وزارة التعليم العالي والبحث العلمي

جامعة د. الطاهر مولاي– سعيدة–

كلية الحقوق والعلوم السياسية

قسم الحقوق

آليات الحماية الجنائية لعقود التجارة الإلكترونية

مذكـــرة لنيل شهادة الماستر

التخصص: قانون اجتماعي

من إعداد الطالبة:

- بن علي جميلة

تحت إشراف الأستاذ:

أ– طيطوس فتحي

السنة الجامعية

1438/1437هـ الموافق لـ 2016 /2017م

بسم الله الرحمن الرحيم

** ..... يَرۡفَعِ ٱللَّهُ ٱلَّذِينَ ءَامَنُواْ مِنكُمۡ وَٱلَّذِينَ أُوتُواْ

ٱلۡعِلۡمَ دَرَجَٰتٖۚ وَٱللَّهُ بِمَا تَعۡمَلُونَ خَبِيرٞ ١١

صدق الله العظيم

سورة المجادلةالآية 11

إهداء

إلهي لا يطيب العيش إلا بشكرك ولا يطيب النهار إلا بطاعتك ولا يطيب اللحظات إلا بذكرك ولا تطيب الأخرة إلا بعفوك، ولا تطيب الجنة إلا برؤيتك جلَّ جلالك.

إلى من بلغّ الرسالة وأدى الأمانة ونصح الأمة إلى نبي الرحمة ونور العالمين سيدنا محمد صلى الله عليه وسلم.

إلى من كللّه الله بالهبة والوقار إلى من علّمني العطاء بدون انتظار إلى من أحمل إسمه بكل افتخار، أرجو من الله أن يمد في عمرك لترى ثماراً قد حان قطافها بعد طول انتظار وستبقى كلماتك نجوم أهتدي اليوم وفي الغدو وإلى الأبد والدي العزيز الحاج.

إلى ملاكي في الحياة إلى معنى الحب وإلى معنى الحنان والتفاني إلى بسمة الحياة وسر الوجود إلى من كان دعائها سر نجاحي وحنانها بلسم روحي إلى أغلى الحبايب أمي الكريمة.

كما أتفضل بالشكر إلى كل أعضاء المكتبة وعلى رأسهم عيسى وكل من ساعدني في إنجاز هذه المذكرة.

شكر وعرفان

الحمد لله حمداً كثيراً طيباً مباركاً فيه سبحانك لا نحصي ثناء عليك كما أثنيت على نفسك، خلقت فأبدعت وأعطيت فأفضت، فلا حصر لنعمك ولا حدود لفضلك وصلى الله وسلم على أشرف عبادك وأكمل خلقك خاتم المرسلين ومعلم المعلمين نبينا ورسولنا محمد بن عبد الله الأمين خير من علم وأفضل من نصح.

كما أشكر الله الذي أعطاني القوة و العزيمة والإرادة والصبر لإتمام هذا العمل المتواضع.

كما أتقدم بالشكر الجزيل لأستاذي المشرف" الدكتور:طيطوس فتحي" على الجهد الذي بذله، والمساعدة في إنجاز هذه المذكرة – فجزاه الله عني كل الخير ووفقه في حياته–

الطالبة: بن علي جميلة

قائمة أهم المختصرات

أولاً: باللغة العربية

صفحة	**ص**
الجريدة الرسمية	**ج.ر**
الطبعة	**ط**
القانون المدني الأردني	**ق.م.أ**
القانون المدني الفرنسي	**ق.م.ف**
القانون المدني الجزائري	**ق.م.ج**
القانون المدني المصري	**ق.م.م**
القانون التجاري الجزائري	**ق.ت.ج**
قانون الجزاء العماني	**ق.ج.ع**
قانون الإجراءات الجزائية	**.ق.إ.ج**
قانون العقوبات الجزائري	**ق.ع.ج**

ثانياً: باللغة الأجنبية

Art	**Article**
N°	**Numèro**
Pl	**Public Law**
Sec	**Section**
P	**Page**
Ed	**Edition**
Opcit	**Option cite**
Préc	**Ouvrage Précité**
Vol	**Volume**
Rev	**Revue**
Rsc	**Revue duscience criminelle**
RIDP	**Revue International du Droit Pénale**

الخطة المنتهجة

مقدمة:

الفصل التمهيدي: ماهية التجارة الإلكترونية وعقودها

المبحث الأول: مفهوم عقد التجارة الإلكترونية

المطلب الأول: نشأة وتعريف عقد التجارة الإلكترونية

الفرع الأول: نشأة عقد التجارة الإلكترونية

الفرع الثاني: تعريف التجارة الإلكترونية

المطلب الثاني: خصائص العقد الإلكتروني

الفرع الأول: العقد الإلكتروني أحد العقود التي تبرم عن بعد

الفرع الثاني: العقد الإلكتروني من عقود المساومة

المطلب الثالث: وسائل إبرام عقد التجارة الإلكترونية

الفرع الأول: جهاز التلكس والفاكس

الفرع الثاني: جهاز الكمبيوتر

المبحث الثاني: إبرام عقد التجارة الإلكترونية

المطلب الأول: التراضي في عقد التجارة الإلكترونية

الفرع الأول: الإيجاب الإلكتروني

الفرع الثاني: القبول الإلكتروني

المطلب الثاني: تحديد زمان ومكان إبرام العقد الإلكتروني

الفرع الأول: زمان إبرام عقد التجارة الإلكترونية

الفرع الثاني: مكان إبرام عقد التجارة الإلكترونية

المطلب الثالث: المحل والسبب في عقود التجارة الإلكترونية

الفرع الأول: المحل في عقد التجارة الإلكترونية.

الفرع الثاني: السبب في عقد التجارة الإلكترونية

الفصل الأول: مشروعية الحماية الفنية للتجارة الإلكترونية

المبحث الأول: الحماية الجنائية ضد الجرائم التقليدية

المطلب الأول: جرائم التزوير في النطاق المعلوماتي

الفرع الأول: أركان جريمة التزوير

الفرع الثاني: طرق التزوير

الفرع الثالث: طرق أخرى في عملية التزوير

المطلب الثاني: جريمة الإتلاف المعلوماتي

الفرع الأول: جريمة إتلاف وتغيير البيانات والمعلومات

الفرع الثاني: جريمة محو البيانات والمعلومات أو البرامج

المطلب الثالث: مخاطر المنافسة غير المشروعة في عملية التجارة الإلكترونية

الفرع الأول: صور إدخال فيروسات من قبل الغير بقصد الضرر

الفرع الثاني: صور تشويه سمعة المؤسسة التجارية أو منتجاتها

المبحث الثاني: الحماية الجنائية ضد الجرائم المستحدثة

المطلب الأول: جرائم إساءة استعمال بطاقات الدفع الإلكتروني

الفرع الأول: الجرائم التي تقع من أطراف البطاقة

الفرع الثاني: الجرائم التي تقع من قبل الغير

الفرع الثالث: الجرائم التي تقع عن طريق شبكة الإنترنت

المطلب الثاني: تعريف الجريمة الإلكترونية

الفرع الأول: مميزات الجريمة الإلكترونية عن غيرها من الجرائم

الفرع الثاني: أركان الجرائم الإلكترونية

المطلب الثالث: الطبيعة الخاصة للجرائم الإلكترونية

الفرع الأول: الأساليب المستخدمة للاعتداء على مكونات الحاسب الآلي

الفرع الثاني: حالة استخدام الحاسب الآلي كأداة لارتكاب الجريمة

الفرع الثالث: سمات مرتكبي الجرائم الإلكترونية

المبحث الثالث: أنواع الجرائم الإلكترونية

المطلب الأول: الجرائم التي تقع على أشخاص

الفرع الأول: جريمة انتحال الشخصية

الفرع الثاني: جرائم التشهير وتشويه السمعة

الفرع الثالث: الجرائم المخلة بالأخلاق و الآداب العامة

المطلب الثاني: الجرائم الواقعة على أموال التجارة الإلكترونية

الفرع الأول: تعريف جريمة السرقة الإلكترونية

الفرع الثاني: النطاق القانوني لحركة السرقة الإلكترونية

الفرع الثالث: أركان جريمة السرقة الإلكترونية

المطلب الثالث: جرائم النصب الإلكتروني

الفرع الأول: تعريف جريمة النصب الإلكتروني

الفرع الثاني: نطاق جريمة النصب الإلكتروني

الفرع الثالث: أركان جريمة النصب الإلكتروني

الفصل الثاني: دور القاضي في حماية وسائل التجارة الإلكترونية وطرق مواجهتها الأمنية

المبحث الأول: الوسائل الوقائية

المطلب الأول: تشفير البيانات

الفرع الأول: تعريف التشفير وأهميته

الفرع الثاني: صور التشفير الإلكتروني

المطلب الثاني: الوسائل الردعية

الفرع الأول: المعطيات الأساسية للجريمة المعلوماتية ومراقبة الاتصالات

الفرع الثاني: مراقبة الاتصالات الإلكترونية

المطلب الثالث: القواعد الإجرائية والتزامات مقدمي الخدمات

الفرع الأول: القواعد الإجرائية لتفتيش المنظومة المعلوماتية

الفرع الثاني: التزامات مقدمي الخدمات بمساعدة السلطات

المبحث الثاني: دور سلطات الضبطية القضائية في كشف الجرائم الإلكترونية

المطلب الأول: طرق كشف التعديل والتلاعب في البرامج

الفرع الأول: التعديل والتلاعب في البرامج

الفرع الثاني: خلق أو إعداد برنامج وهي أو ناقص من الناحية الفنية

المطلب الثاني: أهمية التفتيش في الكشف على الجرائم الإلكترونية

الفرع الأول: إجراءات سلطات الضبطية القضائية في التفتيش عن الجرائم الإلكترونية

الفرع الثاني: الصلاحيات المخولة لجهاز الضبط القضائي في الجرائم الإلكترونية

المطلب الثالث: أنواع الأدلة المتعلقة بالجرائم الإلكترونية وطرق التحقق فيها

الفرع الأول: الأدلة التقليدية بالجرائم الإلكترونية

الفرع الثاني: الأدلة التقنية بالجرائم الإلكترونية

المبحث الثالث: الوسائل القانونية للحد من الجريمة الإلكترونية

المطلب الأول: طرق ووسائل البحث عن الجريمة الإلكترونية

الفرع الأول: معاينة مسرح الجريمة

الفرع الثاني: التفتيش في مجال الجريمة المعلوماتية

الفرع الثالث: الخبرة في مجال الجريمة المعلوماتية

الفرع الرابع: الضبط في مجال الجريمة المعلوماتية

المطلب الثاني: الاختصاص القضائي والعقوبات المقررة

الفرع الأول: الاختصاص القضائي

الفرع الثاني: العقوبات المقررة

المطلب الثالث: الوسائل الدولية للحد من الجريمة الإلكترونية

الفرع الأول: التشريعات على المستوى العربي

الفرع الثاني: التشريعات على مستوى العالمي

الفرع الثالث: المعاهدات والمؤتمرات الدولية

-الخاتمة:

مقـــــــدمة

مقدمة:

شهد الربع الأخير من القرن العشرين تطور هائلا في نظم المعلومات Informatique والاتصالاتTélécommunication التي حولت العالم إلى قرية صغيرة، وربطت هذه التقنية الحديثة بين الشعوب المتباعدة فأصبح الإنسان يستطيع أن يرصد ما يجري على الطرف الأخر بالصوت والصورة في لحظة قيام والحدث وتتمثل هذه الأخيرة في اختراع وتطور الحاسب الآلي الذي أضاف للإنسان قدرات هائلة على الاحتفاظ بالمعلومات ومعالجتها بسرعة خيالية، لم تخطر على باله من قبل وأهمية المعلومات ليست خافية على أحد، وككل ثمين فهي دائما في خطر، وقد حملت هذه الاختراعات الخير للبشرية وقدمت لها خدمات جليلة، إلاّ أنها في المقابل حملت بذور الشر من خلال الاستعمال الخاطئ لهذه التقنية وأصبح هناك نوع جديد من الإجرام يطلق عليه الإجرام المعلوماتي.

حيث أصبحت التجارة الإلكترونية واقعاً بل ضرورة لا غنى عنها في عالم الأعمال، وساعد التطور التكنولوجي الهائل في نهاية القرن العشرين على تعظيم هذا النوع من التجارة وتعزيزها، فكان المزج بين التكلفة المنخفضة والكفاءة العالية لوسائل الاتصالات والحاسب الشخصية عظيم الأثر في ظهور الانترنت، كإحدى القنوات التسويقية الرئيسية لعالم الأعمال حتى أصبحت الشبكة العالمية والبريد الإلكتروني هما حجز الأساس في دنيا الأعمال التجارية.

وتنقسم التجارة الإلكترونية في مفهومها الواسع إلى قسمين:

أولاً: أعمال البيع للمستهلك.

ثانيا: أعمال للأعمال التبادل التجاري الإلكتروني.

ولو عرَّفنا الأعمال"البيع للمستهلك" نجدها اختصار للمصطلح"Business to Customer" وهي عمليات البيع للمستهلك ويطلق عليها"**tailing**"وهي موقع على الشبكة:**www**.

لمراكز تجارة تعرض منتجاتها من خلال كتالوجات بالصورة والأفلام يطلق عليها **Virtual mall** أي المراكز التجارية التخيلية، حيث لا يوجد لها مبنى أو مقر في الواقع، وهي تكون مفتوحة للمستخدم على مدار 24ساعة، ويمكن الشراء منها من أي مكان في الأرض. [1]

ومن أكبر هذه المواقع على شبكة الانترنت التي تتبع هذه الطريقة موقع شركة **www.Amazon.com** وهو موقع متخصص في بيع الكتب، رغم أنها مكتبة خيالية، أي ليس لها مكان ولا مبنى، وإنّما تمارس نشاطها من خلال الشبكة أمّا الأعمال"التبادل التجاري الإلكتروني" فتعني تبادلاً للمنتجات **Business to business** أو خدمات بين منشأتين تجاريتين.

ونلاحظ أنه عند بداية التجارة الإلكترونية في العالم كان الاهتمام منصباً على ما يطلق عليه **E-Tailing** وهي عمليات البيع من المنشآت التجارية إلى المستهلك وكان مع تطور النشاط التجاري على الشبكة بدأ ينشأ النشاط التجاري، وهو تبادل السلع والخدمات بين المصانع والشركات.

ومن هذا المنطق ظهر مصطلح التجارة الصامتة **Client Commerce** ويقصد بها التبادل التجاري بواسطة برامج الانترنت دون تدخل بشري من أي نوع، وسيسمح ظهور التجارة بواسطة برامج الانترنت دون تدخل بشري من أي نوع، وسيسمح ظهور التجارة الصامتة بتوفير سلسة من العمليات التجارية الإلكترونية لتنفيذ التبادلات الفعلية الفورية.

وتعد التجارة الإلكترونية هي موضوع بحثنا أسلوب مميز في عقد صفقات تجارية كبيرة ومتعددة وعلى قدر كبير من النجاح، كما أنّها تعد من الفرص المميزة لاستخدام

[1] – مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، العدد11، مطابع الشرطة، القاهرة، الطبعة الأولى سنة 2001، ص264.

الاستثمار بطريقة سريعة وجديدة غير الطرق التقليدية ومشاكلها التي تنشأ نتيجة صعوبات النقل والمشاكل المالية المتعددة من رسوم جمركية، إلى منافذ حدودية جمركية، أو حتى إلى إجراءات إدارية متعددة وطويلة.

وجاءت دراسة صادرة عن مجلس الوحدة الاقتصادية بجامعة الدول العربية حول قياس معدل نمو التجارة الإلكترونية بالدول العربية يتم بنسبة 15% في مقابل30% خاصة بدرجة النمو العالمي، وأنه في عام 2001 بلغ حجم التجارة الإلكترونية عالمياً 135مليار دولار، وكان نصيب التجارة العربية الإلكترونية منها 3مليار دولار وهذا الأمر يستدعي من الدول العربية أن تعمل بكل قوتها التكنولوجيا والإلكترونية والبشرية والاقتصادية، لكنها في نفس الوقت عليها أن تأخذ حذرها من مخاطر هذه التجارة حتى لا تتعرض لجرائم السرقة، النصب الاحتيال، وإساءة الأمانة والقرصنة وغيرها من الجرائم في مجال التكنولوجيا.

ولموضوع جرائم الحاسب الآلي أهمية متزايدة من الناحية النظرية والعلمية فالجريمة ظاهرة اجتماعية تخضع لتطور اجتماعي في المجتمع الذي نشأت فيه، عن طريق التقدم العلمي والتكنولوجي.

كما أنّ الجريمة تمثل عدواناً على القيم والمبادئ السائدة في المجتمع، ومتى وجدت الجريمة فلا بد للدولة من مكافحتها، عن طريق التشريعات لحماية مصلحة المجتمع وتحقيق الردع العام، لكن لا ننس تقدّم المجتمعات يقاسُ بقدر استخدامها لأحدث الوسائل العلمية المتطورة في مختلف أوجه أنشطتها، وبالتالي فلا بد للدول العربية من الدخول في مجال التجارة الإلكترونية، لكن بحذر شديد، مع سن التشريعات المناسبة والكافية في هذا المجال، ونلاحظ مع كل ما ذكرناه من أهمية التجارة الإلكترونية في وقتنا الحاضر، أي إنّها تقابلها عمليات تحد الثقة بها، كأعمال الاحتيال التي تزدهر على خطوط شبكة الانترنت خصوصاً تلك التي تستهدف رجال الأعمال والمستثمرين والمتسوقين على هذه الشبكة.

وتنتشر عبر الشبكة مواقع إلكترونية ومجموعات إخبارية للمحتالين، كما تنشط عمليات إرسالهم لرسائل البريد الإلكتروني للترويج لمشاريع الربح السريع، وتسويق البضائع والخدمات بأسعار أرخص، ومع اتساع الشبكة العالمية وانتشارها الممتد عالمياً يتمكن المحتالون من الوصول إلى أي مستثمر أو راغب في الشراء بسرعة في أي وقت، مع الأخذ بعين الاعتبار أن هناك صعوبة في اكتشاف أو الوصول إلى مرتكبيها، ويرجع ذلك لكونها لا تترك في أغلب الأحيان شهوداً يمكن سؤالهم أو أدلة مادية يمكن فحصها. [1]

وتتمثل هذه الصعوبات في قيام أجهزة الضبط القضائي والتحقيق بدورها ووسائلها في عمليات المراقبة والتفتيش والضبط والتحقيق وتطبيق القوانين الإجرامية والعقابية، ممّا يؤدي إلى إنزال العقاب الرادع على جناة الجرائم المعلوماتية.

وأصبحت مشكلة جرائم الحاسب الآلي، مشكلة دولية تعاني منها الدول المتقدمة والنامية على السواء، حيث تطبق معظم الدول نظم الحاسب الآلي في كافة ميادين الحياة، ومن هنا ظهرت الحاجة الملحة لمواجهة ظاهرة جرائم الحاسب الآلي، تشريعياً وأمنياً، على المستوى المحلي والإقليمي والدولي بوضع خطة لمواجهتها نظراً لتنوع وانتشار هذه المواجهة تعديل القوانين التقليدية القائمة، بالإضافة إلى نصوص جديدة تواجه هذه الجرائم، ومن الناحية المنية يتطلب الأمر أولا محو أمية الحاسب الآلي، بتعميم تدريسه وتوضيح طرق الجرائم الناشئة عنه لسلطات الأمن، وإرسال البعثات إلى الدول المتقدمة تقنياً في هذا المجال لرفع كفاءة هذه الأجهزة، ثم اتخاذ الإجراءات الوقائية والدفاعية لمنع الجريمة ومواجهتها طبقاً للقوانين القائمة.

وإدراكاً لأهمية الموضوع اقتضت طبيعة هذه الدراسة التطرق إلى النتائج الموجودة منها أن يكون المنهج الذي تم إتباعه جامعاً بين **المنهج التاريخي** لتحديد المفاهيم التي تنطوي

[1] – عمر الفاروق الحسني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية ونقدية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، دار النهضة العربية، الطبعة الثانية سنة1995، ص5

عليها الدراسة، و**المنهج التحليلي** لتحليل النصوص القانونية ذات الصلة بالموضوع، و**المنهج المقارن** فهو اللجوء إلى بحث موضوعي "آليات الحماية الجنائية لعقود التجارة الإلكترونية" وكيفية معالجتها في عدد من القوانين المختلفة، مع بيان ما يجري عليه العمل في العقود التجارية عبر الانترنت وكيفية محاربة مرتكبيها وذلك ع طريق إبرام اتفاقيات الدولية والعربية ذات الصلة بموضوع الدراسة.

تتلخص صعوبات البحث في موضوع "الحماية الجنائية للتجارة الإلكترونية".

1- حداثة الموضوع نوعاً ما خاصة في بلادنا.

2-صعوبة الاستقرار على خطة البحث لتكون متناسقة ومقبولة وذلك بسبب خصوصية الموضوع المبحوث الذي يستوجب التركيز في الدراسة على النقاط، بعينها عند بحث الموضوع والمرور على نقاط أخرى بشكل موجز وهذه الصعوبة استوجبت أن تكون خطة البحث بالطريقة التي هي عليها الآن.

3- الجدل الفقهي المستمر حول الكثير من المسائل التي تناولتها في بحثي المتواضع.

4- إن موضوع التجارة الإلكترونية أحد موضوعات القانون التجاري لكن تعلقت الدراسة بآليات الحماية الجنائية لعقود التجارة الإلكترونية أوجب الخوض في أكثر من فرع من فروع القانون، كالقانون المدني وقواعد القانون الدولي الخاص، قانون الإجراءات الجزائية، قانون العقوبات، هذا فضلا عن اللجوء إلى أكثر من نظام قانوني داخلي لدول مختلفة، مع اللجوء باستمرار إلى الاتفاقيات الدولية والقواعد النموذجية المتعلقة بالموضوع

5- صعوبة ضيق الوقت في موضوع بهذا الحجم و هاته الأهمية إضافة إلى موضوع البحث يعتبر من المواضيع الجديدة وذلك راجع لقلة الدراسات والبحوث الوطنية في هذا التخصص، وقلة المراجع المتخصصة، وإن وجدت فهي تكرار لمّا سبق تناوله خصوصاً المراجع الجزائرية، وهذا لعدم تنظيم المشرع الجزائري قانون خاصاً لقراصنة السطو على التجارة الإلكترونية بواسطة نظم الحاسب الآلي.

لقد تضاعفت أهمية هذا الموضوع مع نمو ظاهرة التجارة الإلكترونية وخاصة تزايد جرائم الانترنت كل يوم من خلال الحاسب الآلي مشكلة دولية تعاني منها الدول المتقدمة والنامية على السواء، وهذا ما أوجب التساؤل عنه:

- هل أوجدت التشريعات الجنائية المختلفة نظام متكامل لحماية التجارة الإلكترونية من الناحية الموضوعية والإجرائية تعيد ثقة المستهلك في التجارة عبر الانترنت؟

-كيف يمكن اختراق مواقع التجارة الإلكترونية؟

- وما هي التهديدات التي تواجهها؟

- هل نظم المشرع الجزائري قوانين لردع جناة مرتكبي جرائم التجارة الإلكترونية؟

- وما هي طرق وسائل الحماية؟

لقد اقتضت المنهجية المتبعة تقسيم البحث إلى مقدمة وفصل تمهيدي وفصلين، حيث تضمنت المقدمة بعض الفقرات التعريفية العامة، موضوع البحث ثم أهميته، وبعدها الدراسات السابقة، ثم أسباب اختيار هذا الموضوع، ثم منهجية البحث، وطرح بعض الإشكاليات.

وقد خصص "الفصل التمهيدي" لماهية التجارة الإلكترونية وعقودها فتم من خلاله تقسيمه إلى مبحثين فخصص المبحث الأول لمفهوم عقد التجارة الإلكترونية، فتناول ثلاثة مطالب في كل مطلب فرعين، أمّا المبحث الثاني من الفصل التمهيدي فقد خصص لكيفية إبرام عقد التجارة الإلكترونية ضمن ثلاث مطالب فكل مطلب فرعين لتحديد زمان ومكان إبرام العقد الإلكتروني.

أمّا الفصل الأول فقد خصص "لمشروعية الحماية الفنية للتجارة الإلكترونية" وقد تم تقسيمه ضمن ثلاث مباحث في كل مبحث ثلاثة مطالب وتضمن كل مطلب فرعين إلى ثلاثة فروع لبيان جرائم ومخاطر بشتى أنواعها للجرائم الإلكترونية.

وقد خصص الفصل الثاني بعنوان "دور القاضي في حماية وسائل التجارة الإلكترونية وطرق مواجهتها الأمنية" في ثلاث مباحث في كل مبحث ثلاثة مطالب تناولت الوسائل الوقائية والردعية ودور إجراءات سلطات الضبطية القضائية والعقوبات المقررة، في كل مطلب تناول من ثلاثة فروع إلى أربعة فروع وذلك حسب الخطة المنتهجة وما يتطلبه الموضوع من دراسة

وللإجابة على هذه الإشكالية اعتمدت على خطة ثلاثية التقسيم وفقا لما سبق.

الفصل التمهيدي

ماهية التجارة الإلكترونية وعقودها

الفصل التمهيدي: ماهية التجارة الإلكترونية وعقودها

شهدت السنوات الأخيرة من القرن الماضي ثورة هائلة في تكنولوجيا الاتصال والمعلوماتية أثرت على جميع مجالات الحياة بما فيها المجال التجاري.

حيث أصبحت الصفقات التجارية تتم عبر شبكات الاتصال الإلكترونية، وظهر ما يسمى بالتسويق الآلي، والدفع الإلكتروني، والتجارة الإلكترونية، هذه الأخيرة فرضت نفسها بقوة مما نتج عنه تغير في المفاهيم السائدة في المعاملات المدنية والتجارية، ومن الأمور التي كانت مثار جدل واختلاف وتعدد وجهات النظر، محاولة وضع تعريف للتجارة الإلكترونية.

وتعني التجارة الإلكترونية عقد الصفقات التجارية في السلع والخدمات عبر الشبكة الدولية للاتصالات عن بعد حيث هناك حالا يتم التسليم والدفع فيها من خلال الشبكة.

وفي حالات أخرى يتم الدفع فقط من خلال الشبكة ، أما التسليم فيتم خارجها أي بشكل مادي، وعلي ذلك، فالتجارة الإلكترونية هي التي تتم من خلال وسيط الإلكتروني، أي أن تفاعل الأطراف يكون إلكتروني لا يأخذ طابعا ماديا. [1]

[1] – لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2010، ص 15.

المبحث الأول: ماهية عقد التجارة الإلكترونية

يعد موضوع التجارة الإلكترونية من أكثر موضوعات عصر المعلوماتية إثارة للجدل القانوني في وقتنا الحاضر، مما يستوجب توضيح مفهومها لاسيما إذ أخذنا بعين الاعتبار تعدد أنواع التقنيات المستخدمة في هذا النوع من التجارة، والتعرض لأشكالها وكذا بيان التنظيم القانوني لها.

المطلب الأول: نشأة وتعريف عقد التجارة الإلكترونية

إن نشأة عقد التجارة الإلكترونية وتعريفها ليس بالأمر اليسير لاسيما إذا أخذنا في الاعتبار تنوع التقنية المستخدمة في هذا النوع من التعامل وتطورها المستمر والتوسع في أساليبها ووسائلها، فنشأة التجارة الإلكترونية عرفت ثورة معلوماتية بفضل حدوث تحول نوعي في المبادلات كما يأخذ مفهوم التجارة الإلكترونية عدّة معان سنتناول كل واحد منهما على حدى:

الفرع الأول: نشأة عقد التجارة الإلكترونية

ولدت التجارة الإلكترونية Trade commerce من رحم التجارة التقليدية بفضل ثورة الاتصالات المعلوماتية فتنوعت أسماء تلك التجارة مثل: " تجارة الانترنت" و " تجارة أون لاين" " و التجارة الرقمية "والتجارة عبر المواقع الإلكترونية "و التجارة الممكنة" وغيرها من الأسماء الأخر المعرفة للتجارة الإلكترونية[1].

فكل التقسيمات تشير إلى شيء واحد هو حدوث تحول نوعي في المبادلات التجارية التقليدية أثر من التطور في تكنولوجيا الاتصالات وخصوصا الشباك الرقمية للكمبيوتر، ومن ثم فالتجارة الإلكترونية تقاس بمعايير التطور في التقنيات الرقمية وبمدى التقدم في الإلكترونية التحتية كسرعة الاتصال التي تساعدنا على عرض سريع للمواقع الإلكترونية، لذلك نجد أن تقويم التجارة الإلكترونية العربية يرتكز على تقويم تقدم الإلكترونية، والتقدم في شبكات الهاتف الخلوي والانترنت والأقمار الاصطناعية الضوئية fiberopiic وغيرها[2] وعقب انتشار الأجهزة الإلكترونية وتقد تقنية المعلومات ومن ثم تغيير عادات وتقاليد الشعوب، فإن هذه التجارة قد صادقت مصلحة المستهلك ورغباته ولذلك فإنه يلمس نتاج وآثار

[1]- شربل غريب، موسوعة التجارة والمال وإدارة الأعمال التجارية الإلكترونية المجلد الثامن، دار نوبليس، الطبعة الأولى، 2008، ص12.

[2]- شربل غريب، المرجع السابق، ص 18.

التقدم العلمي والتكنولوجي على حياته الشخصية والعلمية. [1]، فقد تقدمت وسائل الاتصال المسموعة والمرئية بين الدول والشعوب الأمر الذي يساعد على معرفة المستهلكين ورغباتهم وذلك عن طريق وسائل الإعلام المختلفة من خلال الإعلان التي تقدمها عن المنتجات والاختراعات الحديثة، الأمر الذي يدفع الإنسان إلى اقتناء هذه التكنولوجيا الحديثة.[2]

إن تطّور التجارة الإلكترونية لاحقا من حيث الكم والكيف أدى إلى تدفع السلع و الخدمات من مختلف الدول المقدمة إلى المستهلكين في كل دول العالم حيث سهلت وسائل الاتصال الحديثة، اتصال البائع بالمستهلك بسهولة ويسر في أي كيفية التعاقد وحفظ حق و المتعاقدين وإثباتها وكذلك الحماية الجنائية لهذه التجارة والمعاملين فيها.[3]

الفرع الثاني: تعريف التجارة الإلكترونية.

لم يضع القانون الدولي النموذجي للتجارة الإلكترونية الذي اعتمدته لجنة الأمم المتحدة للقانون التجاري الدولي16ديسمبر1996 تعريف للتجارة الإلكترونية ولكن اقتصر فقط على تعريف تبادل المعطيات الإلكترونية الذي يتضمن التجارة الإلكترونية حيث عرفه بأنه:" نقل المعلومات إلكترونياً من حاسوب إلى حاسوب آخر باستخدام نظام متفق عليه لإعداد المعلومات "وقد اختارت اللجنة لتبادل المعطيات الإلكترونية تعريف واسعاً، شاملا كل استعمالات المعلومات الإلكترونية المتصلة بالنشاط التجاري، و التي يطلق عليها التجارة الإلكترونية، وهذا يعني أن لجنة اليونيسترال على الرغم من أنها أولى الجهات الدولية التي اهتمت بالتنظيم القانوني للتجارة الإلكترونية إلا أنها حصرت على ترك تعريف هذه

[1]- عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، دار الفكر الجامعي، الإسكندرية، 2006،ص 20

[2]- بيل جيتش، المعلوماتية بعد الإنترنت، طريق المستقبل ترجمة عبد السلام رضوان، سلسلة علم المعرفة الكويت ، العدد 231، ص 5 مقتبس من المرجع السابق ص 244.

[3]- عبد الفتاح بيومي حجازي، المرجع السابق، ص 245

التجارة مفتوحا بحيث لا يقتصر فقط على الأنشطة التجارية التي تتم عبر شبكة الإنترنت بل من الممكن إتمام صفقات هذه التجارة بأي وسيلة إلكترونية أخرى كالفاكس والتلكس، ومن هنا ظهرت عدة تعريفات للتجارة الإلكترونية[1].

فالتجارة الإلكترونية تعرف بأنها:" نوع من التجارة يتم من خلال وسيط إلكتروني بما في ذلك التجارة التي تتم عبر الهاتف والتليفزيون، والفاكس وكذلك عبر الانترنت، وشبكات الاتصال المخصصة لذلك"[2].

- وتعرف كذلك بأنها:" نوع من عمليات البيع والشراء المستهلكين والمنتجين وبين الشركات بعضها مع بعض باستخدام تكنولوجيا المعلومات والاتصال، وهي بذلك أداء عملية تجارية، يبين شركاء وتجاريين باستخدام تكنولوجيا معلومات متطورة تضمن رفع كفاءة وفاعلية الأداء"[3].

- كما تعرف بأنها:" مجموعة المبادلات التجارية التي من خلالها يتم الشراء على شبكة الاتصال عن بعد."[4]

- كما تم تعريف التجارة الإلكترونية على أنها:" مجموعة الاستخدامات التجارية للشبكات، ويدخل في ذلك الشركة التي لا تقدم سوى عرض لمنتجاتها أمّا التسليم فيتم خارج الخط"[5].

---

[1]- المادة 2فقرة ب من القانون النموذجي لليونيسترال للتجارة الإلكترونية لسنة 1996.

[2]- عماد الحداد، التجارة الإلكترونية إعداد اللجنة العلمية للتأليف والنشر والتحرير، دار الفاروق للنشر والتوزيع، الطبعة الأولى، سنة 2004، ص 3

[3]- رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية سنة1999، ص 15.

[4] -Bensoussan (A)Le commerce électronique, aspects juridiques éd. Hermas , Paris 1997, P 13

[5]- Bensoussan(A) op , cit , p 13.

- فالمقصود بذلك العلاقات المتصلة بالشركات سواء العلاقات بين الشركات والإدارات، والتبادلات بين الشركات والمستهلكين[1].

[1]-Tourres (CH) ; Internet et La vente aux consommateurs thése de doctorat Université de paris X , Nanterre , présentée en 1996 , p6.

المطلب الثاني: خصائص العقد الإلكتروني

يتميز العقد الإلكتروني بعدّة خصائص تميزه عن غيره من العقود الأخرى نظرا للطبيعة الخاصة للتعاملات الإلكترونية، ولعل أهم خصائص العقد الإلكترونية أنه من العقود التي تبرم عن بعد كما يعد ذلك من عقود المساومة، وسنقوم في هذا المطلب بدراسة هذه السمات على النحو التالي:

الفرع الأول: العقد الإلكتروني أحد العقود التي تبرم عن بعد

إن التعاقد التقليدي بين يتطلب لا نعاقده، وجود طرفية في مجلس العقد من أجل الاتفاق على تفاصيل العقد المراد إبرامه، إلاّ أن العقد الإلكتروني لا يوجد فيه مجلس عقد بالمعنى التقليدي، أو مفاوضات تقليدية للاتفاق على شروط التعاقد، ففي العقد التقليدي تكون هناك مواجهة بين طرفي العقد.

أماّ العقد الإلكتروني فيتم بدون التواجد المادي لطرفية في لحظة تبادل التراضي، حيث يصدر الإيجاب ويقترن به القبول من خلال وسائل الاتصال الحديثة الانترنت أو غيرها، وهو ما دعى البعض إلى اعتبار هذا العقد عقدا فوريا رغم إتمامه عن بعد [1].

والتعاقد عن بعد قد يتم بالمراسلة مثل: الكتالوجات والنشرات ومن ذلك وسائل الاتصال الحديثة والسريعة مثل: الهاتف والفاكس والكمبيوتر والمواقع الإلكترونية.

فالعقد الإلكتروني ينعقد بتحقق القبول الذي يثبته المتعاقد على صفحة موقع الموجب بشبكة للإنترنت إضافة إلى ذلك فإنه يمكن تنفيذ العقد الإلكتروني عن بعد، ودون انتقال أطرافه إلى مكان معين، أي أن طرفي العقد يقومان بتنفيذ التزامها المتبادلة إلكترونيا، كعقود الخدمات المصرفية والتعليمية، والاستشارات، وبرامج الحاسب الآلي[2].

---

[1] – عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، الجزء الرابع، العقود التي تقع على الملكية البيع والمقايضة، دار النهضة العربية، الطبعة الثانية، أ سنة 1986،ص 30.

[2] – محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، سنة 2003 ص 23 و24.

وقد عرفت تقنية الاتصال عن بعد في ذات التوجيه في المادة 4/2 بأنها كل وسيلة يمكن استخدامها "تتيح إبرام العقد بين أطرافه، وذلك دون الحضور المادي لكل من المورد والمستهلك"[1].

فهذا التعريف وضع شرطا يتعين توافره بوسيلة الاتصال عن بعد التي تستخدم لإبرام العقد، وهو شرط عدم الوجود المادي واللحظي للطرفين مجتمعين معا، وقد تضمن ملحق تعليمات الاتحاد الأوروبي بشأن البيع عن بعد أمثلة لتقنيات الاتصال عن بعد، منها المطبوعات المعنونة، والخطابات الموحدة، والدعاية مع نموذج الطلب، والكتالوجات، والهاتف مع تدخل إنساني أو دون تدخل إنساني، وكذلك التليفون المرئي "الفيزيفون " والفيديو تكس والميكرو وكمبيوتر، والمراسلات الإلكترونية، وماكينات التصوير والتلفزيون، ويتميز التعاقد عن طريق الانترنت عن غيره من الطرق الأخرى بسمة النشاط الحواري، والتي تسمح بتحقيق بعض الخدمات فورا على الشبكة كالحصول على المعلومات، كذلك يتسم التعاقد عن طريق الانترنت يؤدي في بعض الحالات إلى انعدام الفترة الزمنية بين تعبير كل منهما عن إرادته، ووصول هذا التعبير للطرف الأخر بالرغم من تباعدهما المكاني[2].

ومن خلال كل ما سبق نلخص إلى أن العقد الإلكتروني يندرج ضمن طائفة العقود عن بعد.

[1]- Une technique de communication a distance comme tout moyen qui sons présenee physique et simultanée du fournisseur et des consommateurs, peut étre ces, L 144 juin 1997,919,,E,C,O J

[2]- إيمان مأمون أحمد سليمان، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه: حقوق المنصورة، سنة 2006، ص 15.

الفرع الثاني: العقد الإلكتروني من عقود المساومة

يذهب رأي الفقه نظرا للوسيلة التي يتم بها التعاقد إلى اعتبار عقود التجارة الإلكترونية من قبيل الإذعان إذا كانت الشروط العاملة للبيع مذكورة بموقع البائع، بحيث لا يكون أمام المشتري المتعاقد، إلا أن يقبلها أو لا يتعاقد مطلقا، حيث يكون قبوله بالضغط في عدد من الخانات المفتوحة أمامه في موقع البائع على المواصفات التي يرغب فيها من السلعة، وعلى الثمن المحدد سلفا، فلا يملك الفرصة الكافية لمعاينة المنتج، كما لا يملك مناقشة، أو المفاوضة عليه مع المتعاقد الآخر، وكل ما هو متاح له هو إمّا قبول العقد برمته أو رفضه كليّا.[1]

بالإضافة إلى ذلك فإن الشركات تضع شروطا مفصلة لا تجوز المناقشة فيها، وفي الغالب تكون لمصلحة المنتج أو التاجر، وتكون في مجموعها من التعقيد بحيث يصعب على المستهلك العادي فهمها، كما أن هذه الشركات قد تكون محتكرة للسلعة أو الخدمة عن طريق شبكة الانترنت، ويكون المستهلك في احتياج لتلك السلعة بهذه الوسيلة، فلا يملك حرية الاختيار بين أكثر من شركة ولا يملك سوى التعاقد مهما، وتأسيسها على ما

يملك حرية الاختيار بين أكثر من شركة ولا يملك سوى التعاقد مهما، وتأسيسها على ما سبق فإنه يتعين النظر للمستهلك بوصفه طرف مذعنا في عقد التجارة الإلكترونية.[2]

إن المستهلك يعد دائما هو الطرق الضعيف التجارة الإلكترونية، ولكن مؤدى ذلك أن تعد عقود التجارة الإلكترونية التي يكون المستهلك طرف فيها، وبصفة خاصة التي تبرم عبر بشبكة الانترنت، هي عقود إذعان؟ أم أنّها عقود المساومة؟

[1] – أسامة أبو الحسن مجاهد، الوسيط في قانون المعاملات الإلكترونية، الكتاب الأولى، دار النهضة العربية، القاهرة، سنة 2007، ص 134.

[2] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 238

يعرّف عقد الإذعان بأنه: "العقد الذي يسلّم فيه القابل بشروط مقررة يضعها الموجب ولا يسمح بمناقشته فيها، وذلك فيما يتعلق بسلع أو مرافق ضرورية تكون محل احتكار قانوني أو فعلي أو تكون المنافسة محدودة النطاق بشأنها" ومقتضى هذا التعريف أن عقد الإذعان يستلزم أن تتوافر فيه ثلاثة شروط مجتمعة وهي:" أن يتعلق العقد بسلعة ضرورية تمس مصلحة حقيقية وتكون خدمة لا يستطيع المستهلك الاستغناء، وأن تكون محل احتكار سواء محتكر وحيد، أو من عدد قليل من المحتكرين لهذه السلعة الذين يقومون بتحديد سعر بيعها بالإضافة إلى شرط أن يسلم أحد الطرفين بشرط آخر دون مناقشته"[1].

[1] – عبد الرزاق السنهوري، المرجع السابق ، ص 293 وما بعدها

المطلب الثالث: وسائل إبرام عقد التجارة الإلكترونية

تعددت وسائل الاتصال الحديثة في إبرام العقود، ومن هذه الوسائل جهاز المينتل، وجهاز التلكس، وجهاز الفاكس (البرق المصور) و التليفون المرئي، والتليفزيون، والكمبيوتر، فجميع هذه الوسائل يمكن من خلال نقل إرادة طرق إلى الطرق الآخر، وذلك ما هيأها لإبرام العقود.

الفرع الأول: جهاز التلكس والفاكس

التلكس هو جهاز لإرسال البيانات عن طريق طباعتها، وإرسالها مباشرة إذ لا يوجد فاصل زمني ملحوظ بين إرسال البيانات، واستقبالها، إلا إذ لم يكن هناك من يرد على البيانات لحظة إرسالها، ويوجه التلكس من المرسل إلى المستقبل على شبكة خاصة مراقبة من مركز رئيسي للاتصالات وسيط ومحايد يحدد هوية المتراسلين، ويكفل استعداد الجهاز المستقبل للاستقبال ، ويؤرخ العملية ، ويحتفظ المركز بما يدل على تبادل الرسائل خلال مدة سنة، وهذا بدوره يوفر الأمان لأنه يوفر عناصر للإثبات عند للإثبات عند حدوث النزاع عن طريق مركز الاتصالات، الذي يقدم خدمته مشابهة لخدمة البريد الموصى عليه المضمون بعلم الوصول، بالإضافة إلى أنه يقوم بالحفظ مدة زمنية معينة مما أدى إلى منح الثقة بالتلكس. [1]

وقد أجاز القانون المصري أن يكون إعذار المدين أو إخطاره في المواد التجارية في أحوال الاستعجال ببرقية أو تلكس أو فاكس أو غيره ذلك من وسائل الاتصال السريعة[2].

[1] محمد السعيد رشدي، وسائل الاتصال الحديثة مع التركيز على البيع بواسطة التلفزيون، ديوان المطبوعات الجامعية، الكويت ، سنة 1998، ص 85.

[2] – المادة 58 من القانون التجاري المصري.

أمّا جهاز الفاكس هو عبارة عن جهاز نسخ بالهاتف حيث يتم عن طريقه نسخ (نقل) المستندات أو الرسائل نسخا مطابقا للأصل، فتظهر نسخ تلك المستندات، والرسائل على جهاز الفاكس الآخر المرسل إليه، ويلاحظ هنا أن هناك فاصلا زمنيا للرد على المرسل. [1]

وقد أقررت الغرفة التجارية لمحكمة النقض الفرنسية لقبول الفاكس كقوة ثبوتية مادام محتوى الوثيقة يمكن نسبته إلى من أنشأه مع إمكانية التحقق منه إذا اشترطت محكمة النقض الفرنسية لقبول الفاكس كقوة ثبوتية أ يحتوي على توقيه المرسل أو نائبه وهذا يعني توقيعه على الأصل المرسل منه قبل إرسال مما يمكن معه تحديد شخصيته، وقد صدرت هذه الأحكام قبل صدور القانون الفرنسي، الخاص بالتوقيع الإلكتروني والذي ساوى بين جميع أنواع الكتابة باختلاف الوسائط المدونة عليها مادامت مقروءة ومفهومة ويمكن نسبتها لمن صدرت عنه[2].

الفرع الثاني: جهاز الكمبيوتر

أخذ الكمبيوتر موقعه في الحياة المعاصرة حيث أصبح أكثر الأجهزة شيوعاً في جمال التعاقد الإلكتروني، وذلك من خلال شبكة الانترنت، وشبكة الإنترانت Intranet وشبكة الإكسترانت Extranet .

أ – شبكة الانترنت Internet:

هي شبكة دولية لمجموعة حواسيب مرتبطة ببعضها البعض، بغرض تبادل البيانات عبر دائرة التسلسل، والتي هي عبارة عن وصلة يمكن بها إرسال، واستقبال البيانات عبر الشبكة، وتعددت وسائل التعاقد من خلال شبكة الانترنت لإجراء عملية الاتصال وغيرها، حيث يتم الربط بين هذه الشبكة من خلال الانترنت، و هي إما أن يتم إبرام العقد عن طريق

[1] – سعيد السيدد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة للنشر، الإسكندرية، سنة 2004، ص 6.

[2] -HUET (J), La Valeur juridique de la télécopie (au fax) , comparée aux télex ,D,S,1992, doctrine, N05,P, 35.

المراسلة من خلال البريد الإلكتروني، والذي يطلق عليه سبيل الاختصار مصطلح E-mail وقد يتم التعاقد بطريق المحادثة أو المشاهدة ، وأهمها الأكثر انتشارا التعاقد عبر شبكة المواقع ويب (Web). [1]

ب- شبكة الانترانت Intranet:

وتستخدم شبكة الانترانت نفس البروتوكولات المستخدمة في شبكة الانترنت لإجراء عملية الاتصال وغيرها، حيث يتم الربط بين هذه الشبكة وشبكة الانترنت بواسطة كمبيوتر أو أكثر، يكون بمثابة المدخل الرئيسي على شبكة الانترنت وعلى ذلك يمكن القول بأن شبكة الانترنت هي بمثابة جزء من شبكة الانترنت، ولكنها تخص مؤسسة محددة دون غيرها، عن طريق استخدام الوسائل التأمينية المختلفة مثل: الحوائط النارية ووسائل التشفير. [2]

ج- شبكة الاكسترانت Extranet:

تستخدم شبكة الاكسترانت ذات البروتوكولات التي تستخدمها شبكة الانترنت، وهي عبارة شبكة خاصة ملك مؤسسة معينة تستخدم في إجراء عملية الاتصال، وتبادل المعلومات بين المؤسسة، وموزعيها، أو شركائها أو عملائها بصورة آمنة.

وعلى ذلك فإن شبكة الاكسترانت على خلاف شبكة الانترانت الداخلية الخاصة بالمؤسسة تتيح الاستخدام لأشخاص خارج المؤسسة، وفروعها.

تحتاج هذه الشبكة إلى استخدام وسائل تأمينية محكمة كالحوائط النارية، ووسائل تشفير المعلومات نظرا لسريتها وأهميتها لما تتضمنه من عقود وصفقات وغير ذلك. [3]

---

[1] - حسين عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، بدون طبعة، دار النهضة العربية، القاهرة، سنة 2000، ص 54.

[2] - محمد أمين الرومي، التعاقد الإلكتروني عبر الانترنت، الطبعة الأولى، دار المطبوعة الجامعية، الاسكندرية، سنة 2004، ص 35.

[3] - محمد أمين الرومي، المرجع السابق، ص 58.

المبحث الثاني: إبرام عقد التجارة الإلكترونية

يقوم العقد على أركان أساسية لابد من توافرها وأهمها ركن الرضا والذي يعبر فيه الطرفان عن إرادتهما العقد متى حصل توافق بين الإيجاب والقبول كما يجب أن يتوافر في العقد ركن **المحل والسبب** والمعروف في المحل أنّه ما انصب عليه العقد من سلعة أو خدمة، أو السبب هو الباعث أو الغرض المباشر ، غير أن الأمر يختلف بالنسبة لعقد التجارة الإلكترونية فرغم أن يتطلب لانعقاده ما سيتطلبه أي عقد آخر، إلا أنه يختلف عن غيره من العقود كونه ينعقد دون أن يكون هناك حضور مادي لطرفيه في مجلس العقد وقت انعقاده، حيث يكون كل طرف في مكان مختلف عن مكان آخر، أي أنّه في حالة التعاقد الإلكتروني، نجد الطرفين يجمعهما مجلس عقد حكمي
(افتراضي)، وسوف نقسم الدراسة في هذا المبحث إلى ثلاثة مطالب كالأتي.

المطلب الأول: التراضي في عقد التجارة الإلكترونية

التراضي هو تطابق الإرادتين،[1] وهو أساس وقوام العقد بما في ذلك التعاقد الإلكتروني، فالإرادة باعتبارها مكونة للرضا ليس لها أي قيمة قانونية، إلا إذا تم التعبير عنها، فالعقد يتم بمجرد أن يتم طرفاه التعبير عن إرادتين متطابقتين مع مراعاة ما يقرره القانون فوق ذلك من أوضاع معينة لانعقاد العقد. [2]

والتعبير عن الإرادة يكون باللفظ وبالكتابة وبالإشارة المتداولة عرفا كما يكون باتخاذ موقف لا تدع ظروف الحال شكا في دلالته على حقيقة المقصود. [3]

وعلى ذلك يصح أن يتم التعبير عن الإرادة التعاقدية عبر الوسائل الاتصال الإلكتروني، وبخاصة عبر شبكة الانترنت، فالتعبير عن الإرادة يكون من خلال الإيجاب والقبول، فما هي خصوصية الإيجاب والقبول الإلكتروني؟

ولذلك سوف نقسم هذا المطلب إلى فرعين:

الفرع الأول: الإيجاب الإلكتروني

الإيجاب هو تعبير عن إرادة شخص يعرض على أخر أن يتعاقد معه، ويتعين أن يتضمن الإيجاب العناصر الأساسية للعقد المراد إبرامه من حيث يتم العقد بمجرد أن يقترن به قبول مطابق، فإذا لم يتضمن الإيجاب العناصر الأساسية للتعاقد فإنه لا يكون تغيرا عن إيجاب بالتعاقد، وإنما عن مجرد دعوة للتعاقد فالإيجاب الذي يتم عبر شبكة الانترنت قد يكون إيجابا خاصا موجها إلى أشخاص محددين وهو الذي يتم في الغالب بواسطة البريد الإلكتروني، أو عن طريق برامج المحادثة، وقد يكون إيجابا عاما موجها إلى أشخاص غير محددين، أو إلى جميع زائري الموقع عبر صفحات الويب، ونظرا التمتع شبكة الانترنت

---

[1] -François (c) et PHILIPE (D), contrats civils et contrats commerciaux, 7 ème édition DALLOZ, 2004,54.

[2] – المادة 89 مدني مصري والمادة 59 القانون المدني الجزائري.

[3] – المادة 1/90ق مدني المصري.

بالصفة الدولية، فإن الإيجاب الموجه عبرها يكون هو الأخر دولياً أي موجها إلى كل زائري الموقع بغض النظر عن الدولة المنتمين لها أو الموجودين فيها، ومع ذلك يجوز أن يكون الإيجاب محدداً بنطاق مكاني، أي النطاق يشمله الإيجاب بالنص على ذلك صراحة، ومما سبق يمكن القول بأن الإيجاب الإلكتروني هو التعبير عن إرادة الراغب في التعاقد عن بعد، ويتم من خلال شبكة للاتصالات بواسطة وسيطة مسموعة مرئية[1].

يشترط القيام الإيجاب الإلكتروني المعلومات الآتية:

- تحديد شخصية الموجب (المهني).
- وصف السلعة أو الخدمة محل التعامل (وصف المنتج والخدمة محل العقد).
- ثمن السلعة أو مقابل الخدمة(تحديد المقابل النقدي–الثمن).
- فترة سريان الإيجاب (تحديد هذا الوقت مرهون بإرادة الموجب).

خصائص الإيجاب الإلكتروني:

أ– الإيجاب الإلكتروني يتم عبر وسيط إلكتروني:

يتطلب الإيجاب الإلكتروني وجود وسيط إلكتروني وهو ما يطلق عليه خدمة الانترنت Internet Service Provider (ISP) فالإيجاب يتم من خلال الشبكة، وباستخدام وسيلة مسموعة مرئية، وبالتالي فإن الوجود الفعلي للإيجاب يكون منذ اللحظة التي يتم إطلاق الإيجاب من خلال شبكة الإنترنت ، وليس هناك ما يحول دون أن يكون الموجب هو نفسه مقدم الانترنت.

ب– الإيجاب الإلكتروني يتم عن بعد:

فهو يتم بين عاقدين لا يجمعهما مجلس عقد حقيقي، حيث يتم التعاقد (بواسطة) باستخدام الوسائل الإلكتروني لهذا فهو ينتمي إلى طائفة العقود التي تتم عن بعد فإنه يخضع

[1] – محمد حسين منصور، المرجع السابق،ص 67

للقواعد الخاصة بحماية المستهلك في العقود المبرمة عن بعد والتي تفرض على المورد مجموعة من القيود، والواجبات التي يلتزم بها اتجاه المستهلك الإلكتروني.

ج- الإلكتروني يكون في الغالب إيجابا دوليا:

يتم الإيجاب الإلكتروني باستخدام وسائط إلكترونية، وعبر شبكة دولية للاتصالات والمعلومات لذلك، فهو يتقيد بحدود الدول السياسية والجغرافية ويكون الإيجاب الإلكتروني تبعاً لذلك، إيجاباً دولياً نظرا لما تتسم به شبكة الانترنت من الانفتاح والعالمية، بحيث يكون له نطاق جغرافي ومكاني معين، فقد يقصر الموجب عرض المنتجات، والخدمات على منطقة جغرافية معينة، أي أن الإيجاب الإلكتروني قد يكون إقليمياً أو دولياً ، ومن ثم فإن الموجب لن يلتزم بإبرام عقود، أو تسليم منتجات، أو أداء خدمات خارج النطاق الإقليمي الذي حدده سلفا.[1]

الفرع الثاني: القبول الإلكتروني

القبول هو التصرف الذي بمقتضاه يعلن الموجب له إرادته بالموافقة على التعاقد ، أي أنه من وجه إليه الإيجاب يعلن صراحة أو ضمنا عن موافقته على ما تم توجيهية إليه، ويجب أن يصدر القبول والإيجاب قائما، فالعقد لا ينعقد إلا بتلاقي الإرادتين، والتوافق والتطابق بينهما.

أما القبول في عقد التجارة الإلكترونية فإنه لا يخرج عن مضمون هذا المفهوم، سوى أنه يتم عبر وسائط إلكترونية من خلال شبكة الانترنت، فهو قبول عن بعد، لذلك فهو يخضع لذات القواعد والأحكام العامة التي تنظم القبول التقليدي، وإن كان يتميز ببعض الخصوصية التي ترجع إلى طبيعته الإلكترونية ويمكن القول أن القبول الإلكتروني لا يشترط صدوره في شكل خاص، أو وضع معين، فيصبح أن يصدر عبر الوسائط الإلكترونية، أو من

[1] - إبراهيم الدسوي أبو الليل، إبرام العقد الإلكتروني، في ضوء أحكام القانون الإماراتي والقانون المقارن، بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي26-28. أبريل، سنة 2003، ص 98.

خلال الطرق التقليدية للقبول، وذلك ما لم يشترط الموجب أن يصدر القبول في شكل معين، فقد يشترط التاجر الإلكتروني أن يكون القبول عن طريق البريد الإلكتروني أو عن طريق ملء الاستمارة المعدة سلفا، والموجودة بالموقع، فإذا حدث وأن أرسل المستهلك قبوله في شكل آخر عن طريق البريد التقليدي أو الفاكس، فإن هذا القبول لا ينتج آثاره ولا يكون صحيحا، وبالتالي لا ينعقد به العقد.[1]

وقد اشترط القانون التجاري الأمريكي الموحد (Ucc) في المادة 3/206 منه على أن التعبير عن الإرادة في القبول يتم بالطريقة ذاتها لعرض الإيجاب، وبالتالي إذا أرسل الإيجاب عن طريق البريد الإلكتروني أو عبر موقع الويب، فيجب على العميل إن قبل التعاقد أن يعبر عن قبوله بالطريقة ذاتها. [2]

2- طرق القبول الإلكتروني:

توجد طرق محددة يكون لها الأثر في إثبات القبول من عدمه، وهذه الطرق إما عن طريق الضغط على الأيقونة المخصصة لإعلان الموافقة ، والقبول ضمن جهاز الحاسب الآلي، وهذه الطريقة تعتبر أكثر الطرق الشائعة لإعلان القبول، ويمكن أن يتم القبول أيضا عن طريق المحادثة الفورية (chating) أو عن طريق البريد الإلكتروني (e.mail)، وقد يكون القبول الإلكتروني عن طريق إلزام بعض المواقع الإلكترونية لمن يتعامل معها بأن يحرر أمرا بالشراء على صفحة الويب، وقد يحتاج الأمر إلى تحرير عدة أوامر فإذا قام العميل الذي دخل على الموقع بتحرير هذه الأوامر، فإن ذلك قبولا منه بالتعاقد.

3- مدى صلاحية السكوت للتعبير عن القبول الإلكتروني:

القاعدة العامة أن السكوت المجرد لا يصلح تعبيراً عن القبول وفقا لما يقول به فقهاء الشريعة الإسلامية فإنه "لا ينسب لساكت قول" وقد اختلفت الآراء بشأن مدى اعتبار

[1] - أبو الحسن مجاهد، المرجع السابق، ص 76.

[2] - Behjamin Wright, janek winn, the lawof electronic commerce adivision of Aspen publishing INC NEW York, USA ,third edition,2000 p 8-17.

السكوت قبولا في العقود الإلكترونية كما هو متبع في العقود التقليدية في حالات معينة، فما هي أحكام السكوت في التعاقد الإلكتروني؟

وما مدى إمكانية اعتبار قبولا؟

فالأصل أن السكوت في حد ذاته مجرد من أي ظرف ملابس له لا يصلح أن يكون تعبيراً عن الإرادة، فالإرادة تستخلص من ظروف إيجابية تدل عليها، وقد قرر الفقه الإسلامي هذه القاعدة بقوله: لا ينسب لساكت قوله" وفي هذا المعنى قضت اتفاقية فينا لعام 1980 الفقرة الأولى من المادة 18 بأن " السكوت أو عدم القيام بأي تصرف لا يعتبر أي منهما في حد ذاته قبولا". [1]

وقد تعرض القانون المدني المصري إلى مدى اعتبار السكوت قبولا فطبقا لما جاء في نص المادة 89منه والتي تقضي على أنه:" إذا كانت طبيعة المعاملة، أو العرف التجاري، وغير ذلك من الظروف تدل على أنه الموجب لم يكن ينتظر تصريحا بالقبول، فإن العقد يعتبر قد تم إذا لم يرفض الإيجاب في وقت مناسب، ويعتبر السكوت على الرد قبولا إذا كان هناك تعامل سابق بين المتعاقدين، واتصل الإيجاب بهذا التعامل، أو إذا تمخض الإيجاب لمنفعة من وجه إليه"[2].

وهذا ما ذهب إليه كذلك المشرع الجزائري في المادة68ق المدني والتي تنص:" إذا كانت طبيعة المعاملة أو العرف التجاري أو غيره ذلك من الظروف، تدل على أنه الموجب لم يكن لينظر تصريحا بالقبول فإن العقد يعتبر قد تم، إذا لم يرفض الإيجاب في وقت مناسب

[1] – المادة 8 الفقرة 1 من اتفاقية فينا لسنة 1980الخاصة بالبيع الدولي للبضائع، وهي مصادقة عليها من طرف الجزائر، وهذا ما ذهب إليه المشرع الجزائري في المادة 68 من القانون المدني الجزائري.

[2] – المادة 98من القانون المدني المصري.

ويعتبر السكوت في الرد قبولا، إذا اتصل الإيجاب بتعامل سابق بين المتعاقدين أو إذا كان الإيجاب لمصلحة من وجه إليه"[1].

وبالرجوع إلى تشريعات المعاملات الإلكترونية لم نجد أي نص من نصوصها يشير إلى اعتبار السكوت وسيلة يعتد بها للتعبير عن القبول الإلكتروني، ومن جانبنا نرى أنه نظر الحداثة التعاقد الإلكتروني، فإنه لابد للقبول أن يكون صريحا ويتضمن لبعض المسائل الخاصة لإتمام العقد كنوع السلعة، أو الخدمة وطريقة الوفاء والتسليم وخدمة ما بعد البيع.

[1] – المادة 68من القانون المدني الجزائري.

المطلب الثاني: تحديد زمان ومكان إبرام العقد

تعتبر مشكلة تحديد زمان ومكان إبرام العقد الإلكتروني من أهم وأدق المشاكل القانونية التي يثيرها التعاقد الإلكتروني عبر شبكة الانترنت، لاسيما وأن القانون النموذجي للتجارة الإلكتروني لسنة 1996 والتوجيه الأوروبي بشأن التجارة الإلكترونية لسنة 2000 لم يحدد أي منها لحظة ومكان إبرام عقد التجارة الإلكترونية تحديداً صريحاً.

الفرع الأول: زمان إبرام عقد التجارة الإلكترونية

تمكن صعوبة تحديد وقد إبرام عقد التجارة الإلكترونية نتيجة لصعوبة تحديد زمان وصول الإيجاب والقبول إلى الطرف الأخر وذلك أنه عندما يتم نقل التعبير عن الإرادة إلكترونيا عن طريق الضغط على مفاتيح الكمبيوتر، فإن هذه الإرادة الإلكترونية تنتقل عن طريق ترددات كهربائية يتم تشفيرها إلى ومضات إلكترونية تصل إلى جهاز الكمبيوتر لدى المرسل إليه، ويصعب تحديد تاريخ وصول الومضات الإلكترونية إلى الطرف الآخر.[1]

وقد انقسم الفقه في تحديد زمان إبرام العقد الإلكتروني إلى أربع مذاهب باعتباره عقداً بين غائبين

أولا: نظرية إعلان القبول

طبقا لهذه النظرية فإن لحظة إبرام عقد التجارة الإلكترونية هي اللحظة التي يحرر فيها القابل رسالة إلكترونية تتضمن القبول، أو اللحظة التي يضغط فيها على الأيقونة المخصصة للقبول وعدم تصديره، وذلك بالنقر على مفتاح التوقف حيث أن القبول لن يخرج في هذه الحالة عن سلطة القابل، وسيبقى بذلك في مرحلة إعلان القبول.

[1] – عبد الرزاق السنهوري، المرجع السابق، ص 97.

ثانيا: نظرية تصدير القبول

يرى أنصار هذه النظرية أن وقت ولحظة إبرام عقد التجارة الإلكترونية يتأخر إلى الوقت الذي يقوم فيه القابل بإرسال قبوله إلى الموجب أي تصديره له في لحظة انعقاد العقد لا تكون بمجرد إعلان القبول، و لكن يجب إرساله إلى الموجب كقيام من وجه إليه الإيجاب على الأيقونة المخصصة للإرسال، حيث لا يشترط وصول الرسالة إلى صندوق البريد الإلكتروني، الموجود على موقع الموجب على شبكة الانترنت. [1]

ثالثا: نظرية تسليم القبول

يذهب أنصار هذه النظرية إلى أن القبول لا يكون نهائيا إلا إذا وصل إلى الموجب سواء علم الموجب أو لم يعلم به، ويعد وصول القبول إلى الموجب قرينة على عمله به، وبالتالي فإنه وفقا لهذه النظرية، فإن وقت انعقاد العقد هو وقت وصول الرسالة المتضمنة للقبول إلى الموجب، والمقصود بالوصول هنا هو السيطرة الفعلية للموجب على الرسالة المتضمنة.

رابعا: نظرية العلم بالقبول

يذهب أنصار هذه النظرية إلى أنه انعقاد العقد لا يكون بمجرد إعلان القبول، أو تصديره أن تسلمه، وإنما في اللحظة التي يعلم فيها الموجب بالقبول وذلك على أساس أن الأصل في التعبير أنه لا ينتج أثره إلا عند وصوله إلى علم من وجه إليه، وأثره هنا هو انعقاد العقد، وفي مجال العقود الإلكترونية التي تتم عن طريق البريد الإلكتروني، فإن لحظة انعقاد العقد هي الوقت الذي يعلم فيه الموجب بقبول من وجه إليه الإيجاب، كأن يطلع على بريده الإلكتروني، ويعلم برسالة القابل التي وافق فيها على ما تم توجيهه إليه.[2]

[1] – أسامة أبو الحسن مجاهد، المرجع السابق، ص 96.

[2] – نفس المرجع، ص 97و98.

الفرع الثاني: مكان إبرام عقد التجارة الإلكترونية

حدد القانون النموذجي للتجارة الإلكترونية مكان إبرام العقد الإلكتروني في المادة (10/الفقرة 40) حيث قرر أن مكان إرسال الرسائل الإلكترونية يتحدد بالمكان الذي يقع فيه مقر عمل المرسل إليه، ما لم يتفق المنشئ والمرسل إليه على خلاف ذلك، وعليه فإن العقد الإلكتروني يكون قد أبرم في المكان الذي يقع فيه مقر عمل المرسل إليه، وذلك بالطبع ما لم يتفق طرفا العقد على خلاف ذلك، وإذا كان للمنشئ أو المرسل إليه أكثر عن مقر عمل واحد، فإن مقر العمل هو المكان الذي يكون أكثر صلة بالمعاملة المعنية، أو مقر العمل الرئيسي أما إذا لم يكن للمنشئ أو المرسل إليه، مقر عمل رئيسي اعتبر محل الإقامة المعتادة هو مقر عمل منهما. [1]

[1] – محمود حسام محمد لطفي، الإطار القانوني للمعاملات الإلكترونية، النسر الذهني للطباعة، القاهرة، 2002، ص 103.

المطلب الثالث: المحل والسبب في عقود التجارة الإلكترونية

لكي يعتبر عقد التجارة الإلكترونية صحيحا يجب أن تتوافر فيه الأركان الثلاثة وهي: **الرضا** و**المحل** و**السبب**، وإذا كنا قد أنهينا من دراسة ركن **الرضا** فإنه يبقى لنا الكلام عن ركن **المحل** و**السبب** باعتبارهما ركنين أساسيين لابد من توفر شرعيتهما، وذلك تماشياً مع ما تقرره القواعد العامة للعقدة حيث يشترط فيهما أن يتفقا مع النظام العام والآداب العامة، وكذلك مع القوانين القائمة وسنقسم هذا المطلب إلى فرعين:

الفرع الأول: المحل في عقد التجارة الإلكترونية:

محل عقد التجارة الإلكترونية هو الالتزامات التي يولدها هذا العقد، ويشترط فيه بصفة عامة أن يكون مشروعا، وأن يكون موجوداً أو ممكنا وقابلا للتعيين، فالمحل طبقا للمادة 1126 من القانون **المدني الفرنسي**" هو الشيء الذي يلتزم أحد الأطراف بتقديمه أو يلتزم بعمل أو الامتناع عن عمل" [1]

أولا: صور المحل في التجارة الإلكترونية

1- تجارة السلع:

ويقصد بها:" التجارة محلها السلع والبضائع، وكلمة بضائع استقر الفقه والقضاء على أنها تشمل المنقولات المادية وغير المادية، المعنوية على السواء"، فوفقا لقانون التجارة المصري فإن أحكام البيع التجاري لا تسري إلا على عقود بيع البضائع التي يبرمها التجار فيما بينهم لشؤون تتعلق بتجارتهم ما لم ينص القانون على غير ذلك.

[1] - Lionel bochurbeng , op ,cit,p119.

2- تجارة الخدمات:

ويقصد بها:" التجارة التي يكون محلها توريد خدمات، ويعتبر مجال الخدمات من المشروعات التي لا تحتاج إلى رأس مال كبير، فهي تعتمد بالأساس على الفكر والمؤهلات العلمية".[1]

ثانيا: الشروط الواجب توافرها في محل في عقد التجارة الإلكترونية.

1- أن يكون موجوداً أو قابلاً للوجود:

يشترط في السلعة أو الخدمة التي يتم الاتفاق عليها أن تكون موجودة فعلا أثناء الاتفاق، أو قابلة للوجود فيما بعد ، فإذا كان التعاقد عن طريق الانترنت، فإنه يكفي عرض السلعة، أو الخدمة على الشبكة أو صورة السلعة.

2- أن يكون المحل معينا أو قابلا للتعين:

اهتمت التشريعات المقارنة للمعاملات الإلكترونية في غالب الدول بتعين محل العقد المبرم عبر الوسائل الإلكترونية حيث أشارت الفقرة **الأولى** من **البند الرابع** منه إلى ضرورة ذكر مسمى الأموال المعينة، ومكوناتها، وأبعادها، وكمياتها و ألوانها وسماتها الخاصة، وغير ذلك من صفاتها الرئيسية، وكذلك أشارت الفقرة الثانية إلى وجوب تحديد محل الخدمات المعروفة ومحتواها.

3- أن يكون مشروعا:

لا يختلف عقد التجارة الإلكترونية عن نظيره في التجارة الإلكترونية التقليدية وهذا يعني ضرورة أن يكون محل العقد مشروعا، فلا يكون مخالفا للنظام العام والآداب العامة، أو لنص قانوني يمنع التعامل فيه، وإلا كان العقد باطلا. [2]

[1] -الطاهر شوقي مؤمن، عقد البيع الإلكتروني، الطبعة الأولى، دار النهضة العربية، الإسكندرية،2007،ص 46.

[2] - المادة 135من القانون المدني المصري.

والأصل أنه يجوز التعامل في كل السلع والخدمات وهو ما يسمى بمبدأ حرية التجارة ما لم يحظر القانون ذلك ويؤكد ذلك نص المادة 1598 من القانون المدني الفرنسي.

الفرع الثاني: السبب في عقد التجارة الإلكترونية

لا يختلف الحال في عقد التجارة الإلكترونية عن عقد التجارة التقليدية، حيث يكون السبب أحد أركان العقد، وتخلفه يؤدي إلى بطلانه، ويشترط في السبب أن يكون موجوداً أو صحيحاً بمعنى ألا يكون وهمياً أو صورياً كما يشترط أن يكون مشروعاً، ويقصد بالمشروعية هنا عدم مخالفة الباعث على التعاقد للنظام العام أو الآداب العامة، وأن يكون مطابقاً للقانون.

حيث تنص المادة 97من **القانون المدني الجزائري** على أنه:" إذا كان التزام المتعاقد لسبب غير مشروع أو لسبب مخالف للنظام العام و الآداب كان العقد باطلا".[1]

لذا فإن كان طرف العقد من جنسية واحدة، فلا تثور أي مشكلة حيث أنهما يخضعان لفكرة واحدة وقانون واحد، ولكن تثور المشكلة عند اختلاف جنسية طرفي العقد، فأي قانون يطبق في هذه الحالة؟ قانون التاجر أو المستهلك؟، وطبقا لقواعد القانون الدولي الخاص يتم اختيار القانون الواجب التطبيق باتفاق الأطراف، وعند عدم الاتفاق يتم اللجوء إلى قواعد الإسناد الموضوعية، ويطبق إما قانون دولة محل تكوين العقد، أو محل تنفيذي سواء كان التنفيذ خارج الخط (التسليم المادي)، أو كان التنفيذ على الخط، كما يمكن تطبيق قانون دولة محل إقامة المدين ويبقى الأفضل دائما للأطراف اختيار القانون الواجب التطبيق على عقدهم حتى يمكن تجنب مشكلة تحديد القانون الواجب التطبيق.[2]

[1] – المادة 97 من القانون المدني الجزائري.

[2] – أحمد عبد الكريم سلامة، القانون الدولي الخاص النوعي (الإلكتروني، السياحي)، دار النهضة العربية، الطبعة الأولى، سنة 2002، ص111.

ملخص الفصل التمهيدي

يعتبر العقد الإلكتروني الذي هو أهم وسيلة من وسائل التجارة الإلكترونية إذ يتميز هذا العقد بخصائص لا تتوفر في العقود المبرمة بالوسائل التقليدية، كونه مبرم في بيئة افتراضية غير مادية وعبر شبكات الاتصالات العالمية لا تعترف بالحدود الجغرافية للدول، كما أنّه غالبا ما يكون محرراً على دعامات غير ورقية مخزنة داخل الأنظمة المعلوماتية، وعلى ذلك فإن مجلس العقد يمثل الإطار المكاني والزماني لالتقاء وتطابق الإرادتين وقد ارتبطت تلك الوسائل الإلكترونية بميلاد شبكة الانترنت وغيرها من وسائل شبكات الاتصال، وظهور ما يسمى بالمعاملات الإلكترونية أو عقود التجارة الإلكترونية، ومن هنا بدأ اهتمام الفقه والتشريع بالعقد الإلكتروني الذي صار مألوف في حياتنا اليومية بل والأكثر انتشاراً في المستقبل بالتوازي مع التطور في وسائل الاتصالات الحديثة.

الفصل الأول

مشروعية الحماية الفنية لجرائم التجارة الإلكترونية

الفصل الأول: مشروعية حماية الفنية لجرائم التجارة الإلكترونية

مع ظهور تكنولوجيا المعلومات والتقدم الهائل فيها أصبحت شبكات المعلومات وسيلة مهمة لتبادل المعلومات والحصول عليها من أي مكان، أياّ كان بعده ومسافته، كذلك سرعة تداول للمعلومات، وتسلم وإرسال الرسائل عن طريق البريد الإلكتروني.

ومن الظواهر العظيمة أيضا في هذا المجال الانترنت و الستالايت اللذين جعلا العالم كله بلداً واحداً، فأصبحت شبكة المعلومات تنمو وتزدهر مع التطور السريع الملحوظ في شبكة الاتصال أيضا، وتعود جذور هذه الشبكة العملاقة إلى عام 1969 عندما أسست وزارة الدفاع الأمريكية مشروعا يهدف إلى تبادل المعلومات وبينها وبين عدد من مراكز البحوث العلمية الهامة في مختلف أنحاء العالم عبر خطوط الهاتف السريعة، وساعد كل هذا على نشر المعلومات بين الأفراد والدول والمؤسسات مما أفاد البشرية فائدة كبيرة وسريعة [1].

لكن مع ظهور أي اكتشاف أو اختراع جديد، تظهر جرائم ومخالفات جديدة ترتبط بهذا الاكتشاف أو الاختراع، حيث إن إفشاء سرّية البيانات والمعلومات من أهم الأمور التي تهدد التجارة الإلكترونية، ولهذا يجب أن تضل المعلومات والبيانات بعيدة عن المتطفلين أو المخربين وإن أهم ما يجب أن تتصف به التجارة الإلكترونية هو حماية هذه التجارة بالمحافظة على سرية المعلومات من الناحية الفنية، كل هذه الأمور متصلة بشبكة المعلومات والاتصالات فلا يمكن لإحداهما لاستغناء عن الأخرى.[2]

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 78.

[2] – نفس المرجع السابق، ص80.

المبحث الأول: الحماية الجنائية ضد الجرائم التقليدية

تثير التجارة الإلكترونية بعض المسائل المهمة، منها مدى حماية صاحب المشروع وصاحب الموقع على الشبكة العالمية، وأيضا حماية اسمه و عنوانه، ومدى سلامة البيانات الواردة على الموقع، ويضاف إلى ذلك حقوق الملكية الأدبية على الموقع و ما يحويه من صور أو قطع موسيقية أو معلومات، وأيضا القانون الواجب التطبيق على التعاملات التي تتم في هذا المجال.

ونرى أن هناك مشكلة قانونية، وهي عدم كفاية العقوبات الحالية لمرتكبي هذه الجرائم، سواء كان ذلك في قانون العقوبات أو القوانين الخاصة المكملة له، وذلك لأن تلك القوانين لا تتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا، كذلك فإننا نتوقف عند العقاب على هذه الجرائم على قاعدة دستورية مهمة جداً وهي أنه:" لا جريمة ولا عقوبة إلا بنص " ويترتب على ذلك إمكانية إفلات كثير ممن ارتكبوا التصرفات من العقاب، لذلك سارعت معظم دول العالم، في إصدار تشريعات عقابية خاصة بالحاسب وخصوصا جرائمية غير مادية لأنها جرائم جديدة ولم يكن لها أي ذكر في القوانين الجنائية التقليدية[1].

وسنقسم هذا المبحث إلى ثلاث مطالب كالآتي:

[1] – مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، للنشر والتوزيع، القاهرة، سنة 2001،ص 112.

المطلب الأول: جرائم التزوير في النطاق المعلوماتي

إن الشبكة المعلوماتية قد تكون موضوعا لبعض الجرائم، وأيضا قد تكون وسيلة لارتكاب بعض الجرائم، وفي الغالب تكون جرائم مادية، لوقوعها على الشاشات والشرائط والكابلات والمعدات والبرامج الموجودة على دعامات، ويعتبر التزوير في النطاق المعلوماتي من أخطر الجرائم التي تؤثر على التجارة الإلكترونية، لأن الحاسب الآلي أصبح الآن يقوم بكافة العمليات في المجالات التجارية مثل: عمليات الدفع، وطلبات البضائع، وتحويل الأموال من بنك إلى بنك آخر، وكل ما يلزم من عمليات البنوك والشركات الكبرى بصفة خاصة، ومما يزيد من خطورة التزوير هو صعوبة اكتشاف وإثبات التزوير الذي يقع في هذا المجال، والتزوير بصفة عامة هو تغيير الحقيقة في محرر بإحدى الطرق التي تنص عليها القانون تغيرا من شأنه إحداث ضرر ومقترنا بنية استعمال المحرر المزور فيما أعد له.[1]

وجريمة التزوير بهذا التعريف لها ثلاثة أركان الركن المادي والركن المعنوي وطرق أخرى في عملية التزوير، وسنتحدث عن ركن منهم في صورة مستقلة:

الفرع الأول : أركان جريمة التزوير

أ– الركن المادي: يقوم الركن المادي في التزوير بتوافر العناصر التالية

- تغيير الحقيقة في محرر، بوسيلة مما نص عليه القانون.
- أن يكون من شأن هذا التغيير إلحاق الضرر بالغير.

والآن سنتناول كلا من هذه العنصرين بشيء من التفصيل:

1– تغيير الحقيقة:

تعتبر الحقيقة معناه استبدلها بما يخالفها، فإذا لم يكن هناك تغيير في الحقيقة فلا يوجد ثمة تزوير، وهناك تطبيقات أو أمثلة على ذلك لكي تتضح الصورة، فقد قضي بأنه لا يعدُ

[1] – جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية للنشر والتوزيع، القاهرة، سنة 2000، ص 113.

مرتكبا للتزوير من يستبدل بورقة مخالصة منه بخطة وإمضائه وتوقيعه، وأمضى عليها الشاهدات الموقعان على المخالصة الأولى فعلا بنفسيهما، ويترتب على اعتبار التزوير هو استبدال الحقيقة بغيرها أي أن التغيير لا يعتبر تزويرا إذا كان من شأنه أن يعدم ذاتية المحرر أو قيمته، كمحو كل الكتابة التي في المحرر، أو شطبها كلها، بحيث تصبح غير مقروءة، أو غير صالحة للاحتجاج، أو الانتفاع بها، وإنما يقع الفعل في هذه الحالة تحت طائلة جريمة إتلاف السندات أو الأوراق الرسمية كليّا أو جزئيا أو تشويهها بصورة تضر بقوتها الثبوتية.[1]

إن جريمة التزوير تقع بتغيير الحقيقة سواء كان هذا التغيير كليا أو جزئيا، ويلاحظ أن المقصود بتغيير الحقيقة ليس المطلقة، وإنّما تغيير الحقيقة القانونية النسبية، وهذا يعني أن جريمة التزوير تقع إذ ثبت في المحرر ما يخالف إرادة صاحب الشأن الذي يعبر المحرر عن إرادته، ولو كان ذلك تعبير صادقا عن الواقع.[2]

2- أن يكون من شأن هذا التغيير إلحاق الضرر بالغير:

لا يكفي لاكتمال الركن المادي في جريمة التزوير أن يقع تغيير الحقيقة في محرر، وأن يحصل هذا التغيير بإحدى الطرق التي بينها القانون، وإنما ينبغي أن يكون من شأنه أن يسبب ضررا للغير، ولا يشترط وقوع ضرر بالفعل بل يكفي احتمال وقوعه، ويستوي أن يكون الضرر ماديا أو معنوياً، فرديا أو اجتماعيا.[3]

ب- الركن المعنوي: ينحصر الركن المعنوي في جريمة التزوير على توافر عنصريين هما:

العلم: أن يحيط علم الجاني بعناصر الجريمة، واقتران هذا العلم بنية العش، أي نية استعمال المحرر المزور فيما زور من أجله، وقد نصت المادة 201 من قانون الجزاء العماني على أنّه:"

---

[1] - فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية للنشر والتوزيع، الطبعة الثالثة، القاهرة، سنة 1982،ص 114.

[2] - جميل عبد الباقي الصغير، المرجع السابق، ص 115.

[3] - المرجع نفسه ، ص 116.

إذا ارتكب التزوير أو استعمل المزور بقصد إثبات أمر صحيح خففت العقوبة وفقا للمادة 109 من هذا القانون والإرادة.[1]

الفرع الثاني: طرق التزوير

لا يكفي أن يقع تغيير الحقيقة في محرر، إنّما يتعين أن يكون هذا التغيير بإحدى الطرق التي بينها القانون على سبيل الحصر أو من ثم يتعين على المحكمة أن يبيّن في حكمها الطريقة التي وقع بها التزوير، إلاّ كان حكمها قاصرا ويتعين نقضه، وطرق التزوير نوعان هما: [2]

أ- طرق التزوير المادية:

وهي وضع إمضاءات أو أختام مزورة، وتغيير محررة أو الأختام، أو الإمضاءات، أو زيادة كلمات، ووضع أسماء أشخاص آخرين ضرورة أو الاصطناع والتقليد، وهذا تفصيل لهذه الأنواع:

- **وضع إمضاءات أو أختام مزورة:** أي توقيع شخص بغير إمضاءه، وليس له الحق في التوقيع به، ويستوي أن يكون الإمضاء الذي وقع به الجاني لشخص حقيقي أو خيالي.
- **تغيير المحررات أو الإمضاءات أو الأختام أو زيادة كلمات:** يقصد بها كل تغيير مادي يدخله الجاني على المحرر بعد تمام تحريره، سواء اتخذ هذا التغيير صورة إضافة إلى كلمة، أو عبارة أو رقم أو توقيع أو حذف شيء من ذلك أو إبداله بغيره.
- **وضع أسماء أشخاص آخرين:** ويقصد بذلك انتحال شخصية الغير والتعامل باسمه، ومثال ذلك: إذ اتخذت المرأة اسم امرأة أخرى في عقد الزواج وتوصلت إلى إتمام العقد بهذا الاسم المنتحل.
- **التقليد:** هو تدوين الجاني لمحرر أو جزء منه بخط يشبه خط شخص آخر من أجل نسبته إلى هذا الشخص الأخر.

[1] - جميل عبد الباقي الصغير، نفس المرجع السابق، ص 116.

[2] - نقض 5 فبراير 1961، مجموعة أحكام محكمة النقض، س 13 رقم 29، ص 107.

الاصطناع: يتحقق الاصطناع بخلق محرر لم يكن له وجود من قبل، ونسبته كذبا إلى شخص آخر غير مصدره.[1]

ب- طرق التزوير المعنوية: يتحقق بتغيير مضمون المحرر أو ظروفه أو ملابساته دون المساس بمادته أو شكله، فلا تختلف عنه آثار ظاهرة يدركها الحس.

الفرع الثالث: طرق أخرى في عملية التزوير.

1- جريمة جمع المعلومات والبيانات وإعادة استخدامها: هو أن الجاني يقوم بجمع المعلومات والبيانات بدون علم أو معرفة أو إذن صاحب البيانات والمعلومات الأصلي، وهنا تقع الجريمة ويعاقب مرتكبيها بالعقوبات المنصوص عليها في المادة 267 من القانون العماني.

2- جريمة تسريب المعلومات والبيانات: هذه الجريمة تختلف عن سابقتها الخاصة بجمع المعلومات وإعادة استخدامها، في أن جريمة تسريب المعلومات والبيانات لا يقوم الجاني فيها بالحصول على المعلومات والبيانات، لنفسه، وإنما هو يقوم بتسريبها إلى غيره، فهو يساعد ويسير ويسهل بأي طريقة وصول المعلومات والبيانات من جهاز حاسب آلي خاص بشخص ما إلى شخص آخر.[2]

3- جريمة التعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع:

التعدي على برامج الحاسب الآلي خاصة بشخص آخر معاقب عليه في قانون الجزء العماني، والتعدي له صور متعددة، ويعاقب القانون:" كل من تعدى على برامج الحاسب

[1] - عبد الفتاح بيومي حجازي، المرجع السابق، ص 238.

[2] - يقصد بذلك أنه إذا قام شخص بفعل ما يؤدي إلى تسريب معلومات من جهاز شخص ماء إلى شخص ثالثا، فإن الأول، فإن الأول يكون مرتكب لجريمة تسريب المعلومات والبيانات.

الآلي بالتعديل أو الاصطناع، والتعديل يقصد به جعل المعلومات والبيانات تبدو في غير طبيعتها الأصلية ".[1]

أمّا الاصطناع، فهو يتحقق بخلق محرر لم يكن له وجود من قبل، ونسبته كذبا إلى غير مصدره، والاصطناع غالبا ما يكون مصحوبا بطريقة من طرف التزوير مثل: التوقيع بإمضاء مزور ومن أمثلة الاصطناع المحررات عموماً اصطناع بطاقة شخصية، أمّا في مجال الحاسب الآلي فيقصد بالاصطناع خلق بطاقة الائتمان أو كارث أو بطاقة ليست صادرة عن المصدر الأصلي لها.

4- جريمة تزوير البيانات والوثائق المبرمجة:

تتطلب هذه الجريمة ضرورة حدوث تغيير في الحقيقة، وبعض التشريعات لا تتطلب أن يكون حدوث هذا التغيير بوسيلة معينة، مثل: القانون الفرنسي الذي أجاز أن يكون تغيير الحقيقة بأي وسيلة كانت، كما قرر أنه يستوي أن يحدث تغيير الحقيقة على محرر أو دعامة أو سند طالما أن هذه الدعامة تصلح في إنشاء حق أو كل ما من شأنه إحداث نتائج قانونية معينة. [2]

5- جريمة نشر استخدام البرامج بما يشكل انتهاكاً لحقوق الملكية والأسرار التجارية:

هذه الجريمة تقع خارج نطاق جهاز الحاسب الآلي، وهي تعني استخدام معلومات أو بيانات أو برامج في أغراض تخرج عن نطاق الحقوق الملكية والأسرار التجارية، مثل: أن يقوم الجاني باستخدام برامج أو معلومات أو بيانات خاصة بشخص آخر، و عليها أفكار أو اختراعات أو علامات تجارية أو أرصدة مالية...إلخ، ويستخدمها أو ينشرها، كأن يأخذ

[1] – المادة 276مكرر من القانون الجزاء العماني، الفقرة التاسعة منه، ص 87.

[2] – محمد محي الدين عوض، القانون الجنائي، إجراءاته، الطبعة الأولى، جامعة القاهرة، والكتاب الجامعي، سنة 1981، ص 117.

قصة أو فكرة ويستخدمها ويستغلها لنفسه أو ينشرها على الجميع، وهذا كله طبعا بدون استئذان صاحبها الأصلي، مما يضر بصاحبها ضرراً بليغا سواء كان هذا الضرر مادياً أو معنويا.[1]

[1] – أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية، للحاسب الآلي، دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، القاهرة، سنة2000، ص407.

المطلب الثاني: جريمة الإتلاف المعلوماتي

كما ذكرت في المطلب السابق أن الشبكة المعلوماتية قد تكون وسيلة لارتكاب بعض الجرائم، وقد تقع جريمة الإتلاف على البيانات أو المعلومات غير المادية، وهنا يكون الاعتداء بواسطة الحاسب، ويكون هو الوسيلة لارتكاب جريمة الإتلاف، وتجدر الإشارة إلى انه لا يوجد قانوني عماني خاص بجرائم الحاسب الآلي، ماعدا إضافة المادة 276 ق، الجزء العماني، لكن لا يعني هذا أن الإضافة شملت جميع الجرائم المتعلقة بالحاسب الآلي ونأمل من المشرع العماني التنبه إلى ذلك.

وجريمة الإتلاف المعلوماتي من جرائم الانترنت، والمشرع العماني في القانون الجزاء العماني حدد العقوبة على هذا النوع من الجرائم والتي تنص " **أنه يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين وبغرامة من مائة** ريال **إلى خمسمائة** ريال **أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب وإتلاف وتغيير ومحو البيانات والمعلومات**".[1]

وجريمة الإتلاف المعلوماتي في تغيير البيانات والمعلومات أو المعلومات أو محو البرامج تتضمن عدة أفعال أو عدة جرائم في الحقيقة، وبهذا التعريف سنأخذ فرعين مستقلين:

الفرع الأول: جريمة إتلاف وتغيير البيانات والمعلومات:

ويقصد به أن يتم تشويه المعلومة أو البرنامج على نحو فيه إتلاف لها يجعلها غير صالحة للاستعمال في حالة تمكن الجاني من الدخول إلى الحاسب الآلي خاص بشخص آخر، ويقوم بتغيير بيانات أو معلومات أو برامج على الجهاز، كأن يقوم بزيادة بعض الأرقام أو المعلومات أو ينقص منها، أو يضيف أسماء أو علامات أو عملاء....إلخ، فكل هذا يدخل تحت باب تغيير بيانات أو معلومات، وتعتبر الجريمة متوفرة، ويعاقب عليها الجاني حتى ولو لم يترتب على تغيير البيانات أو المعلومات ضرر، لأن الحماية هنا مقررة لصالح المجني عليه

[1] – المادة 276 من القانون الجزاء العماني.

وجهازه الذي يجب ألا يتدخل أحد فيه إلا بعلمه، أي تغيير للمعلومات والبيانات فيه برغبته وبما يحقق مصلحته[1].

الفرع الثاني: جريمة محو البيانات أو المعلومات أو البرامج:

يمكن أن يدخل هذا المحو تحت باب الإتلاف، ولكنه يختلف عنه في أنه يمحي المعلومات والبيانات والبرامج على الحاسب الآلي فيجعلها كأن لم تكن، وبالتالي يحرم صاحب الجهاز من استعمال المعلومات ويحرمه منها، والحقيقة أن تجريم إتلاف وتغيير ومحو البيانات والمعلومات له ما يبرره من وجهتين:

الأول: أنه يحرم صاحب المعلومات أو البيانات من الاستفادة من هذه البيانات أو المعلومات.

الثاني: إن هذا الإتلاف والتغيير والمحو يفترض إلى حد كبير، أنه من يقوم به يكون محل ثقة ومعرفة المجني عليه.[2]

[1] – هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، بدون طبعة، دار النهضة العربية للنشر والتوزيع، القاهرة، سنة1992، ص 118.

[2] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 43.

المطلب الثالث: مخاطر المنافسة غير المشروعة في عملية التجارة الإلكترونية

سنتناول فرعين للمنافسة غير المشروعة في مجال التجارة الإلكترونية:

1- صورة إدخال فيروسات من قبل الغير بقصد الضرر.

2- صورة تشويه سمعة المؤسسة التجارية أو منتجاتها.

الفرع الأول: صور إدخال فيروسات من قبل الغير بقصد الضرر.

عندما ظهر الحاسب الآلي ظهرت معه ظواهر كثيرة، منها الإيجابي المفيد، ومنها السلبي الضار، وهذا وضع طبيعي ظهر مع كل الاختراعات مثل: القطار والديناميت والهاتف، بل إذ ذلك موجود في الأدوات والأشياء التي نستعملها يوميا مثل: السكين والأدوية، فكل هذه الأشياء المفروض أن تستعمل فيما يفيد الإنسان، ويريحه ويساعده على تقدمه ورفاهيته.

وهناك صور متعددة للاستخدام غير المشروع والسيئ للحاسب الآلي: منها هذه الصورة التي نتحدث عنها وهي إدخال فيروس من قبل أشخاص بقصد الضرر، وفيروس الحاسب الآلي هو مصطلح دخل حديثا في مجال صناعة الكمبيوتر، ليصف بعض الأساليب الغادرة والماكرة التي يمكن غرو الكمبيوتر.[1]

وكما تتعدد أنواع فيروسات الحاسب الآلي تتعدد أيضا الأغراض المتوخاة من زراعتها والتي يمكن بلورة أهمها علي النحو التالي: [2]

- اختراق النظام المعلوماتي لأحد البنوك بغرض تحويل مبالغ مالية من حساب العملاء إلى الحساب الخاص للمجرم المعلوماتي.

---

[1] – عبادة أحمد عبادة، التدمير المعتمد لأنظمة المعلومات، الإلكترونية، مؤتمر مركز دعم القرار، ندوة بعنوان المواجهة الأمنية للجرائم المعلوماتية، مطابع الشرطة، الطبعة الأولى، دبي، سنة2005، ص 120.

[2] – هلال عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، بدون الطبعة، سنة 2000، ص 117.

- اختراق النظام المعلوماتي للغير بنقل المعلومات المعالجة إلكترونيا أو لنقل برنامج من برامجه كليا أو جزئيا إلى النظام الخاص بالمجرم المعلوماتي.

-اختراق النظام المعلوماتي للغير بقصد التجسس على المؤسسات الهامة في الدولة أو التجسس على الأسرار الشخصية للأفراد، أو التلاعب في بياناتهم ذات الصفة الشخصية بالحذف أو بالإضافة أو التعديل.

-اختراق النظام المعلوماتي للغير لتدمير ثروته المعلوماتية كلها أو جزء منها، ومن الأساليب المنتشرة للفيروس أسلوب الدودة **Worm** هو فيروس يزرع نفسه ثم يتنقل من جهاز إلى آخر عبر الشبكة و هذا الفيروس عبارة عن مجموعة من التعليمات والأوامر المتعارضة و المعلومة وغير المشروعة، وتوجد برامج مضادة له تسمى" **Anti Virus**" توقف انتشاره ويمكن أن تقضي عليه، وهذا الفيروس يظهر بدون مقدمات أو توقعات، فقد يكون الفيروس في شكل صوت مرتفع يظهر الحاسب في ساعة معينة كالساعة الخامسة مثلا، حيث يكون الجهاز مزعجا لصوته المرتفع والنشاز هذا الفيروس يسمى:"**yankeedoodle**"، وهذا الفيروس يؤدي إلى إغلاق الجهاز في التوقيت المحدد له، والفيروسات لا تسبب إزعاجا فقط، ولكن تكبد الشركات التجارية والمؤسسات أموال طائلة، والفيروس المعلوماتي " **Le Verus informatique**" إن صح التعبير له من خصائص المجرم الكثير، فهو يختفي كخطوة أولى لوقت محدد ثم يبدأ في الظهور كخطوة ثانية، ليدمر في الخطوة الثالثة، كالمجرم الذي يضع خطة لارتكاب الجريمة. [1]

[1] – هدى حامد قشقوش، المرجع السابق، ص 99.

الفرع الثاني: صورة تشويه سمعة المؤسسة أو منتجاتها

تحرص كل شركة على اسمها وسمعتها التجارية سواء كانت تعمل بالطريقة التجارية التقليدية، أو بالطريقة التجارية الحديثة، الإلكترونية، على مستوى السوق المحلي و العالمي، حتى تتمكن من زيادة عدد المستهلكين لمنتجاتها، وتزرع الثقة والأمان فيهم، وأصبحت المواقع التجارية الإلكترونية هي الوسيلة الأكثر انتشار، في وقتنا الحاضر والمساس بسلامة تلك المواقع يؤدي إلى قلق التجار لخوفهم من تسرب المستهلكين منها، ولهذا نجد الشركات الكبرى تنفق الملايين لتطوير الملايين لتطوير سبل الدعاية والحماية لتجارتها الإلكترونية، لأنها وإن كانت ستصرف الملايين على حماية سمعتها التجارية وحماية لمنتجاتها ، فإنها ستكسب أكثر وأكثر من خلال الشبكة الإلكترونية، إذا قامت بحماية مواقعها ضدّ محاولات التدمير و الاختراق.[1]

وتشويه سمعة المؤسسة التجارية، منها الدخول على موقعها وتغيير بعض البيانات الخاصة بها، مثل: تقليل حجم رأسمالها أو تقليل عدد المتعاملين معها، تقليل عدد العاملين فيها، أو عدد فروعها كل ذلك بقصد الإضرار بها وذلك بالتقليل من إمكانيتها، كذلك يمكن حذف بعض إنجازاتها بحيث تبدو للمستهلكين وكأنها شركة صغيرة ليس لها تعامل كبير في الأسواق، وأيضا يمكن إلغاء برنامج نشاطها الدولي لتبدو وكأنها شركة محلية فقط، وكذلك يمكن تعديل موصفات منتجاتها بالتقليل من كفاءتها، وذلك لكي ينصرف عنها الجمهور، أو إضافة منتجاتها سيئة السمعة إلى إنتاج هذه الشركة الموجودة على موقعها، أو تعديل سعر بيع منتجاتها برفعه كثيرا، بحيث يصبح أعلى من السلع المنافسة، هذه بعض

[1]- Department of justice / us Attorney General , Northern, District of Texas, available online in Oct, 2000 at: Httpll// www. usdoj,gov/criminal/cybercrime/phonmast.h.tm.

الصورة لتشويه سمعة المؤسسة التجارية أو منتجاتها[1]، وفي سلطة عمان توجد صعوبة بالغة في عقاب الجاني، بغرض ضبطه ومعرفته وذلك لأن من الطرق المعمول بها حاليا في تشويه المؤسسات والشركات لإرسال رسائل نصية عبر SMS وتنتقل من شخص إلى آخر بسرعة البرق، وبالتالي يصعب معرفة الكاتب الأصلي للرسالة، وبالتالي استحالة إنزال العقاب على الجميع، كما أنّه ومن ضمن الأسباب عدم وجود تشريع عماني خاص بالتجارة الإلكترونية، لكن لا يعني هذا أن المجرم يفلت من العقاب بل يطبق عليه النصوص التي أوردها المشرع في قانون الجزاء العماني. [2]

[1] –قضية تشويه سمعة الشركة العالمية للمرطبات المحدودة في سلطنة عمان، عام2005م، عندما قام أحد الهواة بإرسال رسالة عن طريق SMS يفيد فيها أن المياه الغازية التي تنتجها هذه المؤسسة يأتي من مياه المجاري = وانتشرت المعلومة بسرعة البرق، مما سبب خسائر فادحة لهذه الشركة بالابتعاد عن شراء هذا المنتج، وكذلك التكلفة الإعلامية للشركة من أجل تحسين المنتج وتكذيب مرسل المعلومة.

[2] – راجع القانون الجزاء العماني المادة 276، مرجع سابق، ص77

المبحث الثاني: الحماية الجنائية ضد الجرائم المستحدثة

يشهد العالم في الآونة الأخيرة تغيرات وتحولات متسرعة، نتيجة انتشار الوسائط الإلكترونية الحديثة في إطار المعاملات التجارية وتبادل المعلومات والاتصالات، وهي بلا شك تؤثر على مختلف النواحي الاقتصادية والأمنية في المجتمع، ولم تكن الجرائم الإلكترونية موجودة في المجتمعات القديمة حيث كان الجاني يتكبد المشقة والعناء للوصول إلى مخابئ الأموال والذهب، وقد يفقد حياته في سبيل ذلك، ولكن التطور الحديث أو جدت جرائم لم تكن موجودة و أصبح باستطاعته الجاني المحترف أن يسرق البنوك والأموال وهو جالس بمنزله بفضل التكنولوجيا، وأكثر هذه الجرائم جاءت عبر الانترنت الذي فتح المجال أمام هؤلاء القراصنة للسطو على البنوك ولا يقتصر على ذلك فحسب، بل تتعدى إلى التخريب والتدمير المعتمد للمواقع والبرامج المختلفة.[1]

[1] – عبد الرحمن محمد خلف، التجارة الإلكتروني والإجرام المنظم، مجلة مركز البحوث الشرطة، العدد 23،ص 170.

المطلب الأول: جرائم إساءة بطاقات الدفع الإلكتروني

نظرا لطبيعة علية الوفاء ببطاقات الدفع الإلكتروني وكونها عمليات مصرفية دولية متعددة الأطراف، فقد شجع ذلك بعض المجرمين على دخول سوق بطاقات الإلكتروني، وبذلك ظهرت جرائم جديدة لم تكن موجودة من قبل هي جرائم بطاقات الدفع الإلكتروني.

وهذا الجرائم قد يقع بعضها من أطراف البطاقة نفسها، وهم العميل والبنك والتاجر، وقد يقع بعضها الآخر من الغير، سواء في عمليات السحب أو الوفاء، وعند ما تتعرف على هذه الجرائم سوف نجد أن هناك أساليب عديدة وسيئة تكشف عن أساليب وتقنية ومهارة من قبل هؤلاء الجناة.[1]

الفرع الأول: الجرائم التي تقع من أطراف البطاقة

هناك مخاطر أو جرائم عديدة يمكن أن تقع على بطاقات الإلكتروني، وتقع هذه الجرائم أو المخاطر من أطراف البطاقة أنفسهم وهم العميل والبنك والتاجر.

أولا: الجرائم التي تقع من العميل.

إن الاستعمال للبطاقة الإلكترونية هو الاستعمال الذي يتم بواسطة الحامل الحقيقي للبطاقة الصحيحة وبذلك فإن اجتماع صفتي الحامل الشرعي والبطاقة الصحيحة هما شرطا الاستعمال المشروع، وأن أي تغيير يطرأ على هذين الشرطين يخرج هذا الاستعمال من دائرة المشروعية ويخضعه للمسؤولية الجنائية.

1- الاستعمال التعسفي للبطاقة بواسطة الحامل متجاوزا رصيده في البنك:

الاستعمال التعسفي للبطاقة هو قيام حامل البطاقة بالوفاء بقيمة نفقاته لدى التجار، أو لتنفيذ عمليات السحب النقود من خلال أجهزة التوزيع الإلكتروني في أوراق البنوك، في

[1] - هدى حامد قشقوش، المرجع السابق، ص 124.

حين أن حسابه المصرفي الذي تقوم البطاقة بتشغيله لا يوجد به رصيد، أو به رصيد ولكنه غير كاف.[1]

2- استعمال بطاقة إلكترونية منتهية الصلاحية:

عندما يتعاقد العميل مع البنك للحصول على بطاقة إلكترونية فإنه يجب على العميل أن يعيد البطاقة إلى البنك عند انتهاء المدة المحددة لها إلى البنك، لكن يحدث أن العميل طبعا ليس كل العملاء يلجأ إلى استخدامها بعد مدة الصلاحية.

ثانيا: الجرائم التي تقع من موظفي البنك المصدر لها.[2]

الجرائم التي تقع على بطاقات الدفع الإلكتروني من موظفي البنك الذي أصدره تأخذ أحد الأشكال التالية:

1- تواطؤ موظف البنك مع العميل حامل الطاقة الإلكترونية في ارتكاب أحد الأفعال الآتية:

- استخراج بطاقة سليمة بيانات مزورة.
- السماع للعميل بتجاوز حد البطاقة في السحب.
- السماح للعميل بالصرف بموجب بطاقة منتهية الصلاحية، أو بعد صدور قرار بسحبها.

2- تواطؤ موظف البنك مع التاجر في ارتكاب بعض الأفعال مثل: تجاوز حدّ السحب في صرف قيمة إشعارات بيع صدرت استناد إلى بطاقات وهمية، أو مزورة، أو منتهية الصلاحية.

---

[1] - عمر محمد أبو بكر ، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، الطبعة الثانية، القاهرة، سنة2004، ص 130.

[2] - نجاح فوزي، نماذج من جرائم بطاقات الدفع الإلكتروني، ورقة عمل مقدمة إلى ندوة الصورة المستحدثة لجرائم بطاقات الدفع الإلكتروني، التي نظمها مركز بحوث الشرطة بأكاديمية القاهرة، في 14 ديسمبر 1998، ص 137.

ثالثا: الجرائم التي تقع من التاجر:

يقصد بالتاجر هنا الجهة التي تقبل البطاقات من حامليها كوسيلة دفع إلكترونية مقابل السلع والخدمات المقدمة منها لهؤلاء العملاء، وذلك بشرط توقيعهم للتاجر على إشعارات البيع، ولا يحق لأي جهة قبول البطاقات من العملاء كوسيلة دون وجود تعاقد مع أحد البنوك العاملة في هذا المجال، والذي يقوم بتزويد التاجر بالأجهزة اللازمة للتعامل في هذا النشاط سواء كانت الأجهزة يدوية أو إلكترونية ومستلزمات التشغيل الخاصة بها" **إشعارات البيع**" على أن يقوم التاجر بتحصيل قيمة تلك الإشعارات من البنك المتعاقد معه.

الفرع الثاني: الجرائم التي تقع من قبل الغير

كما ذكرنا سابقا أن المخاطر أو الجرائم التي تقع على بطاقات الدفع الإلكتروني حديثة نسبيا في بعض الدول، لأن هذه البطاقات لم تظهر إلى الوجود إلاّ منذ سنوات قليلة، وقبلها سنوات في العالم، ومع انتشار استعمالها فقد ترتب عليها جرائم لم تكن معروفة من قبل، وهناك عدّة صور لاستخدام الغير للبطاقة الإلكترونية، وطبعا المقصود هنا هو استخدام الغير للبطاقة بدون موافقة أو معرفة حاملها الأصلي.

أولا: حالة فقدان البطاقة الإلكترونية:

من هذه الصورة فقد البطاقة الإلكترونية، يجدها شخص آخر ويستعملها، لذلك فإنه يجب على العميل حامل البطاقة الأصلية الإبلاغ فور فقدانها حتى يوقف البنك التعامل بها، وحتى لا يتحمل العميل مسؤولية المبالغ التي يسحبها الغير من رصيده ومن جانبنا نرى أن العميل إذا تقاعس عن الإبلاغ بفقد بطاقته، وكذلك رقمها السري، فإنه قد يترتب على ذلك التزامه بالمبالغ التي سحبت من رصيده بمعرفة الغير، ولا يسأل البنك عن ذلك[1].

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 124.

ثانيا: حالة سرقة البطاقة الإلكترونية:

تعد سرقة البطاقة، أو ضياعها من أهم المشكلات القانونية التي يثيرها التعامل بنظام بطاقات الائتمان الممغنطة وأيضا قد يقوم سارق بطاقة الدفع الإلكترونية أو " السحب" باستخدامها في سحب أوراق البنك من أجهزة التوزيع الآلي للنقود، والسرقة قد تكون حقيقية، وقد تكون صورية، فالسرقة الحقيقية هي التي يقوم فيها الجاني باختلاس البطاقة من صاحبها، و بعض الجناة المحترفين يلجئون إلى سرعة استعمال البطاقة الإلكترونية إلى التجار أو مقدمي الخدمات للحصول على السلع التي يرغبونها، أو الخدمات المتاحة، أو أن يقوموا بحسب مبالغ نقدية كبيرة من أجهزة التوزيع الآلي لأوراق البنك، وذلك قبل قيام حامل البطاقة الأصلي من الإبلاغ عن سرقتها منه أو فقدانها، ذلك أن الجاني أو الواجد لها يعلم أن البنك سوف يلغي هذه البطاقة بوضعها على قائمة المعارضات، ويمحو برمجة أجهزة السحب النقدي الآلي، فإن الجاني يسرع بصرف مبالغ نقدية كبيرة، أو يحصل على سلع وخدمات من البطاقة بأسرع وقت ممكن.

أمّا السرقة الصورية، فتتحقق عند ما يقوم الحامل الشرعي للبطاقة بتنفيذ كل ما يجب عليه في حالة فقدان البطاقة منه أو سرقتها، بأن يبلغ البنك المصدر للبطاقة، وأيضا يبلغ الجهات الأمنية المختصة، في حين أن البطاقة مازالت في حوزته، ويستمر في التعامل لها رغم إبلاغه البنك المصدر لها وجهاز الضبطية القضائية، خاصة في سحب أوراق البنوك من أجهزة التوزيع الآلي للنقود.[1]

إن التكييف القانوني لاستعمال البطاقة الإلكترونية المسروقة أو المفقودة في سحب مبالغ نقدية يرى جانب من الفقه الجنائي، أن استعمال البطاقة الإلكترونية بعد سرقتها

[1] – طارق عبد العال، التجارة الإلكترونية، المفاهيم والتجارب والتحريات والأبعاد، التكنولوجية والمالية التسويقية والقانونية، الدار الجامعية للنشر، الطبعة الأولى، القاهرة، سنة 2003،ص 147.

ينطوي عليها جريمة احتيالا، لأن المتهم انتحل اسما كاذبا، ومن ثم يكون قد استخدم وسيلة احتيالية لإقناع المجني عليه بوجود ائتمان.

الفرع الثالث: الجرائم التي تقع عن طريق شبكة الانترنت

نرى في هذا الموضوع، كما رآه بعض شراح القانون، أن بعض هواة التعامل مع شبكة الانترنت قد تمكنوا من التقاط أرقام بطاقات الدفع الإلكتروني الخاصة ببعض العملاء من الشبكة، واستخدموا أرقامها في الحصول على السلع التي يرغبونها، ويتم خصم القيمة من حساب العملاء الشرعيين لهذه البطاقة، و هذا أمر طبيعي، لأنّه لا توجد شفرة خاصة باستخدام بطاقات الفيزا كارد أو الماستر كارد عند استعمالها في الحصول على السلع أو الخدمات عن طريق شبكة الانترنت فالتحايل في هذه الشبكة في الوقت الحالي أمر سهل، لأن تخليق أرقام بطاقات الدفع الإلكتروني عملية سهلة، حيث يتوافر في الأسواق برامج تشغيل بسيطة تتيح إمكانية تخليق أرقام بطاقات بنك معين، من خلال تزويد الحاسب بالرقم الخاص بالبنك المصدر للبطاقات.[1]

هذا وإن العمل يجري حاليا على تصميم نظام SET [2] على الحاسب الآلي لتأمين استخدام بطاقات الدفع الإلكتروني على شبكة الانترنت.

والأساليب التي يستخدمها قراصنة الحاسب الآلي في الحصول على بيانات بطاقة الدفع الإلكتروني لاستخدامها بطريقة غير مشروعة في الحصول على السلع والخدمات عبر شبكة الانترنت وهي:

[1] – عبد الفتاح مراد، شرح قوانين التوقيع الإلكتروني في مصر والدول العربية، شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني، الإسكندرية، سنة 2004، ص 151.

[2] – secure Electronic Transations.

أ- أسلوب الخداع:

وهو يتحقق بإنشاء مواقع وهمية على شبكة الانترنت على غرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة، بحيث أنه يظهر على الموقع الأصلي المقدم لتلك الخدمة، ويأتي ذلك بعد أن يحصل القراصنة على البيانات الخاصة بالموقع الأصلي، عنوانه، ورقمه من خلال شبكة الانترنت، واستخدامها في إنشاء الموقع الوهمي، مع تعديل البيانات السابقة على الموقع الأصلي بالشبكة، بحيث لا يكون هناك إلاّ موقع واحد بنفس العنوان، ويترتب على ذلك استقبال موقع قراصنة الحاسب الآلي الوهمي على شبكة الانترنت لجميع المعاملات التجارية والمالية التي يقدّمها الموقع الأصلي عبر الشبكة لأغراض التجارة، ومن بينها، وهو ما يتعلق بموضوعنا البيانات الخاصة ببطاقة الدفع الإلكتروني، وكذلك استقبال كافة الرسائل الإلكترونية الخاصة بالموقع الأصلي والإطلاع عليها.

ب- أسلوب التجسس:

وفيه يقوم قراصنة الحاسب الآلي باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالشركات و المؤسسات التجارية العامة على شبكة الانترنت، وبالتالي يتمكنون من الحصول على ما يريدون من المعلومات، ومنها ما يتعلق ببطاقات الدفع الإلكتروني، ورغم صعوبة تحديد شخصية مخترقي أنظمة المعلومات، إلاّ أنه يمكن تحديد كيفية الاختراق وزمانه، وكلمة السرّ التي استخدمت لاختراق النظام، وذلك من خلال مراجعة ملفات الدخول والملفات الخاصة التأمينية الخاصة به، بما سمح بجمع أكبر قدر ممكن من الأدلة التي تشير إلى مرتكب الحادث، وبذلك يتمكن الجاني من سرقة بطاقة

بيانات البطاقة الصحيحة، والتعامل بها من خلال شبكة الانترنت على حساب الحامل الشرعي للبطاقة.[1]

ثالثا: حالة تزوير البطاقة الإلكترونية.

نتناول الآن جريمة أخرى هي جريمة تزوير بطاقات الدفع الإلكتروني، وهذا ما يكون في الغالب مع بطاقات دفع صحيحة، ولكنها مسروقة، ويتم استبدالها ببيانات وغالبا ما يحدث هذا مع الأجانب القادمين من أجل السياحة، في جمهورية مصر العربية، والذين يستخدمون البطاقات المزورة في شراء الأشياء الثمينة من مجوهرات وساعات، بحيث يمكن تصريفها، والحصول على أثمانها بسهولة.[2]

أركان التزوير:

ظهرت فكرة تزوير البطاقات الممغنطة كوسيلة يتحايل بها الجناة على أجهزة الرقابة الآلية للمواصلات، حتى يمكنهم المرور منها بدون دفع الأجرة المستحقة، ثم استخدموها للدخول إلى أجهزة التوزيع الآلي لأوراق البنوك بغرض السحب منها والاستيلاء على ثروة الغير، وعلى ذلك فإن التزوير له ركنان هما:

1- هو تغيير الحقيقة وهذا معناه أن الحقيقة الواقعية يتم استبدالها بما يخالفها، فإذا لم يكن هناك تغيير في الحقيقة فلا يقوم التزوير، وتطبيقا لذلك فقد قضى بأنه لا يكون مرتكبا للتزوير متى كانت هذه الورقة الثانية قد حررت بخطه هو نفسه وتوقيعه، وأمضى عليها الشاهدان الموقعان على المخالفة الأولى فعلا بنفسيهما.

[1] – الرائد حسين على عباس، مخاطر استخدام بطاقة الدفع الإلكتروني عبر شبكة الانترنت، المشاكل، الحلول، ورقة عمل مقدمة إلى ندوة الدور المستحدثة لجرائم بطاقات الدفع الإلكتروني، التي نظمها مركز بحوث الشرطة بأكاديمية في 14ديسمبر 1998، ص18.

[2] – جميل عبد الباقي الصغير، المرجع السابق، ص32.

2- أن يكون تغيير الحقيقة في محرر، أمّا إذا كان تغيير الحقيقة في قول أو فعل فإنه يخرج عن نطاق التزوير، وإن كان يشكل جريمة أخرى كشهادة الزور أو اليمين الكاذبة أو الاحتيال.

ويقصد بالمحرر كل مسطور يتضمن علامات ينتقل بها الفكر لدى النظر أو ما يقوم مقامه كاللمس بالنسبة لنوع معين من الكتابة يدرك فاقد البصر معناه عن طريق اللمس.[1]

وبطاقة الدفع الإلكتروني تعتبر مجموعة من الأفكار والمعاني صادرة عن البنوك أو المؤسسات المالية، لذلك فإن مقومات المحرر تتوافر في هذه البطاقة، وبالتالي فإذا وقع تغيير في أحد بيانات هذه البطاقة.

مثل: البيانات الخاصة باسم الحامل، ورقم الحساب، وتاريخ الصلاحية، فإن الأمر يشكل تزوير، في محرر عرفي، إذا كانت الجهة المصدرة للبطاقة بنكا خاصاً أو أجنبياً، أما إذا كانت بطاقة الدفع الإلكتروني صادرة عن أحد المصارف المملوكة للدولة أو التي تساهم في مالها بنصيب ما، فإن هذا يعتبر تزوير محرر رسمي.[2]

[1] - محمد نجيب حسني، شرح قانون العقوبات، القسم الخاص، مطبعة نادي القضاء، القاهرة، 1987، ص 147.

[2] - فوزية عبد الستار، المرجع السابق، ص246.

المطلب الثاني: مفهوم الجريمة الإلكترونية

مع دخول الحاسب والانترنت إلى مجتمعاتنا في كافة جوانب حياتنا، بد أيظهر نوع جديد من الجرائم تسمى الجرائم الإلكترونية وبالتالي أصبح هناك حاجة لتعريف هذه الجرائم والتوعية حولها حيث عرّفها القانون بأنها هي كل فعل يعاقب عليه القانون أو امتناع عن فعل يقضي به القانون ولا يعتبر الفعل أو ترك الجريمة إلا إذا كان مجرما في القانون.

ومن ناحية أخرى فالجريمة هي كل فعل ضار يأتيه المواطن ويكون لهذا الفعل أثر ضار على غيره من المواطنين، وبالتالي فالجرائم الإلكترونية أي فعل ضار يأتيه المواطن عبر استعماله الوسائط الإلكترونية.

مثل: الحواسيب، شبكات نقل المعلومات، شبكة الانترنت، أو الاستخدامات غير القانونية للبيانات الحاسوبية أو إلكترونية عموما.[1]

الفرع الأول: مميزات الجريمة الإلكترونية عن غيرها من الجرائم.

تعتبر الجرائم الإلكترونية النوع الشائع من الجرائم إذ أنها تتمتع بالكثير من المميزات للمجرمين تدفعهم إلى ارتكابها، حيث تتميز الجرائم الإلكترونية بخصائص منفردة خاصة بها لا تتوفر في أي من الجرائم التقليدية في أسلوبها وطريقة ارتكابها وهذه الخصائص هي:

1- الحاسب الآلي هو أداة ارتكاب الجرائم الإلكترونية:

تعتبر هذه الخاصية من أهم الخصائص التي تميز هذا النوع عن غيرها من الجرائم الأخرى، ذلك لأن شبكة الانترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة وذلك فإن ارتباطها بالحاسب الآلي هو أمر لا مفر منه باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي.

[1] – نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2007، ص35.

2- جرائم ترتكب عبر شبكة الانترنت أو عليها.

تعد شبكة الانترنت الحقل الذي تقع فيه الجرائم الإلكترونية، وذلك لأنها تمثل حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم وغيرها من الأهداف التي تكون غالباً الضحية لها إلاّ أنّه وبالرغم من كونها الوسيلة لارتكاب الجرائم إلى جانب الحاسب الآلي، فإنها كذلك لن تنجو من يد المجرمين لأنها هي الأخرى قد تكون محلا لاعتداءات.[1]

3- مرتكب الجرائم الإلكترونية هو شخص ذو خبرة:

تتطلب هذه الجرائم على غرار الجرائم التقليدية أن يكون الشخص خبيراً بالقدر اللازم بأمور الحوسبة ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي، فإن الشرطة تبحث أولاّ عن خبراء الكمبيوتر عند ارتكاب هذا النوع من الجرائم.

4- جريمة الانترنت جريمة عابرة للحدود:

شبكة الانترنت ذات طابع دولي إذ أنها لا تعترف بتلك الحدود القائمة بين الدول سواء الجغرافية أو السياسية وهذا ما أدى إلى اعتبار أن الجرائم الإلكترونية من الجرائم الدولية، وتأخذ بعدا دولياً من حيث إمكانية أن يكون العمل الإجرامي عبر الانترنت ذو طبيعة عالمية، ذلك حينما ترتكب داخل الدولة إلا أنها تمتد إلى خارج تلك الأخيرة مما يعني خضوعها الأكثر من قانون جنائي، وتعتبر الجرائم الإلكترونية جرائم دولية في الحالة التي يكون أحد أطرافها شخصاً دولياً، كما يمكن أن تكون في مقابل ذلك جريمة وطنية إذ أن لها أثر إقليميا من حيث أن حجم الأثر المكاني يحتويها كأي جريمة ثانية.[2]

[1] - نفس المرجع،ص36.

[2] - نبيلة هبة هروال، المرجع السابق، ص 39.

5- صعوبة إثبات الجرائم الإلكترونية:

تعتبر هذه الخاصية من الخصائص المميزة للجرائم الإلكترونية عن غيرها من الجرائم نظراً لكونها ترتكب بواسطة الانترنت ومن قبل شخص ذو دراية فائقة بها وما ينجم عن ذلك من سهولة إخفاء معالم الجريمة والتخلص من آثارها وبالتالي فإنه تعود صعوبة إثبات الجرائم الإلكترونية إلى:

- صعوبة الإثبات الفني بآثارها إن وجدت.
- يلعب البعد الزمني (اختلاف المواقيت بين الدول)، والمكاني(إمكانية تنفيذ الجريمة عن بعد) والقانوني (أي القانون يطبق)دورا مهما في تشتيت جهود التحري والتنسيق الدولي لتعقب هذه الجرائم.

الفرع الثاني: أركان الجرائم الإلكترونية:

يقصد بأركان الجريمة عناصرها الأساسية التي يطلبها القانون لقيام الجريمة وهي أركان خاصة وهي التي نص عليها المشرع بصدد كل جريمة على حدى وأركان عامة وهي الواجب توافرها أي كان نوع الجريمة أو طبيعتها.

1- الركن المادي:

الأصل أن القانون لا يعاقب على النوايا مهما كانت شريرة مادامت محبوسة في نفس الجاني فالقانون يعاقب على الأفعال المادية التي تصدر من الجاني،[1] لكن كل جريمة تستلزم وجود أعمال تحضيرية وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي الإلكترونية حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية.

[1] – عبد الله سليمان، شرع قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزائر، الطبعة السادسة، 2005، ص 65.

حيث تنص المادة 31 من القانون 06-23 المحاولة في الجنحة لا يعاقب عليها إلا بناءاً على نص صريح في القانون، والمحاولة في المخالفة لا يعاقب عليها إطلاقا.[1]

إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق ومعدلات لفك الشفرات وكلمات المرور وحيازة صور دعارة، فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

2- الركن المعنوي:

هو الجانب الشخصي أو النفسي للجريمة، فلا تقوم الجريمة بمجرد قيام الواقعة المادية التي تخضع لنص التجريم بل لابد أن تصدر هذه الواقعة من إرادة فاعلها وترتبط بها ارتباطها معنويا، حيث برزت مشكلة الركن المعنوي في الجريمة الإلكترونية في قصية موريس الذي كان متهما في قضية دخول غير مصرح به جهاز الحاسب الفيدرالي وقد دفع محامي موريس على انتفاء الركن المعنوي الذي جعل المحكمة تقول هل يلزم أن يقوم الادعاء بإثبات القصد الجنائي في جريمة الدخول الغير مصرح به بحيث تثبت نية المتهم في تحدي الخطر الوارد على استخدام نظم المعلومات في الحاسب وتحقيق خسائر.

أما بالنسبة للمشرع الجزائري فقد نص في المادة 394 مكرر 2 من جريمة المساس بأنظمة المعالجة الآلية للمعطيات، على أنّه كل من يقوم عمداً وعن طريق الغش، وهنا تحقق عنصر العلم والإرادة.

[1] - المادة 31 المؤرخ في 20-12-2006 المعدل والمتمم رقم 66- 156 المؤرخ في 8يونيو 1966(الجريدة الرسمية، رقم 84المؤرخة في 24-12-2006).

3- الركن الشرعي:

يعبر عن الركن الشرعي في الجريمة لا عقوبة ولا جريمة ولا تدابير أمن إلا بنص في القانون.[1]

والركن الشرعي في الجرائم الإلكترونية يعبر عنه بالمعاهدات الدولية التي تنظمها كل دولة محاربة لهذه الجرائم حيث يقوم على موقفين:

أ- أحدهما يصر على وجوب أن يكون التنظيم القانوني في إطار الحد الأدنى، وبأضيق مدى منعا لأية قيود على بيئة الانترنت التي يضعها أصحاب هذا الرأي بأنها البيئة الديمقراطية، والإبداعية والمتفتحة، والتي تستقيم مع القيود التي تحد من هذه السمات.

ب- أمّا الثاني فإنه يرى الانترنت شأنها شأن أي مخترع جديد يحتاج إلى تدابير تشريعية تحمي المصالح وتقييم معايير وقواعد تكفل إحداث التوازن المصالح المتعارضة من جهة وتتيح مواجهة الآثار والظواهر السلبية في بيئة الانترنت.

وفي ظل كل هذا سنت العديد من دول العالم قوانين جنائية خاصة أو عدلت قوانين العقوبات لديها بما يكفل مواجهة الجرائم الإلكترونية حيث بالنسبة للمشرع الجزائري فقد تدارك الفراغ القانوني في مجال حماية المال المعلوماتي من خلال استحداث نصوص تجريمية لقنع الاعتداءات الواردة على المعلوماتية بموجب القانون06-23 المتضمن تعديل قانون العقوبات، كخطوة تظهر اهتمام المشرع الجزائري لمثل هذه الجرائم والتمهيد لجرائم أخرى متصلة بنفس الموضوع، وذلك من خلال جريمة المساس بأنظمة المعالجة الآلية للبيانات والمعطيات والتي جاءت بها المشرع في المادة394 مكرر إلى المادة 394 مكرر من قانون العقوبات الجزائري. [2]

---

[1] - المادة 1من القانون 06-23 المؤرخ في 20-12-2006 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8يونيو 1966.

[2] - انظر قانون 06-23المؤرخ في 20-12-2006 المعدل والمتمم للأمر رقم66-156.

أمّا بالنسبة للدول العربية فقد كانت الإمارات العربية هي أو دولة عربية تصدر قانونا خاصا بمكافحة جرائم المعلومات، حيث أصدر صاحب السمو الشيخ بن زايد آل نهيان، رئيس دولة الإمارات القانون الاتحادي رقم 2لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات.

وكمثيلاتها قامت المملكة العربية السعودية تحت إشراف مجلس الوزراء في جلسته يوم الإثنيين 7فيفري 2007برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز نظام مكافحة الجرائم المعلوماتية، وهو يتضمن 16مادة.[1]

بما أن الدول الغربية قد استأثرت منذ البداية بهذا المجال فإنها كانت سباقة هي الأخرى في مجال الحماية المقررة له، وشمل ذلك العديد من دول أوروبا وأمريكا، حيث تعتبر دول السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت حيث صدر قانون البيانات السويد عام 1973 الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي، وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قوانين خاصة بحماية أنظمة الحاسب الآلي (1976-1985) .

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي، حيث أقرت قانون مكافحة التزوير والتزييف عام 1981، أمّا النموذج الأوروبي الأكثر تطورا فهي اتفاقية بودابست الاتفاقية الدولية للإجرام المعلوماتي أبرمت تاريخ2001/11/08 من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

[1] - الموقع الإلكتروني w.w.w.nasb.net

المطلب الثالث: الطبيعة الخاصة للجرائم الإلكترونية

الجريمة المعلوماتية هي الجريمة التكنولوجية الحديثة، والمطلوب من جهاز الضبطية القضائية مقاومتها وإثبات، لكي تتم محاسبة مرتكبيها، هي جريمة لها أشكال متعددة فقد يتم ارتكاب الجريمة على جهاز الحاسب الآلي نفسه، سواء كان ذلك على مكوناته المادية، أو المعلوماتية، أو غير المادية، وقد يستخدم الحاسب الآلي كأداة لارتكاب إحدى الجرائم المعلوماتية، وما يهمنا في موضوعنا هو وقوع الجريمة على مكونات الغير مادية للحاسب الآلي، وتتحقق هذه الحالة عند ما تكون مكونات الحاسب، محلا أو موضوعا للجريمة.[1]

الفرع الأول: الأساليب المستخدمة للاعتداء على المكونات غير المادية للحاسب.

هناك أساليب تتطلب معرفة فنية معينة يستطيع الجاني من خلالها القيام بعملية ما يسمى" **السطو المسلح الإلكتروني**" الذي يكون هدفه فقط التقاط أو تسجيل المعلومات أو البيانات المعالجة إلكترونيا، ويمكن عرض بعض المسائل فيما يلي:

1- التقاط المعلومات التي توجد ما بين الحاسب والنهاية الطرفية:

يحدث هذا الالتقاط بواسطة توصيل خط تحويلة يعمل على تكبير الذبذبات الإلكترونية وإرسالها إلى النهاية الطرفية التي تقوم بعملية التجسس، وقد يحدث ذلك أيضا باستخدام جهاز مرسل صغير يمكنه نقل البيانات عند بعد، ويمكن الالتقاط كذلك عن طريق هوائيات مطاردة بالقرب من الهوائيات الاحتياطية، وبالتالي يحدث التقاط للإشعاعات العابرة عن طريق النقل الجوي للمعلومات عند بثها بالقمر الصناعي واحتجاز مضمونها.[2]

---

[1] – محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية للنشر والتوزيع، الطبعة الثانية، القاهرة، سنة 2003،ص 223.

[2] – عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دور الشرطة والقانون، دراسة مقارنة، بدون دار النشر القاهرة، سنة 2000، ص 223.

2- التوصيل المباشر بواسطة خط هاتفي:

يمكن إحداث ذلك بواسطة وضع مركز تصنت يجعل من تسجيل الاتصالات أمرا يسيرا، كما يمكن كذلك وضع ميكروفونات صغيرة لأداء هذه المهمة.

3- التقاط الإشعاعات الصادرة عن جهاز المعلوماتي:

تمكن خطورة هذه الوسائل في أنها يمكن أن تؤدي إلى إعادة تكوين خصائص المعلومات التي تبث وتنتقل من خلال الأنظمة المعلوماتية، وهذا لا يحتاج تسجيل الإشعاعات الصادرة من الحاسب وحل شفرتها.

4- التدخل غير المشروع في نظام بواسطة طرفية بعدية:

هو إمكانية الاعتداء على معلومات وبيانات الحاسب الآلي خاص بمؤسسة أو هيئة، مما يشكل خطرا كبيرا عليها، فإن الجاني في هذه الحالة إذا كان لديه قدر من المعرفة الفنية بأنظمة الحاسب فإنه يستطيع القيام بما يلي:[1]

أ- إدخال معطيات أو معلومات وهمية، حيث يمكن بهذه الوسيلة أن يستولى على أموال لنفسه عن إحدى الطرق التالية:

- ضم مستخدم أو عمال موظفين غير موجودين بالفعل في هذه الجهة.
- الإبقاء على موظفين فصلوا، أو تركوا العمل بالفعل.
- إتلاف المعلومات، عن طريق استبدال رقم حساب برقم آخر.

ب- التلاعب في البرامج التشغيلية وهو ما يسمى بـ" **المصيدة**" اصطناع برنامج وهمي.

ج-التلاعب في البرامج التطبيقية وهذه الصور لها أساليب متعددة لأنها من أكثر صور الجرائم المعلوماتية انتشار نذكر منها: [2]

[1] - عفيفي كامل عفيفي، المرجع نفسه، ص 225.

[2] - جميل عبد الباقي الصغير، المرجع السابق، ص 230.

أ- أسلوب سلامي(Salmi) :

ويعتمد على السرقة من عدد كبير من المصادر بكميات قليلة أو ضئيلة بحيث لا يفطن المجني عليه للسرقة، وإذا اكتشافها لا تستحق عناء الإبلاغ أو الشكوى.

ب- زرع برنامج فرعي Unsous- program :

غير مسموح به في البرنامج الأصلي، وهذا البرنامج يسمح لمن قام بزرعه بالولوج غير المصرح به في موردات النظام الخاصي للحاسب الآلي، وتمكن خطورة هذا البرنامج في حجمه الصغير وسريته وإمكانية دفنه بين تعليمات البرامج المتعددة، الأمر الذي يؤدي إلى سلب هذه التعليمات دون إمكانية اكتشاف عملية السلب.

الفرع الثاني: حالة استخدام الحاسب الآلي كأداة لارتكاب الجريمة.

هذه الحالة تختلف عن سابقتيها، فلا يكون الحاسب محل أو موضوع للجريمة وبالتالي لا يكون محلا، أي الحاسب للحماية الجنائية، ولكن الجريمة تقع في هذه الحالة الثالثة بواسطة الحاسب الآلي، أي أنّه يكون أداة في ارتكاب الجريمة.

ومن الناحية النظرية يمكن أن تقع بعض الجرائم بواسطة الحاسب الآلي، **مثل:** الجرائم التي تقع على الذمة المالية من سرقة واحتيال وإساءة الأمانة والتزوير في عمليات السحب على الجوائز وانتهاك حرمة الحياة الخاصة بل وتستخدم في القتل عن طريق "**برمجة جهاز تفجير**" يتم التحكم فيه آلياً، أو جهاز لإطلاق الأشعة القاتلة.[1]

ومرتكب هذه الجرائم هو المستخدم أو المتلاعب في الحاسب الآلي، ونظامه الأخير ما هو إلا وسيلة أو أداة لتنفيذ الجريمة، ومحلها يختلف بحسب الشيء الذي ينصب عليه سلوك الفاعل، والذي يشكل محل الحق أو المصلحة المحمية.

[1] -حاتم عبد الرحمان منصور الشحات، الإجرام المعلوماتي، دار النهضة العربية، للنشر والتوزيع، القاهرة، سنة2002 ، ص 227.

الفرع الثالث: سمات مرتكبي الجرائم الإلكترونية

يتسم المجرم الإلكتروني بعدّة صفات تميزه عن المجرمين العاديين للدرجة التي نقول أن هذا المجرم يتصف بالذكاء ويسبب هذه الصعوبات نجد أن بعض الفقهاء الذين تناولوا هذا الأمر بالبحث إمّا إلى:

أ- التوسع مفهوم (النمط النموذجي) للمجرم المعلوماتي:

تتضح معالم هذا التوسع في أنّه يستخدم مصطلح (أشكال أو الصور النموذجية) للمجرم المعلوماتي في صيغة الجمع، بدلا من النمط النموذجي للتعبير عن السمات أو الخصائص الرئيسية لطائفة من مجرمي المعلوماتية، وفقاً لهذا يمكن استخلاص السمات العامة لشخصية المجرم المعلوماتي بأنه يبدأ في سن النضوج دون حد أقصى للسن وأنه يلاحظ أن معظم الأنشطة الإجرامية المعلوماتية ترتكب في المرحلة السنية المحصورة بين الرابعة عشر والأربعين (14إلى 40) ويلاحظ أن شخصية المجرم المعلوماتي غالباً ما تكون بعيدة عن الاتجاهات السياسية[1].

ب- التحفظ في رسم السياسات للمجرم المعلوماتي:

في مفهوم السمات العامة للمجرم المعلوماتي، وهو الذي يقول الفقهاء "إنه ليس من الدقة التعمق في تحديد الخصائص العامة للمجرم المعلوماتي، ومن ثم فيجب توخي الحذر الشديد في هذا الشأن"، وانطلاقا من هذا المفهوم الحذر فإن السمات المشتركة في معظم حالات الإجرام المعلوماتي تقتصر على ثلاث سمات:[2]

1- صغر السن:

حيث يرى هذا الاتجاه الفقهي أن المجرم المعلوماتي يكون من صغار السن لأن كبار السن لأن كبار السن لم يألفوا التعامل مع الحاسب الآلي، ونقول أن هذه السمة، وإن

[1] - محمد سامي الشوا، المرجع السابق، ص 228.

[2] - حاتم عبد الرحمان منصور الشحات، المرجع السابق، ص 229.

كانت فهي على قدر كبير من الصحة إلاّ أن هذه هذا الأمر مرحلي ومؤقت، ويعود سببه إلى حادثة الطفرة المعلوماتية الهائلة التي يشهدها العالم المعاصر، ولكن مع مرور الزمن، ووصول الجيل الحالي من المجرمين المعلوماتي إلى سن متقدمة، فسوف تختفي هذه السمة من الوجود.

2- مستمدة من ظروف ارتكاب المجرم للجريمة المعلوماتي:

حيث لا تحتاج معظم الجرائم إلى مساعدة من الغير، فيقوم بها الجاني وحده، وذلك رغم أن طبيعة هذه الأنشطة الإجرامية لا تتعارض مع قواعد المساهمة الجنائية.

ونقول أن هذه السمة أيضا لا يمكن التسليم بها في ظل انتشار الجريمة المنظمة وتسهيل شبكة المعلومات لذلك.

3- تقوم على ضرورة توافر قدر من المعلوماتية لدى الجاني:

مما لا شك فيه أن تحديد السمات العامة لكل طائفة من طوائف المجرمين المعلوماتي على حدى تكون أكثر تعبيراً عن دوافع المجرم وبواعثه الإجرامية.[1]

[1] - حاتم عبد الرحمان منصور الشحات، المرجع السابق، ص 230.

المبحث الثالث: أنواع الجرائم الإلكترونية

صنف الفقهاء والدارسون الجرائم الإلكترونية ضمن فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم، فبعضهم يقسمها إلى جرائم ترتكب عن نضم الحاسب الآلي، وأخرى ترتكب بواسطته وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة، فتتوزع الجرائم الإلكترونية حسب التقسيم إلى جرائم تقع على الأموال وجرائم تقع على الأشخاص وهناك أيضا جرائم النصب الإلكتروني ونجد هذا التقسيم شائعاً من خلال الدراسات والأبحاث الأمريكية، ويلاحظ أنّه يقوم على فكرة الغرض النهائي أو المحل النهائي الذي يستهدفه الاعتداء.[1]

[1] – منير محمد الجنبيهي، جرائم الانترنت والحاسب الآلي، ووسائل مكافحتها دار الفكر الجامعي، الإسكندرية،سنة 2005،ص 186-187.

المطلب الأول: الجرائم التي تقع على الأشخاص

هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات الطابع الشخصي البحث، أي الحقوق اللصيقة بالشخص والتي تعتبر من مقومات الشخصية وتخرج عن دائرة التعامل الاقتصادي ومن أهم هذه الحقوق الحق في الحياة، والحق في سلامة الجسم وفي الحرية والحق في الصيانة والشرف.

الفرع الأوّل: جريمة انتحال الشخصية.

هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلّا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الإلكترونية، واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمان وغيره، ومن خلال هذه المعلومات يستطيع المجرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت.

الفرع الثاني: جرائم التشهير وتشويه السمعة

مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة، وذلك بهدف تشهير وتشويه سمعة تلك الرموز، وكذلك لتسميم أفكار الناس أو محاولة ابتزاز الأشخاص بنشر الشائعات عنهم وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على شبكة تحتوي على المعلومات المطلوب إدراجها، ونشرها أو إرسالها عبر المواقع الإلكترونية، ومن أمثلتها إرسال الصور الغير اللائقة أو معلومات غير صحيحة.[1]

[1] – منير محمد الجنبيهي، المرجع السابق، ص 188.

الفرع الثالث: الجرائم المخلة بالأخلاق والآداب العامة.

إذا كانت شبكة الانترنت تتسم بالعالمية ولا تقتصر على مستخدم دون الآخر فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معين قد تشكل جريمة يعاقب عليها القانون في حين أنّها لا تكون كذلك في أي بلد آخر.

وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم عبر الوسائل الإلكترونية أو محاولة إغوائهم لارتكاب هذه الأنشطة، أو نشر معلومات عنهم عبر الحاسب الآلي ودعوتهم إلى القيام بالأعمال الفاحشة، وتصوير القاصرين ضمن أنشطة للجنس، والأعمال الإباحية هي من أشهر الأعمال الحالية وأكثرها رواجا خاصة بالدول العربية وأوروبا والدول الآسيوية وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الانترنت كافة والأشكال سواء كان صور أو فيديو أو حوارات أو أرقام هاتفية مما خول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز.[1]

[1] – المرجع نفسه، ص189.

المطلب الثاني: الجرائم الواقعة على أموال التجارة الإلكترونية

لقد نصت المادة 350من قانون العقوبات الجزائري على أن تحل من اختلس شيئا غير مملوك له بعد سارقا.[1]

فهذا التعريف يهتم بالجانب الموضوعي للسرقة حيث يتطلب لقيام هذه الجريمة أن يرتكب الجاني فعلا ماديا محددا و هو الاختلاس وأن ينصب هذا الاختلاس على منقول مملوك الغير وبعد أن نتطرق لأركان جريمة السرقة وفقاً للقواعد العامة سنفهم كيفية وقوع هذه الجريمة بالطريق المعلوماتي سواء كان محل الاختلاس معلومات أو منقولات، كما أنه ينشأ في الفقه القانوني قبل صدور القانون خلافا حول هل يجوز أن تكون المعلومات أموال؟ وهل هي أشياء من المنقولات؟ حتى يمكن حيازتها، ومن ثم اختلاس هذه الحيازة كما في جريمة السرقة.

الفرع الأول: تعريف جريمة السرقة الإلكترونية

نصت المادة 350من قانون العقوبات الجزائري على أن تحل من اختلس شيئا غير مملوك له يعُد سارقاً ويعاقب بالحبس من سنة إلى خمس سنوات وبغرامة مالية 100.00دج إلى 500.00دج وتطبق نفس العقوبة على الاختلاس.[2]

من هذا التعريف يمكننا القول بأن السرقة جريمة عمدية، يتطلب لقيامها أن يرتكب الجاني فعلاً هو الاختلاس وأن ينصب هذا الاختلاس على منقول مملوك للغير إضافة إلى الركن المعنوي والمتمثل في القصد الجنائي وهو قصد الغش، هذه هي الأركان العامة لجريمة السرقة التقليدية، فما مدى انطباق هذه القواعد على السرقة المعلوماتية؟ وتحديد أما مدى احتمال الأموال في التجارة الإلكترونية لفكرة السرقة؟ هذا ما سوف نتجه إليه.

---

[1] – المادة 350من القانون رقم 06-23المؤرخ في 20ديسمبر2006 المتضمن قانون العقوبات الجزائري

[2] – القانون رقم23/06 المؤرخ في 20ديسمبر 2006، ص 127.

إنّ المعلومات المعالجة أو البيانات بوصفها كبيانات منطقية أصبحت من القيم الاقتصادية المستحدثة، وبالتالي فهي ذات طابع مالي، ولذلك يسلم جانب من الفقه الجنائي بأن المعلومات تصلح لأن تكون محلا للسرقة بالاعتداء عليها من حوزة صاحبها، فالمعلومات لها قيمة تقدر بثروات طائلة ولذلك تتقي صفة المال عن شيء متى انعدمت قيمته، ويتم الحصول على هذه المعلومات عن طريق الحصول على كلمة السّر بطريقة فنية ممن يعملون في مجال المعلوماتية أو من شخص يعمل في وظيفة تساعده في الحصول على كلمة السّر، ويكون ذلك بدخول الجاني إلى نظام معلومات خاص، ويلتقط معلومات أو يسرقها بطريقة النسخ على مستندات أو شرائط وبالتالي أصبحت المعلومات ذات كيان مادي بتسجيلها على شريط أو بطباعتها ونقلها والاستيلاء عليها.[1]

الفرع الثاني: النطاق القانوني لحركية السرقة الإلكترونية

لتحقيق جريمة السرقة الإلكترونية يجب أن تتوفر شروط في موضوع السرقة أو محلها وهذه الشروط هي:

1- أن يكون موضوع السرقة شيء:

اختلف التشريع الفرنسي مع التشريع المصري حيث نجد في المادة 1/311ق عقوبات الفرنسي جاء بصيغة شيء ويعبر عنه في القانون المصري باللفظ المادي و هذا الكلام يقودنا إلى أن الأموال أو الأشياء المعنوية لا تدخل في مجال السرقة إلاّ إذا أخذت شكلها المادي حيث يمكن الاستئثار به أي في ديسك أو قرص مرن فالمعلومات التي تظهر على الشاشة لا تصلح لأن تكون محلا للسرقة، حيث أو سرقة المعلومات تكون قبيل الأوراق والمستندات والحلقات وفقا لنص المادة 1/311ق.ع. فرنسي قد تأكد أن البيانات أو المعلومات تأخذ تشكل نبضات إلكترونية تمثل الرقمين، الصفر والواحد وبهذا يشبه التيار الكهربائي والذي

[1] – انظر د.عبد. الفتاح بيومي حجازي، الكتاب الثاني، المرجع السابق، ص 163.

يعتبر شيء مادي وهي بذلك تشغل حيزا مادياً يمكن قياسه بمقياس معين البايت، الكيلوبايت، والميجابايت.[1]

2- أن يكون موضوع السرقة مادي:

طالما يمكن حيازة الأشياء غير كحق الارتفاق وحق الانتفاع من الممكن سرقة حيازة المعلومات حسب المادة 311 قانون عقوبات الفرنسي.

- يتحقق الاستيلاء على المعلومة عن طريق السمع أو المشاهدة و بالتالي تنتقل المعلومة ممن عقل إلى آخر، ومن ذمة مالية لأخرى، فاكتفى الغير بالتقاط المعلومة في ذهنه دون تسجيلها أو تدوينها لا يقع محلا للسرقة، أما إذا قام بتدوينها أو تسجيلها وحرم صاحبها من الانتفاع بها فهذا يقع تحت طائلة السرقة الإلكترونية.

- قيام محكمة النقض الفرنسية بإدانة شخص قام بإخفاء معلومات مع عمله بالوقائع وقيامه بتقديم صور منسوخة من مسند مسروق متضمن لمعلومات سر التضييع.

- قيام محكمة النقض الفرنسية بإدانة عامل قام بنسخ مستندات سرية دون علم صاحبها.

- إن المعلومات تشكل قيمة مادية حتى بالرغم من انفصالها عن دعامتها المادية فهي ذات قيمة اقتصادية تمكن مستغلها من إبرام عقود مع الغير وحرمان صاحبها من عائدها المادي.[2]

3- أن يكون موضوع السرقة منقول:

حسب نص المادة 311 من قانون العقوبات الفرنسي يعرف: أن المعلومة هي شيء منقول وبمعنى أدق المعلومة المتبادلة عبر الانترنت تعد من المنقولات إن المعلومات المتنقلة عبر الحواسيب بواسطة خطوط الانترنت إذا التقطت بالسمع أو المشاهدة لا تقوم جريمة السرقة

[1] - محمد أمين الشوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية، مكتبة دار الثقافة، للنشر والتوزيع، الطبعة الأولى، بدون بلد، سنة2004، ص148-150.

[2] - نفس المرجع السابق، ص 152-153.

لأنّها لا تنقل الحيازة، إلا أن بعض النصوص الجنائية تجرم فعل الالتقاط فقد تكون هذه المعلومات نادرة وتلحق الضرر بالغير، بالأخص إذا عمل نسخ منها وباعها بسعر أقل من سعر النسخة الأصلية.

4- أن يكون موضوع السرقة مملوكها للغير:

يجب أن يكون الشيء محل السرقة اعتداء على الحيازة وحق الملكية على الشيء وبالتالي تنهي صفة السرقة إذا ما اختلس شخص مالاً مملوكاً له أصلا فهو أولى بحيازته، أو كان يجوز شخص مالا يكون صاحبه ملزما بترك حيازته لسبب معين كوعد البيع كما أن التصرف في مال غير مملوك لأحد معين، إذا يعدّ ذلك اكتسابا مشروعاً للملكية.[1]

الفرع الثالث: أركان الجريمة السرقة الإلكترونية

من المسلم به أن للسرقة ركنين أساسيين ركن مادي وركن معنوي، ذلك أن الطبيعة الخاصة للتعاملات الإلكترونية خاصة وأنها على منقولات مادية:

1- الركن المادي لجريمة السرقة الإلكترونية: يعُّد الركن المادي لجريمة السرقة سلب حيازة الشيء من مالكه أو حائزه بغير رضائه وبذلك أصبحت فكرة الاختلاس في جريمة السرقة تربط بفكرة الحيازة المدنية.

ويقصد بسلب الحيازة كل من فعل مادي يأتيه الجاني ويترتب عليه إخراج شيء من حيازة صاحبه أو حائزه، وإدخال في حيازته أيا كانت الوسيلة المستعملة في سلب الحيازة، وسواء احتفظ الجاني لنفسه بحيازة الشيء المسلوب أو تناول عن هذه الحيازة إلى الغير، ويتحقق فعل الاختلاس بتوافر العنصريين المادي والمعنوي فيتحقق العنصر المادي بانتقال الحيازة عن طريق السلب سواء كانت أم مجرد حيازة وذلك دون رضا المجني عليه أي المالك الأصلي، ويتحقق الركن المعنوي في نية الاستئثار لملكية الشيء والظهور عليه بمظهر المالك إلاّ أن علم المالك الأصلي بانتقال الحيازة إلى غيره ينفي فعل الاختلاس، وقد استقرت

[1] – محمد أمين الشوابكة، المرجع السابق، ص 154.

محكمة النقض الفرنسية صراحة (حتى لأن) حيث جاء في نص المادة 1/311 قانون عقوبات فرنسي" اختلاس شيء" لا يساعدهما في ذلك، كما أنها لا تريد أن تخلط بين قانون حماية حق المؤلف الذي يسري على نسخ المعلومات المحمية بهذا القانون (وهي البرامج وغيرها من المعلومات التي يتوفر فيها شرط الحدة والأصالة). [1]

وقد تعددت جريمة السرقة مع جريمة الإخلال بحق المؤلف عندما يقوم المتهم بنسخ بيانات يحملها قانون حق المؤلف (كأن مؤلفا لا يزال مخزنا في الكمبيوتر ولم يتم نشره أو برنامج كمبيوتر أو قاعدة بيانات)، فلا يشترط القضاء أن يتم نشر العمل الذي تم تقليده إخلالا بحق المؤلف بل يكفي متاحا للجمهور في هذا الفرض يتوفر التعدد المعنوي للجريمتين وذلك نظراً لوحدة النشاط الإجرامي ويعاقب عن جريمة ذات العقوبة الأشد.[2]

2- الركن المعنوي لجريمة السرقة الإلكترونية :

أ- تعريف نية المالك:

هي توفر نية حرمان المالك من سلطاته وبالتالي تقع جريمة السرقة ومهما اعتبرنا نية التملك داخلية في القصد الجنائي العام أي أنها تشكل قصداً جنائياً، فإنها على أية حال من الأحوال ضرورة لوقوع جريمة السرقة، لذا قضت المحكمة بنقض الحكم الذي اقصر، أي أن المتهم استولى على مال مملوك للمجني عليه(قطع من الذهب) دون موافقة صاحبها، وذلك في مقابل ما أداه هذا المتهم للمجني عليه من خدمات، فقد نفت المحكمة أن لم يبين نية، التملك. [3]

[1] - شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة مصر، بدون طبعة، سنة 2007،ص49

[2] - شيماء عبد الغني محمد عطا الله، المرجع نفسه، ص51

[3] - شيماء عبد الغني محمد عطا الله، المرجع نفسه، ص52-53

ب- النتائج المترتبة على استلزام نية التملك:

إن توافر نية الرد لا يحول دون توافر القصد الجنائي في سرقة المعلومات، ذلك لأنه يكتفي بتوفر نية التملك بصفة مؤقتة عليها، استناد إلى أن توافر نية الرد لا يجول دون توافر نية التملك إذا كان المال من طبيعة أن يهلك أو يفقد الشيء قيمته أو أن الاستيلاء عليه يحرم صاحبه من الاستئثارية، وهذا هو الوضع بالنسبة للمعلومات.

ج- نية حرمان المجني عليه من المال المسروق أمر متطلب في القانون المقارن:

لا تقع جريمة السرقة إلا مع توافر نية التمالك وفقاً للقوانين المقارنة، وقد عبر القانون الفرنسي عن ذلك في المادة 1/131ق العقوبات "من اختلس بسوء النيّة، "كما يتطلب في القانون الانجليزي أيضا نية التملك حيث نص القانون السرقة 1968 بتعبير"يعتبر الشخص مرتكباً للسرقة إذا استولى لنفسه، بسوء النيّة، على أموال تنتمي إلى الغير، بنية حرمان هذا الأخير بشكل دائم منه".

د- تحريم استعمال أموال الغير بنيّة الغش:

هذا النوع من التجريم يمكن إعماله على استعمال جهاز الكمبيوتر الخاص بالغير بدون موافقته، فالقانون المصري يتضمن نصاً بخصوص استعمال شيء الغير وهو الذي تقرره المادة 323قانون العقوبات المصري، مكرر(أولا)الخاص باستعمال سيارة بدون إذن صاحبها.

هـ- ضرورة تجريم استعمال النظام بدون موافقة صاحبه بنصوص خاصة:

نتيجة لتشريعات عديدة تجرم استعمال ملك الغير دون رضائه، ويأتي تجريم استعمال كمبيوتر الغير في صورة التداخل فيه متماشياً مع ما تتضمنه بعض التشريعات من تجريم استعمال سيارة ملك الغير بدون رضائه، فعلى الرغم من عدم توافر نية التملك، فإن الفعل

يشكل جريمة بنص المادة 323مكرر 1 من قانون العقوبات المصري على أنّ" يعاقب كل من استولى بغير حق وبدون نية التملك على سيارة مملوكة للغير".[1]

[1] – شيماء عبد الغني محمد عطا الله، نفس المرجع السابق، ص 55.

المطلب الثالث: جرائم النصب الإلكتروني

بالنظر للتباين الموجود بين جرائم الانترنت والجرائم التقليدية وجد الفقهاء في حيرة من الثبات في رأي واحد فتمايزت أراءهم بحسب الموضوع والبيئة التي تنتمي إليها الجريمة، فظهرت العديد من التعريفات المتعلقة مرة بالجانب التقني ومرة أخرى بالجانب القانوني، ولتحديد المفهوم الأساسي والرئيسي للجريمة المعلوماتية ظهرت طائفتين أو اتجاهان:

- طائفة لتعريفات القائمة على معيار واحد، وهو قانوني وتتناول فيه كل من السلوك محل التجريم الوسيلة المستخدمة وموضوع الجريمة.
- طائفة التعريفات القائمة على النمط لكن هذه الطائفة تتمحور تعريفاتها بالتطور التاريخي الذي مرت به جرائم المعلوماتية ذات التقنية العالمية منذ ظهور الحاسوب كاختراع حديث أحدث ثورة في مجال المعلوماتية.[1]

الفرع الأول: مفهوم جريمة النصب الإلكتروني

يحكم قانون العقوبات مبدأين أساسيين أولتها شرعية العقوبات التي تعرض انتقاء العقاب عند انتقاء النص، وثانيتها خطرا القياس في النصوص التجريمية الموضوعية:

وهنا ظهر الفراغ التشريعي في وضع تعريف قانوني يليق بنوع هذه الجرائم وبيان عناصرها وإثبات حجيتها، ومن هنا يجب التمييز بين الظاهرة الإجرامية والجريمة، ووفقاً لما سبق تعريف الجرائم المعلوماتية على أنّها:" الأفعال غير المشروعة المرتبطة بنظم الحاسوب"، أمّا النص القانوني لجريمة النصب التقليدية" الاستيلاء على حيازة مال الغير كاملة بوسيلة يشويها الخداع تسفر عن تسليم ذلك المال" حيث تنص المادة 372 قانون العقوبات: "كل من توصل إلى استلام أو تلقي أموال أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الالتزامات أو الحصول على أي منها أو شرع فيها وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إمّا

[1] – عبد الفتاح بيومي حجازي، الكتاب الثاني، المرجع السابق، ص ص: 460-461.

باستعمال أسماء أو صفات كاذبة أو سلطة حالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء منها يعاقب بالحبس". [1]

وعرّفه بعض الفقه بأنه: " الاستيلاء بطريقة الاحتيال على شيء مملوك للغير بنية التملك".

- أمّا المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم وتواريهم لذلك من الصعب جدا ملاحقتهم والقبض عليهم.

الفرع الثاني: نطاق جريمة النصب الإلكتروني

تستخدم عدة أساليب لارتكاب الجريمة الإلكترونية، وتكون معدات الحاسوب المادية موضوعاً لها وقد تمس هذه الجرائم أموالاً خاصة بالأفراد كما قد تمس أموالا خاصة بالدولة إلا أنّها تعد وسائل تقليدية وهي: [2]

تدمير الدعامات التي تحتويها سواء بإحراقها أو تفجيرها باستخدام القنابل المتفجرة أو سكب سوائل ساخنة على الأجزاء الحساسة من الحاسب، أو إلقاء رماد السجائر المشتعلة على الشرائط والأسطوانات الممغنطة وهذه الأساليب لا تتطلب سوى معرفة فنية متواضعة تتمثل في مجرد سلوك مادي بالنتيجة الاطلاع البصري للمعلومات التي تظهر على شاشة الحاسب، أو القيام بالتنصيب عليها في حالة تجسيدها في صورة سمعية أو عن طريق الاستعانة بوسيط يعمل على تكبير الصوت الصادر من الحاسب، ومن هنا يحصل الجاني على ما يريده بطريق مباشر.

أمّا الأساليب عالية التقنية والتي تتطلب معرفة فنية بالحاسوب حيث يقوم فيها المجرم الإلكتروني بما يسمى" عملية السطو المسلح الإلكتروني"، يكون الهدف من هذه العملية

[1] – القانون رقم06-23 المؤرخ في 20ديسمبر 2006،ص 136.

[2] – عبد الفتاح بيومي حجازي ، المرجع السابق، ص 465.

التقاط أو تسجيل المعلومات والبيانات المعالجة إلكترونيا، وهي في مرحلة الانتقال والبث من الحاسب بواسطة أجهزة شبكة الاتصالات البعيدة" **limatique**" والمعالجة عن بعد "**télétraitement** " كما يمكن عرض بعض الوسائل فيما يلي:

1- التقاط المعلومات التي توجد ما بين الحاسب والنهاية الطرفية:

يحدث هذا الالتقاط بواسطة توصيل خط تحويل يعمل على تكبير الذبذبات الإلكترونية، وإرسالها إلى نهاية الطرفية التي تقوم بعملية التجسس ومن الممكن أن يحدث أيضا باستخدام جهاز المرسل صغير نقل البيانات عن بعد ويمكن الالتقاط.

كذلك عن طريق وضع هوائيات مطاردة بالقرب من الهوائيات الاحتياطية، و بالتالي يحدث التقاط الإشعاعات العابرة عن طريق النقل الجوي للمعلومات عند بثها بالقمر احتجاز مضمونها. [1]

2- التوصيل المباشر بواسطة خط تليفوني:

يتم ذلك بوضع مركز تصنت يجعل من تسجيل الاتصالات أمراً يسيراً كما يمكن الاستعانة أيضاً بوضع ميكروبات صغيرة لأدائها.

التقاط الإشعاعات الصادرة عن الجهاز المعلوماتي:

تمكن خطورة هذه الوسيلة في أنّها يمكن أن تؤدي إلى إعادة تكوين خصائص المعلومات التي تبث وتنقل من خلال الأنظمة المعلوماتية، وهذا الجناح تسجيل الإشعاعات الصادرة عن الحاسب كما لا يحتاج إلى حل شفراتها.

[1] - عبد الفتاح بيومي حجازي ، المرجع السابق، ص 468.

الفرع الثالث: أركان جريمة النصب الإلكتروني

تقوم جريمة النصب الإلكتروني على ركنين، ركن مادي وكن معنوي هما: [1]

أ- الركن المادي:

يتمثل في سلوك إرادي يترتب عليه نتيجة إجرامية تربطها بالسلوك الإجرامي رابطة سيئة مادية هذا هو الركن المادي في جريمة الانترنت وباستقرائنا للتعريف نستنتج أن يتكون من سلوك إرادي ونتيجة إجرامية ورابطة سيئة.

1- سلوك إجرامي:

يعتبر السلوك المادي عبر الانترنت محلا للتساؤل، لاسيما ما يتعلق ببدائية أو الشروع في ارتكاب الجريمة عبر الانترنت يحتاج بالضرورة إلى منطق تقني.

ومن أمثلة السلوك المادي في الجريمة عبر الانترنت، ثم المصرفي الذي ينوي سرقة مبلغ من المصرف الذي يعمل فيه باستخدام الانترنت، ثم الدخول إلى شبكة المصرف عبر مزودات مجهولة يمكن الاستعانة من خلالها ببرمجيات اختراق موضوعية على موقع يتم تحديدها باستمرار في هذا المثال فإن المصرفي المذكور يمارس النشاط المادي للاختلاس عن طريق الحاسوب والانترنت.

2- النتيجة الإجرامية:

يعد هذا العنصر أحد عناصر الركن المادي في الجريمة إلى جوار السلوك الإجرامي وعلاقته السببية، وتثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة أهمها تحديد هل الجريمة المرتكبة سلوك ونتيجة في العالم الافتراضي أم أن هناك امتداد للنتيجة ليتحقق منتهاها في العالم المادي؟[2]

3- العلاقة السببية:

[1] - عبد الفتاح بيومي حجازي ، المرجع السابق ،ص 468.

[2] - عبد الفتاح بيومي حجازي ، المرجع السابق ،ص 469.

هي العنصر الثالث من العناصر التي يتكون منها الركن المادي في الجريمة الإلكترونية، حيث تحدث باستعمال الانترنت وذلك حسب الأحوال في العالم الافتراضي وإن كان النشاط المادي كله يحدث في العالم الافتراضي وكذا العلاقة السببية، فإن النتيجة الإجرامية لها كيان منفصل لكونها تحدث بشكل انقسامي ما بين حدوثها في العالم جزئياً أو كلياً، ومن أهم الآثار المترتبة عنها تؤثر على قواعد الاختصاص في الدول كما أن جرائم الانترنت تنتشر فيها الفيروسات بقصد القرصنة، لأن ذلك يعتبر نتيجة محتملة تشمل الجريمة التي ليس لها منحنى إطلاقا أي حالة التي يكون فيها للضحية وجود مادي وإنما رقمي فقط. [1]

ب- الركن المعنوي:

يتعلق بشخصية الجاني وبمسلكه الذهني والنفسي كما للركن المعنوي ثلاث صور في الجرائم المتعلقة وهذه الصور هي:

1- العمد:

ينبغي لارتكاب الجريمة الإلكترونية أن يكون مرتكبها مكتسبا من المعرفة والتعليم التخصصي ليتمكن من ممارسة هذا النوع من وسائل الاتصال وفي هذه الحالة يكون وقوعها في صورة واحدة وهي صورة العمد حيث أن المجرم الإلكتروني يكون قد خطط ودبر لارتكاب هذه الجريمة سواء من أجل الحصول على المعلومة أو لاختراق شبكة حاسوب شخص آخر كجريمة النصب تتطلب من الفاعل إرادة ارتكاب السلوك تحقيق نتيجة ويكون القصد عاماً أو خاصاً. [2]

2- القصد المتعدي:

يتوفر القصد المعتدي في جرائم الانترنت في الحالة التي يتجاوز فيها قصد الشخص الهدف الذي كان يسعى لتحقيقه مثلا: إذا كان القصد مجر اللهو في مسارات القطارات،

[1] - هدى حامد قشقوش، المرجع السابق، ص 129.

[2] - هدى حامد قشقوش، المرجع نفسه ،ص 130.

فيتعدى الأمر ذلك إلى تدمير بيانات تحريك القطارات عبر الحاسوب وتكون النتيجة حدوث خسائر مادية وبشرية، وبهذا يتعدى النتيجة الهدف الذي كان يصبو إليه محترف الكمبيوتر فيصبح مجرم في أجهزة الحاسب الآلي إلى مجرم إلكتروني.

3- الخطأ غير العمدي:

يحتل الخطأ مرئية هامة في الركن المعنوي في جرائم الانترنت، إذا أن معظم جرائم الانترنت تؤدي إلى تدمير أجهزة المؤسسة لإفراط الموظف المسؤول في استدام حاسوبا بدلا من حاسوباً به الخاص في العمل على حساب الخاص ناسياً متاعب الفيروسات ومعتمداً فقط على مهاراته في تجنبها دون إدراج برامج القضاء على الفيروسات أو محاربتها في الكمبيوتر أو ينقل الفيروسات من القرص المرن إلى أجهزة المؤسسة فتشكل تدميراً كليا أو جزئياً المعلومات أو البيانات بالأخص إذ تنقل فيروس إلى شبكة أو نظام حاسوب لمؤسسة مالية أو فيدرالية.[1]

[1] - هدى قشقوش، المرجع السابق، ص 131.

ملخص الفصل الأول

مع ظهور الحاسب والانترنت إلى مجتمعاتها وفي كافة جوانب حياتنا بدأ يظهر نوع جديد من الجرائم تسمى الجرائم الإلكترونية، وذلك لأنها تمثل حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم وغيرها من الأهداف التي تكون غالبا الضحية لها إلاّ أنه وبالرغم من كونها الوسيلة لارتكاب الجرائم إلى جانب الحاسب الآلي، فإنها كذلك لن تنجو من يد المجرمين لأنها هي الأخرى قد تكون محلا للاعتداءات، حيث صنف الفقهاء والدارسون الجرائم الإلكترونية ضمن فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم فبعضهم يقسمها إلى جرائم ترتكب عن نضم الحاسب الآلي، وأخرى ترتكب بواسطته وبعضهم يصنفها ضمن فئات بالاستناد إلى الأسلوب المتبع في الجريمة فتتنوع الجرائم الإلكترونية حسب هذا التقسيم إلى جرائم تقع على الأموال وجرائم تقع على الأشخاص وهناك أيضا جرائم النصب الإلكتروني، حيث تتطلب هذه الجرائم أن يكون الشخص خبيراً بالقدر اللازم بأمور الحوسبة، لذلك نجد الشرطة تبحث أولاً عن خبراء الكمبيوتر عند ارتكاب هذا النوع من الجرائم.

الفصل الثاني

دور القاضي في حماية وسائل التجارة الإلكترونية وطرق مواجهتها الأمنية

الفصل الثاني: دور القاضي في حماية وسائل التجارة الإلكترونية وطرق مواجهتها الأمنية

لقد عرفت المجتمعات الإنسانية جرائم مختلفة واجهتها بأساليب متعددة ومتنوعة، ولكن التطور التقني الذي نلمسه والمتمثل في أحد صوره استخدام الحاسب الآلي ونظم المعلومات أدى إلى ظهور جرائم لمن تكن معروفة في السابق.

لذا فهي كثيراً ما يطلق عليها بالجرائم المستحدثة، والتي تحتاج إلى تشريعات خاصة، حيث أن الغزو المعلوماتي الكبير الذي عرفته الأموال الإلكترونية من طرف النوابغ المعلوماتية والتي تتضمن الوسائل الوقائية والوسائل الردعية، حيث تكون الوقائية مجرد أنظمة متصلة بالكمبيوتر تعطي لمستخدم الحاسب الأمان لإرسال الرسائل الإلكترونية، إلاّ أن هذه الوسائل تعرضت للغزو، فظهرت بذلك وسائل ردعية أكثر صرامة من سابقتها تمثل في التشريعات والتنظيمات الداخلية حيث يتم معاقبة المجرمين المعلوماتين جنائياً، وسبل مكافحتهم قانونياً.

المبحث الأول: الطرق الوقائية

وضع المشرع طرق وقائية تسمع لمستخدم الانترنت استعماله كتقنية بأمان تام، حيث تتم إرسال الرسائل الإلكترونية وتلقيها بسرية تامة، تمكن المرسل والمرسل إليه، معرفة محتوى الرسالة دون طرف ثالث متطفل على سبيل المثال تشفير البيانات والتوقيع الإلكتروني.

المطلب الأول: تشفير البيانات

يعُد التشفير من الطرق الوقائية لحماية الأموال الإلكترونية ووسائل حفظ سرية المعلومات في نطاق الأنظمة الإلكترونية، ويهدف إلى منع الغير من التقاط الرسائل أو المعلومات، ومن ثم منع وسائل مشوهة إلى الطرق الأخرى من المعاملة التجارية، والذي يقوم بدوره بتحويل الرسالة إلى شكلها الأوّل.[1]

الفرع الأول: تعريف التشفير الإلكتروني وأهمية

أولاً: تعريف التشفير:

إن تعميقنا في معنى التشفير نجد أن عملية حجب المعلومات حيث لا يتم اللجوء للتشفير لجزء التشفير، وإنما قصد حجب المعلومة على التداول، فهو منهج وليس له موضوع ذاتي حيث يتم حصر المعلومة بين شخصين دون طرف ثالث متطفل ويعرّف بأنه:" **مناهج لخط البيانات من خلال لوغاريتمات أو خوارزميات، بحيث لا يمكن قراءتها من خلال طرف ثالث متطفل**".

فالتشفير هو علم تحويل الكتابة إلى أسرار، حيث لا يمكن لطرف ثالث الدخول للموقع دون تصريح المالك، ولذلك باستخدام مفتاح إزالة التشفير، ويتم التمييز بين نص المشفر والنص العادي في التسمية، حيث يطلق على النص العادي اسم النص الكامل أمّا المعلومة التي يتم تشفيرها يطلق عليها اسم النص المشفر، ويستخدم في التشفير أساليب رياضية يطلق عليها مصطلح **خوارزميات التخفي** والذي بدوره يحتاج لمفتاح التشفير، وأخر لفك التشفير معروفا في الخمسينات في المجال العسكري، حيث كان يستعمل لإخفاء المعلومات أثناء الاتصال بين الحكومة والجيش وقت الحروب، أمّا في الستينات فقد توجه

[1] – محمد أبو بكر بن يونس، الأحكام الموضوعية والجوانب الإجرامية، الجرائم الناشئة عند استخدام الانترنت، دار النهضة العربية، بدون طبعة، سنة 2004، ص ،ص379-380.

التشفير نحو الحركة الصناعية، وفي السبعينات أخذت به المصارف، وفي الثمانينات دخل التشفير للهاتف ليشفر في نهاية القرن العشرين في التجارة الإلكترونية.[1]

أمّا التشفير قداسة المعلومة فيستخدم لأمان المعلومات عند إرسالها في العالم الافتراضي فلا يعتدل موضوعها أو يحذف منه وهذا مشهور بكثرة في بث النصوص القانونية والبحوث وكتب الأديان له وأخبار الصحافة وكل موضوع فيه حساسية شديدة وكل موضوع فيه حساسية شديدة عبر الانترنت، أما التشفير المتعلق بأصالة المعلومات فيستخدم في استمرار المعلومة بحيث تدل على المرسل والمرسل إليه، كما لا يستطيع المرسل إنكار إرساله لها، عرف مجلس الدولة الفرنسي التشفير على أنّه إخفاء المعلومات وعرّف الإخفاء بأنه:" كل عمل يوجه لتحويل بمساعدة مصطلحات سريّة معلومات إشارات غير مفهومة للغير أو بإخراجها بعملية معكوسة، بفضل وسائل مادية أو برمجية مصممة لذلك".[2]

ثانيا: أهميته

يعين التشفير كأحد موضوعات الانترنت في الفترة المعاصرة حيث تباينت الآراء الأول بين مؤيد ومعارض كتقنية برمجية فالدول مازالت في صراع بين الإبقاء عليه رفضه وعزل وإبقاء في هذه المنطقة الوسطى بين القبول والرفض يعطي للتشريع دورا حيوياً كاملاً حيث يصبح له كامل الصلاحية في الفعل في هذا الشأن وللتشفير وجوانب سلبية كماله من الجوانب الإيجابية حيث يستخدم في التجارة الإلكترونية، بما فيها رسائل سرية وعروض خدمات وحركة تبادل الأموال كي لا تكون عرضه للنهب والاستيلاء من طرف المجرمين المعلوماتين وذلك يعطي لنا جانبين سلبيين أولهما هو تمكن هؤلاء النوابغ الإلكترونية من فك شفرات ومعرفة المعلومات المرسلة، أمّا الجانب السلبي الثاني فيمكن في صعوبة استطلاع الحركة المالية للمؤسسات الاقتصادية حيث لعب التشفير دوراً ممتاز في التهرب الضريبي في

[1] – نفس المرجع، ص –ص 383 – 386.

[2] – محمد أبو بكر بن يونس، المرجع السابق، ص 387.

العالم الافتراضي كون العالم المادي كان يفترض قاعدة الاستثمار التي تقضي بفرض الضرائب على المعاملات المالية، وبالتالي يمكن لشركة وطنية إعداد صفقات عبر الانترنت باستخدام قاعدة التشفير، دون علم الدولة، بذلك وهذا ما يجعل المؤسسات الضريبية أقوى أعداء برمجيات التشفير، ومن هنا يمكننا القول بأنه لا مجال أمام المشرع سوى إدراج إنشاء حيث أعطى المؤسسات الدولة الحق في انتهاك حرمة التشفير خروجاً على القاعدة العامة لحرمة المرسلات. [1]

إلاّ أنّه وقبل كل شيء يبقى التشفير تقنية برمجية، والتقنية في تطور مستمر، وكلما أمكن للدولة اختراقه كلما قام المستفيد من تطويره لوضع العراقيل أمامها.

على غرار البرمجيات يمكن استخدام آلات وقطع صلبة خصيصا لتشفير فقد قامت حكومة الولايات المتحدة الأمريكية بتصميم هذا النوع عام 1993 تسمح للسلطات بالحصول على مفتاح التشفير لممارسة الرقابة على حركة المراسلات المشفرة وذلك بتركيب رقاقة في كل فاكس أو هاتف أو مودم ، إلاّ أنها عورضت من قبل حركة الحريات، فعدلت الحكومة مشروعها في 1996 فاستحدث مصطلح مفتاح التغطية، حيث سمحت الحكومة بتقنية التشفير شرط الحصول على نسخة المفتاح وعدم إتباع هذا الشرط بقيد جريمة قائمة بذاتها. بالإضافة إلى ما تقوم به المنظمات بما فيها الإجرامية والإرهابية حيث تقوم الأولى بتشفير المعلومات التي تتضمن المؤثرات العقلية وكيفية إعداد وإنتاج المخدرات وتحديد الجرعات ومواعيد تعاطيها وهذا يعدّ جانباً سلبياً للتشفير. [2]

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص361-370.

[2] – عمر محمد أبو بكر بن يونس، نفس المرجع، ص 388.

الفرع الثاني: صور التشفير الإلكتروني

التشفير صورتين هما:

1- التشفير كغطاء لارتكاب الجريمة:

يلعب التشفير دوراً كبيراً في عالم الانترنت أو ما يعتبر عنه بالعالم الافتراضي، فهو من أنواع الحماية الوقائية لعدد من المعلومات المتداولة عبر الانترنت إلاّ أن موضوع التشفير ذاته طرح العديد من التساؤلات وبالتالي لقي اهتماما فقهيا وتشريعيا كبيرا حيث أن جل توابع المعلوماتية يمارسون عدوانا على الموقع إمّا لكشف المعلومات المشفرة أو لكسر الشفرة ذاتها وهنا يجب التمييز بين نوعين من العدوان الأول على المعلومات والثاني بهدف كسر الشفرة، يؤخذ عين الاعتبار في تحديد العقوبة من حيث التشديد وذلك أنّ هذا العدوان عرضه الأول تغطية الأنشطة الإجرامية، وهو في نفس الوقت عقبة كبيرة تواجه منظمات البحث الجنائي وهنا يجب على المشرع تدارك هذا الفرع بشأن القضايا التي يتم فيها كسر الشفرة ثم الولوج إلى المعلومات وهذا يأخذ طابع التشديد.[1]

2- التشفير كوسيلة لإعاقة الحصول على أدلة:

للتشفير عدة أهداف قد تكون ظاهرة وقد تكون خفية، أو يمكننا القول أن خلف الأهداف هناك الهدف الظاهر للحكومة والهدف التضليلي أو الخفي وهو الذي يقصده الشخص، وقد يكون القصد من التشفير إخفاء أدلة التي تمكن من الإدانة في جريمة سواء تقليدية أو جريمة تقنية كما هو الحال في جرائم المخدرات الاتجار بالرقيق البيض، والأطفال والدعارة والإرهاب ويعتبر أخطر نوع من وسائل التشفير هو الذي يرتكب للعدوان على حقوق الملكية الفكرية حيث يصعب على الجهات القضائية فك هذه الشفرات وبالتالي صعوبة الحكم بالإدانة وذلك من حيث.

[1] - نفس المرجع السابق، ص ص: 388- 389.

- تفسير وتحليل الملفات والسجلات المعالجة آليا المخزنة والتي يتم التوصل إليها بمقتضى أمر قضائي أو بإحدى الإجراءات المناسبة.
- تنفيذ أمر قضائي بالمراقبة.

إلاّ أنّه رغم وجود الرقابة التي تمارسها الجهات القضائية إلاّ أنّها تعُّد محليا للطعن فيها لصعوبة إثباتها. [1]

[1] – محمد أبو بكر بن يونس، المرجع السابق ، ص 390.

المطلب الثاني: الوسائل الردعية

بعد التعرض للطرق الوقائية وبالنظر إلى أنّ هذه الوسائل أيضا أصبحت عرضة للغزو المعلوماتي حيث أصبح هذا الأخير موجها ضد الوسيلة، ولهذا فإن هذه التقنية أيضا أصبحت بحاجة إلى حماية قانونية، وبالتالي لم يجد المشرع بدلاً من إصدار تشريعات لمواجهة هذا الهجوم المعلوماتي من طرف نوابغ المعلوماتية وهذه الطرق الردعية تمكن السلطات من متابعة ومراقبة هذه الانتهاكات ومعاقبتهم جنائيا.

الفرع الأول: المعطيات الأساسية للجريمة المعلوماتية ومراقبة الاتصال

يتضمن الأمر 09- 04[1] جل القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وسبل مكافحتها قانونياً، وذلك لتجريم أفعال التوابع المعلوماتية من اختراقات المواقع وجل أعمال التخريب الإلكتروني.

أحكام عامة:

يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ويقصد في مفهوم هذا القانون بما يأتي: [2]

أ- الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال:

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام اتصالات الكتروني.

---

[1] - الأمر رقم 09-04 المؤرخ في 14شعبان 1430الموافق لـ 08/25/ 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ومكافحتها، لجريدة الرسمية رقم47 الصادرة بتاريخ 05 /2009/8.

[2] - أنظر المادة 01و02و03 من الأمر السابق ص ص : 6-5.

ب– منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض، أو المرتبطة أو المتصلة ببعضها البعض، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذاً لبرنامج معين.

ج– معطيات معلوماتية:

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

د– مقدمو الخدمات:

1– أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

2– أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعمليها.

هـ– المعطيات المتعلقة بحركة السير:

أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال ونوع الخدمة.

و– الاتصالات الإلكترونية:

أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات الحماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

الفرع الثاني: مراقبة الاتصالات الإلكترونية

يمكن القيام بعمليات المراقبة المنصوص عليها في المادة الثالثة في الحالات الآتية:[1]

أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر المعلومات عن احتمال اعتداد على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، أو الاقتصاد الوطني.

ج- لمقتضيات التحريات و التحقيقات القضائية عند ما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ طلبات المساعدة القضائية المتبادلة.

- لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

- عندما يتعلق الأمر بالحالة المنصوص عليها في الفقرة" أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 من هذا القانون إذن لمدة ستة أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

- تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة " أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة مكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

[1] - أنظر المادة 04 من الأمر السابق ص 06

المطلب الثالث: القواعد الإجرائية والتزامات مقدمي الخدمات

يتضمن هذا المطلب القواعد الإجرائية في تفتيش المنظومات المعلوماتية والتزامات مقدمي الخدمات بمساعدة السلطات حيث يتضمن الأول حجز المعطيات المعلوماتية الحجز عن طريق منع الوصول إلى المعطيات المحجوزة ذات المحتوى المجرم حدود استعمال المعطيات المتحصل عليها أمّا الثاني فيتضمن حفظ المعطيات المتعلقة بحركة السير والالتزامات الخاصة بمقدمي خدمة "الانترنت".[1]

الفرع الأول: القواعد الإجرائية لتفتيش المنظومة المعلوماتية

يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة الرابعة، الدخول بفرض التفتيش، ولو عن بعد إلى:[2]

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية.

- وفي الحالة المنصوص في الفقرة "أ" من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا لذلك.

- إذا تبين مسبقا بأن المعطيات المبحوث عنها و التي يمكن الدخول إليها انطلاقاً من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية طبقا للاتفاقيات الدولية ذات الصلة وفقاً لمبدأ المعاملة بالمثل.

---

[1] - الجريدة الرسمية رقم 47، قانون رقم 09-04.

[2] - أنظر المادة 5و 6و 7 من الأمر السابق، ص 06.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومة الضرورية لإنجاز مهمتها.

عندما تكشف السلطة التي تباشر التفتيش في المنظومة المعلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنّه ليس من الضروري حجز كل منظومة يتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية قابلة للحجز والوضع في إحراز وفقاً للقواعد المقررة في قانون الإجراءات الجزائية يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، غير أن يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أنّ لا يؤدي ذلك إلى المساس بمحتوى المعطيات إذا استحال إجراء الحجز وفقاً لما هو منصوص عليه في المادة السادسة لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

يمكن للسلطة أن تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلاّ في الحدود الضرورية للتحريات أو للتحقيقات القضائية.[1]

[1] – أنظر المواد 8-9 الأمر السابق 09-04، ص 07.

الفرع الثاني: التزامات مقدمي الخدمات بمساعدة السلطات

في إطار تطبيق أحكام هذا القانون [1] يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها ويوضع المعطيات التي يتعين عليهم حفظها وفقاً للمادة الحادية عشر، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان على سرية المعلومات التي ينجزونها من المحققين وكذا المعلومات المتصلة بها تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق مع مراعاة طبيعة ونوعية الخدمات التي يلتزم بها مقدمو الخدمات بحفظ:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج- الخصائص التقنية و كذا تاريخ ووقت ومدة كل اتصال .

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة أو مقدميها.

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف، يقوم التعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه تحدد مدة حفظ المعطيات المذكورة بنسبة واحدة ابتداءا من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة ، تقوم المسؤولية الجزائية للأشخاص الطبعين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية.

[1] - أنظر المواد 10-11-12، ص 07-08.

ويعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات وبغرامة مالية من 50000دج إلى 500000دج.

يعاقب الشخص المعنوي بالغرامة وفقاً للقواعد المقررة في قانون العقوبات تحديد كيفيات تطبيق الفقرات1-2-3 من هذه المادة، عند الحاجة، عن طريق التنظيم.

زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه، يتعين على مقدمي الخدمات " الانترنت":

أ- التدخل الفوري لسحب المحتويات التي يحتاجونه الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى موزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة، وإخبار المشتركين لديهم بوجودها.[1]

[1] - أنظر المواد 1-2-3-11، من الأمر السابق، ص 09.

المبحث الثاني: دور السلطات الضبطية القضائية في كشف الجرائم الإلكتروني

شبكة المعلوماتية قد تكون موضوعاً لبعض جرائم الأموال كالسرقة والإتلاف العمدي، وقد تكون هذه الشبكات وسيلة لارتكاب بعض الجرائم، وغالبا ما تقع على جريمة السرقة أو الإتلاف العمدي على أجهزة الحاسب الآلي وملحقاتها من شاشات وطابعات وشرائط ومعدات وكابلات، وكذلك البرامج الموجودة على دعامات، ولكن قد تقع هذه الجريمة على بيانات غير مادية، وفي هذه الحالة قد تكون الجريمة قد تمت عن طريق الحاسب الآلي، ويصبح هو الوسيلة لارتكابها.[1]

وتأتي الولايات المتحدة الأمريكية في مقدمة الدول التي واجهت الجرائم المعلوماتية وذلك بالنص على مواجهتها تشريعيا بإنشاء إدارة لمتابعة الجرائم المعلوماتية، بمكتب التحقيقات الفيدرالي (FBI)[2]، الذي يضم داخله مجموعة من الأشخاص المدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتم تحصيله من أدلة.

[1] – أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، القاهرة، سنة 2000،ص 1950

[2] – مصطلح (FBI) هو اختصار لـ(Fédéral – Bureau- Investigation)

المطلب الأول: طرق كشف التعديل والتلاعب في البرامج

هناك أوجه أخرى أو جرائم متعددة تقع باستخدام الحاسب الآلي كأداة إيجابية، منها التدخل في المعطيات أو البيانات المقدمة للحاسب الآلي من أجل معالجتها، والأساليب التي يتخذها الجاني من خلال التدخل في المعطيات تتمثل في إدخال معطيات وهمية أو في تزوير المعطيات المخزنة، كذلك فإن المنطقي للحاسب الآلي، والكيان المنطقي هو عبارة عن مجموع البرامج المخصصة للقيام بالمعالجة عن طريق الحاسب الآلي.[1]

الفرع الأول: التعديل والتلاعب في البرامج

الطرق الاحتيالية هي كل كذب مصحوب بوقائع خارجية، أو أفعال مادية يترتب عليها توليد الاعتقاد لدى المجني عليه بصدق هذا الكذب، مما يدفعه إلى تسليم ما يراد منه تسليمه طواعية واختيار إلى الجاني.

والتلاعب المعلوماتي هو التلاعب بالبرامج والبيانات للتغيير منها بما يترتب عليه اعتقاد المجني عليه بصحتها بما يجعله يسلم بها، ويمكن تعبير النص المتعلق بالطرق الاحتيالية على التلاعب المعلوماتي لشكل أحد أساليب الاحتيال.

والمعطيات أو البيانات التي تتم جريمة التعديل أو التلاعب فيها داخل جهاز الحاسب الآلي تنقسم إلى نوعين:[2]

أولا: إدخال معطيات وهمية.

يقوم جهاز الحاسب الآلي بتخزين أي معلومات يقدمها له الإنسان، فإذا ما قدمت إليه معلومات خاطئة فإنه يقوم بحفظها وطبعها وإخراجها كما هي خاطئة.

[1] – هدى حامد قشقوش، المرجع السابق، ص 197.

[2] – جميل عبد الباقي، المرجع نفسه، ص 180.

ثانيا: تزوير المعطيات الموجودة:

هناك صورتين لتزويد المعطيات الموجودة

أ- استبدال المعطيات:

يحسب أجر العاملين في بعض الشركات على أساس عدد الساعات التي يقضونها في العمل فعلياً، ويوجد لكل عامل بطاقة بها اسمه ورقم قيده، ولكن تحديد ساعات العمل التي أديت بالفعل يتم عن طريق إدخال البطاقة التي يحملها العامل جهاز الحاسب الآلي عند دخوله إلى مقر عمله، وعند انصرافه منه، والغش يتم هنا بقيام المسؤول عن الحاسب الآلي باستبدال رقم القيد الخاص بأحد زملائه، والذي سبق أن أدى ساعات عمل أكثر منه ومثل هذا الغش لا يمكن ضبطه لأن التغيير الذي تم داخل الجهاز لا يمكن كشفه، لأنه لا يوجد له أثر في ملفه الخارجي حيث لا تُدَوَنْ فيه ساعات العمل التي أديت بالفعل.

ب- المحو المنتقى للمعلومات:

في هذه الصورة الإجرامية، قام بعض المسئولين بالاستيلاء على مبلغ 61000 دولار كان قد أرسل إلى إحدى شركات التأمين لصالح أحد المراكز الطبية، وقاموا بفتح حسابات وهمية خاصة بهم ووضعوا فيها المبلغ[1].

ولكي تتم هذه العملية بنجاح قام المسئولين "**بمحو**" حسابات من سجلات الحاسب الآلي للمركز الطبي وهي حسابات المتوفين، وذلك إمّا يجعلها غير قابلة للتحصيل، أو بمعنى أدق أنّه لا يمكن تحصيلها إلاّ بإجراءات معينة ومعقدة ، وإمّا بحذفها من السجلات أو الملفات، وقد استخدم هذا الأسلوب في صندوق المعاشات الألمانية، فقد لاحظت الحكومة أن عدداً غير قليل من المحالين للمعاش يختفي خلال فترة الصيف، وتفسير ذلك أنه بمجرد التبليغ عن حالات الوفاة، فإن المختصين المسئولون عن نظام المعاشات يقومون بتغيير عناوين المتوفين حتى لا يمكن استدعاؤهم إلى الإدارة الخاصة بالمراقبة، وبالتالي

[1] - جميل عبد الباقي الصغير، المرجع السابق، ص 180.

يقوم المسئولون على نظام المعاشات بتوجيه الشيكات الخاصة بالمحالين إلى المعاش إلى حساباتهم الشخصية، وبتغير عناوين المحالين إلى المعاش فإنه لا يمكن استدعائهم إلى الإدارة الخاصة بالمراقبة وهنا يجب على الأجهزة الأمنية مأموري الضبطية القضائية الاستعانة بذوي الخبرة في مجال الحاسب الآلي للكشف عن أي تعديل أو تلاعب، قد يقع على الآلية وذلك من خلال قدرتهم على فحص الأجهزة محل التلاعب بالطرق الفنية، ليسهل عليهم الحصول على الأدلة المناسبة، ومواجهة المتهم بالبيانات والمعلومات التي حصلوا عليها عن طريق الخبير، لكن ومع هذا لا يكتفي جهاز الضبطية القضائية الاستعانة بذوي الخبرة فقط، بل يجب عليه أن يطور خبرته بعلوم الحاسب الآلي، ليستطيع تكوين خلفية قانونية عن الجريمة، وبالتالي يسهل التعامل مع مرتكبيها.[1]

الفرع الثاني: خلق أو إعداد برنامج وهمي أو ناقص من الناحية الفنية

في هذا الفرع هناك صورتين من صور الجرائم التي تقع باستخدام الحاسب الآلي كأداة إيجابية.

أولا: خلق برنامج وهي بأكمله:[2]

الجاني في هذه الصورة الإجرامية يصمم برنامجاً بأكمله من أجل ارتكاب جريمته، مثل ما حدث في أمريكا حيث قامت إحدى الشركات الأمريكية عن طريق الحاسب الآلي الخاص بها، قامت باصطناع وثائق تأمين لأشخاص وهميين بلغ عددها 64000 وثيقة، وإمعانا في التمويه زودت الوثائق بتغيرات في العناوين، والأوضاع الاجتماعية، مع اعتبار أن بعض المؤمن عليهم أموات، بعد ذلك قامت الشركة ببيع هذه الوثائق لأشخاص آخرين، وحصلت في المقابل على عمولات من شركات التأمين التي تعمل لحسابها والتي بلغت قيمتها 200مليون دولار، ولضمان نجاح العملية قام الجناة بوضع شفرة خاصة في البرنامج،

[1] - Aup CLE(N) les infraction , h 33 , P23

[2] - مدحت عبد الحليم رمضان، المرجع السابق، ص 200.

تمت برمجته بدقة تامة، بحيث لا يظهر في الطباعة إلاّ الوثائق السليمة تماماً، وبالتالي لا يتمكن المراقبون الماليون الذين يعملون بالشركة الذي دفعت العمولات عن اكتشاف الوثائق الوهمية.

ثانيا: إعداد برنامج ناقص من الناحية الفنية

هنا يقوم الجاني بإدخال فجوات في برنامج الحاسب الآلي، ذلك أن المجرمين حينما يقومون بإعداد برنامج للحاسب الآلي فإنهم يتركون فواصل في البرنامج حتى يستطيعون تنفيذ التعديلات المطلوبة والضرورية بإدخال شفرات إضافية أو إحداث مخارج وسيطة، وإذا كان من المفروض أن تنزع هذه الفجوات عند الانتهاء من البرمجة، إلاّ أنّه كثيرا ما يضعها المبرمج من أجل استخدامها فيما بعد عن طريق الغش خاصة بالنسبة للبرامج الكبرى المعقدة بسبب عدم إتقان التصميم، وبالتالي تكون فرصة يستطيع أن يتدخل من خلالها الجاني ويخفي تعليماته، بحيث يتعذر على المراقبة الداخلية للحاسب الآلي معرفة، وقد ما يدور، وقد حاول الفقه والقضاء في معظم النظم القانوني للدول المتقدمة خاصة في مجال الحاسب الآلي، تطويع النصوص التشريعية المطبقة لديها، في محاولة لمد سريانها على النوع الجديد من الجرائم خاصة في مجال جرائم الأموال، لذلك فإن المشرع في هذه الدول يتدخل لوضع نصوص عقابية جديدة لمواجهة الجرائم المختلفة والجديدة الناشئة عن استخدام الحاسب الآلي.[1]

[1] – المرجع السابق، ص 201.

المطلب الثاني: أهمية التفتيش في الكشف عن جرائم التجارة الإلكترونية.

الغرض من التفتيش التي تقوم به الأجهزة الأمنية، ألاّ وهو ضبط الأشياء التي تفيد في ظهور الحقيقة، وإثبات الجريمة التي تم ارتكابها، ثم تقديم المجرم إلى العدالة.

والضبط في معظم الأحوال يكون هو الغرض الأساسي من التفتيش، وإن لم يكن هو السبب الوحيد له، فقد يتم الضبط لأسباب أخرى، والضبط لا يخرج عن كونه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها، وعن مرتكبها سواء كان هذا الشيء عقار أو منقولاً.

والضبط بهذا المعنى لا يرد الأشياء فقط بالرغم من أن المشرع قد استخدمه في التعبير عن القبض على الأشخاص أحياناً، كما أنه لا ينصب كذلك إلاّ على الأشياء المادية بحسب الأصل، أمّا الأشياء غير المادية فلا يرد عليها الضبط إلا استثناء بموجب نصوص خاصة، كما هو الحال في مراقبة المكالمات الهاتفية بموجب نصوص وتسجل المكالمات الخاصة التي تجري في مكان خاص.[1]

الفرع الأول: إجراءات سلطات الضبطية القضائية في التفتيش عن الجرائم الإلكترونية

التفتيش (**les Perquisitions**) هو إجراء من إجراءات التحقيق الابتدائي، وهو ليس من إجراءات كشف الجريمة قبل وقوعها، ولا يصح إجراءه أو صدور الإذن به إلاّ لضبط جريمة وقعت بالفعل، وترجحت نسبتها إلى متهم معين، ولا يصح بالتالي اتخاذ التفتيش وسيلة لضبط جريمة مستقبلية، ولو قامت تحريات ودلائل جدية على أنّها ستقع بالفعل وغاية التفتيش وثمرته هي ضبط الأشياء المتعلقة بالجريمة (les saisies) والتي تفيد في كشف الحقيقة، وهذه الأشياء قد تستمد منها أدلة الجريمة، قد تكون أداتها أو موضوعها أو محصلاتها.

[1] – عفيفي كامل عفيفي، المرجع السابق، ص364.

- **موقف الفقه والقضاء من التفتيش الخاص بجرائم التجارة الإلكترونية:**

لجأ الفقه والقضاء في كثير من الدول إلى التوسع في تطبيق نصوص التفتيش التقليدية ومدها للتطبيق على جرائم التجارة الإلكترونية.

لذلك فإن الحاجة باتت ماسة للتدخل التشريعي لتقرير الضوابط القانونية الكفيلة بالتغلب على الصعوبات الإجرائية التي تثار عن إجراء تفتيش بيانات التجارة.

الإلكترونية بواسطة مأموري الضبط القضائي، وبالتالي أجاز المشرع لمأموري الضبط القضائي القائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يصل بها النظام المعلوماتي، دون التقيد بالحصول على إذن مسبق بذلك من قاضي التحقيق ونرى أن هذه السلطة ليست مطلقة، ولكنها مقيدة بثلاثة قيود هي: [1]

1-ألاّ تكون النهاية الطرفية المتصل بها الحاسب موجودة إقليم دولة أخرى، حتى لا يؤدي الاتصال بها انتهاك سرية الدولة الأخرى.

2- أنّ يحل قاضي التحقيق محل الشخص صاحب المكان الذي ينبغي تفتيشه بصورة مؤقتة.

3- أنّ تحوي النهاية الطرفية المتصل بها الحاسب على بيانات ضرورية بصورة معقولة لظهور الحقيقة.

بالنسبة للصعوبة الخاصة بالولوج في أنظمة المعلومات وما بها من بيانات خاصة بالتجارة الإلكترونية لضبط ما يعد صالحاً منها كدليل أو قرينة لارتكاب جريمة ما، فإن التغلب عليها يقضي القيام بإنشاء إدارة شرطية متخصصة لمكافحة جرائم التجارة الإلكترونية مع الاهتمام بعمل دورات تدريبية متخصصة، من حيث المنهاج لجهاز الضبط القضائي العاملين فيها بغرض تدريبهم على تحقيق وضبط كل ما يتعلق بالتعامل مع جرائم التجارة الإلكترونية ونرى أن هذا المنهج المقترح يجب أن يتضمن كافة جرائم الحاسب الآلي، ونذكر منها على سبيل

[1] - عفيفي كامل عفيفي، المرجع السابق، ص365.

التخصص هو مجال موضوعنا جرائم التجارة الإلكترونية، وهذا يقضي أن يكون هذا المنهج به بعض علوم الاقتصاد وقانون التجارة وما إليها، ويكون مرتبطا بالتجارة بصفة عامة والتجارة الإلكترونية بصفة خاصة، وقد أخذ بذلك قانون جريمة الحاسب الهولندي بموجب نص المادة 25 منه والتي تجيز توجيه أمر إلى القائم على تشغيل النظام المعلوماتي للإفصاح عن المعلومات والبيانات اللازمة للولوج والتعامل مع برامجه وملفاته كمفاتيح تشغيل النظام وكلمات السر أو المرور، وإن كانت الكلمات التي تقتضي مصلحة التحقيق الحصول عليها مخزنة في صورة برمز داخل ذاكرة الحاسب فإنه يمكن تكليفه كذلك بتقديم الأكواد والمفاتيح اللازمة لفك الشفرة.[1]

الفرع الثاني: الصلاحيات المخولة لجهاز الضبط القضائي في الجرائم الإلكترونية

1-دور جهاز الضبط القضائي في ضبط أدلة جرائم التجارة الإلكترونية:

الضبط في معظم الأحوال يكون هو الغرض من التفتيش، وإن لم يكن هو السبب الأدق له فقد يأتي الضبط لأسباب أخرى غير التفتيش **مثل:** المعاينة وما يقدمه المتهم والشهود أما إذا تم نتيجة تفتيش المتهم أو مسكنة فيعد في هذه الحالة من إجراءات التحقيق لا الاستدلال.

الضبط لا يخرج عن كونه وضع اليد على شيء يتصل بجريمة وقعت على التجارة الإلكترونية ويفيد في كشف الحقيقة عنها وعن مرتكبيها، سواء في ذلك أن يكون هذا الشيء عقاراً أو منقولاً. [2]

والضبط بهذا المعنى لا يرد إلاّ على الأشياء فقط بالرغم من أن المشرع قد استخدمه في التعبير عن القبض على الأشخاص أحيانا.

كما أنّه لا ينص إلاّ على الأشياء المادية بحسب الأصل، أمّا الأشياء غير المادية فلا يرد

[1] – عبد الفتاح بيومي حجازي، المرجع السابق، ص ص: 210-211.

[2] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 212

عليها الضبط إلاّ استثناء بموجب نصوص خاصة، كما هو الحال في مراقبة المحادثات الهاتفية وتسجيل المحادثات الخاصة التي تجري في مكان خاص.[1]

2- القواعد القانونية المقررة لضبط الأشياء:

يجب على جهاز الضبط القضائي أن يضبط الأشياء التي يحتمل أن تكون قد استعملت في ارتكاب الجريمة، أو نتجت عن ارتكابها، أو يحتمل أن تكون قد وقعت عليها الجريمة وكل ما يفيد في كشف الحقيقة....إلخ".

كما تنص المادة83 على أنّه إن وجدت في مسكن المتهم أوراق مختومة أو مغلقة بأية طريقة، فلا يجوز لجهاز الضبط القضائي أن يفضها، وعليه إثباتها في محضر التفتيش وعرضها على الادعاء العام"[2]

كما أوجبت المادة 89 إجراءات عرض الأشياء المضبوطة على المتهم، كما أجازت أن يبدي ملاحظاته عليها مع وجوب عمل محضر بذلك يوقع عليه المتهم، فإذا امتنع عن التوقيع يجب أن يذكر ذلك في المحضر".

كما أوجبت المادة 88 أن توضع الأشياء والأوراق المضبوطة في حرز مغلق وأن تربط كلما أمكن ذلك مع وجوب ختمها، وأن يكتب على شريط الختم تاريخ المحضر المحرر لضبط تلك الأشياء، مع الإشارة للموضوع الذي حدث الضبط من أجله".

كما لا يجوز الاستناد إلى نص المادة السالفة الذكر ضبط الأوراق التي يسلمها المتهم للمدافع عنه أو للخبير الاستشاري لأداء المهمة التي عهد إليها، ويمتد هذا الحظر إلى المراسلات المتبادلة بينهما في القضية، كما تمتد كذلك إلى الأحاديث التي تجري بينهما في مكان خاص والمحادثات الهاتفية لوجود الحكة من تقرير الحظر في هذه الأحوال.[3]

---

[1] - عفيفي كامل عفيفي، المرجع السابق، ص 213

[2] - المادة 83 من قانون الإجراءات الجزائية العماني.

[3] - عفيفي كامل عفيفي، المرجع السابق، ص 214

3- إمكانية ضبط أدلة الجريمة الإلكترونية.

تمكن الصعوبة في هذه الحالة في قلة خبرة بعض العاملين في الأجهزة الأمنية لقلة التدريب، مع حداثة هذه الجرائم نسبياً، مما يترتب عليه فشلها هي والأجهزة الأخرى المنوط بها التحقيق في جمع الأدلة في هذا المجال.

وثمة صعوبة ثانية تتمثل فيما إذا كانت عملية الضبط لهذه الوسائل التقنية تتم في الأنظمة المعلوماتية الكبيرة أو الشبكات، حيث يصادف الضبط بصورة مؤكدة الصعوبتين الآتيتين:

1- قد يؤدي الضبط إلى عزل النظام المعلوماتي بالكامل عن دائرته لمدة زمنية قد تطول أو تقصر، مما قد يتسبب عنه أضرار بالجهة مستخدمة النظام وهي في الغالب شركة تجارية كبير، وأي تعل أو توقف أو عزل في أنظمتها المعلوماتية فإنه يصيبها بخسائر مالية كبيرة.

2-عدم إبداء مستخدمي الأنظمة المعلوماتية الاستعداد للتعاون الكامل والفعال مع سلطات التحقيق للوصول للحقيقة الكاملة للجريمة، مما يعينه الضبط بالنسبة لها من المساس بحقوق الغير.

3- تتسم الجرائم التي يكون محلها بيانات التجارة الإلكترونية الموجودة على الحاسب الآلي بعدم تركها لأية آثار يمكن الاستدلال بها عليها، ويتجلى ذلك بصورة واضحة في جرائم كثيرة منها الاختلاس والتزوير التي يستخدم فيها الحاسب الآلي.

4- ضخامة البيانات التي من الواجب فحصها من قبل جهاز الضبط القضائي ناهيك عن تطلب قدر من الخبرة الفنية لتحديد البيانات التي تصلح كأدلة جنائية من عدمه، الأمر الذي يحول الوصول إليها في كثير من الأحيان.

5- عدم وجود مدربين مؤهلين و مدربين على التعامل مع البيانات التي تعدد دليلا على الجريمة المعلوماتية التي حدثت، الأمر الذي يؤدي إلى إغفال دليل على الجريمة المعلوماتية التي حدثت، الأمر الذي يتطلب تدريب جهاز الضبط القضائي على القيام بإجراءات فنية

لسلامة وحفظ البيانات المضبوطة وصيانتها من العبث، وهو الأمر الذي يقتضي استخدام وسائل إلكترونية في إجراء التفتيش والضبط بصورة سرية دون التقيد بإخطار المتهم بهذه الإجراءات، وذلك لأن قواعد الضبط والتحرير التقليدية لا تتناسب مطلق مع الأدلة هذه الجرائم التي تكون في معظم الأحوال متخلي عنها الطابع المادي.[1]

والأمر يزداد صعوبة بعض الشيء في حالة ما إذا استخدم الجاني بعض الوسائل الفنية في الإتلاف مثل: استخدام(فيروس) أو زرع برنامج فرعي يسمح لمن قام بزرعه بالولوج غير المصرع به في موردات النظام الخاص بالحاسب الآلي.

وتمكن الصعوبة هنا في قلة الخبرة الفنية لجهاز الشرطة المختصة هذا ليس عيباً أو قصوراً أيضاً لماذا؟ لأن جرائم الحاسب الآلي وخاصة الفنية منها حديثة العهد وجهاز الشرطة بضباطه وأفراده لازالوا حديثي العهد في التعامل مع هذه الجرائم ولكن هذا حق جهاز الشرطة ومنتسبيه يبذلون جهودا كبيرة في سبيل ملاحقة التطور التقني للحاسب، وأيضا أعضاء جهاز القضاء والادعاء العام الجزائي على كيفية التعامل مع هذا النمط الإجرامي، وخاصة في جزئية كيفية ارتكاب الجرائم وطرق الكشف عنها، وكيفية جمع الأدلة والقرائن اللازمة لإثباتها[2].

[1] – هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، سنة 1994، ص217.

[2] – حاتم عبد الرحمان منصور الشحات، المرجع السابق، ص218.

المطلب الثالث: أنواع الأدلة المتعلقة بالجرائم الإلكترونية وطرق التحقق فيها

عندما تقع جريمة من جرائم الحاسب الآلي ويتم الإبلاغ عنها، فإن السلطات المختصة التنفيذية تقوم بواجباتها للتحري عن وقوع الجريمة، والحصول على أدلة وقوعها ثم التحقيق في مرتكبيها، ومن ثم توقيع العقوبة عليه.

وعندما تقوم السلطة المختصة بالتحري عن وقوع الجريمة على الحاسب الآلي فإنها تبحث عن أدلة معينة، إذا وجدتها فإنها تثبت بها وقوع الجريمة، فما هي هذه الأدلة؟.

الفرع الأول: الأدلة التقليدية بالجرائم الإلكترونية.

يقصد بالدليل في صورة التقليدية ذلك الجزء الذي يؤدي إلى اقتناع القاضي بارتكاب شخص لجريمة على وجه اليقين.[1]

ومن أشهر الأدلة التقليدية لإثبات جرائم الحاسب وهي: التلبس، والإثبات بالقرائن، والاعتراف، الشهادة.

أ- حالة التلبس:

يعد التلبس من الظروف العينية التي تلحق بالواقعة الإجرامية ذاتها، حيث يكون الشخص المجرم مجسما تصويريا كجزء في الواقعة المجرمة، ذلك أن مشاهدة الجريمة عينا يعد أقوى مظاهر إثبات الواقعة، لكي يتم استحقاق الإدانة بصورة لا تحمل أي شك أو ظن، كل ما يتطلبه القانون هو نقل الصورة الإجرامية مكتوبة إلى القضاء، فجهاز الضبط القضائي الذي يضبط أحد الأشخاص وهو يرتكب جريمة عبر الانترنت أثناء ارتكابها له، كما لو كان الجاني بصدد اخترق لمصرف أو بنك، فيتم رصده أثناء محاولة الاختراق، أو بعدها ببرهة قصيرة فتتم مطاردته عبر الانترنت، ويتم التعرف عليه وتحديد هويته خصوصاً إذا كان الحاسب ملكاً له، هذه كلها حالات تلبس، إلاّ إذا فات وقت طويل على ارتكابه

[1] - عمر محمد أبوبكر بن يونس، المرجع السابق، 234

للاختراق وليس الأمر كذلك في كل الأحوال، فهناك جرائم لا يمكن رصدها بالتلبس **مثل:** الاعتداء على حقوق الملكية الفردية، والتي تستند غالباً إلى شك المؤلف في أن مؤلفه قد تم طبعه دون إذنه، أو أن يكون أحد المتخصصين قد قرأه وقرأ مؤلفا آخر منقولاً منه، فهنا ينتفي التلبس.

ب– الإثبات بالقرائن:

يعترف القانون الجنائي بالأدلة المباشرة وهي التي لها دلالة مباشرة على ارتكاب الواقعة الإجرامية، ثم إنه إزاء الإمكانيات الكبرى التي يمنحها القانون للقاضي من حيث حريته في تكوين عقيدته، فإنه يمتد لكي يمكن القاضي الجنائي تحديد، من الاستعانة بالأدلة غير المباشرة المتمثلة في القرائن التي تشير دلالتها إلى ارتكاب شخص لواقعة إجرامية.

ويمكن تعرف القرينة بأنها[1]"استنتاج واقعة مجهولة من أخرى معلومة تتحد معها في العلّة"، أمّا القرينة أو الدليل الرقمي فهو أقرب الأدلة لجرائم الحاسب الآلي رغم أنّها تقف على حدود التعرف على بروتوكول الانترنت(Im Adresse).

ج–الاعتراف:

الاعتراف الجنائي هو إقرار المتهم على نفسه بارتكابه للواقعة محل الإجراءات الجنائية. وفي جرائم الحاسب الآلي يثور التساؤل، هل يكفي الاعتراف لثبوت التهمة المعلوماتية على المعترف؟.

للإجابة على هذا السؤال نورد المثال التالي، تمت جريمة اختراق، وتم الحصول على مجموعة أرقام بطاقات ائتمان، واعتراف أحد الأشخاص بارتكاب هذه الجريمة فهل يكفي اعترافه هذا لتوقيع العقوبة عليه؟.

لا يكفي هذا الاعتراف، ولا يجب أن نقيسه على ما يحدث في الجرائم التقليدية، حيث يتأكد القاضي من صحة قواه العقلية وعدم وقوع ضغط عليه، بل يتطلب الأمر في جرائم

[1] – عمر أبوبكر بن يونس، المرجع السابق، ص236.

الحاسب الآلي أن يتأكد القاضي، بالإضافة إلى ما سبق من أن المتهم المعترف يجيد استخدام الحاسب الآلي، لذلك فإن الاعتراف هو دليل جرائم الحاسب الآلي لا يكفي كما هو الحال في الجرائم التقليدية، ولذلك فهو يحتاج إلى ضوابط أكثر لاعتباره دليلا للإدانة.

د–الشهادة:

يمكن تعريف الشهادة بشكلها التقليدي بأنّها "إدلاء الغير الشهود بأقوالهم عن وقائع ترتبط بالجريمة موضوع التحقيق"[1].

ولكن هناك شهادة أخرى غير الموجودة في الجرائم التقليدية هي الشهادة الإلكترونية أي الاستعانة بشهادة الخبير في مجال الحاسبات الإلكترونية، وهي شهادة لا يكون الشاهد فيها حاضراً في جلسات التحقيق بذاته المادية أي بجسمه، وإنما تتم عبر وسائل إلكترونية أو رقمية وهي على حالتين:

الحالة الأولى:

الشهادة المسجلة أي يكون قد تسجيلها في تاريخ سابق وتعرض على المحكمة، وتكون في حالة عدم تمكن الشاهد من حضور الجلسات.

الحالة الثانية:

الشهادة الإلكترونية الفورية، وهي تحدث أثناء المحاكمة ولا يكون الشاهد حاضراً فيها بجسده، وهي تتطلب أن يكون هناك وسائل سمعية ومرئية للحصول على شهادته.

إنّ فكرة جرائم الحاسب الآلي وجرائم التجارة الإلكترونية بالأخص، لها خطورة كبيرة في هذه الجرائم، لأنّه ليس لها الكفاية اللازمة كما في الجرائم التقليدية، حيث أنّ جرائم الحاسب تعتمد على تكنولوجيا عالية وذكاء شديد، كما أنّ معظمها غير مادي وملموس مما يصعب إلى حد ما، إيجاد هذه الدلائل الكافية، لذلك يجب الحصر الكامل من رجال

[1] – هشام محمد فريد رستم، المرجع السابق، ص237.

الضبط فيما يعتبرونه دلائل كافية حصلوا عليها من تحرياتهم، لأن هذه الإجراءات تمس الحقوق العامة الحريات.

الفرع الثاني : الأدلة التقنية بالجرائم الإلكترونية

أهم الأدلة التقنية هي الدليل الرقمي**(Digital evidence)** أو الإلكتروني **Electronic evidence** وهو كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسب الآلي من إنجاز مهمة ما "وإذا ربطنا هذه الجريمة نقول إن الدليل الرقمي هو: "الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة"[1].

ولكي يحصل المحقق على هذا الدليل فهناك طريقتان:

الطريقة الأولى: فحص نظام الاتصال بالأنترنت، فيتم دراسة مسار الأنترنت **(routing)** وفحص ما يعرف ببروتوكول الانترنت**(ip)** والذي يميز كل عضو عن غيره وفحص النظام الأمني للشبكات

الطريقة الثانية: فحص أجهزة الحاسب الآلي وملحقاتها، ويقصد بذلك ضبط وحجز القطع المادية للحاسب**(hard waer)** التي تحتوي على البرامج لفحص وضبط ما بها كما فحص القرص الصلب، والبرمجيات، والنظام المعلوماتي، وذاكرة التخزين، والطابعة، ولوحة المفاتيح، وكذلك كله للوصول إلى الأدلة المطلوبة.

أماكن وجود الأدلة:[2]

من المهم توجيه فريق التفتيش إلى الأماكن التي يبحثون فيها عن الأدلة المحتمل وجودها بهذه الأماكن، بحيث يشمل التفتيش جميع ملحقات الحاسب الآلي، وعدم إغفال الأماكن الدقيقة، والتي ربما يراها المحقوق أنها غير مهمة، أو أن المتهم لن يخفي فيها أية أدلة.

[1] -حاتم عبد الرحمان رستم، المرجع السابق، ص238

[2] -نفس المرجع، ص239

طرق العلم بالجريمة الإلكترونية:

في التعامل مع الجرائم يتم التحري عن وقوعها بعدة طرق منها البلاغ والشكوى، ويقصد بالبلاغ ما يصل إلى علم جهاز الضبط القضائي من معلومات حول واقعة معينة يعدها القانون جريمة، وقانون الإجراءات المصري على سبيل المثال: يلزم رجال الضبط بتلقي البلاغات وتدوينها في المحاضر والاستيضاح بشأنها.

وفي جرائم الحاسب الآلي فإن البلاغ يكون له شأن كبير، لأنه وكما قلنا فإن رجال الضبط ليس لهم خبرات طويلة في هذا المجال نظراً لحداثته، وعدم حصولهم على الدراسات المتعمقة فيه، كذلك لسرية معظم العمليات الإجرامية الخاصة بالحاسب الآلي، أمّا الشكوى فهي لجوء المعني عليه إلى السلطات المختصة لتحريك الإجراءات الجنائية، ويثور التساؤل عن جرائم الانترنت: هل يصلح فيها قيام المجني عليه بالشكوى مع ملاحظة أن معظم هذه الجرائم لا يعرف مرتكبوها؟ والمستقر عليه فقها أنه في هذه الحالة أن مزود الدخول أو خدمات الانترنت مسؤول مسؤولية افتراضية باعتباره المسؤول عن كل الخدمات التي تصلح أن تكون عن طريق الانترنت هذا بالطبع إلا إذا وجدت قرينة على عدم مسؤوليته أو أنّها تم تحديد المجرم.[1]

[1] -نفس المرجع السابق، ص240

المبحث الثالث: الوسائل القانونية للحد من الجريمة الإلكترونية

لقد خالفت الجريمة الإلكترونية النمطية الواحدة التي تمتاز بها الجرائم التقليدية في طبيعتها الكلية والتي رصدت التشريعات القانونية الإجرائية خاصة إيجاد سبلاً لمحاربتها إلاّ أن جرائم العصر الرقمي الجديد أحدثت إشكالا عاماً يبرز كيفية التعامل مع هاته الجرائم التي أرغمت المشرع القانوني إلى تدارك النقص الهائل مسايراً في ذلك معايير أهمها التقنية العالية في هاته الجريمة.

فالجريمة الإلكترونية لا تترك أثراً مادياً في مسرح الجريمة كغيرها من الجرائم ذات الطبيعة المادية كما أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة، ولا تكفي في هذا النمط من الجرائم إعادة نظام الكمبيوتر وقواعد البيانات وشبكات المعلومات.

المطلب الأول: طرق ووسائل البحث عن الجريمة الإلكترونية.

مراحل جمع الأدلة كما حددها القانون هي المعاينة التفتيش والخبرة ومراقبة المحادثات وتسجيلات وسماع الشهود الاستجواب والمواجهة وليس على المحقق الالتزام بإتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساساً بمباشرتها جميعاً وإنما يباشر منها ما تميله مصلحة التحقيق وظروفه، ويرتبها وفقاً لما تقضي به المصلحة وما تسمح به الظروف.

الفرع الأول: معاينة مسرح الجريمة المعلوماتية.

يقصد بالمعاينة فحص فكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته، كمعاينة مكان ارتكاب الجريمة أو أداة المعاينة قد تكون إجراء حقيق لإثبات ما بالجسم من جراء أو على الثياب من دماء أوبها من مزق أو ثقوب.

والمعاينة جوازيه لمحقق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره، سواء طلبها الخصوم أو لم يطلبوها، ولا تتمتع بالمعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية، وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنّه ينبغي مراعاة عدة قواعد وإرشادات أهمها ما يلي: [1]

1- تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه، مع التركيز بشكل خاص على تصوير الأجزاء الخلفية للحاسب ملحقاته ويراعي تسجيل وقت وتاريخ ومكان التقاط كل الصور.

[1] -عبد الله حسين محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، عن موقع:
htt://www.arab la winfo.com/research earch.asp ?validate: articles, ID=148

2- العناية البالغة بالطريقة التي تم إعداد النظام الآثار الإلكترونية، وبوجه خاص التسجيلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال، ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الوقع أو الدخول معاً في الحوار.

3- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي محاولات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات يمكن أن تتسبب في محو البيانات المسجلة.

4- التحفظ على محتوى سلة المهملات من الأوراق الملقاة والممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة، السليمة وغير السليمة أو المحطمة وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

5- إعداد خطة للهجوم بحيث تكون الخطة واضحة ومفهومة لدى أعضاء الفريق، على أن تكون الخطة موضحة بالرسومات وتتم مراجعتها مع أعضاء الفريق قبل التحرك مع الأخذ في الاعتبار قاعدة **Smed** العسكرية والتي تعني الحالة **Situation** الرسالة Mission التنفيذية **Exécution** المداخل والمخارج **Avenues et aprroch**والاتصالات**Communication** هي ملائمة للأجهزة الأمنية وأجهزة تنفيذ القوانين، فالحالة أو الوضع يعني معرفة حجم القضية التي تقوم التحقيق وعدد المتورطين فيها، أمّا الرسالة فهي تحدد الهدف، و التنفيذ يعني كيفية أداء المهمة، أمّا المداخل والمخارج فإن من المهم معرفتها وهي تختلف من جريمة لأخرى، وتحسب وفقاً لمكونات طريق التحقيق بينما يأتي عنصر الاتصال، لضمان السرية وتبادل المعلومات أثناء عملية التحقيق. [1]

[1] -منتدى جامعة قطر كلية القانون: مراحلي إثبات الجريمة الإلكترونية عن موقع:
htt://www.quatar.com/VB/showheard php ?t=20845.

الفرع الثاني: التفتيش في مجال الجريمة المعلوماتية.

يعتبر التفتيش إجراء من إجراء من إجراءات التحقيق يتطلب أوامر قضائية لمباشرته، ويهدف للبحث عن الأدلة المادية التي ترتبط بالجريمة مدار التحقيق، ولا يشمل ذلك الأدلة الشفوية أو القولية للاتصال، هذه الأخيرة هي عنصر الشخص الشاهد، ويجري التفتيش بخصوص جرم تحقق وقوعه ويوجه إلى مكان يتمتع بالحرمة أو يتجه إلى شخص المشتبه به، ويخضع التفتيش في وجوده وإجراءاته التنفيذية إلى أحكام القانون التي من أبرزها صدور أمر التفتيش أو مذكراته الكتابية عن الجهة التي حددها القانون مع بيان الأسباب الموجبة لذلك ومحل التفتيش المخصوص. [1]

ضوابط تفتيش نظم الحاسب الآلي:

يمكن تقسيم ضوابط تفتيش نظم الحاسب الآلي إلى نوعين موضوعية وشكلية:

1- الضوابط الموضوعية لتفتيش نظم الحاسب الآلي: وتنحصر هذه الضوابط في:

أ- وقوع جريمة إلكترونية:

هي كل فعل غير مشروع مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة وهناك العديد من التشريعات التي حرضت على استحداث نص خاص كما هو الحال بالنسبة للأنظمة القانونية التي تم التطرق سابقاً في إطار الجهود الدولية سواء المنفردة منها أو الجماعية في مواجهة هاته الجريمة العصرية، تورط شخص أو أشخاص معينين في ارتكاب الجريمة المعلوماتية أو الاشتراك فيها، ينبغي أن تتوفر في حق الشخص المراد تفتيشه دلالة كافية تدعو إلى الاعتقاد بأنّه قد تساهم في ارتكاب الجريمة الإلكترونية، سواء بوصفه فاعلا لها أو شريكا فيها وفي مجال الحاسب الآلي يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة، كذلك على خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة المعلوماتية إلى

[1] -نبيلة هروال، المرجع السابق، ص221

شخص معين سواء بوصفه فاعلاً أو شريكاً[1].

2- الضوابط الشكلية لتفتيش نظم الحاسب الآلي:

تقتحم قوات الشرطة القضائية بصورة سريعة ومن كافة منافذه في آن واحد وذلك باستخدام القدر الأعظم من القوة بافتراض أن هذا التكتيك يقلل من احتمالية وقوع إصابات بين صفوف رجال الشرطة.

يتم إبعاد سائر المشتبه فيهم عن كافة أنظمة ومعدات الكمبيوتر المتواجدة في المكان على الفور حتى لا يتمكنوا من تشويه أو تدمير أي دليل إلكتروني، ويتم إدخال سائر المشتبه فيهم إلى غرفة لا توجد بها أية أجهزة كومبيوتر، ويوضعوا تحت دراسة مشددة، وفي هذه الخطورة يتم تقديم التفتيش الصادر من النيابة إليهم ويتم تحذيرهم بأن كافة أقوالهم ستسحب عليهم منذ هذه اللحظة وقد تأخذ بمثابة دليل إدانة ضدهم.

توضع النقطة الساخنة في عهدة فريق يضم اثنين من العملاء (مكتشف مسجل)، ويجب أن يكون المكتشف من بين العملاء الذين تم تدريبهم تدريباً متقدماً على نظم المعلومات، وغالباً ما يقوم بهذا الدور العميل المعني بالقضية منذ البداية واستصدار إذن بالتفتيش الخاص بها من القاضي، فهذا الشخص يعرف تماماً الشيء أو الأشياء التي يبحث عنها ويتفهم طبيعتها تماماً ولن نتجاوز إذا ما قلنا أنّه هو الذي يقوم بفتح الأدراج والبحث عن الديسكات والملفات وحاويات الأسطوانات....إلخ.

أمّا المسجل فيتولى تصوير كافة الأجهزة والمعدات على ذات الكيفية التي تم ضبطها عليها، ويقوم المسجل كذلك بتصوير كافة الغرف الأخرى الموجودة بالمنزل حتى لا يدعي أحد المجرمين الماكرين أن الشرطة قد سرقت منزله أثناء التفتيش.[2]

---

[1] -محمد أبوبكر بن يونس، ص380.

[2] -نبيلة هروال، المرجع السابق، ص223

الفرع الثالث: الخبرة في مجال الجريمة المعلوماتية.

-مبررات الخبير وإجراءاته:

يرى المحقق في بعض الأحيان ضرورة الاستعانة بالخبير لإيضاح مسألة تستعصي ثقافته العامة عن فهمها، كتحديد سبب الوفاة أو ساعتها، أو رفع بصمة وجدت في مكان الجريمة، أو فحص سيارة لبيان ما فيها من خلل، وتكتسب الخبرة أهمية بالغة في مجال الجريمة المعلوماتية نظراً لأن الحاسبات وشبكات الاتصال بينها على أنواع ونماذج ومتعددة، كذلك فإن العلوم والتقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية ومتنوعة والتطورات في مجالها سريعة ومتلاحقة الدرجة قد يصعب معها على المتخصص تتبعها واستيعابها، ويمكن القول بصفة عامة بأنّه لا يوجد حتى الآن خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرامجها وشبكاتها، كذلك لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها.

لذا ترك المشرع للمحقق الحرية الكاملة في هذا الشأن ليمكنه من كشف الحقيقة بالسرعة اللازمة وبالطريقة التي يراها مناسبة، وللمحقق في أي وقت إلى أن ينتهي التحقيق بما فيها الكفاءة الفنية اللازمة للاستعانة بخبرته.

وللخصوم حق الحضور أثناء عمل الخبير، ويجوز مع ذلك أن يباشر الخبير عمله في غياب الخصوم، وإن يمنعهم كذلك من الحضور إلاّ إذا كان للمنع سبب، ويعد الحصول على المستندات خلال عملية التفتيش أمراً سهلا حيث يمكن التعرف عليها بالرؤية ولن يحتاج المحقق أي مساعدة من قبل الخبراء، وهذه المستندات مثل: أدلة عمل النظام، سجلات إدارة الكمبيوتر وثائق البرامج السجلات صيغ مداخلات البيانات والبرامج، وكذلك صيغ مخرجات الكمبيوتر المطبوعة ويتم التخطيط على هذه المستندات ما إذا كانت كاملة أو أصلية أو صوراً من خلال استجواب القائمين على حفظها.[1]

[1] -محمد أبو بكر بن يونس، المرجع السابق، ص 382.

الفرع الرابع: الضبط في مجال الجريمة المعلوماتية

يقصد بالضبط في قانون الإجراءات وضع اليد على شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها وهو من حيث طبيعتها القانونية قد يكون من إجراءات الاستدلال أو التحقيق، وتتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط، فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أمّا بمثابة إجراء استدلال.[1]

1- محل الضبط:

لا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه كذلك يستوي أن يكون الشيء المضبوط مملوكاً للمتهم أو لغيره والقاعدة أن الضبط لا يرد إلاّ على شيء مادي أو الأشياء المعنوية فلا تصلح بطبيعتها محلا للضبط والشرط اللازم لصحته أن يكون مفيداً في كشف الحقيقة فكل ما يحقق هذه الغاية يصح ضبطه والأدلة المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات الجرائم الحاسب الآلي ونسبتها إلى المتهم هي:

1- الورق:

كثيراً من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها قدراً كبيراً من الأوراق والمستندات الرسمية منها والخاصة، إلاّ أن وجود أجهزة الحاسب يجعل كثيرا من المعلومات يتم حفظها في الحاسب الآلي والطابعات المتطورة ذات السرعة الفائقة تطبق قدراً كبيرا من الأوراق في وقت قصير، وعليه يعتبر الورق من الأدلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة و الورق أربعة أنواع:

1- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو تصوير للعملية التي يتم برمجتها.

[1] - محمد أبو بكر بن يونس، المرجع السابق، ص 382.

2-أوراق تالفة يتم طباعتها للتأكد ومن ثم إلقاؤها في سلة المهملات.

3-أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.

4- أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحاسبات وتكون لها علاقة بالجريمة خاصة عند تلقيها أو تزويرها بيانات لتنفيذ جريمة الحاسب الآلي.

2- جهاز الحاسب الآلي:

وجود جهاز حاسب آلي مهم للقول بأن هناك جريمة، ولأجهزة الحاسب الآلي أشكال وأحجام وألوان مختلفة، وخبير الحاسب الآلي يستطيع أن يعترف على الحاسب الآلي، ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الإلكترونية والأخرى تحديد أسلوب التعامل معه في حالة الضبط والتحريز.

3- ملحقات الحاسب الآلي:

من السهل التعرف على جهاز الحاسب الشخصي الذي أصبح مألوف اليوم فهو يتكون من وحدة المعالجة المركزية cup لوحة المفاتيح Keyboard والشاشة monitor ومع التطورات السريعة التي يمر بها الحاسب الآلي يوجد إضافات جديدة.

مثل: المودم والماوس والسماعات " والسيرفر" وإذ كنا بصدد الحديث عن الأجهزة الكبيرة فإننا نجد أشكالها تتغير باستمرار خاصة من حيث الحجم والهيكل، ومن الضروري إطلاع العاملين في مجال التحقيق على مختلف أجهزة الحاسب وظهورها.

4- أقراص الليزر Disks and diskettes:

مع جهاز الحاسب الآلي للشخص الطبيعي والشخص المعنوي نجد قدراً كبيراً من أقراص الليزر، علاوة على أن مراكز الحاسب الآلي في الأشخاص المعنوية يوجد فيها الآلاف من الأقراص قد تكون على غلاف قرص بيانات توضح محتويات كل قرص وبمعرفة خبير يقدم الدليل أمام المحكمة، وقد تجد في مكان أقراص الليزر ولا تجد معها أجهزة الحاسب

الآلي ومع ذلك يعدّ جزء من جريمة الحاسب الآلي متى كانت محتوياتها عنصر من عناصر الجريمة.

5- الشرائط الممغنطة: Magnetic Tapes

تستعمل الشرائط الممغنطة عادة للحفظ bakup الاحتياطي وقد تكون في مكان بعيد أمن، كما يقوم البعض بإيداعها في خزائن البنوك التجارية أو مراكز التوثيق الحكومية الآمنة.[1]

[1] - عبد الفتاح بيومي حجازي، المرجع السابق، ص: 306.

المطلب الثاني: الاختصاص القضائي والعقوبات المقررة

الفرع الأول: الاختصاص القضائي

يقصد بالاختصاص القضائي ولاية أو سلطة الحكم بمقتضى القانون في خصومة معينة معروضة على المحاكم، وفقدان هذه السلطة يؤدي إلى عدم الاختصاص وإن كان الاختصاص النوعي أو المحلي بالنسبة للقضايا المعروضة على القضاء لا يطرح إشكالا بالنسبة للأشخاص الطبيعية أو المعنوية في الجرائم التقليدية فإنّه قد طرح عدة مشاكل في مجال الجرائم الإلكترونية، حيث تطبق المبادئ العامة على هذا النوع من الجرائم، إلاّ أن المشرع الجزائري سكت على الفصل في هذه القضية.

1- الاختصاص النوعي:

يتحدد الاختصاص النوعي للمتحكم وفقا لجسامة المجرم التي حددها القانون على أساس العقوبة المقررة لها، فالجنايات من اختصاص محكمة الجنايات، والجنح من اختصاص محكمة الجنح، والمخالفات من اختصاص محكمة المخالفات [1].

حيث وضع المشرع الجزائري عقوبات لجريمة المساس بالأنظمة المعالجة الآلية للمعطيات، لذا ومن خلال الاطلاع على نصوص المواد[2] فإن هذه الجريمة تصنف على أنّها جنحة، ذلك لأن العقوبات المقررة لها وفق ما سبق توافقاً مع أقره المشرع في المبادئ العامة، حيث نجد أن

---

[1] - أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الطبعة الأولى، الجزائري، ص 357.

[2] - المادة 394 مكرر: "يعاقب بالحبس من ثلاث أشهر إلى سنة وبغرامة من 50.000دج إلى 100.000دج..".

- المادة 394 مكرر1:"يعاقب بالحبس من ثلاث أشهر إلى ثلاث سنوات وبغرامة من 100.000دج إلى 5000.000دج.....".

- المادة 394 مكرر7:"يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

هذه الجرائم لا تتعدى عقوبتها ثلاثة سنوات، لذلك فإن محكمة الجنح تكون ذات ولاية بالنظر فيها.

2- الاختصاص المحلي:

لا يكفي أن تتحدث المحكمة المختصة بالنظر إلى جسامة الجريمة إذ تتعدد محاكم الدرجة الواحدة ويتعين على الجهة المختصة بالفصل في الدعوى، وقد وضع المشرع الجزائري ثلاث أماكن لتحديد الاختصاص المكاني:

أ- محل وقوع الجريمة:

فيها اعتداء على الأمن العام، وانتهاك القانون وفيها يسهل جمع الأدلة

ب-محل إقامة أحد المتهمين:

وهو ما ييسر الكشف عن ماضي المتهم وسوابقه ولا سيما أنه قد يتعذر تحديد مكان وقوع الجريمة أو تكون قد وقعت في الخارج ومكان إقامة المتهم هو مكان إقامته المعتاد، وليس المواطن المختار أو القانوني.

ج-محل القبض على المتهم:

وهو ما يجنب السلطة العامة مشقة نقل المتهم إلى مكان وقوع الجريمة واحتمال هروبه، فضلاً عن الجريمة التي تقع في الخارج أو يتعذر معرفة مكان وقوعها أو لا يكون للمتهم محل الإقامة. [1]

وبالتطبيق على الجرائم الإلكترونية فقد يقع النشاط الإجرامي في مكان تحديد النتيجة الإجرامية في مكان آخر، ولذلك فإن كلا المحتكمين التابع لها للمكانين تكون مختصة باعتبارها محل وقوع الجريمة.

وإن كانت الجريمة تتكون من جملة أفعال وقعت في أكثر من مكان كانت جميع المحاكم التي وقعت في دوائرها أفعال التنفيذ مختصة بالنظر في الدعوى من حيث المكان.

[1] - أحمد شوقي الشلقاني، المرجع السابق، ص ص:358-359

الفرع الثاني: العقوبات المقررة.

تناول المشرع الجزائري الجزاءات المقررة لهذه النوع من الإجرام والتي سمّاها بالعقوبات الجزائية على جريمة المساس بأنظمة المعالجة الآلية.

من خلال القانون 23/06المؤرخ في 20ديسمبر 2006 الذي تضمن مواده عقوبات ردعية أصلية وتكميلية تطبق على الشخص الطبيعي لمبدأ المسائلة الجزائية له فحددها المشرع في القسم السابع المكرر:المواد394مكرر إلى 394مكرر7من هذا القانون.

أولاً: العقوبات الأصلية:

من خلال استقرائنا للنصوص المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يتبين لنا وجود المتدرج داخل النظام العقابي ويحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات ونجد من خلال ثلاث حالات هي:

1-الدخول أو البقاء في الغش(الجريمة البسيطة):

اعتبرها المشرع جنحة وأعطى لها عقوبة طبقاً للمادة 394مكرر من القانون 06-23 وهي 3أشهر إلى سنة حبس و 50000 إلى 100000 دج كغرامة مالية كل من يدخل أو يبقى عن طريق الغش في جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك[1].

2-الدخول والبقاء بالغش (الجريمة المشددة):

هي أخرى يعتبرها المشرع جنحة غير أنه ضاعف لها العقوبة في حالة حذف أو تغيير للمعطيات المنظومة وذلك بإقراره لعقوبة الحبس بين 6أشهرإلى سنتين وبغرامة مالية من 50.000دج إلى 150.000دج إذا ترتب على ذلك التزام بالفعل المعاقب عليه لظروف قد تؤدي إلى تنفيذه ألا وهي نتائج الدخول أو البقاء الغير المشروع لتخريب نظام الأشغال

[1] - القانون رقم 06-23المؤرخ في 2006/12/20المعدل والمتمم للأمر رقم 66-156المؤرخ في 08يونيو 1966(الجريدة الرسمية رقم 84 المؤرخة في 2006/12/24)

المنظومة طبقاً للمادة 394مكرر الفقرة2 من قانون العقوبات الجزائية.

3-الاعتداء العمدي على المعطيات:

العقوبة المقررة في حالة الاعتداء العمدي على المعطيات داخل النظام طبقاً للمادة 394مكرر1 من قانون العقوبات هي الحبس من 6أشهر إلى 3سنوات وبغرامة50.000 دج إلى 200.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية وإزال أو عدل بطريق الغش المعطيات التي ينظمها.

ثانيا: العقوبات التكميلية

إلى جانب العقوبات الأصلية للجريمة التي يقوم بها المجرم الطبيعي فإن المشرع أضاف عقوبات تكميلية طبقاً للمادة 394مكرر من القانون 06-23 وهي كالآتي: [1]

1-المصادرة:

تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب إحدى الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة الغير حسن النية.

2-إغلاق المواقع:

وهنا الأمر يتعلق بالواقع التي تتكون محلا للجرائم الماسة بالأنظمة المعلوماتية.

3-إغلاق المحل أو مكان الاستغلال:

هنا يجب أن يتوفر عنصر العلم بالجريمة لصاحبها في **مثل:** إغلاق المقهى الإلكتروني الذي ترتكب فيه الجريمة.

ثالثا: الظروف المشددة.

نصت المادة 394مكرر الفقرة 2و3 على ظرف تشدد به عقوبات جريمة الدخول والبقاء الغير المشرع داخل النظام ويتحقق الظروف عند ما ينتج عن الدخول أو البقاء إمّا

[1] - القانون 06-23 المؤرخ في 20-12-2006.

حذف أو تغيير المعطيات التي يحتويها النظام، ففي الحالة الأولى تتضاعف العقوبة المقررة طبق للفقرة الأولى من المادة 394مكرر وفي الحالة الثانية تكون العقوبة من 6أشهر إلى سنتين وبغرامة من 50.000 إلى 150.000دج وهذا الظرف المشدد هو ظرف مادي يكفي أن تقوم بينه وبين الجريمة الأساسية وهي جريمة الدخول أو البقاء الغير المشروع علاقة سببية للقول بتوافره.

تتضاعف العقوبة في حالة أن الجريمة استهدفت الدفاع الوطني أو الهيئات أو المؤسسات الخاصة للقانون العام.[1]

[1] - القانون 06-23 المؤرخ في 20-12-2006.

المطلب الثالث: الوسائل الدولية للحد من الجريمة الإلكترونية

إن مكافحة الجرائم الإلكترونية على صعيد مستوى الدولة الوحيدة لن يكون مجدياً، إلا إذا كان هناك تعاون دولي على أكبر قدر من التنسيق والتعاون بين الدول والمنظمات، ومن ثم العمل على تنسيق تلك الجهود المبذولة بين كافة دول العالم لتكون هناك أسس ومبادئ وقوانين وثقافة يمكن الاعتماد عليها لخلق مواطن لديه وعليه يجنبه عدم الانزلاق وراء دوافعه لارتكاب إحدى الجرائم الإلكترونية.

الفرع الأول: التشريعات على مستوى العربي.

ليس هناك في العالم العربي ما يستحق الوقوف عنده كثيراً، فإنه للأسف لا توجد أي دولة عربية قامت بسن قوانين جديدة خاصة بها لتستوعب تلك المستجدات الإجرامية، فالدول العربية لازالت بعيدة كل البعد عن ذلك التطور القانوني الذي يحاول اللحاق بالتطور الإجرامي، وعليه يمكن تلخيصها فيما يلي:

أ-تشريع الإمارات العربية المحددة:

يعتبر القانون الاتحادي رقم 02-سنة 2006 في شأن مكافحة جرائم تقنية المعلومات، هو الإطار القانوني لمكافحة هذا النوع المستجد من الجرائم ولعل هذا القانون يعتبر من القوانين الريادية الأولى في العالم العربي الذي ينظم مكافحة الجرائم المعلوماتية.[1]

وسوف نقوم بذكر بعض الجرائم التي تعرض في هذا القانون فمنها:

1-جريمة اختراق المواقع والأنظمة الإلكترونية.

2-جريمة التزوير لمستندات معترف بها معلوماتياً.

3-جريمة التصنت باستعمال الانترنت أو إحدى وسائل تقنية المعلومات.

4-جريمة التهديد باستخدام الانترنت أو إحدى الوسائل التقنية.

[1] - عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت(الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، الطبعة الثانية، بيروت،2007، ص63.

5-جريمة انتهاك الحياة الخاصة عن- طريق الانترنت أو إحدى الوسائل التقنية.

ب-التشريع السعودي:

احتلت السعودية المركز السادس عالمياً بين الدول التي تنطلق منها الهجمات الإلكترونية نسبة إلى عدد مستخدمي، وبدأت السلطات في الإعداد لإصدار قانون جديد لمكافحة الجرائم الإلكترونية وذلك بتاريخ 07فيفري2007 ويتضمن مشروع القانون 16مادة.

حيث يتضمن السجن لمدة لا تزيد عن سنة وبغرامة لا تزيد عن 500ألف ريال أو بإحدى هاتين العقوبتين لكل شخص يرتكب أي من جرائم التنصت على المعلومات المرسلة عن طريق الشبكة العالمية، كما يتضمن تجريم الدخول غير المشروع للمواقع الإلكترونية لتغيير تصميماته أو تعديله أو إلغائه أو إتلافه، وتصل مدة السجن إلى 10سنوات.

ج-التشريع التونسي:

يحدد القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية رقم 83 المؤرخ في 09أوت 2000 بعض الأحكام الخاصة بجرائم المعلوماتية والانترنت فعلى سبيل المثل الفصل 48 من القانون المشار إليه على أنّه يعاقب كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين ستة أشهر وعامين وبخطية تتراوح بين 1000و10.000دج أو بإحدى هاتين العقوبتين، أمّا بموجب الفصل 49 فإنه يعاقب كل مخالف لأحكام الفصول 25و27و29 والفقرة الثانية من الفصل31والفصل 34والفقرة الأولى من الفصل 35من هذا القانون بخطية تتراوح بين 500إلى 5000دج. [1]

[1] - عبد الله عبد الكريم عبد الله، المرجع السابق، ص ص81-85.

د- التشريع على المستوى الوطني الجزائري:

يتناول المشرع الجزائري هذا النوع من الجرائم من خلال القانون 06-23الذي تضمن في مواده عقوبات ردعية أصلية وتكميلية تطبق على الشخص الطبيعي حيث يتضمن جريمة المساس بأنظمة المعالجة الآلية لبيانات والمعطيات، التي جاء بها في المواد من 394مكرر إلى 394 مكرر07 من قانون العقوبات الجزائري.[1]

الفرع الثاني: التشريع على المستوى العالمي.

أ-التشريع السويدي:

تعد دولة السويد من أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الانترنت والحاسب الآلي لتستطيع أن تعاقب المتهمين بارتكاب تلك الجرائم الإلكترونية، حيث صدر أول قانون خاص بها وسمي بقانون البيانات وقد صدر هذا القانون عام 1973 وقد عالج هذا القانون قضاياً الاحتيال عن طريق الانترنت بالإضافة إلى كونه يشمل على فقرات عامة من نصوصه لتشمل جرائم الدخول الغير المشروع على البيانات الإلكترونية. [2]

ب-التشريع الأمريكي:

كانت هي الدولة الثانية في إصدار قوانين خاصة بها تجرم الجرائم الإلكترونية، حيث شرعت قانوناً خاصاً بحماية أنظمة الحاسب الآلي(985-1976)وفي عام 1985 حدد معهد العدالة القومي الأمريكي خمسة أنواع من الجرائم المعلوماتية وهي:

1-جرائم الحاسب الآلي الداخلية.

2- جرائم التلاعب بالحاسب الآلي.

3- جرائم الحاسب الآلي غير المشروع عن بعد.

---

[1] -القانون رقم06-23المؤرخ في 2006/12/20 المعدل والمتهم للأمر رقم 66-156.

[2] -أبوبكر بن يونس، المرجع السابق، ص385.

4-دعم العاملات الإجرامية.

5- سرقة البرامج الجاهزة والمكونات المادية للحاسب.

وقد خولت وزارة العدل الأمريكية في عام 2000خمس جهات حكومية للتعامل مع جرائم الانترنت والحاسب الآلي منها مكتب التحقيقات الفيدرالي**(FBI).**

ج-التشريع البريطاني:

هي ثالث دولة تسن قانوناً خاصاً بها لجرائم الانترنت حيث أقرت قانوناً لمكافحة التزوير والتزييف عام1981م الذي تشمل في تعاريف الخاصة كأداة التزوير، ووسائط التخزين الحاسوبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق الإلكترونية أو التقليدية أو أي طرق أخرى.

د-التشريع الفرنسي:

هي من الدول التي اهتمت بتطوير القوانين الخاصة مع جرائم التكنولوجيا الحديثة (الجرائم الإلكترونية) فقد طورت فرنسا قوانينها الجنائية للتوافق مع المستجدات الإجرامية، حيث أصدرت أول قانون خاص بها عام 1988القانون رقم 88/19 والذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لتلك الجرائم.

الفرع الثالث: المعاهدات والمؤتمرات الدولية.

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي، في مجال مكافحة الجرائم الإلكترونية، وقد تم عقد العديد من المعاهدات التي تعمل على التعامل الدولي في مجال مكافحة هذا النوع من الجرائم ومنها: [1]

أ- معاهدة بودابست لمكافحة جرائم الانترنت.

بتاريخ 2000/08/20 تقدمت اللجنة الأوربية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية بمشروع اتفاقية جرائم الكمبيوتر، تتكون هذه الاتفاقية من مقدمة وأربعة

[1] - عبد الله عبد الكريم، المرجع السابق، ص125.

فصول فبعد أن استعرضت المقدمة أهداف الاتفاقية و منطلقاتها ومرجعياتها السابقة، جاء الفصل الأول لتغطية المصطلحات الأساسية (المادة الأولى) وتضمن الفصل الثاني ثلاث أقسام: يضم الأول المواد 02-13 ويعالج النصوص الموضوعية لجرائم الكمبيوتر، والقسم الثاني يضم المواد من 14-21 وتتعلق بالقواعد الإجرائية والقسم الثالث يضم المادة22 وهي تتعلق بالاختصاص، أمّا الفصل الثالث من الاتفاقية، فقد تضمن قسمين الأول تحت عنوان المبادئ العامة ويضم المواد من 23-28 والقسم الثاني يتعلق بالنصوص الخاصة ويضم المواد من 29-35 أمّا الفصل الخامس فيتضمن الأحكام الختامية ويضم المواد من 36-48.

ب-القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات.

اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العرب ما سمي بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات، وما في حكمها نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة، والذي كان قد اعتمده مجلس وزراء العدل العرب في دورته التاسعة بالقرار رقم 495-د19 بتاريخ 2003/10/08 ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين ويتكون من 27مادة.

ج-المعاهدة الأوربية لمكافحة الجريمة الإلكترونية.

لقد وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الأوربي على المسودة النهائية لمعاهدة شاملة تهدف إلى مساعدة الدول في مكافحة الجريمة الإلكترونية، وبعد أن يتم المصادقة عليها من قبل رئاسة المجلس والتوقيع عليها من قبل البلدان المعنية ستلزم الاتفاقية الموقعين عليها بسن الحد الأدنى من القوانين لمواجهة جرائم التقنية العالية. [1]

[1] - عبد الله عبد الكريم، المرجع السابق، ص140.

ملخص الفصل الثاني

لقد خالفت الجريمة الإلكترونية النمطية الواحدة التي تمتاز بها الجرائم التقليدية في طبيعتها الكلية والتي رصدت التشريعات القانونية الإجرائية خاصة في إيجاد سبلا لمحاربتها، إلاّ أنّ جرائم العصر الرقمي الجديد أحدثت إشكالاً عاماً يبرز كيفية التعامل مع هاته الجرائم التي أرغمت المشرع القانوني إلى تدارك النص الهائل مسايراً في ذلك عدة معايير أهمها، التقنية العالمية في هاته الجريمة.

حيث تقوم الأجهزة الأمنية بضبط الأشياء التي تفيد في ظهور الحقيقة التي تم ارتكابها ثم تقديم المجرم إلى العدالة والضبط في معظم الأحوال يكون هو الغرض الأساسي من التفتيش، حيث يستعملون الأدلة التقنية "**كالدليل الرقمي "أو "الدليل الإلكتروني" و** هو كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسب الآلي من إنجاز مهمة ما وإذا ما ربطنا هذه الجريمة نقول أنّ الدليل الرقمي هو الذي يجد لها أساس في العالم الافتراضي ويقود إلى الجريمة .

فتناول المشرع الجزائري هذا النوع من الجرائم من خلال قانون 06-23 الذي تضمن في مواده عقوبات ردعية أصلية وتكميلية تطبق على الشخص الطبيعي، حيث يتضمن جريمة المساس بأنظمة المعالجة الآلية للبيانات والمعطيات التي جاء لها في مواده من 394مكرر إلى 394مكرر7 من قانون العقوبات الجزائري.

الخـــــاتمة

إن الأهمية المتزايدة للتجارة الإلكترونية، أصبحت تقتضي ضرورة التدخل القانوني لتوفير الحماية اللازمة لهذه التجارة الإلكترونية من جرائم الاعتداء عليها، و بناءا على ذلك اهتمت التشريعات وخاصة المقارنة بتوفير حماية جنائية للتجارة الإلكترونية سواء في نصوص عامة أم خاصة.

وعليه جاءت دراستي للحماية الجنائية للتجارة الإلكترونية من خلال ثلاثة فصول تناولت في الفصل التمهيدي ماهية عقد التجارة الإلكترونية وتحديد زمان ومكان إبرام العقد الإلكتروني، أمّا الفصل الأول فخصص الحماية الجنائية الإجرامية للتجارة الإلكترونية قبل مرحلة المحاكمة في مرحلتي البحث والتحقيق الابتدائي، وفي مرحلة المحاكمة من خلال تحديد المحكمة الجنائية المختصة وسلطة المحكمة الجنائية في قبول وتقدير الأدلة الإلكترونية، في النصوص العامة المتعلقة بجرائم الأموال وجريمة التزوير، والنصب والاختلاس، ومن خلال النصوص الخاصة بالمواقع والبيانات الشخصية لوسائل التجارة الإلكترونية.

وتوصلت من خلال الدراسة إلى أن أحكام القضاء في العديد من الدول على اعتبار المعلومات مالاً في مفهوم جرائم الأموال، وبالتالي تطبق عليه نصوص جرائم الأموال، إلاّ أنّها توفر الحماية الكافية للمعلومات من جريمة الإتلاف، بخلاف بقية نصوص جرائم الأموال الأخرى والتي توفر حماية نسبية وغير كافية للمعلومات، ممّا حدا بالبعض إلى الدعوة لضرورة تدخل تشريعي لحسم هذا الخلاف أو بسط حماية جزائية مباشرة بواسطة نصوص خاصة وهو ما تحقق بالنسبة لجريمة الإتلاف المعلوماتي التي نصت عليها العديد من التشريعات في نصوص خاصة كالتشريع الفرنسي والإنجليزي والجزائري والتونسي وغيرها من التشريعات.

جاء التشريع الفرنسي بحماية جنائية لمواقع التجارة الإلكترونية كنظام معلوماتي، وكانت تلك الحماية متوازنة من خلال توزيع نطاقها، وتقرير عقوبات مناسبة وردعية، لكنها دون أن تكون مشمولة بحماية فنية، كما وفر التشريع الأمريكي حماية جنائية لها باعتبارها نظم في جرائم الكمبيوتر، لكنه اهتم بالتفاصيل أكثر لأنّه يمس بالأمن القومي والجانب

الاقتصادي، ولم يجرم مجرد الدخول بل تطلب أن يتعلق الأمر بمعلومات متعلقة بمصالح الدولة العليا، كما وفرت بعض التشريعات العربية كالتشريع الجزائري والتونسي حماية للمواقع في إطار جرائم الاعتداء بل أنظمة المعطيات في التشريع الفرنسي، وشملت تلك الحماية عدة جرائم لكنها تضمنت عقوبات غير ردعية، كما خصت بعض التشريعات العربية كالتشريع الجزائري في إطار قانون 09-04 والتشريع التونسي في إطار قانون المبادلات والتجارة الإلكترونية لسنة 2001، وتعد تلك الجمهور خطوة جريئة، لكنها تظل غير كافية من ناحية أنّها ضيقت في نطاق المسؤولية الجنائية وقصرتها على جرائم قليلة، وتفتقر إلى عقوبات مناسبة خاصة في جريمة الإفشاء، لم يخص التشريع الفرنسي والجزائري التوقيع الإلكتروني بحماية جنائية خاصة، بل يمكن حمايته في إطار القواعد العامة لقانون العقوبات من خلال جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، وجريمة التزوير، وكذلك الحال بالنسبة للتشريع الفيدرالي الأمريكي من خلال جرائم الكمبيوتر، إلاّ أن تلك الحماية قاصرة كما أسلفنا على مصالح الدولة العليا أو إحدى المؤسسات الاقتصادية.

حاول الفقه والقضاء توفير حماية جنائية لبطاقات الوفاء والائتمان، لكن في الحقيقة أن النصوص القائمة وإن كانت توفر حماية قدراً من الحماية الجنائية لبطاقة الوفاء من الاستخدام غير المشروع لبطاقة الوفاء من قبل حاملها، إلاّ أنّها توفر حماية غير كافية من بعض الجرائم المحدودة فقط، كحالة امتناع حامل البطاقة عن البطاقة الملغاة هي جريمة خيانة الأمانة وأيضاً في حالة تواطؤ حاملها مع التاجر فإنهما يتساءلان جزائياً بجريمة النصب والاختلاس على الرغم من هذه الحماية الجنائية التي توفرها النصوص القائمة من خلال جريمة السرقة والنصب والتزوير واستعمال محرر مزور، إلاّ أن الأمر بحاجة إلى تدخل تشريعي لتحريم بعض الصور كتجاوز الحامل لرصيده أو تقليد البطاقة الصور، وذلك بتعديل النصوص القائمة كما هو الحال في التشريع الكندي، الصادر عام 1985 والتشريع الأسترالي لعام 1983.

بالإضافة إلى الإشكاليات القانونية الموضوعية التي أثارتها جرائم التجارة الإلكترونية، أثارت بعض الإشكاليات الإجرائية، إذ أن التحقيق والبحث في جرائم الانترنت لا سيما جرائم التجارة الالكترونية وملاحقة مرتكبيها يتم بصعوبة وتعقيد بالغبن، ممّا أدى إلى ظهور تحدي كبير لأجهزة الضبط القضائي سواء على المستوى الدولي أو المستوى الوطني نتج عنه بعض الصعوبات التي تعيق عمل هذه الأجهزة وفي إطار تدعيم دور الضبطية القضائية في مكافحة الجرائم المعلوماتية، منح المشرع الجزائري سلطات لضباط أو أعوان الشرطة القضائية المكلفين بالتسرب، أو بعد وقف أو انقضاء مدة التسرب، تتمثل في انعدام المسؤولية الجنائية ومعاقبة كل من يكشف عن هوية المتسرب بالإضافة إلى ذلك تبنى المشرع الجزائري المراقبة الإلكترونية في المادة 04من قانون 09-04 المتعلق بالقواعد الخاصة، بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في بعض الجرائم الخطيرة كحالة الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو الجرائم الماسة بأمن الدولة، أو في حالة توفير معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، أو الوطني أو الدولي.

ومن خلاصة ما توصلت إليه يمكن ذكر جملة ذكر النتائج والتوصيات الهامة التي قد تساهم في التقليل من الآثار السلبية لكثير من التحولات الأمنية المصاحبة لوسائل الاتصال الحديثة لجرائم التجارة الالكترونية ومن بينها:

1- تشجيع الباحثين بالدعم المعنوي والمادي لإجراء المزيد من البحوث والدراسات حول الجرائم المستحدثة وتطبيقات الحاسوب والجرائم المرتبطة به.

2-خلق ثقافة اجتماعية جديدة تصور الجرائم الإلكترونية على أنّها أعمال غير مشروعة مثلها مثل أنماط الجريمة الأخرى والتأكيد على أن مجرم الانترنت يستهدف الأضرار بالآخرين ويستحق العقوبة.

3-تعديل بعض التشريعات على المستوى الدولي بما يتلاءم مع طبيعة جرائم الانترنت والتقنية وتثقيف العاملين في الجهات ذات العلاقة الدولية.

4-تشجيع الخبراء في مجال تقنيات الحاسب والبرمجيات من خلال تشفير البيانات وترميزها.

5-على المشرع الجزائري سن قواعد وقوانين ردعية لقراصنة السطو على الأنظمة المعلوماتية وفرض عقوبات وغرامة مالية لكل المخترقين.

6-وضع وسائل تقنية تحد من ظاهرة الجريمة الإلكترونية مثل: التوقيع الإلكتروني الذي أن يكون من المستحيل تقليده أو تزويره، وذلك لأن خبراء الحاسوب وضعوا له وسائل فنية فعالة للحماية من الاختراق.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولاً: المصادر.

- القرآن الكريم
- السنة النبوية

ثانياً: المراجع.

أ- المراجع العامة

1- أسامة أبو الحسن مجاهد، الوسيط في قانون المعاملات الإلكترونية، الكتاب الأول، دار النهضة العربية، القاهرة، سنة 2007.

2- أحمد عبد الكريم سلامة، القانون الدولي الخاص النوعي (الإلكتروني، السياحي)، دار النهضة العربية، الطبعة الأولى، سنة 2002.

3- عبد الأحد جمال الدين، النظرية العامة للجريمة، دار الثقافة الجامعية، القاهرة، سنة 1993.

4- عبد الرزاق السنهوري، الوسيط في شرح القانون المدني المصري، الجزء الأول، مصادر الالتزام، دار النهضة العربية، القاهرة، سنة 2000

5- د. عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، نظرية الالتزام بوجه عام، مصادر الالتزام، دار الأحياء التراث العربي، الجزء الثاني، بيروت ،لبنان سنة 1973.

6- د.عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، الجزء الرابع، الجزء الرابع العقود التي تقع على ملكية البيع والمقايضة، دار النهضة العربية، الطبعة الثانية، سنة1986

7- د.عبد الله سليمان، شرح قانون العقوبات الجزائري، القسم العام، ديوان المطبوعات الجامعية، الجزائر، الطبعة السادسة، سنة 2005.

8- د.فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية للنشر والتوزيع، الطبعة الثالثة، القاهرة، سنة 1982.

ب- الكتب المتخصصة.

1- د.إبراهيم الدسوي أبو الليل، إبرام العقد الإلكتروني، في ضوء أحكام القانون الإماراتي والقانون المقارن، بحث مقدم إلى مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي26-28. أبريل، سنة 2003.

2- د. إبراهيم الدسوي أبو الليل، الجوانب القانونية للتجارة الإلكترونية مصر القاهرة 2000.

3- د.أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، الحماية الجنائية، للحاسب الآلي، دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، الطبعة الأولى، القاهرة، سنة2000.

4- د.أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الطبعة الأولى، الجزائري.

5- د.أسامة أبو الحسن مجاهد، خصوصية العقد عبر الانترنت، بدون دار النشر، القاهرة سنة2000م

6- د.الطاهر شوقي مؤمن، عقد البيع الإلكتروني، الطبعة الأولى، دار النهضة العربية، الإسكندرية،2007.

7- د.إيمان مأمون أحمد سليمان، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه: حقوق المنصورة، سنة 2006.

8- د.بيل جيتش، المعلوماتية بعد الإنترنت، طريق المستقبل ترجمة عبد السلام رضوان، سلسلة علم المعرفة الكويت ، العدد 231.

9- د.جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دراسة تطبيقية في القضاء الفرنسي والمصري، دار النهضة العربية للنشر والتوزيع، القاهرة، سنة 2000

10- د.حاتم عبد الرحمان منصور الشحات، الإجرام المعلوماتي، دار النهضة العربية، للنشر والتوزيع، القاهرة، سنة2002.

11- د.حسين عبد الباسط جميعي، إثبات التصرفات القانونية التي يتم إبرامها عن طريق الانترنت، بدون طبعة، دار النهضة العربية، القاهرة، سنة 2000.

12- د.رأفت رضوان، عالم التجارة الإلكترونية، المنظمة العربية للتنمية الإدارية سنة1999.

13- د.سعيد السيد قنديل، التوقيع الإلكتروني، دار الجامعة الجديدة للنشر، الإسكندرية، سنة 2004.

14- د.شربل غريب، موسوعة التجارة والمال وإدارة الأعمال التجارية الإلكترونية المجلد الثامن، دار نوبليس، الطبعة الأولى، 2008.

15- د.شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة مصر، بدون طبعة، سنة 2007.

16- د.طارق عبد العال للتجارة الإلكترونية، المفاهيم والتجارب والتحريات والأبعاد التكنولوجية والمالية والتسويقية والقانونية، الدار الجامعية للنشر، القاهرة، الطبعة الأولى، سنة2003.

17- د.عبد الفتاح بيومي حجازي، الحكومة الإلكترونية ونظامها القانوني، دار الفكر الجامعي، الإسكندرية، 2006.

18- د.عبد الفتاح مراد، شرح قوانين التوقيع الإلكتروني في مصر والدول العربية، شركة البهاء للبرمجيات والكمبيوتر والنشر الإلكتروني، الإسكندرية، سنة 2004.

19- د.عبد الكريم أحمد سلامة، القانون الدولي الخاص النوعي، الإلكتروني، السياحي البيئي، دار النهضة العربية، الطبعة الأولى، 2002

20- د.عبد الله حسين محمود، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات، عن موقع:

21- د.عبد الله سليمان، شرع قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزائر، الطبعة السادسة، 2005.

22- د.عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت(الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، الطبعة الثانية، بيروت2007.

23- د.عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دور الشرطة والقانون، دراسة مقارنة، بدون دار النشر القاهرة، سنة 2000.

24- د.عماد الحداد، التجارة الإلكترونية إعداد اللجنة العلمية للتأليف والنشر والتحرير، دار الفاروق للنشر والتوزيع، الطبعة الأولى، سنة 2004.

25- د.عمر أبوبكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، الطبعة الثانية، القاهرة، سنة 2004.

26- د.عمر الفاروق الحسني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، دراسة تحليلية ونقدية لنصوص التشريع المصري مقارنا بالتشريع الفرنسي، دار النهضة العربية، الطبعة الثانية سنة1995.

27- د.عمر محمد أبو بكر ، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، الطبعة الثانية، القاهرة، سنة2004.

28- د.فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية للنشر والتوزيع، الطبعة الثالثة، القاهرة، سنة 1982.

29- د.لزهر بن سعيد، النظام القانوني لعقود التجارة الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2010.

30- د.محمد أبو بكر بن يونس، الأحكام الموضوعية والجوانب الإجرامية، الجرائم الناشئة عند استخدام الانترنت، دار النهضة العربية، بدون طبعة، سنة 2004.

31- د.محمد السعيد رشدي، وسائل الاتصال الحديثة مع التركيز على البيع بواسطة التلفزيون، ديوان المطبوعات الجامعية، الكويت ، سنة 1998.

32- د.محمد أمين الرومي، التعاقد الإلكتروني عبر الانترنت، الطبعة الأولى، دار المطبوعة الجامعية، الاسكندرية، سنة 2004.

33- د.محمد أمين الشوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية، مكتبة دار الثقافة، للنشر والتوزيع، الطبعة الأولى، بدون بلد، سنة2004.

34- د.محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، سنة 2003.

35- د.محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية للنشر والتوزيع، الطبعة الثانية، القاهرة، سنة 2003.

36- د.محمد محي الدين عوض، القانون الجنائي، إجراءاته، الطبعة الأولى، جامعة القاهرة، والكتاب الجامعي، سنة 1981.

37- د.محمد نجيب حسني، شرح قانون العقوبات، القسم الخاص، مطبعة نادي القضاء، القاهرة، 1987.

38- د.محمود حسام محمد لطفي، الإطار القانوني للمعاملات الإلكترونية، النسر الذهني للطباعة، القاهرة، 2002.

39- د.مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، للنشر والتوزيع، القاهرة، سنة 2001.

40- د.مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، العدد11، مطابع الشرطة، القاهرة، الطبعة الأولى سنة 2001.

41- د.منير محمد الجنبيهي، جرائم الانترنت والحاسب الآلي، ووسائل مكافحتها دار الفكر الجامعي، الإسكندرية،سنة 2005.

42- د.نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2007.

43- د.هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، بدون طبعة، دار النهضة العربية للنشر والتوزيع، القاهرة، سنة1992.

44- د.هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، سنة 1994.

– القوانين:

1- القانون رقم 06-23المؤرخ في 2006/12/20المعدل والمتمم للأمر رقم 66-156المؤرخ في 08يونيو 1966(الجريدة الرسمية رقم 84 المؤرخة في 2006/12/24) المتضمن قانون العقوبات.

2- قانون رقم 06-23 المؤرخ في 20سبتمبر 2006، الدار البيضاء، الجزائر بدون طبعة، سنة2007.

3- الأمر رقم 09-04 المؤرخ في 14شعبان 1430الموافق لـ 25أوت 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ومكافحتها، الجريدة الرسمية رقم47 الصادرة بتاريخ 05 أوت 2009.

4- الجريدة الرسمية رقم 47، قانون رقم 09-04.

5- القانون رقم23/06 المؤرخ في 20ديسمبر 2006.

6- القانون رقم06-23 المؤرخ في 20ديسمبر 2006،ص 136.

7- المادة 135من القانون المدني المصري.

8- المادة 276 من القانون الجزاء العماني.

9- المادة 276مكرر من القانون الجزاء العماني، الفقرة التاسعة منه.

10- المادة 2فقرة ب من القانون النموذجي لليونيسترال للتجارة الإلكترونية لسنة 1996.

11- المادة 350من القانون رقم 06-23المؤرخ في 20ديسمبر2006 المتضمن قانون العقوبات الجزائري

– الاتفاقيات والمؤتمرات:

1- المادة 8 الفقرة 1 من اتفاقية فينا لسنة 1980الخاصة بالبيع الدولي للبضائع، وهي مصادقة عليها من طرف الجزائر، وهذا ما ذهب إليه المشرع الجزائري في المادة 68 من القانون المدني الجزائري.

2- المادة 2 فقرة من قانون النموذجي لليونيسترالي للتجارة الإلكترونية سنة 1996.

3- عبادة أحمد عبادة، التدمير المعتمد لأنظمة المعلومات، الإلكترونية، مؤتمر مركز دعم القرار،ندوة بعنوان المواجهة الأمنية للجرائم المعلوماتية، مطابع الشرطة، الطبعة الأولى، دبي، سنة2005.

4- نجاح فوزي، نماذج من جرائم بطاقات الدفع الإلكتروني، ورقة عمل مقدمة إلى ندوة الصورة المستحدثة لجرائم بطاقات الدفع الإلكتروني، التي نظمها مركز بحوث الشرطة بأكاديمية القاهرة، في 14 ديسمبر 1998.

5- الرائد حسين على عباس، مخاطر استخدام بطاقة الدفع الإلكتروني عبر شبكة الانترنت، المشاكل، الحلول، ورقة عمل مقدمة إلى ندوة الدور المستحدثة لجرائم بطاقات الدفع الإلكتروني، التي نظمها مركز بحوث الشرطة بأكاديمية في 14ديسمبر 1998.

6- د.هلال عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الحجائية، مؤتمر الفانون والكمبيوتر والانترنت، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة طبعة، سنة 2000.

-رسائل دكتوراه:

1- د.إيمان مأمون أحمد سليمان، الجوانب القانونية لعقد التجارة الإلكترونية، رسالة دكتوراه، حقوق المنصورة، سنة 2006.

2- د.شيماء عبد الغني، محمد عطاء الله، الحماية الجنائية للتعاملات الإلكترونية، دراسة مقارنة بين النظام اللاتيني والأنجلو أمريكي، رسالة دكتوراه، جامعة المنصورة، سنة 2001.

المراجع الفرنسية والإنجليزية:

1- Bensoussan (A)Le commerce électronique, aspects juridiques éd. Hermas , Paris 1997.

2- Tourres(CH);Internet et La vente aux consommateurs thése de doctorat Université de paris X , Nanterre , présentée en 1996.

3- -HUET (J), La Valeur juridique de la télécopie (au fax) , comparée aux télex ,D,S,1992, doctrine, N05.

4- François (c) et PHILIPE (D), contrats civils et contrats commerciaux, 7 ème édition DALLOZ, 2004.

5- Behjamin Wright, janek winn, the law of electronic commerce adivision of Aspen publishing INC NEW York, USA ,third edition,2000.

6- Department of justice / us Attorney General , Northern, District of Texas, available online in Oct, 2000.
www.Httpll//usdoj,gov/criminal/cybercrime/phonmast.h.tm.

7- Prof.dt. henrik.wk.kas persen.crimes related tot he computer net work, threats and apportunities, a criminological perspective.

- مواقع إلكترونية:

1- Aup CLE(N) les infraction , h 33 , P23

2- htt://www.arab la winfo.com/research earch.asp ?validate: articles, ID=148

3- htt://www.quatar.com/VB/showheard php ?t=20845. عن موقع

4- منتدى جامعة قطر كلية القانون مراحل إثبات الجريمة الإلكترونية

الفهـــــرس

الفهرس