الحماية الجنائية لمواقع التجارة الإلكترونية عبر الانترنت

بقلم
أ/ مريم خليفي
كلية الحقوق والعلوم السياسية. جامعة بشار. الجزائر

الملخص

تهدف هذه الدراسة إلى توضيح أهمية الحماية الجنائية لمواقع التجارة الإلكترونية، باعتبار أن جميع الجرائم التي تمس النظم المعلوماتية تؤثر سلبا على هذا النوع من التجارة.

فالبيئة الافتراضية التي ينعدم فيها الأمن لا تشجع المتعاملين بالقيام بعمليات الشراء عبر الإنترنت دون ضمانات قانونية، لذلك فإن بناء الثقة من خلال تطويع النصوص التي تتناول الحماية الجنائية لمواقع التجارة الإلكترونية ينبغي أن يمثل الأولوية بالنسبة للمشرع، وذلك بهدف توفير إطار قانوني يضمن انسياب معاملات التجارة الإلكترونية العالمية، وعليه فالكثير من التساؤلات القانونية التي تطرح في هذا السياق، هو ما يمثل محور هذه الدراسة.

Résumé:

Cette étude vise à clarifier l'importance de la protection pénale des sites de commerce électronique, parce que tous les crimes qui touchent le système d'information ont un impact négatif sur ce type de commerce.

un tel climat d'insécurité, n'est pas pour encourager les internautes à effectuer des achats via l'Internet sans garanties juridiques.

Instaurer la confiance par l'adaptation de textes traitant de la protection pénale des sites de commerce électronique devrait donc être la priorité du législateur , sans aucun doute , de fournir un cadre juridique favorisant l'éclosion du commerce électronique mondiale.

Ainsi, toutes les questions qui se posent à cet égard, feront le noyau de notre étude

مقدمة

أدى التزاوج ما بين تقنية المعلومات L'informatique وتقنية الاتصال عن بعدLa Télématique إلى تغيير شكل النشاط التجاري من تقليدي إلى إلكتروني، فشاع في ظل الانتشار الهائل للانترنت مصطلح "التجارة الإلكترونية "Le commerce électronique التي أصبحت واقعا عمليا يفرض نفسه على جميع المستويات.

وفي ظل خاصية الانفتاح التي تتميز بها شبكة الانترنت حيث تعتبر عابرة للحدود بطبيعتها سارعت المشاريع التجارية إلى فرض وجودها ضمن هذا الفضاء الجديد من خلال إنشاء مواقع لها على الشبكة تعبر عن نشاطها وتميز منتجاتها وخدماتها، وبذلك أصبحت مواقع الانترنت الوسيلة الأساسية للقيام بعمليات التجارة الإلكترونية.

والحديث عن الحماية الجنائية لموقع التجارة الإلكترونية يعني بالضرورة وجود فعل يشكل بنظر قانون العقوبات جريمة يعاقب عليها، ويرصد لها الجزاء الرادع [(1)]، وهو الأمر المتوفر بالنسبة للنظام المعلوماتي للتجارة الإلكترونية، على اعتبار أن الجرائم التي قد ترتكب بحقها من الجرائم التي ترتكب على أي نظام معلوماتي آخر، وبالتالي فإنها تتعرض لأي مخاطر تهدد المعلوماتية[(2)]، وهي الجرائم التي يطلق عليها انسجاما مع البيئة الرقمية والثورة التقنية بـ: " الجرائم المعلوماتية " Les crimes informatiques [(3)].

وعليه ولما كان مستقبل التجارة الإلكترونية العالمية متوقف على ثقة العملاء فمن الواجب حماية مواقع التجارة الإلكترونية وذلك بتجريم أفعال الاعتداء على هذه المواقع لحماية نظم البيانات الخاصة بالعمليات التجارية عبر الانترنت (المبحث الأول).

ومن جانب آخر ولتحليل موضوع الحماية الجنائية لموقع التجارة الإلكترونية تحليلا معمقا نوعا ما فلا بد من بيان مدى معالجة التشريعات والقوانين العقابية الحالية لهذا النوع من الإجرام الذي يمس التجارة

الإلكترونية، وبيان فيما إذا كانت خطة مختلف التشريعات في موضع النص على الحماية تعتبر كافية، أم أن الأمر بحاجة إلى تعديلات وتغييرات، خاصة وأن محل هذه الحماية هو الموقع التجاري الافتراضي الذي يعد من الأمور المستحدثة عند صدور العديد من التشريعات الجزائية (المبحث الثاني).

المبحث الأول:
تجريم أفعال الاعتداء على المواقع المخصصة للتجارة الإلكترونية

سبق التنويه إلى أن جرائم الاعتداء على مواقع التجارة الإلكترونية تصنف ضمن الجرائم المعلوماتية، وبالأخص ضمن جرائم التعدي على نظام المعالجة الآلية للبيانات أو المعطيات، فكل ما يتعلق بعمليات التجارة الإلكترونية محلها بيانات معالجة إلكترونيا[4]، ومن ثم فإن اختراق موقع التجارة الإلكتروني هو اختراق لنظامها المعلوماتي الذي يستند إلى قاعدة بيانات تخدم هذه التجارة وعليه فإن الدخول غير المشروع للمواقع يعد من أكثر الجرائم خطورة، لذلك فمن المهم بسط البحث والتعرض لجريمة الدخول أو البقاء غير المشروع في النظام (المطلب الأول)، ثم التطرق لجريمة التلاعب في المعطيات الموجودة داخل نظم التجارة الإلكترونية (المطلب الثاني).

المطلب الأول: جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات

بما أن التجارة الإلكترونية تعتمد على تقنية المعالجة الإلكترونية للمعطيات والبيانات، فإن الاعتداء على مواقعها لا يخرج عن كونه أحد تطبيقات الاعتداء على نظم المعالجة الآلية للمعطيات.

ويقتضي الأمر قبل الحديث عن هذه الجرائم، تحديد المقصود بنظام المعالجة الآلية للبيانات وقد عرفه الفقه الفرنسي بأنه:" كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج و المعطيات و أجهزة الإدخال والإخراج و أجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة

المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية "[5].

فالمعالجة الآلية للمعلومات هي مجموعة العمليات التي تتم آليا باستخدام الحاسب الآلي وتتعلق بجمع البيانات، وإدخالها إلى الحاسب الآلي ومعالجتها وفقا لبرامج وصولا إلى إخراجها على شكل معلومات لها دلالة خاصة.

وعلى ذلك فهذه الجرائم تتطلب ابتداء توافر نظام المعالجة الآلية للمعطيات بمكوناته المادية والمعنوية، فإذا وقع الاعتداء على عنصر بمفرده لا يشكل جزءا من هذا النظام فلا يعتبر جريمة من الجرائم الماسة بالمعلوماتية.

وقد تعرضت الكثير من أنظمة الحاسب الآلي، وبصفة خاصة تلك التي تعمل من خلال شبكات المعلومات كالتي تخص عمليات التجارة الإلكترونية إلى الاختراق بواسطة أشخاص غير مرخص لهم بالدخول إليها، وفي هذا الصدد جرم المشرع الجزائري فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات من خلال نص المادة 394 من قانون العقوبات الجزائري [6]، والتي تنص على أنه:" يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50000 دج إلى 100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج".

من خلال النص يتضح أن المشرع الجزائري لم يحدد وسيلة الدخول إلى النظام واختراقه على غرار باقي التشريعات، فتقع الجريمة باستخدام أية وسيلة تقنية، مثل انتهاك كلمة السر أو عن طريق استخدام برامج أو

شفرات[7]، أو بواسطة استغلال ضعف النظام في حد ذاته .

وقد يتم الدخول إلى النظام بطريقة مباشرة بواسطة الحاسب الآلي، أو بطريقة غير مباشرة عندما يتم الدخول بواسطة نظام آخر يتصل بالأول بواسطة شبكة الاتصال، أو بالتقاط الإشارات التي يحدثها الجهاز الإلكتروني دون الحاجة إلى الدخول عبر الشبكة.

ويشبه بعض الفقه الفرنسي فعل الدخول بمثابة الدخول إلى ذاكرة الإنسان في مدلوله المعنوي وفي مدلوله المادي أن يكون الشخص قد حاول الدخول أو دخل بالفعل إلى النظام المعلوماتي.

ويمكن القول بصفة عامة أن الدخول غير المشروع أو غير المصرح به إلى نظام المعالجة الآلية للمعطيات يتحقق بالوصول إلى المعلومات والبيانات المخزونة داخل نظام الحاسب دون رضا المسؤول عن هذا النظام أو المعلومات التي يحتوي عليها [8].

وتقع هذه الجريمة من أي شخص مهما كانت صفته، سواء كان يعمل في مجال الأنظمة أم لا وسواء كانت له المقدرة على الاستفادة من النظام أم لا، فيكفي أن يكون الجاني ممن ليس لهم الحق بالدخول إلى النظام[9]، فالدخول غير المشروع يستمد مشروعيته من كونه غير مصرح به سواء كان مقصودا في حد ذاته أو وسيلة لتحقيق غاية أخرى، فمناط عدم المشروعية إذن انعدام سلطة الفاعل في الدخول مع علمه بذلك، سواء تم دون تصريح، أو تجاوز التصريح الممنوح له بالدخول إلى معطيات لا يشملها التصريح.

كما أن الدخول يعد غير مشروع متى كان ضدا ومخالفا لإرادة صاحب النظام، أو من له حق السيطرة عليه، كأن يضع بعض القيود للدخول ولم يحترمها الجاني[10]، ويتحقق حتى في حالة تطلب الأمر سداد مبلغ معين للدخول كما الحال بالنسبة لبعض المواقع، وتحايل الجاني ودخل مع ذلك.

وسواء تم الولوج إلى كل النظام أو جزء منه يتحقق الدخول غير المصرح به، كما لو دخل الجاني إلى الجزء المسموح به وتجاوزه إلى الجزء غير

المسموح له بالدخول فيه، مثل لو دخل الشخص لأحد المواقع التجارية وهو موقع مفتوح للجمهور لكنه تجاوز الموقع للدخول إلى البيانات الخاصة بإعداد المواقع التي تحتوي على معلومات غير مرخص الاطلاع عليها [11].

وننوه في هذا الشأن أنه يكفي الدخول المجرد للنظام ليشكل جريمة حتى وإن لم ينجح الجاني في الوصول إلى المعلومات أو البيانات والبرامج [12].

أما بالنسبة لفعل البقاء غير المشروع، فقد يجد الشخص نفسه في بعض الأحيان داخل نظام لحاسب آلي معين غير مسموح له بالدخول عن طريق الخطأ[13]، كما لو كان في طريقه للدخول إلى نظام مرخص له بالدخول إليه، ليجد نفسه يستخدم شفرة خاطئة تجيز له الدخول إلى نظام آخر وهنا على هذا الشخص الخروج فورا بمجرد التنبه للخطأ، أما وإن استمر في البقاء داخل نظام المعالجة الآلية للبيانات رغم معرفته بأن بقاءه غير مشروع ففعله يشكل جريمة البقاء غير المصرح به داخل النظام المعلوماتي.

ويمكن تحقق البقاء إذا ما كان للجاني الحق في الدخول إلى جزء من النظام و يتجاوزه إلى جزء آخر ويبقى فيه رغم علمه بعدم مشروعية البقاء، كما قد يكون البقاء لاحقا على دخول غير مشروع فنكون بصدد تعدد مادي بين الجريمتين، وبالتالي قد تتحقق جريمة البقاء بشكل مستقل عن جريمة الدخول وقد تجتمعان، ويذهب البعض إلى القول أن الاختلاف ما بين الدخول والبقاء كون جريمة الدخول جريمة إيجابية، وأن جريمة البقاء جريمة سلبية فرغم دخول الجاني بطريق الخطأ إلى النظام فهو يرفض الخروج منه.

وهنا أيضا يكفي لتحقق الجريمة البقاء في كل النظام أو البقاء في جزء منه فقط، بل حتى ولو كان البقاء مجردا [14].

ومن المهم أن نشير إلى أن جريمتي الدخول والبقاء داخل النظام حسب نص المادة 394 من قانون العقوبات الجزائري السابق الإشارة إليه تتشدد، إذا تحقق ظرفين:

1. إذا نتج عن الدخول أو البقاء محو أو تعديل للمعطيات التي يحتويها النظام.

2. إذا نتج عن الدخول أو البقاء تخريب النظام بمعنى عدم صلاحيته لأداء وظائفه.

ويكفي لتحقق الظرف وجود العلاقة السببية بين الدخول أو البقاء غير المشروع و تلك النتيجة الضارة ولو لم تكن مقصودة.

من جانب آخر وفيما يتعلق بالركن المعنوي للجريمة فيتخذ صورة القصد الجنائي العام الذي يتكون من عنصري العلم و الإرادة، فيجب أن يعلم الجاني بأنه لا يحق له الدخول أو البقاء داخل النظام، و بالتالي لا يتوافر العنصر المعنوي إذا كان الدخول مشروع، أو كان دخوله عن طريق الصدفة أو السهو أو الخطأ، فإذا لم ينسحب منذ اكتشافه الخطأ توافر القصد الجنائي لديه، إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش، فمتى توافر القصد الجنائي وهو العلم و الإرادة فلا محل للاعتداد بالباعث على ارتكاب الجريمة، فتتحقق هذه الأخيرة ولو كان الباعث الفضول أو النزهة أو إثبات الإمكانيات لخرق النظام المعلوماتي.

المطلب الثاني: جريمة التلاعب في المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات

اتجهت أغلبية التشريعات الجنائية التي عنت بحماية المعطيات إلى النص على هذه الجريمة ضمن نصوصها العقابية، وهو ما نجده في نص المادتين 394 مكرر 1، 394 مكرر 2 من قانون العقوبات الجزائري، فالمشرع هنا لا يحمي النظام في حد ذاته وإنما يوفر الحماية للبيانات الموجودة داخل النظام، والتي أدخلت لمعالجتها، ويتخذ التلاعب في معطيات النظام صورتين:

1. الاعتداء العمدي على المعطيات الموجودة داخل النظام:

يتمثل النشاط الإجرامي في هذه الجريمة بفعل الإدخال والمحو والتعديل، ويكفي توافر إحداها لقيام الجريمة، وبذلك يتم الاعتداء على البيانات التي أدخلت لمعالجتها والتي ستحول إلى معلومات بعد المعالجة، حيث جاء في نص المادة 394 مكرر 1 من قانون العقوبات الجزائري:" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو

عدل بطريق الغش المعطيات التي يتضمنها ".

فعل الإدخال Intrusion: يقصد به إضافة معطيات جديدة على الدعامة الخاصة سواء كانت خالية أم كان يوجد عليها معطيات من قبل، كالتلاعب في أرقام الحسابات البنكية بإضافة حسابات وهمية على مستوى موقع التجارة الإلكترونية مما يؤدي إلى التلاعب في بيانات هذه التجارة.

فعل المحو Effacement: يقصد به إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، بما ينجم عنه إتلاف البيانات.

فعل التعديل Modification: يقصد به تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى مخالفة لما كانت عليه.

ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها، مما يعطي في النهاية نتائج مغايرة لتلك التي صمم من أجلها البرنامج [15].

والأفعال السابقة سواء كانت إدخال أو محو أو تعديل وردت في نص المادة المشار إليها على سبيل الحصر، فأي فعل غيرها لا يقع تحت طائلة التجريم.

من جهة أخرى حتى يتوافر قصد التجريم لا بد أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، مع علمه بأن هذا الفعل غير مشروع، ورغما عن إرادة صاحب الحق في المعطيات أو من له السيطرة عليها.

2.المساس العمدي بالمعطيات خارج النظام:

وفر المشرع الجزائري مزيدا من الحماية على المعطيات في حد ذاتها[16]، فلم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات، أو أن يكون قد تم معالجتها آليا ما دامت قد تستخدم لارتكاب الجرائم المنصوص عليها والتي تمس النظام المعلوماتي، وذلك من خلال نص المادة 394 مكرر2 من قانون العقوبات الجزائري:" يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 دج إلى 5000000 دج كل من يقوم عمدا وعن طريق الغش.

1ـ تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2 ـ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم ".

وهنا لا بد أن يتم استخدام المعطيات لارتكاب الجرائم المذكورة عمدا و بطريق الغش، أي توافر القصد الجنائي العام إضافة إلى القصد الجنائي الخاص المتمثل في نية الغش(17).

ومن المفيد في الأخير أن نشير إلى أن المشرع الجزائري على غرار المشرع الفرنسي"(18) عاقب على الاشتراك في الاتفاق الجنائي في نص المادة 394 مكرر5 من قانون العقوبات الجزائري والتي جاء فيها:

" كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها، من خلال نص المادة يتضح أن شروطه الاشتراك لقيام الجريمة تتمثل في:

- مجموعة أو اتفاق في صورة شركة أو مؤسسة أو جماعة.
- هدف التحضير لإحدى الجرائم الماسة بالأنظمة المعلوماتية.
- يتجسد هذا التحضير بشكل فعل مادي.
- توافر القصد الجنائي، باتجاه إرادة كل عضو إلى ارتكاب هذا النشاط الإجرامي.

من خلال ما سبق نلاحظ أن جميع الجرائم التي تمس النظام المعلوماتي تؤثر سلبا على التجارة الإلكترونية كونها تعتمد أساسا على نظم معلوماتية، إذا ما تم اختراقها سبب ذلك تخوف المتعاملين في هذا المجال من وضع ثقتهم بهذا النظام التجاري الحديث، فالاعتداء بالدخول غير المشروع إلى الموقع الإلكتروني أو بحذفه أو تعديله أو تعطيله، يهدد مستقبل التجارة الإلكترونية بشكل عام، الأمر الذي نجم عنه اختلاف خطة التشريعات المختلفة لاستيعاب

مثل هذه الجرائم بما يوفر الحماية الجنائية لموقع التجارة الإلكترونية، وهو ما سنتعرض له بشيء من التفصيل قي المبحث التالي.

المبحث الثاني:
موقف التشريعات في موضع النص على الحماية الجنائية لمواقع التجارة الإلكترونية

الحقيقة أن الاعتداء على مواقع التجارة الإلكترونية لا يخرج عن كونه تطبيقا لأفعال الاعتداء على أجهزة الحاسب والبرامج وقواعد البيانات، والتي تمثل اعتداء على أنظمة الحاسب، حيث يستخدم في إعداد هذه المواقع أنظمة معلوماتية، وقد لاحظ المشرع في أغلبية الدول خطورة هذه الأفعال وتدخل لتجريمها بما يوفر حماية جنائية لها، غير أن خطة التشريعات فيما يتعلق بهذه الحماية تختلف فمنها ما جرمت أفعال الاعتداء على الأنظمة المعلوماتية بصورها المختلفة في قانون خاص وبشكل مستقل، فيما ذهبت أخرى إلى إدخال تعديلات على نصوصها القائمة على نحو يستوعب هذه الصور المستحدثة للجرائم، بينما اكتفت بعض التشريعات بالنصوص التقليدية، وعليه ولمزيد من التوضيح لنا أن نستعرض بشيء من التوسع الحماية الجنائية لموقع التجارة الإلكترونية في التشريعات الأجنبية (المطلب الأول)، وكذا لموضع النص على هذه الحماية في التشريعات العربية (المطلب الثاني) .

المطلب الأول: الحماية الجنائية لمواقع التجارة الإلكترونية في التشريعات الأجنبية

أحدثت ثورة المعلومات والاتصالات تغيرات جذرية في المفاهيم القانونية والتي مست نطاق القانون الجنائي، مما دفع المشرع في بعض الدول ليواكب تشريعيا هذا التطور التكنولوجي الهائل الذي ساهم في إبراز نوع مستحدث من الجرائم، أن يصدر العديد من التشريعات لمواجهة جميع صور المساس بالنظام المعلوماتي والبيانات المتواجدة بداخله، وهو ما اتبعه المشرع في الاتحاد الأوروبي والولايات المتحدة الأمريكية وفرنسا وفي دوقية لكسمبورج.

- أولا: الحماية الجنائية لمواقع التجارة الإلكترونية في الاتحاد الأوروبي:

شعر الاتحاد الأوروبي بخطورة جرائم الكمبيوتر، فعملت اللجنة

الأوروبية بشأن مشاكل الجريمة ولجنة الخبراء في مجال جرائم الكمبيوتر على اعتماد مشروع اتفاقية تتعلق بجرائم الكمبيوتر، وقد أعلن المجلس الأوروبي مشروع هذه الاتفاقية في 27 أبريل 2000، مؤكدا على أن الاعتداءات على مواقع الانترنت التجارية مثل أمازون دوت كوم Amazon.com هي التي وجهت نظر المجتمع الدولي إلى أن جرائم الكمبيوتر تهدد التجارة الإلكترونية والاقتصاد العالمي بشكل عام[19].

وفي نوفمبر 2001 و تحديدا في العاصمة المجرية بودبست وقعت الولايات المتحدة الأمريكية وتسع وعشرون دولة أخرى الاتفاقية الصادرة عن المجلس الأوروبي بشأن جرائم الانترنت.

وجاءت الاتفاقية بشكل عام لمواجهة النشاطات الإجرامية الناتجة عن الدخول غير المشروع لشبكة الانترنت والأنظمة المعلوماتية، وقد وجهت الاتفاقية عناية الدول المتعاقدة إلى أن تجرم الأفعال الماسة بسرية وتكامل بيانات الكمبيوتر وأنظمة الاتصال بها، ومن بين ما حددته من هذه الأفعال الدخول العمدي غير المشروع على نظام الكمبيوتر بصورة كلية أو جزئية.

وأيضا أكدت نصوصها على تشجيع التعاون الدولي للحد من جرائم الانترنت العابرة للحدود بطبيعتها، كما أوصت الدول الأطراف أن توفر الوسائل والإجراءات الكافية للتحقيق والاستدلال في مثل هذه الجرائم.

- ثانيا: الحماية الجنائية لمواقع التجارة الإلكترونية في الولايات المتحدة الأمريكية:

تحظر الحكومة الفدرالية للولايات المتحدة الأمريكية الدخول غير المشروع إلى الكمبيوتر ومواقع الانترنت، وفي هذا الصدد أصدر الكونغرس الأمريكي أول تشريع فدرالي بشأن جرائم الحاسوب سنة 1984 الذي تم تعديله سنة 1986 وكذلك خلال 1990، 1994، 1996، ويعاقب هذا القانون كل من يدخل عمدا على جهاز كمبيوتر دون تصريح أو بتجاوز التصريح الممنوح له، ويحصل على معلومات موجودة في سجل اقتصادي يخص

مؤسسة مالية أو يخص مانح لبطاقة مالية أو المعلومات الموجودة في تقرير يتعلق بالمستهلكين، كما يفرض القانون عقوبات على الأفعال التالية:

- الدخول إلى جهاز كمبيوتر يستخدم في التجارة أو الاتصال بين الولايات و يقوم عمدا بنقل لبرامج أو كود لكمبيوتر أو نظام للكمبيوتر.
- منع أو حرمان أو التسبب في منع أو حرمان الغير من استعمال كمبيوتر أو خدمات كمبيوتر أو نظام أو شبكة أو معلومات أو بيانات أو برنامج.
- نقل مكونات لبرنامج أو كود أو أمر دون موافقة من المسئولين على الكمبيوتر المستقبل للبرنامج أو المعلومات أو الكود أو الأمر إذا أدى هذا النقل إلى خسائر.
- نقل برنامج معلومات أو كود أو أمر بطريق الكمبيوتر لجهاز يستخدم في التجارة أو الاتصال بين الولايات ويشكل الفعل خطورة إذا النقل أضر أو تسبب في الإضرار بكمبيوتر أو بنظام كمبيوتر أو شبكة أو معلومة أو بيان أو برنامج.
- غش كلمات المرور بما يسمح بالدخول على نظام الكمبيوتر دون تصريح إذا كان من شأن ذلك الإضرار بالتجارة بين الولايات أو بالتجارة الخارجية.

- ثالثا: الحماية الجنائية لمواقع التجارة الإلكترونية في التشريع الفرنسي

استقر الفكر القانوني لدى المشرع الفرنسي أنه لا بد من وجود نصوص خاصة تجرم أفعال الاعتداء على المعلوماتية، وقد جسد المشرع ذلك من خلال القانون الصادر في 6 يناير 1978 الذي يواجه الجرائم المتعلقة بالمعالجة الإلكترونية للبيانات"[20]، ثم بعد ذلك وتحديدا في سنة 1985 تقدم وزير العدل بمشروع قانون عقوبات جديد يتضمن تجريم التقاط البرامج أو المعطيات أو أي عنصر آخر من النظام المعلوماتي عمدا، وتخريب أو تعييب كل أو جزء من نظام المعالجة الآلية للبيانات وكذلك عرقلة أدائه لوظيفته، والحصول أو السماح بالحصول على فائدة غير مشروعة عن طريق الاستخدام غير المشروع لنظام المعالجة الآلية للبيانات، لكن هذا المشروع لم يجسد.

وفي 5 أوت 1986 تم اقتراح تعديل لبعض النصوص القائمة في قانون العقوبات وتم الاتفاق فيما بعد بمجلس الشيوخ على أن ينص في قانون العقوبات الجديد على الجرائم المعلوماتية، التي أصبحت تشكل الباب الثالث من الكتاب الثالث من القسم الثاني من قانون العقوبات، حيث تتضمن نصوص المواد تجريم الدخول باستخدام وسيلة تقنية أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات أو في جزء منه [21]، كالدخول باستخدام كلمة السر أو برنامج أو شفرة خاصة [22]، وتتشدد العقوبة في حالة محو أو حذف أو تعديل المعطيات الموجودة داخل النظام أو إفساد وظيفته[23] والتي تشكل في النهاية حماية جنائية لموقع الانترنت، بعد ذلك صدر قانون العقوبات الفرنسي الجديد عام 1994 الذي تضمن جريمة التزوير المعلوماتي لإضفاء الحماية للمستندات القانونية أيا كان شكلها [24].

- رابعا: الحماية الجنائية لمواقع التجارة الإلكترونية في دوقية لوكسمبورج

أقر مجلس نواب دوقية لوكسمبورج قانون التجارة الإلكترونية في يوليو 2000، هذا القانون يعد انعكاسا لتوصيات الاتحاد الأوروبي بشان الاهتمام بحماية التجارة الإلكترونية، كما يعكس من جانب آخر الحاجة لسد الفراغ التشريعي في القوانين القائمة والتي تعجز عن تنظيم الحماية القانونية للتجارة الإلكترونية [25].

وفيما يخص موضع النص على الحماية الجنائية لمواقع التجارة الإلكترونية فإن القانون في نص المادة 41 منه عاقب على الدخول أو البقاء غير المشروع بصورة كلية أو جزئية بنظم معالجة أو نقل البيانات إلكترونيا، وتشديد العقوبة إذا ترتب على هذا الدخول حذف أو تعديل البيانات الموجودة بالنظام.

أما في نص المادة 42 فتضمن إيقاع العقوبة على أي شخص يقوم بالإعاقة أو الإخلال العمدي بتشغيل نظم المعالجة أو النقل الإلكتروني للبيانات، ودون المراعاة لحقوق الغير.

كما عاقب القانون في نص المادة 43 أي شخص يقوم عمدا بالإخلال بحقوق الغير، وذلك عن طريق إدخال مباشر أو غير مباشر لبيانات بنظام المعالجة أو نقل البيانات إلكترونيا أو محو أو إلغاء أو تعديل البيانات التي يحويها النظام أو أسلوب معالجته أو نقله للبيانات، كما جعل القانون الكتابة الإلكترونية محلا للتزوير تماما مثل الكتابة التقليدية، وهو ما تضمنه نص المادة 35 من القانون.

يتضح من خلال استقراء نصوص هذا القانون، أنها تتضمن نفس ما ورد في نصوص قانون العقوبات الفرنسي وكذلك قانون العقوبات الجزائري، وهو ما يؤكد على أن النصوص التي يتضمنها قانون العقوبات الفرنسي وحتى الجزائري بشأن المساس بأنظمة المعالجة الآلية للمعطيات تطبق فعلا بشأن حماية مواقع التجارة الإلكترونية، وما يفسر عدم وجود الحاجة الملحة للتدخل و إصدار نصوص جديدة تتعلق بحماية هذه المواقع.

المطلب الثاني: الحماية الجنائية لمواقع التجارة الإلكترونية في التشريعات العربية

مع انتشار وانسياب معاملات التجارة الإلكترونية ظهرت الحاجة الماسة لتنظيم جميع جوانبها القانونية[26]، وإذا كنا بصدد الحديث عن التشريعات العربية المنظمة للتجارة الإلكترونية ولحمايتها الجنائية، فذلك يستلزم منا البدء حتما بقانون التجارة الإلكترونية في تونس أولا باعتباره أول قانون صدر عن مبادرة من مشرع عربي لمحاولة وضع تأطير متكامل للمبادلات التجارية الإلكترونية وهو نفس ما سعى إليه المشرع الإماراتي ثانيا و الذي حذا حذو مثيله التونسي بسن قوانين تنظم المعاملات الإلكترونية التجارية في جميع جوانبها .

- أولا: الحماية الجنائية لمواقع التجارة الإلكترونية في تونس

تعتبر تونس من أول الدول العربية التي قامت بتنظيم التجارة والمبادلات الإلكترونية وذلك بموجب القانون الخاص بالمبادلات التجارية الإلكترونية التونسي رقم 2000 ـ 83 في 9 أوت 2000 الذي نشر في جريدة الرائد الرسمي

للجمهورية التونسية رقم 64 في 11 أوت 2000 وهو أول تشريع عربي يصدر في هذا المجال.

وقد اهتمت تونس بإصدار هذا التشريع من أجل تطوير المبادلات التجارية الخارجية ومواكبة الاقتصاد العالمي كرؤية مستقبلية منها لتحقيق معدل نمو اقتصادي هام في ظل الاقتصاد الرقمي الذي يعتمد على المعلوماتية والاستخدام الموسع لشبكة الانترنت، وبالتالي ومن أجل الصورة الجديدة للتجارة العالمية بالطريق الإلكتروني والتي تعتمد على مفردات جديدة لم تكن منظمة من قبل قام المشرع التونسي بمعالجة الموضوعات التي تشملها هذه التجارة ضمن ثلاثة و خمسين مادة في سبعة أبواب.

ومن الأحكام التي يتضمنها هذا القانون نجد الأحكام الخاصة بالمخالفات والعقوبات من خلال المواد من 43 إلى 53، والتي تجرم أنماط السلوك التي تمثل اعتداء على مواقع التجارة الإلكترونية

كجريمة التعامل في البيانات الإلكترونية الموجودة ضمن المواقع بدون ترخيص وجريمة الاعتداء على البيانات المشفرة.

فالمشرع التونسي ذكر بعض أفعال الاعتداء على أموال وبيانات التجارة الإلكترونية والتي تمثل جرائم جنائية حتى يوفر الحماية الجنائية لمعاملات التجارة الإلكترونية.

- ثانيا: الحماية الجنائية لمواقع التجارة الإلكترونية في دولة الإمارات العربية المتحدة

يعتبر تشريع إمارة دبي في شان المعاملات والتجارة الإلكترونية والصادر بالقانون رقم 2 لسنة 2002 أول تشريع لاحق للتشريع التونسي، وقد اتخذت دولة الإمارات العربية هذه المبادرة كونها تعد في مقدمة الدول العربية التي دخلت في ممارسات التجارة الإلكترونية وذلك في ظل توافر البيئة الفنية لاستخدام هذه تقنيات، وقد خصص المشرع في هذا القانون الفصل السابع منه للعقوبات حيث حظر أن تنسب شهادة المصادقة الإلكترونية إلى شخص

لم يوقعها أو لم تصدر عنه، كما حظر المشرع أن تستعمل شهادة أوقفت أو ألغيت لأي سبب من الأسباب، ومن جانب آخر يعاقب القانون كذلك كل شخص تمكن بموجب السلطات الممنوحة له من الاطلاع على معلومات أو سجلات أو مستندات أو مراسلات إلكترونية.

وفي شأن حماية مواقع التجارة الإلكترونية، فإن دولة الإمارات العربية المتحدة أول دولة عربية تصدر قانونا مختصا في مكافحة جرائم المعلومات يتناول أغلب هذه الجرائم، وهو أول قانون في الدول العربية يصدر بشكل مستقل لهذا الغرض ونقصد هنا قانون اتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات منشور في العدد رقم(442) في الجريدة الرسمية.

ونظرا لتنبه المشرع الإماراتي إلى أخطار الدخول غير المشروع لمواقع التجارة الإلكترونية أو أي نظام معلومات، فقد عاقب على الأفعال التي تشكل اعتداء عليها وذلك في نص المادة الثانية والمادة الخامسة والمادة السادسة من القانون وبذلك يكون قد جرم الأفعال التالية:

1 - كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به.

2 - فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات.

3 - كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأية وسيلة كانت عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.

4 - كل من أدخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات فيها.

من خلال ما سبق نلمح اهتمام التشريعات العربية على غرار التشريعات الأجنبية بموضوع التنظيم القانوني للتجارة الإلكترونية بما في ذلك الحماية

الجنائية لها، ومن بين الأمور التي ركزت عليها التشريعات في هذا الصدد تجريم الدخول العمدي غير المشروع للمواقع ونظم المعلومات بأي وسيلة تقنية، وقد اختلفت خطة التشريعات في ذلك، فمنها ما منحت الحماية الجنائية للمواقع بموجب تعديل القوانين العقابية القائمة وهو ما اعتمده المشرع الجزائري، ومن التشريعات من نظمت ذلك ضمن التشريع الخاص بالتجارة الإلكترونية كالتشريع التونسي، كما من التشريعات العربية من نظمت الحماية الجنائية للمواقع ضمن قانون مستقل يخص الجرائم المعلوماتية وفق ما سلكه المشرع الإماراتي وكذا السعودي من خلال القانون المتعلق: بنظام مكافحة جرائم المعلوماتية الصادر بالمرسوم الملكي رقم: 17 بتاريخ 1428/3/8، والذي جرم فعل الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع أو إتلافه، أو تعديله، أو شغل عنوانه.

الخاتمة

أدى استخدام الانترنت في الأغراض التجارية إلى انتشار معاملات التجارة الإلكترونية على الصعيد العالمي، وبدأ رجال الأعمال وأصحاب المؤسسات والشركات التجارية في الإقبال على المواقع الخاصة بهذا الغرض، وأصبحوا يبرمون الصفقات ويعرضون منتجاتهم وخدماتهم من خلال مواقع لهم على شبكة الانترنت.

كما أن الاستخدام المكثف للانترنت والحاسب الآلي بشكل موسع قاد إلى ظهور جرائم جديدة مست الأنظمة المعلوماتية، والتي تأتي في مقدمتها جرائم الدخول غير المشروع لمواقع التجارة الإلكترونية عبر الانترنت ونظم المعالجة الآلية للبيانات والمعطيات الخاصة بها(27)، وقد أصبحت هذه الجرائم من أخطر الجرائم وذلك لفداحة تأثيرها على النشاط التجاري الإلكتروني الدولي.

وفي خضم الكم الهائل من الاختراقات التي تتعرض لها المواقع التجارية الإلكترونية أصبحت الحاجة ملحة لتوفير حماية جنائية لها، ولما

كان اختراق موقع التجارة الإلكتروني هو اختراق لنظامها المعلوماتي، فالبحث عن الحماية الجنائية للمواقع لا يعدو أن يكون عبر الحماية الجنائية للأنظمة المعلوماتية بشكل عام.

من هذا المنطلق من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في الجرائم المعلوماتية، فالمواجهة التشريعية ضرورية للتعامل من خلال قواعد موضوعية جديدة تكفل مجابهة هذا الشكل الجديد من الإجرام الناشئ عن سوء استخدام النظم المعلوماتية الحديثة، وحسنا فعل المشرع الجزائري كخطوة أولى وإن كانت غير متكاملة لأنها لا تستغرق بالتنظيم كافة جوانب الاعتداءات في هذا المجال، عندما تدخل لتوفير الحماية الجنائية للنظم المعلوماتية في ظل القانون 15/04 المعدل و المتمم للأمر 156/66 المتضمن قانون العقوبات، بإدماج أحكام خاصة بالإجرام المعلوماتي في صلب قانون العقوبات، فاستحدث نصوص خاصة بالجرائم الماسة بالأنظمة المعلوماتية.

في الأخير نرى ضرورة المواجهة الفنية والتقنية لحماية مواقع التجارة الإلكترونية والتي لا غنى عنها كوسيلة تقنية لردع الجناة، ولمزيد من الحماية لهذه المواقع نأمل أن تنظم الجزائر إلى الاتفاقيات الدولية الخاصة بمكافحة الجرائم المعلوماتية، على غرار الاتفاقية الدولية حول الإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي المعروفة باتفاقية بودابست والتي لم تنضم إليها الجزائر لحد الآن.

- الهوامش:

(1) د عامر محمود الكسواني: التجارة عبر الحاسوب، الطبعة الأولى، دار الثقافة للنشر والتوزيع، 2008، ص 176.

(2) د عبد الفتاح بيومي حجازي: التجارة الإلكترونية وحمايتها المدنية، دار الفكر الجامعي، 2006، ص 346.

(3) يمكن تصور الجرائم المعلوماتية من زاويتين بحسب دورها في التجريم (أي فيما إذا كانت جانيا أو مجني عليها) فمن الزاوية الأولى تكون المعلوماتية وسيلة أو أداة للاعتداء: فيستخدمها الجاني لتنفيذ جرائمه كالاعتداء على حرمة الحياة الخاصة، أو

سرقة بطاقات الائتمان، ومن الزاوية الثانية تكون المعلوماتية موضوعا أو محلا للاعتداء، حيث يتم الاعتداء على المال المعلوماتي، ويقصد بالمال المعلوماتي: الحاسوب بكل مكوناته، وهو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واسترجاعها عند الطلب وهو يتكون من كيانين: الكيان المادي للحاسب الإلكتروني ويتمثل في: وحدات الإدخال ووحدات التشغيل ووحدات الإخراج، والكيان المنطقي أو المعنوي الذي يتمثل في البرامج.

(4) تختلف البيانات أو المعطيات عن المعلومات، ذلك أن البيانات مجموعة من الحقائق أو القياسات أو المعطيات التي تتمثل في شكل أرقام أو حروف أو رموز، تتعلق بفكرة أو بموضوع معين، أما المعلومات فهي نتاج معالجة البيانات داخل الحاسب الآلي، من جهة أخرى تختلف المعلومات عن البرامج ذلك أن البرنامج هو مجموعة من التعليمات يتم إدخالها إلى الحاسب لأداء وظيفته، كإدخال البيانات وتخزينها ومعالجتها وإخراجها في صورة معلومات أكثر تفصيلا محمود أحمد عبابنة: جرائم الحاسوب وأبعادها الدولية، دار الثقافة، 2005، ص 92.

(5) وورد تعريف له ضمن نص المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي، على النحو التالي:

Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent , en exécution d'un programme , un traitement Automatisé de données.

(6) لاحظ المشرع الجزائري خطورة أفعال الاعتداء على أجهزة الحاسب وتدخل لتوفير حماية جنائية لها في ظل القانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات، بإدماج أحكام خاصة بالإجرام المعلوماتي في صلب قانون العقوبات، فاستحدث نصوص خاصة بالجرائم الماسة بالأنظمة المعلوماتية، ومن جانب آخر ونظرا لما تتميز به هذه الجرائم من طابع فني خاص الذي يضيف إلحاحا أكبر ومبررا كافيا للمطالبة بنصوص خاصة لمكافحتها، قام المشرع الجزائري مسايرة منه لموجة الإصلاحات التشريعية بإصدار القانون رقم 04/09 في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

(7) يوجد العديد من البرامج المستخدمة لتخطي أنظمة الحماية الفنية(تزود الأنظمة المعلوماتية بحماية فنية للحيلولة دون الدخول غير المشروع لها) في الحالات الطارئة كحالات اختلال وظائف الحاسب أو توقفه عن العمل.

(8) د نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية - دراسة نظرية وتطبيقية- ، الطبعة الأولى منشورات الحلبي الحقوقية، 2005، ص 316.

(9) د محمد سامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات الهيئة المصرية العامة للكتاب، 2003 ص 71.

(10) د عبد الفتاح بيومي حجازي: مكافحة الجرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، 2006، ص 356.

(11) د عبد الفتاح بيومي حجازي: التجارة الإلكترونية وحمايتها المدنية، ص338.

(12) د نائلة عادل محمد فريد قورة: مرجع سابق، ص 345.

(13) يرى البعض أن البقاء يتحقق حتى و لو كان الدخول مصرح به بموافقة المسؤول لفترة زمنية محددة، وتم تجاوز هذا الزمن ليتحول البقاء داخل النظام إلى فعل غير مشروع.

(14) Mohamed Diyaa TOUMLILT: Le commerce électronique au Maroc: Aspect juridique Editions Maghrébines 2008, p216.

(15) د.عبد الفتاح بيومي حجازي: مكافحة الجرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق ص 386.

(16) آمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية دار هومة، 2007، ص 123.

(17) نشير أيضا إلى أن المشرع الجزائري عاقب على الشروع في إحدى الجرائم الماسة بالمعلوماتية، رغبة منه في توسيع نطاق العقوبة، وذلك من خلال نص المادة 394 مكرر7 من قانون العقوبات .

(18) Art.323-4. (Loi nº 2004-575 du 21 juin 2004 art. 46 II Journal Officiel du 22 juin 2004). La participation à un groupement formé ou à une entente établie en vue de la préparation caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

(19) د مدحت رمضان: الحماية النائية لموقع التجارة الإلكترونية على الانترنت ومحتوياته، المجلس الأعلى للثقافة 2003، ص 191.

(20) Eric FILIOL ,Philipe Richard DUROD: Cyber criminalité , 2006,p 187.

(21) Art.323-1. (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002). (Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004). Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende

(22) Alain BENSOUSSAN: Internet , aspects juridiques, Editions HERMES, Paris , 1996.p 108

(23) Alain BENSOUSSAN: L'informatique et le droit ,HERMES , 1994, p 366

(24) Christiane FERAL SCHUHL: Cyberdroit le droit à l'épreuve de l'internet ,DALLOZ , 2006.p 10.

(25) د مدحت رمضان: مرجع سابق، ص 207.

(26) André LUCAS, Jean DEVEZ ,Jean FRAYSSINEY: Droit de l'informatique et de l'internet , THEMIS , 2001, 665.

(27) Bertrand. Warusfel: La contribution du droit à la sécurité des systèmes d'information Securit, 28 Aout 2006, p 22