جامعة د. مولاي الطاهر – سعيدة –
كلية الحقوق و العلوم السياسية
قسم الحقوق

الحماية الجنائية للتجارة الإلكترونية

مذكرة لنيل شهادة الماستـر

التخصص: قانون اقتصـادي

من إعداد الطالبة: جيدي فارحة
تحت إشراف الأستاذ:

عثماني عبد الرحمان

لجنة المناقشة:

الأستاذ:.....عياشي بوزيان .....رئيسا

الأستاذ:.....عثماني عبد الرحمان.....مشرفا و مقررا.

الأستاذ:.....هني عبد اللطيف.....عضوا مناقشا

الأستاذ:.....فليح محمد عبد الفتاح.....عضوا مناقشا

السنة الجامعية:2016/2015

شكر وعرفان

خير ما نبدأ به هو شكر المولى عز و علا ، فانا نحمده و نشكر فضله فقد من علينا بنعمة العلم و وفقنا في انجاز هذه المذكرة و ما كان التوفيق حليفنا إلا برضاه عز وجل .

اللهم لا تجعل الدنيا أكبر همنا ، و لا مبلغ علمنا ، و لا تسلط علينا من لا يخافك و لا يخشاك

الحمد لله الذي وصبنا التوفيق ، كما نتقدم بالشكر الجزيل إلى الأستاذ المؤطر " عثماني عبد الرحمان " الذي لم يبخل علينا بما انعم الله عليه من علم و ما قدمه لنا من نصائح و توجيهات قيمة .

و في الأخير الشكر و الثناء لكل أساتذة العلوم القانونية و الإدارية و الطاقم الإداري بما فيهم عمال المكتبة .

إهـــــداء

- إلى القلب الذي برحمته رعاني، والنبع الذي من فيضه سقاني، إلى صدري بعمق البحر ضمني إليه في كل أفراحي وأحزاني، إليك ياملكة عرشي، ولحن شفتي، يامنبع الحب والحنان إلى روح أمي الغالية رحمها الله

- إلى الذي مع كل فجر أترقب خطاه، وأتحسس رضاه، مع كل صلاة أرجو دعواه، إلى مرشدي الذي علمني كيف أحب الله وأحب الحياة
الى روح أبي العزيز رحمه الله
إلى من حرص على رؤيتي متفوقة أستاذي الكريم: عثماني عبد الرحمان
إلى أغلى شيء في الوجود، إلى نبض قلبي ونور عيني إخوتي

إلى رفيقات دربي في العمل : أمينة شريفي، ثابتي فضيلة

إهـــداء

كن عالما فان لم تستطع كن متعلما ، فان لم تستطع أحب العلماء ، فان لم تستطع لا تبغضهم .أهدي ثمرة هذا العمل إلى كل إنسان إذا كانت غايته الله ، و إلى كل عقل إذا كانت غايته الإنسانية ، و إلى كل سعي اذا كانت غايته الجميع للجميع .

إلى كل من قال في حقهما الرحمن " و بالوالدين إحسانا "

إلى رمز الاحترام و الوقار ، و من أحمل اسمه بكل عز و افتخار والدي الغالي رحمه الله

إلى منبع الأمل ، العطف ، الوفاء ، العطاء ، و الحنان و من حفظتني بدعائها الصالحة أمي العزيزة رحمها الله .

إلى أملي و سندي في الحياة زوجي الغالي و عائلته و الى قرة عيني هاجر و فلذة كبدي عمر الفاروق وإلى إخوتي و أخواتي الأعزاء حفظهم الله و أطال أعمارهم .

إلى العائلة دون ذكر الأسماء

إلى صديقات المشوار الجامعي

إلى كل من حرص على رؤيتي متفوقة : بن تاج لخضر، بن سكران ليلى

مقدمة.....01
الفصل الأول
خصائص التجارة الإلكترونية و أنواعها**.....05**
المبحث الأول :*خصائص التجارة الالكترونية عبر الانترنت*.....06
المطلب الأول :*:تعاملات الالكترونية الرقمية لا مادية*.....06
المطلب الثاني :*علاقات التجارة الالكترونية ذات طبيعة دولية*.....06
المطلب الثالث: *التجارة الإلكترونية مفهوم قانوني و تطبيق تجاري جديد*.....07
المبحث الثاني :*أنواع التجارة الإلكترونية عبر الإنترنت*.....09
المطلب الأول: *التجارة الإلكترونية فيما بين المهنيين*.....09
المطلب الثاني: *التجارة الإلكترونية مع المستهلكين*.....10
المطلب الثالث: *: التجارة الالكترونية الحكومية*.....10
المبحث الثالث: مواجهات الاعتداءات الواقعة على أموال التجارة الالكترونية.....12.
المطلب الأول: ماهية جريمة السرقة الالكترونية.....13
الفرع الأول: مفهوم جريمة السرقة الالكترونية.....13
الفرع الثاني: أركان جريمة السرقة الالكترونية.....18
المطلب الثاني: خصائص مرتكب الجريمة الالكترونية.....24
الفرع الأول: صفات المجرم الالكتروني.....24
الفرع الثاني: أنواع المجرمين مرتكبي جرائم الانترنت.....24

المطلب الثالث: ماهية جريمة النصب الالكتروني.....25
الفرع الأول: مفهوم جريمة النصب الالكتروني.....26
الفرع الثاني: أركان جريمة النصب الالكتروني.....29
الفرع الثالث: دوافع ارتكاب الجريمة الالكترونية.....33
الفصل الثاني
وسائل حماية التجارة الالكترونية.....32
المبحث الأول: المبحث الأول: الطرق الوقائية.....33
المطلب الأول : المطلب الأول : تشفير البيانات.....33
الفرع الأول: تعريف التشفير الالكتروني وأهميته.....33
الفرع الثاني :الفرع الثاني: صور التشفير الالكتروني.....35
المطلب الثاني: المطلب الثاني: التوقيع الالكتروني.....36
الفرع الأول: الفرع الأول: تعريف التوقيع الالكتروني ومدى تعليقه بالنظام العام.....37
الفرع الثاني: صور التوقيع الالكتروني.....39
المبحث الثاني: الوسائل الردعية.....42
المطلب الأول: المعطيات الأساسية للجريمة المعلوماتية و مراقبة الاتصال.....43
الفرع الأول: أحكام عامة.....43
الفرع الثاني: مراقبة الاتصالات الالكترونية.....44
المطلب الثاني: القواعد الإجرائية و التزامات مقدمي الخدمات.....45

الفرع الأول : القواعد الإجرائية تفتيش المنظومة المعلوماتية**.....45**
الفرع الثاني : التزامات مقدمي الخدمات بمساعدة السلطات.....46
المطلب الثالث : الهيئات الوطنية و الدولية المختصة في مكافحة الإجرام المعلوماتي48
الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاتصال.....48
الفرع الثاني : التعاون و المساعدة القضائية الدولية "الاختصاص القضائي.....48
الخاتمة:.....68
قائمة المصادر و المراجع:.....70
فهرس الموضوعات:.....72.

المقـــــــــــــــدمـــــــــــــــة:

نعيش اليوم في عصر يتميز بالسرعة الفائقة في كل المجالات ، بتدخل التكنولوجيا الحديثة للمعلومات والاتصال في القضايا التي تخص الكون بأجمله وبالأخص الإنسان ، الذي يعتبر المؤثر و المتأثر الرئيسي ، سواء كانت قضايا سياسية ، اجتماعية ،ثقافية أو اقتصادية ومن أهم آثارها هي تطوير اقتصاد المعرفة ، حيث ظهرت الحاجة إليه منذ انهيار مبادئ المدرسة الكلاسيكية من شفافية المعلومات ، والعقلانية المطلقة، فعرفت المنشآت بكل أنواعها وخاصة الاقتصادية أنه لا يمكن تحقيق أهداف الاستراتيجيات الموضوعة إلا بتوفر المعلومات ،المعارف ،الكفاءات و الخبرات وأن الاهتمام بداخل المنشأة أو محيطها القريب والذي له تأثير مباشر عليها لم يعد ذو جدوى كبيرة للوصول لأهدافها وتحقيق ميزة تنافسية تجعلها تحافظ على مكانتها لأمد طويل وتسمح بتطورها وإحداث التجديد باستمرار . وهذا ما يرتكز عليه الاقتصاد اليوم ، أي اقتصاد المعارف أو الاقتصاد المبني على المعرفة ،والذي يعتمد على تكنولوجيا المعلومات والاتصال بشكل كبير في أداء مهامه.

كما انه من الملاحظ وجود تسابق اقتصادي بين القوى الاقتصادية العالمية في مجال التجارة الالكترونية هذا المجال الذي لا تزال الدول النامية غافلة عنه ولهذا يجب عليها محاولة الإسراع في تطوير اتصالاتها في مجال الانترنت للتأقلم ومحاولة مسايرة الأوضاع الاقتصادية العالمية.

ومن خلال التنقيب عن المعلومات ارتأينا تقسيم هذا المبحث إلى ثلاثة مطالبين تناولنا في المطلب الأول بنشأة وتعريف التجارة الالكترونية وفي المطلب الثاني مزايا التجارة الالكترونية و عوامل نجاحها.

للحديث عن نشأة التجارة الالكترونية يجب الحديث عن نشأة الانترنت قبل كل شيء قد كان أول ظهور لعالم الانترنت في أواخر الستينيات زمن الحرب الباردة، إضافة إلى

التطور الاجتماعي والاقتصادي عرف العالم ثورة رقمية كان لها الأثر الكبير على جميع الدول وبالأخص المتطورة منها ومن هنا اعتمدت الولايات المتحدة الأمريكية ممثلة في وزارة الدفاع الأمريكية البنتاغون حيث طرحت فكرة التواصل الدائم وغير المنقطع بين القيادة العسكرية وجهاز داربا[1]، وهو جهاز تمويل مالي لقطاع الأبحاث العسكرية الأمريكية وهذا الأخير أسس لتمويل برنامج أو مشروع لصناعة شبكة معلوماتية تنمي دار بانت تربط الولاية المتحدة الأمريكية بالمعسكر الغربي كانت هذه الشبكة تتكون من مجموعة من الحواسيب المركزية يربط بينها هاتف خط صوتي راديو أقمار اصطناعية بحيث تدمير دارة من الشبكة لا يؤثر في شيء وهنا ظهر الانترنيت بميزة أساسية وهي استعمال بروتوكول موحد يتم فيه تبادل المعلومات بين الجوانب يقصد به Inter Cimmected تسمح للمرسل إليه بمعرفة كل أنواع الرسائل حسب عنوان الإرسال مهما كان اتجاه الرسائل وبهذا كان الانترنت عابرا للحدود الجغرافية وهنا يظهر لنا مشكل الاختصاص القانوني.

لقد بدأ ظهور التجارة الالكترونية في النصف الثاني من تسعينات القرن الماضي حيث بدأت الشركات تستثني موقع لعرض منتجاتها ووسائل الاتصال بينها فانتقلت الأعمال من تبادل الرسائل والإعلان عن المنتجات إلى نشاط والترويح والبيع ومن تم اختيار البضائع ومراسلة البائع الذي يقوم بإرسال البضائع وتحصيل قيمتها عند التسليم ومن هنا ظهرت الحاجة إلى التأمين والسرية، فأنشأت إجراءات التأمين وتوثيق مواقع الشبكة من حفظ معلومات العملاء والتصفح والشراء فأصبحت العملية التجارية تتم عبر الانترنت، فستخدم بطاقات الائتمان في دفع قيمة البضائع من طرف المشتري أما البائع فيتحصل على قيمة البضائع عبر الشبكة.

[1] - universities darpa net: advanced resaerche projet agency 1969 par la liaison de quatre amesicaines

ومن أهم ما نتج عن اندماج وتلاصق اقتصاد المعرفة بتكنولوجيا المعلومات والاتصال هو التجارة الالكترونية التي تعتمد على اقتصاد المعارف في صلب عملها وتغير مستوى الاهتمام وترتيب أهمية السلع المتاجر بها ، حيث كانت تعطى أكبر أهمية للسلع المادية الملموسة وذات الأحجام الكبيرة ،فأصبحت إلى السلع الرقمية ،و المتاجرة بالمعلومات وخدمة مجال الخدمات اللاملموسة ،تحتل المرتبة الأولى في اهتمامات المنتجين ثم تليها السلع المادية، وهذا ما أعطى الأهمية القصوى لاستعمال التجارة الالكترونية بالإضافة إلى التسهيلات الكبيرة والسرعة الفائقة في أداء الأعمال التي تكلف الجهد والأموال الطائلة عند استعملاها للتجارة التقليدية .

وبعد أن كانت الشركات التجارية تعرض فقط مواقع، أصبحت لها مواقع متنقلة dot com ليست تابعة لشركات الإنتاج أو البيع تقوم بعرض منتجات عدة منجين، ليقوم المستهلك بالتسويق من خلالها[1]،من ثم بدأت الأعمال الالكترونية بين الشركات عبر الانترنت، "الصفات، العقود" إلى أن نشأت أسواق رقمية منها: أسواق تجمع بين شركات ذات نشاط متشابه "صناعة السيارات" ومنها ما هو مخصص للخدمات "التأمين، الخدمات المالية والمصرفية" ومن هنا زاد عدد الشركات الصغيرة المتوسطة والكبيرة الجامعة الاتصالات والأبحاث والمؤسسات الدولية والمنظمات" بعضها يغطي عدة أقطار من العالم ولقد كان البروتوكول المشترك الذي يجمع بينها هو الانترنت وأفضل مثال على التسويق للتجارة الالكترونية شركة أمازون[2]التي أسسها "جان بيزوس" سنة 1994 وقد كان يبلغ من العمر آنذاك 29سنة ويعمل محلل مالي ومدير صندوق مالي، بدأ تجارته الالكترونية بتجارة الكتب ثم عام1998 باشر بتجارة الشرائط الموسيقية وشرائط الفيديو ثم بيع الأجهزة المنزلية والفنون والالكترونيات، ومن هنا

---

[1] - جبوري فتيحة، حداد خيرة، الحماية القانونية للتجارة الالكترونية، مذكرة تخرج لنيل شهادة الليسانس في العلوم القانونية و الإدارية، سعيدة 2007 – 2008 ، ص: 10.

2 - شافع بلعيد عاشور، العولمة التجارية والقانونية للتجارة الالكترونية، دار هومه للطباعة والنشر والتوزيع، الجزائر، سنة 2006.

كانت شركة أمازون كواحدة من قصص النجاح الأولية الملموسة بدرجة كبيرة في مجال التجارة الالكترونية وظهرت المشكلة الكبرى فكون الشخص الطبيعي له قدرة تسيير موقعه التجاري على الانترنيت من أي موقع في العالم ما جعل الفقهاء والمشروعين يواجهون تحديا لمحاولة بلورة مفهوم قانوني للتجارة الالكترونية.

من هذا المنطلق رأينا الحاجة الماسة لدراسة التجارة الالكترونية و كيفية حمايتها جنائيا ومحاولة إجلاء الغموض عنها خاصة وأن البلدان النامية كالجزائر مثلا لا تزال بعيدة عن أداء واستغلال فوائد التجارة الالكترونية الحقيقية و أن تحاول القضاء على صعوبات التجارة الالكترونية ،والتي ترجع في الحقيقة إلى صعوبة التحكم في أخلاقيات مستعمليها لا فيها هي كأداة لممارسة التجارة بشكل أسهل وأسرع بكفاءة عالية ، وكما نعلم أن هذه المشاكل الأخلاقية نواجهها حتى في التجارة التقليدية فالتجارة الالكترونية هي مجرد وسيلة يجب معرفة كيف نستغلها[1].

و لتحديد مدى قدرة القواعد التقليدية لقانون العقوبات على التأقلم مع الوسط التكنولوجي الجديد و ما ان كان يمكن إخضاع التجارة الالكترونية لهذه القواعد دون أن يظهر ذلك عجزها؟أم أنه يجب هجر مثل هذه القواعد و البحث عن إطار جديد للحماية الجنائية للتجارة الإلكترونية؟

و عليه للإلمام بموضوع الحماية الجنائية للتجارة الالكترونية ،و ما يثيرة من مشاكل نظرية

و علمية إجابة على الإشكالية التي وضعناها للموضوع فان دراستنا ستكون من خلال فصلين أساسيين حيث انه خصصنا الفصل الأول لخصائص التجارة الالكترونية و أنواعها،لنتناول في الفصل الثاني لحماية أموال التجارة الالكترونية جنائيا.

1- عبد الحميد بسيوني، عبد الكريم عبد الحميد بسيوني ، التجارة الالكترونية ، دار الكتب للنشر و التوزيع ، بدون طبعة، سنة 2003، ص 55/54.

الفصل الأول:خصائص التجارة الإلكترونية و أنواعها:

بالرغم من الاختلاف الفقهي و القانوني الحاصل حول تعريف التجارة الالكترونية ،إلا أن ذلك لم يمنع من أن يجمع الجميع حول خصائصها،خاصة فيما يتعلق بتجاهلها لمفاهيم الحدود و الوقت و كسرها للحواجز الجغرافية،بالنظر إلى اعتمادها على وسائط إلكترونية غيرت كثيرا من هذه المفاهيم و أحلت أخرى لم يكن لنا معها عهد إلى وقت قريب من الزمن،كما تنوعت صور استعمالاتها و استغلالها سوف نتطرق في المبحث الأول خصائص التجارة الالكترونية عبر الانترنت و في المبحث الثاني أنواع التجارة الالكترونية[1].

المبحث الأول: خصائص التجارة الالكترونية عبر الانترنت

إن أبرز مميزات التجارة الالكترونية، هي أنها عبارة عن بيئة تجارية حديثة،اعتمدت في ظهورها و نشأتها على بيئة أخري تقنية أكثر حداثة ،هي بيئة

1- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادي، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2005، ص:123.

الإنترنت،التي أضفت لأول مرة وصف "الالكتروني"على كل ما يتم عبرها أو من خلالها، مما أضفى على التجارة موضوع البحث عن الحماية الجنائية في دراستنا ،مفهوما تجاريا و تقنيا جديدين و تميزت بمجموعة أو جملة من الخصائص سنركز على أهمها من ناحية النتائج و الآثار القانونية على جوانب موضوع دراستنا[1]:

المطلب الأول:تعاملات الالكترونية الرقمية لا مادية

مع التجارة الإلكترونية عبر الانترنت،زالت الدعائم اليدوية التقليدية المتمثلة أساسا في الورق

و حلت محلها دعائم إلكترونية رقمية حديثة،و كتابة إلكترونية رقمية تحمل على هذه الدعائم عوض الكتابة اليدوية التقليدية،و بالتالي حلت المستندات الإلكترونية كسند قانوني جديد لعالم التجارة الإلكترونية.و هو ما سهل كثيرا من إتمام عمليات التجارة الإلكترونية،غير أنه أثار العديد من الصعوبات بخصوص أمن تبادل هذه المعطيات الرقمية و إضفاء الحماية الجنائية عليها.

المطلب الثاني: علاقات التجارة الالكترونية ذات طبيعة دولية.

بالنظر للوسيلة التي تتم عبرها التجارة الالكترونية "الانترنت"،التي سبق القول بأنها دولية مفتوحة ترفض الخضوع لأية سيطرة ،و لا تعترف بالحدود الساسية و الجغرافية للدول ،و إلغائها للحدود و الفواصل الزمنية و الجغرافية،فذلك جعل من

1- محمد أبوبكر بن يونس، الأحكام الموضوعية والجوانب الإجرامية، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، بدون طبعة، سنة2004، ص379 – 380.

التجارة الالكترونية تتسم بالطابع العالمي حتى و إن كان أطرافها يقطنون وطنا واحدا.و أصبحت بذلك علاقات التجارة الإلكترونية عبر الإنترنت تنساب بكل حرية،و تأبى أن تكون حبيسة حدود الدول ،بعدما أزالت من أمامها كل العقبات المادية و القانونية التي كنت تحول دون ذلك و جعلت منها علاقات مقترنة بفكرة التدويل و العولمة.أعجزت أهم أحكام القانون الجنائي المبنية على فكرة الحدود و الإقليمية و الكثير من التحديات القانونية لمختلف الفروع القانونية الأخرى.

المطلب الثالث: التجارة الإلكترونية مفهوم قانوني و تطبيق تجاري جديد

سبق القول بأن التجارة الالكترونية لا تعدو أن تكون مجرد تجارة تقليدية ،لكن تتم عبر ما أتاحته الإنترنت من طرق اتصال تقنية حديثة.و هو ما خلق جدلا فقهيا بين الفقهاء و الباحثين،حول ما إن كانت التجارة الالكترونية عبارة عن مفهوم تقني حديث أثار ضجة سياسية و إعلامية ؟

من جهة و من جهة ثانية، ما إن كانت علاقاتها مجرد علاقات تجارية، شأنها شأن العلاقات التجارية التقليدية،أم تطبيق تجاري جديد من نوع خاص؟

و استقر الرأي في نهاية المطاف، أنها مجرد تجارة تتم عن بعد، شأنها شأن البيع بالمراسلة المعروف منذ زمن،و أن وجه الجدّة الوحيد فيها، مسألة التوصيف الإلكتروني الذي لم يغير في المفهوم القانوني للتجارة.الأمر الذي لا يزال يستدعي الحماية القانونية خاصة الحماية الجنائية لهذا النوع من التجارة.وأن استعمال تكنولوجيا الاتصالات للقيام بالعمليات التجارية ،أمر جائز من الناحية القانونية ،وإن كان قد جعلتها لا تخلو في غالب الأحيان من عنصر النزاع،و هو الأمر الذي طرح

مسألة البحث عن إطار قانوني جديد لهذه التجارة ،و بشكل لم يسبق و أن أثير بهذه الجدّة[1] .

سيما مع ما واكب مزاياها و فوائدها من عيوب و أخطار تتعلق في مجمل بظهور أشكال جديدة من الإجرام ،الذي سمي بدوره بالإجرام المعلوماتي،الذي خلف الكثير من عمليات انتهاك لمواقع التجارة الالكترونية و سرقة بياناتها ووسائل دفعها بالإضافة إلى التخوف الكبير من الأفراد من عدم قدرة الأجهزة الأمنية على متابعة مجرمي الإنترنت الذين استغلوا التطورات التقنية في تطوير أساليبهم الإجرامية،و الأهم من كل ذلك غياب الإطار التشريعي المتعلق بالتجارة الإلكترونية ،الذي يعد العمود الفقري لقيامها،خاصة و أنه للاستفادة بأقصى حد من مزاياها،يجب أن يكون هناك تطور موازٍ و مواكب لتطوراتها من حيث الإطار القانوني ،أو على الأقل أن تكون القواعد القانونية الموجودة مرنة مرونة تسمح بمواكبة التطورات الحاصلة.

المبحث الثاني: أنواع التجارة الإلكترونية عبر الإنترنت

للتجارة الالكترونية ثلاثة أنواع رئيسية ،و ذلك بحسب أطراف علاقاتها ،و هي التجارة فيما بين المؤسسات أو المهنيين و التي سوف نتطرق لها في المطلب الأول،و الأحرى فيما بين هؤلاء

و المستهلكين هذا النوع سنراه في المطلب الثاني و أخيرا في المطلب الثالث نتكلم عن النوع التجارة الالكترونية الحكومية التي تتم عن طريق طرح مناقصات حكومية بالطرق الالكترونية[1].

1-عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، مصر، الطبيعة الأولى، 2006ص406.

المطلب الأول: التجارة الإلكترونية فيما بين المهنيين: business to business

هي تجارة تقدم بواسطة شبكات الاتصالات وتكنولوجيا لتقديم طلبات الشراء إلى مورديها وتسليم القوانين والدفع و تتم فيما بين المهنيين،أي بين تاجر و آخر و تسمى بالتجارة المتبادلة و هو النوع الأكثر انتشارا على الشبكة،بحيث تمثل أكثر من 90% من مجمل النشاطات التجارية الالكترونية عبر الإنترنت و هذا راجع لما حققته هذه التجارة من فوائد للمؤسسات و هذا النوع من التجارة يتم باستعمال احتياطات أمان للحفاظ على (خصوصية وسرية المعلومات ،صحة الرسالة التأكيد على مسؤولية البائع والمشتري نحو العقد .

كما أن فرص الربح التي توفرها التجارة الالكترونية فرص لا يمكن أن تحققها أي تجارة أخرى،سيما مع سرعة و قلة التكلفة التي تتميز بها،و السبب الرئيسي في تطور و نمو و ازدهار التجارة الالكترونية عبر الإنترنت،راجع لهذا النوع بالخصوص.

***المطلب الثاني: التجارة الإلكترونية مع المستهلكين Business to consumer* :**

منحت التجارة الالكترونية للمستهلكين فرص غير مسبوقة ،بحيث مكنتهم و هم جالسين ببيوتهم خلف أجهزتهم من تهافت التجار عليهم في كل ساعات اليوم و على مدار الأسبوع

و أمكنهم لإتمام تعاملاتهم من الضغط على زر الكمبيوتر لتنعقد الصفحة ،غير أن الدراسات بينت بأن هذا النوع من التجارة الإلكترونية لم يلق نفس التطور الذي عرفه النوع السابق،و ذلك راجع بالأساس إلى تخوف المستهلكين من كشف بياناتهم و أرقام بطاقاتهم بمناسبة معاملات لم تفهم من قبلهم بعد ،و اقتصرت تعاملاتهم بخصوصها على معاملات الاستهلاكية اليومية ،و لعل السبب الرئيسي في بحث بعض

[1]- عبد الفتاح بيومي حجازي، المرجع السابق، ص:163.

الدول عن صور الحماية فعالة للتجارة الالكترونية و خاصة الحماية الجنائية،هو لبث المستهلكين فيها و رفع تخوفاتهم بشأنها.

المطلب الثالث: التجارة الالكترونية الحكومية business ti gouvernement :

أمام الفوائد التي وفرتها التجارة الالكترونية عبر الإنترنت للمؤسسات و الأفراد،فان الدول

و الحكومات لم تفوت فرصة الاستفادة منها،سواء داخل الدولة ذاتها،أو في المجال الدولي مع غيرها من الدول و الحكومات، خاصة و أنه ثبت بأن تعاملات التجارة الإلكتروني ة ذات طابع دولي في الغالب،و ذات آثار اقتصادية كبيرة على نمو اقتصاديات الدول.لذلك كان من البديهي أن تعتمد الحكومات هذا النوع من التجارة لممارسة أنشطتها،إذ ليس من المعقول أن تسعى الحكومة بكل الوسائل و الإمكانيات لتوفير المناخ و البيئة المناسبة لتطوير و نمو التجارة الالكترونية ،و توفر لها البيئة القانونية و التشريعية اللازمة حتى يتسنى للأفراد ممارسة هذا النوع من النشاط بأمان و ثقة

و تستثني نفسها من استغلال فرصة تطوير اقتصادها عن طريق هذا النوع من التجارة[1].

و في ختام هذا المبحث يمكن القول أن الإنترنت وفرت الكثير من الإمكانيات للشركات

و المؤسسات التجارية و التجار ،ما لم توفره أية وسيلة من قبل ،و مكنت من الوصول للأسواق العالمية بمجرد ضغطه على زر المفاتيح في أي وقت على مدار

1- محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، مكتبة دار الثقافة للنشر والتوزيع، الطبعة الأولى، سنة 2004 ، ص:148-150.

السنة ،و من أي مكان في العالم مما شجع النشاط التجاري و العولمة ،و فتح أفاق كان يتعذر الوصول إليها من قبل.

المبحث الثالث: مواجهات الاعتداءات الواقعة على أموال التجارة الالكترونية.

لقد تعددت وسائل الاعتداء على الأموال التي أثارت جد لأحول مدى إمكانية تطبيقها على المعلومات، ما بين اختلاسها في حالة السرقة، أو تسليمها بعد إيقاع المجني عليه في غلط في حالة النصب، أو تبديدها في حالة خيانة الأمانة، أو الحصول عليها عن طريق التهديد أو الابتزاز، وحيازتها في حالة إخفاء الأشياء المتحصلة من جريمة، ومدى قابلية النصوص الخاصة بجريمة الإتلاف للتطبيق في حالة إتلاف المعلومات.

المطلب الأول: ماهية جريمة السرقة الالكترونية

لاشك أن لجريمة السرقة تطبيقاتها في مجال تكنولوجيا المعلومات، فأنظمة الحسابات الآلية تتضمن كثيرا من العناصر المادية (الحاسبات الآلية، الطابعات، الأقراص الممغنطة....الخ)، والتي تقبل بطبيعتها أن تكون محلا للسرقة.

إلا أن أنظمة الحسابات الآلية تتضمن مجموعة من البرامج التي تسمح بمعالجة ونقل البيانات، حيث يصعب في كثير من الأحيان تصنيفها وتحديد ما إذا كانت من المكونات المادية للحساب أم أنها من مكونات، كالدوائر المتكاملة، على سبيل المثال، ويمكن لكل هذه العناصر أن تكون محلا للسرقة، فالمعلومات التي تتضمنها لا يمكن فصلها عنها، وبالتالي فإن سرقة المعلومات في هذه الحالة هي السرقة للوسيط الذي يحملها، ولكن الوصول إلى المعلومات والاطلاع عليها قد لا يتم دائما عن طريق سرقة الوسيط المادي الذي يتضمنها، بل وقد يتم بمجرد قراءة هذه المعلومات على شاشة الحاسب أو بعد تسجيلها على قرص ممغنط ملك لمن يقوم بالتسجيل(1).

الفرع الأول: مفهوم جريمة السرقة الالكترونية.

[1] -نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادي، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2005، ص:123.

لقد نصت المادة 350 قانون العقوبات الجزائري على أن:" كل من إختلس شيئا غير مملوك له يعد سارقا....."(1).

فهذا التعريف يهتم بالجانب الموضوعي للسرقة حيث يتطلب لقيام هذه الجريمة أن يرتكب الجاني فعلا ماديا محددا وهو الاختلاس وأن ينصب هذا الاختلاس على منقول مملوك للغير.

وبع أن نتطرق لأركان جريمة السرقة وفقا للقواعد العامة سنفهم كيفية وقوع هذه الجريمة بالطريق المعلوماتي، سواء كان محل الاختلاس معلومات أو منقولات، كما أنه نشا 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 السرقة2

أولا: تعريف جريمة السرقة الالكترونية.

نصت المادة 350 من القانون العقوبات على أن:" كل من اختلس شيئا غير مملوك له يعد سارقا ويعاقب بالحبس من سنة أو خمسة سنوات وبغرامة مالية من 100.000دج إلى 500.000دج، وتطبق نفس العقوبة على الاختلاس(3).

من هذا التعريف يمكننا القول بأن السرقة جريمة عمدية، يتطلب لقيامها أن يرتكب الجاني فعلا محددا 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؟ وتحديدا ما مدى احتمال الأموال في التجارة الالكترونية لفكرة السرقة؟ هذا ما سوف نتجه إليه:

---

[1] - القانون رقم23/06 المؤرخ في 24 ديسمبر2006 ، الجريدة الرسمية العدد 84 لـ 24 / 12 / 2006.

[2] - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، مصر، الطبيعة الأولى، 2006ص406.

[3] - القانون رقم23/06 المؤرخ في 20 ديسمبر 2006، ص127.

إن المعلومات المعالجة أو البيانات بوصفها كيانات منطقية أصبحت من القيم الاقتصادية المستحدثة، وبالتالي فهي ذات طابع مالي ويكفي أن يذكر في هذا المجال أن أكثر من70% من نفقات المعلوماتية، تخص المعلومات المعالجة وحدها. وأن تكلفة برنامج واحد تقدر دائما بعدة ملايين من النقود[1].

ولذلك بسلم جانب من الفقه الجنائي بأن المعلومات نصلح لأن تكون محلا للسرقة بالاعتداء عليها واغتصابها من حوزة صاحبها، فالمعلومات لها قيمة تقدر بثروات طائلة ولذلك تنتقي صفة المال عن شيء متى انعدمت قيمته ولا يصلح محلا للسرقة والمعلومات من الأموال المعنوية، لذلك فهي تصلح لأن تكون محلا للسرقة، ويتم الحصول على هذه المعلومات عن طريق الحصول على كلمة السر بطريقة فنية ممن يعملون في مجال المعلوماتية أو من شخص يعمل في وظيفة تساعده في الحصول على كلمة السر، والسرقة المعلوماتية يترتب عليها ضرر للغير، فقد تكون السرقة بهدف إفشاء سر، ويكون ذلك بدخول الجاني إلى نظام معلومات خاص، ويلتقط معلومات او يسرقها بطريقة النسخ على مستندات أو شرائط وبالتالي أصبحت المعلومات ذات كيان مادي بتسجيلها على شريط أو بطباعتها ونقلها والاستيلاء عليها.

ومحكمة النقض الفرنسية بدورها قضت بأن عمل نسخة مقلدة من مسند، تعد بمثابة سرقة لهذه النسخة من المستند الأصلي.

ويرى جانب من الفقه الفرنسي أن السرقة المعلوماتية تعد بمثابة سرقة لأنها تنطوي على فعل سرقة لوقت الحاسب، وتعادل تماما سرقة الأموال، على حين رأى آخرون أن سرقة وقت الحاسب بمثابة سرقة عادية قياسا على سرقة السيارة

[1] - أنظر: د. عبد الفتاح بيومي حجازي، المرجع السابق، ص:163.

واستعمالها دون إذن صاحبها وكذلك سرقة التيار الكهربائي، على حين يرفض البعض الأخر اعتبار سرقة الوقت من قبيل سرقة الأموال.

وفي كل الأحوال فإن السرقة المعلوماتية لا يترتب عليها خروج المعلومات من حيازة صاحبها أو الحائز القانوني لها. ولكن تخرج فقط نسخة من هذه المعلومات في حين أنه في السرقة التقليدية تخرج الحيازة من الحائز القانوني إلى السارق[1].

ثانيا: النطاق القانوني لحركية السرقة الالكترونية.

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

- أن يكون موضوع السرقة شيء: اختلف التشريع الفرنسي مع التشريع المصري حيث التعبير في المادة1/311 ق عقوبات فرنسي جاء بصيغة شيء ويعبر عنه في القانون المصري بلقطة مادي وهذا الكلام يقودنا إلى أن الأموال أو الأشياء المعنوية لا تدخل في مجال السرقة إلا 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. وهذا الكلام يعني أن الأقراص تعكس شخصيات الالكترونية أو إشارات مغناطسية فتصوير مستندات سرية، فهذا يعتبر اختلاس محتوى المعلومة حيث أن سرقة المعلومات تكون قبيل الأوراق والمستندات والحلقات، كما أن سرقة التيار الكهربائي اعتبرت أيضا سرقة إلكترونية كونها قوى والقوى هي أشياء وفقا لنص المادة 1/311 ق.ع فرنسي وقد تأكد أن البيانات أو المعلومات تأخذ تشكل نبضات إلكترونية تمثل الرقمين، الصفر والواحد وبهذا يشبه التيار الكهربائي والذي يعتبر

[1] –عبد الفتاح بيومي حجازي، المرجع السابق، ص:165.

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

- أن يكون موضوع السرقة مادي: لقد تباينت الآراء في تحديد طبيعة المعلومات أهي مادية أم لا؟ وقد برز في ذلك اتجاهين:

أ/ يجب استبعادها من طائفة الأموال فهي ليست ذات طبيعة مادية كون الأشياء المحسوسة فقط ما يعتبر من قبيل الأشياء المادية وانعدام كيانها المادي كالقرض أو الملف لا يجعلها محلا للسرقة في الحق المالي المتعارف عليه فقها.

ب/ مهما كانت طبيعة الحق ذهبية أو معنوية للشخص على الشيء ويمتد وصف المال إلى المعلومات وذلك استنادا لعدم جواز الخلط بين طبيعة الشيء ذاته وطبيعة حق صاحب الشيء وقد دعم هذا الاتجاه بعض من الفقهاء المؤيدين لصلاحية خضوع المعلومات المخزنة في الحواسيب لوصف السرقة وذلك بالحجج التالية:

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

* يتحقق الاستيلاء على المعلومة عن طريق السمع أو المشاهدة وبالتالي تنتقل المعلومة من عقل الأخر، ومن ذمة مالية لأخرى فغن اكتفى الغير بالتقاط المعلومة في ذهنه دون تسجيلها أو تدوينها على دعامة لا يقع محلا للسرقة، أما إذا قام بتدوينها أو تسجيلها وحرم صاحبها من الانتفاع بها فهذا يقع تحث طائلة السرقة الالكترونية.

* تقاس المعلومة بجهاز معين وتأخذ حيزا ماديا مثل الطاقة الكهربائية.

* قيام محكمة النقض الفرنسي بإدانة عامل قام بنسخ مستندات سرية دون علم صاحبها.

---

[1] - *محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، مكتبة دار الثقافة للنشر والتوزيع، الطبعة الأولى، سنة 2004 ، ص:148-150.*

*** قيام محكمة النقض الفرنسية بإدانة شخص قام بإخفاء معلومات مع علمه بالوقائع وقيامه بتقديم صور منسوخة من مسند مسروق متضمن لمعلومات سر التصنيع.**

*** 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[1].**

- أن يكون موضوع السرقة منقول: إن المعلومات هي الهدف الرئيس المجاني حين أنه لا يستهدف الدعامة الفارغة وإنما يستهدف المعلومات كما أن المعلومات في حد ذاتها تشكل كيان مادي يمكن نقل حيازته من مالك لأخر ووفقا للقانون 652/82 الصادر في 29 يوليو 1982 يعرف المعلومات على أنها :" أصوات وصور ووثائق ومعطيات أو رسائل أيا كانت طبيعتها" وبالتالي فإن هدف الرسالة هو المعلومات التي تنقلها وهذا ما يؤكد أن المعلومات شيء منقول. وقد قضت محكمة النقض الفرنسية أن الشيء إذا انفصل عن أصله أصبح صالحا للانتقال وقابلا للسرقة ويبقى السؤال هل الإشعاعات الصادرة عن الجهاز أو بمعنى أدق المعلومة المتبادلة عبر الانترنت تعد من المنقولات حسب ما نصت عليه المادة 311 من قانون العقوبات الفرنسي[2]؟.

للإجابة عن هذا السؤال نقول أن المعلومات المنتقلة عبر الحواسيب بواسطة خطوط الانترنت إذا التقطت بالسمع أو المشاهدة لا تقوم جريمة السرقة لأنها لا تنقل الحيازة، كما أن سرقة الكهرباء أيضا تعد جريمة إلكترونية باعتباره طاقة يمكن قياسها ولها من يولدها وينتفع بها. إلا أن بعض النصوص الجنائية تحرم فعل الالتقاط، فقد تكون هذه المعلومات نادرة وتلحق الضرر بالغير بالأخص إذا ما عمل نسخ منها وباعها بسعر أقل من سعر النسخة الأصلية.

---

[1] - محمد أمين أحمد الشوابكة، المرجع السابق، ص: 150 – 152.

[2] - محمد أمين أحمد الشوابكة، المرجع السابق، ص:153.

- أن يكون موضوع السرقة مملوكا للغير: للقول بوقوع جريمة السرقة الالكترونية يجب أن يكون الشيء محل السرقة اعتداء على الحيازة وحق الملكية على الشيء وبالتالي تنهي صفة السرقة إذا ما اختلس شخص مالا مملوكا 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 يعد ذلك اكتسابا مشروعا للملكية[1].

الفرع الثاني: أركان جريمة السرقة الالكترونية

من المسلم به أن للسرقة ركنين أساسيين ركن مادي وركن معنوي، بيد أن الطبيعة الخاصة للتعاملات الالكترونية وخاصة أنها ترد على منقولات المادية (التقليدية) [1].

أولا: الركن المادي: حيث نتناول فيه، انتقال الحيازة أو الملكية من المالك الأصلي إلى المالك الجديد بفعل الاختلاس.

ثانيا: الركن المعنوي: ونتطرق فيه إلى نية الملك والاستئثار بالشيء.

أولا: الركن المادي لجريمة السرقة الالكترونية.

يعد الركن المادي في الجريمة السرقة سلب حيازة الشيء من مالكه أو حائزه بغير رضائه، وبذلك أصبحت فكرة الاختلاس في جريمة السرقة تربط بفكرة الحيازة

[1] - المرجع نفسه، ص:154

[1] -شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، مصر، بدون طبعة، سنة 2007، ص:44.

المدنية وتتحدد في ضوئها، كذلك تفرق جريمة السرقة عن جريمتي النص وخيانة الأمانة في هذا الخصوص، فعلى حين أن الآخرين اعتداء على الملكية فقط، فإن جريمة السرقة اعتداء على الملكية والحيازة معا.

ويعود الفصل إلى الفقيه الفرنسي –جاسون- الذي عرف الاختلاس بأنه "سلب حيازة الشيء رغما عن مالكه أو حائزه السابق، أي أنه اغتصاب للحيازة في معناها الحقيقي بعنصريها المادي والمعنوي"[1].

ويقصد بسلب الحيازة، كل فعل مادي يأتيه الجاني ويترتب عليه إخراج الشيء من حيازة صاحب أو حائزه، وإدخال في حيازته هو أيا كانت الوسيلة المستعملة في سلب الحيازة، وسواء احتفظ الجاني لنفسه بحيازة الشيء المسلوب أو تناول عن هذه الحيازة إلى الغير.

فللحيازة عنصرين أحدهما مادي ويشمل مجموع الأفعال أو السلطات التي يباشرها مالك الشيء عليه، فهي بهذا الوصف تخوله الحق في كل الأفعال المادية والتصرفات القانونية على الشيء المملوك، أما المعنوي فهو يعني نية الحائز الاختصاص بالشيء والاستئثار به.

ويتحقق فعل الاختلاس بتوافر العنصرين 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 إلا أن علم المالك الأصلي بانتقال الحيازة إلى غيره ينفي فعل الاختلاس.

كما أن التسليم الذي ينفي الاختلاس في جريمة السرقة لابد وأن تتوفر فيه شروط ثلاثة وهي:

[1] - عبد الفتاح بيومي حجازي، المرجع السابق، ص ص:407 – 408 – 409.

-أن يكون التسليم إراديا.

-أن يكون صادرا من الحائز.

-أن يكون صودا به نقل الحيازة [1].

كما أنه يجب أن يكون محل جريمة السرقة ما لا ماديا وليس مالا معنويا، وأن يكون هذا المال المنقول مملوكا للغير، لأن السرقة لا نقع إلا على الأموال المادية، أي كل شيء له كيان ملموس يكون محلا للتملك.

فالأموال المعنوية لا تصل محلا للسرقة، ومنها الأفكار والآراء والابتكارات فلا يعد سارقا من ليست لنفسه فكرة أو رأي أو اختراع أخذه من غيره.

كذلك يعد سارقا من يتلاعب في عداد المياه أو الغاز لصالحه، ويستوي في الشيء محل السرقة أن يكون ثمينا أو ضئيل القيمة كسرقة التيار الكهربائي حيث أثار الفقه جدلا حول هل التيار الكهربائي من الأشياء المادية بحيث يمكن اختلاسها أم هي منفعة مثل الضوء و الحرارة و بالتالي لا تصلح محلا للسرقة فهي شيء ملموس يمكن حيازته ونقله من مكان لأخر، ولا تتنافى طبيعتها مع فعل الاختلاس. كما انه يلحق بسرقة التيار الكهربائي سرقة الخط التليفوني حيث يقوم شخص بطرقة فنية ممن يعملون في مجال المعلوماتية أو من شخص يعمل في وظيفة تساعده في الحصول على كلمة السر، والسرقة المعلوماتية يترتب عليها ضرر للغير، فقد تكون السرقة يهدف إفشاء سر، ويكون ذلك بدخول الجاني إلى نظام معلومات خاص، ويلتقط أو يسرقها بطريقة النسخ على مستندات أو شرائط وبالتالي أصبحت المعلومات ذات كيان مادي بتسجيلها على شريط أو بطباعتها ونقلها والاستيلاء عليها.

[1] - شيماء عبد الغني محمد عطا الله، المرجع السابق، ص ص45، 46.

وقد قضت محكمة النقض الفرنسية بأن عمل نسخة مقلدة من مستند تعد بمثابة سرقة لهذه النسخة من المستند الأصلي.

ويرى جانب من الفقه الفرنسي أن السرقة المعلوماتية تعد بمثابة سرقة لأنها تنطوي على فعل سرقة الحاسوب، وتعادل تماما ما سرقة الأموال حين رأى جانب آخر أن سرقة وقت الحاسوب يعد بمثابة سرقة عادية قياسا على سرقة السيارة واستعمالها دون إذن صاحبها وكذلك سرقة التيار الكهربائي في حين يرفض البعض الأخر اعتبار سرقة الوقت من قبيل سرقة الأموال.

وفي كل الأحوال فإن السرقة المعلوماتية لا يترتب عليها خروج المعلومات من حيازة صاحبها أو الحائز القانوني لها، ولكن تخرج فقط نسخة من هذه المعلومات على حين أنه في السرقة التقليدية تخرج الحيازة من الحائز القانوني إلى السارق[1].

وقد استقرت محكمة النقض الفرنسية صراحة حتى لأن على أن صياغة المادة 1/311 قانون عقوبات فرنسي "اختلاس شيء" لا يساعدها 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[2].

كما أنه يلحق بسرقة التيار الكهربائي، سرقة الخط التليفوني حيث يقوم شخص بتحويل مسار الخط التليفوني الخاص بغيره ويستعمله في إجراء مكالمات على حساب صاحب هذا الحط، ومن ثم لا يدفع قيمة هذه المكالمة.

وقد تتعدد جريمة السرقة مع جريمة الإخلال بحق المؤلف عندما يقوم المتهم بنسخ بيانات يحملها قانون حق المؤلف (كأن يكون مؤلفا لا يزال مخزنا في الكمبيوتر ولم يتم نشره أو برنامج كمبيوتر أو قاعدة بيانات)، فلا يشترط القضاء أن يتم نشر

[1] - عبد الفتاح بيومي حجازي، المرجع السابق، ص412.
[2] -شيماء عبد الغني محمد عطا الله، المرجع السابق، ص49.

العمل الذي تم تقليده إخلالا بحق المؤلف بل يكفي أن يكون متاحا للجمهور، في هذا الفرض يتوفر التعدد المعنوي للجريمتين وذلك نظرا لوحدة النشاط الإجرامي ويعاقب عن الجريمة ذات العقوبة الأشد[1].

ثانيا: الركن المعنوي لجريمة السرقة الالكترونية.

إن القصد الجنائي الخاص لا يتوفر في حق المتهم في الجريمة إلى إذا توافرت لديه نية السرقة، بالإضافة إلى توافر القصد الجنائي العام من علم وإرادة.

- تعريف نية التملك:

هي توفر نية حرمان المالك من سلطاته وبالتالي تقع جريمة السرقة وعندئذ يحل محله حيث يقوم بممارسة السلطات التي لا تصدر إلا من المالك والمتمثلة في سلطة الاستئثار بالشيء وسلطة، عندئذ يظهر المتهم بمظهر المالك و تتجسد لديه نية التملك .

و مهما اعتبرنا نية التملك داخلة في القصيدة الجبائي العام أو أنها تشكل قصدا جنائيا فإنها على أية حال ضرورية لوقوع جريمة السرقة. لذا قضت المحكمة بنقض الحكم الذي اقصر أن المهتم استولى على مال مملوك للمجني عليه (قطع من ذهب) دون موافقة صاحبها، وذلك في مقابل ما أداه هذا المهتم للمجني عليه من خدمات، فقد نفت المحكمة أنه لم يبين نية التملك[2] .

- النتائج المترتبة على استلزام نية التملك:

يترتب على تخلف نية التملك نتيجة قانونية هامة تتمثل في انتقاء وصف السرقة عن بعض الأفعال، وأهمها الاستخارة، فاستعارة الشيء يقترن بنية الرد، الأمر الذي بيننا مع نية التملك، فلا يعد سارق بسبب انتقاء نية التملك.

---

[1] - شيماء عبد الغني محمد عطا الله، المرجع السابق، ص:51.

[2] - المرجع نفسه، ص ص 52، 53 .

إن توافر نية الرد لا يجول دون توافر القصد الجنائي في سرقة المعلومات، ذلك لأنه يكتفي بتوفر نية التملك بصفة مؤقتة عليها، استنادا 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.

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

لا تقع جريمة السرقة إلا مع توافر نية التمالك وفقا للقوانين المقارنة، وقد عبر القانون الفرنسي عن ذلك في المادة 1/131 قانون العقوبات – تغير من "اختلس بسوء النية"[1].

كما يتطلب في القانون الانجليزي أيضا نية التملك حيث نص القانون السرقة لعام1968 بتعبير:"يعتبر الشخص مرتبكا للسرقة أذا استولى لنفسه، بسوء النية، على أموال تنتمي إلى الغير بنية حرمان هذا الأخير بشكل دائم منه".

ومن خلال استقراء هذه المادة يظهر لنا أن جريمة السرقة لا تتحقق إذا كان الاستيلاء على مال الغير بنية حرمانه نهائيا أما إذا كان مؤقتا، فلا تعتبر هذه الجريمة سرقة إلا أن كل قاعدة عامة لديها أشياء حيث ينص الفصل السادس من نفس القانون أن جريمة، السرقة تتحقق في حالتين:

- إدا كانت نية المتهم تظهر بمظهر المالك على الشيء متصرفا فيه إضرار بصاحب الحق

- إذا استعار المتهم شيئا لمدة وفي ظروف تجعل هذا السلوك استيلاء أو تصرفا في الشيء.

وبهذا حكم في قضية ferandes 1999 بالسرقة كونه قام بالاستيلاء على مبل من النقود من حسابات العملاء دون موافقتهم على الرغم من اعتزامه النية في رد

[1] - شيماء عبد الغني محمد الله، المرجع السابق، ص 54.

المبلغ بعد مدة معتبرا من ذلك من قبيل القرض إلا أنه تنتفي جريمة السرقة إذا كانت نية الرد فورية في القرض كقضية liyod 1985 حيث قام بنسخ مجموعة أفلام سينمائية في الحين، وقام بتسليم أشرطة التسجيل، إذن هذه استعارة وليست سرقة، إذن للمعلومات نوع من الذاتية يميزها عن الأموال المادية فهي لا تقبل النسخ والإعادة لصاحب الحق، ففي هذه الحالة يحرم صاحبها من الاستئثار لاستعمالها فلا يصبح المالك.

- تحريم استعمال أموال الغير بنية الغش:

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

لذلك أدخلت بعض التشريعات حسما للخلاف حول توافر نية التملك وللعقاب على فعال أخرى إضافية، تجريما يعاقب على التدخل في نظام الكمبيوتر أو البقاء فيه بغير موافقة صاحب.

- ضرورة تجريم استعمال النظام بدون موافقة صاحب بنصوص خاصة:

نتيجة تشريعات عديدة إلى تجريم سرقة وقت الكمبيوتر وذلك في صورة تجريم التداخل في النظام أو البقاء فيه بدون وجه حق، بالمخالفة للقواعد العامة التي تنتجها تلك التشريعات من عدم تجريم استعمال ملك الغير دون رضائه.

ويأتي تجريم استعمال كمبيوتر الغير في صورة التداخل فيه متماشيا مع ما تتضمنه بعض التشريعات من تجريم استعمال سيارة ملك الغير بون رضائه، فعلى الرغم من عدم توافر نية التملك فإن الفعل يشكل جريمة بنص خاص حيث نص المادة

323 مكرر1 من قانون العقوبات المصري على أن "يعاقب كل من استولى بغير حق وبدون نية التملك على سيارة مملوك لغيره ....." [1].

المطلب الثاني: خصائص مرتكب الجريمة الالكترونية.

يتميز المجرم الالكتروني بعدة صفات وخصائص يميزه عن المجرمين العاديين.

الفرع الأول: صفات المجرم الالكتروني.

-ذكي : يتميز المجرم الالكتروني بأنه فائق الذكاء بل نابغة معلوماتي لأن المجرم الذي يقوم باختراقات وقرصنة قد تطال حتى الشركات التجارية والمؤسسات العامة وقد تصل حتى أمن الدولة حيث يمكنه التجسس إما لعالم دولته أو لدولة أخرى يجب أن يتميز بنسب عالية من الذكاء ليحقق مبتغاه.

-غير مثال للعنف والقوة: حتى يتمكن المجرم الالكتروني من تحقيق غايته يميل إلى السير الحسن والفعال مع أفراد مجتمعه ويتجنب العنف والمشاجرات واستعمال القوة مع الأشخاص.

- اجتماعي: يميل المجرم المعلوماتي إلى التكييف مع أفراد مجتمعه وإظهار الوجه الحسن والحبر فهو لا يعادي أحد من المحيطين به ويبرع في إخفاء شخصية الإجرامية، فالذكاء هو القدرة على التكيف وهذا ما يزيد من خطورته حيث لا تظهر شخصيته الحقيقية أمام الملء.

الفرع الثاني: أنواع المجرمين مرتكبي جرائم الانترنت.

هناك نوعان من المجرمين المعلوماتيين: الهواة والمجرمين.

-الهواة: يطلق عليهم صغار النوابغ المعلوماتية حيث لا يتوفر لديهم الدافع إنما أوصلتهم الأسباب إلى ارتكاب هذا النوع من الجرائم، كونهم يملكون معلومات لا باس

[1] - شيماء عبد الغني محمد عطا الله، المرجع السابق، ص57.

بها عن أنظمة الكمبيوتر، وغالبا ما ترتكب هذه الجرائم بالصدفة عن طريق البحث من طرف شباب طائش[1].

- المجرمين: يتوفر لدى هذه المجموعة الدافع لارتكاب مثل هذه الجرائم كما أنهم يقصدون إحداث الضرر في المعلومات والبرامج وهم أشد وأكثر خطورة حيث أجريت دراسة من طرف معهد stand-ford-research حيث أثبت أن معظم الجرائم المعلوماتية يرتكبها المحلل وذلك بنسبة 25% بعده المبرمج بنسبة18%، ثم الصراف بحوالي 16%، ثم الشهي الأجنبي على تلك المنشاة بنسبة12% وبقيت 11% من حصة المشغل[2].

المطلب الثالث: ماهية جريمة النصب الالكتروني.

دقت أجراس الخطر لنية المجتمعات لحجم مخاطر ظاهرة جرائم المعلوماتية أو الجرائم التقنية العالمية، أو ما يعرف بجرائم نوابغ الانترنت، فهي ظاهرة حديثة الظواهر، بدأت مؤشراتها بالارتفاع منذ سنة 2000، وقد نجم عن هذه الجرائم التي تمتاز بالتقنية العالمية خسائر كبيرة باعتبارها،"بيانات، معلومات، وبرامج بكافة أنواعها" فهي تعتمد على الحاسب الآلي بشكل رئيسي، يهدف فيها المجرم الالكتروني أو النابغة الالكتروني إلى النيل من الحق في الاستئثار بالمعلومات باستعمال وسائل المعرفة التقنية، وقد يتعدى ذلك إلى معطيات الحاسب الآلي المخزنة والمعلومات المنقولة [3].

---

[1] - محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر الإسكندرية، 2004، ص ص61-64.

[2] - محمد علي العريان، المرجع نفسه، ص65.

[3] - قبلي علال، بن لخضر عبد الكريم، جائم النصب الالكتروني، مذكرة تخرج لنيل شهادة ليسانس في الحقوق، سنة 2007،2008.

تظهر المخاطر الناجمة عن الجرائم المعلومات في كونها تمس الحياة الخاصة للأفراد وتهدد الأمن القومي والسيادة الوطنية وتهدد إبداع العقل البشري ومن هنا وجب علينا إدراك ماهية هذه الجرائم وتحديد مفهومها القانوني[1].

الفرع الأول: مفهوم جريمة النصب الالكتروني.

بالنظر للتباين الموجود بين جرائم الانترنت والجرائم التقليدية وجد الفقهاء في حيرة من الثبات في رأي واحد فتمايزت أراء هو 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 طائفتان أو اتجاهان:

*** طائفة التعريفات القائمة على معيار واحد، وهو قانوني وتتناول فيه كل من: السلوك محل التجريم، الوسيلة المستخدمة وموضوع الجريمة[2].**

*** طائفة التعريفات القائمة على النمط لكن هذه الطائفة تتمحور تعريفاتها وتتعلق بالتطور التاريخي الذي مرت به جرائم المعلوماتية ذات التقنية العالمية منذ ظهور الحاسوب كاختراع حديث أحدث ثورة في مجال المعلوماتية[3].**

أولا: تعريف جريمة النصب الالكتروني.

يحكم قانون العقوبات مبدأين أساسين أولتها شرعية العقوبات التي تعرض انتقاء العقاب عند انتقاء النص، وثانيتها خطر 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، ووفقا لما سبق تعريف الجرائم المعلوماتية على أنها: "الأفعال غير المشروعة

---

1 - عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الثاني المرجع السابق، ص204.

2 - قبلي عادل، بن لخضر عبد الكريم، المرجع السابق،ص30.

3 -عبد الفتاح بيومي حجازي، المرجع السابق، ص ص 460-461-462

المرتبطة بنظم الحاسوب". أما النص القانوني لجريمة النصب التقليدية الاستيلاء على حيازة مال الغير كاملة بوسيلة يشويها الخداع تسفر عن تسليم ذلك المال" حيث تنص المادة 372 ق،ع: "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الالتزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة حالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء منها يعاقب بالحبس"[1].

وعرفه بعض الفقه بأنه: "الاستيلاء بطريقة الاحتيال على شيء مملوك للغير بنية تمله".

كما يمكن لنا التمييز بين النصب والسرقة رغم تماثلها في الموضوع والغاية في رضا المجني عليه حيث ينعدم في السرقة ويتوفر في النصب إلا أنه يتعرض لإحدى طرق الاحتيال من طرف الجاني.

ثانيا: نطاق جريمة النصب الالكتروني.

تتميز جرائم الانترنت بطبيعة خاصة تتمثل في صعوبة اكتشافها وضبط مقترفيها كما تتميز أيضا بأساليب اقترافها إذ يغلب عليها الطابع الفني التقني عكس الجرائم البدوية التقليدية. ونظرا للأهمية التي يلعبها الحاسوب في المجال التطوري المعلوماتي إلا أن الحاسوب الآلي له سلبيات كماله من إيجابيات فمرتكبو جرائم الانترنت استغلوا لتطوير خبرائهم الوسائل التقليدية لارتكاب الجرائم حيث طور وسائل جديدة لتناسب هذا التطور التكنولوجي في مجال الحاسوب ليس لمواكبته

[1] - القانون رقم: 23/06/ المؤرخ في 24 ديسمبر 2006، ص136.

وتنمية المعارف وإنما للاعتداء عليه، وتختلف الأساليب باختلاف العنصر الذي يون محلا للاعتداء (معدات الحاسوب المادية) أي الأسطوانات والشرائط الممغنطة[1].

تستخدم عدة أساليب لارتكاب الجريمة الالكترونية، وتكون معدات الحاسوب المادية موضوعا لها وقد تمس هذه الجرائم أموالا خاصة بالأفراد كما قد تمس أموالا خاصة بالدولة إلا أنها تعد وسائل تقليدية وهي:

- تدمير الدعامات التي تحتويها سواء بإحراقها، أو تفجيرها باستخدام القنابل المتفجرة أوسكب 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 .

أما الأساليب عالية التقنية والتي تتطلب معرفة فنية بالحاسوب حيث يقوم فيها المجرم الالكتروني بما يتسمى بعملية السطو المسلح الالكتروني، يكون الهدف من هذه العملية التقاط أوتسجيل المعلومات والبيانات المعالجة إلكترونيا، وهي في مرحلة الانتقال والبث من الحاسب بواسطة أجهزة شبكة اتصالات بعيدة "limatique" والمعالجة عن بعد "teltraitment" كما يمكن عرض بعض الوسائل فيما يلي.

- التقاط المعلومات التي توجد ما بين الحاسب والنهاية الطرفية: يحدث هذا الالتقاط بواسطة توصيل خط تحويل يعمل على تكبير الذبذبات الالكترونية، وإرسالها إلى نهاية الطرفية التي تقوم بعملية التجسس ومن الممكن أن يحدث أيضا باستخدام جهاز مرسل صغير يمكنه نقل البيانات عن بعد ويمكن الالتقاط كذلك عن طريق وضع

[1] - نائلة عادل محمد فريد قورة، المرجع السابق، ص: 563.

هوائيات مطاردة بالقرب من الهوائيات الاحتياطية، وبالتالي يحدث التقاط الإشاعات العابرة عن طريق النقل الجوي للمعلومات عند بثها بالقمر الاصطناعي واحتجاز مضمونها[1].

-التوصيل المباشر بواسطة خط تليفوني: يتم ذلك بوضع مركز تنصت يجعل من تسجيل الاتصالات أمرا يسيرا كما يمكن الاستعانة أيضا بوضع ميكروبات صغيرة لأدائها.

-التقاط الإشاعات الصادرة عن الجهاز المعلوماتي: تكمن خطورة هذه الوسيلة في أنها يمكن أن تؤدي إلى إعادة تكوين خصائص المعلومات التي تبث وتنقل من خلال الأنظمة المعلوماتية، وهذا الجناح تسجيل الإشاعات الصادرة عن الحاسب كما لا يحتاج إلى حل شفراتها.

-التدخل غير المشروع في نظام الحاسب بواسطة طرفية بعيدة: تعد هذه الوسيلة ألفية من أخطر الوسائل التي يلجأ إليها المحرم المعلوماتي إذ يكون بإمكانه نسخ أو تدمير بعض البيانات والمعلومات بكل يسر ولا يحتاج إلا لمجرد الحصول على حاسب آلي "ميكروي" مع ضرورة التعرف على كلمة السر أو مفتاح شفرة النظام للحاسب المجني عليه.

وهكذا فإن المجرم المعلوماتي أو مرتكبي جرائم الأنترنت اكتفوا بالوقوف مذهولين أمام تكنولوجيا الحاسب وإمكانيته الفائقة التي بلغت حد الخيال من قدرة على التخزين والاسترجاع بسرعة فائقة بالإضافة إلى دقتها ومرونتها في التشغيل، بل نجد هؤلاء وقد استوعبوا هذه التكنولوجيا بطريقة متقدمة جدا واستغلوا خبرائهم

[1] - هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية القاهرة، بدون طبعة، بدون سنة، ص:129 – 132.

المكتسبة منها في تطوير الوسائل التقليدية لارتكاب وابتكار وسائل جديدة وغير معروفة تتناسب مع التطور إنه صراع أبدي بين الخير والشر[1].

الفرع الثاني: أركان جريمة النصب الالكتروني.

من المسلم به أن لجريمة النصب ركنين، ركن مادي وركن معنوي إلا أن الطبيعة الخاصة للتعاملات الالكترونية وخاصة أنها ترد على منقولات ذات طبيعة معنوية تعطي هذه الأركان مفهوما مختلفا عما هو مقرر بالنسبة للمنقولات المادية التقليدية، ويتضح ذلك من دراسة الركن المادي في الفرع الأول بما فيه من سلوك إجرامي ونتيجة إجرامية وعلاقة سيئة والفرع الثاني الركن المعنوي "العمد، القصد المتعدي والخطأ غير العمدي [2].

أولا: 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 أنه يتكون من سلوك إرادي ونتيجة إجرامية ورابطة سيئة.

-سلوك إجرامي: يعتبر السلوك المادي عبر الانترنت محلا للتساؤل، لا سيما فيها يتعلق ببدائية أو الشروع في ارتكاب الجريمة، وهو يختلف عما هو الحال في العالم المادي، وذلك لأن ارتكاب الجريمة عبر الانترنت يحتاج بالضرورة إلى منطق تقني، أي أنها تتم عبر الانترنت أو باستخدام المعالجة الآلية للبيانات كما أنها تحتاج إلى ممارسة نشاط تقني محدد يتمثل في استخدام الحاسوب والانترنت ومن أمثلة السلوك المادي في الجريمة عبر الانترنت المصرفي الذي ينوي سرقة مبلغ من المصرف الذي يعمل فيه باستخدام الانترنت، ثم الدخول إلى شبكة المصرف عبر مزودات مجهولة

[1] - د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، الطبعة الثانية سنة2006، ص301 -314.

[2] - قبلي علال، بن لخضر عبد الكريم، جرائم النص الالكتروني، مذكرة تخرج لنيل شهادة ليسانس في الحقوق، سنة 2007، 2008.

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[1].

- 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 امتدادا للنتيجة ليتحقق منتهاها في العالم المادي [2]؟

- العلاقة السببية: هي العنصر الثالث من العناصر التي يتكون منها الركن المادي في الجريمة الالكترونية، ويجب لقيام جريمة الانترنت أن تكون هناك رابطة مادية ما بين السلوك المادي والنتيجة الإجرامية المتحققة فمثلا يجب لتحقيق جريمة انتهاك الحق في الخصوصية عبر الانترنت أن يكون هناك دخول على الانترنت باستخدام حاسوب عامل والقيام بالاختراق الحواسب المختلفة في مسارها، ثم بعد ذلك التعدي على خصوصية موقع ما/ وكذلك يمكن اعتبار علاقة السببية قائمة بمجرد ثبوت الضرر في مجر البيت، وهذا ما قررته محكمة استئناف مقاطعة Columbia british الكندية في إحدى أحكامها.

إن كل جريمة تحدث باستعمال الانترنت إنما تحدث كلها أو بعضها حسب الأحوال في العالم الافتراضي، وإذا كان النشاط المادي كله بحدث في العالم الافتراضي وكذا العلاقة السببية فإن النتيجة الإجرامية لها كيان منفصل لكونها تحدث بشكل انقسامي ما بين حدوثها في العالم جزئيا أو كليا. ومن أهم الآثار المترتبة عنها تؤثر على قواعد الاختصاص في الدول كما أن جرائم الانترنت تنشر فيها فكرة النتيجة المحتملة، وذلك راجع إلى طبيعة النشاط التقني الذي قد يترتب عليه عدة نتائج منها، انتشار

[1] - د. عبد الفتاح بيومي حجازي، المرجع السابق، ص ص468، 469.
[2] - د. عبد الفتاح بيومي حجازي، المرجع السابق، ص ص 468، 469.

الفيروسات بقصد القرصنة، فإن ذلك يعتبر نتيجة محتملة تشمل الجريمة التي ليس لها منحني إطلاقا أي الحالة التي لا يكون فيها للضحية وجود مادي وإنما رقمي فقط[1].

ثانيا: الركن المعنوي.

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

- العمد: ينبغي لارتكاب الجريمة الالكترونية أن يكون مرتكبها نابغة في استعمال الحاسوب أي أنه يجب أن يكون 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 الالكتروني يكون قد خطط ودبر لارتكاب هذه الجريمة سواء من أجل الحصول على معلومة أو لاختراق شبكة حاسوب آخر كجريمة النصب تتطلب من الفاعل إرادة ارتكاب السلوك تحقيق نتيجة، وقد يكون القصد عاما أو خاصا.

يتحقق القصد العام إذا اعلم المجر أنه يرتكب فعل تدليس من شأنه ارتفاع المجني عليه في الغلط الذي يحمله على تسليم ماله ففي جرائم النصب المعلوماتي يستخدم الجاني أسلوبا للإيهام بوجود ائتمان كاذب أو يتوصل للاستيلاء على مال الغير كله أو بعضه متى وقع على فواتير الشراء باسم كاذب أو استغل صفة كاذبة لتحويل أموال الغير من حساب إلى آخر عن طريق التلاعب في المعطيات أو البيانات الالكترونية ويجب عمله بهذه الوقائع، ومع ذلك تتصرف إرادته إليها رغم عمله بأن فعله من الأفعال التدليسية[2].

[1] - قبلي علال، بن لخضر عبد الكريم، المرجع السابق،ص90.
[2] - عبد الفتاح بيومي حجازي، المرجع السابق،300.

أما القصد الخاص وهو نية التملك، فبقوم متى كان هدف الجاني من هذا الاحتيال، الاستيلاء على مال مملوك لغيره، علما بأنه لا عبرة بالبواعث في ارتكاب جريمة النصب سواء كان الباعث نبيلا أم خسيسا، كما يتوافر القصد الخاص في النصب المعلوماتي، متى قام الجاني مثلا باستخدام البطاقة وهو عالم أن رصيده فارغ أو أن بطاقته موقوفة ويستخدمها[1].

- القصد المتعدي: يتوفر القصد المتعدي في جرائم الانترنت في الحالة التي يتجاوز فيها قصد الشخص الهدف الذي كان يسعى لتحقيقه مثلا: إذا كان القصد مجرد اللهو في مسارات القطارات، فيتعدى الأمر ذلك تدمير بيانات تحريك القطارات عبر الحاسوب وتكون النتيجة حدوث خسائر مادية وبشرية وبهذا يتعدى النتيجة الهدف الذي كان يصبو إليه محترف الكمبيوتر فيصبح من مجر لاه في أجهزة الحاسوب إلى مجرم إلكتروني[2].

- الخطأ غير العمدي: يحتل الخطأ مرئية هامة في الركن المعنوي في جرائم الانترنت إذ أن معظم جرائم الانترنت تحدي نتيجة لخطأ عنبر مقصود كتدمير أجهزة المؤسسة لإفراط الموظف المسؤول في استخدام حاسوبها بدلا من حاسبوه الخاص في العمل على حساب الخاص ناسيا متاعب الفيروسات ومعتمدا فقط على مهاراته في تجنبها دون إدراج برامج القضاء على الفيروسات أو محاربتها في الكمبيوتر أو ينقل الفيروسات من القرص المرن إلى أجهزة المؤسسة فشكل تدميرا كليا أو جزئيا المعلومات أو البيانات بالأخص إذا تنقل فيروس إلى شبكة أو نظام حاسوب لمؤسسة مالية أوفدرالية[3].

الفرع الثالث: دوافع ارتكاب الجريمة الالكترونية.

[1] - عبد الفتاح بيومي حجازي، ، المرجع نفسه، ص320.
[2] - أحمد خليفة الملط، المرجع السابق، ص322.
[3] - أحمد خليفة الملط، المرجع نفسه، ص322.

كل جريمة دافع سواء كانت تقليدية أو الكترونية، وتكون هذه الدوافع إما على الجانب الشخصي للمجرم المعلوماتي أو تأخذ المعني المادي لها.

أولا: الدوافع الشخصية.

للمجرم الإلكتروني عدة دوافع شخصية لارتكاب الجريمة الإلكترونية والرغبة في إثبات الذات والإحساس بالقوة والقدرة على اقتحام الأنظمة وارتكاب جرائم الكمبيوتر وغالبا ما يكون السبب في ارتكابها الحقد والكراهية وحب الانتقام وأفضل مثال على ذلك المحاسب الشاب الذي دفعه حبه للانتقام من الشركة التي سرحته إلى التلاعب في برنامج الكمبيوتر الخاص بها حيث برمج النظام على اختراق كل البيانات الخاصة بدون الشركة بعد مضي ستة أشهر من تركه للعمل وقد حدث ذلك بالفعل حيث اختفت البيانات الخاصة بدون الشركة نهائيا من جهاز الكمبيوتر[1].

قد يكون الدافع مذهبيا كدوافع جماعة الأولوية الحمراء في ايطاليا التي كانت تتعرض للوزارات والمؤسسات المالية عن طرق تدمير مراكز المعلومات الخاصة بها حيث أصدرت هذه الجماعة منشور حددت فيه أهدافها سنة1998، وأغراضها هي مهاجمة الهيئات متعددة الجنسيات التي ترمز للامبرالية وكل هذا بفعله لصالح جماعته.[2].

الولع في جمع المعلومات فمعظم المجرمين الالكترونيتين يرتكبون الجرائم المعلوماتية بهدف الحصول على معلومات جديدة حيث يقوم المجرم الالكتروني باختراق الموقع وفي معظم الأحيان يكون هناك عدة مجموعة مع بعضهم ويتعاملون سويا.

حب المغامرة والإثارة مثلما جاء في كتاب قراصنة الأنظمة في الكمبيوتر المترجمة آمنة يوسف علي في الصفحة 10:" كانت القرصنة هي النداء الأخير الذي

[1] - محمد علي العريان، المرجع السابق، ص65.
[2] - محمد علي العريان، المرجع نفسه، ص350.

يبعثه ماغي فقد كنت أعود إلى البيت بعد يوم عمل سهل وأدير تشغيل الكمبيوتر وأصبح عضوا نخبة قرصنة الأنظمة وكان الأمر مختلفا بمته حيث لا وجود لعطف الكبار، وحيث الحكم هو لموهبتك فقط في البدء كنت أسجل أسماء في لوحة النشرات الخاصة حيث يقوم الأشخاص الآخرين الذين يفعلون مثلي بالتردد على هذه الموقع ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد، وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدا عقلي بقطع عليون في الساعة وأتنقل من جهاز كمبيوتر إلى آخر محاولا العثور على سبيل الوصول إلى هدفي، وكان يرافق ذلك تزايد سرعة الأدرنيالين وكل خطوة أخطوها كان يمكن أن سقطني بيد السلطات، كنت على حافة تكنولوجيا واكتشاف ما وراءها واكتشاف الكهوف الالكترونية التي لم يكن من المفترض وجودي لها[1].

ثانيا: الدوافع المادية.

يسعف كل من الشخصين الطبيعي والمعنوي إلى تحقيق ربح من خلال مباشرة الجرائم الالكترونية.

- الشخص المعنوي: من المعلوم أن بعض البرامج والمعلومات المخزنة داخل جهاز الكمبيوتر لها قيمة مادية كبيرة سواء كانت سيدي أوديسك وباعتبار أن لها قيمة مالية مرتفعة سعى معظم الشركات التجارية أو الصناعية إلى الحصول بسرقتها باستعمال أو استخدام وساطة القائمين على الكمبيوتر من خلال رشوتهم أو خداعهم[2].

- الشخص الطبيعي: يهدف الشخص الطبيعي أو النابغة الالكترونية إلى استخدام مهاراته المعلوماتية إلى الحصول على ربح مالي وذلك بالمساومة على البرنامج والمعلومات المتحصل عليها باختلاس بالكمبيوتر أو عن طريق السحب الآلي من

[1] - د. أحمد خليفة الملط، المرجع السابق، ص352.
[2] - د. أحمد خليفة الملط، المرجع نفسه، ص ص354 – 356.

بطاقة منتهجة الصلاحية أو مزورة وهذا إما نصت أو بالأحرى ما جاءت به مجلة sécurité informatique وهي مجلة مختصة في أمن المعلومات بتصريح من الأستاذ porker أن 43% من الحالات المعلن عنها هي من أجل الاختلاس، و23% من أجل السرقة، و19% من أفعال الإتلاف عن طريق اللهو أو الانتقام، و15% من الجرائم المعلوماتية

الفصل الثاني: وسائل حماية التجارة الالكترونية.

إن الغزو المعلوماتي الكبير الذي عرفته الأموال الالكترونية من طرف التوابع المعلوماتية دفع إلى وضع وتتضمن هذه الوسائل: الوسائل الوقائية والوسائل الردعية، حيث تكون الوقائية مجرد أنظمة متصلة بالكمبيوتر تعطي لمستخدم الحاسب الأمان لإرسال الرسائل الالكترونية إلا أن هذه الوسائل أيضا تعرضت للغزو، فظهرت بذلك وسائل ردعية أكثر صرامة من سابقتها تتمثل في التشريعات والتنظيمات الداخلية حيث يتم معاقبة المجرمين المعلوماتيين جنائيا.

المبحث الأول: الطرق الوقائية.

وضع المشرع طرق وقائية تسمح لمستخدم الانترنت استعماله كتقنية بأمان تام، حيث تتم إرسال الرسائل الالكترونية و تلقيها بسرية تامة، تمكن المرسل والمرسل إليه، معرفة محتوى الرسالة دون طرف ثالث متطفل على سبيل المثال تشفير البيانات والتوقيع الالكتروني.

المطلب الأول : تشفير البيانات.

يعد التشفير من الطرق الوقائية لحماية الأموال الالكترونية ووسائل حفظ سرية المعلومات في نطاق الأنظمة الالكترونية، وبهدف إلى منع الغير من التقاط الرسائل أو المعلومات، ومن ثم منع وصول أو ووصول مشوهة إلى الطرق الأخرى من المعاملة التجارية، والذي يقوم بدوره بتحويل الرسالة إلى شكلها الأول سنتناول في هذا المطلب بالتشفير وأهميته ثم صور التشفير الالكتروني.

الفرع الأول: تعريف التشفير الالكتروني وأهميته

أولا: تعريف التشفير: **إن تعميقنا في معنى التشفير نجد أنه 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 طرق ثالث متطفل ويغرف بأنه "مناهج لخط البيانات من خلال لوغارتميات أو خوارزميات، بحيث لا يمكن قراءتها من خلال طرق ثالث متطفل".**

فالتشفير هو علم تحويل الكتابة إلى أسرار، حيث لا يمكن لطرق ثالث الدخول للموقع دون تصريح المالك، وذلك باستخدام مفتاح إزالة التشفير، ويتم التمييز بين النص المشفر والنص العادي في التسمية، حيث يطلق على النص العادي اسم النص الكامل أما المعلومة التي يتم تشفيرها يطلق عليها اسم النص المشفر، ويستخدم في التشفير أساليب رياضية يطلق عليها، مصطلح خوارزميات التخفي والذي بدوره يحتاج لمفتاح للتشفير ومفتاح آخر لفك التشفير كان التشفير معروفا في الخمسينات في المجال العسكري، حيث كان يستعمل إخفاء المعلومات أثناء الاتصال بين الحكومة والجيش وقت الحروب. أما في الستينيات فقد توجه التشفير نحو الحركة الصناعية، وفي السبعينيات أخذت به المصارف، وفي الثمانيات دخل التشفير للهاتف ليشفر في نهاية القرن العشرين في التجارة الالكترونية يختلف مستوى التشفير بالنظر للمعلومة المراد

تشفيرها فمنها ما يتعلق بالخصوصية ومنها ما يتعلق بقداسة المعلومة ومنها ما يتعلق بالأصالة حيث يحسب هذا الاختلاف عند احتساب العقوبة من حيث التخفيف والتشديد[1].

من أشهر أساليب التشفير تلك التي تتعلق بخصوصية المعلومة حيث يتم بها ردع كل متطفل من الولوج إلى موقع المالك دون تصريح وهنا يجب التمييز بين الحق في الخصوصية والتشفير المتعلق بالخصوصية وهذا يقودنا إلى إطار مدى صلاحية التشفير في فيصلح التشفير فقط في الكلام المباح وتتم حمايته دون غيره.

أما تشفير قداسة المعلومة فسيخدم 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 عبر الانترنت، أما التشفير المتعلق بأصالة المعلومات فيستخدم في استمرار المعلومة بحيث تدل على الراسل والمرسل إليه كما لا يستطيع المرسل إنكار إرساله لها. عرف مجلس الدولة الفرنسي التشفير على أنه إخفاء المعلومات وعرف الإخفاء بأنه:"كل عمل يوجه لتحويل بمساعدة مصطلحات سرية – 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 الأول بين مؤيد ومعارض كتقنية برمجية فالدول مازالت في صراع بين الإبقاء عليه أو رفضه وعزل وإبقاء في هذه المنطقة الوسطى بين القبول والرفض يعطي للتشريع دورا حيويا كاملا حيث يصبح له كامل الصلاحية في الفعل في هذا الشأن وللتشفير وجوانب سلبية كما له من الجوانب الايجابية حيث سيخدم في التجارة الالكترونية بما فيها من رسائل سرية وعروض خدمات وحركة تبادل الأموال كي لا تكون عرضه للنهب والاستيلاء من طرف المجرمين المعلوماتيين وذلك يعطي لنا جانبين سلبيين أولهما هو تمكن هؤلاء النوابغ الالكترونية من فك شفرات ومعروفة المعلومات**

[1] - محمد أبوبكر بن يونس، الأحكام الموضوعية والجوانب الإجرامية، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، بدون طبعة، سنة2004، ص379 – 380.

[2] - محمد أبو بكر بن يونس، المرجع نفسه، ص ص383 – 386.

المرسلة، أما الجانب السلبي الثاني فيمكن في صعوبة استطلاع الحركة المالية للمؤسسات الاقتصادية حيث لعب التشفير دورا ممتاز في التهرب الضريبي في 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 خروجا على القاعدة العامة لحرمة المرسلات[1].

إلا أنه 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 صلبه مصممة خصيصا لتشفير فقد قامت حكومة الولايات المتحدة الأمريكية بتصميم هذا النوع عام 1993 تسمح للسلطات بالحصول على مفتاح التشفير لممارسة الرقابة على حركة المرسلات المشفرة وذلك بتركيب رقاقة في كل فاكس أو هاتف أو مودم، إلا أنها عورضت من قبل حركة الحريات، فعدلت الحكومة مشروعها في 1996 فاستحدثت مصطلح مفتاح التغطية حيث سمحت الحكومة بتقنية التشفير شرط الحصول على نسخة المفتاح وعدم اتباع هذا الشرط بقد جريمة قائمة بذاتها.

بالإضافة إلى ما تقوم به المنظمات بما فيها الإجرامية والإرهابية حيث تقوم الأولى بتشفير المعلومات التي تتضمن المؤثرات عقلية وكيفية إعداد وانتاج المخدرات وتحديد الجرعات ومواعيد تعاطيها وهذا يعد جانبا سلبيا للتشفير[2].

الفرع الثاني: صور التشفير الالكتروني.

---

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

[2] - عمر محمد أبوبكر بن يونس، المرجع السابق، ص 380.

التشفير صورتين هما:

- *التشفير كغطاء لارتكاب الجريمة*: يلعب التشفير دورا كبيرا في عالم الانترنت أو ما يعتبر عنه بالعالم الافتراضي، فهو من أنواع الحماية الوقائية لعدد من المعلومات المتداولة عبر الانترنت إلا أن موضوع التشفير ذاته طرح العديد من التساؤلات وبالتالي قال اهتماما فقهيا وتشريعيا كبيرا حيث أن جل توابع المعلوماتية يمارسون عدوانا على الموقع إما لكشف المعلومات المشفرة أو لكسر الشفرة ذاتها وهنا يجب التمييز بين نوعين من العدوان الأول على المعلومات والثاني على الوسيلة يهدف كسر الشفرة يؤخذ حين الاعتبار في تحديد العقوبة من حيث التشديد وذلك أن هذا العدوان عرضه الأول تغطية الأنشطة الإجرامية وهو في نفس الوقت عقبه 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].

- *التشفير كوسيلة لإعاقة الحصول على أدلة:* للتشفير عدة أهداف وهذه الأهداف قد تكون ظاهرة وقد تكون خفية ، أو يمكننا القول أن أهداف خلف الأهداف أي الهدف الظاهر للحكومة والهدف التضليلي أو لخفي وهو الذي يقصده الشخص، وقد يكون القصد من التشفير إخفاء أدلة التي تمكن من الإدانة في جريمة سواء تقليدية أو جريمة التقنية كما هو الحال في جرائم المخدرات والاتجار 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.

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

تنفيذ أمر قضائي بالمراقبة:

[1] - عمر محمد أبو بكر بن يونس، المرجع السابق ص387 – 388.

إلا أنه رغم وجود الرقابة التي تمارسها الجهات القضائية إلا أنها تعد محلا للطعن فيها لصعوبة إثباتها.[1].

المطلب الثاني: التوقيع الالكتروني.

نصت المادة 16 من القانون العربي النموذجي في شأن جرائم الكمبيوتر والانترنت على أن:" للتوقيع الالكتروني في نفس القيمة في الإثبات المقررة للتوقيع التقليدي ويتمتع بالحماية الجنائية المقررة للتوقيع التقليدي في حالة التزوير وفقا للنصوص المقررة في قانون العقوبات"[2].

فالكتابة ليست دليلا كافيا في الإثبات إلا إذا كانت موقعة من قبل الشخص الذي تنتمي إليه الكتابة، كما يعد التوقيع الشرط الوحيد لصحة الورقة العرفية.

فقد اتجه الواقع العلمي إلى إدخال طرق ووسائل حديثة في التعامل حيث انتشرت نظم المعالجة الالكترونية للمعلومات التي بدأت تغزو الشركات والإدارات والبنوك، فأصبح التوقيع اليدوي عقبة من المستحيل تكييفها مع التنظيم الحديثة للإدارة والمحاسبة، فتم الاتجاه نحو إيجاد بديل له ألا وهو التوقيع الالكتروني.

الفرع الأول: تعريف التوقيع الالكتروني ومدى تعليقه بالنظام العام

أولا : تعريف التوقيع الالكتروني:

يعرف التوقيع الالكتروني بأنه:" هو ذلك التوقيع الناتج عن إتباع إجراءات محدودة، تؤدي في النهاية إلى نتيجة معروفة مقدما، يكون مجموع هذه الإجراءات هو البديل الحديث للتوقيع بمفهومه التقليدي أو ما يسميه البعض توقيع إجرائي أو الكتروني"

ولقد عرف التوقيع الالكتروني في مشروع قانون التجارة الالكترونية المصري على أنه : "حروف أو أرقام أو رموز أو إشارات لها طابع متفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره"[3]

---

[1] - عمر محمد أبو بكر بن يونس، المرجع السابق، ص 388 – 389.

[2] - عبد الفتاح بيومي حجازي، المرجع السابق. ص229.

[3] - عبد الفتاح بيومي حجازي، المرجع السابق،230.

كما عرف كذلك بأنه :"ملف رقمي صغير يصدر عن إحدى الهيئات المتخصصة والمستقلة ومعترف بها من قبل لحكومة تما ما مثل – نظام الشهر العقاري – وفي هذا الملف يتم تخزين الاسم وبعض المعلومات الهامة الأخرى مثل رقم التسلسل وتاريخ انتهاء الشهادة ومصدرها".

أما بالنسبة للقانون الأمريكي الفيدرالي فان ملف التوقيع الالكتروني فيحتوي مفتاحين أحدهما عام والأخر خاص، المفتاح الخاص هو ذلك التوقيع الالكتروني الذي يميز التوقيع الخاص بشخص معين عن توقيعات الآخرين، أما المفتاح العام فيتم نشره في الدليل، وهو مفتاح للعامة من الناس الذين يحق لهم الاطلاع عليه.

كما يعرفه اتجاه من الفقه بأنه علامة خطية خاصة ومميزة يضعها الموقع بأي وسيلة على سنه لإقراره. كما عرفه البعض الأخر بأنه كل علامة شخصية توضع كتابة بحيث تنتج تحديد هوية محدثها على وجه لا يتطرق إليه أي شك وتتم عن ،رادته التي لا يحيطها أي غموض في قبول مضمون المستند أو المحرر [1].

ثانيا : مدى تعلق التوقيع الالكتروني بالنظام العام

وضع المشرع القوانين الإجرائية لخدمة العدالة حتى ترسم على هديها إجراءات التقاضي و يلتزم بها الخصوم و يحترمها القضاة بالمساواة بين جميع المتقاضين فلا يملك أحد فرض إجراءات على المحاكم و لا يملك الخصوم الاتفاق على فرض إجراءات غير مقررة في التشريع .

و قد اختلف الفقه حول قواعد الإثبات و مدى تعلقها بالنظام العام و هل كافة القواعد الخاصة بنظرية الإثبات كالإجراءات أو طرق الإثبات تتعلق بالنظام العام أم هناك قواعد يمكن اتفاق الأطراف على خلافها و أخرى لا يجوز الاتفاق على خلافها ؟

تعتبر قواعد الإثبات إما قواعد إجرائية أو شكلية و إما قواعد موضوعية ، فالقواعد الإجرائية

[1] - خالد مصطفى فهي، النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجديدة، الإسكندرية، 2007.

و هي المتعلقة بإعداد و تقديم الدليل في الإثبات تتعلق بحسن سير العدالة ، فلا يملك الخصوم الاتفاق على اتخاذ إجراءات غير مقررة في التشريع ، و لا يجوز لأحد الخصوم النزول عنها ، مقدما أما بالنسبة للقواعد الموضوعية و هي متعلقة بمصالح خاصة بالأطراف و تشمل محل الإثبات و عينه و طرفه فان هذه القواعد يمكن للأطراف الاتفاق على خلافها [1].

و قد تعرضت محكمة النقض المصرية في أحكامها لبيان طبيعة قواعد الإثبات و خاصة بالنسبة لعبئ الإثبات بوصفها قواعد لا تتصل بالنظام العام و يجوز الاتفاق على مخالفتها و متى كان الطاعن قد طلب من المحكمة إحالة الدعوى إلى التحقيق لإثبات ما يدعيه فليس له أن ينفي على الحكم إجابته إلى ما طلب حتى و لو كان فيما طلب متطوعا لإثبات ما هو غير ملزم لحمل عبئه .

و من هنا يجوز اتفاق الخصوم على أن يكون الإثبات دائما بالكتابة و لو كانت القيمة لا تتجاوز قيمة خمسمائة جنيه أو الاتفاق على جواز الإثبات بغير الكتابة و لو جاوزت القيمة المتقدمة

و قد انقسم الفقه في ظل عدم وجود نص تشريعي حول مدى تعلق تلك القواعد بالنظام العام بين مؤيد و معارض ، و جاءت أحكام محكمة النقض الفرنسية لتقرير أن للأطراف الحرية الكاملة في ترتيب نظام للإثبات الخاص بحقوقهم كما أن لهم حرية التصرف في هذه الحقوق بوصفها لا تتعلق بالنظام العام بل تتصل بالمصالح الخاصة بالأطراف .

أما بالنسبة للمحرزات الالكترونية فان المشرع قد نص على اكتسابها ذات الحجية المقررة للمحررات الكتابية و من ثم فانه يجوز الاتفاق بين الأطراف على خلافها لعدم تعلق قواعدها بالنظام العام ، و لكن تثور المشكلة في حالة الطعن بالتزوير في التوقيع الالكتروني ، فهنا لا يجوز الاتفاق على مخالفة تلك القاعدة لأنها من النظام العام ، حيث أنها تتعلق بقواعد عقابية ، و من ثم لا يجوز الاتفاق على مخالفة قاعدة عقابية و لكن

[1] - خالد مصطفى فهمي ، المرجع نفسه ، ص ص 46، 47 .

يجوز الاتفاق بوجه عام على كافة قواعد الإثبات التي لا توحي طبيعتها أنها تتعلق بالنظام العام (1).

الفرع الثاني : صور التوقيع الالكتروني

للتوقيع الالكتروني صور متعددة من بينها التوقيع الرقمي أو الكودي و ذلك عن طريق استعمال عدة أرقام يتم تركيبها لتكون في النهاية كودا يتم التوقيع به،و هناك التوقيع البيومتري (Biometric System) و يسمى التوقيع بطريقة Pen-ON كما يوجد التوقيع عن طريق الضغط على أحد مفاتيح لوحة الحاسوب على نحو يفيد الموافقة على التصرف القانوني .

أولا : التوقيع الرقمي أو الكودي : يستخدم هذا النظام في التعاملات البنكية و المعاملات المالية و أحسن مثال على ذلك بطاقة الائتمان التي تحتوي على رقم سري لا يعرفه سوى صاحب البطاقة حين يطلب الاستعلام عن حسابه أو صرف جزء من رصيده و هي تعمل بنظامي OFF-LINE و نظام ON –LINE .

و حسب النظام OFF-LINE فانه يتم تسجيل العملية المالية على شريط مغناطيسي،ولا يتغير موقف العميل المالي في حسابه إلا في آخر اليوم و بعد انتهاء مواعيد العمل .

أما نظام ON –LINE فانه يتم فيه موقف العميل و تحديثه فور إجراء المعاملة المالية هو الغالب في التعامل في نظام البطاقات البنكية التي تحتفظ بداخلها بذاكرة تسجل كل عمليات العميل.

و يستخدم التوقيع الالكتروني الرقمي في المراسلات الالكترونية بين التجار الموردين و المستوردين أو بين الشركات فيما بينها .

و يتميز التوقيع الرقمي بمزايا و مخاطر أو سلبيات ، و يمكن إيجاز المزايا فيما يلي :

1-التوقيع الرقمي يؤدي على إفراز المعلومات التي يتضمنها السند أو يهدف إليها صاحب التوقيع.

[1]- عمر محمد أبو بكر بن يونس ، المرجع السابق ، ص ص 425، 427 ، 428 .

2- التوقيع الرقمي دليل على الحقيقة بدرجة أكثر من التوقيع التقليدي.

3-يسمح بإبرام الصفقات عن بعد ، دون حضور المتعاقدين بأشخاصهم ، كما يساعد في تنمية

و ضمان التجارة الالكترونية [1].

كما أيضا يتميز بسلبيات تتمثل فيما يلي :

1-احتمال تعرضه للسرقة أو الضياع مثل التوقيع التقليدي هو عرضة الأخطار كالتزوير و التقليد .2-يمكن تقليد الشريط الممغنط الموجود على بطاقة الائتمان

3-التوقيع الرقمي لا يعبر عن شخصية صاحبه مثل التوقيع التقليدي بالكتابة .

ثانيا : التوقيع بالقلم الالكتروني

يتم باستخدام طريقة Pen-ON أو التوقيع بالقلم الالكتروني و يتم عن طريق استخدام قلم اليكتروني حسابي يمكن عن طريقه الكتابة على شاشة الكمبيوتر و ذلك عن طريق استخدام برنامج خاص للكمبيوتر ، و يقوم هذا البرنامج بوظيفتين[2]:

الأولى هي خدمة التقاط التوقيع و الثانية خدمة التحقق من صحة هذا التوقيع .

حيث يتلقى البرنامج بيانات العميل عن طريق بطاقته الخاصة ،قدور البرنامج هو قياس خصائص معينة للتوقيع من حيث الحجم و الشكل و النقاط و الخطوات و الالتواءات.

و بعد ذلك تأتي مرحلة التحقيق من صحة التوقيع ، يقوم البرنامج بفك الشفرة البيومترية ثم نقارن المعلومات مع التوقيع المخزن و نرسلها إلى برنامج الكمبيوتر الذي يبين إن كان التوقيع صحيحا أم لا؟

و هذا النوع من التشفير البيومتري يقوم بالتحقيق من الشخصية ، عن طريق الاعتماد على الخواص الفيزيائية و الطبيعية و السلوكية للأفراد .

-و هناك طرق عديدة للتعرف البيومتري على الشخص و هي :

1-البصمة الشخصية .

---

[1]-عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 237 ، 238 .

[2] -خالد مصطفى فهمي ، المرجع السابق ، ص 61 ، 62 .

2-مسح العين البشرية .

3-التعرف على الموجه البشري .

4-خواص اليد البشرية .

5-التحقق من نبرة الصوت .

6-التوقيع الشخصي .

7-البطاقة الذكية (*Smart Card*) .

8-طرق أخرى تعتمد على تعاقب نظم الحماية و تعددها في أي نظام .

ثالثا : التوقيع عن طريق الضغط على أحد المفاتيح في لوحة الحاسب الآلي على نحو يفيد الموافقة على التصرف القانوني .

و هي إرسال نموذج للعقد ، إلى موقع المشتري حتى يتمكن من الاطلاع على بنود العقد الذي يحتوي على عبارة تفيد قبوله ، التعاقد (نعم –yes) أو رفضه (لا – NO) و بمجرد قبول المشتري فانه يضغط على مفتاح (return-OK)في لوحة الحاسب الآلي أو في الخانة المخصصة للقبول

و بمجرد التأشير في خانة القبول (OK) يكون المتعاقد قد أفصح عن إرادته في قبول الإيجاب

و بالتالي يبرم العقد .

فهذا ليس كافيا لإثبات العقد ، و لهذا فان مقتضيات التعامل الالكتروني أوجبت ضرورة أن يضع المتعاقد مفتاحه الخاص حتى يتأكد من الشخص المرسل و حتى تتحقق خاصية التوقيع بصفة عامة ، و التوقيع الالكتروني بصفة خاصة [1].

[1] -عبد الفتاح بيومي حجازي ، المرجع السابق ، ص 249 ، 250 .

المبحث الثاني: الوسائل الردعية

بعد التعرض للطرق الوقائية وبالنظر إلى أن 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 بدلا من إصدار تشريعات لمواجهة هذا الهجوم المعلوماتي من طرف نوابغ المعلوماتية وهذه الطرق الردعية تمكن السلطات من متابعة ومراقبة هذه الانتهاكات ومعاقبتهم جنائيا.

المطلب الأول : المعطيات الأساسية للجريمة المعلوماتية و مراقبة الاتصال

يتضمن الأمر 04/09[1] جل القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وسبل مكافحتها قانونيا، وذلك لتجريم أفعال التوابع المعلوماتية من اختراقات للمواقع وجل أعمال التخريب الالكتروني.

وذكر المصدر بأن إنشاء هذه الهيئة نص عليها المرسوم الرئاسي رقم 15-261 المؤرخ **في 24 ذي الحجة عام 1436 الموافق ل 2015/10/08 يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها .**

والمتضمن القواعد الخاصة للوقاية من الجرائم **المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.**

الفرع الأول: أحكام عامة

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

أ- *الجرائم المتصلة بتكنولوجيا الإعلام والاتصال*: 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 14 شعبان 1430 الموافق ل 05 أوت 2009 ، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها الجريدة الرسمية رقم 47 الصادرة بتاريخ 05 أوت 2009

[2]- المادة 01 و 02 و 03 من المرسوم الرئاسي السابق ص: 5، 6 .

ب-*منظومة معلوماتية*: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة أو المتصلة ببعضها البعض أو المرتبطة. يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا 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:

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

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

ه-المعطيات المتعلقة بحركة السير: أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها والطريق الذي يسلكه، ووقت و تاريخ وحجم ومدة الاتصال ونوع الخدمة.

و-الاتصالات الالكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية.

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 الالكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية .

الفرع الثاني: مراقبة الاتصالات الالكترونية

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 اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، أو الاقتصاد الوطني.

ج-لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

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 للإغراض المنصوص عليها في الفقرة "أ" من هذه المادة موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على امن الدولة ومكافحتها، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

المطلب الثاني: القواعد الإجرائية و التزامات مقدمي الخدمات

يتضمن هذا المطلب القواعد الإجرائية في تفتيش المنظومات المعلوماتية والتزامات مقدمي الخدمات بمساعدة السلطات حيث يتضمن الأول حجز المعطيات

[1] - المادة 04 من المرسوم السابق .

المعلوماتية الحجز عن طريق منع الوصول إلى المعطيات المحجوزة ذات المحتوى المجرم وحدود استعمال المعطيات المتحصل عليها أما الثاني فيتضمن حفظ المعطيات المتعلقة بحركة السير والالتزامات الخاصة بمقدمي خدمة "الانترنيت"[1].

الفرع الأول : القواعد الإجرائية تفتيش المنظومة المعلوماتية .

يجوز السلطات القضائية المختصة و كذا ضباط الشرطة القضائية ، في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة الرابعة ، الدخول بغرض التفتيش ، و لو عن بعد إلى[2]:

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

ب-منظومة تخزين معلوماتية.

-و في الحالة المنصوص في الفقرة "أ"من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى ، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا لذلك .

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

يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها ، قصد مساعدتها و تزويدها بكل المعلومات الضرورية لانجاز مهمتها .

عندما تكشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و انه ليس من الضروري حجز كل

---

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

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

منظومة ، يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز و الوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية .يجب في كل الأحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية .

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق ، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات .

إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة السادسة لأسباب تقنية ، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات 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 ، إلا في الحدود الضرورية للتحريات أو للتحقيقات القضائية[1] .

الفرع الثاني : التزامات مقدمي الخدمات بمساعدة السلطات

-في إطار بتطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع و تسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها و يوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة الحادية عشر ، تحت تصرف السلطات المذكورة[2].

[1] - المواد 8 ، 9 الأمر السابق ، ص 07

[2] - المواد 10 ، 11 ، 12 المر السابق ، ص 07 ،08 .

و يتعين على مقدمي الخدمات كتمان على سرية العمليات التي ينجزونها بطلب من المحققين و كذا المعلومات المتصلة بها تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق .

-مع مراعاة طبيعة و نوعية الخدمات يلتزم مقدمو الخدمات بحفظ :

أ-المعطيات التي تسمح بالتعرف على مستعملي الخدمة .

ب-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج-الخصائص التقنية و كذا تاريخ و وقت و مدة كل اتصال .

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

ه-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال و كذا عناوين المواقع المطلع عليها.

-بالنسبة لنشاطات الهاتف،يقوم التعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة و كذا تلك التي تسمح بالتعرف على مصدر الاتصال و تحديد مكانه .

- تحدد مدة حفظ المعطيات المذكورة في هذه الحالة بنسبة واحدة ابتداء من تاريخ التسجيل.

دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة ، تقوم المسؤولية الجزائية للأشخاص الطبيعيين و المعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية ، و يعاقب الشخص الطبيعي بالحبس من ستة أشهر إلى خمس سنوات و بغرامة مالية من 50000 دج إلى 500000 دج .

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات و تحدد كيفيات تطبيق الفقرات 1،2،3 من هذه المادة ، عند الحاجة ، عن طريق التنظيم .

-زيادة على الالتزامات المنصوص عليها في المادة 11 أعلاه ، يتعين على مقدمي خدمات "الانترنيت":

أ-التدخل الفوري لسحب المحتويات التي يحتاجون الاطلاع عليها لمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين و تخزينها أو جعل الدخول إليها غير ممكن .

ب-وضع ترتيبات تقنية تسمح بحصر إمكانية للدخول إلى موزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة و إخبار المشتركين لديهم بوجودها .

المطلب الثالث : الهيئات الوطنية و الدولية المختصة في مكافحة الإجرام المعلوماتي .

يتضمن هذا المطلب لكل من الهيئات الوطنية و الدولية و مجهوداتها لمكافحة الإجرام المعلوماتي .فيتضمن الهيئات الدولية و التعاون الدولي لمكافحة هذا الإجرام المعلوماتي تشمل كل من التعاون و المساعدة القضائية الدولية في الاختصاص القضائي ، المساعدة القضائية الدولية المتبادلة تبادل المعلومات و اتخاذ الإجراءات التحفظية ، وفي الأخير القيود الواردة على طلبات المساعدة القضائية الدولية .

الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاتصال

-تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحته تحدد تشكيلة الهيئة و تنظيمها و كيفيات سيرها عن طريق التنظيم[1] .

-تتولى الهيئة المذكورة في المادة الثالثة عشر، خصوصا المهام الآتية:

أ-تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته .

ب-مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية .

---

[1] - المواد 13 ، 14 ، 15 ، 16 من الأمر رقم 09-04 ، المؤرخ في 14 شعبان 1430 الموافق لـ 05 أوت 2009 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، الجريدة الرسمية ، رقم 47 الصادرة بـ 05 أوت 2009 ، ص 08 .

ج-تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و تحديد مكان تواجدهم .

الفرع الثاني : التعاون و المساعدة القضائية الدولية "الاختصاص القضائي"

-زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية ، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا،و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني .

-في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون

و كشف مرتكبيها . يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني .

يمكن في حالة الاستعجال ، و مع مراعاة الاتفاقيات الدولية و مبدأ المعاملة بالمثل ، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى ، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني ، و ذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها .

-تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة و الاتفاقيات الدولية الثنائية و مبدأ المعاملة بالمثل حيث يرفض تنفيذ طلبات المساعدة إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام .

-يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب[1].

[1] - المواد 17 ، 18 ، 19 : الأمر السابق ، ص 08 .

-و ينشر هذا القانون في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية.

الخـــــاتمة :

إن من انعكاسات استخدام الحاسوب و انتشاره على نحو واسع في حياتنا ظهور فكرة التجارة الالكترونية و هي تجارة تعتمد على وسائل الكترونية بما في ذلك الحاسوب لتمامها ، و لعل الصورة الشائعة لهذه التجارة صورة التجارة عبر الانترنيت أو كما يطلق عليها التعاقد عن بعد ، و مع ذلك فالانترنيت ليس هو الوسيلة الالكترونية الوحيدة لقيام هذه التجارة ، بل حين ظهرت التجارة الالكترونية في القرن الماضي لم تكن هناك مشكلات عملية و قانونية قد ظهرت بعد ، لتؤثر على حركة هذه التجارة و تطورها ، و ذلك لأنها كانت في مهدها ، لكنها في الوقت الحالي و قد انسابت فيها ملايين بل مليارات الدولارات و أصبحت في حاجة إلى تنظيم متكامل ، يضع الأطر المناسبة لنشاطها و ينظمها ، و يكفل الحماية الجنائية للحفاظ على أموال هذه التجارة و بياناتها .

و الحقيقة أن هذه التجارة تعتمد على نظام معلوماتي أدواته كلها الكترونية و تتمثل في جهاز الحاسوب و ملحقاته و أن شبكة الانترنيت و غيرها من التقنيات التي تلعب دورا مؤثرا في هذا النشاط حتى سداد مقابل الوفاء ، يتم بطريقة الكترونية و ذلك عن طريق التحويل الالكتروني للنقود أو التسوق ببطاقات الدفع أو الائتمان.

و ترتبط هذه التجارة بمستوى متقدم من التقنيات الخاصة بالحاسوب و ملحقاته ، وبقدر تقدم الدول ، العلوم يكون دورها في هذه التجارة سواء بوضعها منتجا أو بائعا ، أما البلدان التي لها نصيب متواضع من التكنولوجيا فهي تقوم بدور المستهلك أو المشتري من نطاق هذه التجارة و لهذا فهي ترتبط بالتقدم العلمي ارتباطا وثيقا .

فلم يكن طريق هذه التجارة مهما في بادئ الأمر ، فهناك من المشكلات العملية التي صادفتها الكثير و الكثير من ذلك ثقة المستهلك و مدى اطمئنانه إلى التسوق بعيدا عن المتجر التقليدي الذي يعاين فيه السلعة و يختارها و هو أمر يرتبط بطبيعة المستهلك ، و هناك كذلك بيانات هذه التجارة التي يمكن اختراقها على الشبكة و إساءة استعمالها ، و هو ما أدى بخبراء الحاسوب إلى اللجوء لتقنيات متقدمة لحماية هذه البيانات ، و تمثل ذلك في تشفير هذه البيانات و ترميزها ، و قد أسفر التقدم العلمي عن وسيلة جديدة و آمنة للتوقع على صفقات هذه التجارة ، هي التوقيع الالكتروني الذي يكاد أن يكون من المستحيل تقليده أو تزويره و ذلك لأن خبراء الحاسوب وضعو له وسائل فنية فعالة للحماية من الاختراق .

إذن كان من الملائم أن تتعرض لنظام التجارة الالكترونية و أن ندرجها في فصلين .

فبقي أن نقول بأن رغم قلة النصوص القانونية في الجزائر ارتأينا أن ندرس الحماية الجنائية للتجارة الالكترونية بصفة عامة .

و في الختام نتمنى أن نكون قد وفقنا في انجاز هذه المذكرة فان أصبنا فمن الله و إن أخطأنا فمن أنفسنا و الشيطان ، و الكمال لله عز وجل.

قائمة المصادر والمراجع:

أولا الكتب:

1/ أجمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي القاهرة، الطبعة الثانية، سنة 2006 .

2/ خالد مصطفى فهمي، النظام القانوني للتوقيع الالكتروني في ضوء التشريعات العربية والاتفاقيات الدولية، دار الجامعة الجيدة، مصر، بدون طبعة، سنة2007.

3/ شافع بلعيد عاشور، العولمة التجارية والقانونية للتجارة الالكترونية، دار هوما للطباعة والنشر والتوزيع، الجزائر، بدون طبعة، سنة 2006 .

4/ شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، مصر، بدون طبعة، سنة 2007.

5/ عبد الحميد بسيوني، عبد الكريم عبد الحميد بسيوني ، التجارة الالكترونية ، دار الكتب للنشر و التوزيع ، بدون طبعة، سنة 2003.

6/ عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الحماية الجنائية للتجارة الالكترونية، الكتاب الثاني، دار الفكر الجامعي، مصر، بدون طبعة ، سنة 2007.

07/ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، مصر، الطبعة الأولى، سنة 2006.

08/ محمد أبوبكر بن يونس، الأحكام الموضوعية والجوانب الإجرامية، الجرائم الناشئة عن استخدام الانترنت، دار النهضة العربية، القاهرة، بدون طبعة، سنة .2004

09/ محمد أمين الشوابكة، جرائم الحاسوب والانترنت، مكتبة دار الثقافة للنشر والتوزيع، الطبعة الأولى، سنة 2004.

10/ محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الاسكندرية، بدون طبعة، سنة 2004.

11/ هدى حامد قشقوش، جرائم الحاسب في التشريع المقارن، دار النهضة العربية، بدون طبعة، بدون سنة.

ثانيا: الرسائل و المذكرات

مذكرة تخرج لنيل شهادة ليسانس في الحقوق، جرائم النصب الالكتروني، قبلي علال، بن لخضر عبد الكريم، سنة 2007-2008 .

2- مذكرة تخرج لنسل شهادة ليسانس في العلوم القانونية والإدارية، الحماية القانونية للتجارة الالكترونية، جبوري فتيحة، حداد خيرة، سنة 2007-2008.

ثالثا: القوانين و المراسيم التنفيذية

1/ قانون رقم: 23/06 المؤرخ في 20 ديسمبر 2006، الدار البيضاء، الجزائر بدون طبعة سنة 2007 .

2/ الأمر رقم: 04/09 المؤرخ في 14 شعبان 1430 الموافق 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، الجريدة الرسمية رقم 47 الصادرة بتاريخ: 2009/08/05.

3/ المرسوم الرئاسي رقم 261/15 المؤرخ في 24 ذي الحجة عام 1436 الموافق ل2015/10/08.