتية جرائم مستحدثة تختلف عن الجرائم التقليدية في أنها لا تترك آثاراً مادية خارجية يمكن متابعتها من قبل جهات التحقيق، وبالتالي تظهر الصعوبة في اكتشافها، فلا توجد في مسرح الجريمة آثار دماء، أو بصمات، أو أظرف فارغة، أو جثة، أو لعاب، أو شعر، أو آثار عجلات مركبة، وغيرها كما هو الحال في الجرائم التقليدية.

وقد أشار بعض الفقهاء إلى أن الصعوبة في إثبات مثل هذه الجرائم يرجع إلى عدة أمور منها:

أ- أنها جريمة لا تترك أية آثاراً مادية لها بعد ارتكابها.

ب- صعوبة الإحتفاظ الفني بدليل الجريمة المعلوماتية: إذ يستطيع المجرم المعلوماتي وفي وقت قصير جداً أن يمحو آثار جريمته عن طريق محو أو تغيير البيانات والمعلومات الموجودة في الكمبيوتر.

ج- تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها. لذا يجد مأمورو الضبط القضائي أحياناً أنفسهم غير قادرين على التعامل بالإجراءات التقليدية مع هذا النوع من الجرائم، لأنها تحتاج إلى إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات (http/www.forum.biskra.com).

كما وأن هذه الجريمة إذا اكتشفت فلا يكون ذلك على الأغلب إلا بمحض الصدفة، والدليل على ذلك أنه لم يكتشف منها إلا بنسبة 1% فقط، والذي تم الإبلاغ عنه للسلطات المختصة لا يتعدى 15% من النسبة السابقة (الملط، 2006، 94).

ثالثاً: قلة الإبلاغ عن وقوع الجريمة:

ففي الغالب هناك إحجام من الشركات والمؤسسات في مجتمع الأعمال عن الإبلاغ عما يرتكب داخلها من جرائم، إما لعدم اكتشاف الضحية، أو تجنباً للإساءة إلى السمعة وهز الثقة بهذه الشركات والمؤسسات (http/www.stocksexperts.net).

رابعاً: وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات:

ذهب جانب من الفقه أن من خصائص الجريمة المعلوماتية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالحاسب الآلي، واعتبروا ذلك شرطاً أساسياً لقيام أركان الجريمة المعلوماتية الخاصة بالتعدي على نظام معالجة البيانات (المهيري، 2005، 135).

ويرى الباحث أن هناك ثلاث مراحل تمر بها المعالجة الآلية للبيانات:

الأولى منها: هي مرحلة الإدخال حيث يتم إدخال البيانات من قبل المستخدم وذلك بلغة مفهومة للحاسب الآلي، والثانية هي مرحلة معالجة البيانات المدخلة عن طريق الحاسب الآلي (البرامج) والمرحلة الأخيرة المتعلقة بالمخرجات والنتائج المتحصلة عن عملية المعالجة الآلية للبيانات وهذه تسمى المعلومات المعالجة آلياً.

لذلك فالجريمة المعلوماتية قد تتحقق في المرحلة الأولى مرحلة إدخال البيانات بأن يقوم الفاعل بمحو البيانات الأساسية وإدخال بيانات جديدة لا علاقة لها بالمعطيات، وقد تتحقق هذه الجريمة أيضاً في المرحلة الثانية مرحلة معالجة البيانات المدخلة كأن يقوم الفاعل بإدخال تعديلات على البرامج، وأخيراً قد تتحقق هذه الجريمة في المرحلة الأخيرة مرحلة النتائج وذلك بأن يقوم الفاعل بالتلاعب في النتائج (المعلومات) المخرجة من النظام المعلوماتي.

ومما سبق فإننا لا نستطيع أن نقصر الجرائم المعلوماتية فقط على مرحلة المعالجة الآلية للبيانات، لأن هذه الجرائم كما ذكرنا يُمكن أن تقع في أية مرحلة من المراحل سالفة الذكر.

كما وأن هذه الجرائم قد تقع على المعلومات المخزنة في الحاسب الآلي أو المتدفقة عبر شبكة الإنترنت، والتي تمثل قيماً اقتصادية أو أصولاً أو أموالاً أو معلومات شخصية لصاحبها.

خامساً: عدم وجود مفهوم مشترك للجريمة المعلوماتية:

فمن خصائص الجرائم المعلوماتية هو عدم وجود مفهوم مشترك وتعريف موحد لماهية هذه الجرائم، وقد يرجع السبب في ذلك إلى عدم وجود تنسيق دولي في مجال الجريمة المعلوماتية، وعدم وجود معاهدات دولية ثنائية أو جماعية لمواجهة هذه الجريمة، أو لاختلاف مفهوم الجريمة نتيجة لاختلاف النظم القانونية (إبراهيم، 2009، 82).

ولذلك يرى بعض الفقه أنه في سبيل مكافحة الجرائم المعلوماتية يجب أن تتحرك الدول المختلفة في محورين:

الأول: داخلي بحيث تقوم الدول بسن تشريعات وطنية لمكافحة هذا النوع من الجرائم والسيطرة عليها.

الثاني: دولي عن طريق عقد الاتفاقيات الدولية والمعاهدات، وفي حال غياب التشريعات الوطنية والاتفاقيات الدولية يصبح من الصعب السيطرة على هذا النوع من الجرائم، وهذا يترك الفرصة مُتاحة للمجرمين بارتكاب الجرائم دون عقاب، وبالتالي يؤدي إلى حالة من الانفلات القانوني وعدم السيطرة الأمنية والقانونية على هذه الجرائم الخطيرة (قوره، 2005، 55).

سادساً: الجريمة المعلوماتية جريمة مستحدثة:

تعد الجرائم المعلوماتية من الجرائم الحديثة التي أدت إلى أخطار جسيمة تهدد الأفراد والدول، وأن التقدم التكنولوجي والتقني في مجال المعلوماتية قرب المسافات بين الدول والقارات والأفراد، الأمر الذي جعل العالم كله كمدينة واحدة، هذا التقدم التقني بأساليبه الجديدة والحديثة والتقنية العالية أصبح يفوق قدرات وإمكانات أجهزة الدولة الرقابية، بل إنه أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها (إبراهيم، 2010، 51).

سابعاً: عدم كفاية التعاون الدولي في مجال الجرائم المعلوماتية:

يفتقر موضوع الجرائم المعلوماتية إلى وجود معاهدات دولية كافية للتسليم أو للتعاون الثنائي أو الجماعي بين الدول، وإن وجدت بعض المعاهدات إلا أنها غير كافية لمواجهة هذه التقنية الحديثة لنظم المعلومات، وغير قادرة على السيطرة عليها وإبراز دور أجهزة الدولة الرقابية على مثل هذا النوع من الجرائم (إبراهيم، 2009، 87).

ثامناً: الجرائم المعلوماتية جرائم ناعمة:

يطلق البعض على الجرائم المعلوماتية الجرائم الناعمة وذلك لأنها لا تحتاج إلى مجهود عضلي كما هو الحال في الجرائم التقليدية كجريمة القتل والسرقة والاغتصاب وغيرها، فالجريمة المعلوماتية تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي (المناعسة وآخرون، 2001، 107-108).

تاسعاً: الجرائم المعلوماتية جرائم مغرية للمجرمين:

تعتبر الجرائم المعلوماتية مشاريع اقتصادية تدر أرباحاً لا يستهان بها للإجرام البشري الإلكتروني وهي تقع في مستوى يساوي أو يفوق المشاريع المرتبطة بالمخدرات، لكن الأخطار التي تتعرض إليها أقل فعلاً بكثير، لاسيما أن عمليات الاختلاس فيها سهلة نسبياً وتتطلب القليل من الكفاءات ويكفي فيها حاسوب واستخدام الإنترنت. (لوفيت، 2010، 43).

و نظراً لما يمثله سوق الحاسب الآلي والإنترنت من ثروة كبيرة للمجرمين أو للإجرام المنظم، فقد غدت أكثر جذباً لاستثمار الأموال وغسيلها، وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن من الدخول إلى الشبكات، وسرقة المعلومات وبيعها، أو سرقة البنوك، أو اعتراض العمليات المالية، وتحويل مسارها، أو استخدام أرقام بطاقات السحب أو غيرها (البشري، 2005، 67).

ويُقبل المجرم المعلوماتي على ارتكاب جريمته المعلوماتية وهو هادئ الأعصاب ضابطاً للنفس، دون أي خوف من اكتشاف أمره، ودون أن يستخدم جهداً يذكر بالمقارنة بما تتطلبه الجرائم التقليدية من جُهد عضلي كبير، والحالة النفسية السيئة التي تسيطر على المجرم التقليدي وقت ارتكابه الفعل المجرم، مع العلم أن العوائد والمكاسب التي يحققها المجرم المعلوماتي من جريمته قد تفوق أضعافاً مضاعفة العوائد التي يحصل عليها المجرم التقليدي في بعض الجرائم، الأمر الذي يجعل الجريمة المعلوماتية تشكل إغراء كبيراً لكثير من المجرمين، خاصة عندما يكون الجاني موظفا في شركة استثمارية تعتمد في كل معاملاتها المالية على الحاسب الآلي، فتكون البيئة الجرمية مهيأة للجاني، نتيجة معرفته بآلية العمل وكافة المعلومات المتعلقة بالشركة، فيقوم بارتكاب جريمته المعلوماتية في تلك الشركة وتحقيق أرباحاً طائلة.

عاشراً: تميز مرتكبي الجريمة المعلوماتية بصفات مميزة من حيث الثقافة والعلم بالتكنولوجيا:

فالمجرم في هذا النوع من الجرائم ليس عادياً، فهو يرتكب جريمة متخصصة، خاصة إذا تمثلت هذه الجريمة في سرقة معلومات مشفرة، الأمر الذي يتطلب معه خبرة تقنية عالية في هذا المجال (عبد الله، 2007، 32).

الفرع الثالث: محل الجرائم المعلوماتية ومخاطرها:

أولاً- محل الجرائم المعلوماتية:

اختلف الفقه حول تحديد محل الجرائم المعلوماتية، فذهب جانب من الفقه إلى التمييز بين حالتين لتحديد محل وموضوع الجرائم المعلوماتية كما يلي:

الأولى- ارتكاب الجريمة بواسطة الحاسب الآلي:

حيث اعتبر أصحاب هذا الرأي أن الجرائم التي ترتكب بواسطة الحاسب الآلي لتحقيق

الاعتداء على الأشياء المحمية قانوناً من قبيل الجرائم التقليدية وليست معلوماتية، وأن هذه الجرائم تنطبق عليها النصوص التقليدية الواردة في قوانين العقوبات ولا حاجة إلى نصوص خاصة بالجرائم المعلوماتية، وقد جاء أنصار هذا الاتجاه بأمثلة على هذه الجرائم مثل الأفعال التي تتم باستخدام الحاسب الآلي للاطلاع على الحياة الخاصة، أو للاستيلاء على الأموال، إلا أن هذا الاتجاه انتقد ولم يلق موافقة وتأييد أغلب الفقه الذي يدرج هذه الجرائم ضمن الجرائم المعلوماتية (الصغير، 1992، 14).

والثانية- وقوع الاعتداء على الحاسب الآلي أو ملحقاته وهنا فرقوا بين حالتين:

الحالة الأولى- وقوع الاعتداء على الحاسب الآلي وملحقاته المادية:

كجهاز الحاسب الآلي نفسه، والأجهزة المادية الملحقة به، وأجهزة الإدخال والإخراج، حيث اعتبر أصحاب هذا الرأي أن هذه الجرائم من قبيل الجرائم المعلوماتية، إلا أن هذا الاتجاه انتقد من قبل معظم الفقه لأن الأموال المادية للحاسب الآلي محمية بموجب النصوص التقليدية في قوانين العقوبات التقليدية (عبابنة، 2005، 38-39).

الحالة الثانية- وقوع الاعتداء على معطيات الحاسب الآلي:

مثل تدمير برامج الحاسب الآلي، وسرقتها، وتقليدها، أو العبث في بياناته، أو المعلومات المعالجة آلياً والمخزنة فيه، وهذه تعتبر من قبيل الجرائم المعلوماتية . (عبابنة، 2005، 38-39).

ويتجه معظم الفقه إلى أن محل الجرائم المعلوماتية هي المعلومات بمفهومها الواسع، والتي تشمل البيانات والمعلومات والكيانات المنطقية كالبرامج التطبيقية وبرامج التشغيل، فهذه الجرائم ينصب فيها فعل الجاني على المعلومات المخزنة أو المعالجة في نظام الحاسب الآلي أو المتبادلة عبر الشبكات أو المثبتة على الدعامات المادية (إبراهيم، 2009، 91).

ويرى الباحث أن محل الجرائم المعلوماتية كما الرأي السائد في الفقه هي دائماً معطيات الحاسب الآلي المعنوية والمتمثلة في المعلومات والبيانات والكيانات المنطقية للحاسب الآلي (البرامج)، فحتى يدخل الفعل الإجرامي دائرة الجريمة المعلوماتية لابد أن ينصب على معطيات الحاسب الآلي المعنوية، فموضوع الحماية هنا هو هذه المعطيات ويستوي الأمر أيَ كان الاعتداء وفي أية مرحلة من مراحل المعالجة الآلية للبيانات، سواء وقع في المرحلة الأولى وهي مرحلة إدخال البيانات، أو في المرحلة الثانية عن طريق العبث في البرامج، أو في المرحلة النهائية وهي مرحلة النتائج وخروج المعلومات، أو خلال عملية نقل أو إرسال أو تدفق المعلومات الإلكترونية عبر الشبكة، أو المعلومات المخزنة في الحاسب الآلي.

وقد تقع الجريمة المعلوماتية أيضاً عن طريق تعطيل أجهزة الحاسب الآلي أو تخريبها عبر إرسال الفيروسات أو البرامج التي تحتوي أنظمة هجومية، مما يسبب تلفاً في أنظمة الحاسب الآلي يؤدي إلى شلل كل الأنشطة المرتبطة بهذا الجهاز أو الأنظمة المرتبطة به، مع العلم أن هذه المعطيات ليست ذات طبيعة مادية، فهي أقرب إلى الكيانات الذهنية أو المعنوية والتي تتطلب معالجة قانونية ذات طبيعة خاصة تأخذ بعين الاعتبار الطبيعه الخاصه لهذه المعطيات.

وبمعنى آخر فإن الجريمة المعلوماتية تقع على المعطيات بذاتها، أو بما تمثله هذه المعطيات، والتي قد تكون مخزنة داخل النظام المعلوماتي، أو على أحد وسائط التخزين، أو تكون في طور النقل والتبادل والتدفق ضمن وسائل الاتصال على النظام المعلوماتي.

أما إذا انصب فعل الجاني على المكونات المادية للنظام المعلوماتي، كالاعتداء على الأجهزة والمعدات الملحقة من أسطوانات وشرائط ممغنطة، ولوحة المفاتيح، والطابعات وغيرها دون أن يطال فعله المعطيات المعنوية لهذه الأجهزه، فإن محل الجريمة وموضوع الحماية هو المكونات المادية للحاسوب، وهذه المكونات محمية بموجب النصوص التقليدية في قوانين العقوبات، لأنها ذات طبيعة مادية ملموسة. ومثالها أن يقوم الفاعل بسرقة أجهزة الحاسوب مثلاً أو إتلافها بالضرب عليها بآلات حادة أو ثقيلة أو إشعال الحريق في هذه الأجهزة، فمثل هذه الأفعال تدخل في دائرة الجرائم المادية التي تنطبق عليها النصوص التقليدية في قوانين العقوبات.

ثانياً- مخاطر الجرائم المعلوماتية:

تتمثل مخاطر المعلوماتية في نوعين من المخاطر وهي المخاطر العارضة، والمخاطر المقصودة.

(1) المخاطر العارضة (غير المقصودة):

تتعدد المخاطر العارضة أو غير المقصودة كما يلي:

أ- المخاطر التي تؤدي إلى الإتلاف الجزئي أو الكلي للمعدات المعلوماتية والدعائم التي تختزن المعلومات، والتي تنشأ على سبيل المثال عن حريق، أو صدمات أو احتكاك، أو عناصر كيميائية، أو خلل كهربائي.

ب- تعطيل المعدات المادية أو الكيانات المنطقية، ولو لفترة زمنية قصيرة الأمر الذي قد يلحق بالمنشأة خسارة جسيمة بصفة غير مباشرة.

ج- الأخطاء الخاصة بالتحصيل، ونقل أو استعمال المعلومات، وهي تبدو أمراً حتمياً طالما أن هناك تدخلاً من الإنسان في عملية معالجة المعلومات.

د- وهناك أيضاً أخطاء التشغيل، وتتبلور في إتلاف البطاقات والنسخ والتشغيل السيئ للمعدات المادية، أو التفسير الخطأ للبيانات.

هـ- وتؤدي أخطاء التصميم والتنفيذ إلى خسائر على قدر كبير من الأهمية، بسبب عدم توافق التطبيقات والمعالجات لاحتياجات المنشأة (الشوا، 1994، 13-14).

(2) المخاطر المقصودة:

تتعدد وتتنوع المخاطر المقصودة من سرقة إلى إتلاف المعدات المادية للحاسب الآلي، وغش واختلاس أموال وكيانات منطقية ومعلومات وغيرها، وهذه المخاطر تؤدي إلى أضرار بالغة قد تؤثر بشكل سلبي على الحكومات ومؤسسات الأعمال ومعاملات الأفراد، وقد تؤدي إلى خلق جرائم جديدة وبصفة خاصة في مجالات التوقيع الإلكتروني والتجارة الإلكترونية والبريد الإلكتروني، وهو ما يبرر وجوب التدخل التشريعي لسن قانون خاص للجرائم المعلوماتية (www.nasbcom.net/vb/showthread.php?t=7230.page=1).

وتجدر الإشارة هنا أن جرائم الحاسب الآلي أصبحت سبباً لخسائر سنوية بليغة في الدول المتطورة، ومن الأمثلة على ذلك تكلف الاقتصاد الألماني وحده ما يقدر بخمسة مليارات مارك سنوياً، وذلك بعد استثناء حوادث التلف الناتجة عن الحرائق أو تسرب المياه إلى أجهزة الحاسب الآلي والشبكات، وأخطاء المكونات اللينة، واحتقان البرامج التطبيقية بالفيروسات، ولقد أدى الإحساس المتنامي بهذا الخطر إلى مسارعة هذه الدول إلى استحداث أنظمة للأمن والوقاية، ترمي إلى حماية مخزوناتها المهمة من البيانات والمعلومات (عظيمة، 1999، 81-85).

ويمكن للحاسوب أن يشكل خطراً على الحياة الخاصة للأفراد أو على أموالهم، وذلك من خلال التلاعب في البيانات والمعلومات المخزنة في ذاكرة الحاسب الآلي لهؤلاء الأفراد، وخاصة إن هذه الذاكرة تختزن بيانات تفصيلية عن كل ما يتعلق بالفرد من خلال تتبعها له، ابتداءَ من تاريخ ولادته ومروراً بكافة مراحل حياته العملية والشخصية وغيرها، ومما يزيد خطورة الحاسوب اعتماده تصنيف البيانات والمعلومات المتوفرة لديه ضمن موضوعات معينة سياسية واقتصادية واجتماعية وعلمية وأمنية، مما يجعل إمكانية اختراقها أيسر، ويجعل أمر وصولها إلى منافسي ذوي الشأن أمراً بالغ الخطورة، قد يلحق الضرر بهؤلاء ويهدد حياتهم ويقض مضاجعهم (الدعفيس، 1999، 66-67).

المطلب الثاني: أركان الجرائم المعلوماتية:

إن الجرائم المعلوماتية من الجرائم المستحدثة التي لم يكن يتوقعها المشرع التقليدي في الدول، وقد جاءت هذه الجرائم في حلة جديدة تختلف عن الجرائم التقليدية في أساليب ارتكابها، وخصائصها، وأسبابها، ودوافعها، وفئات مجرميها، فهي جرائم تتصل بالأرقام والتقنيات الحديثة لتكنولوجيا المعلومات، ومن الصعوبة على المشرع التقليدي السيطرة عليها والإحاطة بكافة صورها المتجددة بين الحين والآخر وفي أوقات قياسية قريبة، وفي الحقيقة تختلف أحكام القسم الخاص من قانون العقوبات عن أحكام القسم العام اختلافاً كبيراً، فبالنظر إلى أحكام القسم العام نجد أنها أحكام عامة وشاملة تتصف بالديمومة والثبات، في حين نجد أن القسم الخاص يتناول القانون منها كل جريمة على حده، حيث يحدد شروطها وأركانها وعناصرها وظروفها وقواعدها الخاصة دون سواها.

لذلك فإن نصوص القسم الخاص من القانون الجزائي تحدد نوع الحق أو طبيعة المصلحة التي يحيطها المشرع بحمايته، ونمط السلوك الذي يراه المشرع مضراً بهذا الحق أو هذه المصلحة المحمية قانوناً وبالتالي يجرمه، والعقوبة التي يفرضها المشرع على مرتكب الفعل الإجرامي، والذي يعتدي على هذا الحق أو المصلحة المحمية.

ومن هنا نجد أن الجرائم المعلوماتية شأنها شأن غيرها من الجرائم، تستوجب قوانين جزائية خاصة تحدد شروطها، وأركانها، وعناصرها، وظروفها، وقواعدها الخاصة دون سواها، لأن البيئة التي ترتكب فيها مثل هذه الجرائم تتسم بطابع خاص، فهي بيئة تقنية رقمية واتصال بالنظام المعلوماتي. ولذلك فسوف نبين الركن المادي والمعنوي للجرائم المعلوماتية وذلك كما يلي:

الفرع الأول: الركن المادي في الجرائم المعلوماتية:

لا شـك أن الجرائم المعلوماتية هي من جرائم الضرـر والتي يتطلب ركنها المادي ثلاثة عناصر هي النشـاط التقني الرقمي باستخدام الحاسوب والإنترنت ونتيجة جرمية اتجهت إرادة الفاعل لتحقيقها وعلاقة سببية بينهما

و يُعرف السـلوك الإجرامي بأنه النشـاط المادي الملموس الخارجي الذي يقوم به الجاني ويؤدي إلى تحقيق النتيجة الجرمية، سـواء قصـد الجاني من هذا السلوك تحقيق نتيجة معينة، أم تحققت النتيجة دون أن تنصرف إرادته إليها (الألفي، 1995، 25).

إلا أن النشـاط أو السـلوك الإجرامي في المعلوماتية يتطلب وجود بيئة رقمية وحاسـب آلي واتصـال بشـبكة الإنترنت، ويتطلب أيضـاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، ولا يمكن أن تقوم الجرائم المعلوماتية سـوى باسـتخدام الحاسـوب والإنترنت، فالنشـاط المادي المكون للجريمة إنما يتم بممارسـة نشاط تقني محدد هو اسـتخدام الحاسـوب والإنترنت، لذلك فإن القول بأن جرائم الحاسـوب والإنترنت من جرائم الوسـيلة هو غير صـحيح، فهما ليسـا وسـيلة لارتكاب الجريمة المعلوماتية، وإنما يدخلان في النشـاط المادي المكون لها (يونس، 2004، 254 وما بعدها).

ويتمثل الركن المادي في الجرائم المعلوماتية في عنصرـين الأول السـلوك المادي المؤدي إلى الجريمة والثاني لزوم مباشرة هذا النشاط التقني. وذلك كما يلي:

أولاً: السلوك المادي في الجريمة المعلوماتية:

يختلف السـلوك المـادي في الجرائم المعلومـاتيـة عنـه في الجرائم التقليـديـة، فـارتكـاب الجريمـة المعلوماتية يحتاج إلى منطق تقني حتى يتمكن الجاني من الاتصـال بالإنترنت، ومثل هذا النشـاط يختلف عما هو الحال في العالم المادي، وبدون المنطق التقني لا يمكن للجاني حتى الاتصـال بالإنترنت سـواء أكان بقصـد ارتكاب جريمة أم لمجرد التصـفح أو الدخول في الاتصال المباشر كالمحادثة وغيرها، وقد تدارك المشرع المقارن القصـور السـابق في النصـوص فنجده فيما يتعلق بنصـوص جرائم الحاسـوب والإنترنت يقرر صراحة عبارة... "إذا ارتكبت الجريمة باسـتخدام الحاسـب الآلي" أو عبارة "... باسـتخدام المعالجة الآلية للبيانات... الخ، بحيث يكون المشرـع هنا مدركاً للقيمة الموحدة للشرـوع في ارتكاب جريمة عبر الإنترنت، أو باسـتخدام الحاسب الآلي المرتبط بالإنترنت (إبراهيم، 2009، 100).

ويتمثل السلوك أو النشاط المادي في هذه الجرائم بنشاط رقمي يباشره الجاني حين يرتكب الجريمة عبر الإنترنت، وهذا النشـاط عبارة عن نشـاط تحويل كل فكرة أو مادة تقبل بطبيعتها التحول إلى مجموعة كبيرة من أرقام (0-1)، فهو بذلك يختلف عن النشاط المادي في الجرائم التقليدية (يونس، 2004، 259).

ثانيا: لزوم مباشرة النشاط التقني:

يبدأ السـلوك المادي عادة من الحاسـب الآلي أو من الإنترنت، ولا يمكن اعتبارهما وسـائل يتم بها ارتكاب الجرائم فمثل هذا القول لن يقود إلى التأكيد على أن البرمجيات تحديداً هي التي تعد الوسـيلة في ارتكاب الجرائم، ويلزم هنا الاقتراب من مفهوم أن التعامل القانوني مع الحاسـب والإنترنت يكون على أساس كونهما جزءاً من النشـاط المادي، وينبني على ذلك أن المشـرع هنا لا يجرم الوسـيلة الممثلة في البرامج أو الفيروسـات مثلاً، وإنما العمل غير المشروع ككل والمتمثل بالنشاط المادي القائم على استخدام الحاسب الآلي والإنترنت للولوج إلى النظام ومن ثم ارتكاب الجريمة (إبراهيم، 2009، 102 وما بعدها).

ويسـتلزم مباشرة السـلوك المادي للجريمة المعلوماتية أن يقوم الفاعل باسـتخدام تقني يشـكل هذا النشـاط المادي في جرائم الإنترنت، ويعني الاسـتخدام التقني ضرورة القيام بنشـاط تقني في مجال ارتكاب جرائم الحاسـوب والإنترنت، حيث يكون هذا النشـاط التقني مؤهلاً بذاته لارتكاب الجريمة، ويتم ذلك بأن يقوم مرتكب الجريمة بتجهيز الحاسوب لكي يحقق له قيام الجريمة (يونس، 2004، 262-263).

ويتحقق النشـاط التقني عن طريق قيام الجاني بتحميل الحاسـوب ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسـه، سـواء قبل ارتكاب الجريمة، أو أثناء الاختراق، أو تأهيل الحاسـوب للتعامل مع فيروسات الإنترنت، كأن يقوم بتهيئة صفحات تحمل في طياتها مواد منافية للأخلاق، أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف (Hosting Server)

.(http//www.shaimzatalla.com/vb/showthread.phb?t=7947)

كـذلـك يتحقق السـلوك المادي بأن يقوم مرتكب الجريمة بإعداد البرامج التمهيدية والتفصـيلية الخاصـة بالفيروسـات، أو برامج الدودة، أو القنبلة الزمنية، أو حصـان طروادة أو غيرها، ثم يقوم بضـغطها كبرنامج من خلال برامج ضـغط (Compression Programs) مؤهلة للقيام بذلك، ويقوم بتحديد الأوامر اللازمة للقيام بفك ذاتها في الحاسـوب الهدف أو عبر الشـبكات وتحديد زمن قيامها بذلك ذاتياً، فلا يقوم الجـاني هنـا بالتتبع المادي لجريمته، وإنما يعد العمل الإجرامي والنظام الذي يعمل به لكي يحقق له النتيجة الجرمية المبتغاة، ومثل هذا العمل يدخل في إطار الاستخدام (يونس، 2004، 263).

ولا يقبل القول بأن الحاسب الآلي والإنترنت هما وسيلة لارتكاب الجرائم المعلوماتية، بل يعتبران جزءاً من النشاط المادي، وذلك لأن هذا السلوك المادي إنما يتم بممارسة نشاط تقني محدد، وهو استخدام الحاسب الآلي والإنترنت، ومثال ذلك القتل عبر الإنترنت يستوجب لارتكابه أن يتم بممارسة نشاط رقمي محدد هو استخدام تقنية الحاسب الآلي للدخول إلى الإنترنت، ومن ثم بعد ذلك القيام بارتكاب ما من شأنه أن يؤدي إلى القتل (إبراهيم، 2009، 99 وما بعدها).

وهذا يعني أن القتل عبر الإنترنت يلزم لتحققه أن يقوم مرتكب الجريمة بممارسة نشاط مادي محدد هو استخدام تقنية الحاسوب للولوج إلى الإنترنت، وذلك عن طريق استخدام القطع الصلبة والمرنة للحاسوب تمهيداً لإجراء اتصال بالإنترنت، ومن ثم يتم مباشرة نشاط تقني منتهاه هو الجريمة، ومثال ذلك الطبيب الذي يعمل في إحدى المستشفيات يمكنه أن يلج إلى قاعدة بيانات توزيع الدواء في المستشفى من منزله أو من أي مكان آخر، ومن ثم يقوم بتغيير معدلات الدواء لأحد المرضى بقصد قتله.

وكذلك في جريمة إتلاف وتدمير المعلومات فيلزم لتحققها قيام الفاعل بارتكاب نشاط رقمي معين وهو استخدام الحاسوب والولوج به إلى الإنترنت وقد يحتاج الأمر إلى تجهيز أو إعداد برامج معينة بقصد الوصول إلى عملية مسح للحاسبات والشبكات المختلفة وصولاً إلى الخادم أو المضيف الذي يتواجد فيه الموقع المستهدف، وقد يتطلب الأمر هنا فك شيفرة معينة وهذا يحتاج إلى إعداد برمجة معينة فوراً ثم الولوج في النهاية إلى الموقع المذكور، ثم الدخول على الملفات الداخلية المستهدفة وتدميرها.

وتجدر الإشارة هنا أن المشرع الأوروبي راعى التوحد في اتجاهات التجريم عبر الإنترنت، وذلك في تفصيله للباب الثاني Chapter II لفكرة الرؤية الإجرامية، حيث اعتبر النشاط المادي يتمثل في جزئية استخدام الحاسوب، وساوى بين مصطلح جرائم الحاسوب، والجرائم ذات العلاقة بالحاسوب مباشرة (يونس، 2004، 257).

كما وأن المشرع الأمريكي توسع كثيراً في مصطلح السلوك في القسم (1956) من التقنين الأمريكي ليشمل المبادرة أو المشاركة في المبادرة، وقد برزت مسألة التوسع في تحديد السلوك الإجرامي وبشكل واضح في تعديل عام 2001 للقسم (1030) من التقنين الأمريكي الفيدرالي (18 US Code) بمقتضى القانون الوطني المؤرخ في 2001/10/23 The Patriot Act، حيث قرر المشرع الأمريكي الفيدرالي في مواد القانون العقاب على سلوك مادي محدد هو القيام باستخدام الحاسوب والإنترنت لارتكاب جرائم معلوماتية، مثل السلوك المادي المتمثل في استخدام الحاسب الآلي والإنترنت وإرسال برنامج أو معلومات أو شيفرة أو أمر... الخ.

وقد حدد المشرع الفيدرالي السلوك الإجرامي باستخدام الحاسب الآلي والإنترنت بشكل تفصيلي في ذلك القانون (يونس، 2004، 257، 262).

ومما سبق يتبين أن المشرع الأمريكي والأوروبي أخذا بنظرية الركن المادي للجرائم المعلوماتية، والمتمثلة في إتيان سلوك مادي باستخدام الحاسب الآلي والإنترنت، وذلك للولوج إلى الموقع المستهدف من أجل ارتكاب الجريمة المعلوماتية المخطط لها من قبل الفاعل، وبذلك فإن المشرع الأمريكي ابتعد عن منطق اعتبار كل من الحاسوب والإنترنت من جرائم الوسيلة، لأنهما يدخلان في تكوين النشاط المادي المؤدي إلى النتيجة الجرمية.

وتجدر الإشارة هنا أنه في مجال الجرائم المعلوماتية يصعب الفصل بين الأعمال التحضيرية وبين البدء في التنفيذ الذي يدخل في مجال النشاط المادي في هذه الجرائم (http//www.shaimzatalla.com/vb/showthread.phb?t=7947).

فالقاعدة العامة في التشريع الجنائي أنه لا يعاقب على الأعمال التحضيرية، ما لم تشكل في ذاتها جريمة، بأن يعتبرها المشرع جريمة بحد ذاتها، ومثالها حيازة سلاح ناري بدون ترخيص دون استخدامه في القتل أو الإيذاء، فحيازة هذا السلاح دون ترخيص اعتبره المشرع جريمة يعاقب عليها بحد ذاتها، بصرف النظر سواء استخدم في جريمة أم لم يستخدم.

وفي مجال تكنولوجيا المعلومات يمكن القول بانطباق القواعد العامة على الأعمال التحضيرية فيها، ذلك أن العمل التحضيري في هذه الجرائم يرتبط بالعالم المادي ارتباطاً مرحلياً، ويظل معلقاً ما بين البدء في التنفيذ وبين العدول الاختياري غير المعاقب عليه، فطالما كانت هناك علاقة بين العالم المادي وبين العالم الافتراضي فإن العمل يظل في إطار التحضير (يونس، 2004، 264). ومن ذلك القيام بشراء برامج اختراق أو إعداد فيروسات، وكذلك تأهيل الحاسوب بشراء قطع صلبة معدة لفك التشفير، فالجاني في جريمة بث الفيروسات وإرسالها عبر الإنترنت إلى حواسيب أشخاص آخرين (المجني عليهم) يحتاج إلى تركيب برنامج الفيروس ثم تنشيطه كدودة أو حصان طرواده، أو قنبلة زمنية، ومن ثم زرعه وضغطه في حاسوبه وتهيئته للانطلاق، ولغاية هذه اللحظة يكون الجاني ما زال في مرحلة التحضير للجريمة ولم يبدأ في التنفيذ وهذه الأفعال التحضيرية غير معاقب عليها لأنها لا تشكل جريمة في ذاتها (يونس، 2004، 264).

وتجدر الإشـارة أن قيام الجاني بشرـاء برامج اختراق أو إعداد فيروسـات. وكذلك شراء قطع صـلبة معـدة لفـك التشـــفير مما يتجـاوز المعـدلات الدولية والإقليمية الخاصـــة ببعض الدول التي تحد منه مثل الولايات المتحدة الأمريكية يشـــكل جريمة بذاتها لذلك يعاقب عليها المشرـــع الأمريكي كجرائم مســـتقلة وليست من جرائم الإنترنت (يونس، 2004، 264 وما بعدها).

ويخلص الباحث مما سـبق أن الركن المادي في الجرائم المعلوماتية يستوجب أن يقوم الجاني بإتيان السـلوك المادي وضـمن البيئة الرقمية والاتصـال بالإنترنت، ومن ثم من خلال الولوج إلى الحاسـب الآلي أو الإنترنت يسـتطيع ممارسـة نشـاطاته الإجرامية الرقمية، وارتكاب الجرائم المعلوماتية بشـتى صـورها، لذلك فالحاسـب الآلي والإنترنت هما جزء من النشـاط المادي الإجرامي وليسا وسيلة لارتكاب الجريمة المعلوماتية، أما بالنســبة للأعمال التحضــيرية التي تســبق الجرائم المعلوماتية، فلابد من الرجوع إلى القوانين الجزائية المعمول بها في الدولة التي تقع فيها الجريمة، لمعرفة إذا كانت هذه الأفعال تشـكل جريمة بذاتها، أم أنه غير معاقب عليها، فعلى سـبيل المثال شراء برامج اختراق، أو إعداد فيروسـات، أو شراء قطع صـلبة لفك التشـفير تمهيـداً لارتكـاب جرائم معلوماتية، لا يعتبر جريمة يعاقب عليها المشرـــع الأردني طالما أنها بقيت في مرحلة التحضير دون استخدامها في الجرائم المعلوماتية، أما في الولايات المتحدة الأمريكية فهو معاقب عليه كجريمة مستقلة.

الفرع الثاني: الركن المعنوي في الجرائم المعلوماتية:

ويطلق عليه الركن الأدبي أو الشـخصيـ والركن المعنوي هو الحالة النفسـية للجاني، وفي إطار هذا الركن تتوافر كـافـة مقومـات المســؤوليـة الجنـائيـة، ويعرف بـأنه "العلاقة التي تربط بين ماديات الجريمة وشـــخصـــيـة الجـاني مرتكبهـا، وهذه العلاقة هي محل التجريم ، ومن ثم يوجه إليها لوم القانون وعقابه" (حسني، 1971، 90).

والركن المعنوي يختلف في الجرائم المقصودة عنه في الجرائم غير المقصودة، ففي الجرائم المقصودة يتكون الركن المعنوي من النية الجرمية أو القصـد الجرمي لارتكاب هذه الجريمة، وفي الجرائم غير المقصودة يتكون من الخطأ .

ويعرف الفقه الخطأ بأنه تقصير في سلوك الإنسان لا يقع من شخص عادي وجد نفسه في ذات الظروف الخارجية، أو هو مخالفة واجب الحيطة والانتباه كما تصنعه قواعد السلوك في الجماعة، أو كما نصت عليه قواعد القانون (السعيد، 1991، 230).

وتعد الجريمة المقصودة مثار الكلام في جرائم الإنترنت من حيث مدى البحث في توافر القصد الجنائي، ومدى قبول القول بضرورته، كركن يجب البحث في عملية ثبوته في الجرائم المعلوماتية، ولذلك يقتضى منا ذلك لزوم التعرض إلى مدلول القصد الجنائي، وتطلبه في الجرائم المعلوماتية.

والقصد الجنائي هو النية الجرمية أو القصد الجرمي، وكما أسلفنا سابقاً فقد عرف المشرع الأردني النية في المادة (63) من قانون العقوبات الأردني بأنها " إرادة ارتكاب الجريمة على ما عرفها القانون".

ونصت المادة 1/74 من ذات القانون على أنه "1- لا يحكم على أحد بعقوبة ما لم يكن قد أقدم على الفعل عن وعي وإرادة" ومن خلال نص هذه المادة نجد أن النية أو القصد الجرمي في الجرائم المقصودة يقوم على عنصرين هما العلم والإرادة.

وبمعنى آخر فالقصد الجنائي هو توجيه الإرادة لإحداث أمر يعاقب عليه القانون، وهذا يستلزم أن يكون الجاني عالماً بحقيقة ما يرتكبه، مدركاً أن عمله هذا يجرمه القانون، ويحاسب من حيث القصد على وفق ما يعلمه وقت الفعل، فإذا جهل حقيقة ما يعلمه أو غلط فيه فإن هذا الجهل أو الغلط يؤثر في القصد الجنائي فينفيه (إبراهيم، 2009، 107).

لذلك فإن القصد الجنائي يقوم على عنصرين، الأول إرادة ارتكاب الفعل الذي يؤدي إلى تحقيق النتيجة الإجرامية، والثاني العمل والإحاطة بحقيقة هذا الوضع الإجرامي وبمادياته وعناصر الجريمة.

ويتوافر القصد الجنائي بحق الجاني في ثلاث حالات وهي:

1- إذا كان الجاني يتوقع ويريد أن يترتب على فعله أو امتناعه حدوث الضرر أو وقوع الخطر، والذي يعلق عليه القانون وجود الجريمة.(القصد المباشر)
2- إذا نتج عن فعله أو امتناعه عن الفعل ضرر أو خطر أكثر جسامة مما كان يقصده الفاعل،(إبراهيم، 2009، 108) كما هو الحال في الجريمة المتعدية القصد.
3- إذا تجاوزت النتيجة الجرمية قصد الجاني في حال توقع حدوثها وقبل بالمخاطرة .(القصد الاحتمالي)

وفي إطار الجرائم المعلوماتية فإن توافر القصد الجنائي يثير خلاف من حيث مدى تطلبه في الجرائم المعلوماتية ذات الامتداد بالجريمة الأولى، وهي جريمة الاختراق، وفيما عدا ذلك من جرائم تتعلق ببناء الركن المعنوي فيها، فإن المشرع يتطلب القصد الجنائي أو لا يتطلبه حسب الأصول (يونس، 2004، 290).

ومؤدى ذلك أن الركن المادي في الجرائم المعلوماتية يتحقق بمجرد إتيان الجاني سلوكاً مادياً متمثلاً في استخدام الحاسب الآلي والإنترنت للولوج إلى النظام، وهذه هي جريمة اختراق النظام المعلوماتي والتي يعاقب عليها القانون بمجرد اكتمال أركانها، وقد يقوم الفاعل بعد اختراق النظام بارتكاب أفعال إجرامية أخرى تشكل جرائم معلوماتية، وبالتالي فإن هذه الجرائم لابد من اكتمال أركانها المتمثلة في الركن الشرعي والمادي والمعنوي، لذلك فقد طرح موضوع مدى إمكانية توافر البحث في الركن المعنوي وتحديداً القصد الجنائي في الجرائم ذات الامتداد بالجريمة الأولى وهي اختراق النظام.

وتجدر الإشارة هنا أن هذا الموضوع قد أثير أمام القضاء الأمريكي، حيث تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة المعلوماتية وهيكلته في الجرائم التي يقررها ما بين مبدأ الإرادة ومبدأ العلم، فهو تارة يستخدم مصطلح الإرادة كما هو الشأن في قانون العلامات التجارية في القسم(2320) من التقنين الفيدرالي الأمريكي، وتارة أخرى يقرر مصطلح العلم كما هو الشأن في قانون مكافحة الاستنساخ الأمريكي في القسم (2319) من التقنين الأمريكي (http/www.shaimzatalla.com/vb/showthread.phb?t=7947).

وقد برزت هذه الفكرة لأول مرة في قضية في الولايات المتحدة ضد موريس، والذي كان متهما في قضية دخول غير مصرح به على جهاز حاسب آلي فيدرالي، وقد دفع محامي موريس بانتفاء الركن المعنوي وبالتالي القصد الجنائي لديه، الأمر الذي جعل المحكمة تقول "هل يلزم أن يقوم الإدعاء بإثبات القصد الجنائي في جريمة الدخول غير المصرح به والولوج إلى حاسوب فيدرالي، بحيث تثبت نية المتهم في تحدي حظر استخدام نظام المعلومات في الحاسوب وتحقيق خسائر، ومثل هذا الأمر يستدعي التوصل إلى تحديد أركان جريمة الدخول دون تصريح" (يونس، 2004، 291).

وبذلك ذهبت المحكمة في ردها حول تطلب القصد الجنائي إلى تبني معيارين هما معيار الإرادة بالدخول غير المصرح به، وكذلك معيار العلم بالحظر الوارد على استخدام نظم معلومات فيدرالية دون تصريح" (www.shaimzatalla.com)

وقد برز اتجاه القضاء المقارن باشتراط القصد الجنائي في جريمة الدخول غير المصرح به للنظام فقط، إلا أن هذا الاتجاه انتقد من قبل الفقه، حيث قيل أن تحديد الركن المعنوي في كافة الجرائم المعلوماتية هام جداً لتحديد طبيعة السلوك الجرمي المرتكب، وبالتالي تحديد النصوص المالية واجبة التطبيق، وبدون تحديد الركن المعنوي لن يكون هناك سوى جريمة معلوماتية واحدة وهي الدخول غير المصرح به للنظام (إبراهيم، 2009، 108).

فمثلا إن التمييز بين جريمة الدخول غير المشروع لنظام المعالجة الآلية للبيانات وبين جريمة تجاوز الصلاحيات في الدخول إلى مثل هذا النظام يعتبر تمييزاً دقيقاً، ففي جريمة تجاوز صلاحية الدخول يلزم لتوافرها أن تكون هناك صلاحية للدخول إلى نظام ما، وأن تتوافر داخل النظام أنظمة معينة ليس من حق هذا الشخص الدخول عليها، فيقوم المذكور بالدخول إليها، ففي مثل هذه الحالة لا تتوافر سوى جريمة واحدة، حيث إن المذكور يملك صلاحية الدخول إلى النظام الأساسي ولا يملك الدخول إلى أنظمة خاصة فيه، إلا أن تكوين النشاط المادي هنا يلزم أن يكون السلوك الإجرامي مرتكباً في إطار نشاط ثانٍ وليس النشاط الأول، ومثل هذا الأمر يجعل منطق تجاوز صلاحيات الدخول معتبراً من الجرائم التي لا تتطلب فيها ركناً معنوياً، ومثل هذا الأمر غير صحيح في القانون (يونس، 2004، 293).

فتطلب القصد الجنائي يحدده مدلول الصلاحية وليس منطق النشاط المادي لكون السلوك موحداً في الجرائم المعلوماتية، بحيث يجب أن ينطلق تفسير القصد في معنى دلالة العدوان على الصلاحية في الدخول إلى النظام، وبحث مدى وجود هذه الصلاحية، وكيفية العدوان على الصلاحية المذكورة، بالإضافة إلى الوسائل التي استخدمها الشخص المذكور في العدوان على هذه الصلاحية، كما لو كان قد استخدم برمجيات في التداول، أم قام هو بابتكار برمجيات اختراق، أم أنه استخدم برمجيات نظام التشغيل ذاته... الخ (إبراهيم، 2009، 109).

ونتيجة لذلك فإن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الإنترنت من حيث مدى تحديد ما إذا كانت تتطلب قصداً عاماً أم خاصاً، فنجده لا يمانع في تطلب قصد جنائي خاص في جريمة التهديد، إلا أنه يقرر من جديد أنه يكتفي بالقصد العام عن ذات الجريمة، كما هو الشأن في جريمة التهديد بالبريد الإلكتروني وعبر المجموعات الإخبارية (يونس، 2004، 294).

وبناء على ما تقدم فإن الباحث يذهب مع أن الجرائم المعلوماتية جرائم مقصودة ، يتطلب ركنها المعنوي توافر القصد الجنائي لدى الجاني، وذلك لتحديد طبيعة السلوك المرتكب من قبله، ومن ثم تكييفه وبيان النصوص التي تنطبق على هذا الفعل، فيجب أن تتجه إرادة الفاعل إلى إتيان سلوكه الإجرامي بصورته الإيجابية أو السلبية، مع تحقيق النتيجة الإجرامية سواء الضرر أو الخطر، مع علمه بحقيقة الوضع الإجرامي الذي يقوم به.

ويرى الباحث أن أحكام القسم الخاص من قانون العقوبات يتناول القانون منها كل جريمة على حده، حيث يحدد شروطها وأركانها وعناصرها وظروفها وقواعدها الخاصة بها دون سواها، ومن هذا المنطلق يجب الرجوع إلى هذه الأحكام والتي تنظم الجرائم المعلوماتية لمعرفة أركانها وعناصرها، وبشكل خاص البحث في ماهية الركن المعنوي لهذه الجرائم ومدى تطلبه في الجرائم الممتدة بعد اكتمال أركان جريمة الولوج والاختراق للنظام المعلوماتي، حيث يرى الباحث أن فعل اختراق النظام المعلوماتي هو جريمة بحد ذاتها سواء ارتبط بارتكاب جريمة أخرى كجريمة نسخ المعلومات أو الاحتيال المعلوماتي، أم لم يرتبط بجريمة أخرى، فهذه الجريمة تتطلب ركناً معنوياً متمثلاً في القصد الجنائي لفعل الاختراق، أما ما ارتبط بها من جرائم أخرى يرى الباحث بأنها تحتاج إلى توافر قصد جنائي خاص بها.

المطلب الثالث: المجرم المعلوماتي:

تتميز شخصية المجرم المعلوماتي بخصائص وميزات تختلف عن شخصية المجرم العادي في الجرائم التقليدية، وقد وجد النظام المعلوماتي في عصرنا هذا وأصبح يستخدم في شتى مجالات الحياة السياسية والاقتصادية والمالية والاجتماعية والثقافية وغيرها، وأن تقنيات هذا النظام جاءت لمصلحة الأفراد والدول، إلا أن مصدر ضعف وانتهاك هذه التقنيات الحديثة هو الإنسان ذاته، فهو الذي يهيئ فرصة استغلال الوسيلة المعلوماتية، سواء عن حسن أو سوء نية، وقد وجد الجزاء الجنائي لغايات الردع العام أو الردع الخاص، ومن هنا لابد من إلقاء الضوء على شخصية المجرم المعلوماتي، تمهيدا لإعادة تأهيله اجتماعياً حتى يعود إلى المجتمع مواطناً صالحاً مرة أخرى، مع العلم أن مرتكب الجريمة المعلوماتية قد يكون شخصاً مستقلاً أو شخصاً يعمل مع مجموعة من الأفراد يجتمعون في صفات معينة، ولذلك فسوف ندرس في هذا المطلب سمات المجرم المعلوماتي، وتصنيف هؤلاء المجرمين، ودوافعهم لارتكاب هذه الجرائم.

الفرع الأول: الصفات الشخصية للمجرم المعلوماتي:

أولاً: المجرم المعلوماتي إنسان اجتماعي بطبعه:

يتميز المجرم المعلوماتي عن المجرم التقليدي بأنه إنسان متوافق مع المجتمع قادر على التكيف مع الآخرين، يمارس عمله المعلوماتي ضمن هذا المجتمع، فهو إنسان اجتماعي، إلا أنه يرتكب هذا النوع من الجرائم بدافع اللهو أو بدافع الكبرياء، كالموظف الذي يطرد من عمله فليجأ إلى ارتكاب جريمته، أو لمجرد إظهار تفوقه على الحاسب الآلي أو على البرامج التي يتم تشغيله بها (مراد، لات، 45).

ثانياً: الذكاء:

يتميز المجرم المعلوماتي بالذكاء والمعرفة العالية والكفاءة في استخدام الحاسب الآلي والتقنية الحديثة، فهو يختلف عن المجرم التقليدي الذي يستخدم العضلات والعنف على الأغلب وهو يستخدم ذكاءه وكفاءته ومعرفته العالية في تكنولوجيا المعلومات، ويُقبل على جريمته بكل هدوء أعصاب وبمقدرة عقلية عالية، ويحاول أن يحقق أهدافه بهدوء ودون الالتجاء إلى العنف، فهو يستخدم عقله وذكاءه لارتكاب أفعاله الجرمية، وهو يسعى دائماً إلى اكتشاف طرق جديدة مبتكرة لا يعرفها أحد سواه لاختراق الحواجز الأمنية في البيئة الإلكترونية وتحقيق جريمته المعلوماتية (www.zinj.org/fourm/showthread.php?t=2821).

ويقال عادةً عن الإجرام المعلوماتي بأنه إجرام الأذكياء مقارنة بالإجرام التقليدي الذي يميل إلى استخدام القوة والعنف، فتحقق هذه الجرائم يتطلب المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي، والقدرة على التعديل والتغيير في البرامج، وارتكاب الجرائم المعلوماتية (محمود، 2002، 48-49).

ثالثاً: الخبرة والمهارة:

يتميز المجرم المعلوماتي بالخبرة والمهارة العالية في استخدام التقنيات الحديثة لتكنولوجيا المعلومات والاتصالات، وتتحدد درجة خطورة الجرائم التي يرتكبها هذا المجرم بدرجة الخبرة والمهارة التي يتمتع بها، وبمعرفة التقنية المعلوماتية، والعلاقة بينهما طردية فكلما قلت خبرته ومهارته في هذا المجال قلت خطورة الجرائم المعلوماتية التي يرتكبها والتي قد لا تتعدي جرائم إتلاف المعلومات بالمحو أو الإتلاف، وكلما زادت خبرته ومهارته زادت خطورة هذه الجرائم والتي قد تصل في بعض الأحيان إلى سرقة الأموال والتزوير المعلوماتي والاحتيال، وقد تصل إلى التجسس على أنظمة الدول، وقد يتعداها إلى حد ارتكاب جرائم إرهاب، الأمر الذي يشكل خطورة كبيرة على أمن الأفراد والدول (الفقي، لات، 15).

رابعاً: الميل إلى التقليد:

من صفات المجرم المعلوماتي هو الميل إلى تقليد الآخرين، فعندما يكون الشخص مع آخرين فإنه من السهل الانسياق والتأثر بهم، حيث يحدث أن يقوم الشخص بتقليد غيره من الأشخاص الذين يتعامل معهم، فيأتي المجرم المعلوماتي ويحاول تقليد غيره بالمهارات الفنية التي يتمتع بها، الأمر الذي يؤدي إلى ارتكابه الجرائم المعلوماتية (بهنام، 1982، 176).

خامساً: الميل إلى ارتكاب الجرائم:

يتميز المجرم المعلوماتي بوجود النزعة الإجرامية لديه والميل إلى ارتكاب الجرائم المعلوماتية، فهو يقوم بتعلم المهارات التقنية وتكنولوجيا المعلومات ويطور نفسه في هذا المجال حتى تساعده على ارتكاب جرائمه، وتتبلور النزعة الإجرامية لدى هذا المجرم نتيجة تأثره بعوامل التكوين العضوي والعوامل النفسية المصاحبة لنشأته، ومع اقتران هذه العوامل بعناصر أخرى تساعد على ظهور الحالة الإجرامية لديه وتزيد من رغبته في ارتكاب الجرائم المعلوماتية وتقلل من موانع الإقدام عليها، وهذه العناصر قد تكون اكتساب الشخص للمهارات العلمية والتكنولوجية (إبراهيم، 2009، 135).

سادساً: القابلية على استخدام الوسائل:

مع تزايد وسائل الاتصال بالحاسوب وتزايد أعداد أصحاب الخبرة بهذا المجال، فقد تهيأت الظروف لأصحاب النوايا السيئة في استغلال وسائل الاتصال هذه وغيرها من مصادر الحاسوب سواء ما يتعلق منها بالتخزين أو المعالجة لتنفيذ جريمة الحاسوب (السرحان، والمشهداني، 2001، 115).

سابعاً: المجرم المعلوماتي يبرر ارتكاب جريمته:

يشعر المجرم المعلوماتي دائماً بأن الفعل الذي يقوم به فعل مباح وليس جرمياً أو لا أخلاقياً، فهو يقوم باختراق أنظمة المعلومات بما فيها أنظمة الحماية الخاصة بهذه الأنظمة، والحصول على المعلومات المختزنة في هذه الأنظمة دون أن يعتبر فعله هذا من قبيل الجرائم المعاقب عليها، وخاصة إذا تعلق الأمر باختراق النظام المعلوماتي للشركات الاستثمارية الكبيرة، ويبرر ذلك بأن هذه الشركات قادرة على تحمل نتائج تلاعبه، وعلى العكس من ذلك إذا انصبت الأضرار المتحصلة عن جرائمه لتطال الأشخاص ومصالحهم فهو يعتبر ذلك جريمة لا أخلاقية (www.mst-oman.com/fourms/archive/index.php/t-331.html).

الفرع الثاني: تصنيف مرتكبي الجرائم المعلوماتية:

لم يتفق الفقه على تصنيف محدد وموحد لمرتكبي الجرائم المعلوماتية، حيث وردت تصنيفات متعددة إلا أنها مختلفة فيما بينها، ويرجع هذا الاختلاف في التصنيف إلى اختلاف المعايير التي يعتمدها الفقهاء للوصول إلى تصنيفاتهم، فذهب جانب من الفقه إلى تصنيف مرتكبي الجرائم المعلوماتية بناء على معيار العلاقة بنظام التشغيل الإلكتروني للبيانات وتم تصنيفهم إلى ثلاث مجموعات هي:

الأولى: تضم أخصائيي النظام.

الثانية: تضم مستخدمي الأنظمة.

الثالثة: تضم أفراد المنشأة (Goldberg. 1989, P. 66-67).

وذهب جانب آخر من الفقه إلى تصنيف مرتكبي الجرائم المعلوماتية وبناءً على نفس المعيار السابق إلى ست مجموعات أساسية وهي كما يلي:

1- العاملون المتذمرون أو غير الراضين عن منشآتهم.
2- العاملون داخل المنشأة ويجدون متعة في اختراق نظم المعلومات.
3- العاملون داخل المنشأة ولكن لديهم مشاكل خاصة.
4- عملاء المنشأة ولديهم بعض المشاكل معها ويريدون الانتقام.
5- أفراد ذوو دوافع سياسية لاختراق نظم إلكترونية سرية للمنشأة.
6- المجرمون بطبيعتهم (الملط، 2006، 62-63).

وذهب جانب آخر من الفقه إلى تصنيف مجرمي المعلومات على أساس معيار العمر، وتم تصنيفهم إلى طائفتين هما طائفة صغار السن وطائفة البالغين.

ويرى الباحث أنه وباستعراض الواقع العملي للدول الغربية في مجال تكنولوجيا وتقنية المعلومات وجرائمها، والتي سبقتنا في البحث في مثل هذا النوع من الجرائم، فإننا نجد أن تصنيف مرتكبي الجرائم المعلوماتية على أساس المعايير السابقة تصنيف بعيد عن الواقع، ولا يؤدي الفائدة المرجوة، سواء على الصعيد الموضوعي الخاص بالنصوص القانونية المتعلقة بهذه الجرائم، أو على الصعيد الإجرائي والمتعلق بالإجراءات المتخذة من قبل أفراد الضابطة العدلية وسلطات التحقيق حيال وقوع الجريمة.

ويمكن لنا وفقاً لما توصلت إليه الدراسات والأبحاث التي تناولت مجرمي المعلومات أن نبين بعض الأنماط الخاصة بهم، ونرى أن أفضل تصنيف يحقق الفائدة المرجوة من أهداف هذه الدراسات يجب أن يكون على أساس معيار درجة الخطورة للفاعل، وذلك بتصنيف هؤلاء المجرمين من الأقل خطورة إلى الأكثر خطورة، وبناء على ذلك يمكننا تصنيف مرتكبي الجرائم المعلوماتية إلى أربع فئات كما يلي:

الفئة الأولى- صغار مجرمي المعلوماتية:

وتشكل هذه الفئة الخطر الأضعف على الأنظمة المعلوماتية وهي عادة تقوم بصنع برامج مؤذية للنظام لتبرهن على أنها قادرة على قهر هذا النظام وتحديه (بوكسي وبولان، 2010، 45).

ويطلق عليهم البعض تسمية صغار نوابغ المعلوماتية التي تميل إلى التحدي الفكري، وهم عادة يكونون في مرحلة المراهقة (سليمان، 2005، 25).

ويمتاز هؤلاء المراهقون عن غيرهم من مرتكبي الجرائم التقليدية أن لديهم اعتقاداً بأن ما يقومون بـه من أفعـال لاختراق النظـام المعلومـاتي هي أفعـال مباحة ولا يعتبرونها مجرمة، وذلك انطلاقاً من الفكرة التي مؤداهـا أن النظام غير القادر على حماية نفســه ليس من الخطأ اقتحامه، وبالتالي فهم لا يدركون ولا يقـدرون مـاهيـة الأفعـال التي يقومون بهـا، ولا النتـائج المحتملـة التي يمكن أن تنتج عن هذه الأفعال غير المشرــوعـة، ويمكن لهـذه الفئة أن تتحول إلى فئة القراصــنة مع تطور خبراتهم وكفاءاتهم في نظام التقنية الحديثة (إبراهيم، 2009، 142)، وتجدر الإشـارة هنا أن جانباً من الفقه رأى أنه من الملائم ألا يصنف هؤلاء الشـباب في طائفة أو أخرى من الطوائف الإجرامية لأن لديهم ببساطة ميلاً إلى المغامرة والتحدي والرغبة في الاكتشاف (حجازي، 2007، 47).

الفئة الثانية- القراصنة:

وهذه الفئة أخطر من الفئة السابقة، وقد تم تصنيفها إلى نوعين:

أولهما: الهاكرز HACKERS (الهواه).

وثانيهما: الكراكرز CRACKERS (المحترفون).

ويعرف الهاكرز (الهواة)، بأنهم الأشخاص الذين لهم القدرة الفائقة على اختراق الأجهزة والشبكات أيـا كـانـت إجراءات وبرامج وتـدابير الحمايـة التي تم اتخاذها، إلا أنهم لا يقومون بأي من الإجراءات التي تؤذي من تم اختراق جهازه أو شبكته (الجنبيهي، منير وممدوح، 2005، 22) (الجواد والفتال، 2008، 143).

وطائفة الهاكرز غالباً ما تكون من هواة الحاســوب، فيقومون بأعمالهم لمجرد إظهار أنهم قادرون على اقتحام الأنظمة الأمنية أحيانا، أو لمجرد ترك بصـماتهم التي تثبت وصـولهم إلى تلك المواقع أحياناً أخرى (الزيدي، 2003، 40).

وهناك سـمة مميزة لهذه الفئة من القراصـنة وهي تبادلهم للمعلومات فيما بينهم، والتشـارك في وسـائل الاختراق وآليات نجاحها في مواطن الضعف في نظم الحاسوب والشبكات، خاصة عن طريق النشرات الإعلامية الإلكترونية ومجموعات الأخبار (المومني، 2008، 84).

أمـا الكراكرز (المحترفون)، فيطلق عليهم المخربين وهم يتشــابهون مع الهاكرز في قدرتهم الفائقة على الاختراق وتخطي إجراءات وبرامج الحمايـة، إلا أنهم يقومون بـالعبـث في البيـانات والمعلومات المخزنة على تلك الحاسـبات والشـبكات (الجنبيهي، منير وممدوح، 2005، 28) والقراصـنة المحترفون هم أخطر من الهواة لأنهم قد يحدثون أضراراً كبيرة، وهم غالباً ما يكونون من فئة المكررين للجريمة، وهذه الفئة تســعى إلى تحقيق الأرباح الشخصية.

وهناك دراسات أجراها معهد (Stand Ford Research) بينت أن محترفي الجرائم المعلوماتية من الجيل الحديث هم غالبا من الشباب الذين تتراوح أعمارهم من 25 إلى 45 سنة، وهذه الإحصاءات تبين ما يلي:

- إن 25% من أفعال الغش المعلوماتي يرتكبها المحلل.
- وإن 18% من هذه الأفعال يرتكبها المبرمج.
- وإن 17% يرتكبها المستخدم الذي لديه أفكار خاصة بنظم المعلومات.
- وإن 16% منها يرتكبها الصراف.
- وإن 12% يرتكبها الشخص الأجنبي عن المكان الذي تتواجد فيه نظم المعلومات.
- وإن 11% من هذه الأفعال يرتكبها فني التشغيل (محمود، 2002، 56).

الفئة الثالثة- فئة لصوص نظم المعلومات:

وهذه الفئة أخطر من الفئات السابقة، وهي تحمل نشاطاً إجرامياً خطيراً وكان يطلق على هؤلاء المجرمين متعصبي التليفونات (Les Fanes Du Telephone)، وهذا المصطلح يعني الخبير أو المهووس أو اللص، وهذه الفئة المهووسة بالتليفونات بدأت أفعالها الجرمية تخرج إلى الحيز الخارجي بدايةً للتهرب من فواتير المكالمات الخارجية، ومع تطور وسائل الاتصال وتكنولوجيا المعلومات تطورت نشاطاتهم الإجرامية وتوسعت لتطول نظم الاتصالات والتحكم في الحاسوب الذي بدوره يتحكم بأنظمة الاتصالات، حتى وصل بهم الأمر إلى التعدي على البرامج والبيانات والمعلومات المختزنة في نظام الحاسوب، والاعتداء عليها بالسرقة والإتلاف والاحتيال والتزوير وغيرها من الجرائم المعلوماتية (محمود، 2002، 62).

الفئة الرابعة- فئة المتطرفين أصحاب الآراء المتطرفة:

وهذه الفئة أخطر من الفئات السابقة فهي تتألف من مجموعة أشخاص يدافعون عن قضية أو غاية لا علاقة لها بمصالحهم الخاصة، وهؤلاء يقومون بارتكاب أنشطة إجرامية نتيجة معتقداتهم التي يعتنقونها، هذه الأنشطة تؤدي إلى إلحاق أضرار جسيمة بالآخرين أو بقطاعات كاملة في المجتمع، وذلك لأسباب ذات طابع سياسي أو اقتصادي أو ديني، وتسمى هذه الجماعات بالجماعات الإرهابية أو المتطرفة، فهي تقوم بأنشطتها الإجرامية ليس لتحقيق الربح المادي وإنما لفت الأنظار إلى ما يدعون إليه (المومني، 2008، 85-86).

وخير مثال لهذه الجماعات هي تلك التي تنتمي إلى منظمات إرهابية دولية من اليمين المتطرف واليسار المتطرف مثل جماعات الألوية الحمراء الإيطالية، ومنظمة (LECLODO) وهي منظمة فرنسية متخصصة في تدمير نظم المعلومات وغيرها من المنظمات الأخرى ، حيث قامت هذه الجماعات بارتكاب أفعال اعتداء على أنظمة المعلومات المنتشرة في أوروبا ابتداء من عام 1978 (محمود، 2002، 65).

الفرع الثالث: دوافع إرتكاب الجرائم المعلوماتية:

الباعث أو الدافع لارتكاب الجريمة هو "القوة المحركة للإرادة أو الدافع النفسي- إلى إشباع حاجات معينة كالبغضاء والمحبة، والجوع، وإرضاء شهوة الانتقام وغير ذلك، وهو يختلف في الجريمة الواحدة" (المجالي، 2005، 343).

ويختلف الباعث أو الدافع في الجريمة عن الغرض والغاية فالغرض هو الهدف القريب الذي تتجه إليه الإرادة، أو هو الأثر المترتب على النشاط المقصود بالعقاب، فالغرض في القتل هو إزهاق روح المجني عليه، وفي الضرب المساس بسلامة جسم المجني عليه.

أما الغاية فهي الهدف البعيد للإرادة، ويعد بلوغها إشباعا لحاجات معينة، فالباعث أو الدافع هو الرغبة، والغاية هي إشباع هذه الرغبة (المجالي، 2005، 343).

وأفضل مثال على ذلك لتوضيح هذه المصطلحات، إذا أحس شخص بالبغضاء والكراهية أو الرغبة أو الانتقام من شخص آخر (وهذا هو الباعث أو الدافع)، فيكون إشباع هذا الدافع أو الباعث بقتل المجني عليه (وهذا هو الغرض)، وتعد الإرادة المتجهة إلى القتل (هي القصد الجرمي)، وبعد أن يتم قتل المجني عليه تكون الغاية من الجريمة قد تحققت، وهي إرضاء الشعور بالكراهية أو إشباع شهوة الانتقام وقد عرف المشرع الأردني الدافع في المادة 67 من قانون العقوبات الأردني رقم (16) لسنة 1960 وتعديلاته كما يلي:

1- "الدافع: هو العلة التي تحمل الفاعل على الفعل، أو الغاية القصوى التي يتوخاها.
2- لا يكون الدافع عنصراً من عناصر التجريم إلا في الأحوال التي عينها القانون".

يتضح من هذا النص أن المشرع الأردني اعتبر الجريمة قائمة بمجرد تحقق أركانها وعناصرها، ولم يعتبر الدافع أو الباعث عنصراً من عناصر الجريمة إلا في الأحوال التي يحددها القانون.

أما بالنسبة للجرائم المعلوماتية فإن الدوافع والبواعث التي تدفع المجرم المعلوماتي إلى ارتكاب جريمته متعددة ومتنوعة ومن أهم هذه الدوافع ما يلي:

أولاً: تعلم تقنية المعلومات والشغف بالتقنية المعلوماتية:

قد يكون الدافع لارتكاب الجرائم المعلوماتية هو الرغبة في الوصول إلى مصادر المعلومات والحواسيب الإلكترونية والشبكات وتكنولوجيا المعلومات بغرض التعلم، وقد أشار الدكتور (ليفي) مؤلف كتاب قراصنة الأنظمة HACKERS إلى أخلاقيات هؤلاء القراصنة، والتي ترتكز على مبدأين أساسيين هما:

أ- إن الدخول إلى أنظمة الكمبيوتر يمكن أن يُعلمك كيف يسير العالم.

ب- إن عملية جمع المعلومات يجب أن تكون غير خاضعة إلى القيود (محمود، 2002، 69).

فهناك كثير من القراصنة يدخلون شبكات وأنظمة المعلومات ويخترقون نظام الحماية فيها بهدف التعلم، سواء على المستوى الفردي أو الجماعي، وذلك بتعليم بعضهم بعضا عبر الشبكة، ويحاول هؤلاء القراصنة كسب أكثر وقت ممكن وهم مجهولو الهوية دون اكتشافهم، ليتسنى لهم البقاء في النظام مده أطول، وعادة يكرسون معظم وقتهم في تعلم كيفية اختراق النظام المعلوماتي، ودخول المواقع الممنوعة، واختراق أنظمة حمايتها.

وينطلق هؤلاء الأشخاص من قناعة ذاتية مفادها أن المعلومات المفيدة والموجودة داخل النظام المعلوماتي، يجب أن تكون متاحة للتداول بين الكافة من حيث الإطلاع عليها ونسخها (www.kenanaonline.com/users/internet-safety/topics/.../143404)، ويقرون أيضا بإغلاق بعض المواقع وعدم السماح لأحد من الوصول إليها وخاصة التي تتضمن معلومات سرية خاصة بالأفراد (المومني، 2008، 90).

وقد يكون الدافع لارتكاب الجريمة المعلوماتية هو الشغف بالإلكترونيات والإنبهار بتقنية المعلومات، سواء تعلق الأمر بالمعلومات أو بالحواسيب الإلكترونية.

ويحاول هؤلاء الأشخاص تحقيق انتصارات تقنية على النظام المعلوماتي، وقهر هذا النظام دون أن تتوافر لديهم نوايا سيئة، وبالتالي فهم ليسوا على جانب كبير من الخطورة (العريان، 2004، 65).

ثانياً: تحقيق الربح والثراء السريع:

قد يكون الدافع أو الباعث لارتكاب الجرائم المعلوماتية، هو السعي وراء تحقيق الربح المادي والثراء السريع وبزمن قياسي، وفي كثير من الأحيان قد تدفع الحاجة إلى المال البعض إلى اختراق النظام المعلوماتي والحصول على معلومات هو غير مخول بالوصول إليها وذلك من أجل الحصول على المكاسب المادية،

فهناك الكثير من مجرمي المعلومات يعمدون إلى ارتكاب جرائمهم نتيجة الظروف المادية التي يعيشونها هم وعائلاتهم، فقد يكون البعض منهم غير قادر على تلبية متطلبات عائلته، أو سداد الديون المستحقة عليه، أو لا يستطيع تأمين النقود لتلبية احتياجاته من المخدرات نتيجة الإدمان، وقد يكون آخر يسعى إلى تحقيق الأرباح الهائلة والثراء الفاحش من أجل تحسين وضعه المعيشي، فيلجأ إلى هذا النوع من الجرائم الناعمة (الملط، 2006، 89).

وفي هذا الشأن نورد مثالاً حادثة حول مدى الأرباح والمكاسب المادية التي يحققها بعض مجرمي المعلوماتية، من خلال ما رواه أحد المجرمين المحترفين في سجن ولاية كاليفورنيا حيث قال "لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة كمبيوتر جهاز الضرائب في الولايات المتحدة الأمريكية، وبإمكاني أن أكرر ذلك في أي وقت، لقد كان شيئاً سهلاً، فأنا أعرف أسلوب عمل جهاز الحاسب الآلي للضرائب، وقد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني" (محمود، 2002، 57).

ثالثاً: الإثارة والمتعة وتحدي تقنية المعلومات:

قد يكون الدافع للجرائم المعلوماتية هو الشعور بالإثارة والمتعة من خلال اختراق أنظمة المعلومات والتجوال في مواقع الشبكات وكسر الحواجز الأمنية للنظام دون رقيب أو حسيب، وبهذا يصل قراصنة النظام إلى حد الذروة من الشعور بالمتعة والإثارة

وقد جاء على لسان أحد القراصنة "أنه وعندما كان يعود من المدرسة إلى البيت، كان يدخل إلى الشبكة المعلوماتية عن طريق الحاسب الآلي خاصته، وفي بداية الأمر كان يتردد على موقع النشرات ويسجل اسمه فيه، شأنه شأن باقي الأشخاص الذين يترددون على نفس الموقع، ويقوم بتصفح أخبار المجتمع ويتبادل المعلومات مع الآخرين في جميع أنحاء العالم، إلى أن وصل به الأمر أن أصبح عضواً في نخبة قراصنة الأنظمة، ويقول أنه عندما كان يبدأ عملية القرصنة الفعلية وخلال ساعة واحدة يبدأ عقله بقطع مليون ميل في الساعة، وينسى جسده تماماً بحيث ينتقل من جهاز كمبيوتر إلى آخر محاولاً العثور على هدفه، ويضيف بأن عملية القرصنة هذه كان يصاحبها شعور بالمتعة والإثارة المحظورة بفعل شيء غير قانوني، ويقول أن كل خطوة كان يخطيها يمكن أن تسقطه بيد السلطات، وكان على حافة التكنولوجيا واكتشاف ما وراءها واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض وجوده بها" (محمود، 2002، 73 وما بعدها).

وباستعراض ما ورد على لسان أحد قراصنة أنظمة المعلومات سالف الذكر، نجد أنه ومن خلال وصفه للحالة التي كان فيها، من حيث دخوله من حاسوب إلى آخر، ومن شبكة إلى أخرى ومن موقع إلى آخر، خارقاً بذلك جميع أنظمة الحماية الخاصة بهذه الحواسيب والشبكات، أنه كان يشعر بأعلى درجات الذروة من الإثارة والمتعة خلال هذه الاختراقات للنظام المعلوماتي.

رابعاً: الرغبة في الانتقام:

قد يكون الباعث أو الدافع في ارتكاب الجرائم المعلوماتية هو إشباع شهوة الانتقام من شخص معين أو من شركة معينة أو منشأة معينة أو صاحب العمل أو حتى الأنظمة السياسية، ويكون إخماد هذه الشهوة بأن يقوم الفاعل باختراق النظام المعلوماتي للمجني عليه، وارتكاب جرائم معلوماتية لإيقاع أضراراً مادية أو معنوية بالمجني عليه (المومني، 2008، 92).

والمثال على ذلك قيام موظف كان يعمل في بنك مصرفي وتم إنهاء خدماته بالتلاعب في تقنية المعلومات الخاصة في البنك، بحيث أتلف أو شطب كافة المعلومات المتعلقة بحسابات العملاء في ذلك البنك، الأمر الذي يؤدي إلى أضرار وخسائر جسيمة للبنك وسمعته.

خامساً: دوافع أخرى:

إن الدوافع السالفة الذكر ليست وحدها الدوافع لارتكاب الجرائم المعلوماتية، سيما وأن هناك دوافع أخرى قد تؤدي بالفاعل إلى ارتكاب جريمته، فقد يكون دافع جنون العظمة أو الطبيعة التنافسية هو الباعث في ارتكاب هذه الجريمة، ويحدث ذلك عندما يكون الفاعل يعمل في منشأة معينة مع آخرين فيقوم بارتكاب الجريمة المعلوماتية لإظهار قدراته الفنية العالية في هذه التقنية، في محاولة منه للوصول إلى أعلى المراكز في هذه المنشأة.

وقد يكون دافع التعاون والتواطؤ على الأضرار، وغالباً ما يتم ذلك بالاتفاق بين الشخص المتخصص فنياً بالأنظمة المعلوماتية في منشأة معنية مع آخر من خارج هذه المنشأة وله علاقة في العمل الخارجي معها، فيتم التواطؤ بينهما لتحقيق مكاسب مالية من خلال هذه الجرائم، وقد يكون الدافع التهديد، بأن يقع الشخص الذي يعمل في منشأة تحت تهديد وضغط الغير لارتكاب جرائم معلوماتية في محيط المنشأة أو الشركة، وذلك في نطاق شركات الأعمال التجارية المنافسة (الملط، 2006، 90 وما بعدها).

وقد يكون الدافع ناشئاً عن التنافس السياسي والاقتصادي بين الدول أو التنافس في المجال القضائي والعسكري فيما بينها، كما وأنه وجدت مجموعات تطلق على نفسها مجموعات الكراهية على الإنترنت، تخالف كل القيم الدينية والأخلاقية والاجتماعية السائدة في المجتمعات وبخاصة المرتبطة بالأسرة (المومني، 2008، 93).

المبحث الرابع: التعاون الدولي لمواجهة جرائم الحاسوب والإنترنت:

لم تكن الأخطار الناجمة عن جرائم الحاسب الآلي والإنترنت موضع اهتمام الدول فحسب، بل كانت مثار اهتمام المنظمات الدولية العالمية والإقليمية، لاسيما مع تزايد حجم الأضرار الناتجة عن مثل هذا النوع من الجرائم عابرة الحدود، حيث أصبحت حدود الدول مستباحة نتيجة للتقنيات الرقمية وطبيعتها الخاصة، والتي يصعب على المشرع الوطني مواكبتها حتى في الدول المتقدمة، وفي الوقت الذي لم تقتصر فيه هذه الجرائم على الأنظمة المعلوماتية الخاصة بالأفراد، بل امتدت لتطال باعتداءاتها أنظمة الحكومات والدول وأجهزتها الأمنية والعسكرية والاقتصادية وغيرها، إلى الحد الذي وصلت إلى اختراق سرية البيانات والمعلومات المعالجة آلياً والخاصة بالدول والأفراد، وهذا ما جعل الدول وأ فرادها كتاباً مفتوحاً أمام مجرمين متخصصين في مجال المعلوماتية، لا تقف في وجوههم أية أنظمة خاصة بالحماية، لذلك فقد بات أمر التعاون الدولي لمواجهة هذه الجرائم ضرورةً حتمية، وهذا ما سوف نتناوله في هذا المبحث من حيث بيان جهود الأمم المتحدة للحد من هذه الجرائم ومكافحتها، ودور المجلس الأوروبي، مع إلقاء الضوء على اتفاقية بودابست لمكافحة جرائم الحاسوب لعام 2001 والتي تمخضت عن جهود المجلس الأوروبي حول هذا الموضوع، وأخيراً سوف نتحدث عن الجهود العربية في هذا المجال وبالأخص عن القانون العربي النموذجي أو الاسترشادي وذلك كما يلي:

المطلب الأول: جهود الأمم المتحدة على النطاق الدولي:

منذ ظهور عصر العولمة والتقنية الرقمية وزيادة معدلات ارتكاب الجرائم التقنية، نادت الأمم المتحدة من خلال المؤتمرات الخاصة بمنع الجريمة ومعاملة المجرمين إلى وجوب تعزيز العمل المشترك بين الدول الأعضاء والتعاون فيما بينها للحد من انتشار هذه الجرائم، وذلك لما تشكله من خطورة كبيرة على المجتمع الدولي.

وفي عام 1985 وفي مدينة ميلانو في إيطاليا عقد مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين، حيث كلف لجنة الخبراء العشرين إعداد دراسة لحماية الأنظمة المعلوماتية والحاسب الآلي من الاعتداءات التي قد تطالها، وأقرت هذه اللجنة جملة من المقترحات والتوصيات، وقُدمت إلى مؤتمر هافانا الثامن حيث تبناها وأدخل عليها بعض التعديلات والمقترحات (الحسيناوي، 2009، 147 وما بعدها).

ويمكن إجمال توصيات مؤتمر هافانا لعام 1990 في المبادئ التالية:

(1) تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية.

(2) تحسين أمن الحاسب الآلي والتدابير المعنية بحماية الخصوصية وحقوق الإنسان.

(3) اعتماد إجراءات تدريب كافية للموظفين والقضاة والوكالات المسؤولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والادعاء.

(4) تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات.

(5) اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم.

(6) زيادة التعاون الدولي من أجل مكافحة هذه الجرائم (الهيتي، 2006، 166).

وفي عام 1995 عُقد مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين في القاهرة، حيث انبثقت عنه توصيات حول حماية الحياة الخاصة للإنسان والملكية الفكرية من أخطار الأنظمة المعلوماتية وتكنولوجيا المعلومات، وأكدت التوصيات على موضوع التعاون والتنسيق بين أفراد المجتمع الدولي، وذلك لاتخاذ التدابير والإجراءات اللازمة للحد من هذه المخاطر (الحسيناوي، 2009، 148).

كما وأكدت الأمم المتحدة على اتخاذ الإجراءات اللازمة للحد من أعمال القرصنة في مجال الأنظمة المعلوماتية، وذلك في المؤتمر العاشر لمنع الجريمة ومعاملة المجرمين والمنعقد في بودابست في المجر عام 2000 (عبابنة، 2005، 159).

وكذلك أوصى المؤتمر الأول لحقوق الإنسان والمنعقد في طهران عام 1968 والخاص بدراسة آثار التقدم التكنولوجي على حقوق الإنسان بضرورة احترام الحياة الخاصة في مواجهة التقدم وحماية حقوق الأفراد وحرياتهم من خطر التعدي عليها (قايد، 1994، 81).

المطلب الثاني: دور المجلس الأوروبي:

كان للمجلس الأوروبي دور لا يستهان فيه في مجال حماية البيانات والمعلومات المعالجة آلياً من خطر الأنظمة المعلوماتية، وذلك في محاولة للحد من الاعتداءات التي تقع عليها عبر الحاسب الآلي أو الشبكات المعلوماتية.

وقد ركز المجلس الأوروبي على حماية الحياة الخاصة للأفراد وعلى البيانات ذات الصبغة الشخصية من إساءة استخدامها بواسطة المعالجة الإلكترونية لها، وتمثل ذلك في توصيات البرلمان الأوروبي لسنة 1979، وأيضاً توصيات المجلس الأوروبي لسنة 1980، والخاصة بحماية تدفق ونقل المعلومات ذات الصبغة الشخصية بين الدول الأعضاء (قايد، 1994، 84).

وتجدر الإشارة في هذا الخصوص أن الاتحاد الأوروبي قد بدأ جهوده بشأن توحيد القواعد المقررة في قوانين حماية الخصوصية ابتداءً من عام 1976، وفي هذا الحقل صدرت عن الاتحاد تعليمات عديدة كما يلي:

(1) تعليمات 76/4/8 والمتعلقة بحماية الأفراد من أنشطة التقييم الآلي للبيانات.

(2) تعليمات 79/5/8 والمتعلقة بحماية الأفراد في مواجهة التطور التقني لمعالجة البيانات.

(3) تعليمات 82/3/9 والمتعلقة بذات الموضوع (الجنبيهي، منير وممدوح، 2005، 72).

وفي عام 1981، وقعت اتفاقية تحت مظلة المجلس الأوروبي تتعلق بحماية الأشخاص في مواجهة المعالجة الآلية للبيانات ذات الصبغة الشخصية، وقد بدأ السريان الفعلي لهذه الاتفاقية في شهر 1985/10، ويقتصر نطاق تطبيقها على الأشخاص الطبيعيين وعلى القطاعين العام والخاص، فيما يتعلق بالملفات المعالجة آلياً (الشوابكة، 2009، 74).

ومن أبرز التوصيات التي جاءت بها الاتفاقية ما يلي:

(1) أن تكون البيانات المسجلة صحيحة ودقيقة وأن تكون مدة حفظها محددة.

(2) عدم اطلاع الغير على البيانات الشخصية أو استعمالها في غير الغرض المخصصة له.

(3) إقرار حق الشخص في الاطلاع على البيانات الخاصة به، وتصحيحها وتعديلها أو محوها إذا كانت باطلة، أو حصل عليها بطريق غير مشروع.

(4) اتخاذ الإجراءات اللازمة ضد إساءة استعمال هذه البيانات.

(5) تحديد الأشخاص المسموح لهم الوصول إلى هذه المعلومات وضرورة كتمانها (قايد، 1994، 84).

وكذلك أصدر المجلس الأوروبي العديد من القواعد التوجيهية للحد من الجرائم المعلوماتية، وجرمت كثيراً من الأفعال التي تطال بالاعتداء البيانات والمعلومات المعالجة آلياً (الجنبيهي، منير وممدوح، 2005، 73)، كالغش المعلوماتي، والتزوير المعلوماتي، وسرقة الأسرار المخزنة في الأنظمة المعلوماتية، والتوصل غير المصرح به وسرقة منفعة الحاسب الآلي، كما وتضمنت هذه القواعد بعض قواعد وإجراءات الحماية لاستخدامها للمحافظة على البيانات والمعلومات المخزنة، كاستخدام كلمة السر، وحماية الأوامر الخاصة بالتشغيل، وترميز المعلومات الشخصية (إبراهيم، 2009، 402).

وفي تاريخ 11 آذار من عام 1996 صدر إرشاد أوروبي يحمل الرقم 96/9/CE والذي يتعلق بالحماية القانونية لقواعد البيانات، ولوحظ بأن هذا الإرشاد قد منح جميع قواعد البيانات سواء المعالجة آلياً أو غيرها كالمعلومات التي تدخل ضمن حقوق المؤلف وأدخلها جميعها ضمن أحكام القوانين التي تحمي الملكية الفكرية، وأعطى أيضاً حماية مزدوجة لقواعد البيانات من خلال حماية محتواها من الاقتطاع أو الاستعمال له أو لأي جزء أساسي منه (الشوابكة، 2009، 75).

وفي 2000/4/25 ونتيجة للجهود الفعالة التي قام بها المجلس الأوروبي في مجال الحد من جرائم الحاسب الآلي فقد تكللت هذه الجهود بالنجاح وإصدار اتفاقية شاملة تتعلق بجرائم الحاسوب والتي جاءت في مقدمة خمسة فصول (الحسيناوي، 2009، 151).

وقد جاء في مقدمة هذه الاتفاقية، أن الدول الأعضاء وحرصاً منها على حماية مجتمعاتها من جرائم الحاسب الآلي، فإنه يجب عليها وضع التشريعات اللازمة، وتعزيز التعاون الدولي سيما مع تزايد معدلات الجرائم المرتبطة بالتقنية من جرائم الاعتداء على المعلومات ا لمعالجة آلياً، وجرائم شبكات الحاسب الآلي، والتي تحتاج إلى بذل جهود مضنية للبحث عن الأدلة والإثبات نظراً للطبيعة الخاصة التي تتمتع بها هذه الجرائم، لأن الأدلة فيها تخزن وتنتقل بواسطة الشبكات (عبابنه، 2005، 165).

وأشارت الاتفاقية من خلال فصولها الخمسة إلى إلزام الدول الأعضاء بوجوب اتخاذ الإجراءات التشريعية اللازمة على المستوى الوطني للحد من هذه الجرائم ومكافحتها، ووجوب التعاون الدولي والتنسيق بين الدول وتطبيق التشريعات الدولية المتعلقة بهذا الخصوص (الحسيناوي، 2009، 152)، وإن كانت هذه الاتفاقية في الواقع مسودة أو مشروعاً، إلا أنها تعتبر بمثابة القانون بين الدول الأعضاء والتي بموجبها تلتزم الدول الأعضاء في المجلس والموقعون على الاتفاقية بضرورة العمل على تنفيذ أحكامها والخضوع إليها، وتطويع النصوص القانونية لعدم التعارض معها (عبابنة، 2005، 169).

المطلب الثالث: معاهدة بودابست لمكافحة جرائم الحاسوب لعام 2001:

(The Budapest Convention on Cyber Crimes)

في أواخر عام (2001) شهدت العاصمة المجرية بودابست ميلاد أولى المعاهدات الدولية الرسمية التي تُعنى بمكافحة جرائم الإنترنت، وتبلور التعاون والتضامن الدولي في محاربتها ومحاولة الحد منها، لاسيما بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات، وتهدف هذه الاتفاقية إلى توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت، والتي انتقلت من جرائم بسيطة تتمثل في محاولات التسلل البريئة التي كان يقوم بها هواة في الأغلب الأعم، إلى جرائم أشد خطورة أصبح يقوم بها محترفون على أعلى درجة من الكفاءة والتخصص، كالاحتيال المعلوماتي، والاختلاس، وجرائم تهديد الحياة، وهي جرائم تعرض حياة العديدين من رواد الشبكة المعلوماتية إلى الخطر (الطائي، 2007، 227).

وقد جاءت هذه الاتفاقية نتيجة لما يسمى بالانفلات الأمني في مجال الأنظمة المعلوماتية، وفي الوقت الذي زاد فيه ارتكاب هذا النوع من الجرائم من قبل المخترقين والقراصنة، والذين يتمتعون بدرجات عالية من الكفاءة والتخصص، بحيث لم يكتفوا بالتوصل إلى أجهزة الحاسب الخاصة بالأفراد العاديين والمؤسسات والشركات الخاصة، وإنما اجتازوا هذه المرحلة لاختراق الأنظمة المعلوماتية التابعة لأجهزة الدول والحكومات، وما تحتويه من بيانات ومعلومات معالجة آلياً تتعلق بسياسات الدول واستراتيجياتها العسكرية والأمنية ومنظومتها الاقتصادية والتجارية والصناعية، وما تحويه أيضاً من بيانات ومعلومات تتعلق بالحياة الخاصة للأفراد، وكل ذلك يقابله تدني مستوى السيطرة من قبل الدول وأجهزتها الأمنية للحد من هذه الجرائم ومكافحتها، ولهذه الأسباب مجتمعة فإنه ليس من المستغرب أن يأتي المفكر الإنجليزي الشهير أنتوني جيدنز (Anthony Giddens)، وهو أستاذ علم الاجتماع في جامعة كامبردج، ويصف العالم الحاضر بأنه "عالم منفلت". (Runaway World) لا يمكن الإمساك به او إخضاعه للسيطرة، وأن يصدر كتاباً يحمل هذه التسمية. "عالم منفلت: كيف تشكل العولمة حياتنا".(Anthony, G. 1999, The Title).

لـذلـك فقـد حرص المجلس الأوروبي على صـــيـاغـة بنود هـذه الاتفـاقيـة حول الإجرام الإلكتروني وإصدارها بعد التوقيع عليها في شهر تشرين الثاني من عام 2001 في بودابست، وقد جاءت في مقدمة وثماني وأربعين مادة مقسمة إلى أربعة فصول (الزيدي، 2003، 155).

وقد جاء التوقيع على هذه الاتفاقية من قبل الم ســؤولين في الدول الأوروبية إضــافةً إلى الولايات المتحدة الأمريكية، واليابان وكندا وجنوب أفريقيا، وذلك نتيجة مباحثات ومفاوضــات اســتغرقت أكثر من أربعة أعوام، وأوضحت الاتفاقية أن العديد من الدول لا تستطيع بمفردها مواجهة تلك الجرائم التي ترتكب عبر الإنترنت مهما سن ت من قوانين ومهما غلظت من عقوبات، نظراً لكون هذه الجرائم من الجرائم العابرة للحدود لا يقف أمامها أي عائق جغرافي، لذلك فإن هذه الدول تفضل الانضمام إلى المعاهدات الدولية التي تبرم في هـذا المجال نظراً لكبر حجم الأضرار عن طريق الإنترنت، ولأن العديد من الدول حتى المتقدمة منها لا تستطيع مواجهة تلك الأخطار بمفردها دون وجود تعاون وتضامن دولي (الطائي، 2007، 228).

وقـد تضــمنت هذه الاتفاقية معظم الجرائم المعلوماتية ا بتداءً من الولوج غير القانوني إلى النظام المعلوماتي والاعتراض غير القانوني، ولغاية جرائم الإرهاب الإلكتروني والجرائم ضــد الخصــوصــية، والتزوير المعلومـاتي، والغش المعلومـاتي، وجرائم دعـارة الأطفـال وغيرهـا من الجرائم المعلومـاتيـة الخطيرة (الزيدي، 2003، 156 وما بعدها).

ومن خلال مـا تقدم فإن الباحث يرى أن المجتمع الدولي وبالأخص الأوروبي حاول وبشــتى الطرق وعلى مر سـنين مضـت أن يصـدر تشـريعات وقوانين ومعاهدات وقواعد توجيهية وإرشادية بغرض مواجهة الاعتداءات التي تطال معطيات الأنظمة المعلوماتية، في الوقت الذي كثر فيه اختراق هذه الأنظمة وبشــتى الوسـائل والطرق التقنية وبالأخص في الدول المتقدمة، مع تدني مسـتوى السـيطرة من قبل هذه الدول على الصــعيـد الوطني، الأمر الذي دعا منظمة الأمم المتحدة والمجلس الأوروبي إلى مناداة المجتمع الدولي لعقد اتفـاقيـات ومعـاهـدات بهدف الحد من هذه الجرائم، وضرورة التعاون والتنســيق بين أفراد هذا المجتمع للســيطرة عليها، نظراً لما تتمتع به هذه الجرائم من طبيعة خاصــة تختلف عن ما كان ســابقاً من الجرائم التقليدية.

المطلب الرابع: الجهود العربية لمواجهة جرائم الحاسوب والإنترنت:

حـاولـت الدول العربية أن تنتهج نهج الدول الأوروبية المتقدمة من أجل التعاون والتنســـيق فيما بينهـا لتوفير الحمايـة للبيـانات والمعلومات المعالجة آلياً من خطر الأنظمة المعلوماتية وبالأخص الحاســـب الآلي وشبكة الإنترنت.

ومن أبرز الجهود العربيـة التي تكللت بالنجاح هو اعتماد جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي بالقانون العربي الاسترشادي النموذجي لمكافحة جرائم تقنية المعلومات وما في حكمها، وقد سـمي أيضـاً بالقانون الإماراتي العربي الاسـترشادي نسبة لاقتراحه من قبل دولة الإمارات العربية المتحدة (العزام، 2009، 146).

وقد صـــدر القانون العربي النموذجي أو الاســـترشـــادي والخاص بمكافحة جرائم الحاســـب الآلي والإنترنت – كثمرة عمل مشـترك – بين مجلس وزراء الداخلية العرب، ومجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية، بعد أن تبين أن كليهما قدم مشـروعاً في هذا الخصوص، وبالفعل امتد اجتماعهما المشـترك في 21-2003/5/22 حيث تم النظر في المشروعين اللذين تم إعدادهما في المجلسين، وتم إعداد مشـروع قانون مشـترك، عرض على المجلسـين في الدورة العادية لكل منهما حيث تم إقراره (حجازي، 2006، 10).

وبالرجوع إلى المذكرة الإيضـــاحية لهذا القانون فقد احتوى الباب الســـابع الخاص بالجرائم ضـــد الأشـخاص فصـلاً خاصـاً بالاعتداءات التي تقع على حقوق الأشخاص الناتجة عن المعالجة الآلية للمعلومات وذلك في المواد 461-464، كما أشـــارت المواد 161-163 إلى لزوم حماية الحياة الخاصـــة للأفراد من الأخطار التي قد تقع عليها من الأنظمة المعلوماتية، وكيفية جمع المعلومات الإسمية الشخصية وكيفية الاطلاع عليها (الحسيناوي، 2009، 159)

كما وأن المادة 464 جرمت أفعال الدخول بطريقة الغش إلى النظام المعلوماتي أو جزءَ منه، وعرقلة أو إفســـاد نظـام التشـــغيـل عن أداء وظـائفـه المعتادة، وجرمت أيضـــاً الأفعال التي تطال تغيير وتعديل المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية، وسرقة المعلومات (عبابنة، 2005، 171).

وبشـكل عام فقد وضـع هذا القانون القواعد الأسـاسية التي يتعين على المشرع العربي اللجوء إليها عند سـن تشـريعات وطنية لمكافحة هذه الجرائم، سـواء أكان هذا التشـريع مسـتقلاً لمكافحة هذه الجرائم المسـتحدثة، أم كان تعديلاً لقانون العقوبات التقليدي، كما وأشـار هذا القانون إلى الجرائم التي تقع عن طريق الحاسـب الآلي وشـبكة الإنترنت بصـفة عامة، وحدد عقوباتها، وأحال إلى التشـريع الوطني ما يتعلق بأركان هذه الجرائم وكذلك العقوبات التي تطبق عليها (حجازي، 2006، 9 وما بعدها).

وتعتبر هذه المحاولة وعلى الرغم من تواضـعها من أبرز ما خرج إلى حيز الوجود على صعيد تعزيز التعاون على مستوى الوطن العربي من الناحية التشريعية (العبابنة، 2005، 171).

ويرى الباحث أنه ومن خلال هذه التجربة العربية المتواضعة إلا أنها تعتبر قاعدة الأساس لخطوات تعاون مسـتقبلية على الصـعيد العربي، للوصـول إلى أقصى ـ درجات الحماية الجنائية للبيانات والمعلومات المعالجة آلياً، وحمايتها من أخطار الاعتداءات التي قد تقع عليها من خلال الأنظمة المعلوماتية، ونأمل دائماً أن يتم التعاون الدولي العربي وبشكل دوري ومتناسق من أجل الخروج باتفاقية أو قانون شامل لكافة صور الجرائم المعلوماتية، وأن يُعـ زز التعاون العربي في المجالات الموضـوعية والإجرائية لمثل هذه الجرائم تحقيقاً للحد منها ومكافحتها، وجعل المجتمع العربي مجتمعاً خالياً من الإنفلات الأمني المعلوماتي.

الفصل الثالث-

الحماية الجنائية للمعلومات المعالجة آلياً في إطار نصوص جرائم الأموال:

يعيش العالم في وقتنا الحاضر أكبر أحداث مؤثرة في التاريخ البشـري، حيث الخسـائر المالية الناتجة عن مراوغة الدخلاء المفترضين واختلاساتهم الكبيرة للمال عن طريق نظام المعلومات (إزرائيل، 2010، 35).

ويقوم الاقتصـاد في يومنا هذا مرتكزاً على الثورة المعلوماتية المتجددة، وكان مصـير الدول التي لم تواكب ولم تلحق هذا التطور التهميش، وتشكل شبكة الإنترنت البنية الأساسية لهذا الاقتصاد، حيث أصبحت سـوقاً إلكترونية وقناة للاتصالات تربط الدول بعضـها بعضا، بحيث تؤدي الأعمال الاقتصادية بشتى أنواعها بشكل فوري وبتكلفة أقل وأسعار أقل، مع درجة عالية من الشفافية.

وقـد أصـبحـت المعلومات تلعب دوراً هاماً في الحياة الاقتصـادية، حيث تقوم معظم العمليات الاقتصـادية على لغة الأرقام والمعلومات سـواء المخزنة في الحاسـب الآلي أو المتبادلة عبر الشـبكة العالمية للمعلومات (الإنترنت)، و كما ذكرنا سـابقاً فلم يعد ينظر إلى الم علومات وفقاً للمفهوم التقليدي، فعلى الرغم من الطبيعة المعنوية التي تتمتع بها إلا أنها تشـكل قيماً اقتصـادية، وتتمتع بصـفات الذاتية والاسـتقلال وإمكانية اعتبارها سـلعاً تباع وتشترى كالمال، وإمكانية أن تكون محلاً للعقود شأنها في ذلك شأن المال، وهي إما أن تـ جسـد أو تمثل أموالاً أو أصولاً أو أسراراً أو بيانات شخصية أو لها قيمة بذاتها كالبرامج، وبالتالي يجب أن تكون محلاً للحماية القانونية والجزائية مع مراعاة طبيعتها المعنوية.

وقد جاء التطور التقني لنظم المعلومات ليس خادماً فقط للتقدم الاقتصـادي والاجتماعي والثقافي والسـياسي في الدول، وإنما ذهب الجناة إلى اسـتثماره لكي يرتكبوا جرائمهم عبر شـبكة الإنترنت ويحققوا أغراضـهم في تحقيق الثراء المادي أو غيره، وذلك عن طريق الاعتداء على المعلومات ذات القيم المالية والتي تشـكل أموالاً أو أصولاً لمؤسسات أو شركات استثمارية أو مصانع أو غيرها، الأمر الذي أدى إلى ظهور سلسلة من الجرائم المعلوماتية التي تقع على المعلومات سـواء المخزنة في الحاسـب الآلي أو المتبادلة عبر الشـبكة العـالميـة للمعلومـات (الإنترنـت)، وفي هـذه الحالة نكون أمام جرائم معلوماتية واقعة على المعلومات ذات القيم المالية، وحيث إنه من الصـعب حصر- جميع الجرائم المعلوماتية التي قد تنحصر- تحت هذه الطائفة، وأن المجال لا يتسع للبحث في كافة صورها،

فإننا سوف نتناول في هذا الفصل أهم الجرائم الواقعة على المعلومات ذات القيم المالية، من خلال بيان أركانها، وصـــورها وأســـاليبها التقنية، مقارنة بالجرائم الواقعة على الأموال والمنصـــوص عليها في قوانين العقوبات التقليدية، وبيان مدى كفاية النصـــوص الجزائية الأردنية لمواجهتها وتوفير الحماية الجنائية اللازمة لهذه المعلومات مقارنة بالتشـريع الأمريكي وبعض التشـريعات المقارنة في بعض الأحيان، حيث سـنبحث في جريمـة سرقـة المعلومـات المعـالجـة آليـاً، وجريمة إتلاف المعلومات المعالجة آلياً، وجريمة إعاقة عمل النظام المعلومـاتي نظراً لتـداخلها وترابطها مع جريمة الإتلاف المعلوماتي من حيث إن الأفعال التي قد تؤدي إلى كلٍ منهما واحدة، وأخيراً جريمة الاحتيال المعلوماتي وذلك من خلال المباحث التالية:

أولاً: جريمة سرقة المعلومات المعالجة آلياً.

ثانياً: جريمة إتلاف المعلومات المعالجة آلياً.

ثالثاً: جريمة إعاقة عمل النظام المعلوماتي.

رابعاً: جريمة الاحتيال المعلوماتي.

المبحث الأول: جريمة سرقة المعلومات المعالجة آلياً

إن العالم يشـهد أنماطاً جديدة من الجرائم وقيماً إنحرافية متعددة بسـبب التقدم الهائل في صناعة الإلكترونيات وما يحققه من تطور هائل في تطبيقاتها العملية، فهناك من يقوم بسرقة المعلومات عن طريق النظام المعلوماتي وهناك من يختلس الملفات والبرامج، إذ تنخرط في هذه الأعمال عناصر شـــبابية تبحرت في علوم الحاسـب وحاولت أن تثبت ذاتها في هذا المجال، وهكذا يشهد العالم حوادث اقتحام النظام المعلوماتي وانتهاك أمن المعلومات مما دعا إلى ضرورة الإهتمام بتطوير السياج الأمني لنظم المعلومات (حجازى، أحمد مجدي، 2005، 45).

وقد أصـــبحت المعلومات تتمتع بقدر عال من الأهمية في ظل الثورة المعلوماتية وتقنية تكنولوجيا المعلومات، والتي تعتمد وبشـكل أساسي على نظم المعالجة الآلية للبيانات وتحويلها إلى معلومات قد تكون شخصية خاصة بأفراد معينين أو شركات أو حكومات أو دول، وقد تكون معلومات ذات قيمة اقتصادية تباع وتشـترى وتخص أرقاماً خيالية من الاسـتثمارات والحسابات والأرصدة البنكية، وبالتالي باتت مشكلة يواجهها المشرعون الوطنيون في شتى أنحاء العالم، لاتخاذ الإجراءات اللازمة والتدابير الاحترازية

لســن تشـريعات رصـينة ومحكمة تواكب تطور هذه التقنية الحديثة وتوفر سـبل الحماية لهذه ا لمعلومات التي تشــكل قيماً اقتصــادية ومصــالح يمكن الاعتداء عليها من قبل المجرمين، لذلك أصــبحت لموضــوع جرائم الاعتـداء على المال المعلوماتي أهمية متزايدة ســواء من الناحية النظرية أو العملية، فمن الناحية النظرية يمكن أن ينطبق على مجموعة من جرائم الأموال مثل جريمة السرقة والاحتيال وغيرها، ومن الناحيـة العمليـة ظهرت طائفة من المجرمين تترقب دائماً عمليات نقل وإرســال وتبادل المعلومات ســواء المخزنة في الحاسـب الآلي أو المتبادلة عبر الشـبكة العالمية للمعلومات (الإنترنت)، وذلك من أجل الاسـتغلال غير المشـروع لهذه المعلومات التي تشـكل قيماً اقتصادية ومالية أحياناً، ومن أكثر الأساليب انتشاراً في مجال الاعتـداء على المعلومات هو سرقة المعلومات، وذ ظراً لأننا سـنتناول في هذا المبحث جريمة سرقة المعلومات عبر شـبكة الحاسوب والإنترنت في القانون الأردني مقارنة بالقانون الأمريكي مع إلقاء الضوء أحياناً على بعض التشريعات الأخرى، فإن ذلك يستوجب أن نبين القواعد العامة لجريمة السرقة التقليدية في التشريع الأردني، وكذلك آراء الفقه تجاه هذه الجريمة التقنية، وموقف المشـرع الأردني والأمريكي من جريمة سرقة المعلومات عبر الحاسوب والإنترنت. وذلك من خلال المطالب التالية :

1- القواعد العامة لجريمة السرقة التقليدية.
2- الاتجاهات الفقهية حول مدى اعتبار المعلومات المعالجة آلياً محلاً لجريمة السرقة.
3- موقف المشرع الأردني من جريمة سرقة المال المعلوماتي.
4- موقف المشرع الأمريكي من جريمة سرقة المال المعلوماتي.

المطلب الأول: القواعد العامة لجريمة السرقة التقليدية:

لقد كان القانون الروماني وهو الأصـل التاريخي لمواد السرـقة في التشرـيعات اللاتينية يعتبر السرقة Contraction من قبيل اسـتيلاء الجاني على ملكية المال المسرـوق Furtum، أو منفعته Furtum uses، أو حيازته Furtum Possessions، سـواء بسـواء، وكان يعتبر جريمة السرـقة والاحتيال وإسـاءة الائتمان جريمة واحدة أطلق عليها كلمة Furtum (الملط، 2006، 208).

وتعرف السرـقـة لغة بأنها "أخذ المال خفية عن صـــاحبه، وسرق الشيـــء يعني أخذه منه خفية وبحيلة".(المعجم العربي)

أما قانوناً فالسرـقة هي " أخذ مال الغير المنقول دون رضـاه"، وتقوم جريمة السرـقة التقليدية على ثلاثة أركان وهي:

أ- الركن المادي المتمثل بفعل الأخذ دون رضاء المجني عليه.

ب- محل الجريمة: وهو المال المنقول المملوك للغير.

ج- الركن المعنوي: وهو القصـد الجرمي المتمثل بإرادة ارتكاب فعل أخذ مال الغير دون رضـاه وذلك بنية تملكه.

الفرع الأول: الركن المادي في جريمة السرقة التقليدية:

يقوم الركن المادي في جريمة السرقة على عنصرين أحدهما مادي وهو أخذ المال والاستيلاء على الحيازة والملكية (الاختلاس)، والآخر معنوي وهو عدم رضاء مالك الشيء أو حائزة عن الفعل.

العنصر المادي- المتمثل في أخذ المال والاستيلاء على الحيازة والملكية (الاستيلاء):

اختلف الفقـه حول تحـديد مفهوم أخذ المال (الاسـتيلاء) تبعاً للتطور التاريخي للحماية الجزائية للأموال، وذلك وفقاً لنظريتين هما النظرية التقليدية، والنظرية الحديثة لدى جارسـون (الجبور، 2010، 19 وما بعدها).

وبمقتضىـ الفقه التقليدي فإن أخذ المال في السرـقة يعني نقل الشيـء أو نزعه من المجني عليه وإدخـاله في حيازة الجاني بقصـد تملكه بغير علم من المجني عليه وبدون رضـاه، وعلى الرغم من أن هذا التعريف فرق بين جريمة السرـقة والاحتيال وإسـاءة الائتمان، إلا أنه وجه إليه النقد، إذ أنه يؤدي إلى نتائج خطيرة تتمثل في إفلات الجاني في كثير من الأحيان من العقاب، كما هو الحال حين يقوم البائع بتسـليم المال إلى الشـخص الذي يرغب في شرائه كي يطلع عليه قبل الشرـاء فيغتنم الفرصـة ويهرب بالمال، ووفقاً للفقه التقليدي فإن هذا الشـخص سـوف ينجو من العقاب ولا يسـأل عن جريمة السرـقة (نمور، 2007، 23 وما بعدها).

أما بالنسبة لمفهوم أخذ المال وفقاً للفقه الحديث، فقد رأى أصحاب هذا الاتجاه بضرورة البحث في مـاهيـة فعـل الأخـذ المكون لجريمة السرـقة وفقاً لنظرية الحيازة القانونية في القانون المدني، وهي الحيازة الواقعية التي تخول الشـخص قدرة على الشيء فيستعمله أو ينقله أو يعدمه أو هي وضع مادي يسيطر به الشـخص على الشيـء سـيطرة فعلية، ولذلك فقد عرفوا فعل الأخذ بأنه "سـلب الحيازة الكاملة للشيـء بغير رضاء المالك أو الحائز السابق" (الجبور، 2010، 24).

وقد اســتقر الفقه على تعريف مفهوم فعل الأخذ بأنه "ســلب حيازة الشيــء بعنصرــيها المادي والمعنوي، بدون رضاء مالكه أو حائزه السابقة" (سرور، 1985، 805).

العنصر المعنوي- عدم رضاء المالك أو الحائز عن الأخذ:

لا يكفي لاعتبار الفعل أخذاً للمال أن يترتب عليه خروج الشيء من حيازة المجني عليه ودخوله في حـ يازة الجاني، وإنما يلزم إضافةً إلى ذلك أن يكون انتقال الحيازة على هذا النحو بدون رضاء مالك الشيء أو حائزه، فانتقال الحيازة برضاء المجني عليه لا يشكل جريمة سرقة، ويعتبر العنصر المعنوي المتمثل في عدم رضاء الحائز أو المالك عنصراً جوهرياً هاماً في الركن المادي لجريمة السرقة، وإن عدم توافره يؤدي إلى انعدام وجود السرقة، ويتحقق هذا العنصر بأن يقوم الجاني بسلب حيازة الشيء من المالك أو الحائز ونقله إلى حيازته، أما إذا تم التسليم بإرادة المالك وصادراً عنه فإن ذلك لا يشكل اعتداء على مال مملوك للغير وبالتالي لا يشكل جريمة سرقة.

الفرع الثاني: محل جريمة السرقة التقليدية (مال منقول مملوك للغير):

تعتبر جريمة السرقة التقليدية من الجرائم الواقعة على الملكية، وحتى تقع هذه الجريمة يجب أن يكون محلها مالاً ذا طبيعة مادية، فالمال المادي هو الذي يصلح أن يكون محلاً للملكية، أما الأموال المعنوية فلا تصلح لأن تكون محلاً لجريمة السرقة، ويجب أن يكون هذا المال منقولاً ومملوكاً للغير. وذلك كما يلي:

أولاً: الشيء المسروق مالاً:

يجب أن يكون محل السرقة مالاً مادياً صالحاً للتملك، وقد عرفت المادة (53) من القانون المدني الأردني المال بأنه "كل عين أو حق له قيمة مادية في التعامل بصرف النظر عن ضآلة قيمته"، ومن خلال هذا التعريف نجد أن المال يجب أن تكون له قيمة مادية بصرف النظر عن نسبة هذه القيمة حتى ولو كانت قليلة وضئيلة، فالمشرع الجنائي التقليدي في النصوص الخاصة بالجرائم الواقعة على الأموال أفرد الحماية للأشياء القابلة للتملك والتي لها طبيعة مادية في التعامل، أما إذا كانت غير قابلة للتملك وليست لها طبيعة مادية في التعامل فإن أخذ هذه الأشياء دون رضاء مالكها أو حائزها لا يشكل جريمة سرقة بل قد يشكل جريمة أخرى (الحلبي، 2010، 33 وما بعدها).

وترجع العلة في اشـتراط أن يكون المال محل السرـقة ذا طبيعة مادية لأن جريمة السرـقة هي من جرائم الاعتـداء على الملكيـة ويتطلـب الركن المـادي لتحققهـا إلى انتزاع ملكيـة المـال من حـائزه أو مـالكه وإدخاله في ملكية السـارق، وهذا لا يمكن تصوره إلا في الأشياء المادية، فالسرقة لا تقع إلا على مال ذي كيان مـادي ملموس ويصـــلح للتملـك قانوناً، كالنقود والمجوهرات، والآلات، والمحاصـــيل الزراعية، والحيوانات، والغازات، والسـوائل بشـتى أنواعها... وغيرها فإذا كان الشيـء لا ينطبق عليه وصف المال بهذا المعنى لعدم قابليته للتملك فلا يصلح أن يكون محلاً لجريمة السرقة التقليدية.(نمور، 2007، 58 وما بعدها).

ثانياً: الشيء المسروق منقولاً:

يجب أن يكون المال محل السرـقة منقولاً بحيث يستطيع الإنسان نقله من مكان إلى آخر، فالسرقة مثلاً لا تقوم على عقـار، ونتيجـة للتعـارض بين التشرـــيع الجزائي وبين مـدلول المال في القوانين المدنية فقد ذهـب جـانـب من الفقـه إلى أنـه يدخل في مفهوم المال المنقول كل شيء يمكن نقله من مكان إلى آخر ولو بتلف يسير، وقد وسع المشرع التقليدي من مدلول المال المنقول محل السرقة، بحيث يشمل ما يلي:

- المنقولات المادية كالحيوانات والأثاث والنقود والملابس والسيارات والسفن والطائرات.
- العقارات بالتخصـيص مثل أدوات الزراعة المخصـصـة لخدمة مزرعة، وآلات المصـنع المخصـصة لأغراضه وعربات نقله، والجرارات الزراعية المخصصة لخدمة المزرعة.
- كل أجزاء العقار بالاتصـال إذا نزعت عن أصـلها الثابت كالشـبابيك والأبواب والأحجار إذا اقتلعت من الأرض (الجبور، 2010، 49-50).

ثالثاً: الشيء المسروق مملوكاً للغير:

يجب أن يكون المال محل السرـــقة مملوكاً للغير وليس مملوكاً للجاني، فالسرـــقة لا تقع من المالك على ملكـه حتى ولو كـان سيء النيـة بـأن يعتقـد أن المال مملوك للغير، والعبرة في ذلك هو رغبة المشرـــع الجزائي حماية ملكية الأفراد من الاعتداء عليها.

ولا يشترط لوقوع جريمة السرقة معرفة مالك أو حائز المال المسروق أو تحديد هويته فهذه الجريمة تقع بمجرد نقل حيازة المال المنقول المملوك للغير بصرـف النظر إذا كان مالكه معروفاً أو غير معروف، ومع ذلك فيشترط أن يكون هذا المال مملوكاً للغير

وليس مالاً مباحاً أو متروكاً للكافة، كما وأنه لا يشترط أن يكون هذا المال من الأموال المباح حيازتها قانوناً، فالسرـــقة تقع حتى على المال الذي تعد حيازته من الجرائم أو المخالفات، كأن تقع على ســـلاح غير مرخص مملوك للغير، أو على المواد المخدرة التي يمنع القانون حيازتها (نمور، 2007، 69 وما بعدها).

الفرع الثالث: الركن المعنوي في جريمة السرقة التقليدية:

تعتبر السرقة جريمة قصدية ولوجودها لابد من توافر القصد الجرمي، حيث تتطلب قصداً جرمياً عاماً يتمثل بأن يكون الفاعل عالماً بجميع أركان جريمة السرـــقة وعناصرها، وذلك بأن تتجه إرادته إلى إتيان سلوكه الجرمي المتمثل في أخذ المال المنقول المملوك للغير دون رضاه، ويتوافر عنصري هذا القصد العلم والإرادة، كما وأنها تتطلب قصداً جرمياً خاصاً وهو "نية التملك" المتمثل بانصراف إرادة الفاعل إلى الاستيلاء على المال المنقول المملوك للغير وتملكه وحرمان صاحبه من التصرف فيه، فجريمة السرقة شأنها شأن معظم الجرائم الواقعة على الأموال يستوجب لوقوعها توافر القصد الجنائي الخاص إضافة إلى القصد الجنائي العام.

- وقت توافر القصد الجنائي في السرقة التقليدية:

الأصل في القصد الجنائي بشقيه العام والخاص أن يكون معاصراً في وجوده مع فعل الأخذ والاستيلاء، حيث ذهب أغلبية الفقه إلى القول "إنه إذا توافر القصـــد الجنائي في وقت لاحق على ســـلب الحيازة أو لم يتعاصر معها فإن جريمة السرـــقة لا تقوم"، كمن يقوم بإخراج المال من حيازة مالكه أو حائزه معتقداً أنه ملكه، فلا يتوافر لديه في ذلك الوقت القصد الجرمي لأنه وقت الأخذ كان يجهل أن المال محل الأخذ مملوكً للغير، حتى ولو ساءت نيته في وقت لاحق بعد الأخذ، (الجبور، 2010، 73).

وكذلك الأمر إذا اســـتولى الفاعل على مال كان يعتقد أنه مال مباح ويجهل أنه مملوك لغيره فإن القصد الجرمي لا يتوافر بحقه، وبالتالي لا تتوافر بحقه أركان جريمة السرقة (الحلبي، 2010، 60).

المطلب الثاني: الاتجاهات الفقهية حول مدى اعتبار المعلومات الإلكترونية محلاً لجريمة السرقة التقليدية:

ذكرنا فيما ســبق أن جريمة السرـقة هي الاســتيلاء بنية التملك على مال منقول مملوك للغير دون رضاه، وذلك حسب القواعد العامة في قوانين العقوبات التقليدية،

وبيّنا بأن فعل الأخذ أو الاستيلاء يرد على مال منقول مملوك للغير، ومن المعروف أن المكونات المادية للنظام المعلوماتي والمتمثلة في جهاز الحاسوب والأجهزة والمعدات الملحقة به والأشرطة الممغنطة والدعامات والأقراص والتي تحوي المعلومات والبرامج والبيانات والكابلات وشبكات الربط وغيرها تعتبر مالاً مادياً منقولاً وله كيان مادي ملموس، وبالتالي فهي قابلة لأن تكون محلاً لجريمة السرقة التقليدية المنصوص عليها في قوانين العقوبات التقليدية، وهذا الأمر لا يثير أية إشكالية لأن هذه الأشياء بطبيعتها المادية الملموسة تمثل قيماً مادية ومالية يمكن الاعتداء عليها بالسرقة وبالتالي تطالها تشريعات العقوبات التقليدية بالحماية.

كما وأن التشريعات التقليدية تطبق على جرائم السرقة التي تقع على الأموال المادية الملموسة والتي تستخدم فيها الوسائل الإلكترونية مثل بطاقات الائتمان المصرفية، كأن يقوم شخص بسرقة هذه البطاقة واستخدامها بدلاً من حاملها للحصول على مال الغير، فهنا تطبق النصوص التقليدية لأن محل الجريمة هو مال منقول مملوك للغير ذو طبيعة مادية، ولكن الجاني استخدم في إتيان فعله الإجرامي وسيلة إلكترونية.

إلا أن المشكلة تثور عندما يتعلق الأمر بالسرقة الإلكترونية عبر الحاسوب والإنترنت والتي تنصب بشكل أساسي على المعلومات ذات الطبيعة المعنوية غير المحسوسة، خاصة في البلدان التي لم يواكب مشرعوها التطور التقني ولم يلحقوا بتشريعاتهم هذه الجرائم المستحدثة، وبهذا النطاق يثور سؤال هام وهو هل المعلومات تعتبر من الأموال المادية أو الأموال المنقولة التي تصلح محلاً للسرقة، وبالتالي محلاً لحماية المشرع الجزائي؟

ومن هنا نجد أن الفقه انقسم بين مؤيد ومعارضٍ حول مدى إمكانية أن تكون المعلومات المعالجة آلياً محلاً لجريمة السرقة، وبالتالي انطباق وصف المال عليها، وذلك كما يلي:

الفرع الأول: الاتجاه الفقهي الأول الذي يرى في المعلومات المعالجة آلياً محلاً يقبل السرقة:

ذهب أصحاب هذا الرأي إلى أن المعلومات يمكن أن تكون محلاً لجريمة السرقة التقليدية، حيث أنها تعتبر مالاً ولها قيمة مالية ويمكن تطبيق النصوص التقليدية لجريمة السرقة عليها، وقد استند أصحاب هذا الرأي على الحجج الآتية:

(1) إن المعلومات عبارة عن مجموعة من الأفكار ناتجة عن عمل ذهني لمبتكرها كتلك التي تنشأ بين المالك والشيء الذي يمتلكه، فيكون له نقلها، وإيداعها، وحفظها، وتأجيرها وبيعها، فالمعلومات لها قيمة اقتصادية كالأموال، وتطرح للتداول في الأسواق وتباع وتشترى وفقاً للسوق الاقتصادية، وبالتالي فهي محل لجريمة السرقة (الملط، 2006، 239).

(2) إن سرقة المعلومات الإلكترونية دون رضاء مالكها أو حائزها الشرعي تعتبر من قبيل الاستيلاء أو اختلاس مال مملوك للغير، وهذا بالضرورة يؤدي إلى وقوع جريمة السرقة، وإن هذا الاعتبار لا يتعارض مع النص القانوني من ناحية، ولا حتى مع روح القانون من ناحية أخرى، وإن ذلك نتيجة منطقية للتطور القانوني في مجال السرقة بوجه عام، وبالتالي لابد من توفير الحماية الجزائية لهذه المعلومات عن طريق تطبيق النصوص التقليدية الخاصة بالسرقة، إضافة للحماية التي توفرها قوانين حماية حق المؤلف (الملكية الفكرية) (قوره، 2005، 150)

(3) إن المعلومات تتمتع بصفة المال لأن لها قيمة اقتصادية معينة قد تقدر بثروات طائلة، وأن صفة المال لا تنتفي إلا عن الشيء الذي لا قيمة له، وبالتالي لا يصلح أن يكون محلاً للسرقة، فطالما أن للمعلومات قيمة تقدر بثروات معينة فإنها تصلح لأن تكون محلاً للسرقة (حجازي، 2006، 423).

(4) صحيح أن المعلومات من الأموال المعنوية إلا أنه من الممكن أن تكون محلاً لجريمة السرقة، وذلك بأن يقوم الجاني بالوصول إلى كلمة السر- بطريقة فنية سواء أكان من الأشخاص الذين يعملون في النظام المعلوماتي أم أي شخص آخر يستطيع الوصول إلى هذه الكلمة عن طريق وظيفته، فيقوم هذا الجاني بالتقاط المعلومات المعالجة آلياً أو سرقتها بطريقة النسخ أو طباعتها أو نقلها والاستيلاء عليها ونقل حيازتها من مالكها أو حائزها القانوني إلى حيازته وتتحقق هنا جريمة السرقة (إبراهيم، 2009، 304).

(5) إن جريمة سرقة المعلومات الإلكترونية شأنها شأن الجرائم التقليدية يترتب عليها ضرر للغير، فقد يكون الهدف من السرقة هو الاطلاع على أسرار معينة للغير سواء أكانت شركة أم مؤسسة أم دولة أو غيرها، ويتحقق ذلك بأن يقوم الجاني بالدخول إلى النظام المعلوماتي الخاص بالغير والتقاط المعلومات الخاصة به عن طريق سرقتها ونسخها على مستندات أو شرائط، بحيث تصبح هنا المعلومات ذات كيان مادي بتسجيلها على شريط أو بطباعتها ونقلها والاستيلاء عليها (حجازي، 2006، 423).

ونخلص مما سبق أن أصحاب هذا الرأي اعتبروا المعلومات المخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت من قبيل الأموال المادية المنقولة التي يمكن أن تكون محلاً لجريمة السرقة التقليدية الواردة في قوانين العقوبات، لأن لها قيمة اقتصادية مادية، ويمكن نقلها من مكان إلى آخر شأنها شأن الأموال المنقولة، وما يترتب على ذلك من حماية الملكية الفكرية والذهنية وإخضاعها للقانون الجنائي.

الفرع الثاني: الاتجاه الفقهي الثاني الذي لم يعتبر المعلومات المعالجة آلياً من قبيل الأموال المادية(ليست محلاً للسرقة):

ذهب أصحاب هذا الرأي إلى أن المعلومات ليست مالاً مادياً منقولاً ولا يمكن أن تكون محلاً لجريمة السرقة التقليدية، وقد جاؤوا بالحجج التالية:

(1) أن الكيانات المعنوية للنظام المعلوماتي يمكن أن تكون لها قيمة مالية، وهذا ما جعل البعض يعتبرها مالاً، ولكن المفهوم الأدق هو أن هذه المعلومات لا يمكن أن تكون مالاً منقولاً، ولا محلاً لجريمة السرقة التقليدية، ذلك لأنها يمكن أن تُستغل مالياً، إلا أن هذا الاستغلال لا يضفي عليها صفة المال، كما وأن المعلومات إما أن تكون سرية وخاصة بمبتكرها أو مخترعها من حيث الاطلاع عليها وحيازتها لذلك فأي اعتداء عليها من قبل الغير يشكل انتهاكاً لسريتها وليست سرقة، وإما أن تكون غير سرية وفي هذه الحالة قد تكون مجانية ومباحة للجميع، أو قد تكون بمقابل وهنا يشكل الاعتداء عليها سرقة منفعة الحاسب الآلي وليس سرقة المعلومات (الملط، 2006، 237-238).

(2) أن جرائم الأموال جاءت لحماية المنقولات، وأن خاصية المنقول لا تنطبق سوى على الأشياء، والمعلومات عبارة عن أفكار وليست أشياء، وهناك فرق كبير بينهما، كما وأن المعلومات بطبيعتها الخاصة ذات الكيان المعنوي لا يمكن حيازتها كالأشياء، وجرائم السرقة تعتبر اعتداءَ على الحيازة والحيازة لا تتصور إلا على الأشياء المادية، وبالتالي فالمعلومات لا يمكن أن تكون مالاً مادياً ولا محلاً لجريمة السرقة التقليدية (حجازي، 2006، 422).

(3) إن المعلومات لا تصلح أن تكون مالاً إلا إذا اقترنت بالمادية، فلا يمكن أن تكون مالاً منقولاً إلا إذا تم تسجيلها على دعامات مادية أو اسطوانات، وطالما أنها غير مثبتة ومسجلة على هذه الدعامات أو الاسطوانات فهي ليست منقولاً ولا يمكن تصور وقوع السرقة عليها، حتى لو أدى الاعتداء عليها إلى خسائر مادية فادحة (الملط، 2006، 238، وما بعدها).

(4) إن تطبيق المعنى السابق للاختلاس وفق القواعد التقليدية على المعلومات المعالجة آلياً يلاحظ منه أن الجاني وإن كان يدخل في ذمته ما استولى عليه من معلومات إلا أنه في نفس الوقت لم يخرج هذه المعلومات من ذمة صاحبها الشرعي، إذ تظل رغم مباشرة أفعال الاختلاس عليها تحت سيطرة هذا الأخير دون أدنى انتقاص من محتواها، كما يلاحظ أن الاستيلاء على المعلومات لا يُتصور منذ الوهلة الأولى إلا على أنه انتقال لهذه المعلومات من ذهن إلى ذهن أو من ذاكرة إلى ذاكرة، وهكذا لا تقع جريمة السرقة (القهوجي، 2000، 581).

(5) وفي كل الأحوال لا يترتب على سرقة المعلومات خروجها من حيازة مالكها أو حائزها القانوني، وكل ما في الأمر أن الجاني يكون قد حصل على نسخة من هذه المعلومات، مع بقاء الأصل لدى المالك أو الحائز القانوني، وهذا يختلف عن السرقة التقليدية التي تخرج فيها الحيازة من الحائز القانوني إلى حيازة الجاني (إبراهيم، 2009، 304).

ونخلص مما سبق أن أصحاب هذا الاتجاه من الفقه الجنائي لم يُقروا باعتبار المعلومات من قبيل الأموال المادية المنقولة، لأن لها طبيعة خاصة فهي ذات طبيعة معنوية غير محسوسة وهي ليست كالأشياء التي تدخل في الحيازة ذات الطبيعة المادية والكيان المادي المحسوس، ولأن جريمة السرقة تأتي اعتداءَ على الملكية وعلى الحق في الحيازة فلا يمكن تصور وقوعها على المعلومات والتي لا تصلح أصلاً للحيازة، ونلاحظ أن أصحاب هذا الاتجاه قد تأثروا بفكر الفقه الجنائي التقليدي الذي يعتبر جريمة السرقة جريمة مادية لا تقع إلا على الأموال والقيم المادية بصرف النظر عن قيمتها سواء أكانت باهظة أم رخيصة، فالمهم لديهم أن يكون محل هذه الجريمة شيئاً ذا كيان مادي ملموس، يمكن الاعتداء عليه مادياً بسلوك إجرامي مادي يخرج إلى العالم الخارجي النتيجة الإجرامية وهي نقل حيازة المال من المالك أو الحائز القانوني إلى حيازة الجاني.

ويذهب الباحث مع هذا الاتجاه، وهو الرأي الراجح في الفقه الجنائي حيث إن نصوص السرقة التقليدية لا يمكن تطبيقها في الجرائم المعلوماتية وذلك للأسباب التالية:

(1) إن الركن المادي في جريمة السرقة التقليدية يقوم على فعل الأخذ بعنصريه المادي والمعنوي، وأن مفهوم الأخذ يعني سلب حيازة الشيء بعنصرية المادي والمعنوي دون رضاء مالكه أو حائزه السابق، وسلب الحيازة هنا يُعنى إنهاء حيازة المالك أو الحائز القانوني وإنشاء حيازة جديدة وكاملة للجاني، وهذا يمكن تصوره في المال المادي ذي الطبيعة المحسوسة

ولا يمكن تصوره في المعلومات المخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت، لأن الجاني لا يسلب المجني عليه حيازته لهذه المعلومات وإنما يأخذ نسخة عنها، ففي كل الأحوال تبقى حيازة المالك الأصلي أو المجني عليه قائمة، وبالتالي فإن فعل الأخذ بالمعنى التقليدي لا يقع على المعلومات الإلكترونية.

(2) إن محل جريمة السرقة التقليدية هو مال منقول مملوك للغير، والمنقول هو المال المادي ذا الكيان المحسوس والذي يستطيع الإنسان نقله من مكان إلى آخر، ويرجع في تحديد ذلك إلى قوانين العقوبات والقوانين المدنية، أما المعلومات فهي ذات طبيعة معنوية خاصة، ليست محسوسة أو ملموسة ومع أن لها قيماً اقتصادية إلا أنها لا تصلح أن تكون محلاً لجريمة السرقة التقليدية.

وانطلاقاً من مبدأ شرعية الجرائم والعقوبات والذي يقضي بأنه لا جريمة ولا عقوبة إلا بنص، ومبدأ عدم جواز القياس في النصوص الجزائية، فإنه لا يمكن تطبيق النصوص التقليدية الواردة في قوانين العقوبات على الأفعال التي تطال المعلومات بالاعتداء سواء المخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت، والحاجة ملحة على المشرع الوطني بأن يفسر الطبيعة القانونية للمعلومات الإلكترونية من حيث الاعتراف بتكييف المال المعلوماتي المعنوي على أنه مال بالمعنى التقليدي المنصوص عليه في جريمة السرقة، ووضع قوانين خاصة تعالج موضوع سرقة المعلومات.

المطلب الثالث: موقف المشرع الأردني من جريمة سرقة المعلومات المعالجة آلياً والمخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت:

الفرع الأول: موقف المشرع الأردني وفقاً للنصوص التقليدية الواردة في قانون العقوبات الأردني:

عرف المشرع الأردني جريمة السرقة في الفقرة الأولى من المادة 399 من قانون العقوبات رقم (16) لسنة 1960 وتعديلاته بأنها "أخذ مال الغير المنقول دون رضاه"، وفي الفقرة الثانية من ذات المادة عرف عبارة أخذ المال بأنه "إزالة تصرف المالك فيه برفعه من مكانه ونقله وإذا كان متصلاً بغير منقول فبفصله عنه فصلاً تاماً ونقله"، وفي الفقرة الثالثة من نفس المادة بين المشرع الأردني إن لفظة المال تشمل القوى المحرزه.

ومن هنا نجد أن جريمة السرقة وفقاً للمشرع الأردني لا تقع إلا بقيام ثلاثة أركان مجتمعة وهي كما يلي:

1- محل الجريمة: وهو المال المادي المنقول المملوك للغير.

2- الركن المادي: المتمثل في فعل الأخذ دون رضاء المجني عليه.

3- الركن المعنوي: وهو القصد الجرمي المتمثل بإرادة ارتكاب فعل أخذ مال الغير دون رضاه وذلك بنية تملكه.

وفي البحث في مدى انطباق وصف السرقة الواردة في قانون العقوبات الأردني على سرقة المعلومات، فإن نصوص السرقة التقليدية تطبق على السرقة الواقعة على المكونات المادية للحاسب الآلي، كالجهاز ذاته أو الأجهزة الملحقة به، كما وأنها تطبق على المعلومات المثبتة على الدعامات المادية ذات الكيان المادي الملموس، كالأشرطة الممغنطة أو الاسطوانات المدمجة في حال وقوع السرقة على هذه الدعامات المادية، إلا أن المشكلة تثور لدى المشرع الأردني التقليدي في حال إذا انصب الاعتداء على المعلومات المعالجة آلياً، بذاتها. سواء المخزنة في الحاسب الآلي أو المتداولة عبر الإنترنت أو المثبتة على دعامات مادية علما بأن هذه المعلومات تمثل قيماً اقتصاديه أو أصولاً ماليه أو معلومات شخصية خاصة بالأفراد أو غيرها ، لذا فسوف نبحث ذلك وفقاً لكل ركن على حده.

- محل جريمة السرقة (المال المادي، المنقول، المملوك للغير):

وفقاً لنص المادة 1/399 فإن محل جريمة السرقة المال المنقول المملوك للغير، فجريمة السرقة تشكل اعتداء على الملكية، والملكية لا تكون إلا على الأشياء المادية المقومة بقيمة مادية مالية أوبقيمة معنوية عاطفية، ومقتضى قابلية محل جريمة السرقة للنقل أن يكون ذا طبيعة مادية.

وحتى نحدد مدى انطباق وصف السرقة على المعلومات وفقاً للمشرع الأردني لابد من تحديد مدلو ل المال المنقول قانونياً، وحيث إن قانون العقوبات الأردني لم يحدد في المادة الثانية منه والمخصصة للمصطلحات المقصود بالمال المنقول ، ووفقاً لأصول التفسير لابد من الرجوع إلى أحكام القانون المدني باعتباره القانون المرجع للوقوف على مدلول المال المنقول منه، فقد جاء في المادة (53) من هذا القانون أن "المال هو كل عين أو حق له قيمة مادية في التعامل"، وفي المادة (54) من ذات القانون "

كـل شيء يمكن حيـازتـه مـاديـاً أو معنويـاً أو الانتفاع به انتفاعاً مشرـــوعاً، ولا يخرج عن التعامل بطبيعته أو بحكم القانون يصـــح أن يكون محلاً للحقوق المالية"، وجاء في المادة (58) من نفس القانون أن "كل شيء مســـتقر بحيزه، ثابت فيه لا يمكن نقله منه دون تلف أو تغيير هيئته فهو عقار، وكل ماعدا ذلك من شيء فهو منقول".

وبتحليل هذه النصوص بالاستعانة بالمذكرة الإيضاحية للقانون المدني، فإنه حتى ينطبق وصف المال على المعلومات المختزنة في الحاسب الآلي أو المتداولة عبر الإنترنت فإنه لابد من توافر شرطين هما:

الأول: أن حيازة الشيء تكو ن مادية إذا كان الشيء مادياً، وتكون معنوية إذا كان الشيء معنوياً.

والثاني: الانتفاع المادي بها.

وهذان الشرطان متوفران في المعلومات، فهي قابلة للحيازة المعنوية بصدورها من صاحبها وملكيته لهـا، وإن الانتفـاع المـادي بهـا متحقق، وبنـاء على ذلـك يمكن اعتبـار المعلومات من الأموال المعنوية، إلا أن القانون المدني لا يعتبرها منقولة على الرغم من إسباغه وصف الأموال المعنوية عليها. وذلك للأسباب التالية:

(1) إن القانون يتطلب في المنقول أن يكون ذا طبيعة مادية، والمعلومات ليست كذلك.

(2) إن نقل المعلومات في حال الاعتداء عليها من قبل الجاني لا يؤدي إلى شـغور الحيز الذي كانت تشـغله، فالمجني عليه يبقى محتفظاً بهذه المعلومات.

وحيث إن قانون العقوبات الأردني يشـــترط في المال محل السرـــقة التقليدية أن يكون من الأموال المنقولة فإن المعلومات المعالجة آلياً لا تصلح أن تكون محلاً لهذه الجريمة.

- الركن المادي لجريمة السرقة: (فعل الأخذ):

وفقاً لنص المادة 2/399 عرف المشرـــع الأردني فعل الأخذ بأنه "إزالة تصرـــف المالك فيه برفعه من مكانه ونقله، وإذا كان متصـلاً بغير منقول فبفصـله عنه فصـلاً تاماً ونقله"، ومن هذا النص يتضـح أن فعل الأخذ حتى يتحقق فإنه بحاجة إلى توافر عنصرين هما:

الأول: إخراج المال محل جريمة السرقة من حيازة المجني عليه (إنهاء حيازة المالك).

الثاني: إدخال المال في حيازة الجاني (الزعبي والمناعسة، 2010، 138).

وبـذلك نجد أن المشـــرع الأردني أخذ بنظرية تحريك الحيازة، أي بتحريك المال وإبعاده من مكانه ولو قليلاً حتى يتحقق فعل الأخذ، والقضـاء الأردني مسـتقر في أحكامه على أنه لابد من تحريك المال ونقله لكي يمكن اعتبار الشخص سارقاً (نجم، وتوفيق، 1987، 297).

وقد قضت محكمة التمييز الأردنية بهذا الشأن إنه "إذا لم يرد في الأدلة ما يفيد أن دخول المتهم إلى الغرفة كان بقصـد سرقة الورقة، أو أنه أخذ الورقة وخرج من مكان السرـقة، فإنه لا يمكن اعتبار فعله سرقة بالمعنى المنصـــوص عليه في المادة 399 من قانون العقوبات، فالسرـــقة تتم بنقل حيازة المال من يد الحائز بدون رضاه إلى يد السارق".

(تمييز جزاء رقم 76/50، مجلة نقابة المحامين الأردنيين، 1976، ص1627)

لما تقدم نجد أ نه وفقاً لمفهوم فعل الأخذ في قانون العقوبات والذي يتطلب نقل حيازة الشيء محل السرـقة، فإن سرقة المعلومات المختزنة في الحاسـب الآلي أو المتبادلة عبر شـبكة الإنترنت وبشـكل مستقل لا يمكن أن يقع عليها فعل الأخذ بالمفهوم التقليدي للسرقة، لأن ذلك الفعل لا يؤدي إلى إخراج المعلومات من حيـازة مـالكها أو حـائزها القانوني. أو حرمانه منها وإدخالها في حيازة الجاني لوحده، فالركن المادي المتمثل بفعل الأخذ ونقل الحيازة لم يتحقق هنا.

- الركن المعنوي القصد الجرمي:

كما ذكرنا سـابقاً السرـقة جريمة مقصـــودة ويتطلب فيها إلى جانب القصـــد العام أن يتخذ ركنها المعنوي صورة القصد الخاص المتمثل في انصراف نية الجاني إلى تملك ذلك الشيء المسروق.

ويتوافر القصـد العام في جريمة السرـقة بتوافر عنصرـ العلم والإرادة، فالعلم بأن يكون الجاني عالماً بأن فعله ينطوي على أخذ مال منقول مملوك للغير دون رضاء مالكه.

أمـا الإرادة فتتجـه إلى فعـل أخـذ هـذا المـال المنقول بـإخراجه من حيازة مالكه وإدخاله في حيازة الجاني، ولا يكتمل الركن المعنوي في جريمة السرـقة إلا إذا توافر إلى جانب القصد العام قصد خاص يتمثل في انصراف نية الفاعل إلى امتلاك الشيء المسروق.

ويرى الباحث أنه من خلال ما تقدم وبتدقيق النصوص التقليدية السابقة والواردة في قانون العقوبات الأردني نجد أنه لا يمكن تصور تطبيقها على سرقة المعلومات المعالجة آلياً، وذلك لعدم تطابق أركان وعناصر هذه الجريمة وفقاً لما يتطلبه النص، فالمعلومات الإلكترونية ذات الطبيعة الخاصة بمفهومها الحديث لا يمكن أن تكون محلاً لجريمة السرقة التقليدية، كما وأن فعل الأخذ المكون للركن المادي لا يمكن أن يتحقق في حالة سرقة المعلومات، وعملاً بمبدأ عدم جواز القياس في النصوص الجزائية ومبدأ شرعية الجرائم والعقوبات فإننا لا نستطيع تطبيق نصوص قانون العقوبات الأردني على اعتداءات السرقة التي تقع على المعلومات الإلكترونية حيث أن هذه النصوص لا يمكنها استيعاب هذه المعلومات بالحماية نظراً للطبيعة القانونية المعنوية التي تتمتع بها، ولابد هنا أن نبحث في نصوص القوانين الخاصة الأخرى والصادرة عن المشرع الأردني لمعرفة فيما إذا كانت تتلاءم وطبيعة المعلومات، وهل وفرت الحماية الجنائية لهذه المعلومات ذات الكيان المعنوي أم أنها لم توفرها.

الفرع الثاني: موقف المشرع الأردني وفقاً لقانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010 :

أصدرت الحكومة الأردنية قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010 في محاولة منها للسيطرة على الجرائم المستحدثة في ظل التطورات التقنية لنظم المعلومات، فبعد أن أيقن المشرع الأردني شأنه شأن بقية المشرعين الوطنيين أن النصوص التقليدية قاصرة عن معالجة الجرائم المعلوماتية المستحدثة، والتي تختلف في طبيعتها عن تلك الجرائم التقليدية التي كانت النصوص السابقة تحيطها بالحماية بكافة صورها وأساليبها، وتحيط كافة المصالح والقيم المادية الملموسة بالحماية الجزائية، فجاءت تكنولوجيا المعلومات والتقنيات الحديثة وأصبحت تتعامل بلغة الأرقام عبر الحاسوب والإنترنت، والتي تحتوي كماً هائلاً من المعلومات الإلكترونية المعالجة آلياً سواء المختزنة في الحاسب الآلي أو المتبادلة عبر الشبكة العالمية للمعلومات (الإنترنت)، هذه المعلومات ذات الطبيعة الخاصة والكيان المعنوي غير الملموس، والتي لها قيم اقتصادية تقدر أحياناً بثروات طائلة، أصبحت تستوجب على المشرع الوطني إحاطتها بالحماية الجزائية المناسبة، لسد الطريق في وجه كل من تسول له نفسه بالاعتداء عليها وبكافة الصور.

وقد أورد المشرـع الأردني كما أشرنا في المادة الثانية من هذا القانون والخاصـة بالتعريفات تعريفاً للمعلومات فعرفها بأنها "البيانات التي تمت معالجتها وأصبحت لها دلالة".

وقد جاء في المادة (6/أ) من ذات القانون ما يلي:

"أ- كل من حصـل قصـداً دون تصرـيح عن طريق الشـبكة المعلوماتية أو أي نظام معلوماتي على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تسـتخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنتين، أو بغرامة لا تقل عن (500) خمسمائة دينار، ولا تزيد على (2000) ألفي دينار، أو بكلتا هاتين العقوبتين".

ومن خلال نص المـادة 6 /أ فـإننا نجد أن المشرـع الأردني قد اسـتحدث جريمة جديدة وفقاً لهذا القانون وهي جريمة الحصـول على المعلومات والبيانات الخاصـة ببطاقات الائتمان أو المعلومات المالية أو المصرـفية الإلكترونية دون تصرـيح ومن خلال فهم النص فإن هذه الجريمة تقوم على ثلاثة أركان هي كما يلي:

أولاً: الركن المادي:

يتحقق الركن المـادي في هـذه الجريمـة وفقـاً للمشرـع الأردني بفعـل الحصـول على البيانات أو المعلومات المتعلقة ببطاقات الائتمان، أو التي تسـتخدم في تنفيذ المعاملات المالية، أو المصرـفية الإلكترونية، وذلك دون تصريح.

وبحسـب نص المادة 6/أ من ذات القانون فإن فعل الحصـول على المعلومات والبيانات يقوم على عنصرـين أحدهما مادي والآخر معنوي، ويتمثل العنصرـ المادي في النشـاط التقني المحدد وهو اسـتخدام الحاسـوب والإنترنت والصـادر عن الجاني بحصـوله على هذه المعلومات، أما العنصرـ المعنوي فهو أن يكون الحصـول على هذه المعلومات دون تصرـيح من مالكها أو صاحب العلاقة، حيث عرفت المادة (2) من ذات القانون التصريح بأنه "الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول أو استخدام نظام المعلومات أو موقع إلكتروني أو الشبكة المعلوماتية، بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغيير أو إعادة نشرـ بيانات أو معلومات أو حجب الوصـول إليها، أو إيقاف عمل الأجهزة أو تغيير موقع إلكتروني أو إلغائه أو تعديل محتوياته"،

وعليه فإنه يشـترط لقيام الركن المادي في هذه الجريمة أن يتوافر أمران، أولهما قيام الجاني بنشـاط إجرامي تقني يتمثـل في الحصـــول على البيانات والمعلومات المحددة بنص المادة 6/أ، وثانيهما أن يتم فعل الحصـول بدون تصـريح من صـاحب العلاقة، وبصـرف النظر عن نقل الحيازة كما هو الحال في المال محل جريمة السرقة التقليدية، فالركن المادي يتحقق بمجرد الحصول على هذه المعلومات دون تصريح من مالكها، دون اشتراط نقل الحيازة من المجني عليه إلى حيازة الجاني. (إنهاء حيازة المجني عليه).

وقد اشـترط المشـرع أيضـاً أن يتم ارتكاب هذا السلوك المادي عن طريق الشبكة المعلوماتية أو أي نظام معلومات، ومؤدى ذلك أن جرائم الحاسـوب والإنترنت ليسـا من جرائم الوسـيلة، فهما ليسـا وسـيلة لارتكـاب الجريمـة المعلومـاتية وإنما يدخلان في النشـــاط المادي المكون لها، وقد عرفت المادة (2) من ذات القاذ ون النظام المعلوماتي بأنه "مجموعة البرامج والأدوات المعدة لإنشـاء البيانات أو المعلومات إلكترونياً، أو إرسـالها أو تسـلمها أو معالجتها أو تخزينها أو إدارتها"، وعرفت أيضاً الشبكة المعلوماتية في ذات المادة بأنها "ارتباط بين أكثر من نظام معلومات للحصـول على البيانات والمعلومات وتبادلها". ويبدو أن المشـرع الأردني قد قصد بذلك الحاسب الآلي والشبكة العالمية للمعلومات (الإنترنت).

ثانياً: محل الجريمة:

وفقاً لنص المادة 6/أ من ذات القانون فإن محل هذه الجريمة هي البيانات والمعلومات التي تتعلق ببطاقات الائتمان، أو التي تستخدم في تنفيذ المعاملات المالية، أو المصرفية الإلكترونية.

ثالثاً: الركن المعنوي:

ويتخذ الركن المعنوي في هذه الجريمة صـورة القصـد، حيث تطلب المشـرع فيها القصـد العام القائم على عنصريه العلم والإرادة، والدليل على ذلك أنه استعمل تعبير قصداً ولذلك فهي لا تقوم بالخطأ، حيث ينصرف علم الجاني وإرادته إلى كافة ماديات وعناصر الجريمة.

ولابد من التنويه هنا أن المادة (7) من ذات القانون ضاعفت العقوبة على الجرائم المنصوص عليها في الحالات التي يتم ارتكابها من قبل الشـــخص أثناء تأديته وظيفته أو عمله أو باســـتغلال أي منهما، ولم يحدد المشـرع فيملالالالا ا إذا كان هذا الشخص موظفاً عاماً ينطبق عليه نظام الخدمة المدنية الأردنية، أو عـاملاً في القطـاع الخـاص والـذي يطبق عليـه قـانون العمـل والعمال، حيـث جـاء في نص المادة (7) ما يلي "تضـاعف العقوبة على الجرائم المنصـوص عليها في المواد من (3) إلى (6) من هذا القانون بحق كل من قام بارتكاب أي منها أثناء تأديته وظيفته، أو عمله، أو باستغلال أي منهما".

لما تقدم يرى الباحث أن المشرع الأردني قد أدرك القصور الحاصل في النصوص الجزائية التقليدية لعدم احتوائها على الطبيعة الخاصة للمعلومات الإلكترونية سواء المخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت، والتي كانت سابقاً تترك المجال مفتوحاً للمجرمين بالاعتداء على هذه المعلومات التي تمثل قيماً اقتصادية قد تقدر أحياناً بثروات هائلة والخاصة بالأفراد أو الشركات أو المؤسسات الاقتصادية الاستثمارية وغيرها دون أن ينالوا العقاب على أفعالهم لغياب النص الجزائي، وقد أحاطها المشرع بالحماية الجزائية اللازمة من الاعتداء أو النسخ أو الاعتراض أو الإعاقة وغيرها، فاعتبر مجرد الحصول على هذه المعلومات والبيانات دون تصريح من صاحب العلاقة جريمة معاقب عليها بصرف النظر سواء استخدمها الفاعل أم لم يستخدمها، وسواء حصل على منفعة مالية لنفسه أو لغيره أم لم يحصل.

ويبدو أن المشرع الأردني حاول توفير أقصى درجات الحماية الجنائية للمال المعلوماتي من الاعتداء عليه، ومن باب التحوط عاقب على مجرد الحصول على هذه المعلومات عن طريق الشبكة المعلوماتية، أو أي نظام معلوماتي، حيث ترك المطلق على إطلاقه ولم يحدد في النص كيفية الحصول على هذه المعلومات المالية هل هو بالسرقة أو بالنسخ أو الإعاقة أو اعتراض المعلومات أو بالطرق الأخرى، فاعتبر وقوع الضرر لصاحب العلاقة بمجرد حصول الفاعل على المعلومات بصرف النظر إذا كان قد استخدمها أم لم يستخدمها، أو أنه حصل على منفعة مالية لنفسه أو لغيره أم لم يحصل عليها.

وهذا يحسب بحق للمشرع الأردني بأن أحاط المال المعلوماتي ببعض صور الحماية الجنائية التي لم تكن توفرها النصوص التقليدية، فمبدأ شرعية الجرائم والعقوبات لم يُتيح للقضاء الأردني احتواء الاعتداءات التي كانت تقع على المعلومات المالية، وبالتالي استبعاد تطبيق نصوص قانون العقوبات الخاصة بالسرقة عليها، كما وأن المشرع الأردني في المادة (7) ضاعف العقوبات الواردة في المادة (6) في حال ارتكاب الجريمة من قبل الشخص أثناء تأديته وظيفته أو عمله أو من خلال استغلال وظيفته التي تخوله أحياناً بالدخول إلى نظام المعلومات، وحسناً فعل المشرع الأردني لأنه ومن خلال الواقع العملي لمثل هذه الجرائم أنها وفي كثير من الأحيان ترتكب من قبل أشخاص مخولين بدخول النظام المعلوماتي، إلا أنهم يتجاوزوا صلاحياتهم ويقومون بالاطلاع على معلومات أخرى لا يجوز لهم الاطلاع عليها، ويقومون بارتكاب جرائم معلوماتية قد تؤدي إلى خسائر مادية فادحة بالمجني عليهم.

ومع ذلك فإن الباحث يرى أن مبدأ شرعية الجريمة والعقوبة يوجب على المشرع الأردني النص الصريح على جريمة السرقة المعلوماتية إذا أراد حماية المعلومات المعالجة آلياً من أفعال السرقة التي قد تقع عليها، فمن خلال التدقيق في النصوص الواردة في قانون جرائم أنظمة المعلومات الأردني المؤقت لم نجد أي منها ينص صراحة على جريمة سرقة المعلو مات المعالجة آلياً كما هو الحال في النصوص التقليدية الخاصة بهذه الجريمة والواردة في قانون العقوبات، حتى لو أن المشرع عاقب على مجرد الحصول على المعلومات والبيانات المعالجة آلياً دون تصريح من صاحب العلاقة، إلا أنه لم يحيط هذه المعلومات بالحماية الجنائية الصريحة والقاطعة من كل شك من خطر الاعتداء عليها بالسرقة، فكنا نتمنى على المشرع الأردني احتواء الطبيعة الخاصة للمعلومات المعالجة آلياً وإدخال التعديلات اللازمة في قانون العقوبات التقليدي لاستيعاب هذه الطبيعة، بما يتناسب وإحاطتها بالحماية الجنائية اللازمة، فالمشرع مطالب بالتدخل لإيجاد الصيغة الشرعية بتقنين جرائم السرقة عبر النظام المعلوماتي لمواءمة تقنية المعلومات مع فكرة الاستيلاء على الحيازة فيها، وذلك بما يحقق نوعاً من التوافق بينهما.

المطلب الرابع: موقف المشرع الأمريكي من جريمة سرقة المعلومات عبر الحاسوب والإنترنت:

عند دراسة موقف المشرع الأمريكي حول موضوع سرقة المعلومات الإلكترونية، فلابد من استعراض موقف التشريع الفيدرالي، ومن ثم موقف التشريع في الولايات المختلفة وذلك كما يلي:

الفرع الأول: إتجاه التشريع الأمريكي الفيدرالي:

جاء المشرع الفيدرالي بقانون سرقة الممتلكات القومية لسنة 1994، وقد تضمن ثلاثة تعديلات على قانون 1984 بخصوص المادة A/5 من الفصل 1030، بحيث يشمل التعديل الحاسب الآلي في التجارة ما بين الولايات، ولم يعد أيضاً بمقتضى هذا التعديل الاتصال غير المصرح به متطلباً في كل جريمة، حيث نص البند (2314) من قانون سرقة الممتلكات القومية الأمريكي لعام 1994 تحت عنوان 18 U.S.C.$ 2314 على "تجريم نقل أية بضائع أو سلع أو مستندات أو نقود تصل قيمتها إلى خمسة آلاف دولار أمريكي أو أكثر، من خلال التجارة بين الولايات، مع معرفة المشتري لحقيقة المصدر غير المشروع، ويطبق هذا القانون على جرائم الكمبيوتر المتعددة،

بما في ذلك نقل الودائع المصرفية عن طريق الاحتيال بالحاسب الآلي "، إلا أن المحاكم في ذلك الحين لم تعتبر المعلومات بضـائع أو سـلعاً وفقاً لهذا القانون، وبالتالي لم تعتبرها محلاً لجريمة السرـقة، ورفضـت تطبيق نصوص هذا القانون على الاعتداءات التي تطال المعلومات الإلكترونية "[2]

وقد حاول المشرـع الأمريكي بموجب هذه التعديلات أن يوسـع من نطاق المسـؤولية الجنائية في الأفعال التي ترتكب من شـخص له حق الاطلاع في شركة أو مسـتخدم مصرـح له بذلك، والذين لم يكن التجريم يشملهم بموجب قانون سنة 1986 (شمس الدين، 2006، 139).

وبعد ذلك جاء تشريع عام 1996 والذي صدر بمقتضى قانون البنية القومية للمعلومات، وقد شكل الكونجرس الأمريكي لجاناً متخصصة لإعداد دراسات وإحصاءات، وذلك لمواجهة تنامي الجريمة عبر الإنترنت (إبراهيم، 2009، 266).

---

[2] Article 18u.s.c.$ 2314 of NSPA of 1994

Sec. 2314. Transportation of stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting

Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud; or

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transports or causes to be transported, or induces any person or persons to travel in, or to be transported in interstate or foreign commerce in the execution or concealment of a scheme or artifice to defraud that person or those persons of money or property having a value of $5,000 or more; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce any falsely made, forged, altered, or counterfeited securities or tax stamps, knowing the same to have been falsely made, forged, altered, or counterfeited; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce any traveler's check bearing a forged countersignature; or

Whoever, with unlawful or fraudulent intent, transports in interstate or foreign commerce, any tool, implement, or thing used or fitted to be used in falsely making, forging, altering, or counterfeiting any security or tax stamps, or any part thereof—

Shall be fined under this title or imprisoned not more than ten years, or both.

This section shall not apply to any falsely made, forged, altered, counterfeited or spurious representation of an obligation or other security of the United States, or of an obligation, bond, certificate, security, treasury note, bill, promise to pay or bank note issued by any foreign government. This section also shall not apply to any falsely made, forged, altered, counterfeited, or spurious representation of any bank note or bill issued by a bank or corporation of any foreign country which is intended by the laws or usage of such country to circulate as money.

وقد نص البند رقم (461) من الجزء الأول من الفصل الثالث من ذات القانون، والمتعلق بالمال العام على ما يلي:

"أي شخص يقوم بسرقة أو اختلاس أو استغلال الغير وبشكل مقصود وبدون وجه حق، أو التصريح للغير لأن يقوم بالبيع أو التصرف في أي مستند أو مال أو تسجيل أو أي شيء ذي قيمة للولايات المتحدة الأمريكية أو أية هيئة أو وكالة، وكذلك أي شخص يتلقى أو يخفي أو يحتفظ لنفسه بأي شيء مستقل وهو يعلم ذلك، يعاقب بغرامة لا تزيد على عشرة آلاف دولار أو بالسجن لمدة لا تزيد على عشر سنوات أو كلتا العقوبتين، وإذا كانت قيمة هذه الممتلكات لا تزيد على مائة دولار أمريكي فيغرم الفاعل بما لا يزيد على ألف دولار أمريكي، أو يسجن مدة لا تزيد على سنة، أو كلتا العقوبتين" (Icove and Vonstorch, 1995, p. 209).

نجد من خلال هذا النص أن المشرع الفيدرالي الأمريكي قد شمل المعلومات ذات القيم المالية بالحماية الجنائية حيث عاقب على سرقة أي شيء له قيمة يخص الولايات المتحدة الأمريكية، بما في ذلك إداراتها ووكالاتها وكل من تربطه علاقة تعاقدية مع هذه الوكالات.

وتندرج سرقة المعلومات تما شياً مع ما ذهب إليه القضاء الأمريكي الفيدرالي في كثير من أحكامه تحت سرقة الأشياء ذات القيمة (قوره، 2005، 149)، ومن الأمثلة على هذه الأحكام الحكم الصادر في قضية "USV. Girard"، حيث حاول المتهم الإعداد لجلب مواد مخدرة من المكسيك تمهيداً لإدخالها إلى الولايات المتحدة الأمريكية، وحتى يضمن نجاح هذه العملية اتفق مع أحد الموظفين العاملين في إدارة مكافحة المخدرات، لتزويده بمعلومات هامة وسرية والمخزنة في الحاسب الآلي الخاص بالإدارة، وبالفعل استطاع الموظف الحصول على هذه المعلومات عن طريق جهاز الحاسب الآلي الموجود في مكتبه، وقد قدّم المتهمون إلى المحاكمة بتهمة سرقة أشياء ذات قيمة على أساس أن المعلومات التي تم الحصول عليها بواسطة النهاية الطرفية هي من الأشياء ذات القيمة، وقد ذكر الحكم أن المعلومات التي تم الحصول عليها والمخزنة في ذاكرة الحاسب الآلي أو الأقراص الممغنطة يمكن أن تكون محلاً لجريمة السرقة، شأنها في ذلك شأن الوسيط المادي الذي تم تسجيل المعلومات عليه[3] (قوره، 2005، 149).

---

[3] هناك أحكام قضائية كثيرة صادرة عن محاكم الولايات المتحدة الأمريكية كانت قد توسعت في تعريف المال بحيث يشمل كل شيء ذا قيمة، وهذا الأمر دفع العديد من الولايات إلى التوسع في تعريف الأموال التي يمكن أن تكون محلاً لجريمة السرقة، بحيث تشمل النبضات الإلكترونية، والمعلومات والبيانات المعالجة آلياً، وبرامج

وبذلك أسبغ المشرع الفيدرالي الأمريكي الحماية الجنائية على المعلومات المعالجة آلياً من خلال النص على عبارة كل شيء ذي قيمة للولايات المتحدة، بحيث أصبحت المعلومات وفقاً لهذا النص محلاً لجريمة السرقة.

وقد جاء قانون حق النشر والتأليف الأمريكي والمعدل في ديسمبر عام 2011 في الماده 1101 الفقره A في الفصل (11) والخاص بحماية حق النشر والتأليف، ونص على جرائم النسخ والتسجيلات للأعمال التي تشملها حقوق النشر والتأليف والتي من ضمنها برامج الحاسوب، وذلك مقابل الحصول على منفعه ماديه للفاعل، من خلال الإتجار غير المصرح به ودون الحصول على موافقة صاحب الشأن ، حيث إن مرتكب هذه الأفعال يخضع للأحكام الواردة في المواد 502 – 505 من الفصل الخامس من ذات القانون نتيجة إنتهاكه لحق المؤلف[4].

ونصت الفقره الأولى من البند A من الفصل الخامس من ذات القانون،على أنه إذا كان الهدف من الإستنساخ أو التوزيع أو التعدي لأغراض تجاريه أو لتحقيق مكاسب ماليه للفاعل بما في ذلك الإستنساخ باستخدام الوسائل الألكترونيه، فإن الفاعل يخضع للعقوبات الوارده في الماده 2319 من الباب 18 [5]

الحاسب الآلي، والخدمات التي يقدمها الحاسب الآلي، وكل شيء له قيمة يتصل بنظم أو شبكات الحاسب الآلي. مشار إليه لدى (قورة، 2005، 146 وما بعدها).

[4] Article 1101/A chapter (11) of US Copyright l
aw,December,2011
§ 1101 · Unauthorized fixation and trafficking in sound recordings
and music videos
(a) Unauthorized Acts.—Anyone who, without the consent of the performer
or performers involved—
(1) fixes the sounds or sounds and images of a live musical performance
in a copy or phonorecord, or reproduces copies or phonorecords of such aperformance
from an unauthorized fixation,
(2) transmits or otherwise communicates to the public the sounds or sounds and images
of a live musical performance, or
(3) distributes or offers to distribute, sells or offers to sell, rents or offers to rent, or
traffics in any copy or phonorecord fixed as described in paragraph (1),
regardless of whether the fixations occurred in the United States,
shall be subject to the remedies provided in sections 502 through 505, to the same
extent as an infringer of copyright.

[5] Article 506/A/1 chapter 5 of US Copyright of 2011
§ 506 · Criminal offenses6
(a) Criminal Infringement.—
(1) In general.—Any person who willfully infringes a copyright shall be
punished as provided under section 2319 of title 18, if the infringement was
committed—

وقد تصل العقوبه إلى السجن لمدة ثلاث سنوات للأشخاص الذين يرتكبون الجريمه لأول مره وست سنوات للمكررين. (رستم، 1992، 239 وما بعدها) (www.copyright.gov/title 17/92 apph.pdf)

وفي التعديلات الأخيرة في القانون الأمريكي الفيدرالي حول سرقة المعلومات والبيانات للحاسب الآلي، فقد عالج المشرع الأمريكي أفعال الاستيلاء على بيانات الحاسوب من خلال المادة (2) (a) (1030) من القانون الامريكي الفيدرالي لعام 1994 وقد جاء نصها كما يلي:

"كل من وصل إلى جهاز حاسوب دون تفويض أو تجاوز التفويض المسموح به وحصل نتيجة لذلك على:

1- معلومات يتضمنها سجل مالي لمؤسسة ماليه ،أو من مصدر البطاقة على النحو المحدد في المادة 1602/A/1 من العنوان15،أو وارده في ملف المستهلك.

2- معلومات من أية إدارة أو وكالة في الولايات المتحدة.

3- معلومات من أي حاسوب مشمول بالحماية [6].

وقد أشارت الفقرة (c) من ذات المادة والخاصة بالعقوبات إلى العقوبات التي يمكن إيقاعها على من يرتكب الأفعال السابقة. (الهرش،105،2005)

كما وتنص المادة 1030/A/4 من القانون المذكور على تجريم أفعال الوصول المتعمد بنية الاحتيال وبدون تفويض إلى جهاز حاسوب محمي أو تجاوز الوصول المسموح به إذا أدى ذلك إلى الحصول على أي شيء له قيمة ما لم يكن هذا الشيء هو مجرد استعمال للحاسوب لا تزيد قيمته على (5000) دولار خلال فترة سنة[7].

---

[6] Article 1030/A/2 of CFAA
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer

[7] Article 1030/A/4 of CFAA : (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period

الفرع الثاني: اتجاه تشريع الولايات:

اختلفت تشريعات وقوانين الولايات حول اعتبار المعلومات محلاً لجريمة السرقة، وقد حاولت بعض هذه الولايات الإتيان بقوانين خاصة في محاولة منها لتوفير الحماية الجنائية للمعلومات المالية، وقد اعتبرت بعض الولايات المعلومات الخاصة بالتجارة من ضمن الأموال التي تقع عليها جريمة السرقة، وبعضها الآخر اعتبر المعلومات المختزنة في الحاسب الآلي يمكن أن تكون محلاً للاعتداء والسرقة، وبعضها الآخر توسع في تعريف المال بحيث يشمل كل شيء ذي قيمة للولايات المتحدة أو إداراتها أو وكالاتها المختلفة، بحيث يشمل النبضات الإلكترونية، والمعلومات والبيانات المعالجة آلياً، وبرامج الحاسب الآلي، والخدمات التي يقدمها الحاسب الآلي. وكل شيء له قيمة يتصل بنظم أو شبكات الحاسب الآلي. (قوره، 2005، 146 وما بعدها) ونذكر منها ما يلي:

أولاً: ولاية كاليفورنيا:

اعتبرت ولاية كاليفورنيا أن المعلومات التجارية يمكن أن تكون محلاً للسرقة حيث نصت في الفصل (51) والمتعلق بسرقة الأسرار التجارية بالبند (25) فقرة (6) على أنه "أي شخص يقوم وبشكل متعمد وتتجه نيته إلى سلب المالك الأسرار التجارية الخاصة به، أو تتجه نيته إلى الاستيلاء على هذه الأسرار أو التصميمات أو إجراءات فنية أو برامج الحاسوب أو معلومات مخزنة في الحاسوب، أو أية ابتكارات أو تعديلات سرية، فإنه يعتبر مذنباً ومُتهماً بجريمة السرقة في حال قيامه باستخدام الأجهزة بدون تصريح، أو نقل تلك الأسرار أو الاستيلاء على أي بند أو بيانات تعد أسراراً تجارية كان يؤتمن عليها". (Wiley,J, 1986, p. 55)

ثانياً: ولاية رودأيلاند:

تنص تشريعات هذه الولاية في قانونها جرائم الحاسب الآلي في الفصل (52) البند (11) فقرة (4) على أنه "أي شخص يقوم بشكل مقصود دون وجه حق بنية سلب المالك لما يملكه أو يأخذه لتحويله أو إلغائه، وكان محل تلك الأشياء حاسباً آلياً أو نظام المعلومات أو شبكة معلومات أو معلومات أو برامج يشتمل عليها الجهاز، أو نظام المعلومات أو شبكة المعلومات، بحيث تتعدى قيمته خمسمائة دولار، فإن الفاعل يعاقب بالحبس لمدة عام واحد، أو غرامة لا تزيد على ألف دولار، أو كلتا العقوبتين" (سليمان، لات، 59).

وتجدر الإشارة هنا أن بعض تشريعات الولايات المتحدة اعتبرت المعلومات المعالجة إلكترونياً جزءاً من الذمة المالية للشخص، فلا تمييز بين الاعتداءات التي تقع على المال المادي أو المال المعنوي، حيث أصدرت معظم الولايات الأمريكية قوانين عرفت المال بأنه "كل شيء ذي قيمة مالية" وهذا التعريف وسع من مفهوم المال ليشمل الأموال المادية الملموسة والأموال المعلوماتية ذات الطبيعة المعنوية، ومن هذه القوانين قانون ولاية فرجينيا، الذي يعتبر جُهد الآلة والخدمات التي يقدمها النظام المعلوماتي أموالاً، وبالتالي تصلح لأن تكون محلاً لجريمة السرقة التقليدية (الملط، 2006، 343).

لما تقدم يرى الباحث أن المشرع الفيدرالي الأمريكي قد أحاط المعلومات المعالجة آلياً ببعض الحماية الجنائية دون النص عليها صراحة، وهذا الأمر مختلف عن تشريع الولايات الأمريكية التي نصت صراحة على جريمة السرقة المعلوماتية، والتي محلها الحاسب الآلي أو نظام المعلومات أو المعلومات أو البرامج التي يشتمل عليها المعلومات وحتى المعلومات المتداولة عبر الشبكة، فكانت الحماية الجنائية التي وفرها مشرعو الولايات أعلى درجة ووضوحاً من تلك التي وفرها المشرع الفيدرالي، ومع ذلك فإننا لا نستطيع أن ننكر توجه المشرع الأمريكي وبوجه عام لتوفير الحماية اللازمة لهذه المعلومات ذات الطبيعة الخاصة، والتي تختلف عن المال محل جريمة السرقة التقليدية، حيث أعطى المعلومات الإلكترونية الخاصة بالمعاملات التجارية أهمية خاصة، حتى أن بعض المحاكم تطبق النصوص الجزائية التقليدية على جريمة سرقة المعلومات ذات القيم الاقتصادية والمخزنة في الحاسب الآلي أو المتداولة عبر الشبكة، وذلك من خلال توسع المشرع الأمريكي في تعريف المال بأنه "كل شيء ذي قيمة"، بأن أصبح لفظ المال يعني الأموال المادية والأموال المعنوية الكتابية.

المبحث الثاني: جريمة إتلاف المعلومات المعالجة آلياً:

يعتبر حق الملكية من الحقوق الهامة التي عالجتها التشريعات المدنية والجزائية، حيث جاءت نصوص قانون العقوبات العام وجرمت كافة أشكال الاعتداء على حق الملكية، وقد امتدت تلك الحماية المتعلقة بالأشياء ليس فقط من حيث الملكية والاستئثار، بل لضمان سلامة الشيء محل حق الملكية من أية أضرار قد تقع عليه وبذلك التأثير في هذا الحق إما بإتلافه كلياً أو جزئياً، وهذا ما يسمى بجريمة الإتلاف لذلك يمكن تقسيم هذا المبحث إلى المطالب التالية :

1-مفهوم جريمة الإتلاف.

2-الوسائل التقنية المستخدمة لإتلاف المعلومات المعالجة آلياً.

3-الحماية الجنائية للمعلومات المعالجة آلياً من الإتلاف وفقاً للمشرع الأردني.

4- الحماية الجنائية للمعلومات المعالجة آلياً من الإتلاف وفقاً للمشرع الأمريكي.

المطلب الأول: مفهوم جريمة الإتلاف:

وسوف نتناول ذلك من خلال دراسة مفهوم جريمة الإتلاف التقليدية في التشريع المقارن وأركانها ومن ثم نتناول الإتلاف في مجال المعلوماتية وذلك كما يلي:

الفرع الأول: مفهوم جريمة الإتلاف التقليدية وأركانها:

نصت معظم التشريعات التقليدية المقارنة على جريمة الإتلاف، وذلك في قوانين العقوبات التقليدية، ويتمثل الإتلاف في تخريب الشيء موضوع الجريمة وذلك بإتلافه، أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله.

والإتلاف لا يخرج عن كونه "التأثير على مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية، عن طريق الإنقاص من كفاءته للاستعمال المعد له"، والإتلاف قد يرد على كل المال، أو على جزء منه، ولكن يشترط إذا وقع الإتلاف على جزء من المال أن يجعله غير صالح للاستعمال، كما أنه لا يشترط أن يتم بوسيلة معينة، شريطة ألا تكون هذه الوسيلة مما يخضع إلى نص عقابي آخر (قشقوش، 1993، 564).

والإتلاف قد يؤدي إلى إفناء مادة الشيء تماماً أو هلاكه كلياً، ويقصد بالتخريب توقف الشيء تماماً عن أن يؤدي منفعته حتى ولم تفن مادته، ويكون الشيء غير صالح للاستعمال بجعله لا يقوم بوظيفته المرصود لها على النحو الأكمل، أما التعطيل فيكون بتوقف الشيء عن القيام بوظيفته فترة مؤقتة، وتتحقق جريمة الإتلاف بتحقق إحدى هذه النتائج السابقة (الشوابكة، 2009، 219 وما بعدها).

وجريمة الإتلاف شـأنها شأن أية جريمة أخرى يتطلب لتحققها توافر أركانها المتمثلة في الركن المادي والركن المعنوي ومحل الجريمة، ويتمثل الركن المادي في نشـــاط إجرامي يتخذ عدة صـــور أولها التخريب، ويعني التخريب هنا أن المال أصبح غير قابل للإصلاح أي فقد صلاحيته للاستعمال، والصورة الأخرى هي الإتلاف، ويعني التأثير في المال ولكنه قابل للإصـلاح أي أنقصـت من صـلاحيته للاسـتعمال، وكذلك تعطيل الشيء أي إعاقته عن العمل كلياً أو جزئياً (الشاذلي، فتوح وعفيفي، عفيفي كامل، 2003، 203 وما بعدها).

وجريمة الإتلاف وفقاً لما هو منصوص عليه في معظم التشريعات تعتبر من الجرائم المقصودة، الأمر الذي يتطلب لتحققها أن يتوافر لدى الجاني إضـــافة إلى الركن المادي ركن معنوي يتمثل في القصـــد الجنائي من وراء ارتكاب الجاني لهذه الجريمة.

ويتمثل القصـــد الجنائي في هذه الجريمة بالعلم والإرادة، وذلك بأن يكون الجاني عالماً بكافة عناصر وماديات الجريمة التي ارتكبها، بحيث يعلم أن من شأن سلوكه إتلاف مال الغير على نحو تذهب معه قيمته كلياً أو جزئياً، مع علمه بملكية هذا المال المتلف للغير، وأن تتجه إرادته إلى ارتكاب هذا الســـلوك الإجرامي وإلى تحقيق النتيجة أيضاً.

أما فيما يتعلق بمحل جريمة الإتلاف نجد أن معظم التشـــريعات العربية اســـتلزمت لتحقق هذه الجريمة أن يقع الاعتداء على مال منقول أو غير منقول، حيث نجد المشـــرع الأردني تناول جريمة الإتلاف في الفصـل السـادس من الباب الحادي عشـر من قانون العقوبات الأردني رقم (16) لسـنة 1960 وتعديلاته. في المادة (445) وذلك تحت عنوان الإضرار التي تلحق بأملاك الدولة والأفراد (الهدم والتخريب) ، حيث نصت المادة (445) على أن:

"1- كل من أ لحق باختياره ضرراً بمال غيره المنقول، يعاقب بناءَ على شـكوى المتضرر بالحبس مدة لا تتجاوز سنة أو بغرامة لا تتجاوز خمسين ديناراً أو بكلتا العقوبتين.

2- تنازل الشاكي يسقط دعوى الحق العام".

كما نص المشرع المصري في المادة (361) عقوبات مصري على ما يلي:

" كل من خرب أو أتلف عمداً أموالاً ثابتة أو منقولة لا يمتلكها أو جعلها غير صـــالحة للاســـتعمال أو عطلها بأية طريقة، يعاقب بالحبس مدة لا تزيد على سـتة أشـهر وبغرامة لا تتجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين، فـإذا ترتـب على الفعـل ضرر مالي قيمته خمســـون جنيهاً أو أكثر كانت العقوبة الحبس مدة لا تتجاوز سنتين وغرامة لا تجاوز خمسمائة جنيه أو بإحدى هاتين العقوبتين،

وتكون العقوبة السجن مدة لا تزيد على خمس سنوات وغرامة لا تقل عن مائة جنيه ولا تجاوز ألف جنيه إذا نشأ عن الفعل تعطيل أو توقيف أعمال مصلحة ذات منفعة عامة، أو إذا ترتب عليه جعل حياة الناس أو صحتهم أو أمنهم في خطر" (http://www.Kenanaoline.com).

كما بين المشرع الليبي أحكام جريمة الإتلاف في المادة (1/457) من قانون العقوبات والتي نصت على أنه: "كل من أتلف أو بعثر أو أفسد مالاً منقولاً أو غير منقول أو صيّره غير نافع كلياً أو جزئياً، يعاقب بالحبس مدة لا تتجاوز سنة، أو بغرامة تزيد على مائة جنيه، وتقام الدعوى بناء على شكوى الطرف المتضرر" (عطية، 2001-313).

(http://www.aladel.gov.ly/main/modules/sections/item.php?itemid=68)

ونص المشرع الإماراتي على هذه الجريمة في المادة (424) من قانون العقوبات على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز عشرة آلاف درهم أو بإحدى هاتين العقوبتين، كل من هدم أو أتلف مالاً مملوكاً للغير ثابتاً أو منقولاً جعله غير صالح للاستعمال أو عطله بأية طريقة" (الكعبي، لات، 212). (http://www.gcc-legal.org.com)

أما بالنسبة للتشريعات الأجنبية فنجد أن المشرع الفرنسي نص في الفقرة الأولى والثانية من المادة (322) من قانون العقوبات الفرنسي، على تجريم الإتلاف المقصود للأموال التقليدية شأنه في ذلك شأن معظم التشريعات العربية، حيث أن هذه المادة جرمت أفعال التخريب والإتلاف الواقع على الأموال المنقولة والعقارات (http://www.omanlegal.net).

وأيضاً المادة 291 من قانون العقوبات الدنماركي، والمادة الأولى من الباب الثاني عشر من قانون العقوبات السويدي تحرمان إتلاف الأشياء المادية المملوكة للغير، كما تجرم المادة الأولى من القانون الإنجليزي الصادر عام 1971 الخاص بالإتلاف، أي فعل يعرض الأموال المنقولة المملوكة للغير إلى الإتلاف (قوره، 2005، 191).

ونخلص مما سبق أنه ووفقاً للتشريعات العقابية التقليدية أن جريمة الإتلاف تتحقق بإتيان سلوك مادي من قبل الجاني يتمثل في فعل التخريب أو الإتلاف أو الإفساد الذي يقع على مال منقول أو غير منقول للغير، بحيث يترتب على هذا السلوك أن يصبح المال محل الجريمة غير قابل للإصلاح، أو ينقص من صلاحيته للاستعمال، أو يؤدي إلى تعطيله أو إعاقته عن العمل كلياً أو جزئياً، مع توافر القصد الجنائي العام لدى الفاعل والمتمثل في عنصري العلم والإرادة، وذلك بأن يكون الجاني عالماً بطبيعة السلوك الإجرامي الذي يقوم به والنتيجة المترتبة عليه، وأن تتجه إرادته إلى ذلك الفعل وتلك النتيجة، فجريمة الإتلاف من الجرائم المقصودة لا تقوم بالخطأ.

الفرع الثاني: الإتلاف في مجال المعلوماتية:

إن فعل الإتلاف في مجال المعلوماتية قد ينصب على المكونات المادية للنظام المعلوماتي من ناحية، وذلك بأن يقع على أجهزة الحاسب الآلي ومعداته وملحقاته كالدعامات المادية والبرامج المنسوخ عليها المعلومات والأوراق المستعملة في عمله والشرائط الممغنطة وغيرها من المكونات ذات الطبيعة المادية، ومن ناحية أخرى قد ينصب هذا الفعل على المكونات المعنوية (المنطقية) للنظام المعلوماتي والتي تتمثل في المعلومات نفسها، وذلك يستوجب منا بيان الأحكام القانونية الخاصة في حال وقوع جريمة الإتلاف على هذه المكونات المختلفة بطبيعتها.

أولاً: إتلاف المكونات المادية للنظام المعلوماتي:

كما ذكرنا سابقاً في جريمة السرقة التقليدية ووفقاً للنظم القانونية فقد تأسست قواعد حماية الأموال من مخاطر الجريمة بوجه عام على حماية المال المادي المحسوس أي المال ذي الوجود المادي، وكذلك التعامل مع محل الجريمة الملموس ذي الطبيعة المادية، والتعامل أيضاً مع سلوك جرمي ينتمي إلى عالم السلوكات المادية، وهذا هو الاتجاه التشريعي العام لمختلف قوانين العقوبات الموضوعية، وجرائم الإتلاف شأنها شأن باقي جرائم الأموال تتطلب سلوكاً مادياً موجهاً إلى مال مادي ملموس.

ومما لا شك فيه أن الإتلاف الذي يقع على المكونات المادية للنظام المعلوماتي يخضع للنصوص التقليدية في قانون العقوبات، والتي تتناول بالتجريم فعل الإتلاف الذي يؤدي إلى إلحاق الضرر بالمال المنقول المملوك للغير، كما هو الحال في نص المادة (445) من قانون العقوبات الأردني.

كما وأنه لا صعوبة أيضاً في تطبيق النصوص التقليدية للإتلاف وفقاً لما هو وارد في الكثير من التشريعات، ومنها المادة (361) من قانون العقوبات المصري، والمادة (457) من قانون العقوبات الليبي، والمادة (424) من قانون العقوبات الإماراتي، والمادة (434) من قانون العقوبات الفرنسي، والمادة الأولى من القانون الإنجليزي وغيرها.

فهذه النصوص تعاقب على جرائم الإتلاف العمدي للمال المنقول أو الثابت ذا الطبيعة المادية، والذي يمكن نقله من مكان إلى آخر دون تلف، وليست هناك أدنى مشكلة في خضوع المكونات المادية للنظام المعلوماتي للحماية المقررة في النصوص التقليدية التي تعاقب على الإتلاف (حجازي، 2006، 527 وما بعدها).

والاعتداء على الأموال المعلوماتية المادية بإتلافها يقع على أجهزة الحاسب الآلي ومعداته وملحقاته، كالدعامات والبرامج المنسوخ عليها المعلومات، والأوراق المستعملة في عمله والشرائط المغنطة وغيرها من المكونات المادية (الشوابكة، 2009، 220).

وتجدر الإشارة أن بعض الدول استحدثت نصوصاً خاصة للجرائم المعلوماتية تتعلق بجريمة إتلاف المكونات المادية للنظام المعلوماتي، ومن هذه التشريعات قانون العقوبات الخاص بولاية كاليفورنيا، حيث ذهب هذا القانون إلى تجريم كافة صور إتلاف أنظمة المعالجة الآلية للمعلومات وتخريبها، سواء أكانت تتعلق بالمكونات المادية أم المعنوية (المومني، 2008، 123).

كذلك تضمن التعديل الذي أدخله المشرع الفرنسي في المادة 3/462 من القانون الفرنسي لعام 1988، وذلك في آخر تعديل له عام 1992 والذي أصبح ساري المفعول عام 1994، عقاب كل من قام بإتلاف المال المعلوماتي المادي، مثل أجهزة الحاسب الآلي وملحقاته من آلات مادية (حجازي، 2006، 528).

ثانياً: إتلاف المكونات المعنوية للنظام المعلوماتي (المعلومات):

خلصنا مما سبق إلى أنه لا خلاف حول مدى انطباق النصوص العقابية التقليدية على جريمة الإتلاف في الشق المادي للحاسب الآلي وملحقاته، حيث تنطبق النصوص الجزائية الواردة في قوانين العقوبات التقليدية المقارنة على هذه الجريمة لأن هذه المكونات ذات طبيعة مادية ملموسة، وهي صالحة لأن تكون محلاً لجريمة الإتلاف وغيرها من الجرائم الواقعة على الأموال كالسرقة والاحتيال وإساءة الائتمان، لذلك فهي تتمتع بالحماية الجزائية اللازمة التي وفرتها هذه النصوص التشريعية، شأنها في ذلك شأن الأموال المادية الأخرى التي قد تكون محلاً لمثل هذه الجرائم.

إلا أن المشكلة تثور حول الشق المعنوي أو مكونات الحاسب المعنوية، وبما يخص موضوعنا الذي يتمثل في المعلومات المخزنة في الحاسب الآلي أو المتبادلة عبر شبكة الإنترنت، ومدى انطباق النصوص التقليدية عليها وفقاً لطبيعتها المعنوية غير الملموسة، وفي الحالة التي تكون فيها غير مثبتة على دعامات مادية كالشرائط المغنطة، فمن الناحية القانونية فإن جرائم الإتلاف الواقعة على المكونات المعنوية للنظام المعلوماتي تدخل ضمن الجرائم المعلوماتية ولا يمكن تطبيق النصوص التقليدية عليها كما ذكرنا سابقاً، في جريمة السرقة.

فهذه الجرائم هي أنماط السلوك التي تطال المعلومات المخزنة في الحاسب الآلي أو المعالجة من نظام الحاسب الآلي أو المتبادلة عبر الإنترنت، والتي تمثل أموالاً أو أصولاً أو أسراراً أو بيانات شخصية أو غيرها.

ويقصد بإتلاف برامج الحاسوب ومعلوماته "إتلاف أو محو تعليمات البرامج أو البيانات ذاتها ويطلق عليه أيضاً مصطلح تدمير نظم المعلومات، وعادة لا يستهدف مرتكب هذا الاعتداء فائدة مالية لنفسه، بل لمجرد إعاقة النظام المعلوماتي عن أداء وظائفه وإحداث ضرر فيه" فإتلاف برامج ومعلومات الحاسب الآلي فيه إفقاد لمنفعة هذه البرامج والمعلومات (العبابنة، 2005، 100).

وإتلاف المال المعلوماتي يقع سواء أكان ذلك عن طريق الدخول المتعمد للنظام المعلوماتي من قبل الجاني، أو باستخدامه الطرق التقنية والفنية للإتلاف كالفيروسات مثلاً، وقد يحدث ذلك عن طريق الخطأ أثناء التواجد بالنظام أو الخروج منه (الشوابكة، 2009، 222).

وتجدر الإشارة هنا أن إتلاف المعلومات المخزنة في الحاسب الآلي أو المتداولة عبر الشبكات المحلية أو العالمية من شأنه تخريب هذه المعلومات، وذلك بتدميرها أو تشويهها أو محوها الأمر الذي يؤدي إلى الإضرار بالنظام المعلوماتي وعجزه عن القيام بوظائفه المعتادة، ويتحقق الاعتداء على هذه المعلومات بأن يقوم الجاني بإدخال معلومات أو برامج غير مشروعة وغير صحيحة مستهدفاً التشويش على المعلومات والبيانات الموجودة في النظام المعلوماتي أصلاً، الأمر الذي يؤدي إلى التأثير على صحة وقيمة هذه المعلومات، ومن أكثر الوسائل انتشاراً وخطورة على المكونات المنطقية للنظام المعلوماتي البرامج الخبيثة، والتي يتم إدخالها إلى النظام المعلوماتي بهدف إتلاف المعلومات والإضرار بالنظام (المومني، 2008، 125).

ومن أشهر هذه البرامج الخبيثة هي الفيروسات (Viruses)، وبرامج الدودة، والقنابل المنطقية والزمنية، والتي سوف نستعرضها لاحقاً لبيان مدى تأثيرها في إتلاف المعلومات المخزنة أو المتداولة عبر النظام المعلوماتي.

المطلب الثاني: الوسائل التقنية المستخدمة في إتلاف المعلومات المعالجة آلياً:

إن معظم حالات التسلسل والقرصنة الإلكترونية (Hacking) تحدث بغرض أساسي وهو استخدام الشبكة الأولى كقاعدة للسطو والقرصنة الإلكترونية على النظم المعلوماتية والشبكات الأخرى ذات القيم المادية أو العسكرية أو التكنولوجية، وتحدث حالات قرصنة وتسلل كثيرة بغرض عدائي لتخريب نظم المعلومات وإيقافها عن العمل لفترة زمنية لأسباب شخصية أو مادية (شرف، وعبد الله، 2000، 397).

وتتعدد وسائل إتلاف المعلومات أو المكونات المنطقية لأنظمة المعالجة الآلية للمعلومات، وسوف نستعرض في هذا المطلب أهم هذه الوسائل وأكثرها استخداماً وذلك على النحو الآتي:

الفرع الأول: الفيروسات (Viruses):

أولاً: مفهوم الفيروسات:

الفيروسات هي (برامج مشفرة مصممة بقدره على التكاثر والانتشار من نظام إلى آخر، إما بواسطة قرص ممغنط أو عبر شبكة للاتصالات، بحيث يمكنه أن ينتقل عبر الحدود من أي مكان إلى مكان آخر في العالم، وهو يسمى عادة باسم أول مكان اكتشف فيه، والبرامج الفيروسية لها قدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافها، كما أنها قد تكون مصممة لتدمير برامج أخرى أو تغيير معلومات، ثم تقوم بتدمير نفسها ذاتياً دون أن تترك أثراً يدل عليها، وعلى الرغم من تدميرها للبرامج والمعلومات، إلا أنها لا تسبب عادة تدميراً لأي من المكونات المادية للنظام (قوره، 2005، 192).

لذلك فقد يقع فعل الإتلاف على المعلومات أو البيانات المخزنة بذاكرة الحاسب الآلي عن طريق إدخال الفيروسات، حيث يدخل الفيروس نسخاً من نفسه إلى البرامج أو المعلومات التي أدخل عليها، وهذه البرامج أو المعلومات المصابة بالعدوى تتكاثر بدورها، الأمر الذي يؤدي إلى شغل ذاكرة الجهاز أو الأسطوانة كاملة في لحظة من اللحظات، ويكون من المتعذر التعامل مع هذه البيانات والمعلومات، فالفيروس برنامج صغير يتم تسجيله أو زرعه على الأقراص أو الاسطوانات الخاصة بالحاسوب، ويمكنه في زمن محدد أن يكرر المعلومات أو البيانات المخزنة في الجهاز، الأمر الذي يؤدي إلى تلف الجهاز أو تعديل البرامج أو المعلومات (عطية، 2001، 318 وما بعدها).

وتجدر الإشارة هنا أن للفيروسات غرضاً حمائياً إضافة إلى الغرض التخريبي ويتمثل الغرض الحمائي في حماية البيانات والبرامج من خطر النسخ غير المشروع، حيث ينشط الفيروس بمجرد النسخ (لطفي، 1993، 496).

وأول من ابتكر فيروس الحاسوب هو (جون نيومان) عام 1949، وذلك من خلال مقال له يحمل عنوان "نظرية التعقيد الأوتوماتيكي"، حيث بين فيه الفكرة الأساسية في تصميم الفيروسات والأضرار المترتبة على هذه الفيروسات، والتي قد تصل إلى تدمير الحاسب الآلي تلقائياً (المومني، 2008، 126).

ويقوم مبدأ عمل الفيروسات بحسب تصميمها من قبل الفاعل، فهو الذي يحدد كيفية عملها، فقد يقوم بإرسال هذه الفيروسات عن طريق رسائل البريد الإلكتروني، ويحدد بدء عملها بمجرد فتح هذه الرسائل من قبل الشخص المتلقي، وقد تبدأ هذه الفيروسات العمل بمجرد تشغيل البرامج الموجودة عليه في الجهاز وهكذا (الجنبيهي، منير والجنبيهي، ممدوح، 2005، 47).

وفيروس النظام المعلوماتي كما حدده أحد التقارير الصادرة عن المركز الأمريكي القومي للحاسبات يعتبر بمثابة "برامج مهاجمة تصيب الأنظمة المعلوماتية بأسلوب يُماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان" (الملط، 2006، 540).

وفي نطاق الجرائم المعلوماتية فإن كلمة "فيروس" تستخدم للدلالة على كافة البرامج الخبيثة التي تؤدي إلى إتلاف وتدمير المعلومات وأنظمة المعالجة الآلية للبيانات، وتتعدد هذه البرامج في أنواعها، ويعتبر الفيروس أحدها، وتتسبب هذه البرامج الخبيثة بإتلاف المكونات المنطقية لجهاز الحاسب الآلي، ويمكن التفرقة بينها من خلال أسلوب كل منها في القيام بوظيفة، بحيث تختلف أساليب عملها في إتلاف نظم المعالجة الآلية للبيانات (قوره، 2005، 192).

وتتمتع الفيروسات بقدرة عالية في تغيير الحقيقة أو تعديل المعلومات المخزنة في الحاسب الآلي أو المتداولة عبر الشبكات، فهي تقوم باختراق أجهزة الحاسوب والشبكات، المعلوماتية، وتشويه المعلومات والبيانات وتعطيل الاتصالات، وقد تضلل المستخدم أحياناً ببيانات ومعلومات خاطئة، الأمر الذي يجعلها تشكل خطورة كبيرة على النظام المعلوماتي (المومني، 2008، 126).

وتجدر الإشـارة أن نسـبة جرائم الإتلاف المعلوماتي الناتجة عن الإصـابات الفيروسـية قد ازدادت بشـكل ملفت في السـنوات الأخيرة، خاصـة بعد التوسع في استخدام الإنترنت والاعتماد عليه في كافة نواحي الحياة، والاعتماد على البريد الإلكتروني الذي يشـكل أرضية خصبة ومناخاً ملائماً لمثل هذا النوع من الجرائم، حيث إنه لا يمر يوم واحد دون أن تظهر عشرات الفيروسـات الجديدة التي تسـتهدف الحاسبات الشخصية في المنازل والحاسـبات المسـتخدمة في المؤسـسات الاستثمارية الكبرى وغيرها، والتي تؤدي إلى خسائر فادحة تقدر بمليارات الدولارات.

ومن أسـوأ حوادث الفيروسـات في العالم "ما حدث في شركة ديل لإنتاج الحاسبات الآلية عام 1999 في المصـنع الذي أنشـأته تلك الشركة في إيرلندا ليقوم بتصنيع الحاسبات الشخصية والخادمة التي ستباع في مختلف أنحاء أوروبا والشرـق الأوسـط وأفريقيا، حيث تسـبب فيروس الحب (Fun Love) بإغلاق المصـنع لمدة يومين، فهذا المصـنع يتلقى أوامر التصـنيع عن طريق شـبكة الإنترنت، وكل العمليات التي تتم داخله تتحكم فيها أجهزة الحاسـوب دون تدخل بشرـي، حيث اضـطر المصنع إلى إعادة تصنيع أكثر من إثني عشر ألف حاسـب كانت في مرحلة الإنتاج عندما تسـبب هذا الفيروس في إغلاق الحاسـبات التي تتحكم في مراحـل الإنتـاج، حيـث تسـبب هـذا الفيروس بخسـائر مـاليـة تبلغ عشرـات الملايين من الـدولارات" (الجنبيهي، منير والجنبيهي، ممدوح، 2005، 58 وما بعدها).

ثانياً: أنواع الفيروسات:

للفيروسات أنواع متعددة ويمكن تقسيمها من حيث تكوينها وأهدافها إلى:

(1) فيروس عام العدوى: وهو الفيروس الذي ينتقل إلى أي برنامج أو ملف.

(2) فيروس محـدود العـدوى: وهو الفيروس الـذي يسـتهـدف نوعاً معيناً من النظم لمهاجمته، ويتميز عن النوع السابق بأنه أبطأ في الانتشار وأصعب في الاكتشاف.

(3) فيروس عام الهدف: وهذا النوع تندرج تحته الغالبية العظمى من الفيروسـات التي تم اكتشـافها حتى الآن، ويتميز بسهولة إعداده، واتساع مدى تدميره.

(4) فيروس محـدد الهـدف: وهو لا يؤدي إلى تعطيـل عمـل البرنـامج بل إلى تغيير الهدف منه، ويحتاج هذا الفيروس إلى درجة عالية من المهارة والدراية التامة بالتطبيق الذي يسـتهدفه الفيروس (رسـتم، 2000، 456).

ويمكن الإشارة إلى أهم وأشهر الفيروسات الموجهة ضد الحواسيب والشبكات المعلوماتية وذلك كما يلي:

(1) فيروس الإبطاء: ويتمثل عمل هذا الفيروس في إبطاء عمل النظام المعلوماتي بصورة تدريجية تمهيداً لإيقافه عن العمل.

(2) الفيروسات النائمة: "وتعتبر هذه من أخطر أنواع الفيروسات التي تصيب الأنظمة المعلوماتية على الإطلاق، وتكمن خطورتها في كونها تظل منكمشة إلى حين ثم تنطلق لتنفيذ أهدافها التخريبية، ومن أخطرها فيروس عيد الميلاد المجيد الذي ظهر في عام 1987 وانتشر في أوروبا وأمريكا" (الملط، 2006، 542).

(3) فيروس حصان طرواده: "وهو عبارة عن برنامج فيروس لديه قدرة على الاختفاء في البرنامج الأصلي للمستخدم، وعندما يتم تشغيل البرنامج الأصلي ينشط الفيروس المتمثل في حصان طروادة وينتشر ليبدأ نشاطه التدميري، وهذا الفيروس يؤدي إلى تعديل البرنامج، وتزوير المعلومات، ومحو بعضها، وقد يصل إلى تدمير النظام بأكمله".

(4) الفيروسات التطويرية: "وهي فيروسات لها القدرة على أن تقوم بتغيير شكلها بمرور الوقت، وبذلك تستطيع أن تقوم بمهمة تدمير برامج وبيانات الحاسوب دون صعوبة تذكر" (المومني، 2008، 129).

(5) الفيروس الإسرائيلي: "تم اكتشافه في الجامعة العبرية في القدس، وهو يقوم بإبطاء تشغيل النظام المعلوماتي إلى نصف زمن التشغيل تقريباً بعد نصف ساعة فقط من تشغيل الجهاز".

(6) فيروس السرطان: "وهو فيروس يمسح أجزاء من الشاشة بطريقة تدريجية حتى يقضي على الشاشة كلها" (الشوا، 1994، 193).

(7) فيروس القردة: "هذا الفيروس يعرض على الشاشة مجموعة من القرود، تقوم بعمل بعض الألعاب البهلوانية خلال قيام البرنامج بنسخ نفسه في أكثر من مكان في النظام، وتدمير الفهرس الرئيس للقرص الصلب" (عطية، 2001، 321).

وهناك العديد من الفيروسات المنتشرة خلال الشبكات العالمية والتي توافق مناسبات معينة نذكر منها على سبيل المثال:

(1) فيروس مايكل أنجلو: "وأطلق هذا الفيروس يوم 6 مارس عام 1992 بمناسبة الاحتفال بذكرى ميلاد الرسام الإيطالي الشهير مايكل أنجلو، وقد أصاب هذا الفيروس عدداً كبيراً من أجهزة الحاسوب الشخصية المنتشرة في دول العالم" (رضوان، 1999، 58-60).

(2) فيروس ناسا: "وهذا الفيروس أطلق احتجاجاً على الحرب النووية وإنتاج الأسلحة النووية، فهو يحمل رسالة مناهضة للأسلحة النووية، وتتكاثر هذه الرسالة وتكرر نفسها لتدمير البرامج الأخرى، وكان هدف هذا الفيروس اختراق شبكة الحاسبات التابعة لوكالة "ناسا" الفضائية الأمريكية" (الملط، 2006، 543).

(3) فيروس الكريسماس: "ويتمثل هذا الفيروس برسالة بريد إلكتروني تعرض بطاقة تهنئة بالكريسماس على الشاشة، وفي خلال هذا الوقت يقرأ الملفات التي تحتوي على عناوين المشتركين في الشبكة، ويرسل نسخ من نفسه إلى هؤلاء المشتركين، مما يترتب عليه توقيف النظام كله، حتى يتم عزله والقضاء عليه" (العبابنة، 2005، 102).

الفرع الثاني: برامج الدودة (Worm Software):

وهي عبارة عن برامج مخصصة لاستغلال أية فجوات في نظام التشغيل للحاسب الآلي، حيث تنتقل من جهاز إلى آخر ومن شبكة إلى أخرى عبر الوصلات التي تربط بينهما (Links)، وتقوم بالتكاثر أثناء انتقالها كالبكتيريا وذلك بإنتاج نسخ منها، وتهدف هذه البرامج إلى شغل أكبر حيز ممكن من سعة الشبكة، وتقليل أو خفض كفاء تها، وتؤدي أحياناً إلى التكاثر والانتشار الواسع في الجهاز، مما يؤدي إلى التخريب الفعلي للملفات والبرامج ونظم التشغيل وبروتوكولات الاتصال (رستم، 2000، 453).

وهذا الفيروس يقع على جزء محدد من نظام المعالجة الآلية للبيانات وهو الجزء الخاص بنظام التشغيل (Oprating System)، ويقصد به "مجموعة البرامج التي تتحكم في إمكانات الحاسوب، وفي العمليات التي تستخدمها هذه الإمكانات" (المومني، 2008، 131).

أما بالنسبة لآلية عمل هذه الديدان فتختلف طريقة عملها من نوع إلى آخر، ففي حين تقوم بعضها بنسخ نفسها لمرات متتالية وكثيرة وهائلة داخل الجهاز، يقوم بعضها الآخر وعن طريق البريد الإلكتروني بإرسال نفسها على شكل رسائل على كافة العناوين الموجودة في النظام، ويقوم البعض الآخر بإرسال رسائل بذيئة إلى بعض الأشخاص الموجودة عناوينهم في دفتر العناوين الموجود في الجهاز باسم مالك البريد، الأمر الذي يوقعه في حرج كبير مع من تم إرسال تلك الرسائل إليهم (الجنبيهي، منير والجنبيهي، ممدوح، 2005، 61).

ومن أمثلة برامج الدودة ما يعرف بـ (Internet – warm) "والتي عن طريقها تمكن طالب أمريكي يدعى روبرت مورس (وهو طالب دراسات عليا في جامعة كورنيل في ولاية نيويورك) من تدمير ست عشرة ألف شبكة حاسب آلي منتشرة في الولايات المتحدة الأمريكية، وترتب على هذا الهجوم خسائر تمثلت في تأخير الأبحاث آلاف الساعات، وفي إعادة البرمجة بتكاليف بلغت عدة ملايين من الدولارات" (الشوا، 1994، 194).

الفرع الثالث: البرامج (القنابل) المنطقية أو الزمنية:

وهي إحدى البرامج التي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف، وتقسم هذه البرامج أو القنابل إلى قسمين وذلك كما يلي:

أولاً: القنابل المنطقية:

"وهي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة محددة، أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع" (العريان، 2004، 99).

والقنابل المنطقية تظل ساكنة دون حركة بحيث لا يتم اكتشافها مدة من الزمن قد تطول أو تقصر، وذلك يحدده المؤشر الموجود داخل هذا البرنامج، وهذا المؤشر يبقى ينتظر توافر شروط منطقية معينة داخل برنامج أو ملف معين، وذلك حسب الرمز الذي يحدده البرنامج القنبلة، فإذا حل الميعاد أو توافرت هذه الشروط بدأ البرنامج بالقيام بمهامه التخريبية (الشاذلي، فتوح وعفيفي، كامل، 2003، 225).

ومن الأمثلة الواقعية على برنامج القنابل المنطقية قيام أحد العاملين في إدارة المياه والطاقة في ولاية لوس أنجلوس الأمريكية بوضع قنبلة منطقية في نظام الحاسب الآلي الخاص بهذه الإدارة، مما أدى إلى تخريب هذا النظام ولعدة مرات (الشوا، 1994، 196).

ثانياً: القنبلة الزمنية أو الموقوتة:

وسميت بالزمنية لقيامها با لعمل التخريبي في وقت يحدد سلفاً (عوض، 1993، ص427)، "وهي عبارة عن برامج يتم إدخالها بطرق مشروعة متخفية مع برامج أخرى، وتهدف إلى تدمير برامج ومعلومات النظام وتغييرها وتعمل على مبدأ التوقيت حيث تنفجر في وقت معين" (المومني، 2008، 133).

وعلى سبيل المثال يمكن ضبط هذه البرامج بحيث تنفجر بعد عامين من ضبطها، وذلك في يوم محدد وفي ساعة محددة، بحيث يقوم هذا البرنامج بتحويل مبلغ من النقود من حساب شخص معين في الوقت الذي يكون مرتكب الجريمة متواجداً في دولة أخرى (الملط، 2006، 545).

ومن الأمثلة الواقعية على برامج القنابل الزمنية أو الموقوتة قيام مبرمج في ألمانيا الديمقراطية بزرع برنامج القنبلة الزمنية في النظام المعلوماتي الخاص بالشركة التي يعمل فيها، وتمت برمجة القنبلة بحيث تنفجر بعد عامين من فصله من الشركة، وفي حوالي الساعة الثالثة مساءً، وكما سجل هذا المبرمج في البرنامج، بقي الاستفهام الخاص بيوم وساعة وسنة التنفيذ مستمراً، وكان متأكداً من أن لحظة التدمير ستراعى بكل دقة، وانفجر هذا البرنامج في الوقت المحدد مما أدى إلى انهيار النظام، وأدى ذلك إلى تعطيل أكثر من 300 وحدة طرفية ولبضعة أيام، وكان من الصعب اكتشاف الفاعل نظراً للتفاوت في الزمن بين لحظة ارتكاب الفعل ولحظة تحقق النتيجة (الشوا، 1994، 196).

المطلب الثالث: الحماية الجنائية للمعلوم ات المعالجة آلياً من الاتلاف وفقاً للمشرع الأردني:

تعتبر جريمة إتلاف المعلومات التقنية من أكثر الجرائم المعلوماتية انتشاراً والتي لابد من إحاطتها بالحماية الجزائية اللازمة، وقد خلصنا سابقاً من خلال دراستنا لجريمة السرقة بأن قوانين العقوبات التقليدية لم تطال المال المعلوماتي بالحماية، فجرائم الأموال الواردة في قانون العقوبات الأردني جاءت لحماية حق الملكية، وهذه الملكية لا تكون إلا على الشيء المادي الملموس وليست المعلومات المعالجة آلياً.

وقد تناول المشرع الأردني جريمة الإتلاف في الفصل السادس من الباب الحادي عشر من قانون العقوبات الأردني رقم (16) لسنة 1960 وتعديلاته وذلك تحت عنوان الأضرار التي تلحق بأملاك الدولة والأفراد، في المادة (445)، وتطلب المشرع لقيام هذه الجريمة ركناً مادياً يتمثل بإتيان الفاعل سلوكاً مادياً يقع على مال منقول مملوك للغير، ويلحق به الضرر بان يجعله غير قابل للإصلاح أو الاستعمال أو يؤثر عليه وينقص من قيمته الاقتصادية أو بتعطيل الشيء محل الجريمة وإعاقته عن العمل كلياً أو جزئياً، وبالتالي ترد نفس العقبات التي نصطدم بها دائماً من عدم إمكانية تطبيق النص الجزائي التقليدي على الجرائم المعلوماتية ومنها الإتلاف، نظراً لما تتمتع به المعلومات المعالجة آلياً من طبيعة معنوية بعيدة كل البعد عن الطبيعة المادية الملموسة للمال محل الحماية في قانون العقوبات، فالمشرع الأردني شأنه شأن معظم التشريعات العربية لم يأخذ بعين الاعتبار الطبيعة اللامادية للأموال، وما إذا كانت تصلح لأن تكون محلاً لجريمة الإتلاف التقليدية أم لا، على النقيض من بعض التشريعات الأجنبية.

لما تقدم وعند دراسة موقف المشرع حول مدى توفير الحماية الجنائية اللازمة للمعلومات المعالجة آلياً عبر النظام المعلوماتي، فإن ذلك يتطلب منا الوقوف على اتجاه المشرع الأردني ابتداءً من قانون الاتصالات الأردني رقم (13) لسنة 1995 وحتى قانون جرائم أنظمة المعلومات الأردنية المؤقت رقم (30) لسنة 2010 وذلك كما يلي:

الفرع الأول: الحماية الجنائية للمعلومات من الإتلاف في قانون الاتصالات الأردني رقم (13) لسنة 1995:

أصدر المشرع الأردني قانون الاتصالات رقم (13) لسنة 1995 ، وذلك في محاولة منه لمواكبة التطور الحاصل في مجال تكنولوجيا المعلومات. ولتوفير الحماية الجنائية اللازمة للمعلومات والبيانات المتداولة عبر شبكات الاتصالات الأردنية، سواء العامة منها والتي تقدم خدمة الاتصالات العامة لكافة المستفيدين، أو الخاصة التي تُشغل لمصلحة شخص واحد أو مجموعة واحدة من الأشخاص تجمعهم ملكية مشتركة لخدمة حاجاتهم الخاصة.

ويبدو أن المشرع الأردني قد أشار إلى جريمة الإتلاف من خلال المواد 72، 76، 77 من ذات القانون حيث نصت المادة 72 على ما يلي:

"أ- كل من أقدم قصداً على تخريب منشآت الاتصالات أو ألحق بها ضرراً عن قصد يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل على (200) دينار ولا تزيد على (5000) دينار أو بكلتا العقوبتين، وتضاعف العقوبة إذا تسبب فعله بتعطيل حركة الاتصالات.

ب- كل من تسبب إهمالاً في تخريب منشآت الاتصالات أو إلحاق الضرر بها، يعاقب بالحبس مدة لا تزيد على ثلاثة أشهر أو بغرامة لا تزيد على (100) دينار أو بكلتا العقوبتين".

كما نصت المادة 76 على أنه، "كل من اعترض أو أعاق أو حور أو شطب محتويات رسالة بواسطة شبكات الاتصالات أو شجع غيره على القيام بهذا العمل، يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر أو بغرامة لا تزيد على (200) دينار أو بكلتا العقوبتين".

ونص أيضاً في المادة 77 على "كل من أقدم على كتم رسالة عليه نقلها بوساطة شبكات الاتصال إلى شخص آخر، أو رفض نقل رسائل طلب منه نقلها سواء من قبل المرخص له أو الهيئة، أو نسخ أو أفشى رسالة أو عبث بالبيانات المتعلقة بأحد المشتركين بما في ذلك أرقام الهواتف غير المعلنة والرسائل المرسلة أو المستقبلة، يعاقب بالحبس لمدة لا تزيد على ستة أشهر، أو بغرامة لا تزيد على (1000) ديناراً أو بكلتا العقوبتين".

مما تقدم يرى الباحث أنه باستقراء نص المادة 72 من قانون الاتصالات الأردني أنها جاءت لحماية منشآت الاتصالات من أفعال التخريب التي قد تطالها وتؤدي إلى إلحاق أضرار بها، سواء وقع ذلك بشكل مقصود أم نتيجة الإهمال، إلا أن المشرع لم يوضح المقصود بمنشآت الاتصالات في المادة الثانية من ذات القانون والخاصة بتعريف المصطلحات، ويبدو أن المشرع كان قد قصد بذلك المباني المقامة عليها شبكات الاتصالات، والأجهزة المخصصة للاتصالات والأجهزة الملحقة بها، ولذلك فإن إرادة المشرع لم تأت واضحة ولم تخل من اللبس والغموض من حيث استيعابها للمعلومات والبيانات التي تحتويها هذه الشبكات، الأمر الذي يصعب معه تطبيق هذا النص على إتلاف البيانات والمعلومات المعالجة آلياً.

أما بالنسبة للمادة 76 من ذات القانون فيرى الباحث أن المشرع حاول من خلال هذا النص توفير الحماية الجنائية للرسائل المرسلة عبر شبكات الاتصالات من الاعتراض أو الإعاقة أو التحوير أو الشطب، وفي المادة 77 من ذات القانون عاقب على كتم هذه الرسائل أو نسخها أو إفشائها أو العبث في البيانات المتعلقة بأحد المشتركين، وحيث إن إتلاف المال المعلوماتي يقع عن طريق الدخول المتعمد للنظام المعلوماتي من قبل الجاني، أو باستخدام الطرق التقنية والفنية للإتلاف (البرامج الخبيثة)، وذلك بهدف تخريب المعلومات وتدميرها أو تشويشها أو محوها، الأمر الذي يؤدي إلى الإضرار بالنظام المعلوماتي وعجزه عن القيام بوظائفه المعتادة، فإن ذلك يستوجب من المشرع النص الصريح والقاطع لمثل هذه السلوكات الجرمية الرقمية المتمثلة في استخدام الحاسب الآلي والإنترنت والمؤدية إلى إتلاف المعلومات، وذلك تماشياً مع مبدأ شرعية الجرائم والعقوبات، فيحسب للمشرع الأردن محاولته في مواكبة التطور الحاصل في تقنية تكنولوجيا المعلومات، إلا أن النصوص الواردة في قانون الاتصالات والسالفة الذكر جاءت غير واضحة ويشوبها الغموض فيما يتعلق باحتوائها على البيانات و المعلومات المعالجة آلياً، ويبدو أنها جاءت ترتكز على موضوع الحماية الجنائية لشبكات الاتصالات الهاتفية أكثر منها الإلكترونية.

الفرع الثاني: الحماية الجنائية للمعلومات من الإتلاف في قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010:

كفل المشرع الأردني الحماية الجنائية للمعلومات والبيانات المخزنة في الحاسب الآلي أو المتبادلة عبر شبكات الإنترنت من خطر الإتلاف وذلك من خلال قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010.

حيث نصت المادة (3) من ذات القانون على:

أ- كل من دخل قصداً إلى موقع إلكتروني أو نظام معلوماتي بأية وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، يعاقب بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار أو كلتا العقوبتين.

ب- إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو تعديل أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو أشغاله أو انتحال صفته أو انتحال شخصية مالكه، فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين".

كما ونصت المادة (4) من ذات القانون على: "كل من أدخل أو نشر أو استخدم قصداً برنامجاً عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ أو إلتقاط أو تمكين الآخرين من الاطلاع على بيانات أو معلومات أو إعاقة أو تشويش أو إيقاف أو تعطيل عمل نظام معلومات أو الوصول إليه أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله أو انتحال صفته أو انتحال شخصية مالكه دون تصريح أو بما يجاوز أو يخالف التصريح، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار أو بكلتا هاتين العقوبتين".

ومن خلال نص المادة 3/ب فإننا نجد أن المشرع الأردني قد جرم فعل الدخول المقصود إلى موقع إلكتروني بأية وسيلة ودون تصريح أو بما يخالف أو يجاوز التصريح بهدف إتلاف أو تدمير البيانات أو المعلومات، ومن خلال فهم النص فإن هذه الجريمة تقوم على ثلاثة أركان وذلك كما يلي:

أولاً: الركن المادي:

يتمثل الركن المادي في جريمة إتلاف المعلومات المعالجة آلياً وفقاً للمشرع الأردني في السلوك التقني الصادر عن الجاني باستخدام الحاسوب والإنترنت والمتمثل في الدخول إلى موقع إلكتروني أو نظام معلومات بأية وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح بهدف إتلاف أو تدمير أو إلغاء أو حذف أو إضافة أو تعديل المعلومات.

وهذا السلوك يقوم على عنصرين أحدهما مادي والآخر معنوي، ويتمثل العنصر المادي في السلوك الإجرامي الرقمي الذي يصدر عن الجاني والمتمثل في دخوله إلى موقع إلكتروني أو نظام معلومات وذلك عن طريق الاتصال السلكي أو اللاسلكي بين الشبكات، أو عن طريق الحصول على الرقم السري للنظام والدخول إليه أو أية وسيلة أخرى للدخول غير المشروع، أما العنصر المعنوي فيتحقق بأن يكون الدخول للنظام أو الموقع الإلكتروني دون إذن صاحب العلاقة. وكما سبق وأسلفنا بأن المادة (2) من ذات القانون عرفت التصريح بأنه الإذن الممنوح من صاحب العلاقة ....إلخ.

ثانياً: محل الجريمة:

وفقاً لنص المادة 3/ب وفيما يتعلق بجريمة الإتلاف المعلوماتي فإن محل هذه الجريمة هي البيانات والمعلومات وقد يكون أيضاً الموقع الإلكتروني أو النظام المعلوماتي.

ثالثاً: الركن المعنوي:

تطلب المشرع في الفقرة أ من المادة 3 والخاصة بجريمة الدخول غير المصرح به القصد العام القائم على عنصري العلم والإرادة، فالمشرع استخدم تعبير قصداً ولذلك فهذه الجريمة لا تقوم بالخطأ، أما الفقرة ب من ذات المادة فقد جاءت بظرف مشدد للجريمة، حيث يتطلب لتطبيقها قصداً خاصاً وهو ليس مجرد الدخول وإنما أن يكون هذا الدخول بهدف تعطيل أو تدمير أوإتلاف....، فقد جاء المشرع بالباعث أو الدافع إلى الدخول غير المصرح به واشترطه قصداً جرمياً خاصاً لتشديد العقوبة وفق الفقرة ب.

والملاحظ هنا من خلال تدقيق نص المادة 3/ب أن المشرع الأردني عاقب على مجرد الدخول المقصود وغير المشروع إلى الموقع الإلكتروني أو النظام المعلوماتي بهدف إتلاف البيانات أو المعلومات، فلم ينتظر وقوع فعل الإتلاف وتحقيق نتيجته المتمثلة في إتلاف أو تدمير المعلومات المعالجة آلياً وجعلها غير صالحة للاستعمال، أو الإنقاص من قيمتها الاقتصادية، أو بتعطيلها جزئياً أو كلياً.

ويبدو أن المشرع زيادة في التحوط استخدم عبارة الدخول غير المشروع للنظام المعلوماتي بهدف إتلاف أو تدمير المعلومات، ولم يستخدم عبارة كل من أتلف المعلومات...إلخ، كالعبارات التي عوّدنا عليها في النصوص التقليدية مثل "كل من استعمل بدون حق شيئاً يخص غيره ..إلخ، "كل من اشترى مالاً مسروقاً.. إلخ، "يعاقب الذين يرتكبون السلب في الطرق العامة ..إلخ"، "كل من أدار محلاً عمومياً للمقامرة....إلخ، فنجد أن المشرع اعتبر فعل الدخول غير المشروع للنظام بهدف إتلاف المعلومات مجرماً ولم ينتظر وقوع النتيجة، والحقيقة أن هناك صعوبة في إثبات الغاية

أو الهدف من الدخول غير المشروع للموقع الإلكتروني أو النظام المعلوماتي، وخاصة في الحالات التي يتوقف فيها نشـاط الجاني عند الدخول غير المشـروع إلى النظام دون إتيان سـلوكاً آخر يعبر فيه عن إتلاف المعلومـات، فقد ينجح الجاني في الدخول غير المصرـــح فيه إلى النظام المعلوماتي ويكون هدفه من ذلك هو إتلاف المعلومات إلا أن تلك الغاية أو الهدف يكمن في ذهن الجاني، ويبقى ذا طبيعة نفســية محضــة من الصــعوبة إثباتها إلا إذا انطوت على ســلوك جرمي رقمي يدل عليها ويحقق نتيجتها وفي حال عدم تحقق نتيجة الإتلاف ففي مثل هذه الحالة وفقاً لنص المادة (3) لا يعاقب الجاني إلا عن فعل الدخول غير المشروع إلى النظام المعلوماتي أو الموقع الإلكتروني ولا يُسأل عن جريمة إتلاف المعلومات الإلكتروني، وبذلك يفلت من عقوبة جريمة إتلاف المال المعلوماتي وهي العقوبة الأشــد وفقاً للنص، فجريمة الإتلاف المعلوماتي وفقاً للنص لا يمكن أن تتحقق إلا بتحقق نتيجتها.

ومن خلال نص المادة (4) من ذات القانون نجد أن المشرع الأردني قد جرم إتلاف أو تدمير البيانات والمعلومات أو النظام المعلوماتي أو الموقع الإلكتروني عن طريق إدخال أو نشر أو استخدام برامج عن طريق الشــبكة المعلوماتية أو باســتخدام نظام معلوماتي، ويبدو أن إرادة المشرــع هنا قد اتجهت لتوفير الحماية الجنـائيـة للبيـانـات والمعلومـات والمواقع الإلكترونيـة والنظام المعلوماتي من خطر برامج الفيروســات على اختلاف أنواعها وأشكالها.

ومن خلال مـا تقدم يرى الباحث أن المشرــع الأردني قد وفر الحماية الجنائية اللازمة للمعلومات الإلكترونية من جرائم الإتلاف والتدمير التي قد تقع عليها وبكافة الوسائل، سواء تم ذلك عن طريق الدخول غير المصرح به من قبل الجاني إلى النظام المعلوماتي أو الموقع الإلكتروني ومن ثم إتيانه سلوكاً رقمياً من شأنه إتلاف هذه المعلومات، أو عن طريق قيام الجاني بإدخال أو نشر أو استخدام برامج الفيروسات على اختلاف أنواعها بهدف إتلاف أو تدمير المعلومات أو تدمير وتعطيل الموقع الإلكتروني أو النظام المعلوماتي.

المطلب الرابع: الحماية الجنائية للمعلومات المعالجة آلياً من الإتلاف وفقاً للمشرع الأمريكي:

وسوف نبين هنا موقف التشريع الفيدرالي الأمريكي ومن ثم موقف قوانين بعض الولايات وذلك كما يلي:

الفرع الأول: موقف التشريع الأمريكي الفيدرالي من الإتلاف المعلوماتي:

وفقاً للقانون الفيدرالي لجرائم الحاسب الآلي الصادر عام 1984 فإن فعل الإتلاف الموجه إلى المعلومات والبيانات المعلوماتية لم يكن مجرماً إلا إذا تعلق الأمر بحكومة الولايات المتحدة، ويتضح ذلك من خلال نص المادة (1030) فقرة (3) من ذات القانون والتي نصت على تجريم إتلاف المعلومات المؤدي إلى إعاقة عمل حكومة الولايات المتحدة الأمريكية عند استعمال أنظمة الحاسوب، وجاء في نص المادة أعلاه أنه "كل من توصل بشكل متعمد وبدون تصريح إلى نظام الحاسوب لغير العامة والخاص بحكومة الولايات المتحدة الأمريكية، أو أية وكاله تابعه لها على سبيل الحصر،وبشكل يؤدي الى إعاقة الحكومة عن إستخدام أنظمة الحاسوب الخاصه بها" [8].

ونجد هنا أن هذه المادة اقتصرت على أفعال الدخول التي تطال المعلومات الخاصة بالنظام المعلوماتي الخاص بحكومة الولايات المتحدة الأمريكية، والتي من شأنها إعاقة الحكومة من استعمال هذا النظام.

ووفقا لنص الماده 1030/C/A من ذات القانون والخاصة بالعقوبات فإن الفاعل يعاقب عن الأفعال السابقة بالحبس مدة لا تزيد على سنة أو الغرامة [9].

---

[8] Article 1030/A/3 of US Fedral law of 1984

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

[9] Article 1030/C/A of US Fedral law of 1984

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

وفي عـام 1986 ونتيجـة للانتقـادات التي وجهـت لهذا القانون أدخلت عليه تعديلات وأصـــبحت الفقرة الثالثة من المادة (1030) تنطوي على الدخول غير المصرـــح به إلى النظام المعلوماتي للحكومة فقط، وأضـــيفت فقرة خاصـــة لذات المادة تجرم الإتلاف العمدي للمعلومات الطبية بصرـف النظر عن مقدار الخسـائر المالية المترتبة، وسـواء أكانت هذه المعلومات مخزنة في الحواسـيب الآلية التابعة للحكومة، أم غير التابعة لها ولكن يتم استخدامها من قبلها أو لمصالحها (Griffith, Ds, 1990, p 453).

وجاء المشرـــع الفيدرالي بتعديل آخر في عام 1994 حيث أضـــفى الحماية الجنائية على المعلومات المتعلقة بالدفاع الوطني الأمريكي من أفعال الاعتداء التي قد تطالها.

(Icove, and Vonstorch, 1995, p 260)

وفي عام 1996 أصـدر المشرـع الفيدرالي قانون حماية المعلومات القومية "The NII Protection Act"، وبموجب هذا القانون لم تعد الحماية الجنائية مقتصرة على الأنظمة المعلوماتية الخاصة بالحكومة أو المستعملة من قبلها، وإنما اتسعت لتشمل الأنظمة الخاصة بالمؤسسات الاقتصادية التابعة للحكومة، وكذلك الحواسيب الآلية المستخدمة في قطاعي التجارة والاتصالات بين الولايات، أو بين الولايات والدول.

وعـدلـت الفقرة الخامســـة من المادة 1030/A من القانون الفيدرالي الأمريكي ، وذلك وفقا لنص الفقره الخامسه من الماده 1030/A من القانون الأمريكي الفيدرالي لحماية المعلومات القومية (THE NII PROTECTION ACT 1996) بحيث أصبحت تجرم الأفعال التالية:

1. التسـبب المقصـود في تعديل برنامج أو معلومات أو شـيفرات أو أمر دون الحصول على إذن وإحداث ضرر في الحاسب الألي محل الحمايه.
2. الدخول غير المشرـوع والمقصـود لنظام الحاســب وأدى ذلك الى ضرر في الحاســب الألي على الرغم من توقع الجاني.
3. الدخول غير المشروع والمقصود لنظام الحاسب الألي متى ترتب عليه ضرر[10].

---

[10] Article 1030/A/5 of NII Protection Act of 1996
(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage

حددت الفقرة الثامنة من المادة 1030/E المقصود بالأضرار بأنها" أي إتلاف أو تدمير أو إفساد لسلامة المعلومات والبيانات والبرامج والنظام المعلوماتي[11](http/www.law.cornell.edu/uscode/text/18/1030.) (Stephen, H,1997,379)

وتجدر الإشـــاره هنا ان المشرــع الأمريكي قد جرم أفعال الإعتداء على أنظمة وخطوط الإتصـــالات والمحطات من الإتلاف والتخريب والتدمير، وذلك من خلال الماده 1362 من الفصل 18 من القانون الفيدرالي لعام 1994، حيث نصـت الماده أعلاه على أنه" كل من قام وبشكل مقصود بتدمير أو إتلاف أو الإضرار بأية وســـيلة من وســـائل الإتصـــال ،الراديو أو البرقيه أو الهاتفيه أو الكوابل او الخطوط أو المحطات أو أنظمة الإتصـالات ،أو غيرها من وسـائل الإتصـال التي تسيطر عليها الولايات المتحده ،مما يؤدي الى عرقلة أو إعاقة او التأخير في نقل أية إتصالات ضمن هذه الخطوط أو الأنظمة ،فإنه يعاقب بالغرامة أو الحبس لمدة لا تزيد على عشر سنوات أو بكلتا العقوبتين[12]

---

[11] Article 1030/E/8 of NII Protection Act of 1996

8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that

(A) causes loss aggregating at least $5,000 in value during any 1year period to one or more individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety; and

[12]Article 1362 section 18 of us fedral law of 1994
§1362. Communication lines, stations, or systems

Whoever willfully or maliciously injures or destroys or attempts willfully or maliciously to injure or destroy any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, shall be fined under this title or imprisoned not more than ten years, or both.

الفرع الثاني: موقف تشريع الولايات من الإتلاف المعلوماتي:

أولاً: ولاية نيويورك:

نصـــت الفقرة الأولى من المـادة 25 من قـانون جرائم العبـث في الكمبيوتر على أنه "كل شـــخص يسـتخدم الحاسـب الآلي دون وجه حق وبشـكل متعمد لتغيير أو تبديل أو تعديل في البيانات والمعلومات والبرامج الخاصة با لحاسب الآلي، فإنه يُجرم بالعبث في الحاسب الآلي من الدرجة الثانية.

ونصـت الفقرة الثانية من ذات المادة "إن ذلك الشخص يجرم بالعبث في الحاسب الآلي من الدرجة الأولى في حال كان هذا الاســتخدام بقصــد تغيير أو تعديل أو تحطيم أية خامات للحاســب الآلي وكانت الأضرار تزيد على ألف دولار" (سليمان، لات، 16).

ثانياً: ولاية كاليفورنيا:

اتجهت بعض الولايات في مجال التعامل مع الأنظمة المعلوماتية إلى وضــع نصــوص صريحة تجرم الأفعال التي تسـتهدف إتلاف المعلومات، واهم ما يميز هذه النصـوص أنها تخلت عن إشتراط صفة المنقول أو العقار في المال الواقع عليه فعل الإتلاف، واكتفت بتوافر الصفة المالية للشيء الواقع عليه الإتلاف.

وبنـاءَ على ذلـك فقـد جرم قـانون العقوبـات الخـاص بولايـة كـاليفورنيا أفعال الإتلاف الموجهة إلى أنظمة المعالجة الآلية للمعلومات وتخريبها بمكوناتها المادية والمعنوية (المومني، 2008، 123، 138، 139).

وفي شـــهر يناير من عام 1988 أصـــدرت الولاية قانوناً يجرم أية محاولة مقصـــودة للوصـــول إلى المعلومات والبيانات دون تصريح وذلك بهدف:

- تغيير أو إتلاف أو تدمير معلومات وبيانات وأجهزة الحاسـب الآلي أو نظم أو شبكات من أجل الحصول على أموال وبيانات.

In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defense functions of the United States.

- تغيير أو إضافة أو إتلاف أو تدمير أية بيانات أو برامج في الحاسب الآلي.
- إفساد أو التسبب في إفساد خدمات الحاسب الآلي.
- توفير أو المساهمة في توفير وسيلة للوصول إلى الحاسب الآلي.
- الوصول إلى الحاسب الآلي أو التسبب في ذلك (البشري، 2005، 158 وما بعدها).

ثالثاً: ولاية فلوريدا:

جرم المشرع في ولاية فلوريدا الأفعال الموجهة ضد المكونات المادية والمعنوية للحاسب الآلي، حيث جرم أفعال العبث والتعديل في المعدات والتجهيزات المستخدمة في الحاسب الآلي، أو التي سيتم استخدامها فيه أو الشبكة المعلوماتية (المعلومات والبرامج)، ووضع عقوبة جنحوية من الدرجة الأولى لهذه الجريمة، وشدد العقوبة إلى جنائيه إذا كانت الأضرار والخسائر التي لحقت بمعدات الحاسب الآلي أو نظامه أو شبكة المعلومات تعادل ألف دولار أمريكي أو أكثر، أو إذا أدى ذلك الفعل إلى إعاقة أو إفساد عمليات حكومية. (سليمان، لات، 16 وما بعدها)

وقد ذهبت غالبية الولايات، إلى سن نصوص تشريعية صريحة في تجريم أنشطة إساءة استخدام الحاسوب، فنصت قوانين كل من أريزونا، كولورادو، دوبلاوار، جورجيا، الينوي، متشجان، ميسوري، مونتانا، نيومكسيكو، رودايسلاند، تينسي، أوتاو، سكونسيت على تجريم إتلاف القيم المعلوماتية غير المادية، وغش الحاسوب، والاستخدام غير المصرح به للحاسوب، وسرقة وقت خدمات الحاسوب، وإعاقة استخدامه، والتوصل غير المصرح به لتعديل أو تغيير أو إفشاء أو استخدام البيانات والمعلومات المخزنة في نظام الحاسوب. (عرب، 2006، 5)

ويرى الباحث مما سبق أن المشرع الأمريكي وفر الحماية الجنائية اللازمة للمعلومات المخزنة في الحاسب الآلي أو المتداولة عبر الشبكة سواء أكان ذلك على الصعيد الفيدرالي أم على صعيد تشريعات الولايات.

المبحث الثالث: جريمة إعاقة عمل النظام المعلوماتي:

تعتبر هـذه الجريمـة من الجرائم المتداخلة مع جريمة الإتلاف المعلوماتي من حيث إن الأفعال التي قد تؤدي إلى كل منهما واحدة، كتعديل طرق المعالجة الآلية، أو إدخال معطيات بشـــكل تحايلي، أو تغيير المعلومـات أو محوهـا أو إدخال برامج خبيثة، وقد فرقت منظمة التعاون الاقتصـــادي والتنمية في تقريرها المتعلق بجرائم المعلومـاتيـة بين إتلاف المعلومـات من ناحية، وبين إعاقة أنظمة الحاســـب الآلي من ناحية أخرى (قورة، 2005، 202 وما بعدها)، لذلك فقد تم تقسـيم هذا المبحث إلى مطلبين أولهما مفهوم الجريمة وطرق إرتكابها، وثانيهما موقف التشريعات المقارنة من هذه الجريمة.

المطلب الأول: مفهوم الجريمة وطرق إرتكابها:

فرق المجلس الأوروبي في توصـيته رقم (89) والصـادرة بخصـوص جرائم الحاسـب الآلي بين إتلاف المعلومات والبرامج كســـلوك قائم بذاته، وبين إتلاف المعلومات والبرامج أو التدخل في أنظمة الحواســـيب الآلية بنية إعاقتها عن أداء عملها، وقد انتهت التوصية بتوجيه الدول الأعضاء إلى ضرورة العمل على تجريم كلٍ منهما بنصـــوص منفصـــلة، وبينت التوصـــية أهمية تجريم الأفعال التي تؤدي إلى إحداث خلل وظيفي للحاسب الآلي ونظامه لما قد يترتب عليها من خسائر مادية (قورة، 2005، 203).

وفعـل الإعـاقة قد يحدث بطريقه مادية أو معنوية، ومن أمثلة إعاقة النظام بطريقة مادية أعمال العنف المادية التي تقع على أجهزة الحاسـب الآلي وشـبكات الاتصال عن طريق تخريبها بكسرها، أو سكب السائل عليها أو أية مادة أخرى، أو منع العاملين في النظام من العمل (حجازي، 2009، 34)

وقـد تتحقق الإعاقة عن طريق محو أو تعديل المعطيات الموجودة في النظام المعلوماتي، وذلك عن طريق إضـــافـة معطيـات جـديـدة بهدف تعطيل النظام المعلوماتي، وقد تتحقق الإعاقة عن طريق برنامج معلوماتي كما لو قام الجاني بإدخال فيروس على البرامج كفيروس حصـــان طرواده، أو عدل كلمة السرـــ أو كيفيـة أداء النظـام المعلومـاتي لوظيفتـه بوســـيلـة تؤدي إلى توقف أو تعطيل في أداء وظيفة داخل النظام المعلوماتي (حجازي، 2009، 34 وما بعدها).

المطلب الثاني: موقف التشريعات المقارنة من هذه الجريمة:

تناول المشرـع الفرنسيـ جريمة إعاقة عمل النظام المعلوماتي وجريمة إتلاف المعلومات في الفصـل الثالـث من الكتـاب الأول من قانون العقوبات الفرنسيـ الجديد والخاص بجرائم المعالجة الآلية للبيانات وذلـك في المـادتين 323-2، 323-3، حيـث تنـاول في الأولى إعـاقـة عمل النظام المعلوماتي وفي الثانية الإتلاف المعلوماتي.

وقد جاء نص المادة 323-2 من قانون العقوبات الفرنسيـ الجديد لسـنة 1994 على أنه "يعاقب بالحبس لمدة خمس سـنوات وغرامة مقدارها 75000 يورو، كل من قام بإعاقة أو عرقلة أو التدخل في سـير عمل نظام المعالجة الآلية للبيانات [13] ".

وجاء نص المادة 323-3 من ذات القانون على أنه "يعاقب بالحبس خمس سنوات وغرامة مقدارها 75000 يورو كـل من أدخل إلى نظام المعالجة الآلية للمعلومات بطريقة إحتيالية بيانات أو محا أو عدل في البيانات التي يحويها النظام [14] ".

وبمقتضىـ المادة 323-2 من قانون العقوبات الفرنسيـ الجديد، فإن المشرـع الفرنسيـ جرم كافة الأفعـال التي من شـأنهـا أن تؤدي إلى الحيلولـة دون أن يعمـل نظـام المعالجة الآلية للبيانات على الوجه المحدد له، وشمل التجريم أيضاً الأفعال التي تؤدي إلى الحيلولة دون الوصول إلى النظام.

وبموجب المادة 323-3 من ذات القانون فإن المشرـع الفرنسي جرم أفعال إتلاف المعلومات المخزنة أو المتـداولة عبر النظام المعلوماتي أو حذفها بطرق احتيالية دون تحديد طبيعة هذه المعلومات، حيث ترك النص عاماً ليتسـع لكافة أنواع المعلومات، كما وأن طرق إتلاف المعلومات الواردة في النص تتسـع لتشـمل كافة أشـكال الاعتداء على المعلومات، بما في ذلك استخدام البرامج الخبيثة أياً كانت وسيلة إدخالها إلى نظام الحاسب الآلي.

---

[13] Article 323/2 Of (FCP)

Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

[14] Article 323/3 Of (FCP)

Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

كما وأن المشرع الفرنسي في المادة 323-5 من قانون العقوبات الفرنسي الجديد،" أوجب عقوبات إضافية على الأشخاص الطبيعيين الذين يرتكبون هذه الجرائم إضافةً إلى العقوبات الأصلية وهي كما يلي:

1- المصادرة المدنية والحقوق المدنية والعائلية وفقاً للشروط المنصوص عليها بموجب المادة 131-26.

2- حظر شغل المناصب والوظائف العامة لمدة أقصاها خمس سنوات.

3- مصادرة الأشياء التي استخدمت أو المعدة لارتكاب الجريمة، أو التي نتجت عن الجريمة باستثناء المواد الخاضعة للتعويض.

4- إغلاق المحل التجاري المعد لارتكاب الجريمة لمدة أقصاها خمس سنوات.

5- المنع من الدخول في المناقصات العامة لمدة أقصاها خمس سنوات .

6- حظر الحصول على الشيكات. لمدة أقصاها خمس سنوات

7- درجة العرض العام، أو نشر القرار، وفقاً للشروط المنصوص عليها بموجب المادة 131-35 [15] " .

---

[15] Article 323/5 Of(FCP)

Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;

2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;

3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;

6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;

7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35.

كما وأن المشرع الفرنسي في المادة 323 – 6 من ذات القانون، قد حدد العقوبات المترتبةعلى الأشخاص المعنوية عن هذه الجرائم، وهي الغرامات المالية وفقاً للشروط المنصوص عليها بموجب المادة 131-38، والعقوبات المشار إليها في المادة 131-39 من ذات القانون[16] ".

أما في الولايات المتحدة الأمريكية فقد صدر القانون الفيدرالي رقم (18) المتعلق بجرائم الحاسب الآلي عام 1984، والذي تم تعديله عدة مرات، وأشار إلى جريمة إعاقة عمل النظام المعلوماتي وأطلق عليه مصطلح منع وصول الخدمة، وعوقب مرتكب هذه الجريمة بموجب نصوص القانون (عبابنه، 2005، 85).

وكما أشرنا ف قد اقتصر التجريم وفقاً لقانون عام 1984 في الفقرة الثالثة من المادة 1030/A على إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحواسيب الآلية (قوره، 2005، 214).

وقد نصت الفقرة الخامسة من المادة 1030/A بعد تعديلها على تجريم:

"1- تعديل المعلومات والبرامج والشيفرات والأوامر داخل أنظمة الحواسيب الآلية، ما تترتب عليه أضرار تلحق بحاسب آلي يتمتع بالحماية متى كان إحداث الضرر قد تم عمداً،

2- الدخول المقصود وغير المصرح به إلى حاسب آلي يتمتع بالحماية متى ترتب عليه أضرار تلحق بالحاسب الآلي على الرغم من توقع الجاني.

3- الدخول المقصود وغير المصرح به متى ترتب عليه أضرار تلحق بالحاسب الآلي" ويعد الفعل في الفقرتين الأولى والثانية جناية بينما في الفقرة الثالثة جنحة [17].

---

[16] Article 323/6 Of (FCP)

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38 ;

2° Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise

[17] Article 1030/A/5 NII Protection 1996

وقد حددت الفقره الثامنة من الماده 1030/E المقصود بالأضرار التي تلحق بالحاسب الآلي بأنها "كل إتلاف أو إفساد لسلامة المعلومات والبرامج وأنظمة الحواسيب الآلية[18]".

أما المشرع الأردني فقد عالج جريمة إعاقة عمل النظام المعلوماتي في المادة 3/ب والمادة 4 من قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010، ففي المادة 3/ب جرم فعل الدخول المقصود إلى موقع إلكتروني أو نظام معلومات بهدف تعطيل أو إعاقة عمل نظام المعلومات، وعاقب على ذلك بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار، أو بكلتا هاتين العقوبتين.

كما وأنه في المادة (4) من ذات القانون جرم أفعال الإدخال أو النشر أو الاستخدام المقصود لبرامج خبيثة (فيروسات) عن طريق الشبكة المعلوماتية أو النظام المعلوماتي، بهدف إعاقة أو تشويش أو إيقاف أو تعطيل عمل النظام المعلوماتي، وعاقب على ذلك بالحبس مدة

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage

[18] Article 1030/E/8 NII Protection 1996

8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that

(A) causes loss aggregating at least $5,000 in value during any 1year period to one or more individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety; and

لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار، أو بكلتا هاتين العقوبتين.

ولم يتطرق المشرع الأردني إلى عقوبات إضافية على الأشخاص الطبيعيين الذين يرتكبون مثل هذه الجرائم، كما وأنه لم يتطرق إلى عقوبات الأشخاص المعنويين في هذا القانون كما هو الحال في قانون العقوبات الفرنسي الجديد، ويرى الباحث أن ذلك لا يعني عدم مسؤولية هؤلاء الأشخاص، بحيث يتم الرجوع إلى الأحكام والقواعد العامة الواردة في قانون العقوبات الأردني وذلك في الفقرة الثانية من المادة 74 منه، حيث يسأل الشخص المعنوي عن هذه الجرائم إذا ارتكبت من أحد أعضائه بإسمه أو بإحدى وسائله، ووفقاً لنص الفقرة الثالثة من ذات المادة يعاقب الشخص المعنوي بالغرامة أو المصادرة أو التدبير الإحترازي.

المبحث الرابع: جريمة الاحتيال المعلوماتي:

أصبحت المؤسسات المالية في وقتنا الحاضر تعتمد وبشكل أساسي على التقنيات الحديثة وتكنولوجيا المعلومات في كافة معاملاتها المالية سواء على الصعيد الداخلي أو الخارجي، حيث ترتبط هذه المؤسسات بنوك ومصارف من في شتى أنحاء العالم عن طريق شبكة وأنظمة المعلومات، وهي تقوم بإجراء الحوالات المالية للعملاء داخل البلاد أو خارجها وفي جميع أنحاء العالم في وقت قياسي قد لا يتعدى الثواني المعدودة من خلال الشبكات المعلوماتية ومهما تباعدت المسافات فيما بينها، وحيث أن المعلومات المتعلقة بهذه الحوالات الإلكترونية وبأرقام الحسابات الخاصة بالعملاء تنتقل بين المؤسسات المالية عبر النبضات الإلكترونية سواء داخل أجهزة الحاسوب أو عبر الشبكة العالمية للمعلومات، فإن ذلك خلق بيئة مناسبة لبعض المجرمين لارتكاب جرائم معلوماتية عبر هذه الشبكات وخاصة الاحتيال المعلوماتي، وتعتبر جرائم الاحتيال المعلوماتي من أكثر الجرائم انتشاراً وخطورة في العالم، وتؤدي إلى خسارات مالية فادحة خاصة إذا تعلقت الجريمة بالتحويل الإلكتروني للأموال والودائع المصرفية أو

ما يسمى بالأموال الإلكترونية، فقد أصبحت لعنة تلاحق البنوك وذلك لضخامة حجم الأموال المتداولة عبر الأنظمة المعلوماتية، وإتاحة الفرصة للمجرم المعلوماتي بارتكاب جريمته من أبعد المسافات وتخطي الحدود الإقليمية للعديد من الدول، وسلب الأموال موضوع الجريمة في زمن قياسي قصير قد لا يتعدى ثواني محدودة (القشي، ودهمش، 2005، 49).

وتتعدد الوسائل والأساليب التي تستخدم في جرائم الاحتيال والغش المعلوماتي، مع أنها جميعها تؤدي إلى نتيجة واحدة و هي التعدي على المعلومات والبيانات المخزنة آلياً والتلاعب فيها، للحصول بغير وجه حق على أموال أو أصول، وتحقيق العديد من الأغراض الإجرامية الأخرى.

وللوقوف على جريمة الاحتيال المعلوماتي فإننا سوف نبين في هذا المبحث مدلولها وماهيتها، والوسائل والأساليب التي ترتكب فيها أفعال الاحتيال المعلوماتي، وموقف المشرع الأردني والأمريكي والفرنسي من هذه الجريمة وذلك وفقاً للمطالب التالية :

1- ماهية الاحتيال المعلوماتي والأساليب التقنية المستخدمة في ارتكابه.
2- صور الاحتيال المعلوماتي.
3- الحماية الجنائية للمعلومات المعالجة آلياً من الاحتيال المعلوماتي وفقاً للمشرع الأردني.
4- الحماية الجنائية للمعلومات المعالجة آلياً من الاحتيال المعلوماتي وفقاً للمشرع الأمريكي.
5- الحماية الجنائية للمعلومات المعالجة آلياً من خطر الاحتيال المعلوماتي وفقاً للمشرع الفرنسي.

المطلب الأول: ماهية الاحتيال المعلوماتي والأساليب التقنية المستخدمة في ارتكابه:

وسوف نتناول في هذا المطلب مفهوم الاحتيال المعلوماتي وأساليب ارتكابه ووسائله وذلك كما يلي:

الفرع الأول: مفهوم الاحتيال المعلوماتي:

تعددت التعريفات التي قيلت بشأن الاحتيال أو الغش المعلوماتي، فعرفته هيئة الأمم المتحدة بناءً على التوجيه رقم (R9/89) والتي تبناها المجلس الأوروبي بأنه "إدخال البيانات أو محوها، أو تعديلها، أو كبتها، أو برامج الحاسوب، أو التدخل المؤثر في معالجة البيانات التي تسبب خسارة اقتصادية، أو فقد حيازة ملكية شخص آخر، بقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص آخر" (قندح، 2004، 6)

وقد عرفته لجنة أوديت (Audit Commission) لجنة تدقيق الحسابات في المملكة المتحدة، حيث عرفت غش الحاسوب بأنه "أي سلوك احتيالي أو خداعي مرتبط بالكمبيوتر، يهدف شخص بواسطته إلى كسب فائدة أو مصلحة مالية" (عبابنة، 2005، 55).

وعرفه البعض بأنه "كل سلوك احتيالي يرتبط بعملية التحسيب الإلكتروني، بهدف كسب فائدة أو مصلحة مالية، (صالح، 2000، 7).

وتجدر الإشارة هنا أن الاحتيال المعلوماتي يشمل الاحتيال عن طريق الحاسب الآلي والاحتيال عبر الإنترنت، وقد عرفت وزارة العدل الأمريكية الاحتيال عبر الإنترنت بأنه "شكل من التخطيط الاحتيالي الذي يستخدم محتويات الإنترنت، مثل: الدردشة، البريد الإلكتروني، المواقع الإلكترونية، ... لتقديم صفقات احتيالية أو لإرسال نتائج الاحتيال إلى المؤسسات المالية"

.(Kunz and Wilson, 2004, P. 12)

وعرفه أيضاً مكتب التحقيقات الفيدرالي الأمريكي بأنه "أي مخطط احتيالي عبر الإنترنت، يلعب دوراً هاماً في عرض السلع أو الخدمات غير الموجودة أصلاً، أو طلب دفع ثمن تلك الخدمات أو السلع عبر الشبكة" (الخن، 2011، 38).

وذهب بعض الفقه إلى تعريف الاحتيال المعلوماتي بأنه "التلاعب المقصود بمعلومات وبيانات تمثل قيماً مادية يختزنها النظام المعلوماتي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة أو أية وسيلة أخرى من شأنها التأثير على الحاسوب، حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع وإلحاق ضرر بالغير" (قوره، 2005، 444).

وبناء على ما تقدم يرى الباحث أن هذا التعريف هو الأوسع والأشمل لصور الاحتيال المعلوماتي، وهو ما يذهب معه الباحث.

الفرع الثاني: أساليب ووسائل الاحتيال المعلوماتي:

تنوعت أساليب ووسائل الاحتيال المعلوماتي وفقاً للتطور الذي تشهده تكنولوجيا المعلومات، ولاعتماد المؤسسات المالية في أيامنا الراهنة على وسائل التحويل الإلكتروني للأموال سواء داخل إقليم الدولة نفسها أو خارجه، وهذا ما أدى إلى زيادة ارتكاب مثل هذه الجرائم وشيوعها وتطور أساليب ارتكابها، وزيادة عدد مجرميها، لذلك فسوف نلقي الضوء على أهم الوسائل والأساليب المستخدمة في ارتكاب جريمة الاحتيال المعلوماتي

وذلك كما يلي:

أولاً: التلاعب في المعلومات والبيانات في مراحل المعالجة الآلية للبيانات في الحاسب الآلي (الإدخال والإخراج)، بغية تحقيق أغراض غير مشروعة:

تتنوع وسائل التلاعب في المعلومات والبيانات في مرحلتي إدخال وإخراج البيانات والمعلومات،

فقد يعمد الجاني إلى تغيير المعلومات والبيانات المراد إدخالها إلى نظام المعالجة الآلية دون حذف أي جزء من أجزائها، وقد يقع التغيير على كافة البيانات أو جزء منها، وقد يضيف الجاني بيانات جديدة بهدف تغيير البيانات الأصلية، الأمر الذي يؤدي إلى تغيير في معنى هذه البيانات المراد إدخالها للنظام، فيفهمها النظام وفقاً للمعنى الجديد الذي تم التلاعب فيه، مما يؤدي إلى خروجها عن الحقيقة التي كانت تمثلها، وقد يعمد الجاني إلى حذف جزء أو عدة أجزاء من البيانات المدخلة، أو حذف هذه البيانات كاملة وإدخال بيانات مخالفة لها بهدف تغيير المخرجات الناتجة عن نظام المعالجة الآلية للبيانات، وبهذه الحالة تكون المعلومات المخرجة عن هذه العملية بعيدة كل البعد عن المعلومات التي يرغب المجني عليه بإخراجها، وقد يقوم الجاني بإدخال المعلومات في غير المكان المخصص لها، وهذا يؤدي إلى عرقلة عمل هذه المعلومات عن القيام بوظيفتها التي يستهدفها المستخدم من خلال عملية نظام المعالجة الآلية للبيانات (http/www.coeia.edu.com).

وفي كافة الحالات السابقة فإن الجاني يسعى من خلال سلوكه المادي إلى غش الحاسب الآلي وإدخال بيانات ومعلومات عاريه عن الصحة، أو العبث في البيانات والمعلومات المدخلة أو جزء منها أو تعديلها، لتحقيق النتيجة الإجرامية المتمثلة في الاحتيال على النظام المعلوماتي، للحصول على منفعة مادية واختلاس الأموال.

وبتفصيل أكثر فإن التلاعب في المعلومات والبيانات المعالجة آلياً يمكن أن يتم بطريقتين، الأولى عن طريق قيام الجاني بإدخال معلومات غير صحيحة تخدم أهدافه غير المشروعة، والثانية بقيامه بإتلاف أو تعديل المعلومات المخزنة في الحاسب الآلي لخدمة أهدافه الإجرامية، وذلك كما يلي:

(1) حالة قيام الجاني بإدخال معلومات مبتكرة من قبله وغير صحيحة لتحقيق أهدافه غير المشروعة:

وغالباً ما تستخدم هذه الطريقة من الأشخاص أو الموظفين الذين يعملون في أقسام المحاسبة، وتقتضي- طبيعة عملهم إجراء المعاملات المالية في منشأة معينة أو شركة أو مؤسسة أو دائرة، بحيث يقوم الجاني بإدخال معلومات غير صحيحة إلى النظام المعلوماتي الخاص بالشركة أو المؤسسة

التي يعمل فيها وذلك للحصول على منفعة مادية، كأن يقوم بإضافة مستخدمين مؤقتين أو موظفين أو عمال وهميين للشركة، وفي نهاية الشهر يقوم بتسطير شيكات بنكية بدل رواتب من الشركة بأسماء هؤلاء المستخدمين الوهميين، وبالنتيجة حصوله على هذه المنفعة المالية، وقد يقوم الجاني أيضاً بالإبقاء على مستخدمين تركوا الوظيفة لدى الشركة وكأنهم يزالون على رأس عملهم ويبقي ملفاتهم مفعلة في النظام المعلوماتي، ويقوم هو باستلام رواتبهم في نهاية كل شهر، وقد يقو م الجاني أيضاً باختلاس مبالغ مالية ضخمة من حسابات الشركة، ويكون هذا أكثر شيوعاً في البنوك والمصارف، كموظف البنك الذي يقوم بفتح حسابات وهمية وبأسماء وهمية، ويقوم بإجراء تحويلات مالية ضخمة لهذه الحسابات الوهمية عن طريق النظام المعلوماتي، والحصول على مبالغ ضخمة.

(2) حالة قيام الجاني بإتلاف المعلومات المخزنة في الحاسب الآلي لخدمة أهدافه الإجرامية:

وعادةً ترتكب هذه الجرائم من قبل الأشخاص المسؤولين عن تخزين المعلومات وحفظها، وتقع الجريمة هنا بأن يقوم الجاني بتغيير أو إتلاف المعلومات المسؤول عن حفظها، بحيث يؤدي فعله هذا إلى تغيير الواقع والحقيقة، وذلك لخدمة أهدافه غير المشروعة، وللحصول على المنفعة المادية، كموظف البنك الذي يقوم بتغيير رقم حساب بآخر، أو إحلال بطاقة مكان أخرى، ويعتبر هذا النوع من الجرائم على قدر كبير من الخطورة، حيث إن الجاني قد يستمر بسلوكه الإجرامي لفترة طويلة من الزمن إلى أن يتم اكتشاف أمره.

ومن الأمثلة على ذلك، قيام مجموعة من المستخدمين لدى شركة معينة وخلال عدة سنوات من مضاعفة رواتبهم عن طريق استخدام الحاسب الآلي، دون أن يتم اكتشاف أمرهم إلا بمحض الصدفة، وأيضاً قيام بعض المستخدمين بتقاضي ساعات إضافية لم يقوموا بتنفيذها نهائيا عن طريق استبدال قوائم الحاسبات بساعات العمل (سلامة، 2006، 170-171).

وتجدر الإشارة هنا أن التلاعب في مرحلة إخراج المعلومات هي الأقل حدوثاً من الوسائل الأخرى للاحتيال المعلوماتي، وذلك وفقاً لتقرير لجنة المراجعة في المملكة المتحدة عام 1985، حيث وقعت (77) حالة احتيال معلوماتي من بينها فقط حالتان تمت عن طريق التلاعب في المعلومات في مرحلة إخراج البيانات المعالجة آلياً (قوره، 2005، 458 وما بعدها).

أما في الولايات المتحدة الأمريكية فقد ظهر أن 62% من حالات الاحتيال عبر شـــبكة الإنترنت التي تم اكتشـــافها حتى عـام 1984 تنطوي على تلاعـب في البيـانـات والمعلومـات قبل وأثناء إدخالها إلى نظام المعالجة الآلية للبيانات (السـويلميين، 2009، 80+81). كما وأن المكتب الأعلى للإحصاء في الولايات المتحدة الأمريكية قد أجرى تحقيقاً عام 1976 بخصـــوص ظاهرة الغش في الأنظمة المعلوماتية الخاصـــة بالحكومة الفيدرالية، وقد جاء في نتيجتها أن غالبية أفعال الغش ارتكبت عن طريق إدخال بيانات مصطنعة بما نسبته (62%)، وما نســبته (25%) تنطوي على الاســتعمال غير المشــروع للوســائل المعلوماتية، و(23%) تعديل المعالجات المعلوماتية، و(17%) اختلاس الوثائق الصادرة عن الحاسب الآلي (محمود، 2001، 83 + 84).

ثانياً: التعدي على البرامج التطبيقية ونظم التشغيل:

تعتبر هذه الوسـائل الاحتيالية من جرائم المتخصـصين والمحترفين في مجال الحاسب الآلي، وهي من أكثر الوســـائل الاحتيالية خطورة، فهي تســـتلزم معرفة فنية ودراية كافية في مجال برمجة الحاســـب الآلي، ويمكن أن يتحقق التعـدي خلال مرحلـة إعـداد هـذه البرامج، أو عند صـــيانتها أو تحديثها وذلك كما يلي: (سلامة، 2006، 173)

(1) تعديل البرامج التطبيقية:

وهذه البرامج تقوم بإعدادها شركات متخصـــصـــة في هذا المجال ومن ثم بيعها إلى المؤســـســـات والشـركات والجامعات وغيرها، حيث تقوم الأخيرة باسـتخدامها في مجال عملها داخل إداراتها، ومن أمثلتها برامج المحاسبة في البنوك، وبرامج الرواتب في الشركات والمؤسسات، وبرامج العلامات في الجامعات وغيرها.

ويتم الاعتـداء على هـذه البرامج عن طريق قيـام الجاني الذي يتمتع بالخبرة الفنية في مجال البرمجة بتغيير أو تعديل تلك البرامج المفعلة في النظام المعلوماتي للشـركة أو المؤســســة أو البنك، في الوقت الذي تكون فيه هذه البرامج بحاجة إلى تعديل معين أو تحديث أو صـيانة، فيقوم الجاني بإدخال التعديلات التي تســاعـده على إتمـام أفعـال الغش والاحتيال المعلوماتي لتحقيق أغراضـــه غير المشـــروعة باختلاس النقود والحصول على المنفعة المالية لنفسه.

ومن الأمثلة التي توضح مدى خطورة هذا النمط من الإجرام المعلوماتي:

أ- "قيام مبرمج كان يعمل في أحد البنوك بتعديل برنامج إدارة الحسابات في هذا البنك، بحيث يضيف بموجب هذا التعديل 10 سنتات إلى مصاريف إدارة الحسابات على كل عشرة دولارات، ودولاراً واحداً على الحسابات التي تتعدى عشرة دولارات، وقد تم قيد المصاريف الزائدة في حساب خاص فتحهُ باسم مستعار، وهكذا فقد حصل هذا الجاني المختلس على عدة مئات من الدولارات كل شهر، وكان بالإمكان أن يستمر هذا العمل الإجرامي لولا أن البنك الذي كان يعمل فيه أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافيء أول وآخر عميل له وفقاً للترتيب الأبجدي، وحينئذ اكتشف البنك عدم وجود هذا الإسم المستعار" (سلامة، 2006، 173 وما بعدها).

ب- هناك تقنية أطلق عليها (Perru que) تؤدي إلى برمجة الحاسب الآلي بحيث يستقطع بعض السنتيمات من الإيداعات الدورية وتحويلها إلى حسابات خاصة، ومن أشهر الأمثلة على هذه التقنية قيام مستخدم في إحدى شركات التأمين ببرمجة الحاسب الآلي بحيث يقوم باستقطاع السنتيمات من كل عمليات الشركة، ثم تحويلها إلى حسابه السري (الشوا، 1994، 79).

(2) تعديل برامج التشغيل:

كما ذكرنا سابقاً فهذه البرامج تختص بصناعتها وإعدادها شركات متخصصة في برمجة الحاسوب، وتقوم ببيعها للمستخدمين سواء الأفراد أو الشركات أو الدولة وهي ضرورية لكافة أجزاء وملحقات الحاسب الآلي، وبدونها لا تستطيع هذه الآلات والملحقات أن تقوم بأداء وظائفها، فالبرامج التشغيلية تسمح بتنظيم وتزامن وضبط التعليمات والوظائف الخاصة بالحاسب الآلي. ومن أمثلتها برنامج شركة ميكروسوفت (Microsoft) لتشغيل الحاسب الآلي.

وتتحقق الوسيلة الاحتيالية بأن يعمد الفاعل إلى استخدام التقنية المتمثلة في تعديل هذه البرامج لتحقيق أغراضه الإجرامية. ويطلق على هذه التقنية الحديثة المصيدة (Trappe)، وهي تقع بعدة طرق لتحقيق أهداف غير مشروعة للجاني وأهم هذه الطرق هي كما يلي:

أ- تعديل البرامج عن طريق المداخل المميزة:

قد يحتوي برنامج التشغيل ابتداءً على عيوب وأخطاء فنية من الشركة المصنعة، وقد لا يكتشف البعض منها إلا عند استخدامه، ويقع العبء هنا على عاتق المبرمجين العاملين في الشركة المستخدمة للولوج إلى هذه البرامج الأساسية وتصحيحها، وذلك عن طريق المداخل المميزة، والتي هي عبارة عن ممرات خالية متروكة في البرنامج، بحيث تسمح الشركة المصنعة للمبرمج المستخدم بإجراء تعديلات في الشيفرة والمنافذ الوسطية في حالة اكتشاف أية عيوب في برنامج التشغيل، ولكن قد يصل الأمر في بعض المبرمجين من ذوي النوايا السيئة بأن يتغاضوا عن استبعاد هذه المداخل المميزة، ولا ينبهوا إليها أي شخص، ويبقوا يستخدمون البرنامج المعيب من الناحية الفنية دون تصميمه بالطريقة السابقة، وعن طريق المداخل المميزة يمكن للمبرمج سيء النية الولوج إلى كافة المعلومات الموجودة في ذاكرة الحاسب الآلي، بحيث يصبح هو سيد النظام المعلوماتي ويقوم بارتكاب أفعال الغش والاحتيال المعلوماتي لتحقيق أغراضه الإجرامية، الأمر الذي يؤدي إلى تكبد المجني عليه خسائر فادحة لم يكن ليتوقعها (الشوا، 1994، 82 وما بعدها).

ب- اصطناع برنامج:

ويتحقق ذلك بأن يقوم الجاني باستحداث برنامج يعده ويصممه خصيصاً من أجل التخطيط للجريمة ومراقبتها وتنفيذها لتحقيق أهدافه الإجرامية (سلامة، 2006، 176).

ومن الأمثلة على هذه الطريقة التقنية الاحتيالية قيام شركة أمريكية باصطناع وثائق تأمين لأشخاص وهميين بلغ عددهم (64000) وثيقة، ثم قامت الشركة بعد ذلك ببيع الوثائق لأشخاص آخرين وحصلت مقابل ذلك على عمولات من شركات التأمين التي تعمل لحسابها، وحصل الجناة في هذه القضية على مبلغ (200) مليون دولار (المومني، 2008، 194).

ثالثاً: التعدي على المعلومات المتدفقة عبر شبكة الإنترنت بوسائل احتيالية لتحقيق أغراض غير مشروعة:

يعمد مرتكبو أفعال غش الحاسوب والاحتيال المعلوماتي إلى استخدام البريد الإلكتروني للقيام بجرائهم والتعدي على المعلومات المتدفقة عبر شبكة الإنترنت، وبالتالي لتحقيق أهدافهم غير المشروعة والحصول على المكاسب المالية المتنوعة، ومن أشهر الطرق التقنية التي يستخدمها المجرمون هنا طريقة الرسائل المتسلسلة (Chian letters)، وطريقة الهرم.

وتتحقق الطريقة الأولى بأن يقوم الجاني بإرسال بريد إلكتروني للغير ويتضمن عدداً قليلاً من الأسماء على شكل قائمة، ويطلب فيها من المستقبل إرسال مبلغ معين عبر البريد العادي إلى عنوان الشخص الوارد اسمه في أعلى القائمة (وهو الجاني). ويطلب منه أيضاً إرسال الرسالة التي تلقاها عبر البريد الإلكتروني إلى عدد كبير من أصدقائه وأقاربه والذين عليهم اتباع نفس الخطوات، ويقوم الجاني هنا بإيهام المجني عليه أنه عندما يصل اسمه إلى أعلى القائمة بعد فترة وجيزة ستتدفق عليه الأموال، وهكذا يتحقق الاحتيال بالطريقة التقنية عبر البريد الإلكتروني (الشوابكة، 2009، 183).

وتتحقق الطريقة الثانية بأن يقوم الجاني بإرسال بريد إلكتروني للغير يتضمن قائمة التعليمات وقائمة تضم عشرة أسماء وعناوينهم، ويطلب من المستقبل إرسال مبلغ عشرة دولارات مثلاً إلى الشخص الذي ترتيبه العاشر في القائمة (ويكون نفسه مرسل الرسالة)، وإرسال مبلغ دولار واحد إلى أول خمسة أشخاص في القائمة، ويبين الجاني في التعليمات أنه في حال إرسال المستقبل لمبلغ العشرة دولارات للإسم العاشر في القائمة فإنه سوف يتم شطبه وحلول اسم المجني عليه نفسه (المستقبل)، بحيث يسترجع ما دفعه في حال اشتراك أشخاص عن طريقه، وهكذا يبقى يرتفع اسمه إلى أعلى القائمة تدريجياً، وهكذا تتحقق الجريمة الاحتيالية التقنية ويحصل الجناه على المكاسب المالية (الشوابكة، 2009، 183).

المطلب الثاني: صور الاحتيال المعلوماتي:

إن التقدم التكنولوجي في مجال شبكات الإنترنت المحلية والدولية قد أدى إلى ظهور أساليب كثيرة ومتعددة للاحتيال عبر الإنترنت، ولكثرة وتنوع هذه الطرق فإننا سوف نلقي الضوء على أبرزها لأن المجال لا يتسع لنا لذكر كافة صور هذه الجريمة، كما وأنها تستجد بين الحين والآخر وتتطور وفقاً لتطور التقدم التقني، لذلك يمكن ذكر صور الاحتيال الأساسية عبر الإنترنت كما يلي:

الفرع الأول: الاستيلاء على أموال المصارف:

تُعد الجرائم التي تقع على أنظمة التحويل الإلكتروني للأموال والودائع المصرفية

وبإجماع الفقه من أخطر جرائم غش الحاسوب، وذلك يرجع إلى المبالغ الهائلة التي تمثلها المعلومات والبيانات ذات الأصول المالية، والتي يجري نقلها في وقت قياسي سواء على المستوى الإقليمي أو المستوى الدولي، ولشيوع استخدام تقنيات النقل الإلكتروني للأموال عبر المصارف، ولما يجنيه الجناة من منافع مالية كبيرة وفي وقت قصير جداً، ولشعورهم بالأمان نتيجة تجاوز هذه الجرائم للحدود الوطنية للدولة، ولصعوبة اكتشاف مثل هذا النوع من الجرائم (عرب، 2002، 419).

ومع التقدم التقني في تكنولوجيا المعلومات فقد أصبح بإمكان عملاء المصارف والبنوك الاطلاع على كافة حساباتهم الخاصة وإجراء التحويلات التي يرغبون فيها عبر المواقع الإلكترونية الموجودة على شبكة الإنترنت والخاصة بهذه المصارف أو البنوك، وهذا ما شكل بيئة خصبة لدى مجرمي المعلوماتية باقتحام الأنظمة المعلوماتية الخاصة بالبنوك والمصارف والتلاعب في كشوفات وحسابات العملاء، ونقل الأرصدة من حساب إلى آخر، أو إضافة بضعة أصفار إلى رقم ما في هذا الحساب أو ذاك.

ومن الأمثلة الواقعية على ذلك في الولايات المتحدة الأمريكية قيام موظف مختص بالحسابات في بنك أمريكي بتحويل مبالغ قدرت بأربعة ملايين دولار من حسابات عملاء هذا البنك إلى حساب خاص به قام بفتحه في أحد المصارف السويسرية، وذلك بعد أن اكتشف بطريقة الصدفة شيفرة تحويل حسابات العملاء بين البنك وغيره من البنوك التي تتعامل معه، ولم يتم اكتشاف أمره إلا باعترافه بالواقعة وهو مخمور (الخن، 2011، 48 وما بعدها).

الفرع الثاني: الاحتيال التجاري:

تنتشر عبر شبكة الإنترنت مواقع الشركات العالمية والتجارية المتخصصة في بيع السلع والبضائع عبر هذه الشبكة، ويستطيع أي مستخدم للشبكة وفي أي مكان سواء من منزله أو مكان عمله أو غيرها الدخول إلى هذه المواقع والاطلاع على تلك البضائع والسلع حيث يتم عرضها للبيع المباشر أو عن طريق المزاد، وتتحقق جريمة الاحتيال المعلوماتي عندما يقوم المجني عليه بشراء سلعة معينة من بعض هذه الشركات عبر شبكة الإنترنت ويقوم بدفع ثمنها عن طريق حسابات معينة أو بطاقات الائتمان ويتفاجأ بعد ذلك بعدم التسليم.

وتجدر الإشارة هنا أن هناك مؤسسات مالية تعمل عبر شبكة الإنترنت وتختص باستلام النقود من العملاء الذي يشترون بضائع من الشركات المنتشرة عبر المواقع الإلكترونية، وتقوم المؤسسة بتجميد تلك الأموال لديها حتى يصلها إخطار من المشتري بأنه قد تسلم البضائع التي اشتراها، وأنها مطابقة للمواصفات المطلوبة، ثم بعد ذلك تقوم هذه المؤسسة بتحويل الأموال إلى المواقع التي تم الشراء منها، ويطلق على هذه الخدمة (Escrow House) وفي حال عدم وصول البضائع التي طلبها العميل، أو أنها غير مطابقة للمواصفات، فإنه يمكن استرداد هذه الأموال[19] (الصغير، 2002، 39).

[19] ومن مواقع هذه المؤسسات المالية المختصة بحماية العملاء واستلام البضائع والسلع التي تم شرائها هو – (www.iescrou.com).

الفرع الثالث: الاحتيال المعلوماتي في مجال الأسهم والأوراق المالية:

تزايد إقبال الأفراد في الدول على شراء الأسهم والأوراق المالية عن طريق المواقع الإلكترونية المنتشرة عبر شبكة الإنترنت، الأمر الذي أدى إلى اشتراك معظم طبقات المجتمعات في هذه العمليات المالية، وبصرف النظر عن مهنة هؤلاء الأفراد أو طبيعة عملهم، فنجد بعضهم من المستثمرين المختصين بمضاربة العملة والأوراق المالية والأسهم، ونجد البعض الآخر من الأفراد العاديين الذي لا يمتهنون أية مهنه، ونجد منهم الموظفين في القطاع العام، أو العمال في القطاع الخاص، ومنهم الصيادلة والأطباء والمهندسين والمحامين وغيرهم من تشكيلات المجتمع الواحد، وفي السنوات العشر الأخيرة زاد الإقبال على أسواق البورصات للمشاركة في المضاربات المالية عبر شبكة الإنترنت سواء على الصعيد الإقليمي أو الدولي، حيث أن هذه الطريقة تتيح للجميع بيع وشراء الأسهم من منازلهم عن طريق حواسيبهم الشخصية مع وجود نسب منخفضة من العمولات.

وترتكب جرائم الاحتيال المعلوماتي عادةً في سوق الأوراق المالية من قبل بعض المساهمين في الشركات والذين يملكون كمية كبيرة من أسهمها، حيث يقوم المحتالون بنشر معلومات كاذبة عن هذه الأسهم بهدف زيادة الطلب عليها، وهذه الزيادة في الإقبال على شراء هذه الأسهم تعمل على زيادة قيمة هذه الأسهم بشكل كبير ومضاعف وفي وقت قصير، وفي النتيجة يحصل هؤلاء المحتالون على أرباح مالية هائلة، وبالمقابل يتكبد الأفراد الذين اشتروا هذه الأسهم خسارات كبيرة عندما يقومون ببيعها بأسعار زهيدة جداً عما اشتروها، وهذا ما شهدناه في السنوات الخمس الأخيرة في البورصات العالمية ويعتبر ذلك من بين الأسباب التي أدت إلى انهيار الاقتصاد العالمي.

ومن أمثلة ذلك في الولايات المتحدة الأمريكية قامت إحدى شركات الهواتف الخلوية بالإعلان عن طرح أسهم للشركة للبيع بسعر خمسة آلاف دولار للسهم الواحد، وذلك بهدف بناء شبكة هواتف خلوية في منطقة "بوسطن" بُغية التوسع للشركة وجلب الأرباح وفقاً للإعلان، إلا أن المال الذي تم تحصيله من هذه العملية تم تحويله إلى حسابات مالكي الشركة.

(Hillman, R, 1999, p.8)

الفرع الرابع: الاحتيال بأسلوب إنتحال الشخصية:

ويتحقق الاحتيال التقني هنا بأن يقوم المحتال باستخدام بريد إلكتروني غير صحيح وذلك لإغواء المستخدمين، حتى يتصلوا بالمواقع الإلكترونية الاحتيالية، وذلك بهدف خداعهم وجعلهم يفشون بياناتهم الشخصية والمالية مثل أرقام بطاقات الائتمان، وكلمات السر، وأرقام الضمان الاجتماعي وغيرها، وذلك تمهيداً لاستخدامها من قبل المحتالين في تحقيق أغراضهم غير المشروعة في الحصول على المنفعة المالية. (Kunz and Wilson, 2004, P. 15)

ويعتبر هذا النوع من الاحتيال المعلوماتي من أعلى معدلات الإجرام عبر الإنترنت، بحيث يحقق المحتال فيه أغراضه غير المشروعة بالحصول على المكاسب المالية الهائلة عن طريق استخدام وثائق إثبات شخصية للغير، وتحويل حسابات بنكية بأرقام بطاقات الائتمان التي حصل عليها بالطرق الاحتيالية (يونس، 2004، 417)

الفرع الخامس: الاحتيال عن طريق البريد الإلكتروني:

وأبرز هذه الأشكال البريد الإلكتروني النيجيري (Neigeran letter Fraud)، وتتمثل هذه الطريقة في قيام الجاني بإرسال رسالة إلى ا لمجني عليه عبر البريد الإلكتروني يدّعي فيها أنه الوريث والإبن للرئيس النيجيري المتوفي، وانه سيرث ملايين الدولارات الموجودة في حسابات بنكية في جميع أنحاء العالم، ويطلب من المجني عليه إرسال عدة آلاف من الدولارات حتى يدفعها للمحامي من أجل الحصول على الثروة، ويوهم الضحية بأن نصيبه جزء من هذه الثروة، وبعد أن يرسل الأخير النقود المطلوبة يتفاجأ بأنه ضحية جريمة احتيال معلوماتي عبر البريد الإلكتروني (الخن، 2011، 66).

المطلب الثالث: الحماية الجنائية للمعلومات المعالجة آلياً من خطر الإحتيال المعلوماتي وفقاً للمشرع الأردني:

خلصنا مما سبق أنه لا يمكن تطبيق النصوص التقليدية الواردة في قانون العقوبات على الجرائم الواقعة على المعلومات المعالجة آلياً والمخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت ومنها الاحتيال المعلوماتي.

وجريمة الاحتيال بمفهومها التقليدي تتطلب أن تقع الطرق الاحتيالية بين شخصين طبيعيين (الجاني والمجني عليه)، فالادعاء الكاذب يصدر من الجاني في مواجهة المجني عليه، ومعنى ذلك أن الطرق الاحتيالية نطاقها العلاقات الإنسانية وليس جهاز الحاسب الآلي،

ونتيجة لذلك فقد ثار خلاف فقهي حول مسألة الاحتيال بالطرق التقليدية على الحاسوب بوصفه مجرد آلة وليس إنساناً، حيث انقسم الفقه إلى اتجاهين أحدهما مؤيد لوقوع أفعال الاحتيال على الحاسب الآلي على الرغم من أنه آلة، والآخر ذهب إلى عدم صلاحية نظام الحاسوب لوقوع فعل الاحتيال عليه بالطرق التقليدية ولا يمكن اعتباره مجنياً عليه وهذا هو الرأي الراجح في الفقه والذي نذهب معه، لأن تجسيد مبدأ شرعية الجرائم والعقوبات يتطلب ذلك ويؤدي إلى عدم إمكانية تطبيق النصوص الجزائية التقليدية على هذا النوع من الجرائم، وذلك كما بينا سابقاً أنه وفي كل الأحوال لا يمكن أن تكون المعلومات المعالجة آلياً محلاً لجرائم الأموال التقليدية نظراً للطبيعة الخاصة التي تتمتع بها والتي تختلف عن طبيعة محل هذه الجرائم.

لما تقدم فإنه لابد من البحث في القوانين الخاصة الأخرى لبيان فيما إذا وفر المشرع الأردني الحماية الجنائية للمعلومات المعالجة آلياً من خطر الاحتيال المعلوماتي بصوره المتعددة والمتنوعة، والتي تستجد بين الحين والآخر نظراً لارتباطها بالتطور السريع لتكنولوجيا المعلومات، والتي تؤدي إلى ظهور أساليب تقنية جديدة، لذلك فسوف نبحث في قانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001، وقانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010 وذلك كما يلي:

الفرع الأول: الحماية الجنائية للمعلومات المعالجة آلياً من خطر الاحتيال المعلوماتي وفقاً لقانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001:

أشار المشرع الأردني في هذا القانون إلى صورة من صور الاحتيال حيث نصت المادة (35) منه على ما يلي "يعاقب كل من يقوم بإنشاء أو نشر أو تقديم شهادة توثيق لغرض احتيالي، أو لأي غرض غير مشروع، بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل عن (3000) ثلاثة آلاف دينار ولا تزيد على (10000) عشرة آلاف دينار أو بكلتا هاتين العقوبتين".

وقد عرفت المادة (2) من ذات القانون والخاصة بالتعريفات المقصود بشهادة التوثيق بأنها "الشهادة التي تصدر عن جهة مختصة مرخصة أو معتمدة لإثبات نسبة توقيع إلكتروني إلى شخص معين استناداً إلى إجراءات توثيق معتمدة".

ونصـــت المـادة (34) من ذات القـانون على أنـه "تكون شـــهادة التوثيق التي تبين رمز التعريف معتمدة في الحالات التالية:

أ- صادرة عن جهة مرخصة أو معتمدة.

ب- صادرة عن جهة مرخصة من سلطة مختصة في دولة أخرى ومعترف بها.

ج- صادرة عن دائرة حكومية أو مؤسسة أو هيئة مفوضة قانوناً بذلك.

د- صادرة عن جهة وافق أطراف المعاملة على اعتمادها".

كما ونصت المادة 38 من ذات القانون على أنه "يعاقب كل من يرتكب فعلاً يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الإلكترونية، بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بغرامة لا تقل عن (3000) ثلاثة آلاف دينار ولا تزيد على (10000) عشرة آلاف دينار أو بكلتا هاتين العقوبتين، ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون".

ومن خلال مـا تقـدم نجد أن المادة (35) من قانون المعاملات الإلكترونية جرمت الأفعال الاحتيالية التي تتم باسـتخدام شـهادة التوثيق الخاصـة بالتوقيع الإلكتروني، ومع ذلك فقد جاء النص غامضاً بعيداً عن الوضـوح والتفصيل، ولم يراعِ الصور المتعددة والمتنوعة للطرق الاحتيالية المرتكبة عبر النظام المعلوماتي، وكنا نتمنى على المشرـع الأردني أن يسـتوعب في نصـوص هذا القانون كافة الصور التقنية الاحتيالية. والتي تهدد المعلومات ذات الأصول المالية والتي تقدر بمبالغ مالية هائلة.

الفرع الثـاني: الـ حمايـة الجنـائية للمعلومات المعالجة آلياً من خطر الاحتيال المعلوماتي وفقاً لقانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010:

خلصـنا مما سبق أن الاحتيال المعلوماتي يعرف بأنه "التلاعب المقصود بمعلومات وبيانات تمثل قيماً مـاديـة يختزنها النظام المعلوماتي، أو الإدخال غير المصرـــح به لمعلومات وبيانات صـــحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة أو أية وسـيلة أخرى من شـأنها التأثير على الحاسـوب، حتى يقوم بعمليـاته بناءً على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصـــول على ربح غير مشرـــوع وإلحاق ضرر بالغير".

ومعنى ذلك أن الاحتيال المعلوماتي يتحقق عن طريق التلاعب المقصود بكافة صوره في المعلومات والبيانات في مراحل المعالجة الآلية للبيانات في الحاسب الآلي سواء الإدخال أو الإخراج، أو عن طريق التعدي على البرامج التطبيقية أو التشغيلية، والتي تتضمن الأوامر والتعليمات التي تحكم عملية البرمجة، أو التعدي على المعلومات المتدفقة عبر شبكة الإنترنت من أجل تحقيق أغراض غير مشروعة للجاني وهي الحصول على الكسب المادي وإلحاق الضرر بالمجني عليه.

وبتطبيق ذلك على النصوص الواردة في قانون جرائم أنظمة المعلومات الأردني المؤقت نجد أن المشرع الأردني قد استوعب بعض صور الاحتيال المعلوماتي سالفة الذكر، إلا أنه لم يحط بكافة صور هذه الجريمة الخطيرة والتي تؤدي إلى خسارات فادحة تلحق بالمجني عليهم.

حيث نجد المادة 6/ب من ذات القانون نصت على أنه "ب- كل من استخدم عن طريق الشبكة المعلوماتية أو أي نظام معلومات قصداً دون سبب مشروع بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية للحصول لنفسه أو لغيره على بيانات أو معلومات أو أموال أو خدمات تخص الآخرين، يعاقب بالحبس مده لا تقل عن سنة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد عن (5000) خمسة آلاف دينار".

وبتحليل هذا النص نجد أن المشرع الأردني قد جرم الأفعال التالية:

1- الاستخدام المقصود وغير المشروع لبيانات أو معلومات تتعلق ببطاقات الائتمان للحصول على منفعة مالية.
2- الاستخدام المقصود وغير المشروع لبيانات أو معلومات تستخدم في تنفيذ المعاملات المالية للحصول على منفعة مالية.
3- الاستخدام المقصود وغير المشروع لبيانات أو معلومات تستخدم في تنفيذ المعاملات المصرفية للحصول على منفعة مالية.

ويبدو أن إرادة المشرع هنا قد اتجهت في الحالة الأولى إلى صورة الاحتيال المعلوماتي التي تتحقق عن طريق استخدام الجاني بطرق احتيالية لبطاقة الائتمان الخاصة بالمجني عليه للحصول على منفعة مالية، وفي الثانية والثالثة إلى صورة الاحتيال عن طريق التلاعب في البيانات والمعلومات في مرحلتي الإدخال والإخراج والتي تتحقق عن طريق قيام الجاني بتحويل الحسابات الخاصة بالمجني عليه والمقيدة في مصرف معين للحصول لنفسه على منفعة مالية.

فمن الناحية النظرية نجد أن المشرع الأردني قد أورد وبشكل غير صريح حالتين من الاحتيال المعلوماتي التي سبق وبيناها خلال دراستنا لصور الاحتيال المعلوماتي والتي أوردها الفقه الجنائي، إلا أن هناك صوراً كثيرة لهذه الجريمة والتي تتم بوسائل وأساليب مختلفة ومتنوعة لم يذكرها المشرع الأردني والتي منها الاحتيال التجاري بعدم تسليم البضائع بعد الدفع، والاحتيال بانتحال شخصية المجني عليه، والاحتيال المتعلق بالأوراق المالية والأسهم، والاحتيال عن طريق البريد الإلكتروني وغيرها من صور هذه الجريمة التقنية.

أما من حيث المضمون فإن المشرع لم ينص على جريمة الاحتيال المعلوماتي بشكل مباشر وصريح تماشياً مع مبدأ شرعية الجرائم والعقوبات، وكل ما هنالك أنه جرم الأفعال الواردة في نص المادة 6/ب من ذات القانون وهي الاستخدام القصدي وغير المشروع للمعلومات المتعلقة ببطاقات الائتمان، والاستخدام القصدي وغير المشروع للمعلومات المتعلقة بالمعاملات المالية والمصرفية الإلكترونية، وهذا الواقع الذي نصطدم به دائماً، ذلك لأنه وتماشياً مع مبدأ شرعية الجريمة والعقوبة فإننا لا نستطيع القول بأن المشرع الأردني قد نص على جريمة الاحتيال المعلوماتي، وكان من المستحسن أن يكون النص الجزائي أكثر وضوحاً وتفصيلاً لصور هذه الجرائم المعلوماتية، فجاء القانون المؤقت خالياً من أي نص يتعلق بجريمة الاحتيال المعلوماتي حيث إن المشرع عودنا على التعبيرات الدالة والقاطعة التي لا تترك مجالاً للشك ولا الاجتهاد، فعلى سبيل المثال نص المشرع في المادة 399 الفقرة الأولى من قانون العقوبات الأردني على أن "السرقة هي أخذ مال الغير المنقول دون رضاه"، ونص في الفقرة الثانية من ذات المادة على أنه "وتعني عبارة (أخذ المال) إزالة تصرف المالك فيه برفعه من مكانه ونقله...إلخ، ونص في الفقرة الثالثة من ذات المادة على أنه "وتشمل لفظة (مال) القوى المحرزة"..... وهكذا، فالنص الجزائي يأتي دائماً واضحاً ومفصلاً ويستوجب الالتزام به من قبل الجميع، فلا اجتهاد في موضع النص.

ومما تقدم يرى الباحث أن المشرع الأردني وفقاً لقانون جرائم أنظمة المعلومات الأردني المؤقت لم يحط المعلومات المعالجة آلياً ذات الأصول المالية بالحماية الجنائية من خطر الاحتيال المعلوماتي.

المطلب الرابع: الحماية الجنائية للمعلومات المعالجة آلياً من خطر الاحتيال المعلوماتي وفقاً للمشرع الأمريكي:

واجه المشرـع الأمريكي جرائم الاحتيال المعلوماتي عن طريق القوانين الخاصـة بالاحتيال والغش في مجـال البنوك والبريـد والتلغراف والاتصـــالات الهـاتفيـة، والاتفاق الجنائي لأغراض ارتكاب الاحتيال والغش المعلوماتي، حيث طبقت هذه القوانين على صـــور الاحتيال المعلوماتي التي تقع على المعلومات المعالجة آلياً في النظام المعلوماتي (حجازي، 2006، 484).

وفي عام 1978 صـــدر أول قانون في الولايات المتحدة الأمريكية وتحديداً في "ولاية فلوريدا" والذي يتعلق بالاحتيال المعلوماتي والاعتداء على الحاسب الآلي، حيث اعتبر هذا القانون مجرد الدخول غير المشروع للنظـام المعلوماتي والحاســـب الآلي بمثابة جريمة، بصرـــف النظر ســـواء توافرت لدى الفاعل النية الجرمية للاحتيال أم لم تتوافر (Casey, 2004, P.1).

وقد صـدرت عدة قوانين أمريكية أعطت مفهوماً واسـعاً للمال بحيث يشمل "كل شيء ينطوي على قيمه"، وأصـبح المال وفقاً لهذا المفهوم الواسع يشمل الأموال المعنوية والمعلومات المعالجة آلياً، وبمعنى آخر يشمل الأموال الكتابية أو البنكية، وعاقبت هذه القوانين على الاستخدام غير المصرح به للحاسب الآلي وذلك بغرض ارتكاب أفعال الغش، أو الاستيلاء على المال (الشوا، 1994، 128).

وقـد اهتم المشرـــع الأمريكي بجريمـة الاحتيال المعلوماتي ونجد ذلك واضـــحاً في اتجاه التشرـــيع الفيدرالي حيث طبق المشرـع في هذا المجال التشرـيعات الخاصة بالبريد والاتصالات الهاتفية والبنوك، وذلك في الفصـــل (63) من البنـد (1341) والمتعلق بحـالات الغش والخـداع والتحـايـل وذلـك تحـت عنوان 18 U.S.C.$ 1314 US code-section 1341:Fraud and swindles [20]،

---

[20] 18 U.S.C.$ 1343 fraud and swindles
Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute,supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial

وطبق أيضاً قوانين الاحتيال عبر الأسلاك أو الراديو أو التلفزيون والواردة في البند (1343) وذلك تحت العنوان 18 U.S.C. $ 1343:us code-section 1343: fraud by wire,radio, or television [21]، ونصت القوانين الفيدرالية أيضاً على جريمة إساءة استخدام بطاقة الائتمان أو أية مستندات أو صكوك بنية الاحتيال، وذلك من خلال بيع أو نقل أو استخدام بطاقة ائتمان مسروقة أو مفقودة أو مزورة أو مستبدلة أو تم الحصول عليها بطريقة الاحتيال.

(Icove and Vonstorch, 1995, P. 216)

وفي عام 1984 صـدر قانون جرائم الحاسـب الآلي الفيدرالي، وذلك بعد أن قامت لجنة الكونجرس القانونية بوضع مشروع هذا القانون، وأطلق عليه بعد أن صدر قانون الاحتيال وسوء استخدام الحاسب الآلي (CFAA) وهو اختصار لـ (Computer Fraud And Abuse Act) .

وتم تعديل هذا القانون عدة مرات ، حيث جرمت المادة (4/A/1030) وفقا لأخر تعديل فعل الدخول المتعمد وغير المصرّح به أو المتجاوز التصريح إلى الحاسب الآلي المشمول بالحماية بهدف الحصول على شيء ذي قيمة عن طريق الاحتيال [22].

وعليه فإن جريمة الاحتيال المعلوماتي تتحقق وفقاً لهذا النص عن طريق قيام الجاني بالولوج العمدي إلى الحاسب الآلي دون أن يكون مصرحاً له بذلك أو أن يكون متجاوزاً للتصريح الممنوح له، كما لو دخل العامل في الشركة إلى موقع ومعلومات متجاوزاً بذلك التصريح الممنوح له

---

institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

[21] 18 U.S.C. $ 1343 fraud by wire, radio, or television
Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both

[22]Article 1030/A/4 CFAA of 1994
(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by *means of such conduct* furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

و فقاً لعمله ووظيفته، وذلك بهدف الحصـــول على منفعة مادية أو شيء ذي قيمة عن طريق الأساليب والوسائل الاحتيالية التي أوردناها في مطلب سابق.

وفي عام 2005 صـــدر قانون فيدرالي وهو قانون مكافحة اصـــطياد الضـــحايا عبر البريد الإلكتروني والصـــادر في 28 فبراير 2005 حيث جرم هذا القانون كافة الأفعال المنطوية على طرق احتيالية عن طريق استخدام البريد الإلكتروني لارتكاب الجرائم المعلوماتية (إبراهيم، 2009، 292).

وتجدر الإشـــارة هنا أن معظم التشـــريعات الجزائية الفيدرالية قد اســـتوعبت الأفعال التي تطال الحواســـيب الآلية عن طريق التعدي عليها والتلاعب بها بهدف القيام بأعمال احتيالية، ونذكر منها على سبيل المثال قانون البيانات الخاطئة القسم (1001) من الباب (18)(Doyle, 2008, p. 61) ، وقانون التآمر لارتكاب الاحتيال على الولايات المتحدة الأمريكية في القســـم (371) من الباب (18) وذلك تحت عنوان 18U.S.C.$ 371;Conspiracy to commit offence or to defraud United States حيث نصت هذه الماده على أنه "إذا تآمر شخصان فأكثر لارتكاب جريمه ضد الولايات المتحده أو الاحتيال عليها بأي شكل من الأشكال ولأي غرض كان يعاقب كل من الفاعلين بغرامة أو الحبس مده لا تزيد على خمس سنوات أو بكلتا العقوبتين[23] "

أما بالنســـبة لتشـــريعات الولايات فقد اســـتحدثت الولايات الأمريكية مثل "أريزونا، وكاليفورنيا، وكولورادو، وديلادار، وفلوريدا، وجورجيا، والينوي، وميتشجان، وميسوري، ومونتانا، وأوتاو، ونيومكسيكو ... وغيرها" العديد من القوانين الجنائية التي تعاقب على الاستخدام غير المصرح به للحاسب الآلي وذلك بغرض الاحتيال أو الحصول على مال (الشوا، 1994، 128).

---

[23] 18 U.S.C.$ 371 Conspiracy to commit offense or to defraud United States.
If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.
If, however, the offense, the commission of which is the object of the conspiracy, is a misdemeanor only, the punishment for such conspiracy shall not exceed the maximum punishment provided for such misdemeanor.

وفي تشريع ولاية وست فرجينيا تدخل المشرع في الفصل (61) الخاص بقانون جرائم الحاسب الآلي وإساءة استخدامه في البند (3) الفقرة (ج) وجرم أفعال الدخول المتعمد أو التسبب في الدخول إلى الحاسب الآلي أو النظام المعلوماتي سواء أكان بصورة مباشرة أم غير مباشرة، وذلك بهدف تنفيذ أي مخطط للاحتيال أو الحصول على أموال أو ممتلكات أو خدمات عن طريق وسائل وأساليب احتيالية أو بالمزاعم والوعود الكاذبة على ارتكاب هذه الجناية.

كما وتدخل المشرع في ولاية رود أيلاند في الفصل (52) الخاص "بالانتهاكات الجنائية" في البند (1) بتجريم الدخول المتعمد إلى الحاسب الآلي والنظام المعلوماتي لتنفيذ مخطط بهدف الاحتيال، أو الحصول على أموال أو ممتلكات أو خدمات بوسائل وأساليب احتيالية، أو تحطيم أو استبدال أو إلغاء أو تخريب أو مسح أي برنامج أو معلومات أو بيانات داخل جهاز الحاسب الآلي عن طريق الأساليب الإحتيالية. (سليمان، لات، 35).

المطلب الخامس: الحماية الجنائية للمعلومات المعالجة آلياً من خطر الاحتيال المعلوماتي وفقاً للمشرع الفرنسي:

عالج المشرع الفرنسي- جريمة الاحتيال المعلوماتي في الفصل الثالث من قانون العقوبات الفرنسي- الجديد لعام 1994 والخاص بجرائم المعالجة الآلية للبيانات، وذلك في المواد 323-1، 323-7، 323-6.

حيث نصت المادة 323-1 من ذات القانون على "تجريم أفعال الوصول أو البقاء ضمن أي جزء من أجزاء نظام المعالجة الآلية للبيانات أو النظام المعلوماتي، وذلك عن طريق الاحتيال على النظام، حيث يعاقب مرتكب هذا الفعل بالحبس مدة سنتين وغرامة مقدارها 30000 يورو، وتشدد العقوبة لتصل إلى ثلاث سنوات والغرامة 45000 يو رو إذا أدى هذا السلوك إلى إتلاف أو تعديل البيانات المعالجة آلياً، أو إلى تغيير في عمل هذا النظام [24] ".

---

[24] Article 323/1 Of (FCP)

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

ونصـت المادة 323-7 من ذات القانون على أن الشرـوع في ارتكاب الجنح المنصوص عليها في المادة 323-1 الى 323-3-1 يخضع لنفس العقوبات [25] ".

كما وأن المشرـع الفرنسي- في المادة 323-6 من ذات القانون بين مسـؤولية الأشـخاص المعنوية عن هذه الجرائم حيث نصت هذه المادة على أنه:

" يتحمل الأشــخاص المعنوية المســؤولية الجنائية عن الجرائم المشــار اليها في هذا الفصــل وفقا للشروط المنصوص عليها في المادة 121-2 ، وتطبق عليهم العقوبات التالية:

1- الغرامات المالية وفقاً للشروط المنصوص عليها بموجب المادة 131-38 من ذات القانون،

2-العقوبات المنصـوص عليها في المادة 131-39 ، إضـافة الى الحظر المشـار إليه في الفقرة 2 من ذات المادة [26] "

مما تقدم يرى الباحث أن المشرـعين الأمريكي والفرنسي- قد أحاطا المعلومات المعالجة آلياً بالحماية الجنائية من خطر الاحتيال المعلوماتي حيث واجه المشرـع الأمريكي ذلك باسـتعراض العديد من الصور التي يمكن أن ترتكـب بهـا حـالات الاحتيـال المعلومـاتي، ويلاحظ أن المشرــع الفيدرالي الأمريكي كان يعالج هذه الجريمة سـابقاً عن طريق القوانين الخاصـة بالاحتيال والغش في مجال البنوك والبريد والهواتف والاتصـالات الهاتفية، وبقي الوضع هكذا لغاية صدور التعديل الوارد في القانون الوطني الأمريكي ،

---

[25] Article 323/7 Of (FCP)

La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines.

[26] Article 323/6 Of (FCP)

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38 ;

2° Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise

حيث استوعب هذا القانون وفقاً لهذا التعديل جريمة الاحتيال المعلوماتي بصورة مباشرة ونص عليها صراحةً في المادة (4/A/1030)، وقد جاء التشريع القانوني للولايات المختلفة ليكمل النقص الحاصل في التشريع الفيدرالي ، حيث نجد معظم الولايات كما أسلفنا قد نصت صراحةً على جريمة الاحتيال المعلوماتي التي قد تقع على المعلومات المخزنة في الحاسب الآلي أو المتداولة عبر الشبكة المعلوماتية، أما المشرع الفرنسي فقد نص على هذه الجريمة صراحةً من خلال قانون العقوبات الفرنسي الجديد.

وهذا على خلاف المشرــع الأردني الذي لم ينص في قوانينه صراحةً على هذه الجريمة الخطيرة، الأمر الذي يستوجب تدخل المشرع هنا وأن يحذو حذو المشرعين الغربيين في إضافة عبارة أو "أي شيء ذي قيمة" حتى يوسـع من معنى المال في النصوص التقليدية، بحيث يندرج تحت تعريفه الأموال المعنوية والمعلومات والبيانات المعالجة آلياً، وأن لا يشــترط أن يكون المال منقولاً، أو أن يتدخل بنص عقابي خاص يُطبق في حالة ارتكاب جرائم الاحتيال في مجال المعلوماتية، بحيث يبين وسـائل وأسـاليب وصـور وأركان وعناصر مثل هذه الجرائم في هذه القوانين.

الفصل الرابع-

الحماية الجنائية للمعلومات من الجرائم التقنية المستحدثة في إطار المعالجة الآلية للبيانات:

إن ارتكاب الجرائم المعلوماتية يتطلب ابتداءَ التعامل مع الحاســـب الآلي ونظامه لاعتبارها مرحلة ضروريـة للنشـــاط الرقمي الإجرامي ولارتكـاب أيـة جريمـة من هـذا النوع، وقـد جـاءت جرائم تكنولوجيا المعلومات تقرع أجراس الخطر لتنبه العالم إلى حجم المخاطر والخســائر التي يمكن أن تنجم عنها، لأنها من الجرائم التي تعتمد على ذكاء مرتكبها وخبراته الفائقة في اســتخدام النظام المعلوماتي، وهي تحدث في بيئة إلكترونية رقمية، الأمر الذي يؤدي إلى خسـائر فادحة في المجالات الاجتماعية والاقتصادية والأمنية والثقافية، وهذه الجرائم المســتحدثة تختلف بأركانها وعناصرها وأســاليبها ومجرميها عما ســبقها من جرائم تقليدية، والتي تناولنا بعضـها تفصـيلاً في الفصـل الثالث من هذه الأطروحة، وبينا صورها وأساليبها والوسائل التقنية لارتكابها، وقصـــور التشـــريعات المقارنة من حماية المعلومات الإلكترونية في إطار نصـــوص جرائم الأموال التقليدية، أما في هذا الفصل فإننا سوف نتناول البحث في مدى الحماية الجنائية للمعلومات الإلكترونية من الجرائم المســـتحدثة في إطار المعالجة الآلية للبيانات، والتي يمكن تقســـيمها إلى جرائم المســـاس بســـرية المعلومات والبيانات، ومنها جريمة الدخول والبقاء غير المصـرح به (غير المشـروع) في نظام المعالجة الآلية للبيانات، وجريمة الاعتراض غير القانوني لانتقال المعلومات، وجرائم المســـاس بســـلامة المعلومات والبيانات المعالجة آلياً، والتي منها جريمة التزوير المعلوماتي، وجرائم المساس بالمصـالح القومية والسـلامة الشـخصـية للأفراد (انتهاك الخصـوصـية)، ومنها جريمة التجسـس المعلوماتي وجريمة الاعتداء على الحياة الخاصة للأفراد (انتهاك الخصـوصـية) ، وأخيراً فإننا سـوف نفرد في نهاية هذا الفصـل مبحثاً خاصـاً بالإشتراك الجرمي وتحليل العقوبات الواردة في قانون جرائم أنظمة المعلومات الأردني المؤقت سواء أكانت أصلية أم إضافية ومسؤولية الأشخاص المعنوية في الجرائم الم علوماتية وفقاً لذات القانون والأحكام العامة.

لما تقدم فإننا سوف نقوم بتقسيم هذا الفصل إلى المباحث التالية:

أولا: الجرائم الماسة بسرية المعلومات والبيانات المعالجة آلياً.

ثانيا: الجرائم الماسة بسلامة المعلومات والبيانات المعالجة آلياً.

ثالثا: الجرائم الماسة بالمصالح القومية والسلامة الشخصية للأفراد (الخصوصية).

رابعا: الاشتراك الجرمي والعقوبات ومسؤولية الأشخاص المعنوية في الجرائم المعلوماتية.

المبحث الأول: الجرائم الماسة بسرية المعلومات والبيانات المعالجة آليا:

تعتبر جرائم الحاسوب والإنترنت من الظواهر الإجرامية التي قرعت أجراس الخطر لتنبه المجتمعات إلى حجم المخاطر والخسائر الناجمة عنها، وخاصةً إذا تعلق الأمر بنظام المعالجة الآلية للبيانات والمعلومات وسريتها الأمر الذي يؤدي إلى خسائر مادية كبيرة على المستوى الاقتصادي والاجتماعي والثقافي والأمني وغيرها، ومن هنا تظهر أهمية مشكلة الجرائم المعلوماتية في مجال المعاملات الإلكترونية، وإذا كانت أشكال الجرائم الماسة بسرية المعلومات والبيانات متعددة ومتنوعة إلا أننا سوف نتناول دراسة هذا المبحث وفقاً للمطالب التالية:

1- جريمة الدخول والبقاء غير المصرح به في نظام المعالجة الآلية للبيانات.

2- جريمة الاعتراض غير القانوني لانتقال المعلومات والبيانات.

المطلب الأول: جريمة الدخول والبقاء غير المصرح به في نظام المعالجة الآلية للبيانات:

قد تتعرض الكثير من الأنظمة المعلوماتية إلى الاختراق من قبل أشخاص غير مصرح لهم بالدخول إليها، وعادة ما يطلق عليهم المخترقين، وقد تختلف الغاية من وراء هذه الاختراقات، فقد يكون الهدف المباشر هو المعلومات المخزنة في الحاسب الآلي أو المتبادلة عبر الشبكة المعلوماتية بتغييرها أو شطبها أو سرقتها أو غير ذلك، وقد يكون الهدف هو جهاز الحاسب الآلي نفسه بصرف النظر إن كانت المعلومات والبيانات هي المستهدفة، أم لإثبات قدرة المخترق العالية في تحدي النظام المعلوماتي، وما يهمنا هنا هو حالة الدخول غير المصرح به إلى النظام المعلوماتي بهدف الوصول إلى المعلومات التي يحتويها هذا النظام، لذلك فإن التعرض إلى جريمة الدخول والبقاء غير المصرح به للنظام المعلوماتي يتطلب منا البحث في مفهوم وماهية جريمة الدخول غير المصرح به وصورها وبيان أركانها، وموقف المشرع الأردني والأمريكي من هذه الجريمة وذلك كما يلي:

الفرع الأول: ماهية الدخول والبقاء غير المصرح به للنظام المعلوماتي:

نصت اتفاقية بودابست لسنة 2001 على هذه الجريمة في المادة الثانية منها، حيث أشارت أنه على جميع الدول الأطراف أن تضمن قوانينها الداخلية النص على جريمة الدخول والبقاء غير المصرح به إلى النظام المعلوماتي، وأن تعتبرها جريمة جنائية، وأن تتخذ أية إجراءات ضرورية لمكافحة مثل هذه الجريمة (زين الدين، 2008، 205).

كما ونص القانون العربي النموذجي الاسترشادي بشأن مكافحة جرائم الكمبيوتر والإنترنت والذي تم إقراره من قبل جامعة الدول العربية بناء على مشروع القانون المقدم من وزراء الداخلية ووزراء العدل العرب، حيث نصت المادة الثانية من هذا القانون بفقرتيها الأولى والثانية على هذه الجريمة بصورتيها البسيطة والمشددة (حجازي، 2006، 353).

ويقصد بجريمة الدخول أو البقاء أية صورة تؤدي إلى اختراق نظام الحاسب الآلي والوصول إلى المعلومات والبيانات والبرامج المخزنة داخلة، أو البقاء بصورة غير مشروعة وغير مسموح بها (عبابنة، 2005، 86) ، ويقصد بها أيضاً توجيه الهجمات إلى الحاسب الآلي بقصد المساس بسرية وسلامة المعلومات المعالجة آليا، أو تعطيل قدرة وكفاءة النظام المعلوماتي لعدم القيام بوظائفه وأعماله (إبراهيم، 2009، 242).

ويطلق عليها بعض الفقه الجرائم التي تضر بحماية المواقع الإلكترونية سواء نجم عن هذا الدخول غير المشروع تلاعب في البيانات والمعلومات أم لا، فمجرد الدخول غير المشروع يعتبر ذلك مضراً بالمواقع الإلكترونية (أبو زيد، 2010، 12).

ويتحقق فعل الدخول غير المصرح به عن طريق وصول الجاني للمعلومات والبيانات المخزنة في الحاسب الآلي دون رضاء صاحبها أو الشخص المسؤول عن النظام المعلوماتي وهذه المعلومات، وذلك عن طريق إساءة استخدام الحاسب الآلي من قبل الجاني، والوصول للمعلومات والبيانات المخزنة داخله (إبراهيم، 2010، 84).

ويرى الباحث أن الدخول والبقاء غير المصرح به قد يكون جريمة قائمة بحد ذاتها دون انتظار أفعال لاحقة لهذا الفعل، وقد يكون مرحلة سابقة لارتكاب الجاني لجرائم معلوماتية أخرى كسرقة المعلومات وتزويرها، والاحتيال المعلوماتي والإتلاف المعلوماتي، والتجسس المعلوماتي وغيرها، حيث إن معظم هذه الجرائم تتطلب من الجاني الدخول والبقاء في النظام المعلوماتي تمهيداً لارتكابه الجريمة المعلوماتية الهدف.

ولـذلك فقد انقســم الفقه إلى اتجاهين حول مدى اعتبار فعل الدخول والبقاء جريمة من الجرائم المعلوماتية، وهل يســتوجب الحماية الجنائية أم لا، والاتجاه الأول يرى أنه لا ضرورة لتجريم مجرد الدخول أو البقاء غير المشروع به في النظام المعلوماتي إذا لم تتجه نية الجاني لارتكاب جريمة لاحقة على هذا الدخول أو البقاء، وحجتهم في ذلك أن هذه الأفعال لا تشــكل بحد ذاتها جريمة ولا تســتوجب العقاب، لأن الفاعل هدفه منها عرض قدراته التقنية والفنية والذهنية للتغلب على النظام، وأما الاتجاه الثاني وهو ما يذهب معه الباحث فيرى ضرورة تجريم هذه الأفعال حتى لو لم تكن بقصـد ارتكاب جرائم معلوماتية لاحقة، لأن هـذه الأفعـال قـد تترتـب عليها خســائر مادية فادحة، وبالتالي فهي جرائم معلوماتية تســتوجب العقاب (المومني، 2008، 156 وما بعدها).

وقد ذهب الفقه الفرنسيــ أن فعل الدخول له مدلول مادي ومدلول معنوي، فأما المدلول المعنوي فهو يشبه الدخول إلى ذاكرة الإنسان، وأما المدلول المادي فهو يتمثل في أن الشخص قد حاول الدخول أو أنه دخل بالفعل إلى النظام المعلوماتي، ولم يحدد الفقه الفرنسيـ وسـائل الدخول إلى النظام أو اختراقه (حجازي، 2006، 355).

وتتحقق جريمة الدخول بأية وسـيلة تقنية متى كان ذلك دون رضــاء صــاحب العلاقة، فقد يكون ذلك عن طريق كلمة السر (Pass Word) الخاصة بالمجنى عليه متى كان الجاني غير مخول باستخدامها، أو عن طريق اســتخـدام برنامج اختراق أو حل شــيفرة معينة للنظام، ويمكن أن يتم ذلك الدخول من خلال اسـتخدام رقم الكود الخاص بشـخص آخر أو الدخول من خلال شخص مسموح له بالدخول إلى النظام سواء أكان ذلك عن طريق شبكات الاتصال الهاتفية أم لطرفيات محلية أو عالمية (القهوجي، 2000، 50).

ويعني ذلك أن جريمة الدخول والبقاء قد تأخذ شــكل حل الشــيفرة المتعلقة بالمعلومات والبرامج والبيانات أو النظام ككل، وذلك عن طريق استخدام الجاني لكلمة المرور أو الرقم السري أو الكودات السرية التي توصل إليها عن طريق السرقة أو الاحتيال على من يمتلكها، أو عن طريق برامج قرصنة معدة لذلك، أو حتى عن طريق التجربة لعدة أرقام أو كلمات أو حروف أو رموز أو شـيفرات مركبة من هذه الأشـياء بغية التوصل في النهاية إلى الوسيلة التي يستطيع الجاني كسر نظام الحماية للنظام والدخول.

وقد يتم الدخول غير المصرـــح به كذلك عن طريق قيام الجاني باختراق القيود التي تحدد الدخول إلى النظام والموضـوعة مسبقاً من قبل صاحب العلاقة، كأن يقوم الجاني بالدخول إلى مواقع يتطلب الدخول إليها دفع مبلغ معين من المال دون أن يســدد هذا المبلغ، بحيث يتحايل على النظام المعلوماتي ويدخل إليه بشكل غير مشروع (حجازي، 2006، 356).

ووفقا للمذكرة التفسـيرية لاتفاقية بودابســت فإن فعل الدخول أو الولوج غير القانوني إلى النظام يتحقق متى دخـل الجاني إلى النظام كله أو جزء منه، كالدخول إلى طرفية الحاســب (جزءاً مادياً) أو برامج جزئية، أو معلومات مخزنة في النظام، فالولوج لا يشـمل فقط إرسـال الرسـائل الإلكترونية أو الملفات للنظام المعلوماتي، وإنما يضم الاختراق الموجه إلى نظام معلوماتي متصل بشبكات اتصال عامة، أو إلى نظام معلوماتي متصل بشبكة محلية (شبكة خاصة لشركة) (أحمد، 2003، 71 وما بعدها).

ويتحقق الدخول غير المشرـوع أيضـاً في حال تجاوز الجاني لصـلاحيته في الدخول إلى النظام، ومفاد ذلـك أن يكون الجـاني مخولاً بـالـدخول إلى جزء معين من النظـام دون الأجزاء الأخرى، فيقوم بتجـاوز هذه الصلاحية والدخول إلى جزء غير مسموح له الدخول إليه.

والمثـال على ذلـك لو أن الجـاني دخـل على الموقع الإلكتروني الخـاص بجريدة الرأي الأردنية والمتاح لكافة الجمهور للإطلاع على الأخبار المحلية والعالمية، لكنه تجاوز ذلك بالدخول إلى البيانات الخاصـة بإعداد هذا الموقع وتنظيمه في صـفحة Home Bag، والتي تنطوي على معلومات لا يجوز للجمهور الدخول عليها، فإن فعل الشخص في هذه الحـ الة يعتبر دخولا غير مشروع، رغم أن الموقع في ذاته معداً للكافة إلا أنه تجاوز الدخول المشروع.

وقد يترتب على فعل الدخول خلق عقبات أمام المستخدمين الشرعيين للنظم المعلوماتية والبيانات، وقد يؤدي إلى إتلاف المعلومات وتدميرها وإحداث أضرار مالية هائلة بالمجني عليهم، وقد يترتب عليه أيضـاً الوصـول إلى معلومات وبيانات سرية، أو معلومات عن النظام الهدف وأسرار تسـمح باسـتخدام هذا النظام مجاناً، بل وتشـجع المخترقين والقراصـنة على ارتكاب جرائم أكثر خطورة من الجرائم المتصلة بالحاسب الآلي مثل الغش المعلوماتي، أو التزوير المعلوماتي (أحمد، 2003، 70).

ويرى الباحث أن فعل الدخول غير المصرـح به إلى ا لنظام المعلوماتي هو من أكثر الأفعال انتشاراً في الجرائم المعلوماتية، ويتم الدخول إلى نظام الحاســب الآلي أو شــبكة المعلومات من خلال اســتخدام الجاني لوسائل تقنيه كوسيلة الاتصال عن بعد كالمودم (Modem)

أو عبر نقاط الاتصال والموجهات الموجودة على الشبكة من أجل الدخول إلى نظام الحاسب الآلي بغرض التوصل إلى البيانات والمعلومات والبرامج المخزنة فيه، وهذا الدخول يتطلب دائماً تخطي إجراءات الحماية التقنية الخاصة بالنظام، كتجاوز الرقم السري للمجني عليه، وإجراءات وقيود التعريف الموجودة في بعض المواقع، أو التوصل إلى نقطة ضعف في النظام للدخول من خلالها.

ويلاحظ الباحث أنه إذا كان فعل الدخول غير المصرح به إلى ا لنظام المعلوماتي مجرماً وفقاً لاتفاقية بودابست 2001 وغالبية القوانين الوطنية، فإن الجاني قد لا يكتفي بمجرد الدخول إلى النظام المعلوماتي، بل قد يتعدى هذا الفعل ويرتكب جرائم معلوماتية أخرى أشد خطورة من فعل الدخول، الأمر الذي يتطلب من المشرعين الوطنين إحاطة ذلك بعين الاعتبار.

ونجد ذلك واضحاً في المادة الخامسة من اتفاقية بودابست لعام 2001، والتي تحتم على الدول الأطراف إجراء التعديلات واتخاذ الإجراءات التشريعية اللازمة في قوانينها الوطنية حتى تستوعب الأفعال المجرمة وفقاً لهذه الاتفاقية، والمؤدية إلى إعاقة النظام المعلوماتي والحاسب الآلي عن أداء وظيفته، ومن هذه الأفعال محو أو تدمير أو إدخال أو نقل أو إتلاف البيانات المعلوماتية[27].

ويشترط الفقه لقيام هذه الجريمة ابتداءَ ضرورة وجود نظام معالجة آلية للبيانات (النظام المعلوماتي) مشمولاً بنظام الحماية، وأن يكون الدخول أو البقاء في هذا النظام دون وجه حق، فلا عقاب في حالة الولوج المصرح به من مالك النظام، أو مالك جزء منه، أو صاحب الحق فيه، كما وأنه لا تجريم في حالة ما إذا كان الولوج إلى النظام مجاناً، ومتاحاً للجمهور كبعض المواقع المنتشرة على شبكة الإنترنت والتي تكون متاحة للكافة، فلا يعتبر الدخول إليها دخولاً غير محق إلا إذا تجاوز الشخص هذا الدخول المشروع (زين الدين، 2008، 262 وما بعدها).

---

[27] نص المادة الخامسة من اتفاقية بودابست لسنة 2001.

Each party shall adopt such legislative and other measures as may by necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting transmitting, damaging deleting. Deteriorating or suppressing computer data.

وتجدر الإشارة هنا أن فعل الدخول غير المشروع يعرف بدلالة المكان بأنه "التسلل إلى داخل النظام المعلوماتي"، أما من حيث الزمان فيتمثل في تجاوز حدود التصـريح أو الترخيص داخل النظام والممنوح لفترة زمنية محددة، وذلك عن طريق تجاوز هذه الفترة الزمنية (تمام، 2000، 52).

ويختلف فعل الدخول غير المشـروع إلى النظام المعلوماتي عن فعل البقاء داخل هذا النظام، والذي عرفه البعض بأنه "التواجد داخل نظام المعالجة الآلية للبيانات ضد إرادة من له الحق في السيطرة على هذا النظام" (إبراهيم، 2009، 243).

وفعـل البقـاء غير المشـروع داخـل النظـام المعلوماتي قد يكون ناجماً عن دخول الجاني إلى النظام المعلوماتي بمحض الصـدفة دون قصـد من ناحية، ومع ذلك يبقى داخل النظام وتتصرف إرادته إلى ذلك، وفي هذه الحالة يكون البقاء مجرماً لانصراف إرادة الجاني إلى إتيان هذا الفعل وهو البقاء في النظام مع علمه أن دخوله غير مشـروع، ومثال ذلك أن يكون مسموح للجاني الدخول إلى جزء معين من النظام، ثم يتجاوز هذا الجزء ويدخل إلى أجزاء أخرى بمحض الصدفة ويبقى فيها.

لـذلك فقد اعتبر بعض الفقه أن هذه الجريمة تقوم بسـلوك إجرامي سـلبي، فعلى الرغم من أن دخول الجاني كان بمحض الصـدفة ورغم علمه أن ذلك غير مشـروع، إلا أنه امتنع عن الخروج من النظام وبقي فيه، لذلك فالنشاط الإجرامي في هذه الصورة يُمثل سلوكاً سلبياً من الجاني (حجاري، 2006، 360).

ويتحقق فعـل البقاء غير المشـروع أيضـاً بأن يبقى الجاني داخل النظام المعلوماتي أكثر من المدة المحددة له للبقاء فيه، أو أن يقوم بنسـخ المعلومات الموجودة في النظام في الوقت الذي كان مسـموحاً له رؤية هذه المعلومات والإطلاع عليها فقط (القهوجي، 2000، 52).

ومن نـاحيـة أخرى قـد يكون فعل البقاء غير المشـروع ناجماً عن دخول غير مشـروع إلى النظام المعلوماتي، ويحدث ذلك عندما يقوم الجاني باختراق ودخول النظام المعلوماتي باسـتخدام الوسـائل التقنية دون وجه حق، ورغماً عن إرادة الشخص المسيطر على النظام ويستمر في جريمته ويبقى في هذا النظام بعد الدخول.

الفرع الثاني: أركان جريمة الدخول والبقاء غير المصرح به للنظام المعلوماتي:

تتطلب جريمة الدخول والبقاء غير المشروع في النظام المعلوماتي إلى توافر ركنين أحدهما مادي والآخر معنوي، وسوف نتناولهما على النحو الآتي:

أولاً- الركن المادي:

يتمثل الركن المادي في هذه الجريمة بإتيان الجاني نشاطاً رقمياً يعبر فيه عن إرادته في اختراق نظم الحماية الأمنية الخاصة بالنظام المعلوماتي التي يضعها صاحب العلاقة من أجل حماية نظامه المعلوماتي من محاولات الاختراق والعبث في المعلومات والبيانات، أو تعديلها أو إتلافها أو الإطلاع عليها أو إفشائها أو سرقتها أو نسخها، وكذلك يتمثل الركن المادي أيضاً في النشاط الرقمي الذي يعبر به الجاني عن إرادته في البقاء داخل النظام المعلوماتي دون وجه حق لتحقيق أغراضه الإجرامية، والمقصود هنا بالدخول ليس الدخول المادي المألوف في النصوص التقليدية، وإنما استخدام الجاني للطرق التقنية عن طريق الحاسب الآلي ونظم الاتصال وفقا لتكنولوجيا المعلومات والاتصال للولوج إلى النظام المعلوماتي.

ويشترط هنا لتحقق الركن المادي أن يكون الدخول من قبل شخص آخر غير مالك النظام المعلوماتي أو مستخدمه ودون رضاه، وهذا أمر بديهي فإذا تم الدخول من قبل صاحب النظام أو مستخدمه أو كان بناء على رضاه، فإن الركن المادي لهذه الجريمة لا يتحقق، كما وأنه يشترط في الدخول أن يكون غير مشروع أي بدون وجه حق، فإذا كان للجاني الحق في الدخول إلى نظام المعالجة الآلية للبيانات كما لو كان متاحاً للجمهور مثل بعض المواقع المنتشرة على شبكة الإنترنت كمواقع الأخبار، والشركات التسويقية أو غيرها، فإن الدخول هنا يعتبر مشروعاً ولا يشكل جريمة، وفي كل الأحوال فإن الركن المادي يجب أن يرد على نظام معلوماتي بمكوناته المتعددة والمتكاملة مع بعضها بعضا لهدف واحد وهو معالجة البيانات آلياً (زين الدين، 2008، 272 وما بعدها).

وبالنسبة لفعل البقاء فإن الباحث يرى أن الركن المادي قد يتخذ صورة السلوك الإجرامي السلبي أو الإيجابي، ويكون السلوك سلبياً عندما يكون دخول الجاني إلى النظام المعلوماتي صدفة، ودون قصد، ومع ذلك يبقى داخل النظام وتنصرف إرادته إلى البقاء داخله، مع علمه أن بقاءه هذا غير مشروع في الوقت الذي كان عليه الخروج مباشرة من النظام، فنجد هنا أن الجاني اتخذ موقفا سلبياً

ولم يخرج من النظام المعلوماتي في الوقت الذي يلزمه القانون بالخروج، ويتحقق السلوك السلبي أيضاً في الحالة التي يبقى فيها الجاني داخل النظام المعلوماتي أكثر من المدة المحددة له للبقاء فيه دون الخروج منه، ويكون السلوك الجرمي إيجابياً عندما يكون الجاني قد دخل إلى النظام المعلوماتي عن قصد وهو يعلم أن دخوله غير مشروع، ومن ثم يبقى في النظام لتحقيق أغراضه الإجرامية، ويتحقق السلوك الإيجابي أيضاً بقيام الجاني بنسخ المعلومات الموجودة في النظام، في الوقت الذي كان مسموحاً له رؤية هذه المعلومات والإطلاع عليها فقط.

ومن هنا يرى الباحث أن فعل الدخول يختلف عن فعل البقاء في النظام المعلوماتي ففعل الدخول من الناحية الفنية يتمثل في دخول الجاني إلى النظام المعلوماتي بسلوك إيجابي يتمثل في استخدام الطرق التقنية لإختراق الحاسب الآلي دون أن يتطلب ذلك فعلاً آخر، كما وأنه ينتج آثاره بمجرد الدخول حتى ولو لم يترتب عليه ضرر بالغير، ولذلك نجد أن معظم القوانين المقارنة تعاقب على مجرد الدخول غير المصرح به إلى النظام المعلوماتي، بصرف النظر سواء ترتب عليه وقوع ضرر للغير أم لم يترتب، أما بالنسبة لفعل البقاء في النظام المعلوماتي فهو يعني تواجد الجاني داخل نظام المعالجة الآلية للبيانات، وتجواله داخل المواقع والملفات والبيانات والمعلومات، والإطلاع عليها والانتقال بينها دون تصريح من المالك أو صاحب النظام، وهذا الأمر قد يؤدي إلى ارتكاب جرائم معلوماتية أشد خطورة، مثل الاحتيال والغش المعلوماتي وسرقته المعلومات والبرامج وغيرها من الجرائم المعلوماتية الأخرى.

ثانياً- الركن المعنوي في جريمة الدخول والبقاء غير المصرح به إلى النظام المعلوماتي:

إن جريمة الدخول والبقاء هي من الجرائم المقصودة والتي يتطلب تحققها توافر القصد الجرمي لدى الفاعل والمتمثل قي عنصريه العلم والإرادة، فيجب أن يكون الجاني عالماً بأنه يأتي نشاطاً رقمياً غير مشروع يتمثل في الدخول والبقاء في النظام المعلوماتي الخاص بالغير، وأن يكون عالماً بأنه غير مصرح له بدخوله أو التجوال فيه والاطلاع على محتوياته من معلومات وأسرار وبرامج ونظم وغيرها، وذلك بصرف النظر عن الوسيلة التي يستخدمها لهذا الدخول والبقاء غير المشروعين، أما إذا كان دخوله بمحض الصدفة فإن القصد الجنائي ينتفى لديه، وفي هذه الحالة إذا بقي في النظام فإن القصد الجنائي يتوافر لديه، بحيث تنصرف إرادته إلى البقاء فيه وهو يعلم أن دخوله وبقاءه غير مصرح بهما، فهذه الجريمة مقصودة لا تقع بالخطأ.

الفرع الثالث: موقف المشرع الأردني من جريمة الدخول والبقاء غير المصرح به إلى النظام المعلوماتي:

عالج المشرــع الأردني جريمة الدخول غير المصرــح به إلى النظام المعلوماتي في قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010، حيث نصت المادة (3) من ذات القانون على ما يلي:

"(أ) كل من دخل قصــداً إلى موقع إلكتروني أو نظام معلومات بأية وســيلة دون تصرــيح، أو بما يخالف أو يجاوز التصرــيح، يعاقب بالحبس مدة لا تقل عن أســبوع ولا تزيد على ثلاثة أشــهر، أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد على (200) مائتي دينار، أو بكلتا هاتين العقوبتين.

(ب) إذا كان الدخول المنصـوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشـــاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نســـخ بيانات أو معلومات، أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو إشغاله، أو انتحال صـفته أو انتحال شـخصـية مالكه، فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشـهر ولا تزيـد على ســـنـة، أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار، أو بكلتا هاتين العقوبتين".

وقد عرف المشرـع الأردني التصريح في المادة (2) من ذات القانون والخاصة بالتعريفات بأنه "الإذن الممنوح من صـاحب العلاقة إلى شـخص أو أكثر أو للجمهور للدخول أو اسـتخدام نظام المعلومات أو موقع إلكتروني أو الشـبكة المعلوماتية... الخ"، ويلاحظ من خلال الفقرة (أ) من المادة (3) أن المشرع الأردني عاقب على مجرد الدخول القصدي وغير المصرح به إلى النظام المعلوماتي أو بما يجاوز التصريح الممنوح من صاحب العلاقة، كما وأنه في الفقرة (ب) عاقب على الدخول بصـورته الواردة في الفقرة (أ) إذا كان هدف الجاني من هذا الدخول الاعتداء بكافة صـوره على البيانات والمعلومات المعالجة آلياً، أو الاعتداء على أنظمة المعلومات والمواقع الإلكترونيـة بتعطيلها أو توقيفها عن أداء وظيفتها أو غير ذلك من صـــور الاعتداء، أو حتى انتحال شخصية مالكها.

وبـذلـك يجـد البـاحـث أن المشرـــع الأردني كفـل الحمايـة الجنـائية اللازمة للمعلومات والأنظمة المعلوماتية والمواقع الإلكترونية من أفعال الدخول غير المصرــح به إلى النظام المعلوماتي، والتي قد تؤدي إلى الاعتداء على المعلومات بإتلافها أو حذفها أو تدميرها أو تعديلها أو تغييرها أو غير ذلك، كما وأنه اســتوعب أفعـال الـدخول التي تؤدي إلى تعطيـل النظـام المعلومـاتي والمواقع الإلكترونيـة عن أداء عملها، وبذلك يرى الباحث أن المشرع الأردني وفيما يتعلق بهذه الجريمة

قد واكب التطور الحاصل في مجال المعلوماتية شأنه في ذلك شأن معظم التشريعات الأوروبية والتي استجابت للاتفاقيات الدولية الخاصة بجرائم الحاسب الآلي والإنترنت، ومنها اتفاقية بودابست لسنة 2001 في المادة (2) والمادة (5) والمتعلقة بجريمة الدخول غير المصرح به إلى النظام المعلوماتي، والتي تستوعب الاعتداءات التي تطال المعلومات والمعطيات المعنوية للحاسب الآلي، وأيضاً الاعتداءات التي تؤدي إلى تعطيل النظام المعلوماتي عن أداء وظيفته، ومع ذلك فالمشرع الأردني لم ينص على جريمة البقاء غير المصرح به في النظام المعلوماتي، حيث إن هذا الفعل قد ينطوي على أفعال أخرى، بحيث لا يكتفي الجاني بالبقاء في النظام، وإنما قد يرتكب جرائم معلوماتية أشد خطورة من خلال تجواله بين المعلومات والبرامج والمواقع الموجودة في هذا النظام.

الفرع الرابع: موقف المشرع الأمريكي من جريمة الدخول والبقاء غير المصرح به للنظام المعلوماتي:

يحسب للمشرع الأمريكي بأنه كان سباقاً في تقرير العقاب على هذه الجريمة، وذلك في القانون الفيدرالي الخاص بالاحتيال وإساءة استخدام الحاسب الآلي لعام 1984 ، حيث اعتبر هذا القانون كل دخول غير مشروع يستهدف المعلومات المعالجة آلياً والمخزنة في الحاسب الآلي بمثابة جنحة، أما إذا كان هذا الدخول بهدف الاعتداء على معلومات مالية أو سجلات ائتمان في المؤسسات المالية أو انتهاك حرمة حاسب آلي تابع للحكومة الفيدرالية، فإن الجريمة هنا تكون بمثابة جناية (إبراهيم، 2009، 264).

ويلاحظ على هذا القانون كما ذكرنا سابقاً أنه كان أكثر ارتباطاً بالطابع الحكومي لحركة تكنولوجيا المعلومات (باستخدام الحاسوب)، إلا أنه يعد القاعدة العامة التي تدور حولها كافة التشريعات التي تتعلق بجرائم الحاسوب، وبمقتضى التعديل الثالث لهذا القانون في عام 1996 والذي صدر بمقتضى قانون البنية القومية للمعلومات فقد اعتبر أن الدخول غير المشروع هو مقدمه لازمة لارتكاب الجريمة الهدف، وقد نص على تجريم أشكال الاختراق للنظام المعلوماتي المستخدم من قبل الحكومة الفيدرالية أو المؤسسات المالية أو المؤسسات الاقتصادية أو الاتصالات، وهذه الأشكال هي:

(1) الدخول غير المشروع إلى حاسوب حكومي وكشف معلومات سرية.

(2) الدخول غير المشروع إلى أي حاسوب والولوج إلى معلومات ليس للمخترق الحق في الدخول إليها.

(3) الدخول غير المشروع إلى حاسوب ومن ثم ارتكاب جريمة احتيال.

(4) الدخول غير المشروع إلى حاسوب والتسبب في الأضرار عن طريق العبث في المعلومات أو البرمجة أو شيفرة معينة.

(5) إرسال تهديد إلى مؤسسة اقتصادية بإحداث أضرار في حاسوب بقصد ابتزاز الأموال أو ملكية مـــــــــــــة مـــــــــــــن شـــــــــــــخص أو حائزهـــــــــــــا-(http://ncsi-net.ncsi.iisc.in/cybespace/law/responsibility/cybercrime/www.usdoj.gov/criminal/cybercrime/NIPCadvi.htm.)

كما وأن المادة (6) الفقره (E) من القسم (1030) أضافت تجريم فعل تجاوز الدخول المصرح به إلى نظام الحاسب الآلي، وقد عرفت هذا التجاوز بأنه "الدخول إلى حاسب آلي مع وجود تصريح بهذا الدخول، إلا أن الفاعل يستخدم هذا الدخول للحصول على معلومات أو لتعديلها دون أن يكون مصرحاً له بذلك [28]"

كما وأن الفقره A من القسم 2701 من قانون خصوصية الاتصالات الالكترونيه الأمريكي لعام 1986 (ECPA) جرمت أفعال الدخول غير القانونية إلى الأنظمة الإلكترونية حيث نصت هذه المادة على أنه "

A – باستثناء الحالات المنصوص عليها في الفقره الفرعية (C) من هذا القسم فإن كل من قام بالدخول بشكل مقصود ودون إذن إلى النظام الإلكتروني، أو تجاوز بشكل مقصود تصريح الدخول إلى الأنظمة الإلكترونية، فإنه يعاقب على النحو المنصوص عليه في الفقرة الفرعية B من هذا القسم.

B –العقوبات : تصل عقوبة الجريمة المرتكبة بموجب الفقرة (A) من هذا القسم اذا ارتكبت لتحقيق أغراض ومكاسب مالية وتجارية أو لإحداث أضرار للغرامة أو السجن لمدة سنة أو أكثر أو بكلتا العقوبتين في الحالات التي ترتكب الجريمة فيها لأول مره ، ويعاقب الفاعل بالغرامة أو السجن لمدة لا تزيد على سنتين في حال إرتكاب أية جريمة لاحقة بموجب هذه الفقره الفرعية[29]"

---

[28] Article 1030/E/6 of NII Protection Act of 1996
(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

[29] Article 2701/A and B of ECPA of 1986

(a) Offense.--Except as provided in subsection (c) of this section whoever–

وعلى مستوى تشريع الولايات الأمريكية، فإنه يمكن القول إن كافة الولايات قد ضمنت تشريعاتها النص على تجريم فعل الدخول غير المصرح به إلى ا لحاسوب بقصد ارتكاب جريمة، وأيضاً في حالة إحداث أضرار لمادة مخزنة في الحاسوب، بما في ذلك المحتويات المعنوية غير المادية (يونس، 2004، 321).

ومن هنا يجد الباحث أن المشرع الأمريكي قد ضمّن تشريعاته النص على تجريم الدخول غير المصرح به إلى النظام المعلوماتي، سواء أكان ذلك على المستوى الفيدرالي أم على مستوى الولايات، إلا أنه يلاحظ أن المشرع الأمريكي نص على حالات الدخول وتجاوز الدخول المصرح به إلى النظام المعلوماتي من قبل الجاني، لكنه لم يتناول صراحة وبشكل مباشر الحالات التي تنطوي على البقاء داخل النظام إذا كان الدخول بطريقة الخطأ أو الصدفة.

المطلب الثاني: جريمة الاعتراض غير القانوني لانتقال البيانات والمعلومات عبر النظام المعلوماتي:

وسوف نبحث هذه الجريمة من حيث ماهيتها وكيفية وقوعها وعناصرها وموقف المشرع الأردني والأمريكي من هذه الجريمة وذلك كما يلي:

الفرع الأول: ماهية جريمة الاعتراض غير القانوني لانتقال البيانات والمعلومات عبر النظام المعلوماتي:

أشارت اتفاقية بودابست لسنة 2001 إلى جريمة الاعتراض غير القانوني بدون حق، وذلك في المادة الثالثة منها، حيث أوجبت على جميع الأطراف اتخاذ الإجراءات التشريعية وأية إجراءات أخرى ضرورية لاعتبار هذه الجريمة جنائية، وفقاً لقوانينها الداخلية،

---

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.--The punishment for an offense under subsection (a) of this section is–

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain--

(A) a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

وبينت الاتفاقية أن هذه الجريمة تقع من خلال استخدام تقنية للإرسال غير العلني لبيانات ومعلومات الحاسب الآلي، سواء في مكان وصولها في المنشأة، أو في داخل النظام المعلوماتي، وكذلك الموجات الكهربائية أو الانبعاثات الكهرومغناطيسية من الحاسب الآلي الذي يحتوي هذه المعلومات والبيانات، ويمكن أن ترتكب الجريمة أيضاً من حاسب آلي متصل عن بعد بحاسب آلي آخر، وكل ذلك مع توافر القصد الجرمي لدى الفاعل[30].

وقد أصدر الاتحاد الأوروبي توجيهاً عام 1995، والخاص بمعالجة البيانات الشخصية وحرية انتقال البيانات والمعلومات وحدد مسؤولية من يعترض سرية هذه البيانات والمعلومات، كما اهتمت الهيئات الدولية بإصدار توجيهات بشأن حماية السرية، حيث أصدرت منظمة التعاون والتنمية الاقتصادية المبادئ التوجيهية لحماية الخصوصية وتدفق البيانات الشخصية عبر الحدود عام 1980 (إبراهيم، 2009، 285).

وفعل الاعتراض غير القانوني يعني التدخل غير المشروع بالاتصالات التي تجري عبر شبكات الاتصال، سواء أكان هذا التدخل على صورة اعتراض للرسائل الإلكترونية والمعلومات المنقولة عبر الشبكة المعلوماتية، أو إعاقتها أو تحويرها أو شطب محتوياتها، وقد يأتي على صورة التشويش على الموجات المخصصة لاتصال الغير عن طريق إساءة استخدام الموجات الكهرومغناطيسية، الأمر الذي يؤدي إلى تعطيل الحاسب الآلي عن القيام بوظائفه (العزام، 2009، 121).

ويمكن تشبيه اعتراض نظام الحاسب الآلي بالتنصت على مكالمة هاتفية بين شخصين، بحيث يستطيع الجاني من خلال فعل الاعتراض غير القانوني معرفة محتوى الاتصال الذي ورد داخل نظام حاسب آلي واحد، أو بين نظامين مختلفين عبر الشبكة، أو بين عدة أنظمة مرتبطة فيما بينها من خلال شبكة الاتصالات، وذلك من خلال التقاط المعلومات التي يتضمنها هذا الاتصال عن طريق تتبع الموجات الكهربائية الصادرة عن الحاسب الآلي الذي يرسل هذه البيانات والمعلومات من خلال أجهزة تقنية معينة يستخدمها الجاني لهذا الغرض، ومن ثم يقوم ذات الجهاز بترجمة هذه الموجات إلى معلومات مفهومة ومقروءة وواضحة للمخترق (قورة، 2005، 350).

---

[30] نص المادة الثالثة من اتفاقية بودابست لسنة 2001:

Article 3- Illegal interception:
Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmission of computer data to, from a with in a computer system, including electromagnetic emissions from a computer system carrying such computer data. A party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

ويرى الباحث أن الهدف من تجريم فعل الاعتراض هو حماية الحق في حرية الاتصالات والمراسلات، وحرية نقل البيانات والمعلومات عبر النظام المعلوماتي، وعدم ترك المجال مفتوحاً لأي كان من اعتراض المعلومات المتدفقة عبر النظام المعلوماتي والإطلاع عليها.

وقد يحدث فعل الاعتراض عن طريق التصنت على المحادثات الخاصة بالمستخدمين والتي تتم عبر شبكة الإنترنت وذلك باستخدام طرق فنية تقنية، أو عن طريق الإطلاع على البيانات والمعلومات المتدفقة عبر هذه الشبكة، كاعتراض رسائل البريد الإلكتروني عبر الإنترنت، سواء تم ذلك عن طريق الحصول على كلمة السر الخاصة بالمستخدم (Password)، أو باعتراض هذه الرسائل بالوسائل والطرق التقنية ومن ثم الإطلاع عليها.

وقد يحدث فعل الاعتراض عن طريق استخدام الجاني لأجهزة فنية تقنية للإرسال غير العلني للبيانات والمعلومات والمراسلات، ومبدأ عمل هذه الأجهزة أنها تقوم بالعمل عند تشغيل الحاسب الآلي الهدف، بحيث تقوم باستقبال الانبعاثات الكهرومغناطيسية الصادرة عن هذا الجهاز، ومن ثم التقاطها وترجمتها إلى لغة واضحة ومفهومة للإنسان، وبذلك الوصول إلى البيانات والمعلومات التي يحتويها هذا الجهاز أو الصادرة عنه، وبعد ذلك نقلها أو تسجيلها عن طريق هذه الأجهزة التقنية.

وقد تستخدم هذه الطريقة لاعتراض البيانات والمعلومات المتدفقة عبر الأجزاء الداخلية لنفس الحاسب الآلي، أو لاعتراض المعلومات المرسلة عن بعد من حاسب آلي إلى حاسب آلي آخر عبر شبكة مغلقة، أو لاعتراض البيانات والمعلومات المتدفقة عبر الشبكة المعلوماتية المفتوحة (الإنترنت) مثل اعتراض رسائل البريد الإلكتروني.

ويؤدي اعتراض المعلومات إلى منع وصولها إلى الجهة المرسلة إليها، بصرف النظر سواء تمكن الجاني من معرفة محتواها أم لم يتمكن، وسواء أدى ذلك إلى محو أو إتلاف أو تحوير الرسالة أم لم يؤد . (الزعبي والمناعسة، 2010، 253).

وتعتبر وسيلة استخدام الموجات والانبعاثات الكهرومغناطيسية الصادرة عن الحاسب الآلي باستخدام أجهزة الاستقبال التقنية من أكثر الوسائل الأساسية لاعتراض البيانات والمعلومات المتداولة عبر الشبكة المعلوماتية، ففي الولايات المتحدة الأمريكية يطلق على فعل الاعتراض اسم التقاط الموجات الكهربائية،

والذي يعني جمع المعلومات عن بُعد، حيث يستطيع الجاني جمع معلومات تم إرسالها من جهاز حاسب آلي موجود في مبنى معين، وذلك عن طريق استخدام جهاز مُعد للاستقبال موصولاً بشاشة عرض وجهاز تسجيل خارج المبنى، حيث يتمكن الجاني بهذا الجهاز من استقبال هذه الموجات المنبعثة من الحاسب الآلي الهدف، ومن ثم تحويلها إلى معلومات يتم عرضها على الشاشة ومن ثم تسجيلها (قورة، 2005، 350).

الفرع الثاني: موقف المشرع الأردني من جريمة الاعتراض غير القانوني لانتقال البيانات والمعلومات عبر النظام المعلوماتي:

أولاً- موقف المشرع الأردني وفقاً لقانون الاتصالات رقم (13) لسنة 1995:

جاء المشرع الأردني بقانون الاتصالات رقم (13) لسنة 1995 وذلك لحماية الرموز أو الإشارات أو الأصوات أو الصور أو البيانات مهما كانت طبيعتها، وذلك خلال نقلها أو بثها أو استقبالها أو إرسالها، وبأية وسيلة كانت سواء السلكية أو الراديوية أو الضوئية أو وسيلة الأنظمة الإلكترونية.

وقد جاءت المادة 76 من ذات القانون والخاصة بالرسائل المنقولة عبر شبكات الاتصال ونصت على ما يلي:

"كل من اعترض أو أعاق أو حوَر أو شطب محتويات رسالة بواسطة شبكات الاتصالات، أو شجع غيره على القيام بهذا العمل، يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر، أو بغرامة لا تزيد على (200) دينار أو بكلتا العقوبتين".

ويلاحظ من خلال التدقيق في هذه المادة أنه يمكن تطبيقها في حال توافر عناصرها وأركانها المفهومة من النص كما يلي:

(1) أن يكون هناك نشاط مادي صادر عن الجاني يتمثل في الاعتراض أو الإعاقة أو التحوير أو الشطب، وكذلك في حالة قيام هذا الشخص بتشجيع الغير على إتيان إحدى صور هذا النشاط.

(2) إن محل الجريمة هو الرسائل المنقولة عبر شبكات الاتصال والتي تتمثل في الوسائل السلكية أو الراديوية أو الضوئية أو وسيلة الأنظمة الإلكترونية.

(3) الركن المعنوي في هذه الجريمة يتخذ صورة القصد لا الخطأ.

وبالنظر إلى المادة 80 من ذات القانون والتي تنص على ما يلي:

"أ- كل من قام متعمداً بأي إجراء لاعتراض موجات راديوية مخصصة للغير، أو بالتشويش عليها أو بقطعها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن (5000) دينار ولا تزيد على (25000) دينار أو بكلتا العقوبتين.

ب- كل من قام متعمداً باستخدام موجات راديوية دون ترخيص، يعاقب بالحبس مدة لا تقل عن شهر أو بغرامة لا تقل عن (2000) دينار ولا تزيد على (5000) دينار، أو بكلتا هاتين العقوبتين".

ومن خلال التدقيق في هذه المادة نجد أنها تطبق من خلال ما يلي:

(1) نشاط مادي من قبل الفاعل يتمثل في اعتراض الموجات الراديوية أو التشويش عليها أو قطعها.

(2) محل الجريمة هي الموجات المنتشرة في الأثير والمخصصة من قبل هيئة تنظيم قطاع الاتصالات المنشأة بموجب هذا القانون، وقد حددت المادة الثانية من ذات القانون الموجات الراديوية بأنها موجات كهرومغناطيسية ذات ترددات تقل عن ثلاثة آلاف (جيجا هيرتز) تبث في الفضاء دون موجه اصطناعي.

(3) الركن المعنوي: حيث اعتبر المشرع هذه الجريمة عمدية، وقد نص على ذلك صراحة فهو يتطلب لقيامها توافر القصد العام بعنصرية العلم والإرادة فهذه الجريمة لا تقع بالخطأ.

ومن الناحية الفنية للحاسوب والإنترنت فإن شبكة الإنترنت تتطلب وجود خط هاتف أرضي أو متنقل وجهاز مودم (Modem) لتشغيل هذه الشبكة وتبادل الاتصالات وإرسال ونقل البيانات والمعلومات عبرها، وتستخدم خطوط الهاتف لربط شبكات الحاسب الآلي إذا كانت المسافة بعيدة، وتستخدم أيضاً موجات الميكروويف والأقمار الصناعية، وكل ذلك حتى يتمكن المستخدم من نقل المعلومات والبيانات من وحدة طرفيه إلى وحدة طرفية أخرى، ويستطيع الفاعل الحصول على المعلومات باستخدام جهاز تنصت خاص يستمع عن طريقه إلى خطوط الهاتف التي يجري اتصال الشبكات فيها، وتكثيفها وإعادة استعمالها لتظهر على شبكة المعلومات، كما ويستطيع استخدام جهاز خاص لاستقبال الموجات الكهرومغناطيسية المرسلة من وحدة طرفيه إلى وحدة طرفيه أخرى عبر الأنظمة الإلكترونية، وتحويلها إلى معلومات مفهومة للإنسان لتحقيق أغراضه الإجرامية.

لما تقدم يرى الباحث أن سلوك الشخص باعتراض أو إعاقة أو محو أو شطب الرسائل الإلكترونية المنقولة عبر شبكات الاتصالات وبأية وسيلة كانت ومن ثم توجيهها إلى حاسوبية وإعادة عرضها على شكل معلومات مرئية ومقروءة يعتبر مجرماً وفقاً لنص المادة (76)، (80) من قانون الاتصالات الأردني.

ثانيا- موقف المشرع الأردني وفقاً لقانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010:

نص المشرع الأردني على جريمة الاعتراض المقصود وغير المشروع على الرسائل المنقولة عبر الشبكة المعلوماتية وذلك في المادة (5) من ذات القانون، حيث نصت على ما يلي: "كل من قام قصداً بالتقاط أو باعتراض أو بالتنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات، يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنة، أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد على (1000) ألف دينار، أو بكلتا هاتين العقوبتين".

ويلاحظ هنا أن المشرع الأردني قد واكب التطور الحاصل في تكنولوجيا المعلومات بأن وفر الحماية الجنائية للبيانات والمعلومات المتدفقة عبر أي نظام معلوماتي، وذلك من الاعتداء عليها بالالتقاط أو الاعتراض أو حتى التنصت، وبصرف النظر عن الوسيلة المستخدمة من قبل الجاني لإتمام جريمته، ودون البحث في الغاية أو الهدف من وراء فعل الاعتراض أو الالتقاط أو التنصت.

ويرى الباحث أن ذلك يُحسب للمشرع الأردني من خلال النص على هذه الجريمة في قانوني الاتصالات وجرائم أنظمة المعلومات، حيث أحاط بكافة صور هذه الجريمة ووفر الحماية الجنائية اللازمة للمعلومات والبيانات المتداولة عبر أجزاء الحاسب الآلي الواحد أو عبر الوحدات الطرفية من خلال شبكة الإنترنت، ومع ذلك فإن الباحث يرى أن العقوبات الواردة في نص المادة (5) من قانون جرائم أنظمة المعلومات غير كافية مقارنة مع خطورة هذه الجريمة في بعض الأحيان وخاصة عندما تتعلق المعلومات بأمن الدولة وسيادتها أو عندما تتعلق بأصول وقيم اقتصادية ومالية لشركات استثمارية أو مصارف أو بنوك أو غيرها. والتي تؤدي إلى خسارات مالية هائلة.

الفرع الثالث: موقف المشرع الأمريكي وبعض التشريعات الأجنبية المقارنة من جريمة الاعتراض غير القانوني لانتقال البيانات والمعلومات عبر النظام المعلوماتي:

تضمن القانون الفيدرالي الأمريكي رقم (18) لعام 1984 والمتعلق بجرائم الكمبيوتر، وأشار إلى هذا النمط من الإجرام المعلوماتي، وجرم الاعتداء على وظائف نظام المعالجة الآلية للمعلومات، وأطلق عليه مصطلح منع وصول الخدمة (Denial of Service)،

وعاقب على هذه الأفعال بموجب نصـــوص هذا القانون، كما وجرم في المادة 2701/A من قانون خصـوصـية الإتصـالات الإلكترونية لعام 1986 أفعال الوصـول غير القانوني للمعلومات المخزنة في الحاسـب الآلي، وعاقب عليها بالحبس والغرامة ،حيث نصت الماده أعلاه على أنه " كل من وصل بشكل مقصود ودون إذن من صـاحب العلاقة ،أو تجاوز بشـكل مقصـود الدخول المصرح به وصولاً للمعلومات المخزنة في النظام الإلكتروني، فإنه يعاقب بالعقوبات الوارده في الفقرة الفرعية (B) من ذات المادة[31]"

كما وجرم هـذا القانون الأفعال التي تعيق ســير النظم المعلوماتية، وخاصــةً المعلومات المتعلقة بالخصـوصـية والحياة الشـخصـية للأفراد، حيث جرم أفعال حجز أو إعاقة أو اعتراض الاتصـالات الإلكترونية بدون إذن بقصد القرصنة، أو لاستخدام الحاسب الآلي، أو بغرض إفشاء الاتصالات الإلكترونية لشخص ما [32] (http//floridalawfirm.com).

(Johnston, D and others, 1997, P. 91)

كما ونصــت المادة 2511 من ذات القانون على تجريم إعتراض الإتصـالات السـلكية أو الإلكترونية أوالشـفوية ،حيث نصـت الفقرة (1) منهاعلى أنه "باستثناء ما هو منصوص عليه تحديداً خلاف ذلك في هذا الفصـل، فإن أي شـخص يقوم وبشـكل مقصود باعتراض او يساعد الآخرين في اعتراض الإتصالات السلكية أو الشـفوية أو الإلكترونية ،أو يسـتخدم جهاز إلكتروني لاعتراض الموجات أو يسـاعد الغير على ذلك، أو يتداخل مع اتصـالات سـلكية أو راديويه بهدف كشـف محتوى هذه الاتصالات السلكيه أو الإلكترونيه ، فإنه يعاقب على النحو المنصوص عليه في الفقره الفرعية (4) من ذات الماده [33]".

---

[31] Article 2701/A of ECPA of 1986

(a) Offense.--Except as provided in subsection (c) of this section whoever–

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

[32] chapter 119 – wire and electronic communications international and interception of oral communications.

[33] Article 2511/1 of ECPA of 1986
Sec. 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

وقد جرمت المادة (1030) الفقرة (a) من القانون الفيدرالي الأمريكي الخاص بإساءة استخدام الحواسيب الآلية، أفعال الدخول غير المصرح به الى نظام الحاسب الآلي، بأية وسيلة من أجل الوصول إلى المعلومات المعالجة آلياً باستخدام وسائل إلكترونية، سواء اتخذت هذه الوسائل شكل القيام بعملية دخول غير مصرح به، أو اعتراض نظام الحاسب الآلي للحصول على المعلومات المعالجة آلياً (قوره، 2005، 319 وما بعدها).

ويتضح من نصوص المواد السابقة أن المشرع الأمريكي جرم أفعال إعتراض الموجات السلكية أو الالكترونية ، وافعال الوصول إلى أنظمة المعالجة الآلية أو مساعدة الغير عليها بهدف الإطلاع على مضمون الإتصالات ، أو الوصول الى المعلومات المخزنه أو المتداولة عبر الأنظمة المعلوماتية ، وذلك بأية وسيلة كانت والتي من ضمنها استخدام اجهزة معده لهذه الغاية.

وقد جرمت بعض الولايات الأمريكية أفعال التداخل بشكل متعمد في نظام الحاسب الآلي، أو شبكة المعلومات، أو برامج الحاسب الآلي دون رضاء صاحب النظام عن ذلك، حتى أن بعض الولايات عاقبت على مجرد الشروع في هذا التداخل، إذا لم يتمكن الفاعل من التوصل للنظام المعلوماتي (إبراهيم، 2009، 280).

وبذلك يرى الباحث أن المشرع الأمريكي قد نص صراحة على جريمة الاعتراض غير القانوني للبيانات والمعلومات المعالجة آلياً، والمتداولة عبر شبكة الإنترنت في قانون خصوصية الاتصالات الإلكترونية، والخاص بحماية الخصوصية والمعلومات المتعلقة بالحياة الخاصة للأفراد، وفي الفصل الثامن عشر من القانون الفيدرالي وجرم أيضاً فعل الدخول غير المصرح به إلى نظام الحاسوب الآلي بأية وسيلة إلكترونية تقنية، سواء تمثلت هذه الوسيلة في الدخول الفعلي إلى النظام المعلوماتي، أو في اعتراض هذا النظام وما يحتويه من معلومات وبيانات معالجة آلياً.

---

(1) Except as otherwise specifically provided in this chapter any person who -

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when -

وتجدر الإشارة هنا أن المجلس الأوروبي قد أوصى الدول بإفراد نص خاص يجرم اعتراض نظام الحاسب الآلي بمقتضاه، بحيث يتم تجريم كل اعتراض لاتصال يتم من أو إلى أو داخل الحاسب الآلي أو شبكة الاتصالات (قوره، 2005، 351).

وقد سار القانون البرتغالي على هذا النهج، حيث تجرم المادة الثامنة من القانون رقم (109) لعام 1991 والخاص بجرائم المعلوماتية اعتراض عمليات الاتصال، التي تقوم على نقل المعلومات داخل أنظمة الحواسيب الآلية أو شبكات المعلومات باستخدام وسائل تقنية، وقد حددت المادة الثانية من ذات القانون المقصود بفعل الاعتراض، ووصفته بأنه كل عمل يهدف إلى الوصول إلى المعلومات التي تضمنتها أنظمة المعالجة الآلية للمعلومات، باستخدام أجهزة كهرومغناطيسية، أو سمعية أو ميكانيكية أو غير ذلك (قوره، 2005، 351 وما بعدها).

أما قانون العقوبات الكندي، فقد جرم في المادة (1/430) وبنص صريح اعتراض سبيل البيانات والمعلومات، وجرم أيضاً في المادة (1/342) من ذات القانون، الأفعال المنطوية على استخدام وسائط إلكترونية أو صوتية أو ميكانيكية أو أية أداة أخرى، لوقف أو اعتراض سبيل أو التسبب باعتراض أي وظيفة لنظام الحاسب الآلي، سواءَ أكان ذلك بصورة مباشرة أم غير مباشرة (العزام، 2009، 121 وما بعدها).

وبذلك يرى الباحث أن التشريعات الأردنية والأمريكيه والكندية والبرتغالية قد نصت صراحة على تجريم أفعال الاعتراض أو التحوير أو الإعاقة غير القانونية للمعلومات المعالجة آلياً، والمتداولة عبر الأنظمة المعلوماتية، وبذلك وفرت الحماية الجنائية اللازمة لهذه المعلومات من خطر اعتراضها أو إعاقتها عبر النظام المعلوماتي.

المبحث الثاني: الجرائم الماسة بسلامة المعلومات والبيانات المعالجة آلياً:

تعتبر جريمتا الإتلاف المعلوماتي والتزوير المعلوماتي من أهم الجرائم المعلوماتية التي تهدد سلامة المعلومات والبيانات المعالجة آلياً، وكنا قد تحدثنا عن جريمة الإتلاف المعلوماتي في الفصل السابق والخاص بالحماية الجنائية للمعلومات في إطار جرائم الأموال، وبينا صورها وأساليب ارتكابها وكيفية وقوعها، وبينا أيضاً موقف المشرع الأردني والمشرع الأمريكي من هذه الجريمة الخطيرة،

لذلك فسوف نتناول في هذا المبحث من الفصل الرابع جريمة التزوير المعلوماتي على اعتبارها من أهم الجرائم الماسة بسلامة المعلومات والبيانات الإلكترونية، بحيث نبين مفهوم هذه الجريمه في صورتها التقليدية ثم مفهومها في نطاق نظم المعلومات وذلك وفقاً لاتفاقية بودابست لعام 2001 وصورها، ثم موقف المشرع الأردني وبعض التشريعات المقارنة من هذه الجريمة وذلك على النحو الآتي:

المطلب الأول: جريمة التزوير المعلوماتي:

تعتبر جريمة التزوير في المحررات من الجرائم المخلة بالثقة العامة والتي يكون محلها دائما المحرر المكتوب، حيث اعتمدت الدول والأفراد وباستمرار على إثبات الحقوق والمعاملات عن طريق الكتابة، فالمحررات الكتابية هي وسيلة إثبات لأصحاب الحقوق في كافة مناحي الحياة التي تتطلب إثباتاً بهذه الطريقة، لذلك فقد حرص المشرع الجزائي في الدول المختلفة على تجريم أفعال التزوير التي تقع على هذه المحررات، لأهميتها ولثقة الأفراد والحكومات بها، وبعكس ذلك فإن هذه الثقة لن تتوافر، الأمر الذي يؤدي إلى الإخلال باستقرار المعاملات في كافة مناحي الحياة وبالأخص القانونية منها.

وفي الوقت الراهن أصبح الحاسب الآلي والنظام المعلوماتي يحل محل الأوراق المحررة في معظم المعاملات المالية والاقتصادية والمصرفية والرسمية وغيرها، وأصبحت الإدارات الحكومية وإدارات القطاع الخاص تعتمد وبشكل أساسي في أعمالها اليومية على نظم المعلومات والحاسب الآلي، وذلك من خلال حفظ المعلومات والبيانات المعالجة آلياً في ذاكرة الحواسيب الآلية أو من خلال مستخرجات النظام المعلوماتي من مستندات أو دعامات مادية أو شرائط ممغنطة، الأمر الذي يتطلب من المشرع الجزائي توفير الحماية الجزائية الملائمة لمثل هذه المستندات والمعلومات والبيانات من خطر الاعتداء عليها بالتزوير وتغيير الحقيقة، وما يترتب على ذلك من أضرار جسيمة مادية ومعنوية. ولتوضيح ذلك فسوف نتناول في هذا المطلب مفهوم جريمة التزوير في صورتها التقليديه، وبيان أركانها كما يلي:

الفرع الأول: مفهوم جريمة التزوير في صورتها التقليدية:

التزوير لغة مشتق من كلمة مزور وهو يعني الكذب والتلفيق وإدخال الباطل (معجم لسان العرب، الجزء الأول).

أما الفقه فقد عرف التزوير بأنه "تغيير الحقيقة في محرر بإحدى الطرق التي حددها القانون تغييراً من شأنه أن يرتب ضررا للغير، بنية استعمال هذا المحرر فيما أعد له" (حجازي، 2004، 135).

أما القوانين المقارنة فقد أوردت بعض القوانين العربية تعريفاً للتزوير في نصوصها الجزائية التقليدية ومنها، قانون العقوبات الأردني والذي عرف التزوير في نص المادة 260 بأنه "تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما، نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي"، وعرفه قانون العقوبات الاتحادي في دولة الإمارات العربية المتحدة في المادة (216 /ع) بأنه "تغيير الحقيقة في محرر بإحدى الطرق المبينة فيما بعد، تغييراً من شأنه إحداث ضرر وبنية استعماله كمحرر صحيح ويُعد من طرق التزوير... الخ".

وعرفه قانون العقوبات اللبناني في المادة (453)، والقانون السوري في المادة (440)، وهذه التعريفات لا تخرج عن التعريف الوارد في قانون العقوبات الأردني، أما المشرع المصري فلم يُعرف التزوير في قانون العقوبات المصري في المواد الخاصة بجريمة التزوير، واكتفى بإيراد طرق التزوير في المحررات، ونص على عبارة "تغيير المحررات" في المادة (211/ع)، وعبارة "تغيير إقرار ولي الشأن" في المادة 213/ع).

أما المشرع الفرنسي فقد أورد تعريفاً للتزوير في قانون العقوبات الصادر سنة 1994 والمعدل لقانون العقوبات الفرنسي لسنة 1988، حيث نصت المادة (1/441) على أنه "يعتبر تزويراً كل تغيير تدليسي للحقيقة يكون من طبيعته أن يسبب ضرراً، ويتم بأية وسيلة كانت في محرر أو أي سند للتعبير عن الرأي، والذي يكون موضوعه أو الذي من الممكن أن يكون له أثر في إنشاء دليل على حق أو فعل تكون له نتائج قانونية... الخ [34] " ومما تقدم يرى الباحث أن القوانين الجنائية التقليدية سواء التي أوردت تعريفاً للتزوير أو التي لم تورد كانت قد جرمت التزوير في المحررات، وذلك لتعلق هذه الجريمة بالثقة العامة وتنظيم المعاملات بين الناس، ولما لها من قيمة في إثبات الحقوق والمراكز القانونية على اختلاف أنواعها، إلا أنها أجمعت من خلال نصوصها على أن محل هذه الجريمة هي المحررات المكتوبة، فالجريمة وفقاً للنصوص السابقة لا تقع إلا على المحرر المكتوب وحده، ومؤدى ذلك أن تغيير الحقيقة فيه، والنتيجة الجرمية تظهر فيه أيضاً من حيث صدور محرر مغاير للحقيقة، وضرر يصيب الغير.

---

[34] Article 441/1 Of (FCP)

Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

الفرع الثاني: أركان جريمة التزوير التقليدية في قانون العقوبات الأردني:

عالج المشرـع الأردني جريمة التزوير في المادة (260) من قانون العقوبات الأردني حيث نصت على أن التزوير هو "تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما، نجم أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي"، ومن خلال استقراء النص يتبين أن الأركان العامة لهذه الجريمة وفقا لما ورد هي:

أولاً- الركن المادي:

يتمثل الركن المادي لجريمة التزوير وفقاً للمشرـع الأردني في التحريف المفتعل للحقيقة الصادر من قبل الجاني، ويقابل ذلك في التشريعات الأخرى تغيير الحقيقة.

ويعتبر تغيير الحقيقة هو جوهر الركن المادي في هذه الجريمة، إذ لا يتصور وقوعها إلا باستبدال الحقيقة بما يخالفها، وإذا انتفى ذلك العنصرـ فلا تقوم جريمة التزوير، حتى ولو اعتقد الفاعل أنه يثبت غير الحقيقة، وليس المقصود بتغيير الحقيقة هو التغيير المطلق، وإنما يكتفي القانون بتغيير الحقيقة النسبي لقيام هذه الجريمة (الملط، 2006، 435).

ويجب أن ينصب تغيير الحقيقة على الوقائع والبيانات التي يتضمنها الصك أو المخطوط أو المستند، ويعرف الصك بأنه كل محرر يتضمن الإقرار بالمال أو غير ذلك، أما المخطوط فهو كل محرر مخطوط باليد، وأما المستند فهو كل محرر يمكن أن يستند إليه في توثيق حق أو دعمه حالة قانونية (السعيد، 1997، 76 وما بعدها).

ويلزم توافر عدة شروط حتى نكون بصدد محرر يصلح لأن يكون محلاً لجريمة التزوير، فمن ناحية أولى يجب أن يكون مكتوباً بصرـف النظر عن اللغة التي كتب بها، ومن ناحية ثانية يجب أن يكون هذا المحرر دالاً على المعنى الذي حرر من أجله بأن لا يكون غامضاً وغير مفهوم من قبل الجميع، كما لو كان المحرر عبارة عن خطوط متقاطعة غير مفهومة ويجب أن يحدث أثرا قانونياً، ومن ناحية ثالثة يجب أن يـ كون هذا المحرر معروف المصدر بأن يكون منسوباً إلى شخص معين أو جهة معينة، بصرف النظر سواء أكان شخصا طبيعياً أو معنوياً، وسواء أكان فرداً واحداً أم مجموعة من الأفراد (زين الدين، 2008، 340 وما بعدها).

وقد حدد المشرع الأردني في المادة (1/262) من قانون العقوبات الأردني طرق التزوير المادي وهي:

(1) إساءة استعمال إمضاء أو ختم أو بصمة إصبع.

(2) صنع صك أو مخطوط.

(3) تغيير في مضمون صك أو مخطوط.

وحدد أيضاً في المادة (1/263) من ذات القانون طرق التزوير المعنوي وهي:

(1) إساءة استعمال إمضاء على بياض أؤتمن عليه.

(2) تدوين المزور عقوداً أو أقوالاً غير التي صدرت عن المتعاقدين أو التي أملوها.

(3) إثبات المزور وقائع كاذبة على أنها صحيحة أو وقائع غير معترف بها على أنها معترف بها.

(4) تحريف أية واقعة أخرى بإغفاله أمراً أو إيراده على وجه غير صحيح.

ثانياً- ركن الضرر:

وفقا للمشرع الأردني فإن تغيير الحقيقة لا يعد تزويراً إلا إذا نتج عنه ضرر أو كان من المحتمل أن يترتب عليه ضرر ، ويستوي في هذا المقام أن يكون الضرر مادياً أو أدبياً ،خاصاً أو عاماً، والعبرة في وقت تحديد الضرر الناشئ عن تغيير الحقيقة هو لحظة تغيير هذه الحقيقة. (الملط، 2006، 443 وما بعدها).

ويكون الضرر أدبياً متى أصاب الإنسان في شرفه وكرامته وعرضه، ويكون مادياً متى أصاب الإنسان في ذمته المالية (السعيد، 1997، 89)، أما الضرر الخاص فهو الضرر الذي يصيب الأشخاص أو الهيئات الخاصة، والضرر العام هو الذي يصيب المجتمع أو المصلحة العامة ولا يصيب شخصاً أو مجموعة بعينها (الملط، 2006، 444).

ثالثاً- الركن المعنوي:

تعتبر جريمة التزوير من الجرائم المقصودة التي يتطلب تحققها توافر القصد الجنائي لدى الجاني بصورتيه العام والخاص، ويعرف القصد الجنائي في جريمة التزوير بأنه "تعمد تغيير الحقيقة في محرر تغييراً من شأنه أن يسبب ضرراً، وبنية استعمال المحرر فيما غُيرت من أجله الحقيقة" . (الملط، 2006، 44).

ويقوم القصد الجنائي العام على عنصري العلم والإرادة، وذلك بأن يحيط علم الجاني بعناصر وأركان هذه الجريمة من حيث قيامه بتحريف مفتعل للحقيقة في محرر، وذلك بالطرق المادية أو المعنوية والمنصوص عليها على سبيل الحصر في قانون العقوبات الأردني، وأن يكون مدركا لما يترتب على سلوكه الجرمي من احتمال وقوع الضرر أو وقوعه بالفعل، وأن تتجه إرادته إلى ارتكاب الفعل وإلى تحقيق النتيجة الجرمية المتمثلة في وقوع الضرر أو احتمالية وقوعه.

وإلى جانب القصـد العام فإن القانون يتطلب توافر القصـد الجنائي الخاص لدى الفاعل والمتمثل في اتجاه نيته إلى استعمال المحرر فيما زور من أجله.

المطلب الثاني: التزوير في نطاق نظم المعلومات:

في ظل الانتشـار المتزايد لتقنية المعلومات وزيادة الاعتماد على أنظمة المعلومات في شـتى مناحي الحياة فقد أصبح هناك قلق متزايد من وقوع التزوير على البيانات والمعلومات المخزنة في الحواسيب الآلية، وكذلك أن يقع التزوير على مستخرجات النظام المعلوماتي من مستندات وأشرطة ممغنطة أو دعامات مادية مثبت عليها البيانات والمعلومات، ولأهمية ذلك الأمر وخطورته فإننا سـوف نتناول التزوير المعلوماتي وفقا لاتفاقية بودابسـت الدولية والخاصـة بمكافحة جرائم الحاسـب الآلي لعام 2001 ، وسـوف نبين أيضـاً صـور ارتكاب هذه الجريمة المعلوماتية وذلك وفقاً لما يلي:

الفرع الأول: التزوير المعلوماتي وفقا لإتفاقية بودابست لمكافحة جرائم الحاسب الآلي لعام 2001:

نصـت المادة السـابعة من اتفاقية بودابسـت لمكافحة جرائم الحاسب الآلي لعام 2001 على تجريم أفعـال الإدخـال أو الإتلاف أو المحو أو الطمس العمـدي وبـدون حق، للبيانات المعلوماتية، التي تتولد عنها بيانات غير صـحيحة بقصـد اسـتخدامها لأغراض قانونية كما لو كانت صـحيحة، بصرـف النظر عما إذا كانت سـهلة القراءة مباشرة وواضـحة أم لا، وقد خاطبت الاتفاقية الدول الأطراف باتخاذ الإجراءات التشرـيعية اللازمة لتجريم هذه الأفعال وفقا للقوانين الوطنية [35]

---

[35] Article 7 of The Pudabest Convention Of Cybercrime 2001

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches

وبينت المذكرة التفسيرية للاتفاقية أن الغرض من هذه المادة هو إنشاء جريمة موازية لجريمة تزوير المستندات الورقية، لاستكمال أوجه النقص التي تعتري قوانين العقوبات التقليدية والخاصة بهذه الجريمة في حال وقوعها على البيانات والمعلومات المعالجة آلياً في النظام المعلوماتي[36]، واعتبرت المذكرة التفسيرية للاتفاقية أن التزوير المعلوماتي يتحقق عن طريق خلق أو تعديل غير مصرح به للبيانات المعالجة آلياً، واعتبرت أن العمليات اللاحقة للاتلاف كالتعديلات أو التغييرات الجزئية والمحو كواقعة خروج البيانات الممثلة على دعامة والطمس كواقعة حفظ وإخفاء بيانات تشابه بشكل عام تزوير محرر صحيح (أحمد، 2003، 108 وما بعدها).

يرى الباحث أنه وفقاً للنص الوارد في الاتفاقية فإن وسائل وأساليب التزوير المعلوماتي هي أفعال الإدخال أو الإتلاف أو المحو أو الطمس للبيانات المعلوماتية المعالجة آلياً، وذلك لتغيير الحقيقة فيها، والإدخال مؤداه قيام الجاني بإضافة بيانات جديدة لم تكن موجودة في البيانات الأصلية المعالجة آلياً على نحو يغير من مضمونها، ويترتب عليه آثار قانونية، ومثال ذلك قيام الموظف المختص أو مأمور الضرائب بإضافة أرقام أو كلمات أو حروف إلى البيانات المعالجة آلياً والخاصة بأحد العملاء، بشكل يؤدي إلى زيادة التكاليف الإنتاجية والتي تخصم من الضريبة المستحقة، مما يقلل من المبلغ الضريبي المستحق (زين الدين، 2008، 355)، أما الإتلاف فيتمثل في قيام الجاني بإتلاف بعض البيانات أو المعلومات المختزنة في الحاسب الآلي لتغيير الحقيقة للحصول على مستخرجات غير صحيحة، لاستخدامها في أغراض قانونية، أما المحو أو الطمس فيتمثل في قيام الجاني بمحو بعض البيانات والمعلومات المعالجة آلياً للحصول على مستخرجات غير صحيحة لاستخدامها في أغراض قانونية.

الفرع الثاني: صور التزوير المعلوماتي:

يتخذ التزوير المعلوماتي إحدى الصور التالية:

الصورة الأولى- التلاعب بالمعلومات داخل النظام المعلوماتي لتغيير الحقيقة :

ويتم ذلك عن طريق تعديل هذه المعلومات أو محو جزء أو عدة أجزاء منها، فأما التعديل وكما بينا سابقا فيتم بقيام الجاني بتعديل المعلومات أو المعطيات قبل أو أثناء إدخالها أو في لحظة إخراجها لتغيير الحقيقة والحصول على مستخرجات معلوماتية غير حقيقية،

---

[36] راجع في ذلك باللغة الفرنسية المذكرة التفسيرية لاتفاقية بودابست لمكافحة جرائم الحاسب الآلي في 8 نوفمبر سنة 2001.

كما لو قام الجاني بتغيير البيانات المعالجة آلياً والخاصة بفاتورة الهاتف أو الكهرباء، أو بتغيير البيانات المعالجة آلياً والمنسوخة على الدعامة المغناطيسية للبطاقات الائتمانية، أو تغيير الثقوب التي تدل على بيانات معينة والموجودة على الاسطوانات والديسكات أو غيرها (زين الدين، 2008، 353)، أما المحو فيتم بمحو البيانات المعالجة آلياً أو جزء منها لتغيير الحقيقة والحصول على مستخرجات غير حقيقية، والمثال على ذلك قيام موظفين في أحد المراكز الطبية الألمانية بمحو الحسابات الموجودة في جهاز الحاسوب الخاص بالمركز، لجعلها غير قابلة للتحصيل، وبذلك تمكنوا من اختلاس مبلغ (61.000) دولار، وهي المبالغ المتحصلة والمرسلة من شركات التأمين إلى المركز الطبي (المومني، 2008، 148).

الصورة الثانية- إدخال معلومات مصطنعة (غير صحيحة) إلى النظام المعلوماتي لتغيير الحقيقة:

إن عملية إدخال معلومات مصطنعة قد تتم عن طريق قيام الجاني بادخال بيانات مخالفة للحقيقة إلى النظام المعلوماتي للحصول على حق أو صفة أو ميزة أو مركز قانوني وذلك لإثبات وقائع كاذبة أو غير معترف بها (عقاد، 1993، 202)، والمثال على ذلك ضم مستخدمين غير موجودين بالفعل إلى إحدى المنشآت أو المؤسسات، وعادة يحدث ذلك في المؤسسات أو المنشآت التي تضم فروعا كثيرة ويتغير مستخدموها بحسب الظروف الاقتصادية، فيقوم مدير أحد الفروع بتقديم معلومات وهمية إلى الإدارة المركزية تفيد استئجار مستخدمين مؤقتين، ويقوم هذا المدير بعد ذلك باستلام الشيكات النقدية الخاصة بالمستخدمين الوهميين (الشوا، 1994، 72).

المطلب الثالث: الحماية الجنائية للمعلومات المعالجة آلياً من خطر التزوير المعلوماتي وفقاً للمشرع الأردني:

وفقاً للنصوص التقليدية الخاصة بجريمة التزوير والواردة في قانون العقوبات الأردني فإن هذه الجريمة تقع عن طريق قيام الجاني بتغيير الحقيقة في محرر مكتوب بإحدى الطرق الواردة على سبيل الحصر في ذات القانون، وأن من شأن هذا التغيير إحداث ضرر مع اتجاه نية الجاني لاستعمال المزور فيما أعد له.

ويرى الباحث أنه وعند دراسة جريمة التزوير المعلوماتي فلابد من التفرقة بين أفعال التزوير التي تطال معطيات النظام المعلوماتي والمتمثلة في المعلومات والبيانات المعالجة آلياً عن طريق هذا النظام سواء المخزنة في الحاسب الآلي من ناحية، ومن ناحية أخرى بين مستخرجات الحاسب الآلي سواء أكانت ورقية

عن طريق الطابعة أم الراســم كالمســتند الإلكتروني أم كانت مســتخرجات لا ورقية أو إلكترونية، كالدعامات المادية المثبتة عليها المعلومات، والأشرطة الممغنطة، والأقراص المدمجة وغيرها من الأشــكال غير التقليدية للمحرر المكتوب، والتي يمكن عرضـها بواسطة جهاز الحاسب الآلي على الشاشة الخاصة به أو على الوحدات الطرفية.

حيث يرى الباحث أنه ووفقاً للنصــوص التقليدية في قانون العقوبات الأردني فإنه لا يمكن تطبيقها على حالات التزوير المعلوماتي التي تطال معطيات النظام المعلوماتي من بيانات ومعلومات إلا إذا كانت على شكل مستند إلكتروني باعتباره أحد مستخرجات الحاسب الآلي، كالمستند المستخرج من الآلة الطابعة للجهاز والناتج عن عملية فنية داخل النظام المعلوماتي والذي يكون على صــورة المحرر المكتوب، أما إذا وقع تغيير الحقيقة على مستخرجات الحاسب الآلي الأخرى اللاورقية كالدعامات المادية، والأشرطة الممغنطة، والأقراص المدمجة، فإن هذه المســتخرجات لا تكون على صــورة محرر مكتوب، وبالتالي لا تنطبق عليها النصــوص التقليدية للتزوير، كما وأن تغيير الحقيقة الذي يقع على معطيات النظام المعلوماتي المخزنة في الحاسب الآلي لا يعتبر تزويراً بالمعنى التقليدي.

وتجدر الإشـارة هنا أن الفقه عرف المحرر بأنه "كل مسـطور يتضمن علامات ينتقل بها الفكر لدى النظر إليها من شــخص إلى آخر" (المومني، 2008، 149)، لذلك لا يمكن تطبيق النصــوص التقليدية المتعلقة بالتزوير على المعلومات المعالجة آلياً إلا إذا اتخذت شــكل المســتند الإلكتروني، فبدون ذلك لا تعتبر محرراً مكتوباً ، وكذلك فإن المعلومات والبيانات المعالجة آلياً سواء المخزنة في الحاسب أو التي تعد من مستخرجات الحاســب الآلي وتكون مثبتة على دعامات مادية كالأشرطة الممغنطة لا تعد محرراً مكتوباً، لأنها مســجلة كهرومغناطيســياً على الدعامات المادية، ولا يمكن مشــاهدة المعلومات بالنظر إلى هذه الدعامات إلا عن طريق عرضها على شاشة الحاسب الآلي.

كما وأنه ومن نظر الباحث فإن المشرع الأردني لم يتطرق إلى جريمة التزوير المعلوماتي في ظل قانون الاتصــالات، وقانون المعاملات الإلكترونية، وقانون جرائم أنظمة المعلومات الأردني المؤقت، الأمر الذي يســتدعي تدخل المشــرع لتعديل النصــوص الواردة في قانون العقوبات الأردني لتوفير الحماية الجنائية للمعلومات المعالجة آلياً من خطر التزوير الإلكتروني، أو بالنص على هذه الجريمة في القوانين الجنائية الخاصة.

المطلب الرابع: الحماية الجنائية للمعلومات المعالجة آلياً من خطر التزوير المعلوماتي وفقاً للمشرع الأمريكي والفرنسي:

الفرع الأول: المشرع الأمريكي:

جرم المشرـع الأمريكي في الماده 1029 من القانون الفيدرالي الامريكي لعام 1984 والخاصة بالاحتيال والأنشـطة المتعلقة بالاتصـال مع أدوات الوصـول للحاسب الآلي أفعال التزوير التي تطال معطيات الحاسب الآلي وذلك في الفقره A من البند الثالث[37] ، حيث عاقبت على هذه الأفعال بالحبس لمدة لا تزيد على عشر سنوات أو الغرامة أو بكلتا العقوبتين وذلك وفقا لنص الفقره (C) من ذات المادة والخاصة بالعقوبات[38]

---

[37] Article 1029/A/3 CFAA of 1984

(a) Whoever--

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

[38] Article 1029/C of CFAA of 1984

c) Penalties.--

(1) Generally.--The punishment for an offense under subsection (a) of this section is.--

(A) in the case of an offense that does not occur after a conviction for another offense under this section.--

(i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

(ii) if the offense is under paragraph (4), (5), (8), or (9), of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

ونص المشرع الفيدرالي الأمريكي على حالات تزوير المعلومات من خلال حماية حق النشر والتأليف وذلك في المادة 506/A/1 في الفصل 18 المادة 1030 من القانون الفيدرالي 1994 وذلك عند القيام بتقليد أو استنساخ المنتج أو أي عمل يتمتع بحقوق النشر والتأليف بوسائل الكترونية وتوزيع نسخة أو أكثر تزيد قيمتها على 1000 دولار والحصول على منفعة مادية من بيع المنتج أو لأعمال تجارية أو جعلها متاحة للكافة عبر شبكة الحاسب الآلي [39] .

و يعاقب مرتكب هذه الأفعال بالعقوبات الواردة في الفقرات B,C,D من المادة 2319 من ذات القانون في حال قيامه بنسخ منتجات تتمتع بحق النشر والتأليف وبوسائل إلكترونيه، او قيامه بتوزيع نسخه أو أكثر من تلك المنتجات أو التسجيلات[40]

---

[39] Article 506/A of US Copyright Act(a) Criminal Infringement.—
(1) In general.—Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed—
(A) for purposes of commercial advantage or private financial gain;
(B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or
(C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distributio

[40] 18 U.S.C.$ 2319 :US code- section 2319 :Criminal infringement of acopyright.
(a) Any person who violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b), (c), and (d) and such penalties shall be in addition to any other provisions of title 17 or any other law. (b) Any person who commits an offense under section 506(a)(1)(A) of title 17 -
(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;
(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.
(c) Any person who commits an offense under section 506(a)(1)(B) of title 17 -

كما ونص على التزوير الـذي يقع على بطـاقة الدفع الإلكتروني في الفصـــل (41) من ذات القانون، والذي يأتي تحت عنوان حماية ائتمان المســـتهلك، وذلك في البند (1644) وهو الاســـتخدام غير المشرـــوع لبطاقات الدفع الإلكتروني (سليمان، لات، 98 وما بعدها).

---

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;
(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.
(d) Any person who commits an offense under section 506(a)(1)(C) of title 17 -
(1) shall be imprisoned not more than 3 years, fined under this title, or both;
(2) shall be imprisoned not more than 5 years, fined under this title, or both, if the offense was committed for purposes of commercial advantage or private financial gain;
(3) shall be imprisoned not more than 6 years, fined under this title, or both, if the offense is a second or subsequent offense;
and
(4) shall be imprisoned not more than 10 years, fined under this title, or both, if the offense is a second or subsequent offense under paragraph (2). (e)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.
(2) Persons permitted to submit victim impact statements shall include -
(A) producers and sellers of legitimate works affected by conduct involved in the offense;
(B) holders of intellectual property rights in such works; and
(C) the legal representatives of such producers, sellers, and holders.
(f) As used in this section -
(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17;
(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17;
(3) the term "financial gain" has the meaning given the term in section 101 of title 17; and
(4) the term "work being prepared for commercial distribution" has the meaning given the term in section 506(a) of title 17.

أما بالنسبة لتشريع الولايات فقد نصت ولاية فلوريدا على جريمة التزوير في قسم الجرائم ضد معدات الكمبيوتر وتجهيزاته، وذلك في المادة الأولى والخاصة بمعدات الكمبيوتر وتجهيزاته والمعروفة باسم أسلوب الهندسة المعكوسة، حيث جرمت هذه المادة أفعال التعديل غير المصرح به التي تطال معدات وتجهيزات الحاسب الآلي أو النظام المعلوماتي أو شبكة الحاسب الآلي واعتبرتها جنحة من الدرجة الأولى .(Smith, and Hogan, 1995, p.220)

الفرع الثاني: المشرع الفرنسي:

نص قانون العقوبات الفرنسي الجديد والمعمول به منذ عام 1994 في الفصل الأول من الباب الرابع والخاص بالتزوير وذلك في المادة (1/441) على أنه "يعتبر تزويرا كل تغيير تدليسي للحقيقة يكون من طبيعته أن يسبب ضررا، ويتم بأية وسيلة مهما كانت في محرر أو أي سند للتعبير عن الرأي، والذي يكون أو من الممكن أن يكون له أثر في إنشاء دليل على حق، أو فعل تكون له نتائج قانونية" وقد عاقب المشرع الفرنسي على التزوير واستخدام المحرر بعقوبة الحبس لمدة ثلاث سنوات وغرامة 45000 يورو [41] " .
(http://www.lawjo.net/vb/showthread.php?17807).

وفي الفقرة الثانية من ذات المادة (441-2) ، "شدد المشرع الفرنسي العقوبة لتصل إلى الحبس لمدة خمس سنوات والغرامة 75000 يورو عندما يقع التزوير على وثيقة سلمت من قبل الهيئة العامة لغرض إقامة الحق، كالهوية أو منح ترخيص معين، كما وأن استعمال المزور يخضع إلى نفس العقوبة .

---

[41] Article 441/1 Of (CPF)

Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende.

وشـدد العقوبة لتصـل إلى سـبع سـنوات وغرامة مقدارها 100000 يورو في حال وقوع التزوير من قبـل الموظف العام، أو شـــخص يعمل في ســـلطة عامة، أو في حال الإعتياد او التكرار، أو إذا ارتكب فعل التزوير بقصد تسهيل ارتكاب جناية، أو لتسهيل إفلات المجرم (مرتكب جريمة معينة) من العقاب [42]".

وفي المادة 441-3 جرم المشـرــع الفرنسيــ " فعل حيازة أي من الوثائق المزورة التي حددتها المادة 441-2، وعاقب على ذلك بالحبس لمدة سـنتين وغرامة 30000 يورو، وشـدد العقوبة لتصل إلى السجن لمدة خمس سنوات وغرامة مقدارها 75000 يورو عند حيازة أكثر من وثيقة مزورة بطريقة غير قانونية [43] ".

ونصـــت المادة 441-9 على" أن الشـرـوع في الجنح المشـار إليها في المواد 441-1، 441-2، 441-4، 441-8 يخضع إلى نفس العقوبات الواردة فيها [44] "

---

[42]Article 441/2 Ofa (FCP)

Le faux commis dans un document délivré par une administration publique aux fins de constater un droit, une identité ou une qualité ou d'accorder une autorisation est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

L'usage du faux mentionné à l'alinéa précédent est puni des mêmes peines.

Les peines sont portées à sept ans d'emprisonnement et à 100000 euros d'amende lorsque le faux ou l'usage de faux est commis :

1° Soit par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public agissant dans l'exercice de ses fonctions ;

2° Soit de manière habituelle ;

3° Soit dans le dessein de faciliter la commission d'un crime ou de procurer l'impunité à son auteur.

[43] Article 441/3 Of (FCP)

La détention frauduleuse de l'un des faux documents définis à l'article 441-2 est punie de deux ans d'emprisonnement et de 30000 euros d'amende.

La peine est portée à cinq ans d'emprisonnement et à 75000 euros d'amende en cas de détention frauduleuse de plusieurs faux documents

[44] Article 441/9 Of (FCP)

ونصت المادة 441-10 على "عقوبات إضافية على الأشخاص الطبيعيين المدانين في الجنايات والجنح الواردة في هذا الفصل وهي كما يلي:

1- المصادرة المدنية وفقاً للشروط المنصوص عليها بموجب المادة 131-26.

2- منعهم من شغل الوظائف العامة، أو إجراء نشاط اجتماعي أو مهني وفقاً لشروط المادة 131-27.

3- الاستبعاد من المناقصات العامة.

4- مصادرة الأشياء أو الأدوات المُعدة أو المستخدمة في ارتكاب الجريمة، أو المتحصلة من الجريمة، باستثناء الأشياء الخاضعة إلى التعويض [45] ".

ونصت المادة 441-12 "على مسؤولية الأشخاص المعنوية عن هذه الجرائم عن الجرائم المشار اليها في إطار هذا الفصل وفقاً للشروط المنصوص عليها بموجب المادة 121/2من ذات القانون وحددت العقوبات التي توقع عليهم وهي وفقا للنص كما يلي :

1-الغرامات المالية وفقا لأحكام المادة 131-38

La tentative des délits prévus aux articles 441-1, 441-2 et 441-4 à 441-8 est punie des mêmes peines.

[45] Article 441/10 Of (FCP)
Les personnes physiques coupables des crimes et délits prévus au présent chapitre encourent également les peines suivantes :

1° L'interdiction des droits civiques, civils et de famille suivant les modalités prévues par l'article 131-26 ;

2° L'interdiction d'exercer une fonction publique ou une activité de nature professionnelle ou sociale selon les modalités prévues par l'article 131-27 ;

3° L'exclusion des marchés publics ; 4° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.

2-العقوبات المنصوص عليها في المادة 131-39 ، والحظر المشار اليه في الفقره 2 من ذات المادة [46] ".

وقـانون العقوبات الفرنسيـــ لم يجعل جريمة التزوير قاصرة على المحررات بمعناها التقليدي، وإنما مدها لتشمل مخرجات الحاسب الآلي والوثيقة المعلوماتية مع اشتراطه أن يتضمن ذلك تغييراً للحقيقة، وأن يسـبب ضرراً ، وأن يقع على محرر أو سـند مثبت لحق، أو معد لترتيب آثاراً قانونية معينة (حجازي، 2004، 164).

فالمشرـع الفرنسيـ توسـع في مفهوم المحرر بحيث شـمل كل وسـيط آخر للتعبير عن فكره، وبذلك فقد شـمل الدعامات المادية والأقراص الممغنطة والاسـطوانات المدمجة بالحماية الجنائية من خطر التزوير المعلوماتي (المومني، 2008، 150).

لما تقدم يرى الباحث أن المشرـع الفرنسيـ قد شـمل التزوير التقليدي بالحماية الجنائية، وأضـفى أيضـاً هذه الحماية على المعلومات المعالجة آلياً والمخزنة في ذاكرة الحاسـب الآلي، أو المسـتخرجة من النظام المعلوماتي، أو المثبتة على الدعامات المادية، وكذلك لم يحدد طرق التزوير على سـبيل الحصرـ وذلك لإضـفاء الحماية اللازمة على المعلومات المعالجة آلياً.

المبحث الثالث: الجرائم التي تهدد المعلومات المعالجة آلياً والخاصـة بالمصـالح القومية للدول والسـلامة الشخصية للأفراد (الخصوصية):

---

[46] Article 441/12 Of (FCP)
Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38 ;

2° Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

باتت المعلومات المعالجة آليا والخاصة بالدول أو الأفراد من أخطر المعلومات التي يمكن أن يطالها الاعتداء بالطرق التقنية، وذلك لما تتمتع به من طابع السرية والشخصية في مواجهة الجميع من غير أصحاب الشـــأن، فلم تعد الدول في منأى عن الاعتداءات التي تطال المعلومات والبيانات الخاصـــة بإســـتراتيجياتها العسـكرية وسـياسـاتها العليا ومنظومتها الاقتصادية، وفي عصر المعلومات ومع وجود التقنيات عالية التقدم أصـبحت حدود الدول مسـتباحة بأقمار التجسـس والبث الفضـائي واختراق الأنظمة المعلوماتية، في الوقت الذي عجزت فيه الوسـائل الأمنية المسـتخدمة في حماية الشـبكات الخاصـة بالمؤسسات والهيئات الحكومية من السـيطرة على هـذه الاختراقـات الأمنية، وكذلك الأمر لم يعد الأفراد يأمنون على حياتهم الخاصـــة من الانتهاك ضـمن المنظومة المعلوماتية، وذلك وفقاً للطرق المستحدثة والأساليب التقنية للاعتداء على البيانات الاسمية المتعلقة بحياتهم الخاصة عبر النظام المعلوماتي.

لذلك فسوف نتناول في هذا المبحث جريمة التجسس المعلوماتي، وجريمة الاعتداء على حرمة الحياة الخاصة في نطاق النظام المعلوماتي وذلك كما يلي :

المطلب الأول: التجسس المعلوماتي:

شـهد العالم المعاصر تغييراً كبيراً في مفهوم التجسـس على أثر ثورة المعلومات الكبرى التي تمخضـت عن ميلاد عصرـ جديد، وهو ما يعرف بعصرـ المعلومات المعاصر، فالمفهوم التقليدي للتجســس ولكســب الحروب والذي كان ســائداً في الماضي أصــبح يتلاشى مع ظهور التكنولوجيا الرقمية، وما عادت الأســاليب التقليدية تجدي نفعاً لمن يسـتخدمها في هذا العصر، وفي الوقت الذي كانت فيه عمليات التجسس ترتكز في الماضي على المعلومات الإسـتراتيجية العسـكرية البحتة، فقد أصـبحت الآن تتسـع لتشمل أنماطاً متعددة من المعلومات المتعلقة بالجوانب الصـناعية والتقنية والمالية والتجارية للمؤسـسات الاقتصادية في الدول، إضافة إلى الجوانب العسـكرية والإسـتراتيجية الأمنية والسياسية في منظومة تلك الدول، كما وأن عمليات التجسس في المـاضي كـانـت تتطلـب الوصـــول إلى الحيز المكـاني الذي تحفظ فيه الملفات والمعلومات المتعلقة بأسرار الـدولـة، ســـواء تم ذلـك بطريقة مباشرة من قبل الشـــخص المعني بذلك أم بطريقة غير مباشرة من خلال العاملين في ذلك المكان، ومع ظهور التقنيات الحديثة لتكنولوجيا المعلومات

فقد أصبحت المعلومات المتعلقة بأسرار الدولة سواء السياسية أو العسكرية أو الاقتصادية والمالية والتجارية والصناعية وغيرها تُجمع وتنقل وتعالج آلياً ومن ثم تخزن في ذاكرة الحواسيب الآلية وذلك لاسترجاعها عند الحاجة لاستخدامها وبسرعة فائقة دون أن تأخذ حيزاً مكانياً أو جهداً كما في السابق، وهذا الأمر خلق بيئة خصبة للتجسس المعلوماتي في نطاق الأنظمة المعلوماتية والحاسب الآلي وشبكة الإنترنت، ولا شك أن التقدم الكبير الذي لحق بالاتصالات والأنظمة المعلوماتية قد أسفر عن إيجاد وسائل أكثر فاعلية للتجسس، وهو ما أسفر بدوره عن ظهور ما يسمى بالتجسس المعلوماتي الذي يقع في نظام المعالجة الآلية للبيانات وفي بيئة الحاسوب وشبكة الإنترنت.

وعملية التجسس المعلوماتي أو الاختراق التجسسي- تتيح للشخص المتجسس (الهاكر) أن ينقل أو يمسح أو يضيف ملفات أو برامج كما أن بإمكانه أن يتحكم في نظام التشغيل لجهاز الضحية فيقوم بإصدار أوامر، وذلك باستخدام برامج معينة تساعده على ارتكاب جريمته والتي من أشهرها (Web Cracker 4)، (Net Buster)، (Netbus Haxport)، (Net Bus 1.7).

وتجدر الإشارة هنا إلى ضرورة التمييز بين الحصول غير المشروع على المعلومات وبين التجسس المعلوماتي، فالأول يتعلق بالمعلومات المعالجة آلياً وبصفة عامة بصرف النظر عن طبيعتها، أما التجسس المعلوماتي فهو يتعلق بالمعلومات الصناعية والتجارية والاقتصادية المعالجة آلياً والخاصة بالمؤسسات الاقتصادية المختلفة، والمعلومات السياسية والعسكرية الخاصة بالدولة (قوره، 2005، 274).

وبناء على ما تقدم فإن موضوع التجسس المعلوماتي يستدعي بيان طبيعة البيانات والمعلومات المعالجة آلياً والمستهدفة في هذه الجريمة، والوسائل المستخدمة في التجسس المعلوماتي، والوسائل التقنية المستحدثة لحماية البيانات والمعلومات من خطر التجسس المعلوماتي، وأخيراً موقف المشرع الأردني والتشريع المقارن من هذه الجريمة، ومدى الحماية الجنائية التي وفرها كل منها للمعلومات المعالجة آلياً من أخطار التجسس المعلوماتي

الفرع الأول: البيانات والمعلومات المعالجة آلياً والمستهدفة في جريمة التجسس المعلوماتي:

يؤكد أحد الخبراء في مجال الحرب بأن الحرب في أيامنا هذه قد أصـبحت "حرباً كلية وهناك ثلاثة خطوط رئيسـة تدور حولها المعلومات: فهناك المعلومات السـياسـية، والمعلومات العسـكرية، والمعلومات الاقتصـادية، ولا يمكننا تمييز هذه المعلومات عن بعضـها فكلها معلومات حيوية يجب أن تحصـل عليها من البلاد المعادية قبل وأثناء القتال لتتضح لنا صورة عن قوة العدو"[47] (عفيفي، لات، 306).

لذلك تتعدد وتتنوع المعلومات التي قد تكون محلاً لجريمة التجسـس المعلوماتي، هذه المعلومات التي تكون على درجة عالية من الخطورة فيما لو حصلت عليها الدول المعادية، فالمفهوم التقليدي للتجسس ولكسـب الحروب الذي كان سـائداً في الماضي أصـبح يتلاشى في عصرـ العولمة وظهور تكنولوجيا المعلومات، فالترسـانة العسـكرية لم تعد لوحدها هي التي تشـكل معيار التفوق في الحروب كما في الماضي، وأعمال التجسس لم تعد تقتصر على المعلومات العسكرية لوحدها، ولذلك فإن المعلومات التي يمكن أن تكون هدفا للتجسس المعلوماتي تتمثل فيما يلي:

أولا- المعلومات الاقتصادية:

يقصـد بالمعلومات الاقتصـادية التي يمكن أن تكون محلاً للاعتداء هي "تلك المعلومات التي ترتبط بالاقتصـاد القومي من حقائق وبيانات وأخبار تتعلق بالأمن الاقتصـادي في الدولة" (يونس، 2004، 669)، ويدخل في ذلك أيضا التدابير السرية التي تتخذها الدولة للإفلات سراً من حصار اقتصادي مفروض عليها، أو لمنع تدخل الوسـطاء، أو كبح نشـاط السـوق السـوداء، أو تفعيل أو تقليص نشـاط السـوق الموازي في دول الاقتصاد الموجه (يونس، 2004، 670).

وفي الواقع يعتبر الاقتصـاد من العوامل الأسـاسـية التي تُبنى عليها سـيادة الدولة، والعلاقة طردية بينهما فكلما زاد اقتصاد الدولة وقوي، كلما ارتقت إلى مرتبة أعلى من السيادة والأمن القومي، وهذا ينعكس بالإيجاب على مواطني تلك الدولة.

---

[47] راجع العقيد/ أورسـت بنتو، مكافحة الجاسوسية، ترجمة: حميد الرشيد، عرض وتحليل لواء دكتور/ أحمد ضـياء الدين خليل، مقدم/ أشـرف محمد عبد المنعم، المنشـور بمجلة كلية الشرطة، العدد 11، يوليو 1997، ص70، ومشار إليه لدى عفيفي، لات، 306.

وتهدف أعمال التجسس المعلوماتي التي تطال المعلومات الصناعية والتجارية والمالية إلى معرفة الثغرات الاقتصادية في دولة معينة، والتعرف على مواطن الضعف في تشكيلتها الاقتصادية، وكذلك التفوق عليها اقتصادياً، وقد يتم التجسس على المستوى الدولي، أو على المستوى الداخلي للمنافسة بين المؤسسات الاقتصادية التابعة لذات الدولة (المومني، 2008، 213).

ويستهدف التجسس الذي يقع في نطاق الأعمال التجارية الحصول على الأسرار الخاصة بالتسويق والحسابات المالية التابعة للمؤسسة المستهدفة من عملية التجسس، وذلك من خلال الإطلاع على الحسابات الخاصة بالتكلفة، وكشوفات الميزانية للمؤسسة، وأحوال الأسواق والعناوين الخاصة بالعملاء (الشاذلي، فتوح وعفيفي، 2003، 329).

أما التجسس في مجال الأنشطة الصناعية فيهدف إلى الحصول على أسرار العملية الإنتاجية وتطويرها من خلال التوصل إلى الأبحاث العلمية الخاصة بتطوير هذه العملية، ولذلك تسعى المؤسسات الصناعية أو الدول دائماً إلى الحصول على الأبحاث العلمية والأسرار الخاصة بتطوير عملية الإنتاج، وذلك لتوفير الوقت والمال والحصول على أفضل عملية إنتاج صناعي دون تحمل الأعباء المالية، والمثال على ذلك التطور الذي طرأ على صناعة برامج الحاسوب، وما تتكلفه الشركات الصانعة من تكلفة باهظة وميزانية مالية عالية عند صناعة وتطوير مثل هذه البرامج، الأمر الذي يحفز الشركات المنافسة على التجسس على آخر التطورات في مجال صناعة هذه البرامج وتطويرها، وذلك بهدف منافسة الشركة الصانعة وإعداد نفس البرامج، أو لمجرد الإطلاع على آخر ما توصلت إليه هذه الشركات من برامج معدة للحاسوب (قوره، 2005، 273).

ومن الأمثلة التطبيقية على ذلك قيام وكالة المخابرات الأمريكية CIA ووكالة التحقيقات الفيدرالية FBI بإلقاء القبض على عملاء فرنسيين بعد اتهامهم بالتجسس على إحدى أكبر الشركات الأمريكية في مجال صناعة برامج الحاسوب (عفيفي، لات، 310).

ثانيا- المعلومات السياسية والعسكرية:

يعتبر التجسس المعلوماتي الذي يطال المعلومات السياسية والعسكرية من أخطر أنواع التجسس، وذلك لما تشكله هذه المعلومات من معان لسياسات الدول وخططها الأمنية والإستراتيجية والعسكرية، فهي موضع اهتمام الدول لمعرفة مواطن الضعف والقوة لدى الدول الأخرى.

فالمعلومات السياسية تبين السياسة العليا للدولة والأمن القومي فيها، والتي تطبق من قبل أجهزة الدولة والممثلة في الوزارات أو الهيئات أو المؤسسات السياسية أو الدبلوماسية أو الحربية أو الدينية أو غيرها (يونس، 2004، 667 وما بعدها)، أما المعلومات العسكرية فهي تضم النظم الأمنية والخطط والتدابير العسكرية والأجهزة الاستخبارية والمشروعات النووية، وصناعات الأسلحة وغيرها من الأمور المتعلقة بالنظام الأمني والإستراتيجي للدولة (سلامة، 2006، 147)، ولذلك يهدف التجسس المعلوماتي في هذا المجال إلى الوصول إلى تفاصيل أسرار البيانات والمعلومات المتعلقة بتلك الشؤون، الأمر الذي يكون له بالغ الأثر على أمن وبقاء الدول والحكومات (سلامة، 2006، 147).

ومن الأمثلة التطبيقية على ذلك ما جاء في كتاب صدر في باريس تحت عنوان "عين واشنطن" مؤلفاه صحفيان فرنسيان، حيث كشف عن فضيحة تورط جهازي المخابرات الأمريكية والإسرائيلية في اختراق جميع أجهزة الحاسب الآلي الموجودة في دول العالم، حيث يمكنها التقاط كافة المعلومات المسجلة على هذه الأجهزة سواء العسكرية أو غيرها، وأشار الكتاب أن هناك اتفاقاً بين الولايات المتحدة وإسرائيل على أن يتم تصميم برنامج معلوماتي معين تبيعه الولايات المتحدة لخصوم إسرائيل وأعدائها مقابل قيام إسرائيل ببيع هذا البرنامج لخصوم الولايات المتحدة وأعدائها، وهذا البرنامج مصمم للتجسس المعلوماتي[48] (عفيفي، لات، 311).

ومن الأمثلة الأخرى أيضاً في الولايات المتحدة الأمريكية، تمكن صبي لم يتجاوز الثالثة عشرة من عمره، من اختراق أحد مراكز البحوث الأمريكية والذي يوفر للجيوش الأمريكية التقنيات الضرورية التي تضمن تفوقه في حروب المستقبل (http//www.atsdp.com).

قد تقوم الدولة في بعض الأحيان بعملية جمع وتخزين مجموعة من البيانات والمعلومات الخاصة بالإحصاءات السكانية والاجتماعية، ومن ثم تتم معالجتها آلياً وتخزينها في ذاكرة الحواسيب الآلية التابعة لجهات الدولة المختصة بذلك تمهيداً لاستخدامها في الغرض الذي جمعت من أجله، إلا أنه قد يتم الاعتداء على هذه المعلومات بالتجسس من قبل جهات داخلية في الدولة ولأغراض خاصة، ومن قبل جهات خارجية كالدول المعادية، ذلك بهدف التعرف على التركيبة السكانية والأعداد الإحصائية للسكان والوضع الاجتماعي وغيرها من المعلومات التي قد تهم الدول المعادية في تحقيق أغراضها العدائية.

---

[48] وقد أكد مؤلفا الكتاب الصحفي خابرو كالفي والصحفي تيري بيبيستيه – إن إسرائيل أثناء فترة الانتفاضة الفلسطينية أرادت أن تحصل على كل المعلومات المخزنة لدى الأردن عن الفلسطينيين، فاتفقت مع شركة أمريكية على أن تبيع برنامج معلومات للأردن معد للتجسس على كل المعلومات الموجودة لديها بسهولة عن الفلسطينيين والأرض المحتلة ونقلها إلى إسرائيل، مشار إليه لدى (عفيفي، لات، 311–312).

ومن الأمثلة التطبيقية على التجسس الم علوماتي في هذا المجال قيام موظفَين من العاملين في مركز حاسوب في السويد بنسخ برامج مسجلة عليها إحصاءات وبيانات سكانية، وبعد ذلك قاما ببيعها إلى أحد المكاتب الخاصة بالإحصاءات والبيانات لأغراض استهلاكية مقابل ثمن رخيص (الشاذلي، فتوح وعفيفي، 2003، 332).

الفرع الثاني: الوسائل التقنية المستخدمة في التجسس المعلوماتي:

هناك وسائل تقنية متعددة تستخدم في التجسس ألمعلوماتي وذلك كما يلي:

(1) استعمال تقنية أبواب المصيدة أو الأبواب الخفية أو الخلفية:

وهذه التقنية تستخدم للتجسس على المعلومات المخزنة في الحاسب الآلي، وتقوم على ترك ثغرات تسمح بالدخول إلى البرنامج مرة أخرى عند إعداده وذلك لتلافي ما قد ترد فيه من أخطاء، وهذه الثغرات من المفروض أن يتم إلغاؤها في النسخة النهائية للبرنامج، إلا أنه قد يتم تركها بشكل مُتعمّد وبذلك يستطيع أي شخص إذا ما وجد هذه الأبواب والثغرات أن يتوصل إلى بيانات الحاسب الآلي (الشاذلي، فتوح وعفيفي، 2003، 333).

(2) استعمال هوائيات وربطها بحاسوب خاص:

وهذه التقنية من أخطر الطرق التي تستخدم للتجسس على المعلومات المخزنة في الحاسب الآلي، ولذلك يمكن عن طريق هذه الهوائيات التقاط الموجات الكهرومغناطيسية ذات الترددات العالية والمنبعثة عن الحاسوب خلال فترة تشغيله، مع إمكانية تسجيلها ومن ثم معالجتها وترجمتها إلى معلومات واضحة، ولابد من الإشارة هنا أنه يمكن أن يتم التقاط المعلومات من مسافة تزيد على مئات الأقدام من الحاسوب المستهدف، وذلك بتكبيرها باستخدام أجهزة خاصة أعدت لهذا الغرض (السرحان، سرحان والمشهداني، 2001، 123).

(3) اعتراض المعلومات والبيانات المتداولة عبر شبكة المعلومات:

وهذه التقنية تستخدم للتجسس على المعلومات المتداولة عبر الشبكة المعلوماتية، وبهذه الطريقة يمكن جمع المعلومات عن بعد عن طريق التقاط الجاني للموجات الكهربائية الصادرة عن جهاز المجني عليه بطريقة تقنية، ومثال ذلك قيام الجاني بالتقاط وجمع معلومات مرسلة خلال نظام حاسوبي موجود داخل مبنى معين، وذلك عن طريق استعماله شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى، بحيث يقوم بالتقاط الموجات الكهربائية المحيطة بالحاسوب وتحويلها إلى معلومات مقروءة على الشاشة، ومن ثم تسجيلها (المومني، 2008، 217).

كما يمكن اعتراض الاتصالات التي تتم بين المحطات الأرضية والأقمار الصناعية أي بين نهاية طرفيه وأخرى وترجمة ما ينتج عنها من إشعاعات إلى معلومات واضحة قد تكون غاية في الأهمية، وقد تكون هذه الموجات قصيرة ناتجة عن وصلات محدودة أرضية وقد تكون طويلة ناتجة عن الأقمار الصناعية. (سليمان، لات، 156)، ويستخدم في هذه الطريقة أجهزة التقاط خاملة لا تصدر أية إشارات لاسلكية لاعتراض وصلات الموجات القصيرة التي تحتوي على البيانات والمعلومات (الشاذلي، فتوح وعفيفي، 2003، 334).

(4) التوصيل المباشر على خط تلفون:

وهذه الطريقة تستخدم للتجسس على البيانات في حال انتقالها بين نهاية طرفيه وأخرى، وتقوم هذه الطريقة بوضع مركز تنصت يسهل تسجيل كل الاتصالات، ويمكن أن تؤدي هذه الوظيفة ميكروفونات صغيرة (الشوا، 1994، 69)، ويستعمل في هذه الطريقة أجهزة إلكترونية بسيطة لالتقاط البيانات المنقولة عن طريق الأسلاك المعدنية أو خطوط أجهزة الالتقاط للهاتف ولأنظمة الاتصالات، وتثبيتها بطريقة خفية داخل صناديق التوزيع التي تنتهي إليها معظم وسائل الاتصال السلكية واللاسلكية، ويمكن إضافة جهاز حث إلى أجهزة الالتقاط حتى لا تعمل إلا في حالة وجود بيانات ومعلومات مستهدفة (عفيفي، لات، 214).

(5) إصابة جهاز الحاسوب الخاص بالمجني عليه بملف التجسس:

وتستخدم هذه الطريقة التقنية للتجسس من خلال شبكة الإنترنت، بحيث يقوم الجاني بإرسال ملف التجسس عبر الشبكة إلى جهاز المجني عليه، وعند إصابة هذا الأخير بملف التجسس فإنه يقوم على الفور بفتح أحد المنافذ في جهازه، وهذا هو الباب الخلفي لحدوث اتصال بين جهاز المجني عليه وجهاز المخترق، ويسمى الملف الذي يكون لدى المجني عليه بالخادم، بينما يسمى الجزء الآخر والذي يكون لدى الجاني بالعميل، ومن خلاله يمكن للجاني المخترق أن يسيطر على جهاز المجني عليه دون أن يشعر بذلك (الطائي، 2007، 199).

ويستطيع المخترق هنا فتح القرص الصلب لجهاز المجني عليه والعبث به كما يشاء سواء بحذف أو بإضافة ملفات جديدة، ويستطيع أيضاً التوصل لمعرفة كلمات السر المخزنة في الجهاز بداية من اشتراك الإنترنت وحتى رقم بطاقة الائتمان الخاصة بالمجني عليه، ويستطيع المخترق أيضاً إذا كان لدى المجني عليه ميكروفون أو كاميرا أن يستمع ويرى كل ما يفعله المجني عليه في المساحة التي يغطيها الميكروفون أو الكاميرا (الطائي، 2007، 199).

وتجدر الإشـــارة هنا أنه يتم إدخال ملف التجســـس إلى جهاز المجني عليه عن طريق ثلاث طرق وهي كما يلي:

الطريقـة الأولى: عن طريق برامج المحـادثـة عبر شـــبكـة الإنترنت، حيث يقوم الجاني أو الجهة القائمة على التجســس بإرســال ملف للمجني عليه ويؤكد له أنه يحتوي على ألعاب مثيرة أو أمور تهمة أو أية إغراءات أخرى فينخدع المجني عليه ويقوم باستقبال الملف.

الطريقة الثانية: عن طريق البريد الإلكتروني للمجني عليه، وذلك بأن يقوم الجاني بإرســال رســالة إلكترونية إلى المجني عليه ويقوم الأخير بفتحها وإذا هي تحتوي على ملفات ملحقة تحمل برنامج التجسس (المومني، 2008، 219).

الطريقـة الثـالثـة: عنـد زيـارة الشـــخص المجني عليـه لمواقع مجهولة تغريه بتنزيل بعض البرامج والملفات المجانية ومن ضمنها ملف التجسس (الطائي، 2007، 199).

الفرع الثالث: الوسائل الفنية المستحدثة لحماية البيانات والمعلومات المعالجة آلياً من أخطار التجسس:

لجـأ المختصـــون في مجال أنظمة وتكنولوجيا المعلومات إلى خلق أنظمة وأســـاليب فنية من أجل تحقيق الحماية للبيانات والمعلومات من مخاطر التجسس وذلك كما يلي:

(1) استخدام كلمة السر:

وكلمة السر عبارة عن "رقم رمزي لا يتيح التعامل مع نظام الحاسب الآلي سواء من نهاية طرفيه معينة أو لإدخال بيانات معينة إلا بذكرها، وتتكون هذه الكلمة من حروف أو أرقام توصـف بصورة عشـوائية" (الشاذلي، فتوح وعفيفي، 2003، 335)، وينصح الخبراء بتنزيل كلمات السر بصورة دورية لتجنب كشـفها من الآخرين، وأن تتألف هذه الكلمة من خمسـة أحرف على الأقل، ويفضـل عدم اختيارها من بين الكلمات المعهودة، وإخفائها في مكان لا يجده الآخرون، ويفضل أيضا عدم استعمال كلمة السر القديمة قبل مرور سنة على الأقل (الشاذلي، فتوح وعفيفي، 2003، 335)، إلا أنه ومع ذلك فهناك العديد من البرامج التي تسـاعد على كشـف كلمة السرـ مثلما تسـاعد هذه البرامج على اسـتعادة كلمة السرـ المنسـية أو تخفيف الأضرار في حالة تعمد إغلاق الملفات بكلمات سر، فهناك العديد من الشرـكات التي تعنى بكسرـــ الحماية وابتكار طرق وأدوات اختراق جديدة دائماً (موسى، 2006، 169 وما بعدها).

(2) استخدام أجهزة التشويش الإلكتروني:

وتقوم هـذه الأجهزة بالتشـــويش الإلكتروني على الاتصـــالات الهاتفية والبيانية، بحيث تحولها إلى تداخلات غير مفهومة ولا يمكن فكها إلا بكود خاص (المومني، 2008، 220).

(3) تشفير البيانات:

ويقصـــد بتشـــفير البيـانـات "كتـابتهـا برموز سرية بحيث يتعذر على كل من لا يحوز مفتاح تلك الشـيفرة أن يفهمها وأن يخترق الشبكة المعلوماتية" (شتا، 2001، 95 وما بعدها)، إلا أن جميع نظم التشفير يمكن حلها في زمن طال أم قصر- حسـبما يقتضـيه طول أو قصر المفتاح المستخدم في الشيفرة (عفيفي، لات، 317).

(4) استعمال أجهزة القياس الحيوي أو الأجهزة البيومترية:

وهذه الأجهزة تستخدم في النظام المعلوماتي وتتضمن الخصائص العضوية والطبيعية التي ينفرد بها الشخص عن غيره للتحقق من هويته، مثل بصمات الأصابع والأوعية الدموية المغذية لشبكة العين، أو شكل ومقاسـات الكف، أو التوقيع، أو تحليل نبرات الصـوت وغيرها، وتعمل هذه الأجهزة على قصر- التوصـل إلى نظام الحاســوب فقط على الأشــخاص المصرــح لهم بالدخول إلى النظام بعد التعرف عليهم بواســطة هذه الأجهزة (شتا، 2001، 96).

الفرع الرابع: الحمايـة الجنائية للمعلومات المعالجة آلياً من أخطار التجســس المعلوماتي وفقاً للتشرــيع الأردني والتشريع المقارن:

أولا- الحماية الجنائية للمعلومات المعالجة آلياً من أخطار التجسس المعلوماتي وفقاً للمشرع الأردني:

نص المشرــع الأردني على جريمة التجســس في قانون حماية أسرار ووثائق الدولة رقم (50) لســنة (1971) وقد عرفت المادة الثانية من ذات القانون الأسرار والوثائق المحمية بأنها "أية معلومات شــفوية أو وثيقة مكتوبة أو مطبوعة أو مختزلة أو ورق مشـمع أو ناسخ أو أشرطة تسجيل أو الصور الشمسية والأفلام أو المخططات أو الرسوم أو الخرائط أو ما يشابهها والمصنفة وفق أحكام هذا القانون".

وقد بين المشرــع الأردني في المواد (3، 6، 8) من ذات القانون طبيعة المعلومات التي تشـكل أسراراً والتي لا يجوز المسـاس بها نظراً لخطورتها وأهميتها، وتدرجت من درجة سري للغاية، سري، ولغاية محدود، سـواء تعلقت بالمعلومات العسـكرية والسـياسـية أو الاقتصـادية والمالية والصـناعية والتجارية على اختلاف درجاتها.

كما وبين المشرع في المواد (12-16) الأفعال التي تشكل سلوكاً إجرامياً ترتكب فيه جريمة التجسس.

ويرى الباحث باستقراء هذه النصوص السابقة بأنه لا يمكن تطبيقها في مجال التجسس المعلوماتي، فعلى الرغم من أن المادة الثانية من هذا القانون قد جاءت بتعريف واسع وفضفاض للأسرار والوثائق المحمية بأن شملت المعلومات والوثائق المختزلة، إلا أن السلوك المادي اللازم لارتكاب جريمة التجسس التقليدية وفقاً لهذا القانون بعيد كل البعد عن النشاط الرقمي المتمثل في استخدام أساليب التقنية الحديثة في التجسس المعلوماتي، ففي المفهوم التقليدي يتحقق السلوك بالوصول إلى مركز ومكان هذه المعلومات والبيانات بطريق مباشر والحصول عليها، أما في المفهوم المعلوماتي فبالإمكان الحصول هذه المعلومات والبيانات من خلال التقنيات الرقمية ومن أبعد المسافات ودون الوصول المكاني إليها وذلك باستخدام الحاسوب والإنترنت، وتطبيقاً لمبدأ شرعية الجرائم والعقوبات، ولحظر القياس في مواد القانون الجنائي فإن الباحث يرى أنه لا يمكن تطويع نصوص هذه المواد لتشمل في طياتها التجسس المعلوماتي القائم على التكنولوجيا الرقمية.

وكذلك فإن المشرع الأردني لم ينص صراحة على جريمة التجسس المعلوماتي في المادة (11) من قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010 إلا أنه وفَّر الحماية الجنائية للبيانات والمعلومات المعالجة آلياً والتي تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني وذلك في محاولةً منه لمواكبة التكنولوجيا الرقمية وسد الثغرات التي يحتويها قانون حماية أسرار ووثائق الدولة رقم (50) لسنة1971.

وقد نصت المادة (11) من قانون جرائم أنظمة المعلومات الأردني المؤقت على ما يلي:

"أ) كل من دخل قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو نظام معلومات بأية وسيلة كانت بهدف الإطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، يعاقب بالحبس مدة لا تقل عن أربعة أشهر وبغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد على (5000) خمسة آلاف دينار.

ب) إذا كان الدخول المشـــار إليه في الفقرة (أ) من هذه المادة بقصـــد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسـخها، فيَعاقب الفاعل بالأشـغال الشـاقة المؤقتة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار".

ويرى البـاحث أنه ووفقاً لهذا النص فإنه يعاقب كل من دخل قصـــداً وبدون وجه حق إلى إحدى النظم المعلوماتية أو موقع إلكتروني بأية وسـيلة كانت، بقصـد الاطلاع على البيانات أو المعلومات التي تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.

وتشـدد العقوبة كذلك إذا ما ترتب على اختراق نظم المعلومات إلغاء تلك البيانات والمعلومات، أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها، وذلك بالنظر لأهمية تلك المعلومات وخطورتها.

وبـذلـك يكون المشـــرع الأردني قـد أحـ ـاط المعلومات المعالجة آلياً والمتعلقة بأسرار الدولة والأمن والاقتصـــاد الوطني بـالحمايـة الجنائية اللازمة من الاعتداء عليها عن طريق الأنظمة المعلوماتية، والحقيقة يحســب ذلك للمشـرع الأردني الذي واكب التطور ونهج نهج الدول المتقدمة في هذا المجال، وذلك بأن وفر الحمايـة اللازمـة لمثـل هذا النوع من المعلومات التي يشـــكل الاعتداء عليها خطورة كبيرة على أمن الوطن والمواطن، إلا أنه لم ينص صراحةً على جريمة التجســس المعلوماتي والوسـائل التقنية المسـتخدمة في ارتكاب هـذه الجريمـة، كما وأن العقوبـة الواردة في نص المادة 11/أ لا تتناســب وطبيعة هذه البيانات والمعلومات والتي يشكل الإطلاع عليها خطورة كبيرة على الدولة.

ثانياً- الحماية الجنائية للمعلومات المعالجة آلياً من أخطار التجسس المعلوماتي وفقاً للمشرع الأمريكي:

اتخذ المشرـع الأمريكي الفيدرالي موقفاً حازماً وصـارماً وذلك بشـموله كافة الأسـاليب والصـور التي يمكن أن ترتكب بها جريمة انتهاك أسرار الدفاع، حيث نص على جرائم التجســس في الفصـــل (37) في البند (413) من القانون الفيدرالي الأمريكي. (سليمان، لات، 162)

وقد نصـت المادة 1030/A/1,2 من القانون الفيدرالي الأمريكي والمتعلق بإساءة استخدام الحاسوب والصادر عام (1994) على ما يلي:

"معاقبة كل من اتصل عن علم بدون تصريح بحاسب آلي أو اتصل به على نحو غير مصرح به، وانتهز ذلك لتحقيق أغراض خارج نطاق التصريح المخول له وتمكن بهذا السلوك من:

1- الحصول على معلومات سرية لحكومة الولايات المتحدة الأمريكية تتعلق بالدفاع الوطني أو العلاقات الخارجيه لها بقصد استخدامها، أو بسبب الاعتقاد في إمكانية استخدامها للإضرار بالولايات المتحدة أو لفائدة دولة أجنبية وذلك على النحو المحدد في الماده 11 من قانون الطاقة الذرية لعام 1954.

2- الحصول على معلومات تتعلق بمؤسسة مالية أو بوكالة تقدم تقارير عن المركز الائتماني للمستهلكين وذلك على النحو المحدد في المادة 1602 ،أو معلومات عن أية وزارة أو وكالة تابعة للولايات المتحدة.

3- معلومات من أي جهاز حاسب آلي أو إتصالات بين الولايات المتحدة والدول الأجنبية[49] .(http://www.law.cornell.edu/uscode/text/18/1030.

وبذلك فقد اهتم المشرع الأمريكي بالمعلومات المتعلقة بالدفاع الوطني والعلاقات الخارجيه للولايات المتحدة، واعتبر أنه بمجرد الحصول عليها تقوم الجريمة حتى لو لم يتم تسليم هذه المعلومات إلى دولة أخرى طالما كان الهدف من ذلك الإضرار بالولايات المتحدة،

---

[49] Article 1030/A/1,2 of CFAA 1994.

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

ووفقا لنص المادة 1030/C من ذات القانون والخاص بالعقوبات فقد شـدد المشرـع الأمريكي من العقوبة فيما إذا تم تسـليم هذه المعلومات المعالجة آلياً إلى دولة أجنبية، وقد تصـل العقوبة إلى عشرـين سـنه إذا اقـترن الـفـعـل مـع أيـة جـريمـة مـنصـوص عـلـيـهـا في هـذا الـقـانـون[50] . http://www.law.cornell.edu/uscode/text/18/1030.

وفي عام 1996 أصـدر المشرـع الأمريكي قانون التجسـس الاقتصـادي حيث أصـبحت هذه الجريمة بموجبه جريمة فيدرالية (المومني، 2008، 224).

وبذلك فإن الباحث يرى أن المشرـع الأمريكي قد أولى المعلومات الخاصة بحكومة الولايات المتحدة الأمريكية والدفاع الوطني أهمية كبيرة وفائقة من خلال النص صراحة على الصـور والأسـاليب التي يمكن أن تقع ع لى هذه المعلومات المعالجة آلياً، واعتبر مجرد الحصـول على هذه المعلومات جريمة بحد ذاته بصرـف النظر إذا تم تسـليمها إلى دولة أخرى أم لم يتم تسـليمها طالما اتجهت إرادة الفاعل إلى الإضرار بحكومة الولايات المتحدة الأمريكية، وشـدد العقوبة في حال تسليم هذه المعلومات إلى دولة أجنبية، وبذلك نجد أن المشرع الأمريكي قد وفر الحماية الجنائية اللازمة للمعلومات المعالجة آلياً من خطر التجسس المعلوماتي.

ثالثاً- الحماية الجنائية للمعلومات المعالجة آلياً من أخطار التجسس المعلوماتي وفقاً للمشرع الفرنسي:

عالج المشرـع الفرنسي- جريمة التجسـس المعلوماتي في القسـم الثاني من قانون العقوبات الفرنسي- الجديد لعام 1994، والخاص بانتهاكات مواد أسرار الدفاع، وذلك في المواد 413-9 إلى 413-12 حيث نصـت المادة 413-9 على أنه " تشـمل أسرار الدفاع لأغراض هذا القسـم، العمليات والمعلومات والمقالات والوثائق والبيانات المحوسبة أو الملفات المحوسبة التي لها أهمية في الدفاع الوطني، والتي تخضع إلى إجراءات وقائية للحد من تداولها، والتي يؤدي الكشـف عنها إلى المسـاس بالدفاع الوطني أو الكشـف عن أسرار الدفاع الوطني، ويجوز بقرار من مجلس الـدولة النص على مسـتويات تصـنيف المعلومات والعمليات والمقالات والوثائق والبيانات المحوسـبة أو الملفات المحوسبة التي تعتبر من أسرار الدفاع الوطني، وتقع المسؤولية على السلطات في تحديد الوسائل اللازمة لضممان حمايتها [51] ".

---

[50] Article 1030/C/1/B of CFAA of 1994
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

[51] Article 413/9 Of (FCP)

ونصت المادة 413-10 على " تجريم أفعال تدمير أو سرقة هذه المعلومات السرية أو اختلاسها، أو نقلها إلى الجمهور أو إلى أي شخص غير مصرح له الإطلاع عليها، ومن بين هذه الأسرار البيانات والملفات المحوسبة والتي تدخل ضمن أسرار الدفاع، وأوجبت عقوبة على هذه الأفعال بالحبس لمدة سبع سنوات والغرامة 100000 يورو، وإذا وقعت هذه الأفعال نتيجة الإهمال يعاقب الفاعل بالسجن لمدة ثلاث سنوات والغرامة 45000 يورو [52] ".

ونصـت المادة 413-12 على " أن الشرـوع في ارتكاب الجرائم الواردة في الفقرتين 10، 11، من ذات المادة السابقة يخضع لنفس العقوبات [53] " .

Présentent un caractère de secret de la défense nationale au sens de la présente section les renseignements, procédés, objets, documents, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion.

Peuvent faire l'objet de telles mesures les renseignements, procédés, objets, documents, données informatisées ou fichiers dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Les niveaux de classification des renseignements, procédés, objets, documents, données informatisées ou fichiers présentant un caractère de secret de la défense nationale et les autorités chargées de définir les modalités selon lesquelles est organisée leur protection sont déterminés par décret en Conseil d'Etat.

[52] Article 413/10 Of (FCP)

Est puni de sept ans d'emprisonnement et de 100000 euros d'amende le fait, par toute personne dépositaire, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, d'un renseignement, procédé, objet, document, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit de le porter à la connaissance du public ou d'une personne non qualifiée.

Est puni des mêmes peines le fait, par la personne dépositaire, d'avoir laissé détruire, détourner, soustraire, reproduire ou divulguer le renseignement, procédé, objet, document, donnée informatisée ou fichier visé à l'alinéa précédent.

Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 45000 euros d'amende.

[53] Article 413/12 Of (FCP)

ويرى الباحث أن المشرع الفرنسي قد شمل البيانات والملفات المحوسبة ضمن المعلومات التي تدخل في أسرار الدفاع الوطني، واعتبر أن أي اعتداء عليها بالتدمير أو السرقة أو الكشف عنها وإطلاع الغير عليها يعتبر جريمة معاقب عليها بموجب المادة 413-10، وبصرف النظر عن الطريقة التي ارتكب بها الفعل، سواء بالطرق التقنية أو التقليدية، فلم يحدد المشرع الفرنسي ذلك، واهتم بتحديد المعلومات والوثائق التي تعد من قبيل أسرار الدفاع الوطني.

رابعاً- السويد:

جرم قانون البيانات الصادر عام 1973 مجرد الوصول إلى نظام المعالجة الآلية للبيانات بصورة غير مشروعة في المادة (21)، والتي تنص على ما يلي "يعاقب كل من تمكن بصورة غير مشروعه من الوصول إلى البيانات المخزنة داخل حاسب آلي بالغرامة أو بالحبس مدة لا تزيد على سنتين" (عفيفي، لات، 323).

خامساً- النرويج:

ينص القانون الجنائي على أنه "يعاقب كل من استولى أو حصل على بيانات تخص الغير وعلى نحو غير مشروع والتي تكون منقولة أو مخزنة أو معالجة بواسطة أنظمة المعالجة المبرمجة للبيانات (الشاذلي، فتوح وعفيفي، 2003، 343).

سادساً- القانون الإماراتي الاتحادي رقم (2) لسنة 2006:

نصت المادة (22) من هذا القانون على أنه "يعاقب بالسجن كل من دخل وبغير وجه حق موقعاً أو نظاماً مباشرةً أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة، فإذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها، تكون العقوبة السجن مدة لا تقل عن خمس سنوات" (حجازي، 2007، 220).

La tentative des délits prévus au premier alinéa de l'article 413-10 et à l'article 413-11 est punie des mêmes peines.

المطلب الثاني: جريمة الاعتداء على حُرمة

الحياة الخاصة للأفراد في نطاق المعلوماتية (انتهاك الخصوصية):

إن من أهم الحقوق الأساسية للأفراد هو الحق في احترام الحياة الخاصة لهم، وذلك بما يتضمنه هذا الحق من أسرار وخصوصيات يسعى الإنسان دائماً إلى الحفاظ عليها وعدم اطلاع الغير عليها، وقد نصت كافة الدساتير العالمية على هذا الحق وعلى احترامه، فهو موضع احترام واهتمام كافة التشريعات الدستورية، وهو لصيق بشخصية الإنسان ومرتبط ارتباطاً وثيقاً بحريته.

وقد جاء ظهور الأنظمة المعلوماتية وما تتمتع به من سرعة فائقة على تخزين ومعالجة كم هائل من البيانات والمعلومات وتحليلها واسترجاعها ومقارنتها ونقلها، ومن ثم إعادة تبادلها واستخدامها في الأغراض التي جمعت وخزنت من أجلها، وأدى إلى ظهور أنواع جديدة من الانتهاكات والاعتداءات والاختراقات التي تشكل تهديداً مباشراً وخطيراً على الحياة الخاصة للأفراد، نتيجة سهولة الوصول بطريق غير مشروع لهذه البيانات والمعلومات، واتساع المجالات لإساءة استخدامها، أو توجيهها توجيهاً منحرفاً أو خطأ إذا ما قورنت بالحياة الخاصة للأفراد في الماضي، والتي كانت سبل الحفاظ عليها واحترامها أسهل بكثير من عصر المعلومات الذي يستخدم تكنولوجيا ونظم المعلومات في معالجة هذه البيانات والمعلومات آلياً، وبالتالي تكون أكثر عرضة وسهولة لاختراقها، والاطلاع على أدق تفاصيل الخصوصية للأفراد.

وللوقوف على هذا الموضوع فإن الباحث سوف يتناول هذا المطلب بالدراسة والبحث من خلال بيان ماهية الحق في الحياة الخاصة وبنوك المعلومات، وأخطارها على الحياة الخاصة للأفراد، وصور الانتهاكات والاعتداءات المعلوماتية الواقعة على الحياة الخاصة والحماية الجنائية للمعلومات الطبية والتحريات الجينية الوراثية ، وأخيراً مدى الحماية الجنائية للمعلومات الاسمية والشخصية من خطر النظام المعلوماتي وبنوك المعلومات وفقاً للمشرع الأردني والأمريكي والفرنسي، وذلك كما يلي:

الفرع الأول: ماهية الحق في الحياة الخاصة:

تختلف معايير الحياة الخاصة باختلاف المجتمعات واختلاف الأفراد، ويعتبر موضوع تعريف الحياة الخاصة من الأمور التي تعتريها الصعوبة نتيجة لاختلاف معايير هذه الحياة بين الأفراد أنفسهم، فمنهم من يجعل حياته الخاصة كتاباً مفتوحاً، ومنهم من يجعلها سراً غامضاً، كما وأن مضمون هذه الحياة يختلف من مجتمع إلى آخر نتيجة لاختلاف القيم الأخلاقية، والعادات والتقاليد والثقافة (قايد، 1994، 9).

والواقع أنه تعددت وتنوعت التعريفات الفقهية المتعلقة بالحق في الحياة الخاصة، حيث ذهب بعض الفقه الفرنسي- إلى تعريفه بأنه "الحق في الحياة الأسرية والشخصية والداخلية والروحية للشخص عندما يعيش وراء بابه المغلق"[54].

وذهب البعض الآخر إلى تعريفه بأنه "حق الشخص بأن يحتفظ بأسرار من المتعذر على العامة معرفتها إلا بإرادة صاحب الشأن، والتي تتعلق بصفة أساسية بحقوقه الشخصية، ويقرر أن الحق في الحياة الخاصة يقع في دائرة الحقوق الشخصية للفرد، وإن كان لا يشملها كلها"[55].

وقد ذهب بعض الفقه الأمريكي إلى تعريف الحق في الحياة الخاصة بأنه "الحق الذي يكون للأفراد والجماعات والهيئات والمؤسسات في أن يحددوا لأنفسهم متى وكيف وبأي قدر يمكن إيصال المعلومات الخاصة بهم إلى غيرهم"[56].

وعرفه آخرون بأنه "حق الإنسان بأن تكون له حياة هادئة بلا إزعاج أو قلق"[57]، وقد عرفه مؤتمر استكهولم لرجال القانون الذي عقد عام 1967 بأنه "الحق في أن يكون الفرد حراً، وأن يترك ليعيش كما يريد مع أدنى حد للتدخل الخارجي" (قايد، 1994، 13).

وذهب فريق من الفقه إلى وضع تعريف سلبي للحق في الحياة الخاصة يعتبرون بمقتضاه أن الحياة الخاصة تشمل كل ما قد لا يعتبر من الحياة العامة للشخص، إلا أن هذا التعريف لم يلق تأييداً من جانب الفقه وذلك لصعوبة التفرقة والتمييز بين ما يدخل في نطاق الحياة العامة وما يدخل في نطاق الحياة الخاصة، لصعوبة وضع معيار للتمييز بينها (الشاذلي، فتوح وعفيفي، 2003، 264).

---

[54] تعريف الفقيه الفرنسي Martin مشار إليه لدى (الشاذلي، وعفيفي، 2003، 263).

[55] تعريف الفقيه الفرنسي "Nerson" مشار إليه لدى (قايد، 1994، 11).

[56] تعريف الفقيه الأمريكي (Allen Westin) مشار إليه لدى (المومني، 2008، 165).

[57] تعريف الفقيه الأمريكي (Cooley) مشار إليه لدى (الشاذلي وعفيفي، 2003، 265)

ويرى بعض الفقه أن هناك تطابقاً بين الحق في الحياة الخاصة من جهة والحقوق الشخصية من جهة أخرى، وذلك لتقريرهما حق الفرد في حماية اسمه وشرفه واعتباره ومراسلاته واتصالاته وحياته المهنية والعائلية، وكل ما له تأثير على حياته الشخصية"[58].

وتجدر الإشارة هنا أن معظم الفقه قد أجمع على صعوبة بل استحالة وضع تعريف جامع مانع للحق في الحياة الخاصة بحيث يعطي فكرة قانونية شاملة لمفهوم هذا الحق، وذلك لتداخل حياة الإنسان العامة والخاصة وصعوبة الفصل بينهما أحياناً (المومني، 2008، 166).

ويرى الباحث أن حق الإنسان في الحياة الخاصة من الحقوق الشخصية الملازمة للإنسان نفسه، وإن هذا الحق مرتبط ارتباطاً وثيقاً بالمجتمع الذي يعيش فيه وبثقافته وعاداته وتقاليده والقيم التي نشأ عليها، وأن معيار ضبطه هو معيار صعب بل ومستحيل إذا ما تم تطبيقه على الأفراد باختلاف المجتمعات التي يعيشونها واختلاف الأزمان وكذلك اختلاف العادات والثقافات والقيم، فما هو مسموح في مجتمع معين من حيث الاطلاع عليه من الخصوصية غير مسموح به في مجتمع آخر بل ومستهجن تبعاً للعادات والقيم المتبعة في ذلك الأخير، كما وأن اختلاف العقول البشرية يشكل صعوبة أخرى من حيث مفهوم هذا الحق، فبينما تكون الحياة الخاصة كتاباً مفتوحاً لدى البعض في مجتمع معين فإنها في المقابل تكون سراً غامضاً لدى البعض الآخر وفي نفس المجتمع، الأمر الذي يؤدي إلى صعوبة إعطاء فكرة قانونية عامة وشاملة لمفهوم هذا الحق، فهو حق نسبي يصعب ضبط مفهومه باختلاف الزمان والمكان.

لذلك ومن خلال استقراء التعريفات السابقة للفقه حول الحق في الحياة الخاصة فإن الباحث يرى أنها لم تضع تعريفاً جامعاً ومحدداً لهذا الحق، وإنما انطوت على دواعي ومبررات حماية هذا الحق، واجتمعت على توفير الهدوء والسكينة للإنسان دون التدخل في حياته الخاصة، ولم تحدد الأحوال التي لا يجوز فيها التدخل في هذه الحياة.

وإزاء هذه الصعوبة من وضع تعريف شامل للحق في الحياة الخاصة، فقد أدى ذلك بالفقه إلى القول بضرورة ترك هذا الأمر ليتولاه القضاء، على أن يتم تحديده وفقاً لأسس معينة مستمدة من التقاليد والثقافة والقيم الدينية السائدة والنظام السياسي لكل مجتمع، بما يكفل للإنسان أن تحترم ذاته مما يضمن له الهدوء والسكينة والأمن بعيداً عن تدخل الآخرين في خصوصياته (الشاذلي، فتوح وعفيفي، 2003، 265).

---

[58] هذا ما ذهب إليه الفقيه الفرنسي (Malherbe) ومشار إليه لدى (قايد، 1994، 12).

ويتفرع عن الحق في الحياة الخاصة مدلولان أحدهما حرية الحياة الخاصة والآخر سرية هذه الحياة، وتعني حرية الحياة الخاصة حرية الإنسان في ممارسة حياته بالأسلوب الذي يختاره دون تدخل من الآخرين ومن السلطة بالحدود التي يحددها القانون ودون الإضرار بالآخرين، أما

سرية الحياة الخاصة فتعني احتفاظ الشخص بجميع البيانات والوقائع التي يقرر أن من مصلحته الاحتفاظ بها لنفسه أو لغيره من الأشخاص المتصلين به ويريد اطلاعهم عليها (قايد، 1994، 19 وما بعدها).

الفرع الثاني: ماهية بنوك المعلومات في نطاق المعلوماتية وأخطارها على الحياة الخاصة للأفراد:

أولاً: ماهية بنوك المعلومات في نطاق المعلوماتية:

يُعرف مصطلح بنك المعلومات في نطاق المعلوماتية بأنه "قاعدة بيانات تفيد موضوعاً معيناً وتهدف إلى خدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الإلكترونية لإخراجها في صورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة" (قايد، 1994، 48).

وباستقراء هذا التعريف يتبين للباحث أن مصطلح بنوك المعلومات ينطوي على تجميع المعلومات المتعلقة بغرض معين بهدف معالجتها آلياً عن طريق الحاسب الآلي لاسترجاعها واستغلالها وقت الحاجة إليها، لذلك فبنوك المعلومات تتنوع بتعدد الأغراض المقصودة من وراء هذه المعلومات.

وفي مجال الحياة الخاصة للأفراد فإن بنوك المعلومات تعني تخزين المعلومات بطريقة تسمح بتقديم معلومات أو بيانات عن الأفراد، بصورة تمكن من التعرف على أشخاصهم، سواء من أسمائهم أو بأية وسيلة أخرى (حسبو، 2000، 51).

والمعلومات قد تكون موضوعية أو ذاتية وقد تكون اسمية أو مجهولة، وما يهمنا هنا هو المعلومات الاسمية التي تم معالجتها آلياً والمخزنة في بنوك المعلومات فهي التي تمس بالحريات العامة والفردية وحرمة الحياة الخاصة (حسبو، 2000، 35 وما بعدها).

وتعرف المعلومات أو البيانات الاسمية بأنها "البيانات الشخصية التي تتعلق بالحق في الحياة الخاصة للمرء، كالبيانات الخاصة بحالته الصحية والمالية والوظيفية والمهنية والعائلية، عندما تكون هذه البيانات محلاً للمعالجة الآلية" (صالح، 2000، 10).

أما المعالجة الآلية للمعلومات الاسمية في إطار موضوعنا فيقصد بها "مجموعة العمليات التي تتم آلياً باستخدام الحاسب الآلي، وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو المعلومات الاسمية، وكذلك مجموعة العمليات التي تتم آلياً بهدف استغلال المعلومات وعلى الأخص عمليات الربط والتقريب وانتقال المعلومات الاسمية ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومة ذات دلالة خاصة"[59].

ويرى الباحث أن استخدام النظام المعلوماتي وبنوك المعلومات قد يشكل خطراً كبيراً على حق الإنسان في حريته الشخصية، وبالتالي في حرمة حياته الخاصة، فالمعلومات الاسمية الخاصة بالإنسان يمكن أن تكون مسجلة على دعامات مادية كالأشرطة الممغنطة أو مختزنة في ذاكرة الحاسب الآلي، وهذه المعلومات قد تعطي فكرة كاملة عن الحياة الخاصة بهذا الإنسان وفي كافة نواحي حياته المالية والصحية والعائلية والاقتصادية والثقافية وغيرها، الأمر الذي يجعل من الممكن الاطلاع على هذه المعلومات واختراقها من قبل الأفراد أو الحكومات، وذلك من خلال استخدام الطرق الفنية والتقنية اللازمة للتعدي على هذه المعلومات، ولا شك أن ذلك يشكل خطورة كبيرة على الحق في الحياة الخاصة للأفراد، ويستدعي في ذات الوقت وجود ضمانات قانونية تكفل عدم المساس بالبيانات والمعلومات الاسمية للأفراد.

ثانياً: أثر بنوك المعلومات وأخطارها على الحياة الخاصة للأفراد:

اختلف الفقه حول مدى الخطورة التي تشكلها بنوك ونظم المعلومات على الحق في الحياة الخاصة، حيث ذهب البعض إلى أنه لا خطورة من استخدام المعلوماتية والحاسب الآلي على حُرمة الحياة الخاصة، بينما ذهب البعض الآخر إلى أن هناك أخطاراً عديدة يتعين مواجهتها وذلك كما يلي:

الاتجاه الأول: الحاسب الآلي وبنوك المعلومات لا تشكل خطراً على الحياة الخاصة:

يرى أنصار هذا الاتجاه أنه لا ضرورة لسن قواعد قانونية خاصة لحماية الحياة الخاصة في نطاق المعلوماتية، لأن بنوك المعلومات ونظم المعلومات لا تشكل أدنى خطورة على الحياة الخاصة للأفراد، فالحاسب الآلي وسيلة إلكترونية لتجميع وتخزين المعلومات والبيانات، وهذه الوسيلة جاءت بديلة للوسائل القديمة لحفظ المعلومات وهي الملفات والبطاقات وغيرها،

---

[59] نص المادة الخامسة من القانون الفرنسي الصادر في يناير سنة 1978 والخاص بالمعالجة الإلكترونية والحريات والمشار إليه لدى حسبو، 2000، 50.

وبالتالي يكفي لحماية الحياة الخاصة في مواجهة نظم المعلومات وبنوك المعلومات إعمال القواعد القانونية القائمة والتي وضعت من قبل، كما وأن القضاء قادر على تطبيق النصوص القائمة على الاعتداءات التي قد تطال الحياة الخاصة في نطاق المعلوماتية، وذلك من خلال تطويع هذه النصوص لتكون قابلة للتطبيق (حسبو، 2000، 55 وما بعدها).

الاتجاه الثاني: الحاسب الآلي وبنوك المعلومات تشكل خطراً كبيراً على الحياة الخاصة

وهو الاتجاه الغالب في الفقه والذي يؤيده الباحث حيث يرى أن الحاسب الآلي وبنوك المعلومات تنطوي على أخطار كبيرة على الحياة الخاصة أكثر بكثير من الوسائل التقليدية، خاصة فيما لو استخدمت في غير الأغراض المعدة لها، وذلك لعدة أسباب هي كما يلي:

(1) القدرة الفنية العالية التي يتميز بها الحاسب الآلي في تخزين واسترجاع قدر كبير من البيانات والمعلومات الخاصة بالأفراد والجماعات في مختلف مجالات الحياة وفي وقت قصير، الأمر الذي يجعل الحصول على هذه المعلومات أمراً سهلاً ويسيراً، بعد أن كان من الصعب بل من المستحيل الحصول على معلومات كاملة عن حياة الأشخاص بهذه السرعة والسهولة (قايد، 1994، 56).

(2) يمكن اختراق ذاكرة الحاسب الآلي والنظام المعلوماتي عن بعد باستخدام الطرق التقنية، بحيث لا يقتصر الاختراق على الاطلاع على المعلومات الاسمية الخاصة بالأفراد بل يتعدى ذلك ليصل إلى حد نسخ هذه البيانات والمعلومات تمهيداً لإساءة استخدامها فيما بعد (الشاذلي، فتوح وعفيفي، 2003، 271).

(3) وتزداد خطورة بنوك المعلومات على الحياة الخاصة عندما تقوم الدول بإنشاء بنوك معلومات قومية، من خلال جمع المعلومات الخاصة بالأفراد وتحليلها ومعالجتها آلياً ومن ثم تخزينها في بنوك المعلومات وذلك كنوع من الرقابة على مواطنيها، ولتقديمها إلى السلطات المختصة عند الحاجة إليها، وتعمد أجهزة الدول إلى استخدام الأجهزة الإلكترونية التي تعمل عن بعد والتي تُتيح جمع أكبر قدر ممكن من المعلومات الاسمية الخاصة بالأفراد ومن بنوك متعددة ومتفرقة، ودون علم الشخص نفسه، مما يعد اعتداءً على حياته الخاصة (قايد، 1994، 56).

وهذا ما يُشابه تقنية الحكومة الإلكترونية في الدول المتقدمة والتي تقوم بجمع المعلومات الاسمية عن الأفراد والجماعات ومن ثم معالجتها آلياً وتخزينها في الحواسيب الآلية وتبادلها بين المؤسسات والإدارات الحكومية، وذلك تسهيلاً لإنجاز المعاملات المختلفة في الدولة، الأمر الذي قد يؤدي إلى خرق حق الأفراد في حياتهم الخاصة لو أن هذه المعلومات استخدمت في غير الغرض الذي جمعت من أجله.

وفي هذا الشأن تحتفظ الحكومة الأمريكية في بنوك المعلومات الخاصة بحاسباتها الآلية ما يقارب ثلاثة بلايين ملف تحتوي معلومات شخصية للأفراد، بحيث يكون نصيب كل شخص ما يقارب مائة ملف تقريباً (الشاذلي، فتوح وعفيفي، 2003، 269).

كما أن وكالة المخابرات الأمريكية المعروفة بـــ CIA تقوم بمراقبة كافة الأشخاص داخل الولايات المتحدة عن طريق الموجات الكهرومغناطيسية، بحيث تكون لكل شخص إشارة كهرومغناطيسية معينة (الشاذلي، فتوح وعفيفي، 2003، 270).

وتجدر الإشارة هنا أن بعض الدول كفرنسا والولايات المتحدة الأمريكية وألمانيا احتجت على إنشاء النظام الموحد للمعلومات، والذي يعني جمع المعلومات المتصلة بالفرد في حاسوب مركزي واحد، بحيث يتم جمع المعلومات الضريبية والاجتماعية والدينية والسياسية والصحية، والمالية، والنشاط الحزبي والنقابي لهذا الفرد حتى أوقات تسليته وفراغه والأماكن التي يرتادها، الأمر الذي دفع كل من البرتغال والنمسا إلى تحريم هذا النظام الموحد للمعلومات لما ينطوي على اعتداء على الحياة الخاصة للأفراد (المومني، 2008، 171).

(4) وتزداد مخاطر النظام المعلوماتي على الحياة الخاصة في الحالة التي تكون فيها الحواسيب الآلية مرتبطة مع بعضها بعضا أو بحاسب مركزي أو بشبكة الإنترنت، الأمر الذي يسهل تبادل البيانات والمعلومات عبر هذه الشبكة، حيث يستطيع الأشخاص اقتحام الحواسيب المختلفة والدخول إليها عن طريق شبكة الإنترنت، وذلك باستغلالهم النقاط الضعيفة في منظومة الأمن الخاصة بهذه الشبكة، ومن ثم الوصول إلى بنوك المعلومات المتعلقة بالحياة الخاصة للأفراد (الشاذلي، فتوح وعفيفي، 2003، 273).

ويخلص الباحث مما سبق أن بنوك المعلومات تشكل خطراً كبيراً على الحياة الخاصة للأفراد، وذلك من خلال وجود قاعدة بيانات تتضمن هذه المعلومات الإسمية المعالجة آلياً والمخزنة في النظام المعلوماتي، إما في ذاكرة الحاسب أو على الدعامات المادية كالأقراص المغنطة، ومع سهولة اختراق هذه المعلومات فإن ذلك يتطلب توفير الحماية اللازمة لها من خطر الاختراق.

الفرع الثالث: صور الإنتهاكات المعلوماتية الواقعة على الحياة الخاصة (الخصوصية):

تعتبر جرائم الاعتداء على حرمة الحياة الخاصة للأفراد من أخطر الجرائم التي يمكن أن ترتكب عن طريق الأنظمة المعلوماتية وشبكات الاتصالات المعلوماتية بما فيها الإنترنت، وذلك لما تشكله الحياة الخاصة من معاني الخصوصية التامة لصاحبها، والتي يسعى دائماً إلى أن تظل هذه ا لحياة في الظلام بعيداً عن الأضواء، فالإنسان بطبيعته يميل دائماً إلى الاحتفاظ بأسراره العائلية والشخصية ومشاعره الداخلية وعلاقاته الخاصة وغيرها من الأمور التي تدخل في الخصوصية، ولا يسمح على الأغلب لأي كان بالاطلاع عليها إلا إذا اقتضت الضرورة لذلك، ونظراً لعدم فاعلية الحماية التقنية والرقابة على الأنظمة المعلوماتية سواء الحاسب الآلي أو شبكات الاتصالات والمعلومات، فإن ذلك أدى إلى بروز التهديد المعلوماتي على الحياة الخاصة، وذلك من خلال الاعتداءات والانتهاكات التي تطال الأسرار المعلوماتية الخاصة بالأفراد والجماعات، وما تتضمنه من بيانات ومعلومات اسمية مخزنة في الحاسب الآلي أو متداولة عبر شبكة الإنترنت، علماً بأن هناك صوراً وأشكالاً متعددة لهذه الاعتداءات، إلا أننا يمكن أن نتطرق في دراستنا هذه إلى أبرزها والتي تنتهك حرمة الحياة الخاصة للأفراد والأشخاص وذلك كما يلي:

أولاً: جمع أو تخزين بيانات شخصية صحيحة على نحو غير مشروع:

قد يتم انتهاك الخصوصية والحق في الحياة الشخصية في نطاق المعلوماتية عن طريق قيام الجاني سواء تمثل في شخص عادي أو مؤسسات حكومية أو خاصة بجمع معلومات وبيانات شخصية صحيحة في ذاتها ولكن على نحو غير مشروع، وصفة عدم المشروعية التي تلحق أفعال الجمع والتخزين قد يكون مصدرها الأساليب غير المشروعة للحصول على هذه البيانات والمعلومات، وقد يكون مصدرها مضمون هذه البيانات ذاتها (سلامه، 2006، 188).

ومن بين الأساليب غير المشروعة في الحصول على البيانات والمعلومات الشخصية والتي تشكل انتهاكاً واضحاً للخصوصية أسلوب التقاط الارتجاجات الناتجة عن الأصوات في الجدران الإسمنتية للحجرات، وترجمتها إلى كلمات وعبارات بعد معالجتها عن طريق حاسب آلي مزود ببرنامج خاص لذلك، وأسلوب مراقبة واعتراض الرسائل المتبادلة عبر البريد الإلكتروني، أو توصيل أسلاك بطريقة خفية إلى الحاسب الآلي الذي يحتوي على البيانات والمعلومات، أو التوصل بطريق غير مشروع إلى ملفات البيانات والمعلومات الشخصية التي تخص الآخرين (عفيفي، لات، 257).

أما بالنسبة لعدم مشروعية مضمون البيانات والمعلومات التي يتم جمعها وتخزينها، فالبيانات والمعلومات الشخصية التي تدخل في الحياة الخاصة للأفراد متعددة ومتنوعة، وهناك جزئية معينة من هذه المعلومات الاسمية من المفترض أنه لا يجوز جمعها وتخزينها وذلك للمحافظة على سرية الحياة الخاصة التي هي حق كل إنسان، وتكمن الصعوبة في تحديد هذه البيا نات والمعلومات تمهيداً لحماية الحق في الخصوصية (سلامه، 2006، 189).

وتتعدد البيانات والمعلومات الشخصية فمنها البيانات الصحية، والتعليمية والبيانات المتعلقة بالخدمة العسكرية، والعمليات البنكية والمصرفية، والمعاملات الضريبية، ومعاملات بطاقات الائتمان، وطلبات الإعانة التي تقدم إلى الجهات الحكومية، والاشتراك في صحف معينة وغيرها من مجالات الحياة الشخصية للأفراد، لذلك فإن جمع وتخزين هذه المعلومات آلياً يتيح مراقبة هؤلاء الأفراد وتحليل سلوكهم والتعرف على أبرز سماتهم المميزة وحياتهم الشخصية، الأمر الذي يجعل حياتهم أشبه بكتاب مفتوح، وبمقدور أي شخص لديه إمكانية التوصل إلى ملفات الحاسب الآلي من الاطلاع على هذه المعلومات الشخصية، فعدم وجود ضوابط قانونية في هذا المجال يؤدي إلى إمكانية جمع وتخزين ونقل كم هائل من المعلومات التي قد تتعلق بأدق الأمور الخاصة بالأفراد (سلامة، 2006، 190).

ونخلص مما سبق أن البيانات والمعلومات الشخصية خاصة بشخص صاحبها لذلك كان لابد من حظر جمعها وتخزينها للمحافظة على سريتها والتي هي من حق صاحبها ابتداءَ، والإنسان بطبيعته يميل دائماً وعلى الأغلب في معظم المجتمعات إلى الاحتفاظ بخصوصياته الشخصية والعائلية وبالتالي لا يجوز لأي كان أن يخرق هذه الخصوصية عن طريق بنوك المعلومات التي تجمع في طياتها كم هائل من البيانات والمعلومات الاسمية،

إلا أنه لابد من التنويه أن حق الخصوصية والحياة الخاصة هو حق يتمتع بقدر من المرونة والذي يسمح في بعض الأحيان وفي حالات الضرورة لبعض الجهات الرسمية في الدولة أو المؤسسات أو الشركات الخاصة وفي حدود اختصاصاتها جمع البيانات والمعلومات الشخصية عن الأفراد كنوع من الرقابة عليهم وتحليل تصرفاتهم للتعرف على أبرز السمات المميزة لسلوكهم واستنتاج صورة تقريبية لشخصياتهم، ولتسهيل إجراء المعاملات الرسمية لدى الجهات المعنية إلا أن هناك جزئية معينة من هذه البيانات والمعلومات الاسمية الشخصية لا يجوز التدخل بها ولا الاطلاع عليها من أي كان وذلك للمحافظة على كيان وخصوصية صاحبها.

ثانياً: إساءة استعمال البيانات والمعلومات الاسمية:

الأصل في البيانات والمعلومات الاسمية التي يتم تجميعها ومعالجتها وتخزينها في النظام المعلوماتي أن يكون الهدف منها محدداً وواضحاً سلفاً، وقبل البدء بعملية الجمع والتخزين. وأن لا يكون ذلك يتعارض مع النظام العام والآداب (المومني، 2008، 175).

ومؤدى ذلك أن على الجهة القائمة بعملية تجميع هذه المعلومات والبيانات وتخزينها آلياً في الحاسب الآلي أن تلتزم بحدود الهدف والغاية من وراء جمع هذه المعلومات الشخصية، فلا يجوز لها أن تتجاوز هذا الهدف، بحيث يسمح لها بعملية الجمع والتخزين بالقدر الذي يخدم ويؤدي الغاية التي تمت عملية الجمع من أجلها ، مع الأخذ بعين الاعتبار أيضاً أن يكون الهدف المعين لعملية الجمع من المهام الوظيفية التي تدخل في اختصاص الجهات القائمة على النظام المعلوماتي.

والمثال على ذلك ما قام به القضاء الألماني بوقف عملية التعداد السكاني الرسمية عام 1984، وذلك بعد أن ثبت لها أن وزارة الداخلية قد حصلت على عناوين مجموعة إرهابية من خلال البيانات الإحصائية في تلك العملية، حيث استندت إلى إساءة استعمال البيانات والمعلومات الاسمية ووقف عملية التعداد السكاني لتجاوزها للهدف والغاية التي جرت علمية جمع وتخزين المعلومات من أجلها[60] (قايد، 1994، 53).

[60] اعتبرت المحاكم الألمانية أن ذلك يشكل اعتداءً على الحياة الخاصة للأفراد وانتهاكاً لسرية البيانات والمعلومات الشخصية، وتعد ألمانيا من الدول الغربية التي وضعت تشريعاً خاصاً لحماية البيانات الشخصية ضد إساءة استخدامها عند معالجتها إلكترونياً، وسمي القانون الفيدرالي من أجل حماية البيانات لسنة 1977 (مشار إليه لدى قايد، 1994، 53).

ثالثاً: الإفشاء غير المشروع للبيانات والمعلومات الشخصية:

وتتحقق هذه الحالة بأن تتم عمليات الجمع والتخزين والمعالجة الآلية للبيانات والمعلومات الشخصية بطريقة مشروعة ومن قبل الجهات التي تملك الصلاحية في ذلك سواء القطاع العام أو الخاص وضمن حدود الأهداف والغايات المرجوة من عملية الجمع، إلا أن هذه البيانات والمعلومات يتم إفشاؤها من قبل القائمين على حفظها وبطريقة غير مشروعة، الأمر الذي يشكل انتهاكاً للحق في الحياة الخاصة للأفراد.

وتجدر الإشارة هنا أن استخدام الحاسب الآلي والأنظمة المعلوماتية في المجال الأمني وقطاع الشرطة يؤدي إلى الاحتفاظ لديهم بكم هائل من البيانات والمعلومات الخاصة بالملايين من الأفراد، الأمر الذي يشكل خطراً على الحياة الخاصة في حال لو تم إفشاء هذه المعلومات من قبل أشخاص يفترض أنهم أمناء عليها (عفيفي، لات، 259).

وإفشاء البيانات والمعلومات الشخصية لا يقتصر فقط على الجهات الرسمية أو الأمنية، وإنما قد يحدث في القطاع الخاص كالشركات والمؤسسات الخاصة والمعاملات المصرفية والبنوك وغيرها من الجهات التي تستخدم بنوك المعلومات، ولعل أكثر البيانات الشخصية السرية تعرضاً إلى خطر الإفشاء غير المشروع هي المخزنة والمعالجة آلياً في ذاكرات الحواسيب الآلية للبنوك (سلامة، 2006، 191).

رابعاً: الاعتداء على خصوصية الاتصالات والمراسلات وسريتها:

الحق في الخصوصية يمتد ليشمل حق الإنسان في حرمة اتصالاته ومراسلاته وسريتها، فلا يجوز لأي كان الاعتداء على هذا الحق إلا في الحالات المحددة في القانون، ويشمل الحق في حماية الاتصالات والمراسلات كافة الطرق التقنية الحديثة في إجراء هذه العمليات من خلال النظام المعلوماتي، فلا يجوز التصنت على المحادثات الخاصة للأفراد والتي تتم عن طريق شبكة الإنترنت، كما أنه لا يجوز الاطلاع على مضمون الرسائل الإلكترونية التي يتم تبادلها عبر الشبكة، سوء تم ذلك عن طريق الحصول على كلمة السر للمستخدم (Password) ، أو باعتراض هذه الرسائل والاطلاع على مضمونها، فذلك كله يُعد انتهاكاً لحرمة الحياة الخاصة للأفراد (المومني، 2008، 179).

كما وأن التقاط الصور وتداولها عبر شبكة الإنترنت يعتبر انتهاكاً للخصوصة والحق في الحياة الخاصة.

خامساً: مخالفة القواعد الشكلية المنظمة لجمع ومعالجة ونشر البيانات الشخصية التي تدخل في نطاق الحماية التشريعية لخصوصية المعلومات:

تتطلب غالبية النظم القانونية إلى وضع مجموعة من القواعد الشكلية لتنظيم عملية جمع ومعالجة وتخزين ونشر البيانات والمعلومات الشخصية، مثل ضرورة حصول الجهة القائمة على عملية الجمع والتخزين على ترخيص بذلك، واتجهت الدول لذلك من أجل حماية الحق في الحياة الخاصة وحماية خصوصية المعلومات، حيث إ ن كثيراً من هذه الدول اعتبرت خرق هذه القواعد الشكلية جريمة يعاقب عليها القانون (سلامة، 2006، 193).

وتطبيقاً لذلك أدان القضاء الفرنسي شركة S.K.F لقيامها بتخزين البيانات الخاصة بالعاملين فيها والمتعلقة باتجاهاتهم السياسية وعضوية الاتحادات والنقابات العمالية والتي قامت بجمعها من طلبات التوظيف التي سبق وقدموها إلى ال شركة، حيث اعتبرت المحكمة هذا الأمر مخالفاً لأحكام القانون الصادر في 6/يناير 1978 والخاص بالمعالجة الإلكترونية للبيانات الاسمية (عفيفي، لات، 263).

وتجدر الإشارة هنا أن المشرع الفرنسي نص في قانون العقوبات الفرنسي الجديد لعام 1994 في المادة (226) على أهم جرائم الاعتداء على حرمة الحياة الخاصة عبر الإنترنت، والتي منها جريمة المعالجة الإلكترونية للبيانات الشخصية دون ترخيص، وجريمة التسجيل غير المشروع للبيانات الاسمية، وجريمة الحفظ غير المشروع للبيانات الاسمية (العزام، 2009، 62 وما بعدها).

ومن خلال ما تقدم فإن الباحث يرى أن هناك صوراً متعددة ومتنوعة للانتهاكات التي تطال بالاعتداء الحياة الخاصة في مجال المعلوماتية، ويظهر ذلك بصورة واضحة من خلال اعتماد الكثير من المؤسسات والشركات سواء أكانت حكومية أو خاصة على الأنظمة المعلوماتية لقدرتها الفائقة على جمع وتخزين ومعالجة كم هائل من البيانات والمعلومات الإسمية المتعلقة بالحياة الخاصة للأفراد وتخزينها في بنوك للمعلومات في ذاكرة الحاسب الآلي، وهذه الجهات القائمة على عملية الجمع والتخزين تتناول أدق التفاصيل الخاصة بأفراد المجتمع والمتعلقة بالوضع الصحي والتعليمي والعائلي والمادي والعلاقات الخاصة والعادات الاجتماعية وغيرها من التفاصيل الدقيقة الهامة في حياة الإنسان، الأمر الذي جعل إمكانية الوصول غير المشروع إلى هذه البيانات والمعلومات الاسمية أسهل بكثير من الماضي، وفتح المجال لإساءة استخدامها وانتهاكها والاطلاع على أدق التفاصيل لخصوصيات الأفراد من خلال الوصول إلى سجلات وملفات البيانات الشخصية المخزنة في الحاسب الآلي، ويرى الباحث أن هذه الانتهاكات قد ترتكب من نفس الجهات القائمة على هذه العملية من ناحية،

ومن ناحية أخرى قد ترتكب من قبل الأفراد أنفسهم بما يخص البيانات والمعلومات الشخصية الخاصة بالغير، كالاعتداء الذي يقع من أشخاص ذوي خبرة وكفاءة عالية في استخدام تقنية تكنولوجيا المعلومات، فلا يشترط لتحقق هذا الاعتداء أن يكون صادراً عن جهة قائمة على جمع المعلومات، وإنما قد يقع من الشخص العادي، ولكن على اختلاف الظروف التي يتم بها الاعتداء.

ويقع الاعتداء من قبل الجهة القائمة على عملية الجمع والتخزين نتيجة عدم تقيدها بالهدف والغرض المرجو من هذه العملية، أو نتيجة عدم تقيدها بالشروط الشكلية لعملية الجمع والتخزين، أو نتيجة إفشاء البيانات والمعلومات الشخصية من قبل القائمين على حفظها بطريقة غير مشروعة، أو إساءة استخدام هذه البيانات بعد جمعها وتخزينها بطريقة مشروعة، أو جمع هذه البيانات بطريقة غير مشروعة، أو بالاعتداء على خصوصية الاتصالات والمراسلات للأفراد بغير الطرق التي حددها القانون، الأمر الذي يؤدي إلى انتهاك الخصوصية والحياة الخاصة للأفراد، وعلى الصعيد الآخر قد يقع الاعتداء من قبل شخص عادي ذي خبرة وكفاءة فنية عالية في استخدام الأنظمة المعلوماتية ويتصور ذلك بالدخول للنظام المعلوماتي والتداول غير المشروع للمعلومات الاسمية الخاصة بالغير، وذلك عن طريق الحصول على كلمة السر للمستخدم (Password)، ومن ثم اختراق الملفات المخزنة والاطلاع عليها دون إذن أو ترخيص، ويتصور ذلك أيضاً عن طريق الدخول إلى البريد الإلكتروني للمستخدم والاطلاع على الرسائل التي يحتويها، أو اعتراض هذه الرسائل عبر الشبكة ومن ثم الاطلاع على مضمونها، الأمر الذي يؤدي إلى اختراق الحياة الخاصة للغير والذي يتطلب ترتيب مسؤولية جزائية في مواجهة هذه الأفعال.

وهناك صور كثيرة ومتعددة للاختراقات التي تستهدف الحق في الحياة الخاصة والتي تحتاج إلى دراسات مستفيضة تخصص للبحث في مثل هذا الموضوع، إلا أن الباحث يرى أن كل ما يدخل في خصوصية الإنسان يجب أن يبقى في الظلام وبعيداً عن الأضواء من حيث اطلاع الغير عليه، وذلك من أهم الحقوق الإنسانية التي تنادت بها الدساتير على اختلافها ومنذ القدم، مع الأخذ بعين الاعتبار أن هذا الحق يشتمل على شيء من المرونة وتحت مظلة القانون وفي حالات محددة، بأن يسمح للجهات المعنية الرسمية وبحكم تسهيل المعاملات الرسمية وكنوع من الرقابة البناءة على الأفراد أن تقوم بتنظيم بنوك معلومات خاصة بالأفراد ضمن قيود معينة، ودون المساس ببعض البيانات والمعلومات الاسمية والشخصية الخاصة بالأفراد، وغير الصالحة للجمع والتخزين والمعالجة في نظام الحاسب الآلي بسبب مضمونها.

الفرع الرابع: الحماية الجنائية للمعلومات الطبية والتحريات الجينيه الوراثية:

إن تجريم التلاعب في البيانات الشخصية خاصة البيانات الطبية والفحوصات الخاصة بها ذات ارتباط وثيق بحرمة الحياة الخاصة للأفراد، والتي يجب عدم الإطلاع عليها إلا بإذن صاحبها هذا فضلاً عن إضرارها بصاحب الشأن نفسه (حجازي، 2009، 100).

وتعتبر المعلومات الخاصة بعلم الوراثة والجينات الوراثية والحمض النووي من أهم المعلومات والبيانات الإسمية التي تدخل في الحياة الخاصة للأفراد، ويختص علم الوراثة بدراسة الصفات الموروثة للكائنات الحية وكيفية انتقالها من الآباء إلى الأبناء، والتي تسمى الموروثات (الجينات)، وهي تمثل مناطق معينة في شريط (DNA) ، والذي يمثل المعلومات الوراثية لصفات الكائن الحي (http://www.wikipedia.org/wiki.com).

وقد أثار مشروع قانون "التحكم في الهجرة" المطروح للمناقشة بالجمعية الوطنية الفرنسية (البرلمان)، اجتماعات واسعة بين أوساط منظمات الإنسان الفرنسية وأحزاب المعارضة التي اعتبرته بمثابة اعتداء على الأجانب من قبل الدولة، حيث تعترض المنظمات الحقوقية على البند المتعلق بفرض فحوصات جينية وراثية "DNA" على كافة الأفراد الراغبين في الهجرة إلى فرنسا للالتحاق بعائلاتهم بهدف إثبات صلة القرابة، حيث اعتبرت المنظمات الحقوقية هذا الأمر بمثابة فضيحة وانتهاك للخصوصية لا سابق لها للاستهانة بالمهاجرين.

(http://www.thearabhc.maktoobbloy.com)

وقد عالج المشرع الفرنسي الجرائم المرتكبة ضد الأشخاص والخاصة بفحص الخصائص الجينية أو تحديد الحمض النووي، وذلك في القسم السادس من قانون العقوبات الفرنسي الجديد، في المواد 226-25 إلى 226-30.

وقد نصت المادة 226-25 على تجريم " كل من قام بدراسة الخصائص الوراثية لشخص ما، وذلك لغير الأغراض الطبية أو لأغراض البحث العلمي دون الحصول على موافقة مسبقة من ذلك الشخص، وذلك وفقاً للشروط المنصوص عليها في المادة 16-10 من القانون المدني، حيث يعاقب مرتكب هذه الأفعال بالحبس لمدة سنة وغرامة مقدارها 15000 يورو [61]".

---

[61] Article 226/25 Of (FCP)
Le fait de procéder à l'examen des caractéristiques génétiques d'une personne à des fins autres que médicales ou de recherche scientifique, ou à des fins médicales ou de recherche scientifique, sans avoir recueilli préalablement son consentement dans les conditions prévues par l'article 16-10 du code civil, est puni d'un an d'emprisonnement et de 15 000 Euros d'amende.

كما ونصت المادة 226-26 من ذات القانون على تجريم " كل من قام بتسريب أو إفشاء المعلومات التي تم جمعها عن شخص ما، وذلك عن طريق دراسة الخصائص الوراثية له والمقصودة من البحوث الطبية والعلمية، حيث يعاقب مرتكب هذه الأفعال بالحبس لمدة سنة وغرامة مقدارها 15000 يورو [62] ".

كما ونصـــت المـادة 226-28 من ذات القـانون على " تجريم الأفعال التي تؤدي إلى تحديد هوية الشخص من خلال الحمض النووي لأغراض ليست طبية أو علمية، أو في غير التحقيق أو الإجراءات القضائية، حيث يعاقب مرتكب هذا الفعل بالحبس لمدة سـنة وغرامة 15000 يورو ، كما وأن الكشف عن معلومات يؤدي إلى تحديد هوية الشـــخص من خلال الحمض النووي أو الشرـــوع في ارتكاب هذه الجرائم المذكورة يخضع إلى نفس العقوبة [63]".

ونصـــت المادة 226-30 من ذات القانون على تحديد العقوبات التي يمكن إيقاعها على الأشـــخاص المعنوية في حال ارتكاب هذه الجرائم باسمهم أو بوسائلهم، وحدد القانون هذه العقوبات بالغرامات المالية وفقاً للشرـوط المنصوص عليها بموجب المادة 131-38 من ذات القانون، والعقوبات المشار اليها في الفقرات 2, 3,4,5,7,8,9من المادة 131-39 من ذات القانون ، والحظر المشار إليه في ذات المادة [64] ".

---

[62] Article 226/26 Of (FCP)

Le fait de détourner de leurs finalités médicales ou de recherche scientifique les informations recueillies sur une personne au moyen de l'examen de ses caractéristiques génétiques est puni d'un an d'emprisonnement et de 15000 euros d'amende.

[63]Article 226/28 Of (FCP)

Le fait de rechercher l'identification par ses empreintes génétiques d'une personne, lorsqu'il ne s'agit pas d'un militaire décédé à l'occasion d'une opération conduite par les forces armées ou les formations rattachées, à des fins qui ne seraient ni médicales ni scientifiques ou en dehors d'une mesure d'enquête ou d'instruction diligentée lors d'une procédure judiciaire est puni d'un an d'emprisonnement ou de 1 500 Euros d'amende.

Est puni des mêmes peines le fait de divulguer des informations relatives à l'identification d'une personne par ses empreintes génétiques ou de procéder à l'identification d'une personne par ses empreintes génétiques sans être titulaire de l'agrément prévu à l'article L. 1131-3 du code de la santé publique.

[64] Article 226/30 Of (FCP)

وهذا على خلاف المشرع الأردني الذي لم يتطرق إلى موضوع المعلومات والبيانات الإسمية الخاصة بالأفراد، والتي من ضمنها المعلومات الخاصة بالفحوصات الطبية الجينية الوراثية، حيث خلا قانون العقوبات الأردني وقانون جرائم أنظمة المعلومات الأردني المؤقت من أية نصوص تعالج موضوع التحريات الجينية الوراثية.

الفرع الخامس: الحماية الجنائية للحياة الخاصة والمعلومات الإسمية (الشخصية) من أخطار النظام المعلوماتي وبنوك المعلومات وفقاً للتشريع الأردني، والأمريكي، والفرنسي.

أولا: موقف المشرع الأردني:

كفل الدستور الأردني الحقوق والحريات الفردية في الفصل الثاني من الدستور حيث نصت المادة السابعة منه على أن "الحرية الشخصية مصونة"، كما بينت المادة الثامنة من الدستور بأنه "لا يجوز أن يوقف أحد أو أن يحبس إلا وفق أحكام القانون"، وجاء في المادة العاشرة منه أن "للمساكن حرمة فلا يجوز دخولها إلا في الأحوال المبينة في القانون وبالكيفية المنصوص عليها فيه".

وقد جاءت المادة الثامنة عشرة من ذات الدستور لتكفل سرية المراسلات والمخاطبات، ونصت على ما يلي "تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية سرية، فلا تخضع للمراقبة أو التوقيف إلا في الأحوال المعنية في القانون"،

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section.

Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38 ;

2° Les peines mentionnées aux 2°, 3°, 4°, 5°, 7°, 8° et 9° de l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

وقد كفل المشرع الدستوري أيضاً حرية الأديان والعقيدة في المادة الرابعة عشرة، وحرية الرأي في المادة الخامسة عشرة، وحرية الاجتماع وتأليف الجمعيات والأحزاب السياسية في المادة السادسة عشرة، أما قانون العقوبات الأردني فنجد أن المادة (355) قد عالجت جريمة إفشاء الأسرار الرسمية أو المهنية، وقد نصت على ما يلي: "يعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من:

1- حصل بحكم وظيفته أو مركزه على أسرار رسمية وأباح هذه الأسرار لمن ليس له صلاحية الاطلاع عليها، أو إلى من لا تتطلب طبيعة وظيفته ذلك الاطلاع وفقاً للمصلحة العامة.
2- كان يقوم بوظيفة رسمية أو خدمة حكومية واستبقى بحيازته وثائق سرية أو رسوماً أو مخططات أو نماذج أو نسخاً منها دون أن يكون له حق الاحتفاظ بها، أو دون أن تقتضي ذلك طبيعة وظيفية.
3- كان بحكم مهنته على علم بسر وأفشاه دون سبب مشروع".

وباستقراء هذا النص فإن الباحث يرى أن الحماية المقررة بموجب الفقرتين الأولى والثانية منه هي للمعلومات ذات الطبيعة السرية والرسمية، والمتمثلة في الأسرار الرسمية كالوثائق السرية أو الرسومات أو المخططات أو النماذج، والتي تم الحصول عليها من قبل الفاعل بحكم وظيفته أو مركزه الرسمي، وإن صفة الرسمية والسرية وفقاً لهذا النص تخرج من دائرة التجريم المعلومات والبيانات الإسمية الخاصة بالأفراد، على الرغم من أن هذه المعلومات الشخصية تتشابه مع الأسرار في أن نطاق العلم بها ينحصر في عدد محدود من الأشخاص إلا أنها ليست رسمية، وبالتالي لا تكون محلاً للإفشاء، أما بالنسبة للفقرة الثالثة من ذات المادة فإن الباحث يرى أن المعلومات المهنية التي تصل إلى الشخص العامل في تلك المهنة قد تكون معلومات وبيانات شخصية تتعلق بالحياة الخاصة للأفراد، كعلم الطبيب -على سبيل المثال- بمعلومات طبية عن حالة المريض الصحية، وتخزينها في الأنظمة المعلوماتية لديه، وبالتالي فإن إفشاء هذه البيانات والمعلومات الشخصية أو إساءة استعمالها يُعد انتهاكاً لحق الخصوصية لهذا المريض إلا في الحالات التي يتطلبها القانون، على اعتبار أن المعلومات الطبية تدخل في إطار المعلومات الاسمية المتعلقة بالحياة الخاصة للأفراد، أما المواد (356) و(357) من ذات القانون فقد جاءت لحماية الرسائل العادية والمكالمات الهاتفية التي تتم عن طريق الهواتف، ولم تتطرق للاتصالات والمراسلات التي تتم عبر الشبكة المعلوماتية.

حيث يرى الباحث أن المواد السابقة لم تعالج خصوصية الاتصالات والمراسلات وسريتها كصورة من صور الاعتداء على الحياة الخاصة للأفراد والتي تقع من خلال النظام المعلوماتي باستخدام التقنيات الحديثة سواء تمثلت باعتراض الرسائل الإلكترونية المتبادلة عبر شبكة الإنترنت والتي تتضمن بيانات ومعلومات اسمية خاصة بالأفراد، أو التصنت على المحادثات التي تتم عبر شبكة الإنترنت.

أما قانون الاتصالات الأردني فقد حاول المشرع الأردني في المادة (71) توفير الحماية الجزائية للمحادثات التي تتم بواسطة شبكات الاتصال العامة أو الخاصة وللرسائل الهاتفية من خطر الإفشاء، وذلك من قبل الشخص بحكم وظيفته، كما وحاول في المادة (77) من ذات القانون توفير الحماية للرسائل المنقولة عبر شبكات الاتصال من خطر الإفشاء أو النسخ أو العبث، وأيضاً حماية البيانات المتعلقة بالمشتركين من حيث أرقام هواتفهم غير المعلنة، والعبث في الرسائل المرسلة والمستقبلة.

أما قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010، فإن الباحث لم يجد فيه أي نص يتعلق بالبيانات والمعلومات الإسمية والمتعلقة بالحياة الخاصة للأفراد، كما وأن هذا القانون لم يتطرق إلى بنوك المعلومات وطبيعتها ومدى أثرها وخطورتها على المعلومات المعالجة آلياً والخاصة بالحياة الشخصية للأفراد، وكل ما هنالك أن بعض المواد الواردة في هذا القانون جاءت بنصوص عامة حول حماية البيانات والمعلومات المعالجة آلياً دون تحديد طبيعتها، مثل المادة (3) من ذات القانون، والتي جاءت لحماية البيانات والمعلومات المعالجة آلياً وبشكل عام من الإتلاف أو الإلغاء أو الإفشاء أو التعديل أو التغيير..إلخ، والمادة (4) أيضاً والتي جاءت لحماية البيانات والمعلومات المعالجة آلياً من الأخطار التي تشكلها الفيروسات والبرامج التقنية، والتي قد تؤدي إلى إتلاف أو حذف أو إلغاء أو تدمير أو إفشاء هذه المعلومات، والمادة (5) من ذات القانون والخاصة بحماية المعلومات المعالجة آلياً من خطر اعتراضها أو إلتقاطها أو التنصت عليها، وهكذا فيرى الباحث أن معظم المواد الواردة في قانون جرائم أنظمة المعلومات الأردني المؤقت قد جاءت لتوفير الحماية للبيانات والمعلومات المعالجة آلياً، إلا أنها لم تحدد طبيعة هذه المعلومات، ولم يرد في ذات القانون أي نص حول تحديد المعلومات الإسمية والشخصية، أو الطرق التقنية لانتهاك الحق في الخصوصية، وانتهاك الحياة الخاصة للأفراد في البيئة الرقمية، وأخطار بنوك المعلومات على الحياة الخاصة في نطاق الأنظمة المعلوماتية، الأمر الذي يتطلب تدخل المشرع الأردني بأن يضمن تشريعاته المعلومات الإسمية وأن يضفي عليها الحماية اللازمة من خطر بنوك المعلومات والمعالجة الآلية للبيانات.

ثانيا: موقف المشرع الأمريكي:

نص الدستور الاتحادي في الولايات المتحدة الأمريكية وبصفة عامة على الحقوق الأساسية للمواطن، إلا أن هـذه الحقوق أعطيـت للأفراد بصـــورة عـامـة في مواجهـة الإجراءات الحكوميـة فقط وليس القطاع الخاص، كما وأنها جاءت ســلبية بحيث لا تلزم الحكومة بعمل أي شيء ســوى الامتناع عن اتخاذ إجراءات معينة. (كيت، 1999، 68)

لذلك فلا يوجد ضـمان دستوري صريح لحق الخصوصية، إلا أن المحكمة الفيدرالية العليا الأمريكية وجدت عدداً من حقوق الخصوصية وذلك في أربعة مجالات هي:

(1) حماية التعديل الأول للدستور لحرية التعبير والمشاركة والديانة.

(2) القيود التي جاء بها التعديل الرابع على عمليات التفتيش والاسـتيلاء، واتخاذ القرارات الأسـاسية القائمة على أثر قانون الحقوق.

(3) والضمانات التي جاء بها التعديل الرابع عشر لمبدأ المحاكمة المشروعة.

(4) وتوفير الحماية التي جاء بها التعديل الرابع عشر لعدم كشف المعلومات الشخصية (كيت، 1999، 83 وما بعدها).

أما على المسـتوى الفيدرالي فإن المشرـع الأمريكي لم يضـع قوانين خاصـة باسـتخدام الحاسـب الآلي كبنوك معلومات لجمع وتخزين ومعالجة البيانات والمعلومات الاسـمية، إلا أنه وضـع قوانين خاصـة لحماية البيانات والحياة الخاصـة والتي من خلالها أسـبغ الحماية على البيانات والمعلومات الشـخصية وعلى الأغلب اقتصرـ ذلك على الأنشــطة الحكومية، حيث أصــدر قانون تقرير الائتمان العادل عام 1970 (عفيفي، لات، 286)، وينظم هذا القانون عملية تسجيل البيانات المتعلقة بالقدرة المالية والمركز الائتماني للأفراد، ويعطيهم حق الاطلاع على هذه البيانات والاعتراض على عدم صـحتها ودقتها، ويفرض على الجهة القائمة بعملية جمع المعلومات التحقق من ذلك وتصــحيح الأخطاء، وتعويض الأفراد عن الأضرار التي قد تلحق بهم جراء هذه الأخطاء (سليمان، لات، 199).

وفي 31/ ديسـمبر سـنة 1974 أصـدر المشرع الأمريكي ت شريعاً خاصاً لحماية الحياة الخاصة (THE Privacy ACT of 1974) والمعدل بالقانون رقم 94-393 لسـنة 1976، والقانون رقم 95 – 38 لسنة 1977، وجاء هذا القانون لحماية البيانات والمعلومات المخزنة بأي شـكل، ويتضـمن هذا القانون عدة مبادئ حيث حـدد شروط انتقـال المعلومات، واشــتـر ط أن يتم تداولها ســواء داخل الإدارة أو خارجها بناءً على الموافقة الخطية لصــاحب الشــأن حيث حددت الماده 552/B من هذا القانون شروط الإفصــاح عن أية معلومات خاصه تتعلق بالأفراد

ونصت على ما يلي " لا يجوز لأية وكالة الكشف عن أي سجل أو معلومات محفوظه في سجلاتها وبأية وسيلة الى شخص اخر أو وكالة أخرى إلا بناءً على طلب خطي مسبق ،وموافقة خطية مسبقة من الفرد صاحب العلاقة وذلك وفقا لشروط معينه وهي :

1-أن يكون الكشف للضباط العاملين في الوكالات وعند الحاجة لهذه المعلومات مع المحافظة عليها.

2-مطلوب بموجب المادة 552 من هذا القانون.

3-للحصول على الاستخدام الروتيني لهذه السجلات.

4-لمكتب التعداد لأغراض التخطيط أو التعداد أو المسح أو الأنشطة ذات الصلة.

5-الى مستلم قدم ضمانات كافية مسبقاً مكتوبة والتي سيتم استخدامها في السجل الذي يقتصر على البحوث الإحصائية أو سجل التقرير.

6-الى الأرشيف الوطني والسجلات الإدارية.

7-الى وكالة أخرى أو أي جهاز تابع لسيطرة الولايات المتحدة.

8-لشخص آخر لظروف قاهرة تؤثر على صحة الفرد أو سلامته.

9-أي من مجلسي الكونجرس.

10-المراقب المالي العام.

11-وفقاً لأمر صادر عن المحكمة.

12-للمستهلك وكالة التقرير[65] "

---

[65] Article 552/B of The Privacy Act of 1977

b) Conditions of disclosure

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except

pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of Title 31

وكان الهدف من هذا القانون تقرير حماية للأفراد من الاعتداءات التي قد تطال حياتهم الشخصية، حيث وضع قواعد لحمايتهم من الاطلاع على المعلومات الخاصة بهم والمحفوظة في الحاسب الآلي .

وقد أورد هذا القانون استثناءَ وهو نقل المعلومات عن طريق الموظفين القائمين على عملية التخزين لاستخدامها العادي والرسمي (المصلحة العامة)، وأعطى رقابة للقضاء لمراقبة تنفيذ القانون فيما يتعلق بعملية الجمع والتخزين (http://www.justice.gov./opl/privstat.htm) (قايد، 1994، 70)

وأعطى هذا القانون الحق للأسرة في مراجعة البيانات المسجلة في هذه المؤسسات والمتعلقة بأبنائها، وأيضاً أعطى الحق للعاملين في هذه المؤسسات في معرفة البيانات المسجلة عنهم فيها (عفيفي، لات، 287).

وكذلك قانون حماية السرية لسنة 1980، والذي يقيد حرية الموظفين الحكوميين أثناء بحثهم وضبطهم لمواد إنتاج العمل عن الأفراد الذين سوف يستعملونها في الاتصالات العامة، وعدم جواز إفشائها باعتبارها من الأسرار الشخصية (سليمان، لات، 200).

وقانون الخصوصية الأمريكي لعام 1984، والذي يعتبر أقوى بكثير من سابقه، والذي يعطي الحق للأفراد بإعلامهم عن ما يجمع عنهم من سجلات شخصية، ويعطيهم الحق في الاطلاع عليها وتصحيحها، ويمنع استخدام المعلومات التي تم جمعها في غير الأغراض التي جمعت من أجلها (الجنبيهي، منير وممدوح، 2005، 63).

ويحظر قانون سياسة الاتصالات السلكية لعام 1984 اختراق خصوصية الأفراد من خلال المكالمات الهاتفية التي تجري بينهم عبر الكابلات (عفيفي، لات، 288).

كما وأن قانون خصوصية الاتصالات الإلكترونية لعام 1986 (ECPA) قد فرض حماية لخصوصية الأفراد أثناء عملية الاتصال الإلكترونية وتبادل المعلومات، حيث جرم هذا القانون أفعال المراقبة غير المصرح بها للاتصالات إلكترونية المخزنة أو المتبادلة، بما فيها الاطلاع على رسائل البريد الإلكتروني والاتصالات الإلكترونية المخزنة، وجرّم أ يضاً الدخول غير المشروع إلى المراسلات والبيانات المخزنة في الحاسب الآلي . (http//floridalawfirm.com/privacy.html)

حيث جاءت المادة (1) من القسم 2511 من ذات القانون (ECPA) ، والخاصة باعتراض أو حجز أي اتصال برقي أو شفاهي أو اتصال الكتروني ونصت على أنه : "

1- باستثناء ما هو منصوص عليه تحديدا خلاف ذلك في هذا الفصل أي شخص:

A-اعترض بشكل مقصود ، أو سعى أو ساعد الغير على اعتراض أو حجز أي اتصال برقي أو شفاهي أو اتصال إلكتروني

B-استخدم بشكل مقصود، أو سعى لاستخدام أو ساعد الغير على استخدام أية أجهزة إلكترونية أو ميكانيكية أو غيرها لاعتراض أية اتصالات بهدف كشف محتوى الاتصالات السلكية أو الإلكترونية [66] ".

وجاء في نص المادة (4) من ذات القسم ، أنه يعاقب مرتكب هذه الأفعال على النحو المنصوص عليه في هذه المادة ، وتكون العقوبه الغرامة أو السجن لمدة لا تزيد على خمس سنوات أو بكلتا العقوبتين، وذلك باستثناء الحالات المنصوص عليها في الفقره B من ذات المادة [67] .

فالمشرع الأمريكي اهتم في هذا القانون بتجريم أفعال الاعتراض أو الحجز لأي اتصال برقي أو شفاهي، أو أي اتصال إلكتروني وكذلك مساعدة الغير على ذلك. (Rosenoer, 1999, p.170)

وتجدر الإشارة هنا أن الفقرتين A, B من القسم 2702 من ذات القانون ، جرمت أفعال الكشف عن محتوى الإتصالات الإلكترونية ومضمون الرسائل حيث نصت على أنه "

---

[66]Article 2511/1 of (ECPA) of 1986
Sec. 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who -

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when -

[67]Article 2511/4 of (ECPA) of 1986
(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

A- باستثناء الحالات المنصوص عليها في الفقرة الفرعية (B) من هذه المادة ، يحظر على أي شخص أو أية جهة تقدم خدمة الإتصال الإلكتروني الإفصاح عن محتوى الاتصالات.

B-لا يجوز لأي شخص أو جهة الكشف عن محتوى الرسائل إلا :

1-للمستلم أو المرسل اليه المقصود من هذه الإتصالات، أو من يمثل المرسل اليه أو المتلقي.

2-على النحو المسموح به في القسم 2517/2/A ، أو القسم 2703 من هذا القانون.

3- بموافقة قانونية من المنشيء أو المستلم.

4-لشخص يعمل في الخدمة لإعادة توجيه الرسالة على وجهتها.

5-لوكالة خاصة لإنفاذ القانون[68]."

---

[68] Article 2702/A,B of (ECPA) of 1986
(a) Prohibitions.--Except as provided in subsection (b)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--
(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(b) Exceptions.--A person or entity may divulge the contents of a communication–

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

وفي عام 1994 أصدر المشرع الأمريكي قانون مساعدة الاتصالات الخاص بتنفيذ القانون، كما وأصدر قانون أخلاق الاتصالات لسنة 1996، والذي جاء لحماية الحق في الخصوصية المتعلقة بحركة الاتصالات بالمراسلة الرقمية أو الالكترونية (يونس، 2004، 607).

كما واهتم المشرع الأمريكي بحماية الحياة الخاصة للأطفال، وذلك عن طريق قانون حماية خصوصية الأطفال عبر الإنترنت لعام 1998 ، والذي يحظر على مُعدي المواقع الإلكترونية والمتواجدة عبر الإنترنت نشر أية معلومات شخصية للأطفال الذين لا تتجاوز أعمارهم الثلاثة عشر عاماً إلا بإذن مسبق من أولياء الأمور، وكذلك ألزمهم بالمحافظة على هذه المعلومات في حال موافقة أولياء الأمور، وأصدر المشرع قانون لجنة التجارة الفيدرالية والذي أعطى صلاحيات لهذه اللجنة بمراقبة الخصوصية عبر الإنترنت (يونس، 2004، 607 وما بعدها).

أما المشرع الولائي الأمريكي فقد أقرت الكثير من الولايات ضمانات قانونية لحماية الحق في الخصوصية، إلا أنها اتبعت ذات النهج الفيدرالي من حيث اقتصارها على الأنشطة الحكومية، حيث جرم قانون العقوبات لولاية فلوريدا كل ولوج بسوء نية إلى النظام المعلوماتي بغرض الحصول على معلومات غير مسموح بها تتعلق بسمعة الغير، كما وجرم الأفعال التي تنطوي على إدخال معلومات مصطنعة بغرض تحسين أو إساءة سمعة الغير (العزام، 2009، 107).

ولما تقدم يرى الباحث أن المشرع الأمريكي سواء على المستوى الفيدرالي أو الولائي لم يضع تشريعاً خاصاً لحماية البيانات والمعلومات الإسمية المعالجة آلياً عبر النظام المعلوماتي، وإنما نظم ذلك عن طريق قوانين أخرى خاصة بحماية الخصوصية، ومن خلال استقراء القوانين السابقة يجد الباحث أنها كانت تركز على عملية تسجيل البيانات وكيفية الاطلاع عليها، وحق الأشخاص في الاعتراض عليها في حال الخطأ فيها، أو إخلالها بحق الخصوصية، إلا أن هذه الحماية أيضاً اقتصرت على الأنشطة الحكومية دون القطاع الخاص من مؤسسات وشركات حينما تقوم هذه الأخيرة بعملية جمع وتخزين ومعالجة آلية لبيانات ومعلومات اسمية تدخل في نطاق الحق في الخصوصية، وبذلك فإن المشرع الأمريكي لم يوفر الحماية الجنائية اللازمة للبيانات والمعلومات الشخصية الخاصة بالأفراد بنصوص مباشرة، إنما حماها بطريقة غير مباشرة بالنصوص العامة لحماية الخصوصية والمعلومات، وذلك على عكس المشرع الفرنسي الذي أصدر قانوناً خاصاً لحماية الحياة الخاصة في مواجهة نظم المعلومات وبنوك المعلومات.

---

(6) to a law enforcement agency--

ثالثا: موقف المشرع الفرنسي:

على خلاف المشرـع الأمريكي فقد أصـدر المشرـع الفرنسي القانون رقم (17) في 6 يناير لسنة 1978 والخاص بالمعالجة الإلكترونية والحريات، والذي يتعلق بحماية الحياة الخاصــة في مواجهة الأخطار الناشــئة عن استخدام الحاسبات الإلكترونية كبنوك للمعلومات (قايد، 1994، 62 وما بعدها).

وقد تضـــمن هذا القانون مجموعة من المبادئ والضـــمانات والتي من أهمها أن عملية المعالجة الآلية للبيانات والمعلومات لابد أن تكون في خدمة كل مواطن، ولا يجوز أن تلحق هذه العملية بأي إنسـان ضرراً بهويته أو حقوقه أو حياته الخاصـة ولا بحرياته الفردية أو العامة، وأعطي الحق لصـاحب البيانات في الوصول إليها والاطلاع عليها (المومني، 2008، 183).

وقد جاء هذا القانون أيضـاً بضـمانات لحماية الحق في الخصـوصـية من خلال النص على تشـكيل اللجنـة الوطنيـة للمعلومـاتيـة والحريـات، والتي تُعنى بمراقبـة احترام هـذا القانون من قبل القائمين عليه، وأوجبت على أية جهة قائمة على جمع وتخزين ومعالجة البيانات الشـخصـية إعلام هذه اللجنة قبل إجراء العملية باسـتثناء أجهزة الدولة ولكن بعد أخذ الموافقة أيضـاً، وجرم القانون عملية جمع وتسـجيل البيانات الشـخصية بوسائل غير مشروعة كالغش والتدليس، وكفل أيضاً للشخص الاعتراض على البيانات التي جُمعت عنه، وحقه في ضرورة إعلامه عن ما تم جمعه من بيانات خاصة به (عفيفي، لات، 291 وما بعدها).

وقد جاء المشرـع الفرنسيـ في قانون العقوبات الفرنسيـ الجديد والذي أصـبح سـاري المفعول عام 1994، ونص على أهم جرائم الاعتداء على حرمة الحياة الخاصة عبر النظام المعلوماتي، وذلك كما يلي:

المادة 226-15:

نصـت هذه المادة على تجريم " أفعال الإطلاع على رسـائل الغير الشـخصـية وذلك بسـوء نيه أو تدميرها أو فتح أو حذف أو تحويل المراسـلات المرسـلة إلى طرف ثالث، أو اسـتخدام طرق احتيالية للإطلاع على الرسـائل الشـخصـية، وأوجبت عقوبة على كل من يقوم بذلك بالسـجن لمدة سنة وغرامة 45000 يورو، كما وأوجبت ذات المادة نفس العقوبة على من يقوم باعتراض واستخدام وتحويل أو الكشف عن المراسلات المرسـلة أو المسـتقبلة عبر وسـائل الاتصـالات السـلكية أو اللاسـلكية عن طريق اسـتخدام جهاز مصمم لهذا الاعتراض [69] ".

---

[69] Article 226/15 Of (FCP)

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre

وفي القسم الخامس من ذات القانون والخاص بانتهاك الحقوق الشخصية الناتجة عن الحاسب الآلي أو العمليات، جاءت المواد 226-16 ولغاية 226-24، والخاصة بجرائم الاعتداء على حرمة الحياة الخاصة عبر النظام المعلوماتي وذلك كما يلي:

المادة 226-16:

نصت هذه المادة على جريمة المعالجة الآلية للبيانات الشخصية أو التسبب فيها ، وأوجبت عقوبة السجن لمدة خمس سنوات وغرامة 300000 يورو، حتى عندما ترتكب هذه الجريمة عن طريق الإهمال، وتطبق نفس العقوبات على الأفعال التي تطال معالجة البيانات أو التسبب في ذلك في حال الإهمال أو الشروع في الأفعال المنصوص عليها في المادة 45 من القانون رقم 78-17 لعام 1978 والخاص بتكنولوجيا المعلومات والحريات [70] ".

المادة 226-18:

---

frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.

Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.

[70] Article 226/16 Of (FCP)

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

نصـت هذه المادة على " معاقبة كل من يقوم بجمع البيانات الشخصية للأفراد بطريقة احتيالية أو غير قانونية بالسجن لمدة خمس سنوات وغرامة 300000 يورو [71]

المادة 226-19:

وقد نصـــت هذه المادة على أنه "إلا في الحالات التي ينص عليها القانون، لا يجوز لأحد تســـجيل معلومات شـخصـية خاصـة بالآخرين والاحتفاظ بها في ذاكرة حاسبه الآلي، بشكل مباشر أو غير مباشر ودون موافقتهم وتصـريح منهم، سـواء تعلقت هذه المعلومات بأصول الآخرين أو عرقهم أو أفكارهم وانتماءاتهم السـياسـية أو آرائهم الفلسفية أو الدينية أو انتماءاتهم النقابية أو أية معلومات صحية أو ميولهم الجنسية، وتكون العقوبة الســجن خمس ســنوات وغرامة 300000 يورو، ويعاقب بنفس العقوبة كل من احتفظ في ذاكرة الحاسب بمعلومات متعلقة بالجرائم والإدانات أو تدابير رقابية خارج الحالات التي نص عليها القانون ." [72]

المادة 226-20:

---

[71] Article 226/18 Of (FCP)

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

[72] Article 226/19 Of (FCP)

Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté.

ونصـــت على أنه " يكون الإبقاء على البيانات الشـــخصـــية وتحديد المدة وفقاً لما يحدده النظام الأساسي، عن طريق طلب إذن أو إخطار اللجنة الوطنية للمعلوماتية والحريات، وكل من يخرق ذلك يعاقب بالسجن لمدة خمس سنوات والغرامة 300000 يورو، ويستثنى من ذلك إذا كان الاحتفاظ بهذه البيانات من قبل أجهزة الدولة ولأغراض إ حصائية أو علمية وفقاً للشروط التي يحددها القانون [73] " .

لذلك يتعين على القائمين على عملية جمع البيانات الشـخصـية إخطار اللجنة الوطنية للمعلوماتية والحريات، والتي قد يؤدي نشرها إلى التقاطها أو تزويرها أو تدميرها أو الاستيلاء عليها، وتفرض اللجنة أيضاً ضرورة إخطار المواطنين بالمخاطر المترتبة على وضـع بياناتهم عبر النظام المعلوماتي، وحقهم في الاعتراض على نشرـ هذه البيانات في أي وقت، بالإضـافة إلى حقهم في الاطلاع علىها في أي وقت، وتصـحيحها ومحوها وفقاً لأسباب مشروعة.

المادة 226-21:

نصت هذه المادة على " جريمة إساءة البيانات والمعلومات الإسمية من خلال عدم التزام الجهة القائمة على عملية جمع البيانات الإســمية وتخزينها في الغاية من عملية الجمع، وإســاءة اســتعمال هذه البيانات، حيث يعاقب مرتكبها بالسجن خمسة سنوات وغرامة 300000 يورو [74]".

---

[73] Article 226/20 Of (FCP)

Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.

[74] Article 226/21 Of (FCP)

Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

المادة 226-22:

نصـــت هذه المادة على " تجريم أفعال الكشـــف عن المعلومات والبيانات المســـتخدمة في نظام المعالجة الآلية بدون إذن، وبشـــكل يؤدي الى الإضرار بســـمعة الشـــخص المعني أو يســـبب ضرراً في حياته الخاصة ، حيث يعاقب مرتكب هذه الأفعال بالسجن لمدة ثلاث سنوات وغرامة 300000 يورو وإذا ارتكبت هذه الأفعال نتيجة الإهمال أو اللامبالاه يعاقب الفاعل بالسـجن لمدة ثلاث سنوات والغرامة 100000 يورو، وفي الحالات المذكورة في الفقرتين الســـابقتين تســـمع الدعوى فقط بناءَ على شـــكوى المجني عليه أو وكيله القانوني [75] ".

المادة 226 – 24:

نصـت هذه المادة على أنه " يتحمل الأشخاص المعنوية المسؤولية الجنائية، وفقا للشروط المنصوص عليها في المادة 121-2 ، وذلك عن الجرائم المرتكبة والمنصوص عليها في هذا الفصل،

وتطبق عليهم العقوبات التالية:

1-الغرامات المالية وفقاً للشروط المنصوص عليها بموجب المادة 131-38 من ذات القانون،

---

[75] Article 226/22 Of (FCP)

Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

2-العقوبات المنصوص عليها في الفقرات 2-3-4-5-7-8-9 من المادة 131-39 ، إضافة الى الحظر المشار إليه في الفقرة 2 من ذات المادة [76] ".

وبذلك يرى الباحث أن المشرع الفرنسي قد وفر الحماية الجنائية اللازمة للحياة الخاصة من خطر بنوك المعلومات والمعالجة الآلية للبيانات والمعلومات الاسمية، وذلك بأن نص على ذلك صراحة بموجب القانون سالف الذكر، وشدد العقوبه لتصل الى الحبس لمدة خمس سنوات والغرامه لغاية 300000 يورو، وهذا على خلاف المشرع الأمريكي الذي نظم هذه الحماية بطريق غير مباشرة من خلال القوانين العامة الخاصة بالخصوصية والمعلومات.

المبحث الرابع: الاشتراك الجرمي والعقوبات ومسؤولية الأشخاص المعنوية في الجرائم المعلوماتيه:

الجريمة هي كل فعل أو امتناع عن فعل يحظره القانون ويقرر عقوبة لمرتكبه، وإذا كان صحيحاً أن معظم الجرائم تقوم بفعل إيجابي، فإنه من المسلم به أيضاً أن القانون الجزائي يعاقب كذلك على بعض صور الامتناع في الحالات التي يوجب القانون على الممتنع إتيان فعل معين في ظروف معينة فيمتنع عن إتيانه رغم قدرته على ذلك، وباعتبار الجريمة ذلك الفعل غير المشروع الصادر عن إرادة إجرامية يقرر القانون لهذا الفعل عقوبة أو تدبيراً احترازياً، وهذه الجريمة قد يرتكبها الجاني بمفرده بأن يقدم على تنفيذها وحده فلا تثار أية مشكلة ما دام أنه من يرتكب جريمة تقع عليه عقوبتها، إلا أنه أحياناً يساهم عدد من الجناة في تنفيذ جريمة واحدة فيقوم كل منهم بدوره في الجريمة

---

[76] Article 226/24 Of (FCP)

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section.

Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38 ;

2° Les peines mentionnées aux 2°, 3°, 4°, 5°, 7°, 8° et 9° de l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

وهذا ما يطلق عليه الاشتراك الجرمي، وللوقوف على أحكام الاشتراك الجرمي في الجرائم المعلوماتية، والعقوبات الواردة في قانون جرائم أنظمة المعلومات الأردني المؤقت، ومسؤولية الأشخاص المعنوية فقد تم تقسيم هذا المبحث وفقاً للمطالب التالية:

المطلب الأول:الاشتراك الجرمي.

المطلب الثاني: تحليل العقوبات طبقاً لخطة الشارع الأردني.

المطلب الثالث:مسؤولية الأشخاص المعنوية عن الجرائم المعلوماتية.

المطلب الأول: الاشتراك الجرمي:

الفرع الأول: الأحكام العامة في الاشتراك الجرمي:

يقصد بالاشتراك الجرمي تعدد الأشخاص الذين ارتكبوا الجريمة، ومعنى ذلك أن الاشتراك الجرمي يتطلب ركنين هما تعدد الجناة ووحدة الجريمة، والتعدد الذي تقوم به حالة الاشتراك الجرمي هو التعدد الاحتمالي (أو التعدد غير الضروري) أي التعدد غير اللازم لقيام الجريمة، لأنه إذا كان المشرع يتطلب تعدد الأشخاص في جريمة ما فلا نكون هناك بصدد اشتراك جرمي، إنما نكون بصدد ما يسمى بالتعدد الضروري والذي يعد ركناً من أركان الجريمة لا تقوم بدونه، فلا يمكن تصور قيام جريمة زنا – على سبيل المثال – من زوج دون أن تكون معه شريكه، كما لا يمكن أن تقوم جريمة رشوة من موظف دون أن يكون معه راش (المجالي، 2005، 280).

وعليه يتعين الوقوف عند النص القانوني الخاص بأية جريمة، والبحث فيما إذا كان التعدد ضمن عناصر تحقق هذا النص أم لا، فإذا لم يتطلبه المشرع فعندئذ يكون تعدد الجناة في ارتكاب الجريمة مع وحدتها هو اشتراك جرمي (المجالي، 2005، 280).

وحتى يتحقق الاشتراك الجرمي لابد أن يجمع بين عناصرها وحدة مادية ووحدة معنوية، وتتطلب الوحدة المادية أمرين الأول وحدة النتيجة الإجرامية، والثاني ارتباط هذه النتيجة بنشاط كل مساهم برابطة السببية، أما الوحدة المعنوية فتتمثل في الرابطة الذهنية والنفسية التي تقوم بين المشتركين في الجريمة، أي علم كل واحد من الجناة بالمشروع الإجرامي وانصراف إرادته لتحقيق نتيجته الجرمية (http://www.blog.amin.org/eyad/2010.com).

وقد ميز قانون العقوبات الأردني رقم (16) لسنة 1960 بين الشريك والمتدخل، فسمى الفاعل مع غيره شريكاً بحيث يقوم كل منهما بدور رئيس في التنفيذ، وذلك في المادة (76) من ذات القانون، أما المتدخل فتقتصر مساهمته في الجريمة على دور تبعي، وخص المحرض بمركز مستقل، وذلك وفقاً للمادة (80) من ذات القانون، وتطرق إلى جريمة إخفاء الأشياء المملوكة للغير والتي نزعت أو اختلست منه بارتكاب جناية أو جنحة، وجعلها جريمة مستقلة بحد ذاتها في المادة (83)، وفي غير الحالات المنصوص عليها في الفقرة (هـ) من المادة (80) من ذات القانون.

وعرف قانون العقوبات الأردني في المادة (75) فاعل الجريمة (الفاعل الأصلي) هو من أبرز إلى حيز الوجود العناصر التي تؤلف الجريمة أو ساهم مباشرة في تنفيذها، وقد يكون الفاعل مادياً بحيث يرتكب الجريمة وحده وبنفسه، كمن يقوم بإطلاق النار على رأس المجني عليه فيرديه قتيلاً، وقد يكون الفاعل معنوياً بحيث يحمل غيره على ارتكاب الفعل المكون للجريمة، فهذا لا يرتكب الجريمة بيديه وإنما يسخر غيره لتنفيذها إما لأن الغير حسن النية وإما لأنه "غير أهل لتحمل المسؤولية الجزائية" كالمجنون والصبي غير المميز، ومثال ذلك من يحرض مجنوناً على عدوه حتى يقتله فتقع الجريمة، ومثال الغير حسن النية كمن يطلب من الخادم في مقهى أن يسلمه معطفاً لأحد الزبائن م وهماً إياه أنه معطفه فيسلمه إياه بناءَ على هذا الإيهام (المجالي، 2005، 292).

أما المحرض فهو من يحمل غيره على ارتكاب جريمة بإعطائه نقوداً أو بتقديم هدية له، أو بالتأثير عليه بالتهديد أو بالحيلة والدسيسة (http://www.e-thesis.mutah.edu.jo).

ولم يعرف قانون العقوبات التدخل مما اضطر الفقه لتعريفه بأنه "العمل الذي يرتكبه المساهم في الجريمة ويساعد على تنفيذ الجريمة، دون أن يشكل هذا النشاط عملاً تنفيذياً للجريمة، كما لو كان المساهم فاعلاً أو شريكاً" (المجالي، 2005، 299) ، لذلك فالمتدخل من يباشر نشاطاً تبعياً(غير تنفيذي) في الجريمة، إلا أن نشاطه لا يشترط فيه أن يكون ثانوياً، بل قد يكون رئيسياً في إرتكاب الجريمة، كالمتدخل الذي يعطي سلاح الجريمة للفاعل أو الذي يعطي شيفرة الخزنة للسارق.

وقد حصر قانون العقوبات الأردني الحالات التي يعتبر فيها الشخص متدخلاً في جريمة في الفقرة الثانية من المادة (80) وهي ست حالات.

وبمقتضى المادة (81) فقد عاقب قانون العقوبات المحرض والمتدخل بما يلي:

1- أ. بالأشغال الشاقة المؤبدة أو بالأشغال الشاقة من عشرين سنة إلى خمس وعشرين سنة إذا كانت عقوبة الفاعل الإعدام.

ب. بالعقوبة ذاتها عشرين سنة إذا كانت عقوبة الفاعل الأشغال الشاقة المؤبدة أو الاعتقال المؤبد.

2- في الحالات الأخرى يعاقب المحرض والمتدخل بعقوبة الفاعل بعد أن تخفض مدتها من السدس إلى الثلث.

3- إذا لم يفض التحريض على ارتكاب جناية أو جنحة إلى نتيجة خفضت العقوبة المبينة في الفقريتين السابقتين من هذه المادة إلى ثلثها.

ولا يعاقب المتدخل إلا إذا تحقق شرطان وهما:

1- أن يكون الفعل الذي تدخل فيه جناية أو جنحة، فلا عقاب على التدخل بمخالفة وفقاً لنص المادة (82) عقوبات أردني.

2- أن يكون التدخل بإحدى الوسائل المحددة في القانون.

(http:www.blog.amin.org/eyad/2010.com)

الفرع الثاني: الاشتراك الجرمي في الجرائم المعلوماتية:

قد تتم الجريمة المعلوماتيه عن طريق تعاون أكثر من شخص على ارتكابها وذلك إضراراً بالجهة المجني عليها، والمثال على ذلك أن يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والإنترنت، بحيث يقوم بالجانب الفني من المشروع الإجرامي، ويساعده شخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

(http://www.shabab20.net/index.php?option=com)

وقد عالج المشرع الأردني موضوع الإشتراك الجرمي في الجرائم المعلوماتية وذلك في المادة (13) والمادة (14) من قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010.

حيث نصت المادة (13) على أنه "يعاقب كل من قام قصداً بالاشتراك أو التدخل أو التحريض على ارتكاب أي من الجرائم المنصوص عليها في هذا القانون بالعقوبة المحددة لمُرتكبيها".

ونصت المادة (14) على أنه "كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية، أو أية نظام معلومات أو اشترك أو تدخل أو حرض على ارتكابها، يعاقب بالعقوبة المنصوص عليها في ذلك التشريع".

ووفقاً لنص المادة (13) فقد عاقب المشرـع الأردني الشرـيك والمتدخل والمحرض بالعقوبة المحددة للفـاعـل الأصـــلي للجريمة المعلوماتية، وهذا على خلاف القواعد التقليدية في قانون العقوبات الأردني والتي ســـاوت في العقوبة بين الفاعل الأصـــلي عندما يرتكب الجريمة لوحده، وبين الشرـكاء الذين يرتكبون هذه الجريمـة، بحيـث يعـاقب كل منهم بالعقوبة المعينة للجريمة في القانون كما لو كان فاعلاً مســـتقلاً، وخفض المشرع التقليدي عقوبة المحرض والمتدخل عن عقوبة الفاعل الأصلي أو الشريك.

ووفقاً لنص المادة (14) فقد عاقب المشرـع الأردني الشريك والمتدخل والمحرض في الجرائم المعاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتيه بالعقوبة المنصوص عليها في ذلك التشريع.

وقد ضـاعف المشرـع الأردني العقوبة المنصوص عليها في هذا القانون في حال تكرار أي من الجرائم الوارده فيه، وذلك وفقاً لنص المادة (15) منه.

المطلب الثاني: تحليل العقوبات ط بقاً لخطة الشارع الأردني في قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010:

بعد دراسـة الإشـتراك الجرمي في الجرائم المعلوماتيه طبقاً لخطة الشـارع الأردني فإننا سوف نتناول في هذا المطلب العقوبات المنصوص عليها في القانون المؤقت، سواء من جهة العقوبات الأصلية أو العقوبات غير الأصلية أي العقوبات الإضافية (التكميلية).

الفرع الأول: العقوبات الأصلية:

يمكن اســـتخلاص العقوبات الأصـــلية الواردة في قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010 وذلك كما يلي

أولاً: الأشغال الشاقة المؤقتة:

تُعد عقوبة الأشـــغال الشـــاقة المؤقتة من العقوبات الجنائية طبقاً لقانون العقوبات الأردني، وقد عرفت المادة (18) من ذات القانون الأشـغال الشـاقة بأنها "تشـغيل المحكوم عليه في الأشـغال التي تتناسب وصحته وسنه، سواء في داخل السجن أو خارجه".

وتدور عقوبة الأشـغال الشاقة المؤقتة بين حدين، أدنى وهو ثلاث سنوات وأقصى وهو عشرون سنه، وذلك طبقاً لنص الفقرة الثانية من المادة (20) من ذات القانون.

وقد خصص المشرع الأردني في قانون جرائم أنظمة المعلومات المؤقت عقوبة الأشغال الشاقة المؤقتة لثلاث جنايات معلوماتية وهي:

(1) جناية الاستغلال المقصود للقصر والمعا قين نفسياً أو عقلياً في الدعارة أو الأعمال الإباحية باستخدام نظام المعلومات أو الشبكة المعلوماتية. م(8/ج)

(2) جناية إنشاء موقع إلكتروني للقيام بأعمال إرهابية، أو دعم جماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية لاتباع أفكارها أو تمويلها، وذلك باستخدام نظام المعلومات أو الشبكة المعلوماتية. م(10).

(3) جناية الدخول المقصود وبدون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو نظام معلومات بأية وسيلة كانت، بقصد إلغاء أو إتلاف أو تدمير أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني، أو العلاقات الخارجية للمملكة، أو السلامة العامة أو الاقتصاد الوطني.

ثانياً: الحبس:

تعتبر عقوبة الحـ بس عقوبة أصلية للجنح طبقاً لنص المادة (15) من قانون العقوبات الأردني، وقد عرفت المادة (21) من ذات القانون الحبس بأنه "وضع المحكوم عليه في أحد سجون الدولة المدة المحكوم بها عليه، وهي تتراوح بين أسبوع وثلاث سنوات، إلا إذا نص القانون على خلاف ذلك" أما الحبس التكديري فهي عقوبة أصلية مقررة لمواد المخالفات، وتتراوح بين أربع وعشرين ساعة وأسبوع، ونصت المادة (23) من قانون العقوبات على أن تنفذ هذه العقوبة في المحكوم عليه في أماكن غير الأماكن المخصصة بالمحكوم عليه بعقوبات جنائية أو جنحية ما أمكن.

وقد خصص المشرع الأردني في قانون جرائم أنظمة المعلومات المؤقت عقوبة الحبس لعشر جنح معلوماتية وهي كما يلي:

(1) جنحة الدخول المقصود إلى موقع إلكتروني أو نظام معلومات بأية وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح. م3/أ.

(2) جنحة الدخول المقصود إلى موقع إلكتروني أو نظام معلومات بأية وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بهدف إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو توقيف أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه. م3/ب.

(3) جنحة إدخال أو نشر أو الاستخدام المقصود لبرنامج عن طريق الشبكة المعلوماتية أو باستخدام نظام معلومات، بهدف إلغاء أو حذف أو تدمير أو إتلاف أو حجب أو التقاط، أو الإطلاع على بيانات أو معلومات أو إعاقة أو تعطيل عمل النظام المعلوماتي. م(4).

(4) جنحة الالتقاط أو الاعتراض أو التنصت المقصود على الرسائل المرسلة عبر الشبكة المعلوماتية. م(5).

(5) جنحة الحصول المقصود دون تصريح وعن طريق الشبكة المعلوماتية على بيانات أو معلومات تتعلق ببطاقات الإئتمان،أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية. م6/أ.

وكذلك إذا استخدم الجاني هذه البيانات أو المعلومات للحصول لنفسه أو لغيره على بيانات أو معلومات أو أموال أو خدمات تخص الآخرين. م6/أ.

(6) جنحة نشر أعمال إباحية، أو الاستغلال الجنسي للقصر عبر الشبكة المعلوماتية. م8/أ.

(7) جنحة إعداد أو حفظ أو عرض أو طباعة أو نشر أو ترويج أعمال إباحية، للتأثير على القصر أو المعاقين نفسياً أو عقلياً، أو تحريضهم على ارتكاب الجريمة. م8/ب.

(8) جنحة الترويج للدعارة عبر الشبكة المعلوماتية.

(9) جنحة الدخول المقصود دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو نظام معلوماتي، بهدف الإطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني، أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.

ثالثاً: الغرامة:

تعتبر الغرامة العقوبة المالية الأصلية في الجنح والمخالفات وفق نص المادتين 15، 16 من قانون العقوبات الأردني، ففي الجنح تتقرر الغرامة إلى جانب الحبس كعقوبة وجوبية أو منفردة، أو مع الحبس على سبيل التخيير.

وقد عرفت المادة (22) من ذات القانون الغرامة بأنها "إلزام المحكوم عليه بأن يدفع إلى خزينة الحكومة المبلغ المقرر في الحكم، وهي تتراوح بين ثلاثين ديناراً ومائتي دينار، إلا إذا نص القانون على أكثر من ذلك، وذلك وفق شروط معنية في القانون".

وفي قانون جرائم أنظمة المعلومات الأردني المؤقت أورد المشرع الأردني في بعض المواد عقوبة الغرامة إلى جانب الحبس أو الأشغال الشاقة المؤقتة، وفي مواد أخرى أوردها مع الحبس على سبيل التخيير.

الفرع الثاني: العقوبات الإضافية (التكميلية):

أورد المشرع الأردني في قانون جرائم أنظمة المعلومات الأردني المؤقت عقوبة مصادرة الأجهزه والأدوات والوسائل المستخدمه في الجريمة وتوقيف أوتعطيل عمل النظام المعلوماتي أو الموقع الإلكتروني المستخدم لارتكابها ومصادرة الأموال المتحصله منها كعقوبات إضافية تلحق بجريمة معينة من الجرائم الواردة في ذات القانون، حيث نصت الفقرة ج من المادة (12) منه على أنه "للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل وتوقيف أو تعطيل عمل أي نظام معلومات، أو موقع إلكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون، ومصادرة الأموال المتحصلة من تلك الجرائم والحُكم بإزالة المخالفة على نفقة مرتكب الجريمة".

ووفقاً لهذا النص فقد أجاز المشرع للمحكمة المختصة – في جريمة نص عليها في قانون جرائم أنظمة المعلومات المؤقت – أن تحكم بمصادرة الأجهزة والأدوات أو غيرها من الوسائل التي إستخدمت في هذه الجريمة المعلوماتية، وكذلك الأموال المتحصلة منها، ومن جهة أخرى أجاز المشرع كذلك للمحكمة أن تحكم بتوقيف أو تعطيل عمل النظام المعلوماتي أو الموقع الإلكتروني المستخدم في ارتكاب أي من الجرائم المنصوص عليها في ذات القانون.

المطلب الثالث: مسؤولية الأشخاص المعنوية في الجرائم المعلوماتية:

لم ينص قانون جرائم أنظمة المعلومات المؤقت على مسؤولية الأشخاص المعنوية، ولم يتطرق إلى الجرائم المعلوماتية التي قد ترتكب باسم الشخص المعنوي عن طريق أعضاء إدارته أو مديرية أو ممثليه أو عماله، إلا أن الفقرة الثانية من المادة (74) من قانون العقوبات الأردني نصت على أنه:

"يعتبر الشخص المعنوي باستثناء الدائرة الحكومية أو المؤسسة الرسمية أو العامة مسؤولاً جزائياً عن أعمال رئيسه، أو أي من أعضاء إدارته أو مديريه أو أي من ممثليه أو عماله، عندما يأتون هذه الأعمال باسمه أو بإحدى وسائله بصفته شخصاً معنوياً".

كما ونصت الفقرة الثالثة من ذات المادة على أنه "لا يحكم على الأشخاص المعنويين إلا بالغرامة والمصادرة".

وهذا على خلاف قانون العقوبات الفرنسي ـ الجديد لسنة 1994 الذي حدد مسؤولية الأشخاص المعنوية في الجرائم المعلوماتية التي ترتكب باسمهم أو بأحد وسائلهم، وذلك بنص صريح في كافة الجرائم المعلوماتية التي نص عليها.

والمثال على ذلك المادة 323-6 من ذات القانون، والخاصة بالعقوبات التي توقع على الأشخاص المعنوية في حال إرتكاب أي من الجرائم المعلوماتية المنصوص عليها في ذلك الفصل، والتي ترتكب باسمهم أو بأحد وسائلهم ،حيث نصت هذه المادة على أنه:

" يتحمل الأشخاص المعنوية المسؤولية الجنائية عن الجرائم المشار اليها في هذا الفصل ، وفقا للشروط المنصوص عليها في المادة 121-2 ،

وتطبق عليهم العقوبات التالية:

1- الغرامات المالية وفقاً للشروط المنصوص عليها بموجب المادة 131-38 من ذات القانون،

2-العقوبات المنصوص عليها في المادة 131-39 ، إضافة الى الحظر المشار إليه في الفقرة 2 من ذات المادة "(77)

ويرى الباحث أنه ونتيجة عدم النص على مسؤولية الأشخاص المعنوية عن الجرائم المعلوماتية في قانون جرائم أنظمة المعلومات الأردني المؤقت، فإنه يتم تطبيق القاعدة العامة الواردة في المادة (74) من قانون العقوبات الأردني والتي تنص على المسؤولية الجزائية للأشخاص المعنوية والعقوبات.

---

(77) Article 323/6 Of (FCP)

Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

1° L'amende, suivant les modalités prévues par l'article 131-38 ;

2° Les peines mentionnées à l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

الفصل الخامس-

النتائج والتوصيات:

بعد الحمد لله رب العالمين إنتهينا من هذه الدراسة عن مدى الحماية الجنائية للمعلومات المعالجة آلياً والمخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت، وذلك من خلال البحث في موضوع الحماية في نطاق النصوص التقليدية لجرائم الأموال الواردة في قانون العقوبات الأردني، وفي نطاق الجرائم التقنية المستحدثة عبر النظام المعلوماتي، بهدف تحديد مدى كفاية التشريعات الأردنية لمعالجة هذه الجرائم الواقعة على المعلومات عبر النظام المعلوماتي مقارنة بالتشريع الأمريكي، وبيان مدى الحاجة إلى نصوص قانونية خاصة أو تعديلات على النصوص الحالية لتوفير هذه الحماية، ونبين في خاتمة البحث أهم النتائج التي توصلنا إليها من خلال دراسة هذا الموضوع، والتوصيات المقترحة وذلك كما يلي:

أولاً- النتائج:

نبين فيما يلي أهم النتائج التي توصل إليها الباحث من خلال هذه الدراسة:

1- تحديد الطبيعة القانونية للمعلومات المعالجة آلياً والمخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت، بأنها ذات طبيعة خاصة معنوية وغير محسوسة بعيدة كل البعد عن الطبيعة المادية للأشياء والأموال التي هي محل جرائم الأموال في النصوص العقابية التقليدية، إلا أنه بتوافر صفات الذاتية والاستقلال لهذه المعلومات فهي تعد قيمة بذاتها دون ارتباطها بالوسائط المادية (الدعامات)، وهي ذات قيمة اقتصادية معينة، نظراً لما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية، فقد تكون هذه المعلومات مالية خاصة بالأموال والاستثمارات وفي هذه الحالة إمكانية اعتبارها سلعاً تُباع وتُشترى، وإمكانية أن تكون محلاً للعقود شأنها شأن الأموال، وقد تكون تجارية وصناعية تتعلق بالدراسات الخاصة بالأسواق ومشروعات الاستثمار والتصنيع والإنتاج والتوزيع، وقد تكون اسميه خاصة بالحياة الخاصة للأفراد، وقد تكون متعلقة بأسرار الدولة الاقتصادية أو الصناعية أو السياسية أو العسكرية أو غيرها من مناحي الحياة التي يمكن أن تمثلها هذه المعلومات من قيم أو أموال أو أصول أو أسرار.

2- عدم وجود تعريف مُجمع عليه للجريمة المعلوماتية، ولم تُعرف التشـريعات العربية هذه الجريمة، وكل مـا هنـالك هي محاولات فقهية تحاول إيجاد تعريف جامع لأنماط هذه الجريمة المعلوماتية، وقد عرف الباحث الجريمة المعلوماتية الواقعة على المعلومات المعالجة آلياً بأنها "كل دخول مقصـود وغير مصرـح بـه إلى نظـام الحـاســب الآلي، يؤدي إلى الاعتـداء على معطياته المعنوية وكياناته المنطقية بأية طريقة تقنية".

3- إن كل جرم يمس مصــلحة يقدر الشــارع أهمية التدخل لحمايتها، والمصــلحة محل الحماية في ميدان الجرائم المعلوماتية هي الحق في المعلومات بمفهومها الواســع (كعنصرــ معنوي ذي قيمة اقتصــادية عالية) ويمتد تعبير الحق في المعلومات ليشـمل الحق في إنسـيابها وتدفقها وتبادلها وتنظيم اسـتخدامها، والحق في المعلومات بذاتها، أو بما تمثله من أموال أو أصـول أو أسرار أو بيانات شـخصية وكل ذلك على نحو مشروع دون مساس بحقوق الآخرين في المعلومات.

4- عـدم وجود تعريف واضــح ومحدد لكافة الجرائم التقنية المتنوعة والتي تقع على المعلومات المعالجة آلياً سـواء المخزنة في الحاسـب الآلي أو المتداولة عبر شـبكة الإنترنت، كجريمة سرقة المعلومات المعالجة آلـ يـاً، وجريمـة الإتلاف المعلومـاتي، والاحتيـال المعلومـاتي، والتجســس المعلومـاتي، وغيرهـا من الجرائم المعلوماتية، وكل ما هنالك هي عبارة عن محاولات ودراســات فقهية قانونية حاولت بيان كيفية وقوع هذه الجرائم وأساليبها ووسائلها التقنية والمختلفة عن الجرائم التقليدية.

5- وفقـ اً للنظم القانونية التقليدية فقد تأسـسـت قواعد حماية الأموال من مخاطر الجريمة بوجه عام على حماية المال المادي المحسوس أي المال ذو الوجود المادي، وكذلك التعامل مع محل الجريمة الملموس ذي الطبيعة المادية، والتعامل أيضـاً مع سـلوك جرمي ينتمي إلى عالم السـلوكات المادية، وهذا هو الاتجاه التشرـيعي العام لمختلف قوانين العقوبات الموضـوعية، وسـبب الإشكالية في إطار جرائم الأموال هو أن مفهوم المال فقهاً وقضـاءَ هو الشيـء المنقول ذو الطبيعة المادية، وإن مفهوم الاختلاس والاسـتيلاء هو بالضرـورة الاعتداء على الملكية والحيازة، وهو ما اسـتقر عليه التفسـير الفقهي والقضـائي، إلا أنه يمكن اسـتيعاب النصوص القانونية لخلاف ذلك، الأمر الذي لا يتصور معه تطبيق النصوص الجزائية التقليدية على الجرائم الواقعـة على المعلومات المعالجة آلياً والمخزنة في الحاســب الآلي أو المتداولة عبر شــبكة الإنترنت،

نظراً لطبيعتها المعنوية المختلفة عن الأموال المشمولة بحماية النصوص الجزائية وذلك كما يلي:

- صعوبة تطبيق نص المادة (399) من قانون العقوبات الأردني على جريمة سرقة المعلومات المعالجة آلياً نظراً للطبيعة الخاصة لهذه المعلومات، ولأن مفهوم فعل الأخذ (الاستيلاء) المكون للركن المادي في جريمة السرقة التقليدية لا يمكن تصوره في الحالة التي يقوم بها الفاعل بالحصول على المعلومات المخزنة في الحاسب الآلي دون وجه حق، ففي كل الحالات لا تنتهي حيازة المجني عليه لهذه المعلومات، كما وأن المال الذي يصلح محلاً لجريمة السرقة التقليدية هو المال المادي المنقول، والذي له كيان خارجي ويشغل حيزاً في محيطنا ويمكن لمسه، وبالتالي فإن المعلومات المعالجة آلياً لا تصلح محلاً لجريمة السرقة لكونها مالاً معنوياً يتجرد من الصفة المادية.
- صعوبة تطبيق نص المادة (417) من قانون العقوبات الأردني على جريمة الاحتيال المعلوماتي والتي تتم بالأساليب والطرق التقنية، لأن الاحتيال في المفهوم التقليدي يستوجب أن تقع الأفعال الاحتيالية في إطار العلاقات الإنسانية، أي من المحتال في مواجهة إنسان آخر وليس آلة (جهاز الحاسب الآلي).
- صعوبة تطبيق نص المادة (445) من قانون العقوبات الأردني على جريمة الإتلاف المعلوماتي، نظراً لاستحالة أن تكون المعلومات المعالجة آلياً محلاً لهذه الجريمة، والتي تقع على مال منقول مملوك للغير.

وتماشياً مع مبدأ شرعية الجرائم والعقوبات، فإن النصوص الجزائية الخاصة بجرائم الأموال التقليدية لا يمكن تطبيقها على الجرائم المعلوماتية التي تطال بالاعتداء المعلومات المعالجة آلياً والمخزنة في الحاسب الآلي، أو المتداولة عبر شبكة الإنترنت.

6- لم يرد في قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010 أي نص صريح بشأن جريمة سرقة المعلومات المعالجة آلياً، أو الاحتيال المعلوماتي أو غيرها من جرائم الأموال باستثناء جريمة الإتلاف المعلوماتي، وكل ما هنالك أن المشرع الأردني نص في الفقرة (أ) من المادة (6) من ذات القانون على جريمة الحصول قصداً ودون تصريح عن طريق النظام المعلوماتي على بيانات أو معلومات معالجة آلياً تتعلق ببطاقات الائتمان، أو تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية، كما ونص في الفقرة (ب) من ذات المادة على جريمة الاستخدام القصدي وغير المشروع للبيانات والمعلومات المعالجة آلياً، والمتعلقة ببطاقات الائتمان، أو تستخدمه في تنفيذ المعاملات المالية، أو المصرفية الإلكترونية، للحصول على منفعة مادية.

7- ومن البحث في جريمة الدخول غير المصرـــح به إلى النظام المعلوماتي، والتي قد تكون جريمة قائمة بحد ذاتها دون انتظار أفعالاً لاحقة، أو قد تكون مرحلة ســـابقة لارتكاب جرائم معلوماتية أخرى كجريمة الحصول على المعلومات المعالجة آلياً، أو جريمة التزوير، أو الإحتيال المعلوماتي، أو الإتلاف المعلوماتي أو غيرها، حيث انقسمت الآراء الفقهية بهذا الأمر إلى مسارين:

المسار الأول: تتمثل فكرة أصحابه أنه لا ضرورة لتجريم مجرد الدخول غير المصرح به إلى النظام المعلوماتي، إذا لم تتجه نية الجاني لارتكاب جريمة لاحقة على هذا الدخول، وذلك لأن هذه الأفعال بحد ذاتها لا تشـــكل جريمة ولا تســـتوجب العقاب، لأن الفاعل هدفه منها عرض قدراته التقنية والذهنية للتغلب على النظام.

المســـار الثاني: ويذهب أصـــحابه إلى ضرورة تجريم هذه الأفعال حتى لو لم تكن بقصـــد ارتكاب جرائم معلوماتية لاحقة، لأن هذه الأفعال قد يترتب عليها خســـائر مادية فادحة، وبالتالي فهي جرائم معلوماتية تستوجب العقاب.

وقد تضـــمن قانون جرائم أنظمة المعلومات الأردني المؤقت تجريم أفعال الدخول غير المصرـــح به للنظام المعلوماتي، أو تجاوز الصـــلاحية في الدخول إلى النظام، حيث عاقب المشرـــع على مجرد الدخول غير المشروع بصرف النظر سواء ترتب على هذا الفعل ضرر للغير أم لم يترتب، وشدد العقوبة في حال إذا كان الهدف من الدخول إتلاف أو تدمير أو إفشاء المعلومات المعالجة آلياً.

8- لم يرد في قانون جرائم أنظمة المعلومات الأردني المؤقت أي نص على جريمة البقاء غير المصرـــح به في النظام المعلوماتي، الأمر الذي يشـــكل خطورة على هذا النظام، لأن هذه الجريمة مرتبطة ارتباطاً وثيقاً بجريمة الدخول غير المصرح به للنظام المعلوماتي، ولا يمكن تصورها دون دخول إلى النظام سواء تمثل ذلك بشكل قصدي أم غير قصدي (بالصدفة)، وتثور الإشكالية في حالة دخول الفاعل للنظام بمحض الصدفة وبدون قصد، وتماشياً مع النص السابق والوارد في قانون جرائم أنظمة المعلومات الأردني المؤقت فإن هذا الدخول غير معاقب عليه، لذلك فإن بقاء الفاعل في النظام والناتج عن دخول غير مقصود هو غير معاقب عليه، وهذا يؤدي إلى إفلات الفاعل من العقاب، ويشـــكل خطورة كبيرة على النظام المعلوماتي، حيث أن فعل البقاء قد ينطوي على أفعال أخرى، بحيث لا يكتفي الفاعل بالبقاء في النظام، وإنما يرتكب جرائم معلوماتية أشد خطورة من خلال تجواله بين المعلومات والبرامج والمواقع الإلكترونية الموجودة في هذا النظام.

9- لا يمكن تطبيق النصـــوص التقليـديـة الواردة في قانون العقوبات الأردني على حالات التزوير المعلوماتي التي تطـال المعطيـات المعنويـة للنظـام المعلوماتي من بيانات ومعلومات معالجة آلياً إلا إذا كانت على شـكل مسـتند إلكتروني باعتباره أحد مسـتخرجات الحاسب الآلي، كالمستند المستخرج من الآلة الطابعة للجهاز، والناتج عن عملية فنية داخل النظام المعلوماتي، والذي يكون على صـــورة المحرر المكتوب، أما إذا وقع تغيير الحقيقة على مســتخرجات الحاســب الآلي الأخرى اللاورقية كالدعامات المادية والأشرطة الممغنطة والأقراص المدمجة، أو على المعلومات المعالجة آلياً والمخزنة في الحاســب الآلي، فإن النصــوص التقليدية لا يمكن تطبيقها على هذه الحالات.

10- لم تتضـمن القوانين الخاصـة الأردنية سـواء قانون الاتصـالات، أو قانون المعاملات الإلكترونية، أو قانون جرائم أنظمة المعلومات الأردني المؤقت، النص على جريمة التزوير المعلوماتي وصـورها المتمثلة في أفعال الإدخـال أو الإتلاف أو المحو أو الطمس العمـدي وبـ دون وجـه حق للبيانات والمعلومات المعالجة آلياً، لاستخراج بيانات ومعلومات غير صحيحة بقصد استخدامها لأغراض قانونية كما لو كانت صحيحة.

11- أسبغ المشرع الأردني الحماية الجنائية على البيانات والمعلومات المعالجة آلياً والخاصة بالأمن الوطني أو العلاقـات الخارجية للمملكة أو الســـلامة العامة أو الاقتصـــاد الوطني وذلك في المادة (11) من قانون جرائم أنظمة المعلومات الأردني المؤقت، والتي جرمت أفعال الدخول المقصـــود وغير المشـــروع للنظام المعلوماتي بهدف الاطلاع على هذه البيانات والمعلومات، وشـــددت العقوبة أيضـــاً إذا كان الهدف من ذلك بقصد إلغاء أو إتلاف أو تدمير أو تعديل أو تغيير أو نسخ تلك البيانات والمعلومات، إلا أنه لم ينص صراحة على جريمة التجســـس المعلوماتي والتي تقع على هذه المعلومات، ولم يتطرق أيضـــاً للوســـائل التقنية المسـتخدمة في ارتكاب هذه الجريمة، كما وأن العقوبة الواردة في المادة 11/أ لا تتناسب وطبيعة هذه البيانات والمعلومات، والتي يشـــكل الاطلاع ع ليها خطورة كبيرة على الدولة، فالمشـــرع هنا لم يراعِ التوازن والتنـاســـب بين الفعل المجرم وبين العقوبة المقررة ضـــمن القانون، ويمثل انعدام التوازن هذا خروجاً على المبادئ المستقرة في التشريعات الجزائية المعاصرة.

12- ومن البحث في مفهوم بنوك المعلومات في مجال الأنظمة المعلوماتية، اتضح بأنها قاعدة البيانات المعالجة آلياً والمتعلقة بتخزين المعلومات الاسمية والبيانات الشخصية التي تتعلق بالحياة الخاصة للأفراد، كالمعلومات الخاصة بحالتهم الصحية، والمالية والوظيفية والمهنية والعائلية والعلاقات الخاصة وغيرها، عندما تكون هذه البيانات محلاً للمعالجة الآلية في النظام المعلوماتي، سيما وأن بنوك المعلومات تنطوي على أخطار جسيمة على الحياة الخاصة للأفراد مقارنةً بالوسائل التقليدية، خاصةً فيما لو استخدمت في غير الأغراض المعدة لها.

13- لم يتضمن قانون جرائم أنظمة المعلومات الأردني المؤقت أي نص يتعلق بالبيانات والمعلومات الإسمية والمتعلقة بالحياة الشخصية للأفراد، كما وأنه لم يرد في هذا القانون أي نص يتعلق ببنوك المعلومات وطبيعتها ومدى خطورتها على الحياة الشخصية للأفراد في نطاق الأنظمة المعلوماتية، وكل ما هنالك وردت نصوص عامة لحماية البيانات والمعلومات المعالجة آلياً من بعض صور الاعتداءات التي قد تطالها عن طريق الأنظمة المعلوماتية، دون تحديد طبيعة هذه المعلومات، ولم يرد أي نص في ذات القانون حول تحديد المعلومات الاسمية والشخصية، كما وأنه لم يحدد الطرق والأساليب التقنية لانتهاك الحق في الخصوصية، وانتهاك الحياة الخاصة للأفراد في البيئة الرقمية، وأخطار بنوك المعلومات على الحياة الخاصة في نطاق الأنظمة المعلوماتية.

14- ليس هناك أية قواعد قانونية في النظام القانوني الأردني تقرر ضوابط معينة على الجهات الحكومية، بشأن جمع البيانات والمعلومات المعالجة آلياً والمتعلقة بالحياة الخاصة للأفراد، ولم تقرر أية مسؤولية مدنية أو جزائية في حال تجاوز عملية الجمع أو الاستغلال لمثل هذه المعلومات في حال استخدامها لغير الأغراض التي جمعت من أجلها، والتي تؤدي إلى انتهاك الحق في الخصوصية التي تنادت به معظم الدساتير.

15- إن ظهور الجرائم المعلوماتية أدى إلى وجود تحديات كبيرة تواجه الدول، وفي الوقت الراهن، ومع وجود بعض الاتفاقيات والمعاهدات الدولية الخاصة بمثل هذه الجرائم، إلا أنها غير كافية للإحاطة بكافة جوانب الحماية اللازمة للبيانات والمعلومات المعالجة آلياً من صور الجرائم التي تقع عليها، سيما مع تطور الأساليب والوسائل التقنية لارتكاب هذه الجرائم عبر النظام المعلوماتي، فهي جرائم مستحدثة ومتطورة وبشكل سريع تسبق التشريعات الدولية والوطنية دائماً.

ثانيا- التوصيات:

وبناءً على ما تقدم من نتائج، فإن هذه الدراسة توصي بما يلي:

1- وجوب تدخل المشرع الجزائي الأردني بالنص صراحةً لتحديد مفهوم الجرائم المعلوماتية، والتي تقع على المعلومات المعالجة آلياً، سواء المخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت، وذلك بتحديد صور هذه الجرائم وعناصرها وأركانها وأساليبها التقنية الإجرامية، وعدم ترك المجال مفتوحاً لمجرمي المعلوماتية لارتكابها وإفلاتهم من العقاب، في ظل قصور النصوص الجزائية القائمة عن استيعاب كافة صور هذه الجرائم.

2- ضرورة تخلي المشرع الأردني عن الأسلوب التقليدي في النصوص الجزائية، وضرورة استيعابه للطبيعة القانونية الخاصة للمعلومات المعالجة آلياً ذات الطبيعة المعنوية، بحيث يعطي مفهوماً أشمل للمال حتى يستوعب الأموال المعلوماتية المعنوية (المعلومات)، وذلك بتعديل نصوص قانون العقوبات التقليدية والخاصة بجرائم الأموال، من خلال تخلي المشرع عن فكرة المال المادي الملموس، وأن يصبح مفهوم المال يشمل كل شيء ينطوي على قيمة، بصرف النظر عن طبيعته، وبذلك تستوعب هذه النصوص في طياتها المعلومات المعالجة آلياً في النظام المعلوماتي، وتحقق الحماية الجنائية للمصالح العامة والخاصة من خطر الاعتداء عليها، وتفوت الفرصة على المجرمين من استغلال الثغرات القانونية القائمة في النظام القانوني.

3- ضرورة تدخل المشرع الجزائي الأردني بتعديل بعض النصوص القانونية القائمة حتى يمكن تطبيقها في حال ارتكاب الجرائم المعلوماتية، على أن يختص هذا التعديل بجزئية النص الخاص بمحل تلك الجرائم من حيث كونه مالاً منقولاً ذا طبيعة مادية ، وأن يتم التعديل بعدم اشتراط صفة المنقول والمادية في الشيء محل الجريمة، حتى يستوعب النص القانوني المعلومات المعالجة آلياً، وبالتالي يمثل الاعتداء عليها جريمة تخضع لنصوص قانون العقوبات، كما في جرائم السرقة، والإتلاف، وغيرها من جرائم الأموال.

4- تعديل نص المادة (3/أ) من قانون جرائم أنظمة المعلومات الأردني المؤقت، وتطويعها لتستوعب صراحةً جريمة البقاء غير المصرح به في النظام المعلوماتي، لأن هذه الجريمة مرتبطة ارتباطاً مباشراً ووثيقاً بجريمة الدخول غير المصرح به إلى النظام المعلوماتي، بحيث لا يمكن تصورها دون الدخول إلى النظام، وحتى لا يترك المجال مفتوحاً للمجرم المعلوماتي، وخشيةً من إفلاته من العقاب في حال كان الدخول صدفة، فإنه لابد من النص صراحةً على هذه الجريمة، والتي تنطوي على خطورة كبيرة كونها قد تكون تمهيداً لجرائم معلوماتية أشد خطورة.

5- تعديل نص المادة 6/أ من قانون جرائم أنظمة المعلومات الأردني المؤقت، بحيث تنص صراحةً على جريمة سرقة المعلومات المعالجة آلياً، والتي تجسد أموالاً أو أصولاً أو قيماً مالية أو اقتصادية، وذلك في ضوء ما أثاره الفقه من عقبات عديدة أمام تطبيق النصوص الخاصة بجرائم الأموال على المعلومات المعالجة آلياً، مع الأخذ بعين الاعتبار عدم اشتراط إنهاء حيازة مالك المعلومات لها، لأن مفهوم الإستيلاء وفقاً للطبيعة الخاصة للمعلومات المعالجة آلياً يختلف عنه في الجرائم التقليدية، ففي كل الأحوال تبقى المعلومات المعالجة آلياً في حيازة مالكها ولا تنتهي حيازته، إلا أن السارق يحصل على نسخة مماثلة لها.

6- تعديل نص المادة (11 /أ) من قانون جرائم أنظمة المعلومات الأردني، بحيث تنص صراحةً على جريمة التجسس المعلوماتي وعناصرها وأركانها والأساليب التقنية لارتكابها، نظراً لما تشكله هذه الجريمة من خطورة كبيرة على الأمن القومي للدولة، وتعديل العقوبة الواردة في ذات المادة لتتناسب مع طبيعة وخطورة هذه الجريمة، لتحقيق التوازن والتناسب بين الفعل المجرم وبين العقوبة المقررة ضمن القانون، وذلك تماشياً مع المبادئ المستقرة في التشريعات الجزائية المعاصرة.

7- ضرورة تدخل المشرع الجزائي الأردني لتجريم الاحتيال المعلوماتي الذي يقع عبر شبكة المعلومات، وذلك بنص عام يشمل كافة صور هذه الجريمة والأساليب والطرق التقنية لارتكابها، سواء أكان ذلك بالنص الصريح في قانون جرائم أنظمة المعلومات الأردني المؤقت، أم بتعديل نص المادة (417) من قانون العقوبات الأردني، بتطويعها لإستيعاب أفعال الاحتيال التي تقع على المعطيات المعنوية للنظام المعلوماتي، والابتعاد عن فكرة اشتراط وقوع أفعال الاحتيال في مواجهة الإنسان، حتى تستوعب النصوص فكرة وقوع هذه الأفعال في مواجهة الحاسب الآلي والنظام المعلوماتي، واختيار العقوبات المناسبة، والتي تتدرج وفقاً لخطورة الفعل المرتكب، تحقيقاً للردع العام والخاص، وتماشياً مع مبدأ التوازن بين الفعل المجرم والعقوبة المقررة.

8- ضرورة النص الصريح على جريمة التزوير المعلوماتي، وصورها المتمثلة في أفعال الإدخال أو الإتلاف أو المحو أو الطمس العمدي وبدون وجه حق للبيانات والمعلومات المعالجة آلياً، لاستخراج بيانات ومعلومات غير صحيحة بقصد استخدامها لأغراض قانونية كما لو كانت صحيحة، فالمشرع الأردني في قانون جرائم أنظمة المعلومات الأردني المؤقت كان قد وفر الحماية الجنائية للمعلومات المعالجة آلياً من أفعال الإتلاف أو المحو أو الطمس العمدي وبشكل عام، إلا أن هذه الحماية غير كافية لتستوعب جريمة التزوير المعلوماتي، والتي تنطوي على استخدام الجاني لمستخرجات النظام المعلوماتي من بيانات ومعلومات لأغراض قانونية كما لو كانت صحيحة.

9- ضرورة تدخل المشرع الجزائي الأردني في قانون جرائم أنظمة المعلومات الأردني المؤقت لبسط الحماية الجنائية في مجال حق الخصوصية والحياة الشخصية للأفراد من خطر بنوك المعلومات والأنظمة المعلوماتية، وذلك من خلال النص الواضح والصريح على طبيعة البيانات والمعلومات الاسمية والمتعلقة بالحياة الشخصية للأفراد، وإفراد مادة يخصصها المشرع لحماية هذا النوع من المعلومات والابتعاد عن العموميات، مع عدم اقتصارها فقط على الجهات القائمة بعملية جمع وتخزين المعلومات الاسمية المتعلقة بالحياة الخاصة، وإنما مد تلك الحماية على المستوى الشخصي، من خلال إيجاد نص عام ينص على كفالة حماية كافة المعلومات والبيانات المتعلقة بالأشخاص في مواجهة جميع الاعتداءات التي قد تقع عليها وبنص صريح مع الأخذ بعين الاعتبار ضرورة التنظيم التشريعي لجوانب هذه الحماية، من خلال توفير معيار مقبول مبني على التوازن بين حقوق وحريات الأفراد وحماية خصوصياتهم، وبين موجبات المكافحة للجرائم المعلوماتية وحاجتها إلى قواعد استثنائية فرضتها تحديات هذه الجرائم التي تزيد على الجرائم التقليدية..

10- ضرورة عقد دورات تدريبية مشتركة بين الجهاز القضائي الأردني والنيابة العامة ورجال الضابطة العدلية والخبراء المختصين في مثل هذا النوع من الجرائم، وذلك بهدف إكسابهم الخبرات اللازمة في مجال جرائم الحاسب الآلي والإنترنت، من خلال فهم الطبيعة القانونية لمحل هذه الجرائم والوسائل التقنية لارتكابها، وتأهيلهم وتوسيع قدراتهم ومداركهم في هذا المجال، وتحقيق المعرفة الكافية بالتقنيات الحديثة للأنظمة المعلوماتية وتذليل الصعوبات التي تشوب هذه الجرائم في مجال التحقيق والقضاء والإدانة والإثبات، والعمل بروح الفريق الواحد لتحقيق أعلى درجات من الحماية الجنائية الموضوعية والإجرائية للمعلومات المعالجة آلياً، والمخزنة في الحاسب الآلي أو المتداولة عبر شبكة الإنترنت.

11- ضرورة تكثيف الجهود الدولية والتعاون الدولي لمواجهة الجرائم المعلوماتية عابرة الحدود، التي تشكل خطورة كبيرة على أمن وسيادة هذه الدول، وذلك من خلال عقد اتفاقيات ومعاهدات دولية جديدة تجرم الصور المستحدثة لهذه الجرائم، وتواكب التطور السريع الحاصل بها، والذي يسبق دائماً المعاهدات والاتفاقيات المبرمة في هذا المجال، وأن تبين هذه الاتفاقيات الاختصاص المكاني في حال وقوع هذه الجرائم، والإجراءات المتخذة حيال ذلك، وكيفية تسليم مجرمي المعلوماتية، وغيرها من الإجراءات التي تحقق حماية جنائية رصينة للمعلومات المعالجة آلياً والمتداولة عبر شبكة المعلومات الدولية.

12- طرح مواد الأنظمة المعلوماتية لتدرس في الجامعات والكليات الأردنية على مختلف التخصصات، واعتبارها متطلباً أساساً لكافة التخصصات، وذلك لتوفير الحد الأدنى من المعرفة بمثل هذا النوع من الجرائم لدى جميع الخريجين، والإلمام بها تماماً من قبل طلاب الحقوق والمعاهد القضائية ورجال الضابطة العدلية.

ثالثاً- المراجع:

1- الكتب

أ- الكتب باللغة العربية:

- إبراهيم، خالد ممدوح، (2008)، **أمن مراسلات البريد الإلكتروني**، الإسكندرية، الدار الجامعية.
- إبراهيم، خالد ممدوح، (2009)، **الجرائم المعلوماتية**، الإسكندرية، دار الفكر الجامعي.
- إبراهيم، خالد ممدوح، (2010)، **أمن الجريمة الإلكترونية**، الإسكندرية، الدار الجامعية.
- أحمد، هلالي عبد اللاه، (1997)، **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي "دراسة مقارنة"**، ط1، القاهرة، دار النهضة العربية.
- أحمد، هلالي عبد اللاه، (2003)، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001**، ط1، القاهرة، دار النهضة العربية.
- الألفي، أحمد عبد العزيز، (1995)، **شرح قانون العقوبات القسم العام**، مصر، مكتبة النصر بالزقازيق.
- البشري، علي بن هادي، (2005)، **الجهود القانونية للحد من جرائم الحاسب الآلي**، ط1، الرياض، لان.
- بهنام، رمسيس، (1982)، **المجرم تكويناً وعقيدة**، الإسكندرية، منشأة المعارف.
- تمام، أحمد حسام طه، (2000)، **الجرائم الناشئة عن استخدام الحاسب الآلي**، القاهرة، دار النهضة العربية.
- الجبور، محمد عوده، (2010)، **الجرائم الواقعة على الأموال في قانون العقوبات الأردني دراسة مقارنة**، ط2، عمان، دار وائل للنشر والتوزيع.

- الجنبيهي، منير محمد والجنبيهي، ممدوح محمد، (2005)، **بروتوكولات وقوانين الإنترنت**، الإسكندرية، دار الفكر الجامعي.

- الجنبيهي، منير محمد والجنبيهي، ممدوح محمد،(2005)، **أمن المعلومات الإلكترونية**، الإسكندرية، دار الفكر الجامعي.

- الجواد، دلال صادق والفتال، حميد ناصر، (2008)، **أمن المعلومات**، عمان، دار اليازوري العلمية للنشر والتوزيع.

- حجازي، عبد الفتاح بيومي، (2004)، **الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت**، مصر ـ المحلة الكبرى، دار الكتب القانونية.

- حجازي، عبد الفتاح بيومي، (2006)، **مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي "دراسة متعمقة في القانون المعلوماتي"**، ط1، الإسكندرية، درا الفكر الجامعي.

- حجازي، عبد الفتاح بيومي، (2007)، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت**، مصر ـ المحلة الكبرى، دار الكتب القانونية.

- حجازي، عبد الفتاح بيومي، (2009)، **جرائم الكمبيوتر والإنترنت في التشريعات العربية دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية**، ط1، القاهرة، دار النهضة العربية.

- حسبو، عمرو أحمد، (2000)، **حماية الحريات في مواجهة نظم المعلومات "دراسة مقارنة"**، القاهرة، دار النهضة العربية.

- حسني، محمود نجيب، (1971)، **النظرية العامة للقصد الجنائي**، ط2، مصر، دار النهضة العربية.

- حسين، محمد عبد الظاهر، (2003-2004)، **المسؤولية القانونية في مجال شبكات الإنترنت**، القاهرة، لان.

- الحسـيناوي، علي جبار، (2009)، **جرائم الحاسـوب والإنترنت**، عمان، دار اليازوري العلمية للنشر والتوزيع.

- الحلبي، محمد علي السـالم عياد، (2010)، **الجرائم الواقعة على الأموال في القانون المقارن**، ط1، عمان، مؤسسة الوراق للنشر والتوزيع.

- الخن، محمد طارق عبد الرؤوف، (2011)، **جريمة الاحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية)**، ط1، بيروت، منشورات الحلبي الحقوقية.

- رسـتم، هشـام محمد فريد، (1992)، **قانون العقوبات ومخاطر تقنية المعلومات**، مصر، مكتبة الآلات الحديثة، أسيوط.

- الزعبي، جلال محمد والمناعسة، أسامة أحمد، (2010)، **جرائم تقنية نظم المعلومات الإلكترونية دراسة مقارنة**، ط1، عمان، دار الثقافة للنشر والتوزيع.

- الزيدي، وليد، (2003)، **القرصـنة على الإنترنت والحاسـوب "التشـريعات القانونية"**، ط1، عمان، دار أسامة للنشر.

- زين الدين، بلال أمين، (2008)، **جرائم نظم المعالجة الآلية للبيانات في التشـريع المقارن والشـريعة الإسلامية**، الإسكندرية، دار الفكر الجامعي.

- السرحان، سرحان سـليمان والمشهداني، محمود عبد المنعم، (2001)، **أمن الحاسوب والمعلومات**، عمان، دار وائل للنشر.

- سرور، أحمد فتحي، (1985)، **الوسيط في قانون العقوبات الخاص**، ط3، القاهرة، دار النهضة العربية.

- السـعيد، كامل (1991)، **شرح قانون العقوبات الأردني - الجرائم الواقعة على الإنسان**، ط2، عمان، دار الثقافة للنشر والتوزيع.

- السعيد، كامل، (1997)، **شرح قانون العقوبات الأردني (الجرائم المضرة بالمصلحة العامة)**، الأردن، لان.
- سلامة، محمد عبد الله أبو بكر، (2006)، **جرائم الكمبيوتر والإنترنت**، الإسكندرية، منشأة المعارف.
- سليمان، أيمن عبد الحفيظ عبد الحميد، (2005)، **الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية**، مصر، لان.
- سليمان، أيمن عبد الحفيظ عبد الحميد، (لات)، **إستراتيجية مكافحة جرائم استخدام الحاسب الآلي**، مصر، لان.
- الشاذلي، فتوح وعفيفي، عفيفي كامل، (2003)، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "دراسة مقارنة"**، بيروت، منشورات الحلبي الحقوقية.
- شتا، محمد محمد، (2001)، **فكرة الحماية الجنائية لبرامج الحاسب الآلي**، مصر، دار الجامعة الجديدة للنشر.
- الشوا، محمد سامي، (1994)، **ثورة المعلومات وانعكاساتها على قانون العقوبات**، مصر، دار النهضة العربية.
- الشوابكة، محمد أمين، (2009)، **جرائم الحاسوب والإنترنت الجريمة المعلوماتية**، ط1، الأردن، دار الثقافة للنشر والتوزيع.
- الصغير، جميل عبد الباقي، (1992)، **القانون الجنائي والتكنولوجيا الحديثة الكتاب الأول الجرائم الناشئة عن استخدام الحاسب الآلي**، ط1، مصر، دار النهضة العربية.
- الصغير، جميل عبد الباقي، (2002)، **الإنترنت والقانون الجنائي**، القاهرة، دار النهضة العربية.
- الصغير، حسام الدين، (2007)، **الجديد في العلامات التجارية**، مصر، دار الفكر الجامعي.

- الطائي، جعفر حسن جاسم، (2007)، **جرائم تكنولوجيا المعلومات - رؤية جديدة للجريمة الحديثة-**، ط1، عمان، دار البداية ناشرون وموزعون.

- طلبه، محمد فهمي، وآخرون، (1992)، **الحاسبات الإلكترونية ومستقبلها "موسوعة دلتا كمبيوتر"**، مصر، مطابع الكتاب المصري الحديث.

- العبابنة، محمود أحمد، (2005)، **جرائم الحاسوب وأبعادها الدولية**، عمان، دار الثقافة للنشر والتوزيع.

- عبد الله، عبد الله عبد الكريم، (2007)، **جرائم المعلوماتية والإنترنت (الجرائم الإلكترونية) "دراسة مقارنة"**، ط1، بيروت، منشورات الحلبي الحقوقية.

- عرب، يونس، (2002)، **جرائم الكمبيوتر والإنترنت، موسوعة القانون وتقنية المعلومات**، ط1، منشورات اتحاد المصارف العربية.

- العريان، محمد علي، (2004)، **الجرائم المعلوماتية، انعكاسات ثورة المعلومات على قانون العقوبات مشكلة عام 2000**، مصر، دار الجامعة الجديدة للنشر.

- العزام، سهيل محمد، (2009)، **الوجيز في جرائم الإنترنت**، ط1، الأردن، لان.

- عفيفي، كامل عفيفي، (لات)، **جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة**، مصر، لان.

- علي، جمال عبد الرحمن محمد، (2003)، **الخطأ في مجال المعلوماتية "دراسة في العلاقة بين بنوك المعلومات والمستخدم النهائي"**، ط2، القاهرة، لان.

- فضالة، خالد أبو الفتوح، (1999)، **المدخل العلمي إلى الحاسب الشخصي وأنظمة التشغيل**، دار الكتب العلمية للنشر والتوزيع.

- الفقي، عمر عيسى (لات)، **الجرائم المعلوماتية "جرائم الحاسب الآلي والإنترنت في مصر والدول العربية"**، القاهرة، المكتب الجامعي الحديث.

- فهمي، علاء الدين محمد، وآخرون، (1991)، **الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني "موسوعة دلتا كمبيوتر"**، مصر، مطابع الكتاب المصري الحديث.

- الفيومي، محمد (1998)، **مقدمة الحاسبات وتشغيل الحاسبات الصغيرة**، الإسكندرية، المكتب الجامعي الحديث.

- قايد، أسامة عبد الله، (1994)، **الحماية الجنائية للحياة الخاصة وبنوك المعلومات دراسة مقارنة**، ط3، القاهرة، دار النهضة العربية.

- قشقوش، هدى حامد، (لات)، **جرائم الحاسب الإلكتروني في التشريع المقارن**، القاهرة، دار النهضة العربية.

- قوره، نائلة عادل محمد فريد، (2005)، **جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية**، ط1، بيروت، منشورات الحلبي الحقوقية.

- الكعبي، محمد عبيد، (لات)، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت "دراسة مقارنة"**، القاهرة، دار النهضة العربية.

- كيت، فريره، (1999)، **الخصوصية في عصر المعلومات (ترجمة محمد محمود شهاب)**، ط1، القاهرة، مركز الأهرام للترجمة والنشر.

- لطفي، محمد حسام محمود، (1987)، **الحماية القانونية لبرامج الحاسب الآلي**، عمان، دار الثقافة للنشر والتوزيع.

- المجالي، نظام توفيق، (2005)، **شرح قانون العقوبات القسم العام، دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية**، ط1، عمان، دار الثقافة للنشر والتوزيع.

- محمود، عبد الله حسين علي، (2002)، **سرقة المعلومات المخزنة في الحاسب الآلي**، ط2، القاهرة، دار النهضة العربية.

- مراد، عبد الفتاح، (لات)، **شرح جرائم الكمبيوتر والإنترنت**، مصر، لان.

- مصري، عبد الصبور عبد القوي علي، (2010)، **الجريمة الإلكترونية**، القاهرة، دار العلوم للنشر.

- الملط، أحمد خليفة، (2006)، **الجرائم المعلوماتية دراسة مقارنة**، ط2، الإسكندرية، دار الفكر العربي.

- المناعسة، أسامة أحمد والزعبي، جلال محمد والهواوشة، صايل فاضل، (2001)، **جرائم الحاسب الآلي والإنترنت "دراسة تحليلية مقارنة"**، ط1، عمان، دار وائل للطباعة والنشر.

- المهيري، خالد محمد كدفور، (2005)، **جرائم الكمبيوتر والإنترنت والتجارة الإلكترونية**، دبي، دار الغرير للطباعة والنشر.

- موسى، مصطفى محمد، (2006)، **الجهاز الإلكتروني لمكافحة الجريمة**، مصر ـ المحلة الكبرى، دار الكتب القانونية.

- المومني، نهلا عبد القادر، (2008)، **الجرائم المعلوماتية**، ط1، الأردن، دار الثقافة للنشر والتوزيع.

- نبيه، نسرين عبد الحميد، (2008)، **الجريمة المعلوماتية والمجرم المعلوماتي**، الإسكندرية، منشأة المعارف.

- نجم، محمد صبحي وتوفيق، عبد الرحمن، (1987)، **الجرائم الواقعة على الأشخاص والأموال في قانون العقوبات الأردني**، عمان، مطبعة التوفيق.

- نمور، محمد سـعيد، (2007)، **شرح قانون العقوبات القسـم الخاص، الجزء الثاني الجرائم الواقعة على الأموال**، ط1، عمان، دار الثقافة للنشر والتوزيع.

- الهادي، محمد محمد، (1989)، **تكنولوجيا المعلومات وتطبيقاتها**، ط1، القاهرة، دار الشروق.

- الهيتي، محمد حماد مرهج، (2006)، **جرائم الحاسـوب ماهيتها موضـوعها أهم صـورها والصـعوبات التي تواجهها دراسة تحليلية**، ط1، عمان، دار المناهج.

- يونس، عمر محمد، (2004)، **أشـهر المبادئ المتعلقة بالإنترنت في القضـاء الأمريكي**، ط1، ترجمة دار اكاكوس.

ب- المراجع الأجنبية:

- Anthony, G. (1999); **"Runaway world: How Globalization is reshaping out lives",** London, Profile books.
- Casey, E, (2004), **Digital Evidence And Computer Crime,** second edition, Acadimic Pres, ISBN, Chapter-2.
- Doyle, C. (2008); **Cyber Crime, An Over view of The Fraud Computer, Fraud and abuse statute,**
- Edwards, L, Waelde, C, (2000), **Law and the Internet Framework of Electronic Commerce,** Second Edition.
- Gold berg, D, (1989): **"Leg Protetion of EDP Software datramation"**, Vol 18, no5, (May).
- Griffith, D S. (1990), **The Computer Fraud and abuse act of 1986: A measured response to growing problem**, Vanderbilt Law review, Vol. 43.
- Hillman, R. (1999), **Securities Frand, The internet poses challenges to Regulaters and Investors**, United States General Accounting Office.
- Icove, D, Vonstorch, W (1995), **Computer Crime, O,rielly and associates**, inc, August.
- Johnston, D. and Handa, S. and Morgana, CH, (1997), **Cyber Law, (What you need to Know about doing Business on Line)**, Stoddar Publishing Co.

-

- Kunz, M, Wilson, P. (2004), **Computer Crime and compter Fraud,** University of Mayland.

- Rosenoer, J, (1999), **Cyber law. (The Law of internet springer – verlag,** NewYork, ink.

- Smith, G.C, Brain, H. (1995), **Criminal Law Cases And Materials, Butter Worths,** Fourth, edition.

- Stephen, H. (1997), **Legislating Computer crime,** Harvard Journal on legislation, Vol, 34.

- Wiley, J, (1986),**Urlich Syber The Internstional:Handbook on Computer Crime**,Computer related economice and the fringements of privacy.

2- الرسائل الجامعية:

- السـويلميين، إبراهيم بشـارة، (2009)، **جريمة الاحتيال عبر شـبكة المعلومات الدولية دراسة مقارنة بين القانون الأردني والقانوني المصري**، أطروحة دكتوراه، غير منشورة، جامعة عمان العربية، عمان، الأردن.

- محمود، عبدالله حسـين علي، (2001)، **سرقة المعلومات المخزنة في الحاسـب الآلي**، أطروحة دكتوراه، جامعة عين شمس، كلية الحقوق، مصر.

- ميلاد، علي ميلاد، (2007)، **جريمة إتلاف نظم المعلومات "دراسة مقارنة"**، رسالة ماجستير، غير منشورة، جامعة عمان العربية، عمان، الأردن.

- الهرش، توفيق جواد عبدالرحيم، (2005)، **الحماية الجزائية لبرامج الحاسـوب دراسـة مقارنة**، أطروحة دكتوراه، غير منشورة، جامعة عمان العربية، عمان، الأردن.

- يونس، عمر محمد أبو بكر، (2004)، **الجرائم الناشـئة عن اسـتخدام الإنترنت**، أطروحة دكتوراه، غير منشورة، جامعة عين شمس، مصر.

3- الأبحاث العلمية:

1- رستم، هشام محمد فريد، (2000)، **الجرائم المعلوماتية أصول التحقيق الجنائي والفني**، بحث مقدم إلى مؤتمر القـانون والكمبيوتر والإنترنـت، المنعقد في جامعة الإمارات العربية، الإمارات العربية المتحدة، في الفترة ما بين (1-3) مايو.

2- السعدي، واثبه، (2004)، **الحماية الجنائية لبرامج الحاسوب**. بحث مقدم إلى مؤتمر القانون والحاسوب، المنعقد في جامعة اليرموك، الأردن، في الفترة ما بين (12-14) تموز.

3- شرف، عادل محمود وعبدالله، عبدالله إسـماعيل، (2000)، **ضـمانات الأمن والتأمين في شـبكة الإنترنت**، بحـث مقـدم إلى مؤتمر القـانون والكمبيوتر والإنترنـت، المنعقـد في جـامعـة الإمارات العربية، الإمارات العربية المتحدة، في الفترة ما بين (1-3) مايو.

4- صالح، نائل عبدالرحمن، (2000)، **واقع شبكة الحاسوب في التشريع الجزائي الأردني**. بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في جامعة الإمارات العربية، الإمارات العربية المتحدة، في الفترة ما بين (1-3) مايو.

5- عرب، يونس، (2006)، **قراءة الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان**، ورقة عمل مقدمة إلى ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، المنعقد في سلطنة عمان – مسقط، في الفترة ما بين (2-4) نيسان.

6- عرجاوي، مصطفى محمد، (2000)، **الحماية المدنية لبرامج الكمبيوتر في القوانين الوضعية**، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في جامعة الإمارات العربية، الإمارات العربية المتحدة، في الفترة ما بين (1-3) مايو.

7- عقاد، محمد، (1993)، **جريمة التزوير في المحررات للحاسب الآلي "دراسة مقارنة"**. بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، والمنعقد في القاهرة، في الفترة ما بين (25-28) أكتوبر، منشورات دار النهضة العربية.

8- عوض، أسامة محمد محي الدين، (1993)، **جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات**. بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، والمنعقد في القاهرة، في الفترة ما بين (25-28) أكتوبر.

9- قشقوش، هدى حامد، (1993)، **جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات**. بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، والمنعقد في القاهرة، في الفترة ما بين (25-28) أكتوبر، منشورات دار النهضة العربية.

10- قندح، خليل، (2004)، **الجرائم المرتكبة بواسطة المعلوماتية**، بحث مقدم إلى مؤتمر القانون والحاسوب، المنعقد في جامعة اليرموك، الأردن، في الفترة ما بين (12-14) تموز.

11- القهوجي، علي عبدالقادر، (2000)، **الحماية الجنائية للبيانات المعالجة آلياً**. بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، المنعقد في جامعة الإمارات العربية، الإمارات العربية المتحدة، في الفترة ما بين (1-3) مايو.

12- لطفي، محمد حسام محمود، (1993)، **الجرائم التي تقع على الحاسبات أو بواسطتها**. بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان "الجرائم الواقعة في مجال تكنولوجيا المعلومات"، والمنعقد في القاهرة، في الفترة ما بين (25-28) أكتوبر، منشورات النهضة العربية.

13- جمال، فؤاد، (لات)، **جرائم الحاسبات والإنترنت (الجرائم المعلوماتية)**. بحث منشور على شبكة الإنترنت الموقع

http/www.shaimzatalla.com/vb/showthread.phb?t=7947,

تاريخ 2011/8/5، الساعة 10 مساءً.

14- آل عدينان، عبدالله محمد، (لات)، **الاحتيال المعلوماتي**، بحث منشور على الموقع الإلكتروني:

http/www.coeia.edu.sa/index.ph/ar/1486-Fraud-information.html,

تاريخ 2011/10/11، الساعة 12 مساءً.

15- المومني، نهلا عبدالقادر، (لات)، **الجرائم المعلوماتية**، بحث منشور على شبكة الإنترنت الموقع

http/www.shabab20.net/index.php?option=com-kunena.

تاريخ 2011/10/11، الساعة 12,30 مساءً.

16- الحداد، هنا أو حريش، لات، **الجريمة الإلكترونية فيروس - قرصنة - احتيال وتزوير** - بحث منشور على شبكة الإنترنت على الموقع

http/www.f-Law.net.,

تاريخ 2011/9/21، الساعة 10 مساءً

4- الدوريات:

1- أبو زيـد، أحمد، (2010)، **تهدد أمن الدول والأفراد وتمثل الوجه الآخر للتكنولوجيا: الجريمة الإلكترونية الخطر القادم عبر الإنترنت**، مثال منشـور في مجلة الرافد، المجلد (160) العدد (160)، الصـفحات (10-18).

2- إزرائيل، مورو، (2010)، **أمن المنظومات وشبكات المعلوماتية**، مقال منشور في مجلة الدراسات الأمنية، المجلد (28)، العدد (158)، الصفحات (28-35).

3- بوكسي- سـتيفن وبولان، غي، (2010)، **التحالف بين الإرهاب والإجرام البشري الإلكتروني "المعلوماتي"**، مقال منشور في مجلة الثقافة العالمية، المجلد (28)، العدد (158)، الصفحات (44-53).

4- حجازى، أحمد مجدي، (2005)، **العولمة والتدفق المعلوماتي، الأبعاد الاجتماعية والآثار السـلبية**، مقال منشور في المجلة العربية 3000، المجلد (5)، العدد (1)، الصفحات (27-54).

5- الدعفيس، محمد تركي، (1999)، **لا قانون يحاكم جرائم الحاسوب علينا إيجاده قبل استفحال الجريمة**، مقال منشور في المجلة العربية، المجلد (24)، العدد (268)، الصفحات (66-67).

6- رضـوان، رضـا عبدالحكيم، (1999)، **التقنيات العلمية الحديثة في مكافحة فيروسـات الكمبيوتر**، مقال منشـور في مجلة الأمن والحياة، تصـدر عن أكاديمية نايف العربية للعلوم الأمنية، السعودية تموز العدد (204)، الصفحات (58-60).

7- عطيـة، حمـدي رجـب، (2001)، **الإتلاف العمدي لأموال المعلوماتية للحاسـوب في التشـريع الليبي والمصري والفرنسي-** مقال منشور في مجلة الجديد للعلوم الإنسانية، المجلد (7)، العدد (7)، الصفحات (301-342).

8- عظيمة، عدنان، (1999)، **أمن المعلومات وجرائم الحاسـوب**، مقال منشـور في مجلة الفيصـل، المجلد (24)، العدد (279)، الصفحات، (81-85).

9- القشي- ظاهر ودهمش، نعيم، (2005)، **هل أصبح استخدام الإنترنت لعنة تلاحق البنوك**، مقال منشور في مجلة البنوك في الأردن، المجلد (24)، العدد (4)، الصفحات (49-50).

10- لوفيت، غليوم، (2010)، **الأشـكال الاقتصادية للإجرام البشري الإلكتروني**، مقال منشور في مجلة الثقافة العالمية، المجلد (28)، العدد (158)، الصفحات (36-43).

5- القوانين والأنظمة والمعاهدات:

- الدستور الأردني.
- قانون العقوبات الأردني رقم (16) لسنة 1960 وتعديلاته.
- القانون المدني الأردني رقم (43) لسنة 1976.
- قانون الاتصالات الأردني (13) لسنة 1995 وتعديلاته.
- قانون المعاملات الإلكترونية الأردني رقم (85) لسنة 2001.
- قانون حماية أسرار ووثائق الدولة الأردني رقم (50) لسنة 1971.
- قانون حماية حق المؤلف الأردني لسنة 1992.
- قانون جرائم أنظمة المعلومات الأردني المؤقت رقم (30) لسنة 2010.
- قانون العقوبات الفرنسي لسنة 1994 (FCP) ، باللغه الفرنسية .
- القانون الفيدرالي الأمريكي رقم 18 لســـنة 1984 (Computer Fraud And Abuse Act Of 1984) (CFAA 1984)
- القانون الفيدرالي الأمريكي لسرقة الممتلكات القومية لسنة 1994 (NSPA 1994)
- القانون الفيدرالي الأمريكي لحماية المعلومات القومية لســـنة 1996 (The NII Protection Act Of 1996)
- قانون خصوصية الإتصالات الإلكترونية الأمريكي لسنة 1986 (ECPA 1986)
- قانون حق النشر والتأليف الأمريكي والمعدل في ديسمبر 2011 (US Copyright Act)
- قانون الخصوصية الأمريكي لسنة 1977 (The Privacy Act Of 1977)

- القانون الاتحادي لدولة الإمارات العربية رقم (2) لسنة 2006.
- نظام مكافحة جرائم المعلوماتية والتعاملات الإلكترونية السعودي لسنة 2007.
- قانون مملكة البحرين للمعاملات الإلكترونية رقم (28) لسنة 2002.
- قانون سلطة عمان للمعاملات الإلكترونية رقم (69) لسنة 2008.
- قانون دبي للمعاملات والتجارة الإلكترونية رقم (2) لسنة 2002.
- قانون العقوبات لدولة قطر رقم (11) لسنة 2004.
- قانون التوقيع الإلكتروني المصري رقم (15) لسنة 2004.
- قانون العقوبات الإماراتي.
- قانون العقوبات الليبي.
- قانون العقوبات الإنجليزي لسنة 1971.
- قانون العقوبات السوري. الصادر بالمرسوم التشريعي رقم (148) لسنة 1949.
- قانون العقوبات اللبناني الصادر بالمرسوم التشريعي رقم (340) لسنة 1943.
- مجلة نقابة المحامين الأردنيين 1976.
- اتفاقية بودابست لمكافحة جرائم الحاسب الآلي لسنة 2001.
- المذكرة التفسيرية لاتفاقية بودابست لمكافحة جرائم الحاسب الآلي في 8 نوفمبر لسنة 2001.
- المذكرة الإيضاحية للقانون المدني الأردني لسنة 2003.

6- مواقع شبكة المعلومات الدولية (الإنترنت):

- http//convention.cone.Int/treaty/en/progect seyber crime.Httm.

- http/www.oecd.org.com.

تاريخ 2011/9/20، الساعة 11:30 مساءً

- http/www.arab.elaw.com.

تاريخ 2011/9/20، الساعة 11:30 مساءً

- http/www.forum.biskra7.com

تاريخ 2011/10/11، الساعة 10 مساءً

- http/www.stocksexperts.net/show thread

تاريخ 2011/9/25، الساعة 9 مساءً

- http/www.atsdp.com

تاريخ 2011/9/25، الساعة 10 مساءً.

- http/www.zinj.org/fourm/show thread.php?t=2821

تاريخ 2011/10/18، الساعة 11 مساءً

- http/www.mst-oman.com/fourms/archive/index.php/t=331.html.

تاريخ 2011/10/18، الساعة 11:30 مساءً

- http/www.kenana on line.com/users/internet-safety/topics/…143404

التاريخ 2011/10/18، الساعة 12 مساءً

- http/www.nasbcom.net/vb/show thread. php?t=7230.page=1.

تاريخ 2011/10/18 الساعة 12:30 مساءً.

- http://www.neuae.com/?p=25

تاريخ 2011/9/5 الساعة 10 مساءً.

- http://www.traidnt.net.

تاريخ 2011/9/5 الساعة 10 مساءً.

- http://wwww.omanlegal.journal.com

تاريخ 2011/9/5 الساعة 10 مساءً.

- http://wwww.helmylawyers.maktoobblog.com.

تاريخ 2011/9/7 الساعة 11:30 مساءً.

- http://www.gcc-legal.org.com.

تاريخ 2011/9/7 الساعة 11:30 مساءً.

- http://www.egy-law.com.

تاريخ 2011/9/7 الساعة 11:30 مساءً.

- http://www.kenanonline.com

تاريخ 2011/9/13 الساعة 10 مساءً.

- http://www.aladel.gov.ly/main/modules/sections/item.php?itemid=68.

تاريخ 2011/9/13 الساعة 10 مساءً

- http://wwww.gcc-legal.org.com.

تاريخ 2011/9/13 الساعة 10:30 مساءً.

- http://www.omanlegal.net.

تاريخ 2011/9/13 الساعة 10:30 مساءً.

- http://www.lawjo.net/vb/shothread.php?17807.

تاريخ 2011/9/15 الساعة 10 مساءً.

- http://www.blog.amin.org/eyad/2010.com.

تاريخ 2011/9/15 الساعة 10:30 مساءً.

- http://www.e-thesis.mutah.edu.jo.

تاريخ 2011/9/15 الساعة 11 مساءً.

- http://www.shabab20.net/index.php?option=com.

- http://wwww.wikipedia.org/wiki.com.

تاريخ 2011/9/15 الساعة 11:30 مساءً.

-((www.copyright.gov/title 17/92)

-(http/www.law.cornell.edu/uscode/text/18/1030.)

(http://ncsinet.ncsi.iisc.in/cybespace/law/responsibility/cybercrime/www.usdoj.gov/criminal/cybercrime/NIPCadvi.htm.)

-(http//floridalawfirm.com)

-http://www.law.cornell.edu/uscode/text/18/1030.

-(http://www.justice.gov./opl/privstat.htm)

-(http//floridalawfirm.com/privacy.html)

-(http://www.thearabhc.maktoobbloy.com.)

تاريخ 2011/9/17 مساءً.