المسؤولية الجزائية عن المساس بنطاق التجارة الإلكترونية

Criminal responsibility for prejudice to the scope of e-commerce

الدكتورة بـادي بوقميجة نجيبة[1]

D. boukemidja nadjiba

كلية الحقوق، جامعة الجزائر n.boukemidja@univ-alger.dz

تاريخ الاستلام: 2020/03/19 تاريخ القبول: 2020/05/02 تاريخ النشر: 2020/06/30

ملخص:

نتيجة سرعة التعاملات المتعلقة بالتجارة الإلكترونية، نجد عدة صور تترتب عن المساس بهذه الأخيرة. بحيث لا يمكن حصر هذه الصور، باعتبار أن التعدي يمكنه أن يتخذ عدة أشكال، إلا أنه يمكننا التطرق إليها على سبيل المثال لا الحصر. وبالتالي تناول الجرائم الواقعة على التجارة الإلكترونية، من منظورين.

من جهة الجرائم المتعلقة بعروض التجارة الإلكترونية، باعتبار أن التعاملات في هذا الاطار تتعلق بالسلع والخدمات، وذلك في شكل عروض. ومن جهة مقابلة الجرائم الواقعة على مواقع التجارة الإلكترونية، خاصة وأنه غالبا ما يتم التعدي على المواقع الإلكترونية، التي تعرض فيها السلع والخدمات إلكترونيا، وذلك بغرض الاعتداء على مختلف العروض وتحويلها، بالإضافة إلى أنه جراء ذلك نكون أمام إمكانية انصراف النية إلى تحويل الزبائن.

كلمات مفتاحية: التجارة الإلكترونية، الجرائم، العروض، المواقع الإلكترونية، الأنظمة.

المؤلف المرسل: بادي بوقميجة نجيبة ، **الإيميل:** n.boukemidja@univ-alger.dz

Abstract:

In view of the speed of transactions resulting from e-commerce, several images are arranged for the violation related to the latter. So that these images can not be limited, as the infringement can take many forms, but we can address them for example, but not limited to. Thus, dealing with crimes against e-commerce, from two perspectives.

On the one hand, crimes related to e-commerce offers, as transactions in this context relate to goods and services, in the form of offers. And on the one hand to meet the crimes that occur on e-commerce sites, especially since the websites that offer goods and services electronically are often infringed, in order to attack and transfer various offers, in addition to that, as a result of that, we are facing the possibility of deviating the intention to convert customers.

Keywords: E-commerce, crimes, presentations, websites, systems.

1. مقدمة:

إن ظهور الإنترنت وامتداد استعمالاتها في نقل المعلومات وتخزينها وتبادل السلع والخدمات القابلة للنقل إلكترونيا، ساهم في تشكيل ركيزة أساسية في التجارة الدولية والمحلية خاصة في الدول المتقدمة، باعتبارها الوسيلة الهامة في إنجاز اتفاقيات الأعمال والإعلان والتسويق والتبادل التجاري، مما أدى إلى انتشار مفهوم التجارة الإلكترونية الذي تعاظم دورها نظرا لتأثيرها الفعال على الأسواق وأداء المؤسسات وقدراتها التنافسية. (ايت مبارك، 2016)

وهناك العديد من المسائل الهامة الملازمة لانطلاق التجارة الإلكترونية، وأن كل مسألة من هذه المسائل ترتبط وبصفة أكيدة بزيادة مستويات الثقة والحفاظ عليها والتي تعتبر الأشخاص سواء كان عاديون أو اعتباريون كأساس لإنجاز أي معاملة الكرتونية تجارية، وزيادة على ذلك المسائل المتعلقة بالبيئة الاجتماعية، وأخرى متعلقة بالبنية التحتية، ومسائل متعلقة بالإطار القانوني والتشريعي، وكل هذه المسائل مرتبطة ببعضها البعض.

كما أن حماية خصوصية المستهلك في التجارة الإلكترونية من مختلف الجرائم أمر ضروري ومهم ،يفرض إيجاد الآليات التي تمنع استعمال المعلومات الناتجة عن التعاملات التجارية لأهداف وأغراض غير معلنة، ومن أهم عوائق استعمال التجارة الإلكترونية من وجهة المستهلك تكمن في صعوبة تحديد مصدر المنتجات وتحديد المسؤوليات، عندما يتضح أن هذه المنتجات لا توافق النوعية المعلن عنها أو غير ملائمة، هنا تكون الوضعية أكثر تعقيدا خصوصا إذا تعلق الأمر بمنتجات مادية، هذه المسألة تتضح بأنها حرجة بوجه خاص بالنسبة لأولئك المتعاملين الجدد داخل السوق عندما لا يكونون قد حصلوا بعد على المكانة المرموقة على مستوى السوق الإلكتروني خاصة عندما يتعلق الأمر بمنتجات مادية. لذلك من الضروري إيجاد إطار قانوني لحماية المستهلك من هذه الجرائم، مع وضع أنظمة حمائية الكترونية (بن رجدال، 2002، ص82).

وكل ذلك يندرج بداية تحت مظلة المسؤولية الجزائية المنصوص عليها في قانون العقوبات، باعتبارها الحماية العامة. بالإضافة إلى مقتضيات القانون 18- 05 المتعلق بالتجارة الإلكترونية، كون الحماية هنا خاصة.

حيث أن قانون العقوبات أدرج القسم السابع مكرر، بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، والمواد من 394 مكرر إلى 394 مكرر 07، تحت الفصل الثالث بعنوان " الجنايات والجنح ضد الأموال". ويلاحظ على الجرائم المذكورة أنها متعلقة بمنظومة المعالجة الآلية للمعطيات، ولم يخص بالذكر جرائم التجارة الإلكترونية. مما يستدعي الالتزام بمقتضيات مبدأ الشرعية وتطبيق النص الخاص إذا تعلق الأمر بجرائم التجارة الإلكترونية، والتي وردت صريحة في القانون 18- 05 المتعلق بالتجارة الإلكترونية.

وبالتالي التساؤل في إطار الإشكالية عن فحوى الجرائم الماسة بالتجارة الإلكترونية ؟

وقد ارتأينا تناول هذه الجرائم التي لا يمكن حصرها، بالاعتماد على تقسيمين ومن خلال المبحثين التاليين:

المبحث الأول: الجرائم المتعلقة بعروض التجارة الإلكترونية.

المبحث الثاني: الجرائم الماسة بمواقع التجارة الإلكترونية.

وبالتالي فإن المساس بنطاق التجارة الإلكترونية يشهد تعدد الجرائم، والتي يمكن تصنيفها فيما يتعلق بالعروض وفيما يتعلق بالمواقع الإلكترونية. وعليه فإن الدراسة في هذا الإطار تستوجب الاعتماد على وصف الجرائم، أي المنهج الوصفي، وأيضا تحليل بعض النقاط القانونية المتعلقة بها، بغرض التوصل للنتائج، وهو بمثابة اعتماد للمنهج التحليلي.

2. المبحث الأول: الجرائم المتعلقة بعروض التجارة الإلكترونية

نشير بداية إلى أن العروض المتعلقة بالتجارة الإلكترونية، تكون في إطار الأنواع المتعددة لهذه الأخيرة، وهي كالتالي :

أ-التجارة الإلكترونية من الأعمال إلى المستهلك B2C) Business to Consumer هنا :(يتم البيع السلع والخدمات مباشرة إلى الزبائن وهو ما يطلق عليه البيع بالتجزئة.

ب- التجارة الإلكترونية من الأعمال إلى الأعمال B2B)Business to Business التعاملات بين :(الشركات بعضها ببعض (تجار الجملة، تجار التجزئة، المصدرين و الموردين).

ج - التجارة الإلكترونية من المستهلك إلى المستهلك C2C) Consumer to): Consumer تعامل الزبائن مع بعضهم البعض و بدون وسطاء حيث تتم عمليات الشراء و البيع مباشرة.

د- التجارة الإلكترونية من الأعمال إلى الحكومة B2G(Business to) Gouvernementالعلاقة بين المشاريع التي تنفيذها الحكومة واتفاقيات البيع بين مؤسسة تجارية والحكومة نفسها.

هـ- التجارة الإلكترونية من الحكومة إلى الأفراد (Gouvernement to Consumer G2C)ويكون هذا النوع بين الأفراد والحكومة وتستخدم في دفع رسوم الضريبية والفواتير ورسوم

البلدية ،كما يمكن للحكومة أن تدفع رواتب عامليها مباشرة الكترونيا عند نهاية كل شهر (لونيس، 2011، ص100).

ولقد كانت الأموال في اطار الأداء الذي تقدمه التجارة الإلكترونية ، ومن وجهة النظر التقليدية تقتصر على الأموال المادية، لهذا اقتصرت الحماية الجزائية بدورها على الأموال المادية، لكن مع التطور التكنولوجي ظهرت أموال معلوماتية معنوية ذات أهمية كبيرة كالبرامج والمعلومات، فاستدعى الأمر إعادة النظر في حصر الأموال في الأشياء المادية لوحدها. (القهوجي، 1999، صفحة 81)

وفي اطار الأموال المعلوماتية، تقدم عروض للتجارة الإلكترونية. لكن يتم التساؤل عن مختلف العروض التي تبث على شبكات الأنترنت والتي يكون الغرض منها بيع منتجات وخدمات مختلفة في لإطار التجارة الإلكترونية، ويطلب من المتلقي الاتصال بشتى أنواع الاتصالات الحديثة، عبر الأنترنت لاقتناء هذه المنتجات.

خاصة إذا علمنا أن هذه العروض تتناول جميع صفات ومميزات السلعة أو الخدمة وفي أغلب الأحيان تكون هناك صور وفيديوهات تبين المنتوج كما أنها تحدد الثمن. (حواس، 2015، صفحة 14)

لقد اختلفت الأنظمة القانونية الوضعية في تكييف هذه العروض فهناك بعض الأنظمة اعتبرت ذلك العرض مجرد إعلان Advertising تجاري ولا يحتوي على إيجاب، وبالتالي لا يرتب أثرا، ولا تترتب عنه أي جريمة متعلقة بالتجارة الإلكترونية، كالقانون الكويتي.

وتكييف آخر يعتبره دعوة إلى التعاقد Invitation to Treat، أو تمهيدا للتفاوض Preliminary nogotiation كالقانون الإنجليزي، أو إيجابا offer ورغبة في التعاقد كالقانون الفرنسي والإيطالي والبلجيكي، أما القانون المدني الألماني، فقد ذهب إلى أنه فيما يتعلق بالعرض الموجه إلى أكثر من شخص، فإن للمحكمة أن تفصل في كل حالة على حدة دون الالتزام بقواعد معينة وقد سلكت اتفاقية فيينا بشأن البيع الدولي للبضائع لعام 1980 نفس الاتجاه حيث بينت في المادة 2/14 أنه يستلزم في الإيجاب أن يكون موجها إلى شخص أو مجموعة أشخاص، و اعتبرت أن العرض الذي يخلو من تحديد الشخص أو الأشخاص الموجه إليهم يعد بمثابة دعوى إلى الإيجاب أي دعوى للتفاوض، ما لم يتضح أن

إرادة الأطراف اتجهت إلى خلاف ذلك، فإن هذا يعد تعبيرا قاطعا عن إرادة صاحبه للتعاقد مع كل من يقبل العرض ويتقدم إليه لإبرام العقد.

أي أن الإعلان يعتبر إيجابا إذا تضمن ما يفيد التزام الشخص بإبرام العقد في حالة صدور قبول مطابق.

كما أنه ضمانا لسلامة الرّضا الذي يصدره المستهلك وعدم اعتباره مشوبا بالغش والتدليس، بات من الضروري أن يكون الإعلان واضحا في كل تفصيلاته، وبصفة خاصة تلك التي قد تؤثر في قرار المستهلك في الشراء. وذلك من خلال الجرائم التي يمكنها أن تنجم عن التجارة الإلكترونية.

وتتجلى أهمية وجود هذا المبدأ في أنه يجنب المستهلك الخلط بين الرسائل التي تقصد فقط إعلامه بشيء ما، أو تقدم على هذا الشيء بعض البيانات والتي يطلق عليها الرسائل الإعلامية، وبين الرسائل التي تروّج لشراء السلع والخدمات والتي يطلق عليها الرسائل الإعلانية. (غنام، 2008، صفحة 53)

وقد قضت محكمة النقض المصرية باعتبار طرح مناقصات التوريد وغير ذلك من البيانات الموجهة للجمهور أو الأفراد كالنشرات والإعلانات ليس إيجابا وإنما دعوة إلى التفاوض، فالإيجاب هو الاستجابة لهذه الدعوى ويتم التعاقد بقبول الجهة صاحبة المناقصة لهذا الإيجاب.

وبعدم اعتبار العرض الموجه للجمهور إيجابا وإنما يعد دعوة للتفاوض هو ما يتفق مع طبيعة ومستلزمات عقود التجارة الإلكترونية، فقد يتسلم المنتج أو العارض مئات بل آلاف الرسائل الإلكترونية بالموافقة على طلب الشراء دون أن يكون لديه الكمية الكافية، أو تكون لديه ولكن بأسعار أزيد مما كانت عليه وقت الإعلان نتيجة ازدياد الطلب على السلعة، أو لارتفاع الأسعار، ولذلك فإن اعتبار الإعلان الإلكتروني الموجه للعامة عبر شبكة الأنترنت مجرد دعوة للتعاقد من شأنه أن يمكن العارض من رفض الطلبات الزائدة عن إمكانياته، كعدم توفر الكمية الكافية من المنتج أو الخدمة.

وأيضا بعدم اعتبار العرض الموجه للجمهور إيجابا يكون التاجر قد تجنب خسارة كبيرة سواء من ناحية التزامه بالتعويض أو لتقديمه بضاعة بأسعار غير مناسبة (ممدوح، 2008)، وينجر ذلك حتى على الآثار المتمثلة في الجرائم الواقعة في إطار عروض التجارة الإلكترونية.

كما يمكن للتاجر أن يحمي نفسه، وذلك بأن يحتفظ لنفسه بإمكانية الرجوع في العرض بحيث لا يكون التاجر ملتزما بموجب هذا العرض الذي كان سيكفي مجرد قبوله لانعقاد العقد لو لم يحتفظ التاجر بمكنه الرجوع فيه، ولذلك ينصح الموجب بأن ينص في إيجابه على أن العرض الصادر منه ليس إلا دعوة للدخول في مفاوضات أو دعوة للتعاقد وذلك باستخدامه بعض العبارات مثل "دون التزام" « sans engagement » أو بعد التأكيد « Après confirmation »، وعندئذ فإن إجابة مستعمل الشبكة تجعل منه هو الموجب وتكون الرسائل الإلكترونية التي يرسلها البائع في إطار التجارة الإلكترونية، بعد ذلك هي القبول الذي ينعقد بها العقد . (أبو الحسن، 2003، صفحة 73)

هذا ويمثل نظام المعالجة الآلية للمعطيات المسالة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام. فإن ثبت تخلف هذا الشرط الأولي، لا يكون هناك مجال لهذا البحث، ويؤدي توافر هذا الشرط إلى الانتقال إلى المرحلة التالية وهي بحث توافر أركان أية جريمة من الجرائم السابقة، إذ أن هذا الشرط يعتبر عنصر لازما لكل منها، ولذلك يكون من الضروري تحديد مفهوم نظام الآلية للمعطيات .

حيث أن نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن انه تعبير متطور يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية. (القهوجي، 1999، صفحة 120)

كما أن الدعامات المادية للحاسب الآلي قد احتلت مكانة المحررات والصكوك ونظرا لأهمية وخطورة ما تحتويه من بيانات والتي قد تكون محلا للاعتداء بتغيير حقيقتها بقصد الغش في مضمونها، والذي من شأنه إحداث أضرار مادية أو معنوية. (قارة، 2007، صفحة 193) كتزوير المستخرجات الإلكترونية بخصوص الأوراق المالية فيما يتعلق بالتجارة الإلكترونية. وهنا يجب على المستخدم اتخاذ جميع التدابير المعقولة للحفاظ على أمن الأجهزة الشخصية وإبلاغ مقدم الخدمة دون تأخير بأي استخدام غير مصرح به . ولكن لا يمكن أن يخضع لافتراض الإهمال. وبالتالي ، فإن الأمر متروك لمقدم الخدمة لإثبات أن المستخدم تصرف

بطريقة احتيالية أو لم يمتثل ، عن قصد أو عن طريق الإهمال الجسيم ، لالتزاماته. (LARRIEU, 2019, p. 2266)

ومثال ذلك الموقع الإلكتروني Doctopharma.fr، الذي ينحصر دوره في توصيل الأدوية والمستحضرات الصيدلانية لمستخدمي الانترنت. وذلك على عكس ما يتبادر بالذهن عند استخدام هذا الموقع، نتيجة ما يدعيه مقدم الخدمة[1]. (MARIGNIER-MERRAN, 2019, p. 387)

ومن بين الجرائم المتعلقة بعروض التجارة الإلكترونية نجد جريمة التزوير، وهي متعلقة بالمحرر، والمحرر في مضمونه كتابة مركبة من حروف أو علامات تدل على معنى أو فكرة معينة، وإمكانية القراءة البصرية لمحتواه، وهو ما تفرضه نصوص التزوير التقليدية، وعليه يمكن إجمال خصائص المحرر في ثلاث نقاط (فشار، أكتوبر 2009):

- أن يتخذ المحرر شكلا كتابيا ويجب إدراك مضمون المحرر بالنظر إليه أو لمسه وإذا استحالت قرأته فلا يصلح وسيلة للإثبات ولا عقاب على ما احتواه من تغيير.
- أن تكون الكتابة منسوبة لشخص معين .
- أن يحدث المحرر أثارا قانونية.

فهل يعتبر البيان المعالج آليا من قبيل المحررات التقليدية التي يسري عليها النص الجنائي الخاص بالتزوير ؟

بإسقاط المفهوم التقليدي للمحرر على مجال المعالجة الآلية للبيانات ، نجد أن تغيير الحقيقة الذي يكون محله الأشرطة الممغنطة لا تقع به جريمة التزوير في المحررات وذلك لعدم وجود عنصر الكتابة فجريمة التزوير تشترط الكتابة فأي تغيير في الوعاء ألمعلوماتي لا يعتبر تزويرا لانتفاء هذا الشرط .

[1] - Quand la plateforme Doctopharma.fr met en relation des internautes et les sites de pharmacies d'officine pour l'achat de médicaments et de produits parapharmaceutiques en ligne, elle ne se cantonne pas, contrairement à ce qu'elle prétend et à ce qu'a retenu la cour d'appel, à un rôle de « sous-traitant technique des pharmaciens » ou de simple « support technique des sites des pharmaciens d'officine » étranger au rapport contractuel, même si chaque site d'officine est exploité directement et sous la seule responsabilité de chaque pharmacien, qui détermine unilatéralement les produits qu'il propose à la vente en ligne et leur prix. La Cour de cassation.Com. 19 juin 2019, n° 18-12.292, D. 2019. 1394 .

الفقيه (DEVEY) يقرر أن الكتابة مطلب تقليدي في جرائم التزوير، لكن تجدر الإشارة إلى أن بعض الفقه الفرنسي يرى إمكانية تغليب روح النصوص واعتبار ما يظهر على شاشة الحاسب شكلا مستحدثا للمحرر. (قارة، 2007، صفحة 137)

ويلاحظ بأن جريمة التزوير في المجال المعلوماتي، ومن بينه مجال التجارة الإلكترونية، من اخطر صور غش المعلوماتية نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسب الآلي الآن والذي اقتحم كافة المجالات وأصبحت تجري من خلال كم هائل من العمليات ذات الآثار القانونية الهامة والخطيرة والتي لا يصدق عليها وصف " المكتوب" في القانونين المدني والجنائي، وقد أثار هذا الوضع الشك حول دلالتها في الإثبات وحول إمكانية وقوع جريمة التزوير العادية ولهذا كان التدخل التشريعي ذو أهمية بالغة.

وتجدر الإشارة إلى أن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، ربما اقتداء بما فعله المشرع الفرنسي الذي أخضع أفعال التزوير ألمعلوماتي للنصوص العامة للتزوير وذلك بعد أن قام بتعديله بجعل موضوع التزوير أي دعامة مادية وليس محررا، الفرق أن النصوص الواردة في قانون العقوبات الجزائري الخاصة بالتزوير تجعل التزوير يرد على محرر وعليه لا يمكن إخضاع أفعال التزوير المعلوماتي للنصوص العامة للتزوير كما هو عليه الحال في التشريع الفرنسي مما يستدعي تدخلا تشريعيا، إما بتعديل نصوص التزوير التقليدية أو بإدراج نص خاص بالتزوير المعلوماتي.

وبهذا فإن التشريع الجزائري يعد من التشريعات التقليدية، حيث أدرج النصوص الخاصة بتزوير المحررات في الأقسام الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد 124 إلى 229 التي تشترط المحرر لتطبيق جريمة التزوير، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من أجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير، وكان من الأفضل لو أضاف المشرع الجزائري في باب التزوير في المحررات نصا يعرف فيه التزوير، خصوصا ما تعلق منها بالتجارة الإلكترونية.

وعليه يقترح البعض إضافة نص إلى باب التزوير في المحررات يعرف فيه التزوير على النحو التالي: كل تغيير للحقيقة بطريق الغش في مكتوب أو في أي دعامة أخرى تحتوي تعبيرا عن الفكر.

وهذا النص قد يكون أشمل حيث يمكن أن تدرج فيه جميع المستندات المعلوماتية حتى وإن كانت غير معالجة آليا، وهو ما يتضمن حماية جزائية فعالة لكافة المنتجات المعلوماتية، من بينها تلك المتعلقة بالتجارة الإلكترونية. (فشار، أكتوبر 2009)

إلى جانب ذلك نجد السرقة المتعلقة بالتجارة الإلكترونية. حيث استقر الفقه على أن المال موضوع جريمة السرقة يجب أن يكون ماديا أي له كيان مادي ملموس، وهذا ما تفرضه طبيعة الاختلاس في جريمة السرقة باعتباره الاستيلاء على الحيازة الكاملة، وهو ما لا يتصور إلا بالنسبة للأشياء المادية. (قرشوش، 2007، صفحة 30)

ولقد قام فريق من الفقه وفقا لذلك بقياس سرقة البرامج والمعلومات على سرقة التيار الكهربائي إلا أن ذلك غير مستساغ ففي ذلك خروج على مبدأ شرعية الجرائم والعقوبات والذي يمنع التفسير بالقياس في مسائل التجريم بالإضافة إلى ذلك فالكهرباء تعتبر شيئا ماديا لا معنويا يخضع للسيطرة كغيره من الأشياء المادية، فهي تعبأ وتنقل وتحاز وتقاس ويتحكم فيها سواء بالاستهلاك أو عدمه، وترد عليها الملكية، وكل هذا يؤكد صلاحيتها للاختلاس. (عادل قور، 2005، صفحة 162)

ووفقا لنصوص جريمة السرقة تصلح برامج الحاسوب والمعلومات الخاصة بالتجارة الإلكترونية لأن تكون محلا للاختلاس. والأخذ في جريمة السرقة باعتبار أنها أشياء معنوية يصدق عليها وصف المال لعمومية تلك النصوص الجنائية المنظمة لجريمة السرقة. ومما لاشك فيه أن عدم انطباق وصف المال على البرامج والمعلومات يؤدي حتما إلى تجريده من الحماية القانونية الجنائية مما يفتح المجال واسعا أمام قرصنة البرامج والمعلومات، إلا أنه يتعين عدم الاكتفاء بتطبيق تلك النصوص بعمومها، بل يجب أن يتدخل المشرع بالنص على صلاحية هذه الأموال المعنوية لأن تكون محلا لجريمة السرقة، أو إعطاء مفهوم واسع للمال كما فعلت بعض التشريعات التي عرفته على أنه كل شيء له قيمة مالية، مما يدخل فيه الأشياء المعنوية. (عفيفي، 2003، صفحة 142)

أما بالنسبة للنشاط الإجرامي المكون لجريمة السرقة، حتى في علاقتها بالتجارة الإلكترونية، وهو الاختلاس وبتطبيقه على برامج الحاسب الآلي أو المعلومات المعالجة بصفة عامة، نلاحظ أن الجاني وان كان

يدخل في ذمته ما استولى عليه من برامج إلا انه في نفس الوقت لم يخرج هذه البرامج من ذمة صاحبها الشرعي إذ تظل رغم مباشرة أفعال الاختلاس عليها تحت سيطرة هذا الأخير دون انتقاص من محتواها، كما يلاحظ إن الاستيلاء على البرامج باعتبارها معلومات لا يتصور من الوهلة الأولى إلا على انه انتقال لهذه المعلومات من ذهن إلى ذهن أو من ذاكرة إلى ذاكرة. (القهوجي، 1999، صفحة 95)

كما أن تطبيق النشاط الإجرامي لجريمة خيانة الأمانة في المجال المعلوماتي، وفي علاقته بالتجارة الإلكترونية ،تطبيق نسبي فلا جدال في وقوع جريمة خيانة الأمانة بالنسبة للدعامات المثبتة عليها البرامج والمعلومات وذلك في الحالة التي يقوم فيها الأمين بنسخ البرنامج لحسابه الخاص متجاوزا الاتفاق الذي يربطه بصاحب البرنامج إذ يتحقق بهذا النسخ فعل الاستعمال والذي يقصد به استخدام الأمين للمال استخداما يستنزف قيمته كلها أو بعضها مع بقاء مادته على حالها إلا انه من الصعب القول بقيام جريمة خيانة الأمانة في حالة البرامج والمعلومات المستقلة عن الدعامة وذلك لعدم إمكانية قيام النشاط الإجرامي للجريمة ألا وهو التسليم بناء على عقد من عقود الأمانة لعدم وجود نشاط مادي مجسم يتحقق به فعل الاستلام، مما يحول دون صلاحية البرامج والمعلومات للخضوع للنشاط الإجرامي في جريمة خيانة الأمانة. (قارة، 2007، صفحة 45)

3. المبحث الثاني: الجرائم المتعلقة بمواقع التجارة الإلكترونية

إن أغلب الجرائم التي تمس بالتجارة الإلكترونية، متعلقة بمواقع هذه الأخيرة، باعتبارها الأكثر عرضة للانتهاك. ومثال ذلك، الدخول للمواقع الإلكترونية المتعلقة بالتجارة الإلكترونية بدون وجه حق. ولا عبرة في هذه الجريمة بصفة مرتكب الفعل الإجرامي، فقد يكون الفاعل يعمل في مجال الأنظمة أو لا يعمل، وسواء كان يفهم أو لا يفهم أسلوب تشغيل النظام، فيكفي أن يكون الجاني ليس ممن لهم الحق في الدخول إلى النظام حتى تتوفر جريمة الدخول غير المشروع.

وبالتالي فإن الركن المادي لجريمة الدخول غير المرخص به يتحقق بمجرد شروع أي شخص في الدخول أو الدخول بالفعل إلى نظام المعالجة الآلية للمعطيات بأي طريقة، وتقع هذه الجريمة بالدخول إلى كل النظام أو جزء منه.

وأيضا نجد جريمة البقاء غير المشروع ويقصد به التواجد داخل نظام مواقع التجارة الإلكترونية ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق البقاء المعاقب عليه مستقلا عن الدخول إلى النظام إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ لكن المتدخل لم ينسحب وبقي رغم ذلك فيعاقب في هذه الحالة على جريمة البقاء غير المشروع إذا توافر ركنها المعنوي.

ويقصد بالإدخال إضافة معطيات جديدة على الدعامة سواء كانت خالية أم كان يوجد بها معطيات من قبل، وقد يتم إدخال هذه المعطيات بقصد التشويش على صحة المعطيات القائمة.

ولعل اصطناع المعلومات هو الأكثر سهولة في التنفيذ ولاسيما المؤسسات ذات الأموال، ويتحقق هذا الفعل في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب والائتمان سواء من حاملها الشرعي، أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال ، بإدخال برنامج غريب (كفيروس، أو قنبلة معلوماتية) يضيف معلومات جديدة.

هذا وشهدت التشريعات المجرمة لأفعال الدخول والبقاء غير المصرح بهما واعتراض أنظمة المعلومات اختلافات عدة وعرفت الآراء الفقهية بهذا الشأن تضاربا كبيرا.

وقد ثار بين الفقهاء جدل الواسع ما بين مؤيد ومعارض لتجريم الدخول غير المصرح به إلى أنظمة المعلوماتية، سنوضح فيما يلي طبيعة الاختلاف الفقهي بين الاتجاهين وموقف بعض التشريعات من هذا الجدل.

بحيث يرى الاتجاه المؤيد لتجريم الدخول غير المصرح به إلى أنظمة المعالجة الآلية للمعطيات أن الدخول غير المصرح به إلى النظام سواء كان مقصودا في ذاته أو كان بغرض ارتكاب جريمة أخرى كالإتلاف أو الإفشاء أو السرقة، فإن له الكثير من الآثار السلبية التي تلحق صاحب النظام أو المعلومات. بالإضافة إلى ذلك فإن قابلية المعلومات المبرمجة آليا للوصول غير المشروع إليها يفوق كثيرا ما كان عليه الحال قبل عصر تقنيات الحاسبات والاتصالات، ذلك أن المعلومات الهامة والمدونة في أوراق وسجلات كان يتم حفظها في أماكن يصعب الوصول إليها، مما يجعلها بمنأى عن التلاعب بها والاطلاع عليها، وخاصة في مواجهة غير المتعاملين في المؤسسات المحفوظة بها، في حين أن المعلومات المبرمجة آليا والمتصلة فيما بينها عن طريق شبكات الاتصالات تكون أكثر عرضة للوصول غير المشروع إليها. وتترتب في كثير من الحالات

خسائر مادية كبيرة على مجرد محاولة وقف الدخول ولو لم تترتب عليه أضرار فعلية تلحق بالنظام وبالمعلومات التي يحتوي عليها.

وهناك موقف يخالف ذلك ويرى أنه لا ضرورة لتجريم الدخول غير المصرح به إلى النظام لأنه لا توجد حاجة ملحة تستدعي هذا التجريم، حيث لم تبين الدراسات والإحصاءات المختلفة هذه الضرورة كما أن مجرد الدخول غير المصرح به إلى أنظمة المعلومات دون أن يكون لدى صاحبه نية ارتكاب جريمة لاحقة على هذا الدخول، لا يعدو أن يكون مجرد استعراض لبعض الملكات الذهنية والفنية التي يمتلكها، وهو ما لا يمكن أن يشكل جريمة يعاقب عليها .فضلا عن ذلك فحالات الدخول غير المصرح به والتي لا يترتب عليها إتلاف للمعلومات أو استخدامها لغرض غير مشروع لا يمكن الكشف عنها حيث لا تترك أثرا يدل عليها، فالصعوبة العملية التي سوف تواجه جهات التحقيق في حالات الدخول غير المصرح به.- وذلك نظرا لما تنطوي عليه من صعوبة فنية بالغة، وبالتالي ستكون عائقا دون تجريم هذا السلوك-.

تم تجريم الدخول غير المصرح به إلى أنظمة المعلوماتية في العديد من الدول، وإن اختلفت فيما بينها من حيث الشروط المتطلبة لتطبيق نصوصه. أثار تحديد الهدف الذي يعقب عملية الدخول خلافا أظهرته النصوص القانونية المختلفة التي تناولت الجريمة، فالدخول غير المصرح به إلى نظام المعلوماتية يستمد عدم مشروعيته من كونه غير مصرح به أو كونه مخالف لأحكام القانون. غير أن هذا الدخول قد يكون مقصودا في ذاته كما قد يكون مقصودا باعتباره وسيلة لتحقيق غاية أخرى، سواء تمثلت هذه الغاية في الحصول على المعلومات لتحقيق غرض ما، أو كان الدخول إلى النظام ممرا يتم من خلاله الدخول إلى نظام آخر من الصعب على الفاعل الدخول إليه ابتداء.

وقد أسفر ذلك عن التساؤل حول مدى ملائمة تدخل المشرع الجنائي للعقاب على الدخول المجرد إلى نظام المعلوماتية، وتنازعت الإجابة عن هذا السؤال ثلاثة اتجاهات، يرى الأول أنه لا يمكن عقاب كل من يقرع باب النظام، في حين يذهب اتجاه آخر إلى أن جريمة الدخول إلى الأنظمة المعلوماتية وإنما يجب أن يحاط التجريم بشروط محددة.

بينما يذهب موقف ثالث إلى اعتبار أنه تقوم بمجرد فعل الدخول غير المصرح به بغض النظر عن النتيجة التي تعقب هذا الدخول إلى اعتبار جريمة الدخول غير المصرح به إلى الأنظمة الجريمة المعلوماتية الجريمة الأساسية، أما ما يعقب ذلك من أفعال فهي لا تشكل سوى ظروف مشددة. وقد حدا المشرع الجزائري حدو المشرع الفرنسي في تجريمه لمجرد الدخول غير المصرح به [2].

كما نشير إلى التمييز بين الدخول والبقاء داخل الأنظمة، بحيث يرجع البعض الاختلاف القائم بين جريمتي الدخول والبقاء غير المصرح بهما إلى أن جريمة الدخول جريمة إيجابية تقتضي إتيان فعل الدخول، في حين تقوم جريمة البقاء بسلوك إجرامي سلبي، فرغم دخول الجاني صدفة أو خطأ إلى مواقع التجارة الإلكترونية، ورغم علمه بأن ذلك غير مشروع فهو يرفض الخروج من النظام وبمعنى آخر يمتنع عن الخروج.

لذلك فالنشاط الإجرامي – حسب هذا الجانب– يمثل في هذه الصورة سلوكا سلبيا من الجاني. إلا أن هناك جانب آخر يرى أن الامتناع عن الخروج من النظام الذي تم الدخول إليه ليس مناط التجريم، بل أن السلوك المجرم هو البقاء داخل هذا النظام الخاص بالتجارة الإلكترونية، بعد الدخول إليه مع العلم بأن هذا البقاء غير مصرح به وهو ما يشكل سلوكا إيجابيا.

ذهبت بعض الآراء للقول بأن طبيعة البقاء هي طبيعة الدخول ذاتها وينطبق عليه كل ما ينطبق على الدخول. لكن يذهب رأي إلى اعتبار كل من جريمتي الدخول وما يميز بينهما هو وقوع الجريمة في وقت واحد أو استمرارها، البقاء من الجرائم المستمرة، بينما يرى رأي آخر اعتبار جريمة الدخول جريمة متتابعة الأفعال وجريمة البقاء مستمرة.

ورأي ثالث يجد جريمة الدخول إلى مواقع التجارة الإلكترونية وقتية ذات أثر ممتد، وجريمة البقاء جريمة مستمرة. حيث أن لهذا التمييز أهمية في الإشكالات المطروحة حول هاتين الجريمتين المتعلقتين بحدود كل من جريمتي البقاء والدخول غير المصرح بهما. فقد ذهب رأي فقهي إلى القول أن جريمة الدخول تتحقق منذ اللحظة التي يتم فيها الدخول فعلا إلى النظام، وإن كان الدخول في نظر هذا الرأي يفترض بالضرورة البقاء

[2]– وذلك من خلال المادة 394 مكرر من قانون العقوبات أيا كانت النتيجة التي تعقبه، وكان موفقا في اتجاهه كونه أحاط نظام المعالجة الآلية بضمانات فعالة تحميه من الاختراق.

فترة قصيرة من الزمن تنتهي عندها جريمة الدخول وتكتمل، وبعد تلك اللحظة تبدأ جريمة البقاء داخل النظام وتنتهي بانتهاء حالة البقاء.

ويؤخذ على هذا الموقف أنه لا يحدد لحظة بداية جريمة البقاء بطريقة حاسمة، لهذا ذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه المتدخل أن بقاءه داخل النظام غير مشروع، وأخذ على الرأي الثاني أيضا صعوبة إثبات علم المتدخل.

هذا ويرى رأي ثالث أن جريمة البقاء داخل النظام تبدأ منذ اللحظة التي ينذر فيها المتدخل بأن تواجده غير مشروع فإذا لم ينسحب يرتكب منذ تلك اللحظة جريمة البقاء داخل النظام، غير أن هذا الرأي وإن أمكن توفير تقنياته الفنية إلا أنه لن يكون متاحا إلا بالنسبة للشركات والمؤسسات الكبيرة فقط، في اطار تعاملاتها، ومن بينها التجارة الإلكترونية.

فإذا كانت جريمة الدخول غير المصرح به لمواقع التجارة الإلكترونية، وقتية، فإنها في بعض صورها تكون متتابعة الأفعال حيث تقوم على أفعال متعددة تجمع بينها وحدة الحق المعتدى عليه ووحدة الغرض الإجرامي المستهدف بها. يتحقق ذلك في حالة النصوص التي تجرم الدخول غير المصرح به الذي يستهدف الوصول إلى المعلومات أو البرامج، أو تلك التي تجرم الدخول إلى كل جزء من النظام، ذلك أنه بعد دخول الفاعل إلى النظام يمكن القول من الناحية التقنية، أن فعل الدخول يتكرر بالدخول إلى كل برنامج وكل جزء من النظام. فنكون أمام أفعال متماثلة يعد كل منها جريمة في ذاته لو اكتفى الجاني به لعوقب من أجله.

ينتهي أصحاب هذا الموقف إلى أنه في هذه الحالة يمكن العقاب على البقاء غير المصرح به، لأنه بعد اكتساب الدخول صفته غير المشروعة فإن الدخول يتحقق بالوصول إلى أية معلومة بعد ذلك أو أي جزء من النظام. تثور الصعوبة في القوانين التي تتطلب لقيام جريمة الدخول غير المصرح به أن ينطوي الدخول على اختراق الإجراءات الأمنية الخاصة بالنظام، إذ يجب لاعتبار الجريمة متتابعة الأفعال في هذه الحالة أن يكون كل جزء من النظام تم الدخول إليه مشمولا بهذه الحماية. أما في حالة النصوص التي تجرم مجرد الدخول إلى النظام، فإنه لا يمكن العقاب على البقاء غير المصرح به ما وهو ما فعله المشرع الفرنسي حيث نص صراحة على تجريم البقاء داخل النظام إذ لم ينص على ذلك صراحة، تجريمه للدخول المجرد غير المصرح به.

وقد عمل المشرع الجزائري على ألا تفلت مثل هذه الحالات من العقاب، فقام بتجريم البقاء عن طريق الغش في كل أو جزء من نظام المعالجة الآلية للمعطيات مسايرا في ذلك ما ذهب إليه المشرع الفرنسي . (عباوي، 2017، صفحة 279)

وبموجب المادة 394 مكرر 1 من قانون العقوبات »يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات 2 وبغرامة من 000. 00 5دج إلى .2000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها". حيث أن هذا النص يعاقب على كل تلاعب بمحو أو تعديل المعطيات داخل النظام، بغض النظر عن النتائج.

ويلاحظ على هذه المادة أنها تدرج ثلاث صور في إطار التجريم، بما فيه ذلك المتعلق بالتجارة الإلكترونية، وهي كالتالي :

الإدخال: وذلك بإضافة معطيات جديدة على الدعامة الخاصة بها، ويتحقق فعل الإدخال كذلك بإدخال برنامج غريب (فيروس، حصان طروادة...) ليضيف معطيات جديدة.

المحو: وذلك بإزالة جزء من المعطيات الموجودة داخل النظام.

التعديل: وذلك بتغيير المعطيات الموجودة سواء بطريق مباشر أو باستخدام برامج خبيثة كالفيروسات.

هذه الصور الثلاث وردت على سبيل الحصر، فلا يقع تحت طائلة التجريم أي فعل آخر غير هذه الأفعال. ولو تضمن اعتداء على المعطيات داخل النظام كفعل النسخ أو النقل ولا تقوم هذه الجريمة إلا إذا كانت هذه العمليات تمت مع قصد جنائي وخارج الاستعمال المرخص، يتكون القصد الجنائي في الوقت الذي يحدث فيه إدخال المعطيات بإرادة التغيير في النظام وبغض النظر عن النتائج التي تحدث فيه. (أحمد مسعود، 2013، صفحة 75)

ومن جهة مقابلة فقد نصت المادة 394 مكرر2 ق ع في القسم الثاني منها « « يعاقب بالحبس من شهرين (2) إلى ثلاث (3)سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي – 2 :حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم« .

حيث أن هذه المادة تهدف لحماية هذه المعطيات من استعمالها في أغراض غير مشروعة كالمنافسة غير المشروعة ، إن لم تشكل جرائم أشد فيعاقب مرتكبها بالعقوبة الأشد.

وأيضا تعاقب المادة 394 مكرر5 ق ع الاشتراك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في المواد 394 مكرر إلى 394 مكرر2 من قانون العقوبات، وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية. وهذه الجريمة يعاقب عليها بنفس العقوبة للجريمة المراد ارتكابها، أو بالعقوبة الأشد في حالة تعدد الجرائم..والأفعال المادية تكون مثلا بتبادل معلومات مثل رموز الدخول، ولتقوم الجريمة يجب تواجد مجموعة منظمة بغرض ارتكاب الجرائم المنصوص والمعاقب عليها في المواد 394 مكرر ق ع إلى غاية 394 مكرر2 ق ع، ولا يكفي الاتفاق وحده، وإنما يجب أن يتبع بتحضير لجريمة أو أكثر، هذا التحضير لا يعاقب عليه إلا بتجسيده بعمل مادي أي بإتيان عمل إيجابي.

وتجدر الإشارة أنه يسعى المتخصصون بأمن المعلومات، حتى في إطار التجارة الإلكترونية، للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص حاليا شبكة الأنترانت فهم يسعون لتأمين سرية الرسائل الإلكترونية وسرية البيانات المتناقلة وخاصة بالأعمال التجارية الرقمية. ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الإلكترونية.

وتنقسم الأنظمة إلى ثلاثة أنواع :

- أنظمة مفتوحة للجمهور.
- أنظمة قاصرة على أصحاب الحق فيها ولكن بدون حماية فنية.
- أنظمة قاصرة على أصحاب الحق فيها وتتمتع بحماية فنية.

ومقتضى تطبيق هذا العنصر أن النوع الثالث فقط من تلك الأنظمة هو الذي يتمتع بالحماية الجنائية أما النوع الأول والثاني فلا يتمتعان بتلك الحماية، وهناك من يصرون عليه لأن الحماية الجزائية في نظرهم يجب أن تقتصر على الأنظمة المحمية فنيا.

لأنه من الطبيعي في نظرهم، أن من يقوم بالاستغلال يضع الوسائل الفنية اللازمة لمنع الغش وأن القانون الجنائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم، وليس من يهمل منهم في توفير الحد الأدنى لحماية أمواله، ويكون دور القانون الجنائي في هذه الحالة دور وقائي وهذا أيضا هو ما يتفق وسياسة المشرع الجنائي وما نلاحظه من المفهوم العام للحماية الجزائية للملكية. (قارة، 2007، صفحة 131)

كما أنه بالرجوع إلى النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، بما تعلق منها بالتجارة الإلكترونية، لا تتضمن شرط الحماية الفنية وخرجت تلك النصوص الخالية منه تماما. ومن المبادئ العامة المستقرة في تفسير القانون الجنائي أنه لا يجوز تقييد النص المطلق، أو تخصيص النص العام، إلا إذا وجد نص يجيز ذلك.

ولا يوجد في هذه الحالة نص خاص يقيد إطلاق النص أو يخصص عمومه، ولذلك فإن عدم ذكر المشرع لشرط الحماية الفنية يعني أن المشرع أراد استبعاده. هذا بالإضافة إلى أن الحماية الجزائية يجب أن تمتد لتغطي كل أنظمة المعالجة الآلية للمعطيات سواء كانت تتمتع بحماية فنية أم لا.

وتطبيقا لذلك، فإنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا بوجود حماية فنية ولكن إذا نظرنا للوقائع، نلاحظ أن غالبية أنظمة المعالجة الآلية للمعطيات تتمتع بنظام حماية فنية، بالإضافة إلى أن وجود مثل تلك الحماية يساعد على إثبات أركان الجريمة وبصفة خاصة الركن المعنوي. (القهوجي، 1999، صفحة 123)

4. خاتمة:

نصل في الختام إلى أن الجرائم الواقعة على التجارة الإلكترونية، وإن كانت في ظاهرها تنصب على التجارة، مثلها مثل الجرائم الواقعة على التجارة بمعناها الضيق، إلا أنها أشمل من ذلك، باعتبارها تهدف أيضا إلى هدر الطريق الذي تتم بواسطته هذه التجارة، ودليل ذلك الجرائم الواقعة على مواقع التجارة الإلكترونية.

ومن أجل مواجهة كل تلك الجرائم، تبقى أدوات الرقابة على التجارة الإلكترونية من أحسن السبل، ويتجلى ذلك عن طريق تقوية سبل الأمن الإلكتروني، ومن بينها وسيلة التشفير الإلكتروني. وأمام هذه

الأخيرة وباعتبارها متعلقة برموز خاصة، فإنه يستعصي على أي كان التوصل إلى المعلومات، دون التزود المسبق بالمفتاح.

إلا أنه ككل الآليات المعتمدة بغرض ضمان الأمن الإلكتروني عموما أو الأمن في مجال التجارة الإلكترونية خصوصا، يجب على التشفير أن يستعمل وفق معايير موضوعية، وذلك حتى لا نتواجد أمام التشفير الماس باستخدام تقنيات أخرى، وأيضا إمكانية المساس ببعض الحريات، ومن بينها حرية العملاء والزبائن في الاطلاع على المعلومات المتعلقة بالتجارة الإلكترونية.

المراجع باللغة العربية

المؤلفات:

-آمال، قارة .(2007) .*الحماية الجزائية للمعلوماتية في التشريع الجزائري* .الجزائر :دار هومة ، الطبعة الثانية

-شريف، غنام. (2008). *التنظيم القانوني للاعلانات التجارية عبر شبكة الأنترنت*. مصر: دارالجامعة الجديدة.

-عبد القادر، القهوجي. (1999). *الحماية الجنائية لبرامج الحاسوب*. مصر: الدار الجامعية الجديدة.

-عفيفي، كامل عفيفي. (2003). *جرائم الكمبيوتر، دراسة مقارنة*. لبنان: منشورات الحلبي الحقوقية.

-قرشوش، هدى .(2007) .*شرح قانون العقوبات، القسم الخاص* .مصر :دار النهضة العربية.

-مجاهد، أسامة أبو الحسن. (2003). *خصوصية العقد عبر التعاقد*. مصر، القاهرة: دار النهضة العربية.

-نائلة، عادل قور. (2005). *جرائم الحاسب الآلي الاقتصادية*. لبنان: منشورات الحلبي الحقوقية.

الرسائل:

-أحمد مسعود مريم .(2013) .آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم .04-09*رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة ورقلة.*

-جوهر بن رجدال. (2002، ص82). الأنترنت والتجارة الإلكترونية. *مذكرة ماجستير، جامعة الجزائر، .*

-رقية حواس. (2015). العقد الإلكتروني. *رسالة التخرج المعهد العالي للتسيير والتخطيط*، 14.

-لونيس نادية(2011) .، ص .(100اثر تكنولوجيا المعلومات والاتصالات في تفعيل الأعمال التجارية للمؤسسات .*مذكرة لنيل شهادة ماجستير في العلوم التجارية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر3.*

المقالات:

-سامية ايت مبارك. (العدد33, 2016). التجارة الإلكترونية بالجزائر في ظل تطور استخدام تكنولوجيا المعلومات والاتصال. *مجلة علوم الاقتصاد والتسيير والتجارة*، صفحة 31.

-عباوي نجاة (2017) .، جانفي ، العدد .(16الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات .*دفاتر السياسة والقانون.*

المداخلات:

-ابراهيم خالد ممدوح. (2008). التحكيم الإلكتروني في عقود الاستثمار الدولية. *النظم القانونية للتجارة الإلكترونية*، (صفحة 104).

-فشار عطاء الله .(أكتوبر 2009)التزوير المعلوماتي .*الملتقة المغاربي حول القانون والمعلوماتية .* ليبيا :أكاديمية الدراسات العليا بليبيا.

المراجع باللغة الفرنسية:

MAGNIER-MERRAN, kevin. (2019, juin 19). Obs cass. com. n°18-12.292. *AJ Contrat*, p. 1394.

LARRIEU, Jacques. (2019). *Droit du numérique.* Recueil Dalloz.