- دراسات اقتصادية -
ISSN 2602-7925
https://www.asjp.cerist.dz/en/PresentationRevue/417

المجلد: 17 العدد: 01(2023) ص274-287

جرائم التجارة الالكترونية ومعوقاتها

E-commerce crimes and their obstacles

حورية قويقح
جامعة الجزائر 1 (الجزائر)
h.gouigah86@gmail.com

معلومات المقال

تاريخ الارسال:
2022/12/13
تاريخ القبول:
2023/02/02

الكلمات المفتاحية:
- ✓ التجارة الالكترونية،
- ✓ الجرائم المعلوماتية،
- ✓ المعوقات والعراقيل،

الملخص:

الاقتصاد الرقمي عمل بطريقة آلية على تطوير وتنميّة التجارة الالكترونية، وبسّط العمل كثيرا بين الهيئات التجارية المختلفة والمستهلكين عرضًا وبيعًا وشراءً...؛ فالتغيرات الطارئة في السوق التجارية وتحول طرق الدفع التقليدية، والانتقال إلى الدفع الالكتروني، ساعد على ظهور الجرائم ذات الصلة بالتجارة الالكترونية، فبقدر ما عرف هذا التطور من امتيازات وسرعة في المبادلات وقلة في التكلفة، بقدر ما أحدثت هذه الأخيرة انعكاسات مسّت مختلف الخدمات التجارية الالكترونية والتي ظهرت في صور جرائم مستحدثة ذات طابع تقني تجاري متميز عمّا هو متداول في الميدان الإجرامي، هذه المميزات كلها وأخرى ساعدت على تفشي هذه الجرائم في الجزائر، وفي دول العالم والتي اعتبرت كأحد أهم المعوقات المؤثرة إلى حد كبير في هذه التجارة التي حالت دون سيرورتها المتوازنة.

Article info

Received
13/12/2022
Accepted
02/02/2023

Keywords:
- ✓ *e-commerce*
- ✓ *cybercriminality*
- ✓ *constraints and obstacles*

Abstract :

The digital economy has worked in an automated way to develop e-commerce, and has greatly simplified the work between different business organizations and consumers through exposure, sale and purchase...;
The sudden changes in the commercial market and the transformation of traditional means of payment, as well as the transition to electronic payment, have favored the emergence of crimes related to electronic commerce, insofar as we know this development of privileges, speed exchanges and low cost, as much the latter has caused repercussions that have affected various electronic commercial services, which have appeared in images of new crimes of a technical and commercial nature distinct from what circulates in the criminal field, all these characteristics and others contributed to the spread of these crimes in Algeria, and in the countries of the world, which was considered as one of the most important obstacles affecting to a large extent this trade which prevented its balanced process

1. مقدمة:

تعتبر التجارة الالكترونية من أهم الوسائل المساعدة على خلق التنافسية بين مختلف المؤسسات الخاصة والعامة، إذ يتم من خلالها إجراء المبادلات بسرعة فائقة وبسهولة كبيرة، فالشبكات المعلوماتية أخذت قسطا وافرا في مجال المعاملات التجارية، هذه الأخيرة كان لها بالغ الأثر في سرعة العرض والدفع وتبادل السلع على الأرضية الالكترونية وعرض المنتوج بصوة واضحة أمام المستهلك، لكن هذه العوامل الإيجابية كلها لم تمنع من المساس بهذه المعاملات سلبا ممّا أدّى إلى ظهور فجوات إجرامية في المجال التجاري الالكتروني، وظهرت واستفحلت جرائم لا تعد ولا تحصى في هذا المجال الخصب، كما ظهرت عدة عقبات وعوائق تجارية وتقنية واجتماعية..... حالت ولا زالت كذلك دون انتشار وتوسع هذا النوع من التجارة خاصة في الدول النامية، الأمر الذي فرض علينا طرح الإشكالية الآتية:

_ **ما ماهية التجارة الالكترونية، وما هي معوقاتها؟** والتي تفرعت عنها جملة أسئلة نصوغ بعضا منها على النحو الآتي:

_ ما مفهوم جرائم التجارة الالكترونية؟

_ وماهي أنواع هذه الجرائم؟

_وما هي العقبات والعوائق الحائلة دون السيرورة المنتظمة والمنضبطة لهذه التجارة؟

المحور الأول: تعريف جرائم التجارة الالكترونية

نحاول في هذا العنصر تعريف التجارة الالكترونية ابتداءً لننتقل بعد ذلك إلى مفهوم الجرائم التي تختص أو تتصل بمثل هذه التجارة، وذلك على النحو التالي:

أولًا: تعريف التجارة الالكترونية

1_ المشرع الجزائري عرّفها في قانون التجارة الالكترونية الصادر بموجب القانون 18_05 مؤرخ في 24 شعبان 1939هـ الموافق 10 مايو سنة 2018م المتضمن قانون التجارة الالكترونية، حيث جاء في المادة (6) منه يعتمد مفهوم هذا القانون بما يأتي: "التجارة الالكترونية هو النشاط الذي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان أو توفير سلع أو خدمات عن بعد لمستهلك إلكتروني، عن طريق الاتصالات الالكترونية."

2 – وعرفت التجارة الالكترونية فقها أيضا بأنّها: "عبارة عن عمليات بيع وشراء لمختلف السلع والخدمات أو المعلومات وبرامج الكمبيوتر عبر شبكة الانترنت والشبكات التجارية العالمية الأخرى، أي باستخدام تكنولوجيا المعلومات والاتصالات، فهي تجارة بمفهومها التقليدي لكن تتم عبر قنوات الكترونية (صباح عبد الرحيم، وهيبة عبد الرحيم، جرائم التجارة الالكترونية، المجلة الدولية للبحوث القانونية والسياسية، العدد 1، ص 35).

3_ وعرِّفت التجارة الالكترونية بمفهوم مغاير وموسع بأنّها: "جميع المعاملات التي تجري بواسطة الانترنت ويبدوا أنّ هذا النوع من التجارة لا يختلف في مفهومه عن التجارة العادية فيما عدا ارتباطه بوسيلة الانترنت (زيجة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدوليين، عين ميلة، الجزائر، 2011م، ص29).

والتعريف الذي نستقر عليه في الأخير **للتجارة الالكترونية** هو: "أنّها مختلف المعاملات التجارية التي تتخذ الشبكة المعلوماتية وسيلة لها، للقيام بأيِّ عمل من أعمال التجارة." ونستطيع القول بأنّ هذا التعريف جامع مانع للتجارة الالكترونية كونه ربط كل عمل تجاري بأي وسيلة من وسائل الشبكة المعلوماتية.

ثانيًا: تعريف جرائم التجارة الالكترونية

أمّا فيما يخص تعريف **الجرائم الالكترونية** عموما فقد وردت تعريفات متعددة ومتباينة، ومن بين ما ذكر نتطرق لتعريف المشرع الجزائري والذي اصطلح على تسميتها "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال" بموجب المادة 02 من القانون 09_04 الفقرة (أ) بأنّها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحدَّدة في قانون العقوبات، أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية."

وبعد قراءة مجموعة تعريفات متعلقة بالجريمة الالكترونية نقول بأنّها: "كل سلوك غير مشروع صادر عن إرادة جنائية معاقب عليه قانونا، ويكون متصلا بمعطيات الحاسب الآلي (قويقح حورية، الجرائم الاقتصادية عبر الشبكة المعلوماتية، دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، 2020م2021م، ص 46).

أمّا فيما يتعلق بتعريف **جرائم التجارة الالكترونية** هو نفسه التعريف السالف الذكر، فقط يخصَّصُ في نوع السلوك الإجرامي، فننتقل بالتعريف من عموميته إلى خصوصيته فنقول: **"هو كل سلوك تجاري أو أيُّ سلوك يتعلق بأعمال التجارة غير مشروع، يتصل بمعطيات الحاسوب ويتم بواسطة شبكات المعلومات، ويكون صادرًا عن إرادة جنائية ومعاقب عليه قانونا."**

المحور الثاني: أنواع جرائم التجارة الالكترونية

تتنوع وتتعدد الجرائم التي ترتكب في ظل المبنى الالكتروني أثناء المعاملات التجارية وذلك على حسب اختلاف صفة المتعاقد أو المستهلك الالكتروني، فقد يكون بنك أو مؤسسة تجارية أو شركة أو شخص طبيعي، ولهذا سنحاول من خلال هذا العنصر ضبط وطرح أهم هذه الجرائم التجارية استفحالا وانتشارا وفي الوقت ذاته خطورة.

أولًا: جريمة اختراق مواقع التجارة الالكترونية

هذه الجريمة تقوم أساسا على الاختراق أو القرصنة لمواقع يتم من خلالها ممارسة نشاطات تجارية، وهذا الاختراق يأخذ عدة صور فقد يمس البيانات أو الأنظمة أو معطيات الحاسوب. هذا وعرفت جريمة القرصنة بعدة تعريفات نقتصر على التعريف الفني الذي ساقه الفقه بقوله: "هي الاستيلاء على المعلومات من برامج وبيانات مخزنة في دائرة الكمبيوتر بصورة غير شرعية، أو نسخ برامج وبيانات مخزنة في دائرة الكمبيوتر بصورة غير شرعية أو نسخ برامج معلوماتية بصورة غير مشروعة، بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر بواسطة التقاط الموجات الكهرومغناطيسية الصادرة عن الحاسب الآلي أثناء تشغيله وباستخدام هوائيات موصلة بحاسبة أخرى (أمير فرج يوسف، حقوق الملكيَّة الفكريَّة الالكترونيَّة والمساس بها باعتبارها جريمة معلوماتية، الإسكندرية، 2016م، ط1، ص 191).

إذا هو اعتداء على مواقع يرتادها المستهلكون، وذلك من خلال تدميرها أو تخريبها عن طريق إطلاق فيروسات توجه خصيصا لهذه المواقع، وكأنّه تخريب وتدمير للمحل التجاري الذي تعرض فيه السلع والخدمات الموجهة للزبائن (ينظر، صباح عبد الرحيم، وهيبة عبد الرحيم، جرائم التجارة الالكترونية، مرجع سابق، ص 41). وهو اختراق للأنظمة للمساس بالمعلومات أو البيانات أو المعطيات المخزنة داخل الحاسوب من قبل المخترقين أو القراصنة الهواة أو المحترفين، وهؤلاء الأشخاص يدخلون دخول غير قانوني، وهو دخول غير مسموح به وغير مشروع قانونا لأنّه دخول غير مأذون به.

ولقد أصبح من الممكن جدًا لقراصنة الحاسوب "الهاكرز" الوصول إلى أهدافهم المنشودة، والتوصل أيضا إلى المعلومات المالية أو الشخصية، واختراق خصوصيات الأفراد والمعاملات التجارية وساعد على ذلك سرية المعلومات وتداولها بسهولة كبيرة، وذلك لما يشهده الحاسب الآلي من تطور مذهل في نظمه المعلوماتية، وكذلك لما يتميز به مجرمو المعلوماتية من خبرة كبيرة في المجال التقني سواء أكانوا من المحترفين أم من الهواة (فهد بن سيف الحوسيني، جرائم التجارة الالكترونية ووسائل مواجهتها، دار السحاب للنشر والتوزيع، ط1، 2010، ص 57).

وتتم قرصنة المعلوماتية عن طريق الدخول لموقع معين عن طريق اختراقه واستعمال طرق آمنة تعتمد على نظام الأمان الالكتروني والمعلوماتي، ويتم الاختراق بطريقة مباشرة وغير مباشرة، مستغلين في ذلك شفرات الدخول للأنظمة المعلوماتية والحصول على معلومات سرية وثمينة، ولهذا الصدد فرضت العديد من الدول عقوبات ضد من يتصدر لهذا الفعل الإجرامي في حين أنّ بلدان أخرى لم تولي لها اهتماما ظانين أنّها مجرد تسلية لسدِّ الفراغ (Sous la direction de Rodolphe Saric 1999, Rapport Liang Jiansheng, (de stage : Criminalité informatique, P31.).

وتتم عملية الاختراق الالكتروني عن طريق تسريب البيانات الرئيسية والرموز الخاصة لبرامج شبكة الانترنت، وهي عملية تتم من أيّ مكان في العالم دون الحاجة إلى وجود شخص مخترق في الدول التي يتم اختراق مواقعها (عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإليكتروني في عصر العولمة، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الانترنت، المنعقد بالقاهرة في المدة من 2_4 يونيو 2008م، على الموقع WWW.f.law.net/law/ threads/ 28535).

ومن الحالات المسجلة على مستوى الدرك الوطني بالجزائر العاصمة في مجال القرصنة والاختراق لبرامج شبكة المعلومات نذكر ما يلي:

الحالة الأولى: اختراق النّظام المعلوماتي للمؤسسات

في فيفري 2013م شنَّ القرصان (س) هجوما واسعا على مشتركي شبكة الانترنت، مستغلا ثغرة حساسة في ملف نظام مودم "WIFI" المقدم من طرف المتعامل (س، ش، ع)، وانتقد بعض المشتركين الذين تعرضوا للقرصنة هذا الهجوم على منتديات عبر شبكة الانترنت.

وبعد فتح تحقيق في القضية، باشر متخصصون من الدرك الوطني التحقيق وجمع الدلائل على النحو الآتي:

أ_ طريقة عمل القرصان:

من أجل إتمام عملية القرصنة (الاختراق) اتبع القرصان الخطوات التالية:

1_ مسح شبكة الانترنت للمتعامل (س، ش، ع).

2_ تحديد الأهداف على المتصلة (مشتركو ADSL).

3_ تحديد ما إذا كان مودم الضحية مضبوطا بطريقة تسمح بالاختراق (وضع جهاز التوجيه).

4_ تحميل نسخة عن ملف ضبط المودم.

5_ فتح تشفير ملف ضبط المودم للحصول على كلمة المرور لاختراق المودم.

6_ اختراق المودم والاستيلاء على المعلومات الشخصية للمشترك (رقم الخط، اسم الشبكة اللاسلكية، الرمز السري للمودم "WIFI").

7_ تغيير ضبط المودم وذلك بإنشاء شبكة لاسلكية جديدة باسم (مثال: wi-fi 123) غير مشفرة وغير آمنة.

8_ تجميع المعلومات المحصلة في ملف نصي.

9_ مشاركة وتوزيع الملف النصي (المعلومات الشخصية) على الانترنت.

ب_ أعمال التحقيق:

أعمال التحقيق التي باشرها متخصصو الدرك الوطني:

1_ تحديد هوية عدة ضحايا لهذه الهجومات.

2_ استغلال مصادر المعلومات المتاحة على شبكة الانترنت سمح بجمع معلومات هامة من تصرفات القرصان الذي استعمل موقع على يوتيوب أنشئت سنة 2009م من أجل بث تسجيلات مصورة تظهر وتشرح خطوات وتقنيات القرصنة المعلوماتية كما يلي:

_ قرصنة أجهزة مودم وأجهزة التوجيه لمتعاملي الانترنت في الجزائر(حوصلة نشاط مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية ومكافحتها للدرك الوطني الجزائري، لسنة 2017م).

_ قرصنة المواقع الالكترونية للوزارات والمؤسسات العامة.

_ استهداف أرقام الهاتف النقال من خلال الرسائل القصيرة (SMS) عن موقع فايسبوك.

_ استحداث شبكة افتراضية خاصة (VPN).

_ هجمات تستهدف المواقع الالكترونية للجامعات الجزائرية.

_ هجمات تستهدف المواقع الالكترونية الإسرائيلية.

3_ نشر نسخة على شبكة الانترنت خاصة بقاعدة بيانات شركة معروفة وتضم هذه القاعدة أكثر من 120.000 تسجيلًا متعلقًا بطلبيات الزبائن خلال 04 سنوات (رقم التسجيل، اسم ولقب الزبون، العنوان، رقم الهاتف...).

4_ تطوير ونشر برنامج يسمح بالحصول على أرقام هواتف مستخدمي الانترنت في الجزائر من خلال حسابات الفايسبوك.

5_ اختراق الموقع الالكتروني للوزارة M1 ونشر قاعدة بياناته التي تضم أسماء المستخدمين وكلمات المرور والعنوان الالكتروني لمستخدمي الموقع المذكور.

إضافة إلى أنَّ نفس القرصان يسيِّر صفحة على موقع التواصل الاجتماعي فايسبوك باسم (S?S) وفيها يقدم نفسه على أنَّه خبير أمني في الأنظمة المعلوماتية (حوصلة نشاط مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية ومكافحتها للدرك الوطني الجزائري، لسنة 2017م).

وكل أعمال الاختراق والقرصنة سالفة الذكر تدخل ضمنا في مدلول أو مضمون المادة 394 مكرر: "يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 50000 دج إلى 500000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة. تكون العقوبة الحبس من ستة 6 أشهر إلى سنتين والغرامة من 50000 دج الى 300000 دج."

وبما أنّ جريمة الاختراق هي دخول للنظام أو بقاء في النظام لكن عن طريق الغش، ويكون الهدف من هذين الفعلين هو التدمير فهو يدخل في إطار الجرائم الموجهة للتجارة الالكترونية عموما، وبالتحديد لجرائم القرصنة المعلوماتية.

وفي قانون العقوبات الجزائري جاء في نص المادة 394 مكرر ومكرر 1 ذكر جرائم الاعتداء على بيانات المواقع، وتمثلت في التلاعب بالمعطيات والتعامل بمعطيات غير مشروعة، حيث جاء في نص المادة:" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500000 دج إلى 4000000 دج، كل من أدخل بطريق الغش معطيات نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

هذا وقد قد أشارت إلى ذلك الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ضمن ما اعتبرته الدخول غير المشروع حيث نصت المادة (6) منها على أنّه: " 1_ الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات، أو الاستمرار به. 2_ تشدد

العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال: أ_ محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة للأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفدين.

ب_ الحصول على معلومات حكومية سرية، فعبارة "نسخ" أو "نقل" الواردة في النص أعلاه يقصد به السرقة (المؤلف مجلة المحقق الحلي للعلوم القانونية والسياسية، معوقات التجارة الالكترونية ومتطلبات النظام القانوني لمواجهتها (دراسة مقارنة)، العدد الثاني، السنة التاسعة، 2017م، ص83).

ثانيًا: جريمة الاتجار بمعلومات تجارية غير مشروعة

ويقصد بها: "الاتجار عمدا بمعلومات غير مشروعة ومخزنة في أنظمة الكترونية، قصد الربح غير المشروع منها وذلك باستخدامها لارتكاب جرائم ورائها (صباح عبد الرحيم، وهيبة عبد الرحيم، جرائم التجارة الالكترونية، مرجع سابق، ص 40).

وهو ما نصت عليه المادة 394 مكرر 2 حيث جاء فيها: "يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات، وبغرامة من 1000000 دج إلى 10000000 دج، كل من يقوم عمدا أو عن طريق الغش بما يأتي:

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

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

ثالثًا: جريمة السطو على بيانات البطاقة الائتمانيَّة والبنكيَّة

أول ما ينبغي أن نشير إليه هو أنّ السطو هنا يتعلق ببيانات البطاقة الائتمانية أو البنكيَّة، لأنّه لو تعلق بالبطاقة ذاتها لانتقل بها من الجريمة المستحدثة إلى العادية أو التقليدية ؛ لأنّ السطو يكون منصب على محل مادي ملموس وعليه تقرّر لها العقوبة المنصوص عليها في النصوص التقليدية، بينما يتغير الحال حينما يتعلق الأمر بالسطو على البيانات أو البرامج أو المعلومات، فهنا تأخذ الجريمة مجرى الجرائم المستحدثة، والتي لم يقرر لها تشريعيا نصوصا صريحة، وهو ما سنتناوله في هذا العنصر، والذي يتطلب منا ابتداء التعرف على مدلول البطاقة البنكيَّة والتي يعنى بها: "هي كل بطاقة تسمح لحاملها بسحب أو بنقل الأموال، ولا يمكن أن تصدر إلّا من طرف هيئة قرض أو مؤسسة ماليَّة أو مصلحة مرخص لها بوضع أو اصدار البطاقات كالمصارف، الخزينة العامة مصالح البريد، وفيها عدة أنواع تسمح بالدفع عن طرق شبكة الانترنت مثل: البطاقات الائتمانية، بطاقات الدفع، بطاقات خاصة تصدرها المحلات التجارية (صباح عبد الرحيم، مرجع سابق، ص 38).

وارتبط استخدامها من خلال شبكة الانترنت فظهر العديد من المتسللين هدفهم الإجرامي السطو عليها بلا هوادة، فالبطاقات الائتمانية تعد نقودا الكترونية والاستيلاء عليها يعد استيلاءً على مال الغير.

وخاصة أنّ الاستيلاء على بطاقات الائتمان أمرا ليس صعبا فلصوص بطاقات الائتمان مثلا: يستطعون سرقة مئات الآلاف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت، ومن ثم بيع هذه المعلومات للآخرين. مديرية تكنولوجيا المعلومات الجمهورية العامة للاتصالات والمعلومات، ص9.

ويعتبر الاستيلاء على البطاقة البنكية عموما وعلى البطاقة الائتمانية نوعا من الهجوم على ممتلكات فكرية مملوكة للغير وهذا السطو يأخذ أو يأتي في عدة صور كالاستيلاء على رقم التشفير للبطاقة، أو من خلال الحصول على الرابط الذي يحوي كل المعلومات المتعلقة بحساب الشخص، ويتم ذلك في حالة استعمالهم نفس اسم المستخدم (Djamal Djenane, Criminalité informatique, le phénomène prend de l’ampleur Publié dans Info Soir le 18 Mai 2008. Colloque international « la sécurité des systèmes d’information au service de la sécurité publique » P7).

وعن أمثلة عن جرائم السطو على البطاقات الائتمانية نذكر أيضا على سبيل ضرب المثال: سحب الحامل الشرعي لمبالغ مالية تزيد عن الرصيد، وسحب الحامل الشرعي لأموال بعد إلغاء البطاقة أو بعد انتهاء مفعولها، استعمال البطاقة من قبل حاملها الشرعي بعد إقدامه على إبلاغ الجهة مصدرتها عن فقدانها أو سرقتها، استعمال الغير ممن استولى على البطاقة بعد سرقتها أو فقدانها (أمير فرج يوسف، عنوان الكتاب والمعلومات، مرجع سابق، ص 54 وما بعدها). وأصبح قراصنة الانترنت يقومون بخلق أرقام للبطاقات الالكترونية ويتم ذلك من خلال برامج تشغيل، أو قد يتم التقاط هذه الأرقام عن طريق الانترنت نفسه، ولكن بطريقة غير مشروعة وذلك عن طريق التسوق عبر الانترنت، وتتم هذه الاساءة عن طريق حامل البطاقة نفسه، وذلك من خلال الحصول على بطاقة ائتمان صحيحة بناءً على مستندات مزورة. أو يتم عن طريق الغش، وذلك باستخدامها رغم انتهاء مدة صلاحيتها، أو استعمالها رغم الغاء البنك لها. أو قد يتجاوز حد السحب من خلال التواطؤ مع الموظف أو التاجر أو قد يقوم الغير بإساءة استخدام بطاقة الائتمان، وذلك في حالة ضياع الرقم السري لبطاقة الائتمان (أمير فرج يوسف، مرجع سابق، ص 263، 264).

وتوسع في الآونة الأخيرة مجال استخدام بطاقات الدفع الالكترونية، وأخذت متسعا إذ أصبحت تستخدم في المتاجر والفنادق وفي الأعمال المصرفية، وسبب ذلك هو تسهيلها لسرعة إجراء المبادلات، وتجنب مخاطر حمل النقود، واستخدامها في التجارة الالكترونية من خلال شبكة الانترنت لعقد الصفقات التجارية بين المتعاملين في داخل الدولة الواحدة أو بين دول العالم المختلفة، وقد تمخض عن ذلك كله أخذها الكثير من الصور الإجرامية وذلك نتيجة التلاعب والتحايل أثناء استخدامها، كالنصب وخيانة الأمانة والسرقة (أحمد شوقي عمر أبو خطوة، الجرائم الواقعة على الأموال في قانون العقوبات، الاتحادي لدولة الامارات العربية المتحدة، دراسة مقارنة، مطابع البيان التجارية، دبي، ط1، 1990م، ص 92). وزادت الخطورة أكثر اتجاه هذه البطاقة لما أصبح هناك سوق لشراء بطاقات وفاء ممغنطة مسروقة أو الضائعة واستخدامها من قبل التّجار والاستيلاء على ما فيها من أموال.

كما قد تتم الإساءة من قبل التاجر الذي قد يسيء استخدام بطاقات الدفع عندما يتمم عمليات البيع باستخدام البطاقة. فالتاجر يمثل حلقة وصل بين الماكينة واشعارات البيع المسلمة له من البنك المتعاقد معه، وهو من يتولى أيضًا التأكد من صلاحية هذه البطاقة والتحقق من شخصية حاملها، ومراجعة التوقيع الموجود على ظهر البطاقة.

ولذلك فإنّ أساليب التلاعب في بطاقات الدفع الالكتروني _كما سبق توضيحه_ يقع من أطراف متعددة، بعضها من أطراف البطاقة ذاتها (العميل، البنك، التاجر)، والبعض الآخر من الغير، وتتم من خلا ل مراحل فقد تأتي في مرحلة السحب أو الوفاء، وسواء تم الدفع مباشرة للتاجر، أم من خلال شبكة الانترنت (السيد عبد الحميد أحمد، مرجع سابق، ص 59، 60).

رابعًا: جريمة إتلاف وتدمير المواقع الالكترونية التجارية

الإتلاف نوعان أحدهما كلي؛ وهو الإتلاف الذي يمس أو تتعرض له البيانات والمعلومات أو الصفحات الشخصية للأفراد عبر صفحات الانترنت، وذلك من خلال محو هذه المعلومات وتدميرها الكترونيا ويتم ذلك بعدة طرق بحيث لا يمكن الاستفادة منها مرة أخرى. أو أن يكون الاتلاف جزئي حيث تشوه المعلومة بشكل جزئي كوضع بعض الرموز وتشفير بعض الكلمات فتصبح غير واضحة وغير مفهومة عند قراءتها (أمير فرج يوسف، مرجع سابق، ص 270).

وقد أشارت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات إلى جريمة الإتلاف وأطلقت عليها تسمية الاعتداء على سلامة البيانات وذلك في المادة (8) منها والتي تنص على أنّه:" تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق. 2_ للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (3) من هذه المادة، أن تتسبب في ضرر جسيم (مجلة المحقق للعلوم القانونية والسياسية، معوقات التجارة الالكترونية ومتطلبات النظام القانوني لمواجهتها (دراسة مقارنة)، مرجع سابق، ص 684).

وعن مدى اعتبار البرنامج كمحل لجريمة الاتلاف نجد ذلك وارد في المادة 407 من قانون العقوبات الجزائري: "كل من خرَّب أو أتلف عمدا أموال الغير المنصوص عليها في المادة 396 بأيَّة وسيلة أخرى كليًا أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 20000 إلى 100000دج."

كما تنص المادة 412 من قانون العقوبات الجزائري:"كل من أتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعة وذلك بواسطة مواد من شأنها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبغرامة من 20000 دج إلى 100000دج."

ومن خلال هذه المادة 412 نجدها قد حصرت الأشياء القابلة للإتلاف وتتمثل في المكونات المادية للحاسوب سواء كانت أجهزة أم بضائع، كما أنّ الكيان المنطقي يمكن أن يخضع لهذا النص التجريمي باعتباره مالًا أيضا واستنادا لما له من قيمة اقتصادية معتبرة (السيد عبد الحميد أحمد، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولية، مكتبة الوفاء، الإسكندرية، ط1، 2018م، ص335).

هذا وبالنسبة لمدى امكانية تطبيق النشاط الإجرامي لجريمة الاتلاف في المجال المعلوماتي: فهذا أمر وارد ذلك أنَّ المشرع الجزائر لم يقيد النشاط الاجرامي في جريمة الاتلاف بوسيلة معينة إذ هي من الجرائم ذات القالب الحر، ولهذا لا يوجد مانع من دخول جريمة الاتلاف الالكتروني المتعلقة ببرامج الحاسب الآلي من دخولها في جريمة الاتلاف عموما، خاصة وأنّ المشرع الجزائري لم يحدد طريقة بعينها لوقوع الجريمة ولم يحدد نتيجة واحدة محددة لقيامها، ولم يقم بتحديد النشاط الاجرامي ولذا فإنّه يدخل ضمنا النشاط الإجرامي المتعلق بالبرنامج والدَّعامة المسجل عليهما معا، أو إلى البرنامج فقط دون الدعامة، وقد تقع الجريمة عن طريق الاتصال المباشر بالجهاز كما قد تقع من خلال الاتصال عن بعد.

وعليه فإنّ جريمة الاتلاف المنصوص عليها في قانون العقوبات توفر حماية جنائية كافية لبرامج الحاسب خلاف باقي جرائم الأموال كالسرقة والنصب والخيانة والتي توفر حماية نسبية فقط (السيد عبد الحميد، مرجع سابق، ص340، 341).

ويتم الإتلاف الالكتروني باستعمال طرق متعددة وتستعمل البرامج الخبيثة لذلك وهي: كل وسيلة الكترونية معنوية تعمل على تخريب النظام المعلوماتي إما تخريبا كليا أو جزئيا ومن أهمها الفيروسات، والقنابل المعلوماتية، والديدان..... وغيرها، نذكر أهمها فيما يلي:

أ_ استخدام برنامج القنبلة المنطقية:

تعرف القنبلة المنطقية بأنَّها: "عبارة عن برنامج أو جزء من برنامج ينفذ لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكات المعلومات بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع، ومن ذلك مثلا إدخال تعليمات في برنامج نظام التشغيل..... وتسعى القنبلة المنطقية إلى البحث عن حرف معين وليكن حرف الألف في أي سجل يتضمن الأمر بالدفع، وعندما تكتشفه تتحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل (محمد أمين الرومي، المستند الالكتروني، درا الكتب القانونية، مصر، 2008، ص94).

ومن الأمثلة الواقعية التي استخدمت فيها القنبلة المنطقية نسوق ما يلي: "تمكن خبير في نظم المعلومات في الدنمارك من وضع قنبلة منطقية في نظام إحدى الحاسبات أدت إلى محو أكثر من مائة برنامج. وقد تم أيضا محو النسخ الاحتياطية عند تشغيلها نظرًا لانتقال أثار القنبلة إليها، ويتم ضبط المجرم وحكم عليه القضاء الدانماركي بالحبس لمدة سبعة أشهر (هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلاء الحديثة، أسيوط، 1992م، ص 160).

ب_ استخدام برنامج القنبلة الزمنية:

وهي عكس القنبلة المنطقية فيحدد زمن وتاريخ تفجيرها في السنة، فيمكن إدخالها في برنامج تحديد توقيت انفجارها بيوم محددا مثلا 2006/03/18م على الساعة 3:10 بتوقيت غرينتش مع تحويل النقود من حساب شخص لآخر أو عن طريق محو وشطب كل البيانات التي يحتويها مستند الكتروني داخل أحد أجهزة الحاسب الآلي ومن الأمثلة الواقعية التي استخدم فيها أسلوب القنبلة الزمنية نذكر مما يلي:

قام أحد الخبراء في فرنسا مختص في نظم المعلومات بوضع قنبلة زمنية في شبكة الخاصة بالمنشأة بحيث تنفجر بعد مرور ستة أشهر من رحيله من المنشأة وذلك بدافع الانتقام على إثر فصله من المنشأة التي يعمل بها، وترتب على ذلك إتلاف كل البيانات المتعلقة بهذه المنشأة (محمد أمين الرومي، مرجع سابق، ص95).

ج_ استخدام الفيروسات:

الفيروسات من أخطر وأكثر الوسائل التخريبية المعمول بها في أنظمة المعلومات، فهي تعمل على زعزعة أمن المعلومات، وتعد أهم الطرق المستعملة للسيطرة على الجهاز وإتلاف كل ما يحتويه من معلومات معنوية ويمكن تحديد معناها بأنّها: "عبارة عن برنامج صغير له قدرة على العمل في الخفاء، ويتكاثر بحيث يتم وضعه في الكمبيوتر فيصيبه، وينتقل إذا توافرت وسائل انتقاله ليصيب الأجهزة الأخرى وفقا للأغراض المصمَّم من أجلها الفيروسات، فليس شرطا أن تكون لبرنامج الفيروسات أهدافا تخريبية (خديجة حامي، الأنظمة المعلوماتية في مواجهة القرصنة والتخريب، (المخاطر المحدقة والحلول الناجعة)، ص 41، جامعة مولود معمري، تيزي وزو، قسم اللُّغة العربية وآدابها، مخبر الممارسات اللغوية في الجزائر، الملتقى الوطني حول الأمن المعلوماتي مهدداته وسبل الحماية 03_ 04، نوفمبر 2015م، ص 41).

د_ استخدام برامج الدودة المعلوماتية:

وتعد الدودة المعلوماتية من بين الطرق المستعملة في العملية التخريبية وهي عبارة عن: "برمجة تقوم بالانتقال من حاسب آلي لآخر دون حاجة إلى تدخل انساني لتنشيطها، فتغطي شبكة بأكملها، ولديها إمكانية تعطيل نظام الحاسب الآلي بصورة كاملة عن طريق استغلال أي خلل أو فجوة في نظام التشغيل الحاسب (دلخار صلاح بوتاني، الحماية الجنائية الموضوعية للمعلوماتية دراسة مقارنة، دار الفكر الجامعي، الاسكندرية، 2016، ص 238).

وتهدف برامج الدودة إلى أخذ أكبر مساحة ممكنة من سعة النظام وذلك بهدف التقليل من قدراته، وقد يتجاوز ذلك في بعض الأحيان فتقوم بأعمال التخريب حقيقية للملفات والبرامج وأنظمة تشغيل الحاسب وبروتكولات الاتصال (دلخار صلاح البوتاني، مرجع سابق، ص 238).

المحور الثالث: عراقيل انتشار التجارة الالكترونية في الجزائر

تواجه الدول العربية كاملة ودول العالم الكثير من العقبات والعراقيل الحائلة دون سيرورة التجارة الالكترونية بصورة تلقائية وبوتيرة سريعة، نذكر منها ما يلي:

أولًا: العقبات التقنية والتكنولوجيا

والتي تعد أهم عقبة حائلة دون السيرورة المنتظمة والمتطورة لمثل هذه الجرائم وهذا ما سيتوضح أكثر فيما يلي:

أ_ ضعف البنى التحتية الالكترونية:

البنية التحتية للشبكة الالكترونية ولنظام الاتصال الالكتروني في الدول العربية عموما، وفي الجزائر على وجه التحديد لا تزال تواجه الكثير من التباطؤ والتأخر فالدول العربية تواجه الكثير من العقبات التكنولوجية مثل: نوعيَّة وسرعة تقديم خدمات وسائل الاتصال ونقل المعلومات والربط الالكتروني، وقلة توفر قطع تقنية المعلومات مثل الحاسبات والأقراص الصلبة والمرنة وأجهزة الهواتف الرقمية وغيرها من العقبات التي باتت تعرقل سير تدفق الانترنت، والتي تعتبر من الوسائل الأساس للدخول في الانترنت والقيام بأيِّ عمل تجاري عبر الوسائل

التقنية (عابد العبدلي، التجارة الالكترونية في الدول الإسلامية الواقع _ التحديات_ الآمال، المؤتمر العالمي الثالث للاقتصاد الإسلامي، جامعة أم القرى، مكة المكرمة، 1426هـ، 2005م، ص36).

وهذا الأمر حاصل هو الآخر بكثرة في الجزائر فبالرغم من وجود الإطار القانوني للتجارة الالكترونية في الجزائر ومصادقة البرلمان له، إلّا أنّ هذا لا يعني بتاتا نجاح هذه العملية أو اعتبارها إضافة للاقتصاد الجزائري، إذ لا نجاح لهذه التجارة في الجزائر على أرض الواقع، وذلك راجع لأسباب متعددة أهمها: يتعلق بتدفق الانترنت الضئيل جدًا وانعدامها في مناطق أخرى كمدن الجنوب، وعدم تكافؤ الفرص بالنسبة للمواطنين والذي شكل أحد العوائق أمام التجارة الالكترونية (أمال مشتي، مرجع سابق، ص 21).

كما تواجه الجزائر ضعفا في البنية التحتية للاتصالات وعدم مواكبتها للتطورات التقنية العالمية وما يرتبط بها من برامج وتجهيزات وأنظمة سوف يحد من أمن الشبكة المالية ويعيق سرعة تنقل البيانات في الشبكة التجارية، وهذا هو الأمر الحائل دون تطور وانتشار التجارة الالكترونية، فرغم المجهودات التي تبذلها الجزائر لتعزيز البنية التحتية لاتصالاتها إلّا أنّها مازالت متأخرة في هذا المجال فأصبحنا اليوم نسمع خدمات الجيل الرابع والخامس في دول العالم ، في حين أنّ الجزائر لا تزال تجد صعوبة وتعسر حتى في إدخال خدمات الجيل الثالث (صراع كريمة، مرجع سابق، ص173).

ب_ ضعف الثقافة التقنية والوعي الالكتروني بين أفراد المجتمع:

الثقافة بالتجارة الالكترونية لها بالغ الأثر لانتشارها وتطورها خاصة بين المؤسسات التجارية والقطاعات الإنتاجية. ومن الطرق المساعدة على ذلك هو مستوى ونوعية التعليم إذ يعتبر وسيلة مهمة في نشر ثقافة الاستخدام الالكتروني. وفي هذا الصدد تشير نتائج بعض الدراسات إلى أنّ انتشار الحاسبات الآلية في المؤسسات التربوية، وبتوفير فرص الدخول في الانترنت في المؤسسات التعليمية بمختلف مراحلها في الدول الإسلامية لها أهميتها في نشر التجارة الالكترونية، في حين نجد خلاف ذلك على أرض الواقع (IBID ; ALSO ; TRE .(WORLD BANK ; 2003 ;OP

كما أنّه ثمة ضعف كبير في مجال الثقافة التقنية والوعي التكنولوجي لدى الفرد الجزائري ولازال متأخرا في مجال التجارة الالكترونية، وسببه عائد إلى عدم اهتمام الدولة والمؤسسات التجارية لنشر ثقافة التجارة عبر الانترنت كتجارة من نوع جديد تتيح للمستهلك العديد من المزايا والفرص، كما أنّ عدم تخصيص الاستثمارات الموجهة للاشهارات والإعلانات لدعم هذه التجارة عمل هو الآخر على الحد دون انتشار وتوسع هذه التجارة ، فعقلية الجزائريين دائما مختلفة في كل المواضيع الجديدة ويلزمها الوقت من أجل التكليف والانصهار في مجتمع المعلومات كباقي الدول (صراع كريمة، مرجع سابق، ص74).

ثانيًا: العقبات القانونية

من المواضيع التي أثارت الجدل في الساحة القانونية تتعلق بالقانون الواجب التطبيق على جرائم التجارة الالكترونية، وظهرت لأجل ذلك ثلاثة نظريات الأولى ترى أن مثل هذه الجرائم محميَّة في قانون العقوبات يعني من خلال النصوص التقليدية أو الكلاسيكية، وظهرت نظرية ثانية تقول أنَّها محميَّة من خلال نصوص الملكيَّة الفكريَّة، في حين ظهر فريق آخر ودافع عن رأيه بشدة وفنَّد حجج الفريقين واستقر على أنَّه يجب حمايتها بنصوص مستحدثة تُسنّ خصيصا لمثل هذه الجرائم باعتبارها جرائم لم تكن معروفة من قبل، وطال البحث عن إمكانية تطبيق النصوص التقليدية على الجرائم الالكترونيَّة، كما وقع الإشكال أيضا حول القواعد الإجرائية التقليدية الواجبة التطبيق خاصة أنَّها تعرقل من عمل أجهزة العدالة وتصعب كشف جرائم عبر الحدود وهو الذي يقتضي من الناحية العلميَّة أن يتم في نطاق إقليم دولة أخرى (صالح شنين، الحماية الجنائية للتجارة الالكترونية (دراسة مقارنة)، رسالة لنيل شهادة الدكتوراه، في القانون الخاص، جامعة أبو بكر، بلقايد تلمسان، كلية الحقوق، 2012م/ 2013م، ص 87).

ومما هو مقرر جنائيا حضر القياس والتفسير الواسع وهذا هو الأمر الحائل دون تطبيق النصوص التقليدية المتعلقة بجرائم الأموال السرقة والنصب والخيانة على نفس الجرائم في صورهم التقليدية لأنَّ هذه النصوص إنَّما شرعت لحماية المحل المادي المنقول المملوك للغير، وله من الخصائص ما يجعله مختلف عن معطيات الحاسوب والتي هي عبارة عن معلومات أو برامج أو بيانات وكلها عبارة عن محل معنوي فيصبح من الصعب بمكان توفير حماية جنائية وقانونية شاملة لهذا المال المعلوماتي.

ولهذا لازالت مواضيع التجارة الالكترونية تثير العديد من المشاكل الفنية والقانونية، منها حماية الموقع على الشبكة العالمية، ومدى صحة المعلومات المسجلة عليه، وحقوق الملكيَّة الفكريَّة لما يحتويه الموقع من معلومات أو مصنفات فنية أو أدبية أو علامات تجارية. إلى جانب حماية المستهلك (بيانات الشخصية، تعاملاته البنكية، رقم بطاقة الائتمان الخاصة به) حماية متنوعة من الغش فيما يقدم له سلع وخدمات، أو حمايته من النصب والسرقة أو خيانة الأمانة، كما يقع الاشكال أيضا حول القانون الواجب التطبيق على العقود المتعلقة بالتجارة الالكترونية.

وللحد أو التقليل من هذه المشاكل الفنية والقانونية وجب توفير تقنيات لازمة لتوفير هذه الحماية فنيا، وضرورة التدخل التشريعي لحماية المستهلك، ومواجهة الجرائم المختلفة الناشئة عن هذه الصورة المستحدثة من المعاملات التجارية، فضلا عن التأمين ضد مخاطر التجارة الالكترونية (السيد عبد الحميد أحمد، مرجع سابق، ص 42، 43).

ومع هذا كله فإنَّنا في كل مرة نؤكد على ضرورة التدخل التشريعي لاستحداث نصوص قانونية تتماشى والطبيعة المعنوية للمال المعلوماتي وتكون هذه النصوص شاملة ودقيقة وذلك مثلما فعلت أغلبية دول العالم مثل فرنسا والسويد.

كما أنّه يوجد أيضا العديد من المشكلات في المجال الإجرائي سواء فيما يتعلق بالدليل الالكتروني، فهو يعتمد على الخبرة للتعامل مع الدليل الفني المتوفر في مجال تكنولوجيا المعلومات والانترنت فالخبرة لها دور لا يستهان به خاصة مع نقص معرفة رجال القانون بالجوانب التقنية فيما يتعلق بالجرائم الالكترونية.

كما ثمة نقص فادح فيما يتعلق بالمعرفة التقنية عند رجال القانون، وذلك راجع للخاصيَّة التي يتمتع بها الدليل الالكتروني في كل مراحله سواء على مستوى التحقيق أم المحاكمة وعند اثباتها أيضا (أشرف عبد القادر قنديل، الوسائل الالكترونية ودورها في الاثبات الجنائي، دار الجامعة الجديدة، الاسكندرية، 2018م، ص149).

ثالثًا: العقبات الحكومية

مما ينبغي التركيز عليه هو الاستعداد والعمل المستمر للحكومات لدعم وخدمة المشروعات التجارية، وتخطي مختلف العقبات المادية والمعنوية حتى تتمكن من تطوير هذه المشروعات، إذ أنَّ الحكومات فشلت في وضع استراتيجيات مناسبة لتدعيم المشروعات التجارية الوطنية للمنافسة مع نظيراتها العالمية، ولعل من أهم الأسباب المانعة أو المعرقلة من انتشارها هو استفحال الأنظمة البيروقراطية في إجراءات التصدير والاستيراد وطول فترات إتمام وتخليص العمليات الجمركية بجانب القيود المفروضة على الصادرات والواردات مثل: التراخيص ونظام الحصص والتي تمثل تحديات أمام أنشطة التجارة الالكترونية التي تتصف بالكفاءة والسرعة (عابد العبدلي، مرجع سابق، ص 38).

رابعًا: العقبات التجارية

ما فتأت الجزائر من المحاولات المتلاحقة نحو تطوير وتكريس تجارة وطنية ودولية رابحة، حتى ظهر نمط مغاير للتجارة التقليدية وهي التجارة الالكترونيَّة، وهذه الأخرى تحتاج الكثير من المساهمات والجهود حتى تتمكن من الوصول ولو جزئيا لمسايرة التجارة الالكترونيَّة الدولية وخاصة أنّها تتطلب الكثير من الجهد والوقت؛ فالتحول من بيئة التجارة التقليدية إلى بيئة التجارة الالكترونيَّة يتطلب تبادل الأعمال والأنشطة التجارية بوسائل رقمية شبكية يمثل منطلقا جديدا وصعبا أمام المؤسسات والمشروعات التجارية في الجزائر، حيث تفتقر غالبيتها إلى مقومات وأسس المؤسسات الإلكترونية وأغلبها لا يمتلك مؤهلات التجارة الالكترونية، وذلك يرجع لعدم استيعابها بشكل كاف

للأعمال الالكترونية، والذي يتطلب أولا قناعة المستهلك أو المورد بأهمية وفائدة التجارة عبر الانترنت، وبعد ذلك يتم اتخاذ جملة خطط واستراتيجيات للتحول إلى التجارة الرقمية، كما يلمس نقص الخبرة في هذا المجال من قبل المؤسسات الجزائرية وصعوبة فهم معنى التجارة الالكترونية من قبل العديد من المؤسسات الجزائرية (صراع كريمة، مرجع سابق، 175).

خامسًا: العقبات الإجرائية

فالبحث والتحقيق والمتابعة والتفتيش في المجال الاجرائي يمثل صعوبة كبيرة إذا ما اتصل بالوسائط الالكترونية، كما سبق وأن أشرنا إلى الاشكاليات التي لا تزال تعاني منها التجارة الالكترونية فنجد في نفس الوقت إشكاليات أخرى إجرائية، إذ أنّ التحقيق والبحث والتحري والاثبات في جرائم الانترنت سيما جرائم التجارة الالكترونية وملاحقة مرتكبيهم أمر صعب للغاية وتشكل صعوبة وتعقيد بالغين مما أدى إلى ظهور تحدي كبير لأجهزة الضبط القضائي على المستوى الدولي أو على المستوى الوطني نتج عنه بعض الصعوبات التي تعيق عمل هذه الأجهزة (شنين صالح، مرجع سابق، ص 319).

فهناك صعوبات كثيرة كانت ولا تزال تعيق الأجهزة الأمنية عن التصدي لهذه الجرائم، وخاصة فيما يتعلق بالتحقيق في هذا النوع المستحدث من الجرائم، سواء في كشف غموضها أم إجراء التفتيش والضبط اللازمين، أم التحقيق فيها إذ الأمر تطلب إحداث برامج تدريب وتأهيل لهذه الكوادر من الناحية الفنيَّة وبالتالي تكون على دراية تمكنها من تحقيق المهمة المطلوبة منها وبالكفاءة المطلوبة. ففي أول ما ظهرت هذه الجرائم وقعت الشرطة في أخطاء جسيمة أدت إلى الاضرار بالأجهزة أو الملفات، والأدلة الخاصة بإثبات الجريمة وذلك لنقص أو انعدام خبرتها في المجال (السيد عبد الحميد أحمد، مرجع سابق، ص 72).

وخلاصة القول فإنَّه سبق وأن أكدنا على عدم كفاية النصوص القانونية التقليدية لمواجهة هذه الجرائم المستحدثة وعلَّلنا لذلك بعدة أسباب، فالأمر سيسير على النحو ذاته في المجال الإجرائي لأنَّهما عاملين متكاملين ومتداخلين، خاصة وأنَّ هذه المعلومات والبرامج ذات طبيعة معنوية، فنصوص قانون الإجراءات الجنائية غير قادرة على استيفاء الإجراءات اللازمة وفقا لطرق الاثبات التقليدية.

وهذا الأمر سيخلق فجوات قانونية وإجرائية في منتهى الخطورة وسيؤدي إلى إفلات الجناة فيما يتعلق بالجرائم الالكترونية، كما أنّ الأمر سيضطر القضاء إلى التوسع في تفسير النصوص العقابية التقليدية وبالتالي الإخلال بمبدأ شرعية الجرائم والعقوبات، وقد ترتكب هذه الجرائم المستحدثة ويصعب إثباتها لعدم ملائمة طرق الاثبات التقليدية لإثباتها، وقد يتم اثباتها بطرق تقليدية فيتم انتهاك الحريات الشخصية للأفراد (أشرف عبد القادر قنديل، مرجع سابق، ص63).

خاتمة:

التجارة الالكترونية ضرورة اقتصادية تتطلبها استمرارية نجاح العملية التنموية، فالعلاقة التعاقدية عبر الشبكة المعلوماتية بين المورد والمستهلك مهما اختلفت طبيعتها، لا يمكن لها النجاح بحال من الأحوال إلَّا بتعاون جهات عديدة تشريعية وتنظيمية واجرائية نقتصر على أهمها فيما يلي والتي ننظمها وفق نتائج وتوصيات وذلك من خلال ما يأتي ذكره:

_لا بد من تطوير وتثقيف المجتمع بمثل هذه المعاملات حتى تصبح أكثر ائتلافا وفي الوقت ذاته أكثر قبولا وبالتالي ممارسة.

_ الأجدر بالمتخصصين في المجال أن تكون لديهم حلقة وصل في تطوير وتوفير وتثقيف الأشخاص بطرق الحماية التقنية والقانونية، وهذه الحماية لا تتأتى إلا بتظافر جهود متعددة من ذوي الاختصاص في المجالين التقني والفني، حتى يتسنى لهم توفير ركيزة حادة من الحماية تكون متوافقة من حيث التطور والسرعة والنوعيَّة والكيفيَّة مع مثل هذه الجرائم المستحدثة.

_ ضرورة إعادة رسكلة معظم القوانين في أطر واضحة تتماشى وسيرورة الجرائم المعلوماتية عموما وجرائم التجارة الالكترونية على وجه التحديد والتدقيق، مع تحيين القوانين ووضع نصوص قانونية شاملة ومستوعبة لكل ما يتعلق بالتجارة الالكترونية.

_ لا بد من اتخاذ سبل فعالة تكون حازمة وجديَّة ونافعة حتى تسترجع وتثبَّت الثقة بين المستهلك والتُّجار في السوق الالكتروني، ويصبح المستهلك يتصرف بطمأنينة كبيرة إذ لا بد من فرض حماية الكترونية تقنية على مثل هذه التجارة وذلك من خلال توفير نظام الأمان.

_ لا بد من توفير حماية جنائية وطنية ودولية للمال الالكتروني الذي يتخذه المستهلك كوسيلة للتعامل في المجال التجاري الالكتروني، وذلك راجع للطابع الدولي التي تتميز به مثل هذه العمليات التجارية.

قائمة المصادر والمراجع:

المؤلفات:

- أحمد شوقي عمر أبو خطوة، 1990م الجرائم الواقعة على الأموال في قانون العقوبات، دراسة مقارنة الاتحادي لدولة الامارات العربية المتحدة، مطابع البيان التجارية، دبي، ط1.
- دلخار صلاح بوتاني، 2016م، الحماية الجنائية الموضوعية للمعلوماتية دراسة مقارنة، الإسكندرية، دار الفكر الجامعي.
- زيدان زيجة،2011م، الجريمة المعلوماتية في التشريع الجزائري والدوليين، عين ميلة، الجزائر.
- فرج يوسف أمير، 2016م، ط1، حقوق الملكيَّة الفكريَّة الالكترونيَّة والمساس بها باعتبارها جريمة معلوماتية، الإسكندرية.
- رستم هشام فريد، 1992م، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلاء الحديثة، أسيوط.
- ينظر: Djamal Djenane, Criminalité informatique, le phénomène prend de l'ampleur Publié dans Info Soir le 18 Mai 2008. Colloque international « la sécurité des systèmes d'information au service de la sécurité publique ».
- OP ;2003 ; TRE WORLD BANK ; ALSO ; IBID.
- قنديل أشرف عبد القادر، 2018م، الوسائل الالكترونية ودورها في الاثبات الجنائي، الاسكندرية، دار الجامعة الجديدة.
- الحوسيني فهد بن سيف، 2010م، جرائم التجارة الالكترونية ووسائل مواجهتها، دار السحاب للنشر والتوزيع، ط1.
- الرومي محمد أمين، 2008م، المستند الالكتروني، مصر، درا الكتب القانونية.
- السيد عبد الحميد أحمد،2018م، ط1، جرائم الشبكة العنكبوتية وغسل الأموال في إطار الملاحقة الأمنية والقضائية الدولية، الإسكندرية، مكتبة الوفاء.

الأطروحات:

- قويقح حورية، 2020م2021م، الجرائم الاقتصادية عبر الشبكة المعلوماتية، دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه، الجزائر، كلية أصول الدين.
- شنين صالح، الحماية الجنائية للتجارة الالكترونية (دراسة مقارنة)، 2012م/ 2013م، رسالة لنيل شهادة الدكتوراه، في القانون الخاص، جامعة أبو بكر، بلقايد تلمسان، كلية الحقوق.

المقالات:

- عبد الرحيم صباح، عبد الرحيم وهيبة، 2017م، جرائم التجارة الالكترونية، المجلة الدولية للبحوث القانونية والسياسية، العدد 1.
- المؤلف مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الثاني، السنة التاسعة، معوقات التجارة الالكترونية ومتطلبات النظام القانوني لمواجهتها (دراسة مقارنة).

المداخلات:

- العبدلي عابد، 1426هـ، 2005م، التجارة الالكترونية في الدول الإسلامية الواقع _ التحديات_ الآمال، المؤتمر العالمي الثالث للاقتصاد الإسلامي، جامعة أم القرى، مكة المكرمة.
- حامي خديجة، الأنظمة المعلوماتية في مواجهة القرصنة والتخريب، (المخاطر المحدقة والحلول الناجعة)، 03_ 04، نوفمبر 2015م. الملتقى الوطني حول الأمن المعلوماتي مهدداته وسبل الحماية جامعة مولود معمري، تيزي وزو، قسم اللُّغة العربية وآدابها، مخبر الممارسات اللغوية في الجزائر.
- **مواقع الانترنيت:**

http://adresse complète (consulté le jour/mois/année

sous la direction de Rodolphe Saric 1999, Rapport de stage : Criminalité Liang Jiansheng, informatique.

بن فهد العجلان عبد الله بن عبد العزيز، في المدة من 2_4 يونيو 2008م، الإرهاب الإلكتروني في عصر العولمة، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الانترنت، المنعقد بالقاهرة على الموقع WWW.f.law.net/law/ threads/ 28535

_ حوصلة نشاط مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية ومكافحتها للدرك الوطني الجزائري، لسنة 2017م.