جـــــــامعة يـــــحي فـــــارس بالمدية

كليـــــة الحقوق والعلوم السياسية

العنوان

الاحتيال في التجارة الإلكترونية

مذكرة مقدمة لنيل شهادة ماستر في الحقوق

تخصص: قانون أعمال

من إعداد الطالبتين:

- هامل حنان
- محمدي حياة

تحت إشراف الأستاذ:

د/ فخار هشام

لجنة المناقشة:

الاسم واللقب	المؤسسة الأصلية	الدرجة العلمية	الصفة
د. سبتي عبد القادر	جامعة المدية		رئيسا
د. فخار هشام	جامعة المدية		مشرف
د. طنجاوي مراد	جامعة المدية		مناقشا

السنة الدراسية: 2025/2024م


بسم الله الرحمن الرحيم

شكر وتقدير



أولا وقبل كل شيء نشكر الله جل جلاله، ونحمده حمدا دائما الذي وفقنا ويسر لنا الأمور في انجاز مذكرتنا .

لنتقدم بعدها بالشكر و التقدير مع فائق الاحترام الى أستاذنا الفاضل الدكتور

"فخار هشام "

حفظه الله تعالى، الذي قبل وتكرم بالإشراف على مذكرتنا، وعلى ما قدمه لنا من توجيهات ونصائح قيمة، الذي خصص لنا من وقته الثمين، برغم من انشغالاته، فجزاه الله خير الجزاء في الدّارين دنيا والآخرة .

كما نشكر السادة ألأفاضل أعضاء اللجنة على قبولهم وتفضلهم بمناقشة هذه المذكرة، ورغبتهم في إبداء نصائحهم و تقييمهم لمذكرتنا .

كما نتقدم بالشكر الخالص الى كل من ساعدنا من قريب أو بعيد في انجاز هذه المذكرة .

وأخيرا نتقدم بالشكر للقائمين على جامعة المدية التي آوتنا كطلبة وبالأخص كلية الحقوق والعلوم السياسية، التي تشرفنا بالانتساب اليها .

الاهداء

الحمد الله حمدًا طيبًا مباركًا فيه، الحمد الله الذي وفقني لإتمام هذا العمل المتواضع وسدّد خطاي في طريق البحث والعلم، فله الحمدُ أولا و آخرًا .

إلى من غرست في قلبي حب العلم وسقتني من حنانها ما يكفي لعمر كامل، إلى روحك الطاهرة يا جدّتي أهدي هذا العمل عربون وفاء ودعاء لا ينقطع .

إلى من تحملت وصبرت وسهرت من أجلي اللّيالي، إلى من كانت دعواتها سرًا في كل نجاح إلى أمي الصبورة أطال الله في عمرها.

إلى السند والقوة، من علمني أن لا مستحيل مع الإصرار إلى أبي الغالي أطال الله في عمره.

إلى ركائزي وأحبتي وفرحتي إخوتي عماد ومريم وعمر .

إلى عمي العزيز، صاحب القلب الكبير والمواقف الأصيلة أهديك هذا العمل المتواضع عرفانًا لكلماتك الداعمة .

إلى زوجة خالي العزيزة، صاحبة القلب الطيب والروح الداعمة التي لم تبخل يوما بكلمة طيبة أو نصيحة صادقة، أهديك هذا النجاح .

إلى بنات خالي رفيقات دربي، مايسة وهديل .

إلى عائلة هامل ورحماني أهديكم هذا العمل المتواضع تقديرا لمحبتكم واعترافًا بفضلكم .

إلى تلك الراحلة الباقية في قلبي صديقتي الغالية "إيمان غيدي" رحمها الله .

إلى رفيقات الحياة الجامعية كل واحدة باسمها، وإلى كل من أحبهم قلبي .

حنان

الاهداء

حمد لله أولًا، الذي لولاه ما وصلت، وما صبرت، وما حققت هذا الإنجاز

إلى نفسي...

التي تعبت، صبرت، وسارت في طريق لم يكن سهلًا

أهديك هذا النجاح لأنكِ تستحقينه،

لأنكِ كنتِ دائمًا القوّة رغم كل شيء

وإلى أمي الحبيبة نبض الحنان الأول، وجوهرة العمر، التي كانت ولا تزال نور طريقي، ودعاؤها ركن قوتي... حفظكِ الله وأدامكِ سندًا لا يميل.

وإلى أمي الثانية، مربّيتي العزيزة، التي غرست فيّ القيم، وربّتني بحب يشبه حنان الأرض، فكانت لي أمًا بكل ما تحمله الكلمة من معنى... حفظكِ الله وأطال في عمرك.

إلى أبي الغالي الرجل الذي أفتخر بحمل اسمه، رجل المواقف الصعبة، وملهم الثقة والطمأنينة، فخرٌ لي أنني ابنتك... حفظك الله وبارك فيك.

إلى روحيْن لا يغيبان عن قلبي

إلى جدي العزيز، وجدتي الحنونة، كنتما الأمان الأول، والظل الذي احتميت به حين كان حضنكما هو العالم الوحيد الذي أفهمه، رحمكما الله وغفر لكما، وجعل الجنة مثواكما

وإلى أخواتي الغاليات : شيماء، آية و فرح، زهور بيتي، صديقات وأمان روحي، وفرحي في كل نجاح، وإلى أخي الصغير زهير، كنتم الدفء الذي رافقني، محبتي لكم لا تقاس، جعل الله أيامكم فرحًا دائمًا، وقلوبكم لا تعرف إلا السلام

ولكل من شاركني هذه الرحلة، وأثروا حياتي بلمساتهم الطيبة

أهديكم هذا العمل عربون وفاء وامتنان، محفور في القلب والذاكرة.

حياة

مـــــــقدمة

مقدمة

يعيش العالم اليوم مرحلة من التحولات السريعة والتطورات المتلاحقة خاصة في مجالات تكنولوجيا المعلومات والاتصالات والتي أصبحت تعرف بثورة المعلومات، وقد أثر هذا التطور بشكل مباشر على حياة الأفراد و المجتمعات، إذ قرّب المسافات وغير أساليب التواصل وسهل المعاملات بفضل استخدام الأجهزة الذكية المرتبطة بشبكة الأنترنت .

ومن أبرز ما أفرزته هذه الثورة هو مفهوم التجارة الإلكترونية الذي شكل نقلة نوعية في مجال المعاملات التجارية، فقد أصبح بإمكان الافراد والمؤسسات ابرام الصفقات وتبادل السلع والخدمات عن بعد، دون الحاجة إلى التقاء الأطراف مما ساهم في تسريع حركة الاقتصاد، وتوسيع الأسواق على الصعيدين المحلي والدولي .

وتتميز التجارة الإلكترونية بعدّة خصائص تجعلها مختلفة عن التجارة التقليدية، أبرزها :

- غياب التعامل الورقي في التجارة الالكترونية.

- الطابع العالمي للتجارة الإلكترونية .

-سرعة تغيير المفاهيم والأنشطة في التجارة الالكترونية .

لكن هذا التطور لم يأتي دون ثمن، فقد فتح بابًا واسعاً أمام ظواهر احتيالية مستحدثة، اتخذت من الفضاء الالكتروني ساحة لها ومن ثقة المستهلكين نقطة انطلاقها .

ولقد أصبح الاحتيال في التجارة الالكترونية واحدا من أبرز التحديات التي تهدد أمن التعاملات الرقمية، وتؤثر سلبا على مصداقية الأسواق الافتراضية، بل وتمس بثقة الافراد في التكنولوجيا ذاتها، فرغم ما تحققه التجارة الالكترونية من سهولة وسرعة في الأداء إلى أنها في غياب رقابة صارمة ووعي كاف قد تتحول إلى ساحة فوضى، يستغل فيها الجهل والثقة على حد سواء .

وفي ظل هذه التحديات جاءت جهود المشرّع الجزائري لمواكبة التطورات الرقمية، من خلال إصدار القانون رقم 18-05 المؤرخ في 10 ماي 2018 المتعلق بالتجارة الإلكترونية، وكذا تعديل بعض أحكام قانون العقوبات للتصدي لأشكال الاحتيال المستحدثة عبر الوسائل الإلكترونية .

تنبع أهمية دراسة موضوع الاحتيال في التجارة الإلكترونية من الواقع المعاصر الذي يشهد توسعاً متزايدًا في استخدام الفضاء الرقمي لإبرام وتنفيذ المعاملات التجارية، كما أن معالجة هذا الموضوع تساهم في تحليل مدى فعالية الإطار القانوني الجزائري في مواجهة هذه الظاهرة، وتبيان النقائص التي تعتريه .

كما تتمثل أهمية دراسة هذا الموضوع أيضا بارتباطه الوثيق بواقع المجتمع الجزائري، الذي يشهد توسعا ملحوظا في استخدام الأنترنت في المعاملات اليومية لاسيما بعد جائحة كوفيد-19 .

حيث ترجع أسباب اختيار الموضوع إلى أسباب ذاتية وأخرى موضوعية فالأولى مردها الرغبة والميول لدراسة هذا الموضوع نظرا لما له من صلة بالتجارة الإلكترونية إذ يعتبر من الموضوعات المستجدة في تخصص قانون الأعمال .

أما الثانية تتمثل في حداثة الموضوع، حيث شهدت التجارة الإلكترونية في السنوات الأخيرة انتشارًا واسعًا وما رافقته من تزايد حالات الاحتيال التي باتت تُهدد أمن المعاملات الرقمية .

من خلال الاطلاع على الدراسات السابقة ،تبيّن وجود بعض الأعمال الأكاديمية التي تتقاطع مع موضوع بحثنا مما يعكس أهمية الموضوع في الساحة البحثية ونذكر منها :

حطاب كمال، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم الجنائية .

بوصيد أحسن، واقع ومستقبل التجارة الإلكترونية في الجزائر، مذكرة لنيل شهادة الماستر تخصص مالية وتجارة دولية .

ومن خلال ما سبق التطرق إليه، نطرح الإشكالية التالية :

ما مدى فعالية الإطار القانوني الجزائري في التصدي لظاهرة الاحتيال في التجارة الإلكترونية وحماية المستهلك الإلكتروني ؟

أما الصعوبات التي سيجدها أي باحث عن محاولته التطرق إلى مثل هذه المواضيع هو عدم تمكنه من استيعاب مجال الدراسة، فالأمر لا يتوقف عند قانون معين بل سيجد نفسه يبحث في مختلف القوانين والمراسيم و القرارات التي قد تعالج مسألة معينة قد تكون مرتبطة بالموضوع ارتباطًا وثيقًا .

وللإجابة على هذه الإشكالية المطروحة وبغية الإلمام والإحاطة بمختلف جوانب هذا الموضوع والوصول الى النتائج المرجوة، تم الاعتماد على المنهج الوصفي التحليلي الذي يقوم على تحديد

خصائص التجارة الإلكترونية، وبيان طبيعتها ومميزاتها التي تُشكل بيئة خصبة لظهور سلوكيات احتيالية مستحدثة، ثم التطرق لمختلف أشكال وأساليب الاحتيال في هذا المجال، إضافة إلى أركان الجريمة الاحتيالية الإلكترونية وشروط قيامها، كما تم تسليط الضوء على موقع المشرع الجزائري من هذه الجريمة من خلال دراسة الأساس القانوني لتجريمها، والنصوص المعتمدة في مواجهتها، وقد مكّن هذا المنهج من الوصول إلى نتائج دقيقة تُسهم في فهم الإطار القانوني لجريمة الاحتيال في التجارة الإلكترونية وتحديد سبل مكافحتها بفعالية .

سنقوم بدراسة هذا الموضوع بتقسيمه إلى فصلين، حيث سنتطرق في الفصل الأول إلى الإطار المفاهيمي للتجارة الإلكترونية والذي قسمناه بدوره إلى مبحثين منفصلين، الأول يتعلق بمدلول الاحتيال في التجارة الإلكترونية والثاني يتعلق بالإطار القانوني لتجريم الاحتيال في التجارة الإلكترونية .

أما الفصل الثاني فقد خصصناه لحماية التجارة الإلكترونية من جريمة الاحتيال الإلكتروني، حيث تناولنا في المبحث الأول الإجراءات الوقائية من الاحتيال في التجارة الإلكترونية، والمبحث الثاني تضمن الإجراءات الردعية للاحتيال في التجارة الإلكترونية .

وفي الأخير انتهينا بخاتمة تضمنت أهم النتائج المتوصل إليها من خلال هذه الدراسة وقدمنا بعض الاقتراحات .

الفصـــل الأول:

الاطار المفاهيمي للاحتيال في التجارة الالكترونية

الفصل الاول: الاطار المفاهيمي للاحتيال في التجارة الإلكترونية

شهد العالم في العقود الأخيرة تحولا جذريا في أساليب التجارة، حيث أصبحت التجارة الإلكترونية أحد أبرز مظاهر التطور التكنولوجي والاقتصادي ومع انتشار الأنترنيت الواسع واعتماد التقنيات الرقمية، لم يعد البيع والشراء مقتصرين على الأسواق التقليدية، بل امتد ليشمل منصات إلكترونية تنتج التعاملات التجارية بسهولة .

كما نرى اليوم أن التجارة الإلكترونية تمثل أحد أسس الاقتصاد الرقمي نظرا للتزايد الكبير في الاعتماد عليها، وقد ساعدت التطورات التقنية في تحسين بيئة التجارة الإلكترونية وجعلها أكثر أمانا.

حيث سنتطرق في هذا الفصل على مفهوم التجارة الإلكترونية من خلال المباحث التالية:

المبحث الأول: مدلول الاحتيال في التجارة الإلكترونية

المبحث الثاني: الإطار القانوني لتجريم الاحتيال في التجارة الإلكترونية

المبحث الأول: مفهوم الاحتيال في التجارة الإلكترونية

في عصر التحول الرقمي والتطور التكنولوجي السريع أصبحت التجارة الإلكترونية واحدة من أهم الوسائل الحديثة لممارسة الأنشطة التجارية فقد غيرت طريقة البيع والشراء وجعلت الأسواق أكثر انفتاحا وسهولة في الوصول، مما أتاح للأفراد والشركات فرصا غير مسبوقة للنمو والتوسع .

وعليه للتفصيل في الموضوع نتناول مدلول التجارة الإلكترونية (المطلب الأول) المقصود بالاحتيال في التجارة الإلكترونية (المطلب الثاني) .

المطلب الأول: مدلول التجارة الإلكترونية

إن الوصول إلى مفهوم محدد وشامل للتجارة الإلكترونية ليس أمرا سهلا لأن ذلك يتطلب إلماما كبيرا بالعناصر التي تتضمنها والخصائص التي تتمتع بها وآلية عملها وتطبيقها القانوني، وإذا كان العديد من الناس يعتقدون أن التجارة الإلكترونية تتمثل في إنشاء موقع على شبكة الانترنيت والتعامل من خلاله مع الزائرين لهذا الموقع بعمليات البيع والشراء الإلكتروني إلا أن حقيقة هذا المفهوم البسيط للتجارة الإلكترونية تعبر عن أحد أشكالها وهنا ينبغي علينا عدم الخلط بين تعريف التجارة الإلكترونية وأشكالها.[1]

سنتطرق في هذا الصدد الى كل من تعريف التجارة الإلكترونية (الفرع الأول)، خصائصها وأهميتها (الفرع الثاني).

الفرع الأول: تعريف التجارة الإلكترونية

تعددت الجهات والمنظمات الدولية في تعريف التجارة الإلكترونية لعدم وجود تعريف موحد لها كمنظمة التجارة العالمية، وحسب البنك الدولي، الإتحاد الأوروبي، منتدى التعاون الاقتصادي لآسيا والمحيط الهادي وتعريف القانون رقم 18-05 المتعلق بالتجارة الإلكترونية .

أولا- حسب منظمة التجارة العالمية: "أنشطة إنتاج السلع والخدمات وتوزيعها وتسويقها وبيعها أو تسليمها للمشتري من خلال الوسائط الإلكترونية". [2]

[1] محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الالكترونية، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، دمشق، سوريا،2009، ص29 .

[2] ابراهيم العيسوي، التجارة الالكترونية، الطبعة الأولى، المكتبة الاكاديمية، الإسكندرية ,مصر، 2003، ص11.

ثانيا- حسب البنك الدولي: "إستخدام شبكة الحاسبة لتسهيل المعاملات الخاصة بالإنتاج والتوزيع والبيع والإعلان عن بيع السلع والخدمات ".[1]

ثالثا- الإتحاد الأوروبي: عرف التجارة الإلكترونية بأنها كل الأنشطة التي تتم بوسائل الكترونية سواء تمت بين المشروعات التجارية والمستهلكين، أو بين كل منها على حدى وبين الإدارات الحكومية كذلك تسليم السلع أو الخدمات بشكل مادي أو معنوي (برامج الكومبيوتر، مجلات إلكترونية مثلا).[2]

رابعا- منتدى التعاون الاقتصادي لأسيا والمحيط الهادي: عرفها منتدى التجارة الإلكترونية بأنها أي شكل من أشكال صفقات التجارة الخدمية والسلعية التي يتعامل فيها الأطراف بطريقة إلكترونية سواء بين شخص وشخص آخر أو بين شخص وكومبيوتر أو بين كومبيوتر وكومبيوتر . [3]

خامسا- القانون رقم 18-05 المتعلق بالتجارة الإلكترونية هي النشاط التي يقوم بموجبه مورد إلكتروني باقتراح أو ضمان، توفير سلع وخدمات عن بعد لمستهلك إلكتروني عن طريق الاتصالات الإلكترونية . [4]

ويرى البعض بأن تعريف التجارة الإلكترونية ينطوي على أي نوع من أشكال التعاملات التجارية التي تتم إلكترونيا عبر شبكة المعلومات الدولية (الأنترنت)، وتتم هذه التعاملات بين الشركات أو بين الشركات وعملائها أو بين الشركات والحكومات، كما تشمل التجارة الخارجية والتجارة الداخلية، ويمكن للتجارة الإلكترونية أن تقوم بوظائف جديدة في عمليات التبادل التجاري من بينها الإعلان والتسويق والمفاوضات وتسوية المدفوعات والحسابات وفتح الامتيازات والتراخيص وإعفاء أوامر البيع والشراء والتبادل لبعض السلع والخدمات .[5]

ونلاحظ من التعاريف السابقة أن:

1-التجارة الإلكترونية لا يمكن تصورها بدون وسائل إلكترونية .

---

[1] عبد الباقي حياة، عبدوس عبد العزيز،(آليات التصدي للجرائم المعلوماتية الواقعة على التجارة الالكترونية)، مجلة البصائر للدراسات القانونية الاقتصادية، جامعة بلحاج بوشعيب عين تموشنت، الجزائر، العدد1، المجلد1، مارس2021، ص132.

[2] علاوة محمد لحسن، مولاي لخضرعبدالرزاق، مداخلة بعنوان: (آليات التجارة الالكترونية كآداة لتفعيل التجارة العربية البينية)، الملتقى الرابع، عصرنة نظام الدفع في البنوك الجزائرية واشكالية اعتمادها في الجزائر،جامعة قاصدي مرباح ورقلة، الجزائر , ص9.

[3] المرجع نفسه، ص 5

[4] المادة 6 من القانون رقم 18-05، المؤرخ في 24شعبان 1439 الموافق ل10 مايو 2018، يتضمن التجارة الإلكترونية، الجريدة الرسمية الجمهورية الجزائرية، العدد 28.

[5] عصام عبد الفتاح مطر،التجارة الإلكترونية في التشريعات العربية والأجنبية، د.ط، دار الجامعة الجديدة، الإسكندرية، مصر،2015، ص16.

2-أن التجارة الإلكترونية لا تخص فقط عملية البيع والشراء إنما تشمل عمليات تصميم وإنتاج وعرض وتوزيع وبيع السلع والخدمات، وتسوية عمليات الدفع والسداد .
3-أن التجارة الإلكترونية مثل أي نشاط تقليدي يمكن أن تتم داخليا أو خارجيا .

الفرع الثاني: خصائص التجارة الإلكترونية وأهميتها

تعد التجارة الالكترونية من أبرز مظاهر التحول الرقمي في العصر الحديث ،إذ تتميّز بالسرعة والمرونة وتتجاوز القيود الجغرافية ،كما تكمن أهميتها في تحقيق فوائد محليا ودوليا وبالنسبة للمستهلك

1.خصائص التجارة الإلكترونية

تتميز التجارة الإلكترونية بعدة خصائص تجعلها مختلفة عن التجارة التقليدية، ويمكن ابرازها في كل من الطابع العالمي للتجارة الإلكترونية (أولا) الطابع المتداخل في التجارة الإلكترونية (ثانيا) غياب التعامل الورقي في المعاملات التجارية (ثالثا) عدم الكشف عن هوية المتعاملين (رابعا) سرعة تغيير المفاهيم والأنشطة في التجارة الإلكترونية (خامسا).

اولا: الطابع العالمي للتجارة الإلكترونية

فالتجارة الإلكترونية أو بالأحرى الوسائط الإلكترونية التي يجري من خلالها أنشطة التجارة الالكترونية، لاسيما الانترنيت لا تعرف الحدود المكانية او الجغرافية، ومن ثم فإن اي نشاط تجاري يقدم سلعا أو خدمات على الانترنت لا يحتاج الى التوجه الى منطقة جغرافية بعينها . [1]

كما يستطيع المستهلك ان يتجول في الأسواق الإلكترونية بكل حرية مع توفر كم هائل من المعلومات (كالمواصفات والاسعار) عن السلع المطلوبة .

ثانيا: الطابع المتداخل في التجارة الإلكترونية

إن الفوارق في توزيع الوسائل المادية بين المؤسسات سواء كانت هذه المؤسسات كبيرة أو صغيرة في التجارة الالكترونية أقل وضوحا وحدة، فأصبح بالإمكان تسليم السلع والخدمات بالطريقتين التقليدية أو بطريقة الكترونية مباشرة على الانترنت مثل الموسيقى والأقراص المدمجة، وأفلام الفيديو والأقراص التي تحتوي على برامج الكومبيوتر أو المعلومات، وهذا ما يخلق صعوبة فرض الضريبة على المنتج إذا ما كان سلعة أو خدمة وهذا يجبر المؤسسات على إعادة هيكلة نفسها لمواجهة التغيرات التي تفرضها ممارسة التجارة الإلكترونية . [2]

[1] إبراهيم العيسوي، المرجع السابق، ص31.
[2] محمد سعيد احمد إسماعيل، المرجع السابق، ص 66.

ثالثا: غياب التعامل الورقي في المعاملات التجارية

يطلق بعض الفقهاء الامريكيين على التجارة الالكترونية ونظام التبادل الالكتروني للبيانات تعبيرا بديل هو التجارة الإلكترونية اللاورقية وقد أصبح هذا المصطلح شائعا في تشريعات التجارة الإلكترونية، وهناك العديد من الفوائد التي نجنيها من غياب المستندات الورقية المادية، وأهمها:

أ-خفض التكاليف الناتجة عن إنشاء ومعالجة وتوزيع وحفظ واسترجاع المعلومات الورقية، حيث قدرت تكلفة انتاج ومعالجة الاوراق في الصفقات التجارية ب 10بالمائة من قيمة المنتجات والبضائع .

ب-الأتمتة الكاملة للصفقات التجارية التي يمكن أن تشمل الايجاب والقبول والتعاقد والدفع والتسليم وغيرها .[1]

رابعا: عدم الكشف عن هوية المتعاملين

إن التعاملات التجارية تتم بين أطراف قد يفصل بينهما آلاف الأميال كما يختلف التوقيت الزمني بينهم، وبالتالي غياب المعلومات الكافية عن المتعاملين بين بعضهم قد يخلق سلبيات كتقديم معلومات زائفة او تقديم بطاقات ائتمان مسروقة أو اساءة استخدام المعلومات أثناء التعامل وهذا ما يثير مسألة الخصوصية وسرية المعلومات [2]،ولكن هذا التطور التكنولوجي المستمر سيساهم بلا شك في تعزيز الامان والموثوقية، مما يضمن مصداقية التعاملات التجارية عبر الانترنيت .

خامسا: سرعة تغيير المفاهيم والانشطة في التجارة الإلكترونية

نلاحظ أن هناك تغييرات متسارعة في نوعية الأنشطة التي تندرج تحت مفهوم التجارة الإلكترونية، وثمة احتمالات ضخمة لاتساع نطاق هذه الانشطة ومن جهة اخرى فإن ارتباط التجارة الإلكترونية بوسائط الاتصال الإلكتروني بصفة خاصة [3] ومجالات الاتصالات والمعلومات بصفة عامة وهي جميعا تتعرض لتغيرات تكنولوجية متسارعة يجعل النظم التي تخضع لها التجارة الإلكترونية عرضة هي الأخرى للتغيير السريع .

[1] محمد سعيد أحمد إسماعيل، المرجع السابق، ص 67.
[2] صراع كريمة، واقع وآفاق التجارة الالكترونية في الجزائر، مذكرة نيل شهادة الماجستر، تخصص استراتيجية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، الجزائر،2013-2014، ص32.
[3] إبراهيم العيسوي، المرجع السابق، ص32 .

2-أهمية التجارة الالكترونية

تكمن أهمية التجارة الالكترونية في الفوائد التي تحققها على كافة المستويات ،فهي تحقق فوائد على المستوى المحلي والدولي ،وبالنسبة كذلك للمستهلك

أولا: أهميتها على المستوي المحلي

تتيح التجارة الالكترونية فتح أسواق جديدة للمنتجات المحلية ،تعمل على تسويق السلع والخدمات عالميا ،إذ تستطيع كل شركة وطنية متخذة موقع على شبكة الأنترنت أن تروج لمنتجاتها وتوزعها على كافة دول العالم ،مما يعور بالنفع على الدولة والاقتصاد المحلي .

كما أن التجارة الإلكترونية تؤدي إلى انشاء مشاريع متوسطة وصغيرة ودخولها هذا المجال مما يعود بالنفع على الاقتصاد العام الوطني ،كما تؤدي التجارة الإلكترونية إلى رفع مستوى الكفاءة و الإنتاجية من خلال عملها على تلاقي عدد كبير من الموردين والمشترين وكذلك تحقق وفرة هامة /تنتج من عدم حاجته إلى إقامة مشاريع فخمة بأقل التكاليف ،وبالتالي فإن التجارة الالكترونية تحقق تسويقا أكثر فعالية وأسرع وصولا للعملاء .[1]

ثانيا: أهميتها على المستوى الدولي

تعمل التجارة الالكترونية على تحرير التجارة والذي هي من أهم أهداف التجارة العالمية ،فهي تدعو الدول الأعضاء بها بإتباع التجارة الالكترونية ،كما تعمل التجارة على انفتاح الدول وتبادل الخبرات والثقافات التكنولوجية ،وثقافات التسويق للمنتجات مما بؤدي إلى دعم العلاقات بين الدول .

كما تساهم التجارة الإلكترونية في زيادة الإنتاج والتسويق والمبيعات والتنوع في السوق العالمية ،لتقديم أفضل المنتجات والخدمات بما يتلاءم مع طبيعة الأسواق الجديدة فكانت الحاجة إلى إيجاد أسواق جديدة ،بحيث استحوذت هذه التجارة على الاهتمام العالمي وخاصة من قبل الشركات العالمية الكبرى ،التي وجدت فيه مجالا خصبا لاختراق الأسواق الدولية متجاوزة بذلك الحدود الزمانية والمكانية .[2]

ثالثا: أهميتها بالنسبة للمستهلك

بالرغم من تحمله التجارة من بعض المخاطر ،إلا أنه تحقق فوائد عديدة للمستهلك فليس على المستهلك إلا الدخول على المواقع التجارية الإلكترونية وفي ظرف قياسي يمكنه التسوق عبر الويب ،مما يمكنه من

[1] محمد مدحت عزمي ،المعاملات التجارية الإلكترونية ،مركز الكتاب ،الإسكندرية ،مصر،2008 ،ص43.
[2] محمد سعيد أحمد إسماعيل، المرجع السابق ،ص27 .

التعاقد لاقتناء أي منتج أو خدمة وكذا يمكنه من تسلمها إلكترونيا ،وعلى ذلك يتضح أن التجارة تمنح للمستهلك بدلائل كثيرة للاختيار من بينها اختيار أوسع للسلع والخدمات ،كما يمكن أن يتعاقد مع شركات دولية لا يمكنه أن ستوصل إليها إلا عن طريق التجارة الإلكترونية .[1]

المطلب الثاني: المقصود بالاحتيال في التجارة الإلكترونية

تعتبر التجارة الإلكترونية كغيرها من العمليات الإلكترونية التي شهدت العديد من العراقيل التي تعرقل سيرها، ويعتبر الاحتيال من أهم الجرائم التي تعترض العملية وتهدد امن المعاملات التجارية وثقة المستخدمين لذا أصبح من الضروري تطوير وسائل أمان وفعالة واعتماد تقنيات متقدمة للحماية من هذه التهديدات .

في هذا المطلب سنتناول مفهوم الاحتيال في التجارة الإلكترونية (الفرع الاول) وأنواع الاحتيال في التجارة الإلكترونية (الفرع الثاني).

الفرع الاول: مفهوم الاحتيال في التجارة الإلكترونية

لتحديد مفهوم جريمة الاحتيال الإلكتروني، لابد أولا من تناول الاحتيال بصورته العامة .

1-تعريف الاحتيال الإلكتروني

أ- لغة: الاحتيال هو الحذق، وجودة النظر والقدرة على دقة التصرف[2]، والاحتيال والمحاولة: مطالبتك بالشيء بالحيلة، والحيلة هي المكر والخديعة والكيد لكل فعل يقصد فاعله به خلاف ما يقتضيه ظاهره[3] .

ب-اصطلاحا: اختلف الفقهاء في الوصول الى تعريف محدد لتعريف جريمة الاحتيال الإلكتروني لاختلافهم في الزاوية التي ينظر اليها منه، ومن تعريفاته الاصطلاحية نتناول على سبيل المثال:

جريمة الاحتيال هي الاستيلاء على الحيازة الكاملة لمال الغير بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال، وعرفها آخر بأنها استعمال وسيلة من وسائل التدليس التي نص عليها القانون على سبيل الحصر لحمل المجني عليه على تسليم الجاني مالا مملوكا لغيره نتيجة الوقوع في الغلط .[1]

---

[1] أحمد مداح ،التجارة الإلكترونية من المنظور الفقهي الإسلامي ،مذكرة لنيل شهادة ماجستير في الفقه وأصوله ،جامعة احاج لخضر ،باتنة ،الجزائر ،2005_2006، ص30.

[2] هيثم حمود الشلبي، إدارة مخاطر الاحتيال في قطاع الاتصالات، دار صفاء للنشر والتوزيع، طبعة 1، عمان، الأردن، 2009، ص 22 .

[3] عبيد علي، ناصر موفق وآخرون، (ماهية جريمة الاحتيال الالكتروني)، مجلة كلية القانون للعلوم القانونية والسياسية، كلية الحقوق، جامعة تكريت، بغداد، العراق، ص338.

اختلفت التشريعات القانونية في تحديد ماهية هذه الجريمة، ففي القانون الفرنسي وردت لأول مرة بصياغة دقيقة ضمن نص المادة 405 التي نصت على انه "كل من يتوصل الى أن يسلب او يشرع في سلب مال أو بعض ثروة الغير، وأضاف ظرفا مشددًا لجريمة الاحتيال والشروع فيها يتحقق عندما ترتكب أما بانتحال صفة ضابط في الشرطة القضائية، أو مأمور الضبط في دائرة الدولة المدنية أو في الجيش الفرنسي الأجنبي .[2]

أما المشرع الجزائري تناول جريمة الاحتيال في قانون العقوبات ونص في المادة 372 على أنها "كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو إلى الحصول على أي منها أو شرع في ذلك وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة من 500 إلى 20.000 دينار" .[3]

ويمكن القول بصفة عامة انه لا يوجد تعريف جامع ومانع لجريمة الاحتيال الإلكتروني يمكن الرجوع إليه، فقد تعددت التعاريف التي تناولت الاحتيال الإلكتروني او كما يسمى بالاحتيال المعلوماتي واختلفت فيما بينها من حيث العناصر التي ينبغي توافرها لتحقيقه، ولقد توسعت غالبية التعريفات في مفهوم الاحتيال المعلوماتي حيث تربط بين الاستخدام غير المشروع للحاسبات الآلية لتحقيق ربح مادي غير مشروع بصفة عامة وبين الاحتيال الإلكتروني .

الفرع الثاني: أشكال وأساليب الاحتيال في التجارة الإلكترونية

أولا: أشكال الاحتيال في التجارة الإلكترونية

يأخذ الاحتيال في التجارة الإلكترونية عدة أشكال، تختلف باختلاف الأطراف المتورطة والأهداف المرجوة، والوسائل المستخدمة حيث يمكن أن يصدر من البائع أو المشتري، وقد يكون من طرف ثالث خارجي، من أشكال الاحتيال، نرى:

---

[1] عبيد علي ،المرجع السابق، ص 338.

[2] بولحية شهيرة، (الاحتيال الالكتروني)، مجلسة الدراسات القانونية والاقتصادية، المركز الجامعي سي الحواس بريكة، باتنة،الجزائر, العدد4، ديسمبر 2019، ص38.

[3] المادة 372، الأمر رقم 56-156، المؤرخ في 18صفر 1386، الموافق ل 8يونيو 1966، الذي يتضمن قانون العقوبات المعدل والمتمم .

***الاحتيال باستخدام بطاقات الدفع الإلكتروني**

انتشرت بطاقات الدفع الالكتروني في كافة أنحاء العالم ودخلت في كل الأنظمة النقدية، نظرا للتيسيرات التي تمنحها لحاملها ليتمكن من شراء أي سلعة أو منتج من أي مكان في العالم، وكان من الطبيعي أن تظهر أشكال إجرامية جديدة اتخذت من بيئة الدفع الإلكتروني وسطا لتنمو فيه وتزدهر، فقد اتخذت صور من أهمها: الاحتيال بالبطاقة الائتمانية من قبل الحامل الشرعي لها أو من قبل الغير .

1-الاحتيال في استعمال البطاقة من قبل حاملها:

ومن صورها استعمال البطاقة بعد انتهائها، واستعمالها رغم الغائها، وتجاوز حد السحب

أ-استعمال البطاقة بعد انتهاء مدة صلاحيتها

ينص العقد المبرم بين العميل والبنك على ان يسلم العميل البطاقة للبنك بعد انتهاء مدة صلاحيتها، الا ان هذا العميل قد يرى استخدام البطاقة بعد انتهاء مدة صلاحيتها ومن الناحية العملية فإن ماكينة السحب الآلي سوف تبتلع البطاقة المنتهية الصلاحية دون ردها للعميل، أما إذا استعمل العميل هذه البطاقة لدى التجار كأداة وفاء، وكان له رصيد كاف لدى البنك فإن ذلك من شأنه أن يثبت حسن نيته، حيث جرى العمل على قيام البنك بإعطائه بطاقة جديدة بمجرد انتهاء صلاحية الاولى، أما في حالة غياب الرصيد فإن البنك يرفض الوفاء للتاجر بقيمة المعاملة لإخلاله بأحد الالتزامات التي يفرضها العقد المبرم بينهما، وهو التحقق من تاريخ انتهاء البطاقة [1].

ب-استعمال البطاقة رغم الغائها

للبنك في أي وقت حق الغاء البطاقة لسبب من الأسباب مثل غلق الحساب، أو تغيير نظام التعامل، أو تغيير نوعية الخدمة التي تؤديها البطاقة، ومع ذلك تظل البطاقة مع العميل وقد يستخدمها بعد الغائها، فإن كان الاستعمال بعد غلق الحساب بمعرفة العميل وعدم وجود رصيد له و فإن الاستعمال يعد شروعا في سرقة ما لم يتحصل على مال، لأنه يعلم بأنه ليس لديه حساب لدى البنك ويستعمل البطاقة قصد الحصول على مال [2].

[1] محمد قدري حسن عبدالرحمان، جرائم الاحتيال الالكتروني، بدون طبعة، المجلد20، العدد79، دار المنظومة، الامارات المتحدة العربية ، 2016، ص62 .

[2] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، بيروت، لبنان ,الطبعة الأولى، 2005، ص524.

ج-تجاوز حد السحب

قد يقوم الحامل الشرعي للبطاقة بسحب مبالغ تتجاوز الرصيد الموجود بالفعل في حسابه مخالفا شروط العقد المبرم مع البنك مصدر البطاقة الذي يكون أحد شروطه عدم تجاوز الرصيد الفعلي للعميل.[1]

2- الاحتيال في استعمال البطاقة من قبل الغير

يقصد بذلك هو قيام أحد الاشخاص بسرقة البطاقة من صاحبها أو العثور عليها عند فقدانها ورفض الشخص ردها الى حاملها الشرعي وللنوع هدا عدة صور:

أ-الاستعمال الغير مشروع للبطاقات المسروقة او المفقودة

يقترن هذا الاسلوب بجريمة تزوير توقيع صاحب البطاقة الأصلي، وتتحدد مسؤولية البنك المصدر للبطاقة وصاحب البطاقة الأصلي عن الاستخدام غير المشروع لها وفقا للتوقيت الزمني الذي يتم فيه ابلاغ البنك المصدر بواقعة سرقة البطاقة أو فقدها، حيث يتحتم على البنك ايقاف العمل بها فور ابلاغه بذلك [2].

ب-تزوير بطاقات الدفع الإلكتروني

ويتم تزوير البطاقة بإدخال تعديل عليها من شأنه تغيير حقيقتها، سواء كان هذا التغيير في الحروف المطبوعة أو المسجلة الكترونيا عليها، أو على الاسطوانة الموجودة داخل آلة توزيع النقود .

وقد يكون التزوير باصطناع بطاقة دفع الكتروني ونسبتها الى مؤسسة مالية أو أشخاص حقيقيين، وذلك بإدخال بيانات صحيحة خاصة بأسماء وأرقام حسابات لأشخاص يحملون بطاقات دفع الكتروني صالحة للاستعمال، والغالب في هذه الحالة عدم استعمالها لسحب النقود في اجهزة السحب الآلي وانما تستعمل فقط لدى التجار الغير مزودين بالنهايات الطرفية [3].

ج-الاستيلاء على أموال بطاقة الدفع الإلكتروني

وذلك بسرقة أرقام البطاقات عن طريق الاستيلاء على ايصالات واشعارات البيع أو من خلال الاستعانة بأي موظف في محل تجاري أو الاستقبال في أحد الفنادق، أو الاتصال بأشخاص واخبارهم بأنهم فازوا برحلة مجانية ويريدون التأكد من رقم البطاقة الائتمانية الصحيح واسم العميل بالكامل وجميع البيانات التفصيلية، أو الاتصال بحاملي البطاقات والادعاء بأنهم من موظفي البنك المصدر للتأكد من

[1] حسين محمد الشبلي، (صور الاحتيال والتزوير في البطاقات الائتمانية)،المجلة العربية للدراسات الأمنية والتدريب، إدارة البحث الجنائي، المملكة الأردنية الهاشمية، عمان ,الأردن ,المجلد 29، العدد58، ص67

[2] محمد قدري حسن عبد الرحمان، المرجع السابق، ص64.

[3] كيلاني عبد الراضي محمود، المسؤولية عن الاستعمال غير المشروع لبطاقات الوفاء والضمان، دار النهضة العربية، القاهرة، مصر، 2001، ص 106.

المعلومات، وذلك بهدف اعادة استخدام هذه البيانات والمعلومات في الحصول على الاموال باستخدام بيانات البطاقات[1] .

ثانيا: أساليب الاحتيال في التجارة الإلكترونية

مع التطور التكنولوجي وانتشار التجارة الإلكترونية أصبحت المعاملات عبر الانترنت جزءا لا يتجزأ من حياتنا اليومية، لكن هذا التوسع جذب أيضا مجرمين ومحتالين يسعون لاستغلال الثغرات لتحقيق مكاسب غير مشروعة، وتتعدد أساليب الاحتيال في التجارة الإلكترونية فنذكر منها:

1-تقليد واستعمال المعلومات والماركات التجارية المتشابهة

وهذا يتم عن طريق قيام بعض المواقع باستعمال العلامات والماركات المشهورة واستعمالها بهدف جذب الزبائن والاحتيال عليهم ومن ثمة تحقيق أرباح عن طريق الاحتيال والنصب[2] .

2-عمليات القرصنة

والتي يقوم بها مجرمون غير مرئيون سواء من طرف (crackers) الدين يقومون بخرق المواقع الإلكترونية وسرقة المعلومات الشخصية والمالية، أو من طرف (hackers) وهم أشخاص متسللون يتابعون باستمرار آخر التطورات في مجالات الأمن السيبراني وبرامج الحماية، غالبا ما يشكلون نواد لتبادل الخبرات والمعلومات التقنية بعضهم يستخدمون مهاراتهم في اختراق الأنظمة للمواقع الالكترونية بهدف التخريب أو سرقه المعلومات مما يشكل تهديدا حقيقيا لأمن البيانات .[3]

3-طلب شراء السلع عبر الاحتيال

وهو من أهم أساليب الاحتيال الإلكتروني عبر الانترنت، يتمثل في شحن البضائع الإلكترونية المشتراة ببطاقات الائتمان المسروقة من مستهلك ما إلى بلاد بعيدة عن محيط السرقة، حيث يحصل المحتالون على السلع بأسعار أقل داخل الولايات المتحدة واوروبا على سبيل المثال ثم يقومون بشحنها إلى الخارج بأسعار أعلى بقليل من قيمتها الحقيقة [4].

[1] محمد قدري حسن عد الرحمان، المرجع السابق، ص65.
[2] حياة هراكي (واقع جريمة الاحتيال الالكتروني في التجارة الالكترونية)، مجلة التغييرالاجتماعي، جامعة محمد خيضر بسكرة، الجزائر ,العدد2، المجلد الثامن، 31-12-2023، ص55 .
[3] عزالدين غبش (حماية المستهلك الالكتروني في ظل الجرائم السبيرانية)، المجلة الدولية للتحولات القانونية والسياسية، جامعة الشهيد حمة لخضرالوادي، العدد1، المجلد1، وادي سوف ,الجزائر ,أفريل 2022، ص 28.
[4] حياة هراكي، المرجع السابق، ص 55.

4-الإحتيال على المستهلك في المزادات

يتمثل هذا النوع من الاحتيال في قيام بعض الجهات بإدخال عروض وهمية في المزادات الإلكترونية، وذلك بهدف رفع سعر المنتج المعروض للبيع عبر الانترنت، ويستغل في ذلك قلة خبرة المستهلك أو ضعف وعيه بالسعر الحقيقي للسلعة .[1]

5-الخداع والنصب

ذلك بفتح مواقع تجارية على الشبكة تكون وهمية تحمل كل الصفات التي تجذب المستهلك، كالتخفيضات والخصومات على السلع التي تكون وهمية وهذا بغية سرقة أموالهم[2]، وهذه من أكثر أساليب الاحتيال انتشاراً .

[1] حياة هراكي، المرجع السابق ص، 56.
[2] عزالدين غبش، المرجع السابق، ص 99.

المبحث الثاني: الإطار القانوني لتجريم الاحتيال في التجارة الإلكترونية

يثير تجريم الاحتيال الالكتروني عدة تساؤلات قانونية، من بينها مدى كفاية النصوص التشريعية التقليدية لمواجهة هذا النوع المستحدث من الجرائم، ومدى توافق التشريع الجزائري مع المعايير الدولية في تجريم الاحتيال الالكتروني، كما أن مواقف القضاء تختلف في تفسير وتطبيق النصوص المتعلقة بهذه الجريمة، مما يؤثر على تحقيق العدالة وحماية الضحايا . ونظرًا لتعدد الجهود القانونية على المستويين الدولي والوطني لمجابهة الاحتيال الإلكتروني، ارتأينا تقسيم هذا المبحث إلى مطلبين رئيسيين، وهما كلآتي تجريم الاحتيال في التجارة الإلكترونية (المطلب الأول)، وأركان الاحتيال في التجارة الالكترونية (المطلب الثاني) .

المطلب الأول: تجريم الاحتيال في التجارة الإلكترونية

مع تطور تقنية المعلومات، واهتمام الأنظمة الدولة بموضوع الجرائم المعلوماتية وقعت العديد من الصكوك والمواثيق الدولية من طرف دول أدركت فعلا مدى الخطورة التي تشكلها هذه الجريمة بوصفها من الجرائم العابرة للحدود، فقد يكون الجاني في بلد والمجني عليه في بلد آخر، ومزود الخدمة في بلد ثالث و المستضيف للموقع والذي صر منه الفعل المجرم في بلد آخر ومن هنا أثيرت مسألة تطبيق نصوص القانون الجنائي، لذلك سنحاول التطرق إلى المواثيق الدولية لجرائم الكمبيوتر والانترنت . ومن خلال هذا المطلب سنسلط الضوء على دور الاتفاقيات في تجريم الاحتيال الإلكتروني في التجارة الإلكترونية (الفرع الأول) ودور المشرع الجزائري (الفرع الثاني) .[1]

الفرع الأول: دور الاتفاقيات الدولية في تجريم الاحتيال الإلكتروني في التجارة الإلكترونية

أدى التطور التكنولوجي المتسارع، والانفتاح اللامحدود على شبكات الاتصال والمعلومات، إلى بروز أشكال جديدة من الجرائم، من بينها جريمة الاحتيال الإلكتروني، التي باتت تهدد الأفراد والمؤسسات وحتى الدول، وأمام تزايد ارتكابها عبر وسائل الاتصال الحديثة في إطار التجارة الإلكترونية، تبين أن هذه الجريمة تتطلب تعاونا دوليا في تجريمها، ومن هذا المنطلق جاءت الاتفاقيات الدولية لوضع معايير موحدة للدول من أجل مكافحتها .

[1] ليندة شرابشة، (السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية، الاتجاهات الدولية في مكافحة الجريمة الالكترونية)، المركز الجامعي سوق أهراس، الجزائر، ص 244 .

أولا/- توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 1994 البرازيل بشأن جرائم الكمبيوتر:

حيث نصت على الأفعال المجرمة في جرائم المعلوماتية كالاحتيال والغش المرتبط بالكمبيوتر من خلال إتلاف ومحو معطيات والتي أيضا تعرف بالتزوير المعلوماتي .

أما من الناحية الإجرائية فإن القرار الصادر عن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات تضمن جملة من القواعد الإجرائية في بيئة الجرائم المعلوماتية، تتمثل فيما يلي:

- القيام بإجراء التفتيش والضبط في بيئة تكنولوجيا المعلومات وأيضا تفتيش شبكات الحاسب الآلي .
- التعاون الفعال بين المجني عليهم والشهود وكذا مستخدمي الملومات من أجل إتاحة استخدام المعلومات لأغراض قضائية .
- اعتراض الاتصالات داخل نظام الحاسب الآلي ذاته وممارسة الرقابة عليها.[1]

ثانيا/- اتفاقية بودابست لمقاومة جرائم المعلوماتية والاتصالات:

1/-التعريف بالاتفاقية: اتفاقية بودابست هي اتفاقية دولية تم توقيعها في العاصمة الهنغارية بودابست في عام1994، وهي تعتبر إحدى الاتفاقيات الرئيسية في مجال حقوق الانسان والحريات الاساسية في أوروبا .

وقعت على هذه الاتفاقية الدول الاعضاء في منظمة الامن والتعاون في أوروبا، من بين النقاط الرئيسية في الاتفاقية هي التزام الدول الاعضاء بضمان حقوق الإنسان والحريات الاساسية لجميع الافراد الموجودين على أراضيها بما أر في ذلك الاشخاص الذين ينتمون إلى الاقليات الوطنية والعرقية والدينية واللغوية، وتلزم أيضا الأعضاء باتخاذ التدابير الضرورية لضمان حقوق المواطنين في الوصول إلى المعلومات وحرية التعبير، وبالتالي يمكن القول أن اتفاقية بودابست تمثل تعهدًا دوليا لتعزيز حقوق الانسان والحريات الاساسية في أوروبا وتلعب دورا هاما في نطاق الديمقراطية والحكم القانوني في القارة الأوروبية .[2]

[1] ليندة شرابشة، المرجع السابق، ص 245، ص 246 .
[2] العالية ختام، حجاج درة، (جريمة الإحتيال المعلوماتي في التشريع الجزائري،) مذكرة مكملة لنيل شهادة الماستر في الحقوق، جامعة العربي بن مهيدي أم بواقي، الجزائر، كلية الحقوق والعلوم السياسية، السنة الجامعية 2024/2023، ص 69 .

2 /- مضمون الاتفاقية:

وهي اتفاقية دولية تحدد جرائم الحوسبة وتوفر إطارا للتعاون الدولي في مجال مكافحة الجرائم المعلوماتية، فالاتفاقية الأوروبية لتعيين الجرائم المرتبطة بنظم المعلومات المعروفة أيضا باسم اتفاقية بودابست هي اتفاقية دولية تم تبنيها بواسطة مجلس أوروبا بهدف مكافحة جرائم الحوسبة وتوفير إطار قانوني للتعاون الدولي في هذا المجال، تم توقيعها في عام 2001 في بودابست بالمجر ودخلت حيز التنفيذ عام 2004 .

تتضمن اتفاقية بودابست تعريفا لجرائم الحوسبة والأنشطة ذات الصلة بالتكنولوجيا المعلوماتية مما يتيح للدول الأعضاء توحيد التشريعات والتدابير القانونية وتشمل هذه الجرائم على سبيل الحصر الوصول الغير مشروع إلى الأنظمة الحاسوبية واختراق الأمن السيبراني وتدمير بيانات الحوسبة والاحتيال الإلكتروني .[1]

قانون الأونستيرال النموذجي ودوره في تنظيم المعاملات الإلكترونية

لجنة الأمم المتحدة للقانون التجاري الدولي (الأونيسترال)، التي تأسست في عام 1966 هي هيئة فرعية تابعة للجمعية العامة للأمم المتحدة وتتمثل مهمتها العامة في تعزيز التوحيد التدريجي لمواءمة لقانون التجارة الدولية ،ومنذ تأسيسها أعدّت الأونيسترال مجموعة واسعة من الاتفاقيات والقوانين النموذجية وغيرها من الأدوات القانونية التي تتناول القانون الموضوعي المنظّم للمعاملات التجارية أو الجوانب الأخرى من القانون التجاري التي تؤثر في التجارة الدولية.[2]

أولًا: قانون الأونستيرال النموذجي والتوقيعات الإلكترونية:

صدر هذا القانون في 5 يوليو 2001، حيث أُقر بهدف توفير إطار قانوني لاستخدام التوقيعات الإلكترونية في المعاملات التجارية، خاصةً مع تزايد الاعتماد على التقنيات الرقمية في التوثيق، وأمام هذه التطورات تلاشت وظيفة التوقيع التقليدي ليحل محله التوقيع الإلكتروني الذي يعتمد على كود سري أو شفرة سرية يتم الحصول عليها بعد اتباع جملة من الإجراءات لضمان الموثوقية والمصداقية .

[1] العالية ختام، حجاج درة، المرجع السابق، ص 69 .
[2] لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال)، الموقع الرسمي، https://uncitral.un.org/ar، تاريخ الاطلاع: 27 جوان 2025.

ثانيًا: قانون الأونستيرال النموذجي والتجارة الإلكترونية:

يشمل نطاق تطبيق هذا القانون جميع أنواع المعلومات التي تكون على شكل رسالة بيانات مستخدمة [1].

في المعاملات التجارية، بحيث يتم استلامها أو تخزينها عبر الوسائل الإلكترونية، ويتم تبادل هذه البيانات من خلال نقلها إلكترونيا من حاسوب إلى آخر باستخدام معيار متفق عليه، مع الأخذ بعين الاعتبار تفسير هذا القانون لمصدره الدولي ولضرورة توحيد تطبيقه .[2]

الفرع الثاني: موقف المشرع الجزائري في تجريم الاحتيال الإلكتروني

الجزائر كغيرها من الدول تأثرت باتفاقية بودابست 2001، وذلك من خلال التعديلات التي ادرجها في قانون العقوبات والنصوص القانونية.[3]

ومع التطور السريع للتكنولوجيا الرقمية، برزت أشكال جديدة من الجرائم التي تستهدف الأنظمة المعلوماتية، بما في ذلك الاحتيال الإلكتروني الذي يُعد من أخطر الجرائم المعلوماتية نظرًا لتأثيره المباشر على الاقتصاد والأمن السيبراني.

وأمام هذا الواقع، استشعر المشرع الجزائري الحاجة إلى وضع إطار قانوني يجرّم هذه الأفعال ويحدد العقوبات المناسبة لها، مما دفعه إلى تعديل قانون العقوبات عبر القانون رقم 04-15 الصادر في 10 نوفمبر 2004 المتمم لأمر رقم 22-15 وقد تضمن هذا التعديل استحداث مواد جديدة تحت القسم الثامن من قانون العقوبات بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، حيث نصت المادة 394 مكرر وما يليها على تجريم الأفعال التي تستهدف الإضرار بالأنظمة المعلوماتية، بما في ذلك عمليات الاحتيال التي تتم باستخدام الوسائل الإلكترونية[4].

فبالنسبة للجريمة المعلوماتية التي نصت عليها المادة 394 مكرر من القانون رقم15/04 يعاقب بالحبس من ثلاثة أشهر الى سنة أو بغرامة مالية قدرها ست آلاف دينار جزائري إلى مئة ألف دينار جزائري (6000 دج إلى 1000000 دج) "كل من يدخل أو يلقي عن طريق الغش في كل أو جزء من

[1] ليندة شرابشة، المرجع السابق، ص247، ص 248 .
[2] المرجع نفسه، ص 248 .
[3] العالية ختام، حجاج درة، المرجع السابق، ص 73 .
[4] د. بوضياف إسمهان، (الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر)، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الحادي عشر، المجلد 03، جامعة محمد بوضياف المسيلة، الجزائر، سبتمبر 2018، ص 362 .

منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك...إذا ترتب على الأفعال إعلام تخريب النظام واستغلال المنظومة وبذلك تكون العقوبة من ست أشهر ..."[1]

وعند استقراء الفصل الثالث في إجرام الجنايات والجنح ضد الأموال من قانون العقوبات حسب المادة 394 مكرر،394 مكرر01، 394 مكرر02، 394 مكرر03، 394 مكرر04، 394 مكرر05، 394 مكرر06، 394 مكرر07.

تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات إذ نجد أن المشرع الجزائري جرم هذا الفعل وقسمه إلى أربع طوائف، وهي:

الطائفة الأولى: تتضمن جرائم التلاعب بنظم المعالجة الآلية للبيانات مثل التغيير والتخريب وهذه البيانات يعاقب فيها الجاني بالسجن من شهر الى سنة أو بغرامة مالية تتراوح ما بين (50000 دج و1000000 دج) وتزداد العقوبة إذا ما تسبب الفعل الإجرامي في حذف أو تغيير البيانات.

الطائفة الثانية: تتعلق بجرائم الحاسوب واستخدام النظام المعلوماتي مثل إفشاء أو نشر معلومات محظورة قانونيا، في حين تتراوح عقوبة هذه الجرائم من شهرين إلى ثلاث سنوات أو بغرامة مالية تتراوح من (1000000 دج إلى 10000000) .

الطائفة الثالثة: تتعلق بجرائم الأمن السيبراني وجرائم أمن الدولة ومؤسساتها تتضاعف فيها العقوبة المتعلقة بالقسم السابق وتطبق عليها اشد عقوبة.

الطائفة الرابعة: تتعلق بالجرائم الإلكترونية بالنسبة للشخص المعنوي التي تكون عقوبتها خمس مرات ضعف الشخص الطبيعي.

ومن الملاحظ أن المشرع الجزائري يفتقر إلى وجود معايير واضحة وموحدة في تقسيمه للجرائم الإلكترونية وتحديد العقوبات المقررة لها، وكان من الأنسب أن يتبع في تشريعه المنهج المعتمد في الفقه والذي يقسم الجرائم الإلكترونية إلى جرائم واقعة على النظام المعلوماتي، وجرائم بواسطة النظام المعلوماتي، ويتم ذلك بضبط مصطلحات الخاصة بهذه الجرائم لتسهيل فهم طبيعتها وتصنيفها استنادا للمادة 394 مكرر05 من القانون 15/04 والمتمم لقانون العقوبات.[2]

[1] العالية ختام، حجاج درة، المرجع السابق ص 26، ص 27 .
[2] المرجع نفسه ، ص 27، ص 28 .

المطلب الثاني: أركان جريمة الاحتيال في المجال الإلكتروني

ثبت الفقه على أنه لا وجود لجريمة إلا بتوافر نص قانوني يحدد ماهيتها وطبيعتها ويفرض عقوبة على مخالفيها، فأركان الجريمة تعتبر عنصرا جوهريا في تكوينها ولا تبقى هناك جدوى من توقيع العقاب إذ انعدمت، ومن خلال دراستنا سنبين في هذا المطلب الاركان التي تقوم عليها جريمة الاحتيال الإلكتروني، وذلك من خلال ركنها المادي في (الفرع الأول)، ثم الركن المعنوي في (الفرع الثاني)، وأخيرا الركن الشرعي في (الفرع الثالث) .

الفرع الأول: الركن المادي لجريمة الاحتيال الإلكتروني

يقصد بالركن المادي للجريمة هو الفعل المشكل للجريمة (المجرّم)، ولـذلك فلا جريمة بلا ركن مادي، فهو الفعل أو السلوك الذي يقوم به الشخص ويجرمه القانون الجزائي ويرتب على القيام به عقوبة، ويتكون الركن المادي من عناصر ثلاثة وهي: السلوك الإجرامي والنتيجة الإجرامية وعلاقة السببية بين السلوك.

ويتمثل هذا الركن في سلوك إجرامي يستعمل فيه الجاني وسائل احتيالية أو أساليب كاذبة، من شأنها التأثير على المجني عليه لتسليم ماله طواعية للجاني معتقدا بصدقه .[1]

أولا/-السلوك:

حسب نص المادة 372 من قانون العقوبات الجزائري حصر المشرع الجزائري الأفعال التي تعتبر السلوك الإجرامي لجريمة الاحتيال التي عرفها البعض أنها أكاذيب مدعمة بمظاهر خارجية من بينها:

1/-الكذب:

هو تحويل الحقيقة الى شيء كاذب وهو عمل ينطوي على إعطاء معلومات غير صحيحة وتزويرها كحقائق، ويمكن أن يكون الكذب شفويا أو حتى مطبوعا في حالات الكذب يتم تغير الواقعة وتقديم معلومات زائفة لآخرين على سبيل المثال: يمكن لشخص أن يدعي أنه يملك قدرات خارقة مثل قدرته على شفاء الأمراض وتحديد الإماءات وحركات الإقناع الأخرين بصحة هذا، ونتيجة لذلك يمكن أن يقع الآخرون في خطأ بتعرضهم للاحتيال وفقدانهم لأموالهم .[2]

[1] محمد طه ابراهيم الفليح، (جريمة الاحتيال الإلكتروني في إطار التجارة الإلكترونية ضمن التشريعات الأردنية)، مجلة جامعة الزيتونة الأردنية، الأردن، للدراســــــات القانونية، المجلد (3)، الإصدار (3)، سنة 2022، ص 74.
[2] العالية ختام، حجاج درة، المرجع السابق، ص 28 .

2/ المظاهر الخارجية لجريمة الاحتيال:

فالطرق الاحتيالية لا تقوم الا في حالة تأييد الكذب لمظاهر خارجية وهو ما يقو م به الجاني من أجل تعزيز أكاذيبه وتحقيق أهدافه الاحتيالية وإيقاع المجني عليه، ويتحقق ذلك في صور معينة:

-استعانة الجاني بشخص آخر وذلك لدعم ادعاءاته امام المجني عليه.
- الاستعانة بأوراق صحيحة أو كاذبة.
- الاستعانة بوسائل الإعلام والنشر.
- إساءة استخدام صفة صحيحة .
- الظهور بصورة تمثيلية أمام الآخرين.
- قيام الجاني بأعمال يدوية والاستعانة بأشياء مادية.
- استغلال الجاني وقائع ناقصة وغير كاملة لتأييد أكاذيبه.
- اتهام المجني عليه بأمور قانونية محددة من خلال نشر أكاذيب بهدف خداعهم .

مثلا عن طريق إيداع مشروع غير حقيقي، وتعد هذه الأعمال في نظر الفقه **"غاية الكذب"** أو" **أغراض الكذب"**

ويمكن حصر هذه **الغايات** فيما يلي:

♦الاتهام بوجود مشروع كاذب.
♦الاتهام بوجود واقعة مزورة غير حقيقية.
♦إحداث أمل بحصول على ربح وهمي.
♦إحداث أمل بتسديد المبلغ الذي أخذ بطريقة احتيالية.
♦اتهام بوجود سند دين غير صحيح أو سند مخالصة مزور.

ثانيا/-النتيجة:

الشيء الذي يسعى الجاني في تحقيقه هو تسليم المجني عليه مال أو منقول للجاني، وهو عنصر أساسي لقيام الجريمة إذا ما انتفت معه الجريمة، أما عنصر التسليم في هذه الحالة هو ما يميز جريمة الاحتيال عن جريمة السرقة، وفي هذا المقام تكون عن رضى المجني عليه، لكن في حالة السرقة يكون الاستيلاء عن الشيء خفية ودون علم المجني عليه أو دون رضاه .[1]

[1]العالية ختام، حجاج درة، المرجع السابق، ص 28، ص 29 .

ثالثا/-العلاقة السببية:

يقصد بها في هذا المقام أن يقوم المجني عليه بتسليم المنقول بعد اقتناعه التام للجاني ولكن لقيام هذه العالقة السببية يجب أن تتوفر شروط محددة، وتتمثل في:

- تسليم المنقول بشكل الحق على الاحتيال .
- عدم علم المجني عليه بالحقيقة .
- أن يكون الاحتيال من شأنه التسليم[1] .

وعليه، فإن الركن المادي لجريمة الاحتيال الإلكتروني يتمثل في فعل الاحتيال، وهذا الفعل يتخذ صورًا متنوعة ومتجددة مسايرة للتقدم التكنولوجي في هذا المجال، وبالتالي يصعب عدها أو حصرها، نذكر أهمها:

1/- الاحتيال عن طريق انتحال شخصية المواقع التسويقية الشهيرة: وذلك عن طريق إنشاء مواقع إلكترونية وهمية على شبكة الانترنت على غرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة، بحيث يظهر بأنه الموقع الأصلي المقدم لتلك الخدمة، مما يؤدي إلى الإضرار بالشركات والمؤسسات صاحبة الموقع الأصلي، ويدمر ثقة المستهلكين في التجارة الالكترونية.

2-/ الاحتيال عبر البريد الإلكتروني: وذلك باستخدام بريد إلكتروني مغشوش لجذب المستهلك أو المستخدم من أجل الاتصال بمواقع إلكترونية لشركات تجارية مشهورة، وعند دخول المستهلك أو المستخدم على الموقع الالكتروني المزور ويطلب السلعة وتتم الموافقة، فإنه يطلب منه إرسال المعلومات الخاصة به (أرقام بطاقة الائتمان أو رقم الحساب البنكي الالكتروني) فيقوم هذا الأخير بإرسالها معتقدا بأنه موقع الشركة التجارية الحقيقية عندما يستلم المستهلك رسالة إلكترونية تتضمن طريقة اتصال بموقع إلكتروني خاص بالشركة التجارية المزيفة عن طريق الرابط الإلكتروني الخاص بها، فعندما ينقر المستهلك على هذا الرابط، فإنه يدخل على الموقع المزيف، إلا أنه وبالتفحص الجيد يمكن أن يظهر أن عنوان الصفحة مختلف عن الموقع الحقيقي لكن الضحية لن يلاحظ هذا الفرق، حيث يقوم بإعطاء معلومات عنه، مثل كلمة السر ورقم بطاقة الائتمان الخاصة به.

يطلق على هذا الشكل من الاحتيال بالتصيد، حيث يلجأ الجاني في هذا السلوك الإجرامي إلى تقمص شخصية شخص آخر، وذلك بإرسال رسالة إلكترونية إلى المستهلك أو المستخدم للتغرير به من[2]

[1] العالية ختام، حجاج درة، المرجع السابق، ص 29، ص 30 .
[2] محمد طه ابراهيم الفليح، المرجع السابق، ص 76 .

أجل الحصول على المعلومات الخاصة به، مثل أرقام الحسابات المصرفية، أو أرقام بطاقة الائتمان وكلمة السر المرتبطة بها.

3/- الاحتيال عن طريق ترويج السلع والخدمات باستخدام الخداع الإعلاني: وذلك عندما يلجأ المنتج أو المزود متعمدا، ولأجل الترويج لمنتجاته أو خدماته إلى الإعلان التجاري الخادع الذي قد ينطوي في بعض الأحيان على مغالطات علمية أو غير صحيحة تكون على حساب المستهلك الذي يخدعه هذا الإعلان .

الفرع الثاني: الركن المعنوي لجريمة الاحتيال الإلكتروني

يقصد بالركن المعنوي العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها، حيث تعبر عن نية الجاني أو قصده في ارتكاب الفعل، ومن ثم يوجه إليها لوم القانون وعقابه، فالقاعدة العامة أنه لا جريمة بغير ركن معنوي فيه حيث يتم تحديد مسؤولية الفاعل عن الجريمة بحيث لا يسأل الفاعل عن الجريمة ما لم تكن هناك صلة بين مادياتها ونفسيته.

فجريمة الاحتيال الإلكتروني تعتبر من الجرائم العمدية التي تقوم إذا ثبت علم الجاني بأن الوسيلة التي استعملها من شأنها أن تؤدي إلى خداع المستهلك، واتجاه إرادته إلى تحقيق النتيجة الإجرامية دون إدراكه، أي أن يقوم بالفعل الإجرامي وهو مدرك وواع بنية إيقاع المستهلك بالغلط أو قصد الإضرار به، وهذا يتطلب سوء النية الواجب إثباتها بطرق الإثبات كافةً، أي أن الركن المعنوي لجريمة الاحتيال الإلكتروني قد يتخذ صورة القصد ولكنه قصد عام يضاف إليه في بعض الحالات قصد خاص.

حيث إنه لا يكفي لقيام جريمة الاحتيال الإلكتروني إتيان الجاني للفعل الإجرامي، والمتمثل باستعمال الطرق الاحتيالية التي من شأنها أن تؤدي إلى إيهام المستهلك أو إيقاعه في الغلط بشأن السلعة أو الخدمة المقدمة، بل يجب بالإضافة لذلك تحقق القصد الجنائي العام والمتمثل بعنصريه **العلم والإرادة.**[1]

أولا: العلم

1/- العلم بالاحتيال:

لإدراك جريمة الاحتيال يجب أن يكون الفاعل على علم بأنه يمارس الخداع والكذب، على سبيل المثال إذا كان الفاعل مسؤول عن جريمة الاحتيال يجب أن يكون على علم بأنه يتصرف بمنقول غير

[1] محمد طه ابراهيم الفليح، المرجع السابق، ص 76، ص 77 .

مملوك له فإن الجريمة في هذه الحالة تقوم لإدراكه بأفعاله الغير مشروعة، وبالمفهوم المخالف بحالة ما لم يكن الجاني على دراية بأنه يقوم بأعمال غير قانونية ما لم يقم بتظليل الآخرين يسقط عنه الجرم .

2/- العلم بالجريمة الإلكترونية:

لا يكفي أن يقوم الشخص بتنفيذ فعل ما في مجال المعلوماتية حتى يتم اتهامه ومحاكمته بارتكاب الجريمة، بل يجب أيضا أن يكون لديه نية لارتكاب ذلك الفعل وتتحقق النية الإجرامية فقط إذا كان شخص يعلم أن فعله يشكل جريمة ويتمتع بالقدرة على تنفيذ تلك الفعل، وبالتالي إذا دخل شخص ما إلى شبكة المعلوماتية فقط لأغراض التصفح المسموح به، لكن ارتكب خطأ بسبب جهله في أنظمة المعلوماتية ما مما أدى إلى إلحاق الضرر بشخص آخر سواء طبيعي أو معنوي، فأنه سيسأل هنا عن الخطأ الغير المقصود وفقط.

ثانيا/- الإرادة:

يشير بهذا العنصر اتجاه إرادة الجاني إلى ارتكاب جريمة الاحتيال الإلكتروني بمعنى ثبات وإلحاح المجرم لتحقيق هدفه والوصول إلى النتيجة الإجرامية من سلوكه، ومثال ذلك دخول الجاني لشبكة المعلوماتية لأجل التغيير بإدخال أو إخراج بعض المعلومات أو البيانات بمحاولات تكرارية، وهذا الفعل يؤدي إلى ثبوت القصد الإجرامي والدلالة على عزم الجاني للوصول إلى هدفه ألا وهو الاحتيال الإلكتروني .[1]

الفرع الثالث: الركن الشرعي لجريمة الاحتيال الإلكتروني

الركن الشرعي هو ضرورة وجود نص في القانون يحدد الافعال غير المشروعة التي إذا ارتكبها الشخص تقوم مسؤوليته، وبالتالي إيقاع العقوبة المناسبة عليه. فالهدف الذي يقصده المشرع من وراء تجريم الاحتيال الإلكتروني هو حماية مال، وذلك من خلال تجريم جميع الممارسات والأساليب الاحتيالية التي تواجه الأفراد للاستيلاء على أموالهم بطرق الغش والخداع.[2]

وبالتالي فإن الاحتيال المنصوص عليه في المادة 372 من قانون العقوبات الجزائري تنص على أنه" كل من توصل الى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبذاء من الالتزامات أو إلى الحصول على أي منها أو شاع في ذلك وكان في ذلك باحتيال لسلعة ثروة الغير أو بعضها أو شرع في ذلك وكان الاحتيال لسلب كل ثروة الغير أو بعضها إما

[1] العالية ختام، حجاج درة، المرجع السابق، ص 31، ص 32.
[2] محمد طه ابراهيم الفليح، المرجع السابق، ص 73 .

باستعمال أسماء أو صفات كاذبة أو سلطة خالية أو اعتماد مالي خيالي أو بإحداث الأصل في الفوز بشيء أو في وقوع حادث أو أية واقعة أخرى".

"...إذا وقعت الجنحة من شخص بقصد إصدار أسهم أو سندات أو تفويضات أو حصص أو أية سندات مالية لشركة أو مشروعات تجارية أو صناعية ..."

ومن خلال هذه المادة نجد أن المشرع الجزائري نص على تجريم السلوكيات التي تدخل ضمن نطاق عمليات النصب والاحتيال، كما نجد أنه نص على العقوبات المقررة في حالة ما وقعت الجريمة المتمثلة في حبس من سنة إلى أقل من خمس سنوات ب غرامة من خمسة مئة إلى عشرين ألف دينار جزائري وهذا تطبيقا لنص المادة الأولى في قانون العقوبات التي تنص على أنه لا الجريمة ولا العقوبة أو لا تدابير أمن بغير نص لا يستطيع في هذه الحالة القاضي أن يبيح أفعال يجرمه القانون، ولا يمكنه أن يقضي بعقوبة غير التي انتهجها القانون نوعًا ومقدارًا .[1]

[1] العالية ختام، حجاج درة، المرجع السابق، ص 26 .

خلاصة الفصل

من خلال دراستنا لهذا الفصل الذي هو تحت عنوان الاطار المفاهيمي للاحتيال في التجارة الإلكترونية، تم التطرق أولا الى مفهوم التجارة الإلكترونية من خلال تعريفاتها المختلفة ووفق لما جاء به القانون 18-05 المتعلق التجارة الالكترونية بالإضافة الى إبراز خصائصها واشكالها التي تعكس تطور المعاملات التجارية في العصر الرقمي، ثم انتقلنا الى توضيح المقصود بالاحتيال في هذا المجال، سواء من حيث المفهوم أو الأشكال المتعددة التي يتخذها .

بعد ذلك استعرضنا الإطار القانوني الذي يؤسس عليه لتجريم الاحتيال الإلكتروني في التجارة الإلكترونية مع التركيز على أركان الجريمة الإلكترونية والتي تشمل الركن المادي والمعنوي والشرعي، كما تم التطرق إلى الجهود الدولية المبذولة في هذا الصدد من خلال الاتفاقيات الدولية .

الفصـــــل الثاني

حماية التــجارة الإلكترونية من جـــرائم الاحتـــيال الإلكتروني

الفصـــــل الثاني حماية التـــجارة الإلكترونية من جـــرائم الاحتـــيال الإلكتروني

تُمثل التجارة الالكترونية بيئة خصبة لارتكاب جرائم الاحتيال الإلكتروني ، نظراً لطبيعتها المفتوحة و الافتراضية، وما توفره من سهولة في تنفيذ المعاملات دون قيود جغرافية أو تحقق فعلي من هوية الأطراف، ومع اتساع رقعة هذا النوع من التجارة وتزايد الاعتماد عليه في مختلف التعاملات الاقتصادية، برزت تحديات قانونية وأمنية تهدد الثقة في البيئة الرقمية واستقرار السوق الإلكترونية، ما استدعى ضرورة وضع حماية قانونية فعالة تتوزع بيت تدابير وقائية للحد من وقوع الجريمة، و إجراءات ردعية تضمن ملاحقة الجناة ومعاقبتهم وفقا للقانون .

وفي هذا الإطار، يتناول هذا الفصل سبل حماية التجارة الإلكترونية من هذه الجرائم، حيث خُصّص (المبحث الأول) لاستعراض الإجراءات الوقائية من خلال تسليط الضوء على أهم أساليب الحماية إلى جانب حماية البيانات والمستهلك الإلكتروني، أما (المبحث الثاني) فيتناول الجانب الردعي من خلال الوقوف على الآليات الإجرائية المعتمدة في مكافحة جرائم الاحتيال الإلكتروني مع التطرق إلى خصوصية المحاكمة في هذا المجال .

المبحث الأول: الإجراءات الوقائية للحماية من الاحتيال في التجارة الإلكترونية

من خلال المبحث الأول، سيتم التطرق إلى أهم أساليب الحماية المعتمدة في البيئة الإلكترونية التجارية، وذلك من خلال تناول وسائل الدفع الإلكتروني كآلية رئيسية تعتمد عليها هذه التجارة، بالوقوف على مفهومها، أنواعها، وأساليب الحماية القانونية المقررة لها (**المطلب الأول**)، ثم التعرض لمختلف الوسائل المستعملة لمكافحة الاحتيال الالكتروني في التجارة الإلكترونية (**المطلب الثاني**) .

المطلب الأول: أساليب الحماية للتجارة الإلكترونية

تعد أساليب حماية التجارة الإلكترونية من أهم الأمور التي يجب أخذها بعين الاعتبار وخاصة في الفترة الأخيرة تماشيا مع التطور التكنولوجي المتسارع، ويتطلب ذلك اعتماد سياسات وإجراءات واضحة تهدف إلى تأمين بيانات المستخدمين وتأمين عمليات الدفع الإلكتروني، كما ينبغي توفير الحماية للمؤسسات والشركات الناشطة في هذا المجال، عبر تأمين بنيتها الإلكترونية وحمايتها من الاختراقات والهجمات الإلكترونية، ويكون ذلك بواسطة استخدام تقنيات التشفير والتوقيع الرقمي وإجراء فحص دوري للأمن الإلكتروني لضمان سلامة النظام والحماية من الهجمات الإلكترونية المحتملة.

الفرع الأول: وسائل الدفع الالكتروني وأساسها القانوني في مكافحة الاحتيال

تزايد الاعتماد على بطاقات الدفع الإلكتروني في شراء السلع والخدمات عبر الإنترنت، غير أن هذا الانتشار ترافق معه العديد من حالات الاحتيال والاعتداء، مما دفع عدة دول إلى سن تشريعات جنائية تهدف إلى حماية المستخدمين ومكافحة الجرائم المتعلقة بالاستخدام غير المشروع لهذه البطاقات .

أولا-/ تعريف وسائل الدفع الإلكترونية:

1-/ التعريف الفقهي: هي تلك الأداة المقبولة اجتماعيا من أجل تسهيل التعاملات الخاصة بتبادل السلع والخدمات وتسديد الديون، وتدرج ضمن وسائل الدفع إلى جانب النقود القانونية وتشمل أيضا السندات التجارية وسندات القرض التي يدخلها حاملوها في التداول عندما يؤدون أعمالهم.

كما عرفها البعض الآخر بأنها عملية تحويل الأموال في الأساس ثمنا مقابل سلعة أو خدمة بشكل رقمي باستخدام الحواسيب وإرسال البيانات عبر خط تليفوني أو شبكة معينة أو أي طريقة لإرسال البيانات .[1]

[1] بن حميدة هجيرة، عتيق ستي، (النظام القانوني لوسائل الدفع الإلكتروني في التشريع الجزائري)، مذكرة الماستر في الحقوق تخصص قانون أعمال، جامعة الدكتور مولاي الطاهر السعيدة، الجزائر، كلية الحقوق والعلوم السياسية، السنة الجامعية 2021/2020، ص 10، ص 11 .

عرفت أيضا انها: بطاقة تصدرها مؤسسة مجازة أو تمنحها إلى عميلها بهدف دفع ثمن السلع والخدمات للموردين دون أن يقتصر قبولها بالمؤسسة مصدرة البطاقة فقط .

ومن خلال ما سبق يمكن تعريفها بأنها عبارة عن بطاقات تقوم بوظيفتي الوفاء والائتمان، بحيث تتيح لحاملها القدرة على تسديد قيمة مشترياته وخدماته .

2-/التعريف القانوني: تُعرَّف وسائل الدفع قانونًا ضمن الإطار التشريعي المنظّم للنظام النقدي والمصرفي في الجزائر، والذي كان في السابق منصوصًا عليه في الأمر رقم 03-11 المؤرخ في 26 أوت 2003، المتعلق بالنقد والقرض. غير أن هذا الأمر تم إلغاؤه، وحلّ محله القانون رقم 23-09 المؤرخ في 21 جوان 2023، الذي يتضمن أحكامًا مستحدثة لتنظيم وسائل الدفع والتعاملات المالية[1].

كذلك عرف المشرع الجزائري وسيلة الدفع الإلكتروني في المادة 06 من قانون رقم 18-05 قانون التجارة من الإلكترونية بأنها: كل وسيلة دفع مرخص بها طبقا للتشريع المعمول به تمكن صاحبها من القيام بالدفع عن قرب أو عن بعد عبر منظومة إلكترونية .

ثانيا-/ أنواع وسائل الدفع الإلكترونية:

1/- السفتجة الإلكترونية: يمكن تعريف السفتجة الإلكترونية بأنها محرر ثلاثي الأطراف يعالج الكترونيا وبصورة كلية أو جزئية، ويتضمن أمر صادر من شخص يعرف بالساحب إلى شخص آخر وهو المسحوب عليه، بأن يدفع مبلغا لفائدة شخص ثالث هو المستفيد أو حامل السند، وذلك بمجرد الاطلاع أو في تاريخ قابل للتعيين .[2]

2/- الشيك الإلكتروني: الشيك الإلكتروني يعتبر المكافئ الإلكتروني للشيكات الورقية التقليدية الشائعة في التعامل، وهو رسالة الكترونية موثقة مؤمنة يرسلها محرر الشيك إلى مستلم الشيك ليعتمده

ويقدمه للبنك الذي يعمل عبر الأنترنت، ورغم أن المشرع الجزائري لم يورد تعريفا صريحا للشيك، واكتفى بالنص على بياناته في المادة 472 من القانون التجاري، كما أنه لم يشير صراحة الى إمكانية إصداره الكترونيا، غير أنه يفهم ضمنيا من خلال قانون النقد والقرض رقم 79-03 المتعلق بغرف المقاصة في المادة 2/3 .

[1] تم إلغاء الأمر رقم 03-11 المؤرخ في 26 أوت 2003 بموجب القانون رقم 23-09 المؤرخ في 21 جوان 2023، المتعلق بالقانون النقدي والمصرفي، الجريدة الرسمية رقم 39 لسنة 2023.
[2] راجع بن حميدة هجيرة، عتيق ستي، المرجع السابق، ص 11، ص 12، ص 13، ص 14، ص 27 .

يتمتع الشيك بصلاحية زمنية محددة كوسيلة دفع، حيث أنها تدوم سارية لمدة سنة تبدأ بعد انقضاء مهلة تقديم الشيك التي هي ثمانية أيام .

3/- التحويلات المصرفية: لم يضع المشرّع الجزائري تعريفًا صريحًا لوسائل الدفع، غير أنّ استقراء النصوص القانونية السابقة، لاسيما ما ورد في الأمر رقم 03-11 المؤرخ في 26 أوت 2003 المتعلق بالنقد والقرض، وخاصة المادة 51 منه، يُبيّن أن المشرع كان يعتبر وسائل الدفع جزءًا من العمليات المصرفية المرتبطة بفتح الحسابات والتحويلات. إلا أن هذا الأمر تم إلغاؤه بموجب القانون رقم 23-09 المؤرخ في 21 جوان 2023، المتعلق بالقانون النقدي والمصرفي، والذي لم يورد تعريفًا مباشرا لها، لكنه كرّس تنظيمها من خلال إنشاء اللجنة الوطنية للدفع وتوسيع وسائل الدفع لتشمل أدوات الدفع الرقمية.[1]

كما تبنّى المشرع الجزائري ذات التوجّه عبر إصداره لقانون جديد رقم 18-04 المحدد للقواعد المتعلقة بالبريد والاتصالات الإلكترونية حيث سمح المشرع بموجب المادة 6/46 بأن يتم تحويل الأموال عن طريق جميع وسائل الدفع الكتابية والإلكترونية .

4/- البطاقات البنكية: تعرف على أنها بطاقة مغناطيسية تصدر من قبل البنوك والمؤسسات المالية التي تتيح لحاملها بتسديد ثمن المشتريات أو سحب الأموال من الماكينات الالكترونية كبطاقة الائتمان . كما عرفتها المادة 543 مكرر 23 من القانون التجاري على أنها: "تعتبر بطاقة دفع كل بطاقة صادرة من البنوك والهيئات المالية المؤهلة قانونا وتسمح لصاحبها بسحب أو تحويل الأموال".

5/- البطاقات الذكية: هي عبارة عن بطاقة مزودة بمعالج دقيق يسمح بتخزين الأموال من خلال البرمجة الأمنية، وتتميز هذه البطاقة بقدرتها على التعامل مع بقية الكمبيوترات دون اللجوء إلى تفويض أو تأكيد صلاحية البطاقة من أجل نقل الأموال من المشتري على البائع.

6/- المحافظ الإلكترونية: تعتبر بطاقة بلاستيكية ممغنطة تثبت على الكمبيوتر الشخصي، أو قد تكون على شكل قرص مرن يمكن إدخاله في فئة القرص المرن في الكمبيوتر الشخصي، تستخدم لنقل القيمة[2] المالية عبر الانترنت باستخدام برامج مخصصة، كما سمكن استخدام المحفظة الإلكترونية في عمليات الدفع عبر الانترنت في الأسواق التقليدية التي تعتمد على أنظمة الدفع الإلكتروني .[3]

---

[1] تم إلغاء الأمر رقم 03-11 المؤرخ في 26 أوت 2003 بموجب القانون رقم 23-09 المؤرخ في 21 جوان 2023، المتعلق بالقانون النقدي والمصرفي، الجريدة الرسمية رقم 39 لسنة 2023.

[2] راجع بن حميدة هجيرة، عتيق ستي، المرجع السابق، ص 32، ص 34، ص 35، ص 41، ص 45، ص 47.

[3] بن حميدة هجيرة، عتيق ستي، المرجع السابق، الصفحة 47 .

7/- النقود الإلكترونية: تعرف على أنها مجموعة من البروتوكولات والتوقيعات الإلكترونية، التي تسمح للرسالة الإلكترونية ان تحل محل تبادل العملات التقليدية وبعبارة أخرى فإن النقود الإلكترونية او الرقمية هي المكافئ للنقود التقليدية التي اعتدنا عليها .

إذ تشير النقود الرقمية إلى سلسلة الأرقام الإلكترونية التي تمثل قيم معينة وتصدرها البنوك التقليدية أو البنوك الافتراضية لصالح المودعين، ويحصل عليها في صورة نبضات كهرومغناطيسية على بطاقة ذكية أو ضمن حساب شخصي .[1]

ثالثا/- الحماية القانونية لوسائل الدفع الإلكترونية:

تُعتبر تجربة الجزائر في مجال الدفع الإلكتروني جديدة، حيث شهدت بعض المبادرات في هذا المجال من خلال التأسيس القانوني الذي تم إطلاقه في سنة 2006، إذ كانت انطلاقته الفعلية عبر قانون النقد والقرض رقم 01/03. أما التنفيذ العملي فقد بدأ سنة 2007، حين قام المشرّع الجزائري في وضع مجموعة من النصوص القانونية سنة 2005 في القانون التجاري 05/02 التي تنظّم استخدام البطاقات البنكية، وتحديد الجهة المصدرة لها والمعتمدة من طرف البنوك، وقد لوحظ أن هذا القانون لم يوضح بشكل كاف كيفية التعامل بهذا النوع منا الدفع، لكنه لم يصدر تشريعًا مستقلاً مخصصًا لحماية وسائل الدفع الإلكتروني، بل تم تضمينها في بعض المواد القانونية في القانون المدني والقانون التجاري، إضافة إلى القواعد المتضمنة في القانون 09-04 والذي يشمل القواعد الخاصة بالوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، ونظرا لطبيعة المعاملات الإلكترونية التي اعتمدتها المنظومة الجزائرية فقد تم تعديل قانون العقوبات 15-04 المعدل والمتمم للأمر 66-156 وقد خصص القسم الثالث للجرائم الإلكترونية من المادة 349 مكرر 7، كما تجد عدة هيئات مسؤولة عن مكافحة الجريمة الإلكترونية بشكل عام، بما في ذلك الجرائم المتعلقة بوسائل الدفع الإلكتروني في الجزائر، [2]

وتتمثل فيما يلي:

1/- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: تم إنشائها بموجب القانون 04-09 المؤرخ في 05 أوت 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام

[1] السايس إبتسام، نيلي صفاء، (وسائل الدفع في التجارة الإلكترونية)، مذكرة لاستكمال متطلبات شهادة ماستر أكاديمي، جامعة قاصدي مرباح ورقلة، الجزائر، كلية الحقوق والعلوم السياسية، السنة الجامعية 2020/2019، ص 18، ص 19. .

[2] فريد مشري، آمنة قاجة، المزاودة رياض، (الحماية القانونية لوسائل الدفع الالكتروني – الجزائر نموذجا)، الملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي: ضرورة الانتقال وتحديات الحماية، 23 و24 أفريل، المركز الجامعي عبد الحفيظ بوالصوف، ميلة، الجزائر، ص 11، ص 12 .

والاتصال ومكافحتها، ومن بين مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني على الصعيدين الدولي والوطني، وإدارة وتنسيق عمليات الوقاية والمساعدة التقنية الموجهة للجهات القضائية والأمنية، كما يمكنها إجراء خبرات قضائية في حال وقوع اعتداءات على المنظومة المعلوماتية على نحو من شأنه تهديد مؤسسات الدولة، الدفاع الوطني، أو المصالح الاستراتيجية للاقتصاد الوطني .

2/- الهيئات القضائية الجزائية المتخصصة: أنشئت بموجب القانون 14/04 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 329، 30، 40 من قانون الإجراءات الجزائية، تتمتع باختصاص إقليمي موسع طبقا للمرسوم التنفيذي 348/06 المؤرخ في 2006/01/05، من مهامها النظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال التي تم ارتكابها في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني حسب المادة 15 من القانون 09/04 .

3/- المعهد الوطني للأدلة الجنائية وعلم الجرائم: يتكوّن من إحدى عشرة دائرة متخصصة في مجالات متعددة، جميعها تضمن تنفيذ الخبرة، والتكوين والتعليم، وتقديم المساعدة والدعم التقني، تُكلَّف دائرة الإعلام الآلي والإلكتروني بمعالجة وتحليل وتقديم الأدلة الرقمية التي يمكن أن تُفيد وتساعد العدالة، كما توفّر المساعدة التقنية للمحققين أثناء المعاينات .

4/- المديرية العامة للأمن الوطني: تتصدى هذه المديرية للجريمة الإلكترونية من عدة جوانب، من بينها الجانب التوعوي، حيث لم تغفل المديرية العامة للأمن الوطني عن أهمية الوقاية والتحسيس، وذلك من خلال برمجة دروس توعوية في مختلف المراحل الدراسية، بالإضافة إلى المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطنين حول خطورة الجرائم الإلكترونية .
ومن خلال ما سبق، يتبيّن أنه رغم اعتماد الدفع الإلكتروني في الجزائر، إلا أن المشرّع الجزائري لم يصدر بعد قوانين واضحة وصريحة تنظّم استخدام هذه الوسائل وتحدد أساليب الحماية القانونية المرتبطة بها .[1]

الفرع الثاني: وسائل الحماية من جريمة الاحتيال في التجارة الإلكترونية

[1] فريد مشري، آمنة قاجة، المزاودة رياض، المرجع السابق، ص 12 .

إن الجرائم المرتبطة بالتجارة الإلكترونية أصبحت تشكل تهديدًا واضحًا للاقتصاد الوطني والعالمي، مما يستدعي توحيد الجهود لتوفير آليات فعالة للحماية، فقد بات من الضروري حماية هذه البيئة الرقمية لما تحمله من مخاطر تتمثل في النصب والاحتيال الذي يستهدف بدرجة كبيرة مستخدميها، كما أن تعدُد وسائل الدفع يزيد من احتمال الاستغلال، وهو ما يجعل المستهلك الحلقة الأضعف، ما يحتم حمايته بوسائل قانونية وتقنية فعّالة .

أولا/- التشفير الإلكتروني: يُعد التشفير وسيلة تقنية مهمة تُستخدم لتأمين البيانات عند الدفع الإلكتروني، فهو يمنع تسرب المعلومات الحساسة كالرموز السرية والأرقام إلى جهات غير مخولة، ويتم ذلك عبر تحويل البيانات إلى رموز غير مفهومة لمن لا يملك مفتاح فك التشفير.

من خلال هذه التقنية يمكننا التغلب على العديد من المخاطر وتجاوزها، والتي من خلالها يمكننا تجنب:

- الوصول إلى المعلومات المحظورة والشخصية.
- محاولة تفعيل البيانات المنقولة على الشبكة.
- إعادة توجيه البيانات إلى جهة أخرى.
- تغيير محتويات الرسائل المتبادلة.
- تغيير كلمة مرور المستفيدين.
- انتحال شخصية المستخدم الحقيقية.[1]

ثانيا/- الرقم السري والكلمات السرية: يعتبر حماية الرقم السري من أبرز الإجراءات التي توفر الحماية للمستخدم في العصر الرقمي الحديث، وإجراءات فتح النافذة واستعمال الرقم السري يسمح لصاحب البرامج التأكد من هوية المستعمل الذي يحاول الدخول إلى العنوان الالكتروني أو جزء منه، وذلك عند محاولة الدخول إلى النظام الإلكتروني أو فتح نافذة معينة، وعند محاولة الوصول إلى نافذة آمنة، يجب إدخال كلمة مرور صحيحة لتأمين العمليات وضمان عدم تسريب البيانات الشخصية . يعد استخدام كلمات المرور من أبسط وأسهل الوسائل من حيث التكلفة، ولضمان فعالية هذا الأسلوب،[2] ينبغي توعية المستخدمين بضرورة عدم مشاركة كلمة المرور مع أي شخص، مع إلزامهم بتغييرها

[1] شرفي كميليلة، فريفرة دنيا، (الحماية القانونية لوسائل الدفع الإلكتروني)، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون خاص، جامعة بلحاج بوشعيب لولاية عين تموشنت، الجزائر، كلية الحقوق، السنة الجامعية 2023/2022، ص 28 و29 .

[2] واقد يوسف، (النظام القانوني للدفع الإلكتروني)، مذكرة لنيل درجة ماجستير في القانون، فرع القانون العام، تخصص قانون التعاون الدولي، جامعة مولود معمري تيزي وزو، الجزائر، كلية الحقوق، مدرسة دكتوراه للعلوم القانونية والسياسية، سنة 2011، ص 153 .

بشكل دوري، كما يجب تشفير كلمات المرور في الملفات المخصصة لتخزينها على الحاسوب، وعدم عرض حروفها أثناء إدخالها لتفادي كشفها من قبل المتطفلين.[1]

ثالثا/- التوقيع الإلكتروني: هو مجموعة من المعلومات التي يتم تضمينها إلكترونيا أو التي ترتبط بها منطقيا والتي تستخدم لتحديد هوية الموقع وتصدق على موافقته.[2]

كما أن المشرع الجزائري فقد عرف التوقيع الإلكتروني من خلال ما نصت عليه المادة 03 فقرة 02 من المرسوم التنفيذي رقم 162/07 على أنه "التوقيع الإلكتروني المؤمن يفي بالمتطلبات الآتية:

- يكون خاص بالموقع .
- يتم إنشاءه بوسائل يمكن أن يحتفظ بها المقع تحت مراقبته الحصرية .
- يضمن مع الفعل المرتبط به تلك الصلة التي توجب كل تعديل لاحق للفعل قابلا الكشف عنه .[3]

يندرج الهدف من التوقيع الإلكتروني تحت إطار الأمن والسلامة الرقميين، وعند التحقق من صحته فإنه بالطبع يحقق جميع الجوانب العملية والأهداف المرجوة منها وذلك لعدة أهداف قانونية بحتة تهدف إلى إبعاد المتطفلين عن التلصص وسرقة البيانات .[4]

رابعا/- التصديق الإلكتروني: يعتبر عامل السرعة والثقة من أبرز مزايا المعاملات الإلكترونية، مما جعل الحاجة إلى آلية تضمن صحة هذه المعاملات ضرورية. ولهذا السبب، تم إنشاء سلطة محايدة التي تساعد على تأمين هذه المعاملات والتأكد من هوية الأطراف المتعاملة فغالبا ما يجهل التجار هوية المتعاملين معهم وصحة بياناتهم، لذا تم العثور على جهة تسعى إلى تحمل عبء التحقق من شخصية المقاولين وبياناتهم من خلال إصدار شهادات التصديق الإلكتروني، كما قد نظم المشرع الجزائري هيئة المصادقة الإلكترونية وحدد مهامها والنظام القانوني في القانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني، بينما خص القانون 05/18 بتنظيم التجارة الإلكترونية .[5]

خامسا/- البصمة الإلكترونية: هي بصمات منقولة رقميا لضمان تأكيد الاتصال وصحة صدور المعلومة لحماية البيانات من الاحتيال والسرقة الإلكترونية، وتعتبر وسيلة هامة لحفظ المعلومات.

---

[1] واقد يوسف، المرجع السابق، ص 153 .
[2] شرفي كميليلة، فريفرة دنيا، المرجع السابق، ص 26 .
[3] السايس إبتسام، نيلي صفاء، المرجع السابق، ص 67 .
[4] واقد يوسف، المرجع السابق، ص 155 .
[5] شرفي كميليلة، فريفرة دنيا، المرجع السابق، ص 26 .

سادسا/- استخدام المواقع الوسيطة: تم اللجوء إلى فكرة الموقع الوسيط أو الشخص الوسيط في العلاقة وهي جهة تؤكد صحة التعامل على الخط، وهي شركات ناشطة في ميدان الخدمات التقنية تقوم بتقديم شهادات تتضمن تأكيد أن الطلب قد صدر عن الموقع المعني وتحدد تاريخ ووقت صور الطلب، حيث استطاعت الشركات التقنية أن توفر وسائل ومعايير فاعلة في قل أمن الشبكة إلا أنها ليست آمنة بالقدر الكافي.[1]

المطلب الثاني: حماية البيانات والمستهلك في التجارة الإلكترونية

تقوم المعاملات الإلكترونية في الغالب على بيانات شخصية يرسلها المستهلك الإلكتروني للتاجر بهدف اتمام عملية البيع الإلكتروني مثل هذه المعلومات، البيانات الاسمية، الإقامة، والموقع وغيرها من المعلومات التي يريد المستهلك غيره الاطلاع عليها لذلك قد يستغل التاجر هذه المعلومات والبيانات دون إذن صاحبها، كما أن الإعلان التجاري هو الأخير مظهر من مظاهر المنافسة المشروعة أي عامل من عوامل تسويق المنتجات والخدمات وإعلان جمهور المستهلكين بها وقد يتم بصور تقليدية إلكترونية، كالتلفزيون والراديو وقد يكون بوسائل إلكترونية مستحدثة وهي الانترنيت والتي أصبحت تشهد انتشارا واسعا ولكن قد يشوب البعض الغموض والتزييف، لذا سنتطرق في هذا الصدد حماية البيانات الشخصية في التجارة الإلكترونية (الفرع الأول) وحماية المستهلك من الإعلانات التجارية الكاذبة والخادعة (الفرع الثاني).

الفرع الأول: حماية البيانات الشخصية في التجارة الإلكترونية:

جعل المشرع الجزائري حماية المعطيات الشخصية التزام ملقى على عاتق المورد الإلكتروني في مواجهة المستهلك الإلكتروني ورتب مسؤوليته عند الإخلال بها، فيمكننا تعريف المورد الإلكتروني بأنه:

أولا: تعريف المورد الإلكتروني :

1-التشريع المصري: عرف قانون المستهلك المصري رقم 181 لسنة 2018 في المادة الأولى فقرة 5 منه المورد بأنه: "كل شخص يمارس نشاطا تجاريا أو صناعيا أو مهنيا أو حرفيا يقدم خدمة للمستهلك، أو ينتج سلعة أو يصنعها أو يستوردها، أو يصدرها أو يبيعها أو يؤجرها أو يعرضها أو يتداولها أو يوزعها أو يسوقها، وذلك بهدف تقديمها إلى المستهلك أو التعامل أو التعاقد معه بأي طريقة من الطرق بما في ذلك الوسائل الإلكترونية وغيرها من الوسائل التقنية الحديثة .[2]

[1] حياة هرلكي، المرجع السابق، ص 58 .
[2] انظر المادة 01، القانون رقم 181 لسنة 2018، بشأن حماية المستهلك المصري .

2-التشريع الجزائري: بصدور القانون رقم 18-05 أطلق المشرع الجزائري تسمية المورد الإلكتروني على البائع المحترف عبر الأنترنت وهي تسمية جديدة لم تكن منصوص عليها في القوانين السابقة، حيث عرفت المادة 06 فقرة 4 المورد الإلكتروني على أنه: "المورد الإلكتروني كل شخص طبيعي أو معنوي يقوم بتسويق أو اقتراح توفير السلع أو الخدمات عن طريق الاتصالات الإلكترونية "[1].
ومن خلال هذا التعريف يتضح أن الأمر يتعلق بكل شخص طبيعي أو معنوي يقوم بعرض وترويج بضائعه أو خدماته باستعمال الوسائل الحديثة .

بما أننا في إطار التجارة الإلكترونية فإن المورد الإلكتروني يعرض السلع عبر مواقع الأنترنت وهذا لجذب واستقطاب المستهلكين، فيعتمد المور الإلكتروني على الإشهار الإلكتروني[2] كونه الدعامة الأساسية لممارسة التجارة الإلكترونية والترويج للسع والخدمات .

كما أن المشرع الجزائري قد أشار في نص المادة 06 فقرة 4 الى طريقة عرض السلع: "عن طريق الاتصالات الإلكترونية"، والتي عرفتها المادة 10 فقرة 1من القانون رقم 18-04 على أنه "الاتصالات الإلكترونية كل ارسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات مهما كانت طبيعتها، عبر الألياف البصرية أو بطريقة كهرومغناطيسية"[3].

فيمكن القول أن المشرع الجزائري يعتبر المورد الإلكتروني كل من له علاقة بالتسويق أو اقتراح السلعة أو خدمة معينة عن بعد .

ومن التزامات المورد الإلكتروني ضمان احترام مبادئ معالجة المعطيات الشخصية، ونجد المعالجة أساسها القانوني في المادة 26 من قانون التجارة الإلكترونية التي تسمح للمورد بجمع المعطيات الشخصية ذات الطابع الشخصي فهي نوع من المعلومات التي تتعلق بالشخص الطبيعي دون المعنوي وترتبط به بشكل مباشر أو غير مباشر فتعرفه أو تجعله قابلا للتعريف وذلك بغض النظر عن شكلها أو نوعها .

وهو تعريف واسع يدخل في مضمونه مجموعة كبيرة من المعطيات، من بينها ما اتفق الفقه والقضاء بأنها تتمتع بالحماية دون أدنى شك كبيانات التعريف المباشرة للأشخاص وهي الاسم واللقب والصورة (ثابتة أو متحركة) بحيث تسمح لنا بالتعرف عليهم بالتأكيد وكذا بيانات التعريف التي لا تكشف

[1] انظر المادة 06، القانون رقم 18-05، المتعلق بالتجارة الالكترونية .
[2] انظر المادة 06 فقرة 06، القانون 18-05 المتعلق بالتجارة الالكترونية "الاشهار الالكتروني كل اعلان يهدف بصفة مباشرة أو غير مباشرة إلى ترويج بيع سلع أو خدمات عن طريق الاتصالات الالكترونية"
[3] انظر المادة 10، القانون رقم 18-04، مؤرخ في 24 شعبان 1439، الموافق ل10مايو 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية، العدد27، الصادرة في 13مايو 2018 .

أو تحدد بشكل مباشر هوية الشخص الذي تنطبق عليه، ولكنها مرتبطة به في سياق معين، يتضمن بيانات رقم الهاتف أو الضمان الاجتماعي، والعنوان الجغرافي، ولوحة الترخيص أو بصمات الأصابع، وعنوان البريد الإلكتروني وتاريخ الميلاد .[1]

فعملية جمع المعطيات الشخصية التي يقوم بها المورد الإلكتروني تدخل في نطاق القانون 18-07 ذلك أن العمليات التي تندرج في إطار مفهوم المعالجة متنوعة وتتراوح من جمع البيانات إلى اتلافها، فأي أجزاء يمكن القيام به يتعلق بالبيانات الشخصية واستخدامها يقع ضمن تعريف "المعالجة" والهدف من ذلك هو حماية الأفراد من اللحظة التي فيها جمع البيانات المتعلقة بهم وتسجيلها، وبالتالي فقد حرص المشرع على تضمين فكرة المعالجة عند تطبيق أي عملية على المعطيات الشخصية .

كما ألزمت المادة 26 من القانون 18-05 المورد الإلكتروني بمجموعة من الالتزامات هي:

1-ألاّ يجمع إلاّ البيانات الضرورية لإبرام المعاملات التجارية، أي ان يقتصر على الحد الأدنى من المعطيات الشخصية والضروري لغرض إبرام عقد التجارة الإلكترونية، وهو ما يتفق على مبدأ تحديد الغرض ومبدأ تقليل البيانات، فلا يسمح له أن يطلب رقم البطاقة المصرفية مع أن الدفع سيكون عند التسليم، كما لا يسمح له بجمع المعلومات الخاصة بالميولات الاستهلاكية وغيرها . [2]

2- أن يقوم المور الإلكتروني بإعلام المستهلكين بالبنود المتعلقة بحماية المعطيات ذات الطابع الشخصي لتمكينهم من الموافقة عليها، ولا يمكن أن تتّم عملية جمع المعطيات الشخصية للمستهلك إلاّ بعد أن يتلقى هذه البيانات ويواف عليها صراحة[3]، وكل تغيير في الشروط بعد الموافقة يستدعي رضا جديد، فالموافقة هي المبدأ الأساسي لعملية معالجة البيانات الشخصية .

3- يلتزم المورد بضمان أمن نظم المعلوماتية وسرية البيانات، فأمن المعطيات يتعلق بالمحافظة عليها من الفقدان أو الضياع أو التخريب بأي وسيلة من الوسائل، أو مشاركتها من طرف ثالث بأية صورة كانت، ويكون ذلك بوضعه للتدابير التقنية والتنظيمية الملائمة لحماية المعطيات [4].

---

[1] علال نزيهة، عاشور فاطمة، (الحماية القانونية للمعطيات الشخصية في معاملات التجارة الالكترونية)، دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي عبدالله مرسلي تيبازة، الجزائر, العدد02، المجلد06، 2022، ص181

[2] سهام قارون، (التزام المورد الالكتروني بحماية المعطيات الشخصية للمستهلك)، مجلة الباحث والدراسات الاكاديمية، سوق اهراس ,الجزائر ,المجلد07، 2020 , ص 1020.

[3] انظر المادة 26، من القانون 15-08، المتعلق بالتجارة الالكترونية .

[4] انظر المادة 38 من القانون 18-07 المؤرخ في 25 رمضان عام 1439 الموافق ل10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعين في مجال معالجة المعطيات الشخصية ذات الطابع الشخصي

4-ألزمت التشريعات القانونية والتنظيمية المورد الإلكتروني بضرورة الالتزام بالأحكام التي تنظم معالجة البيانات ذات الطابع الشخصي، فطبقا لأحكام القانون 18-07 يشترط الحصول على ترخيص مسبق من السلطة المختصة لمعالجة أي بيانات شخصية، ولا يجوز مباشرة هذه العملية بدون اشعار السلطة الوطنية المختصة أو الحصول على الموافقة المسبقة حسب الحالة، كما يُلزم القانون المورد الإلكتروني بضمان أن تتم معالجة البيانات الشخصية بطريقة مشروعة، نزيهة، وملائمة للغرض الذي جمعت من اجله، دون الاحتفاظ بها لمدة تتجاوز ما هو ضروري لتحقيق ذلك الغرض، ويجب أن تحفظ هذه البيانات بطريقة تضمن عدم المساس بهوية الأشخاص المعنيين . [1]

ثانيا: جزاء مخالفة المورد الإلكتروني لالتزامه بحماية المعطيات الشخصية

باعتبار أن المورد الإلكتروني هو المسؤول عن تخزين المعلومات ومعالجتها فهو ملزم باتخاذ كافة الإجراءات المناسبة لحمايتها، وفي حال اخلاله بهذه الالتزامات او انتهاكه لحقوق الشخص موضوع المعالجة فإنه يتحمل المسؤولية الجزائية والمدنية الى جانب العقوبات الإدارية التي تصدرها اللجنة الوطنية لحماية المعطيات الشخصية [2].

1-الجزاءات التي تفرضها الجهات الإدارية

عمل المشرع على إقرار وجود سلطات إدارية تسهم الى جانب الجهات القضائية، في السهر على حماية المعطيات الشخصية وكذا حماية حقوق المستهلك، ومنح هذه الهيئات صلاحية توقيع بعض العقوبات الإدارية على المخالفين من المسؤولين .

وقد منح المشرع السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي سلطة اتخاذ مجموعة من الإجراءات التصحيحية ضد مراقبي البيانات والتي تتراوح من الإنذار البسيط الى حظر العلاج، وتكون قراراتها قابلة للطعن امام مجلس الدولة وفقا للتشريع المعمول به[3] .

كما يمكن ان تصدر غرامة محددة ب500، 000 دج ضد المسؤول عن المعالجة التي يرفض، دون سبب شرعي، حقوق الشخصي المعني المتعلقة بالإعلام والولوج او التصحيح أو الاعتراض المنصوص عليها في المواد 32و34و35و36 من القانون 18-07 (المادة 47)، أما في حالة العود فتطبق العقوبات الجزائية المتعلقة بالحبس الذي قد يصل الى سنتين أو بالغرامة التي قد تصل كحد أعلى 200.000دج (المادة 64) .

[1] انظر المواد 12 الى 21 من القانون 18-07، السابق الذكر.
[2] علال نزيهة، عاشور فاطمة، المرجع السابق، ص 188.
[3] انظر المادة 46، من القانون 18-07، السابق الذكر.

هذا وقد منح المشرع للإدارة المكلفة بحماية المستهلك صلاحية فرض غرام الصلح على المورد الإلكتروني الذي يخالف التزاماته المنصوص عليها في القانون 18-05 المتعلق بالتجارة الإلكترونية، من بينها المخالفات المتعلقة بإخلاله بالتزاماته المتعلقة بحق المستهلك الإلكتروني في الاعلام المسبق بالبنود المتعلقة بحماية المعطيات الشخصية، وكذا الخاصة بإخلاله بضوابط الاشهار الإلكتروني، مالم يكن في حالة العود، ويكون مبلغ غرامة الصلح هو الحد الأدنى للغرامة [1].

2-الجزاءات المنصوص عليها في القانون 18-05 المتعلق بالتجارة الإلكترونية

يعاقب على مخالفة التزام المورد الالكتروني بالإعلام المسبق بالبنود المتعلقة بحماية المعطيات الشخصية بغرامة قد تصل إلى 500.000دج وإمكانية تعليق نفاذه الى منصات الدفع الإلكتروني لمدة لا تتجاوز 6أشهر (المادة 39).

يعاقب بغرامة من 50.000 إلى 500.000دج المورد الالكتروني الذي يقوم باستغلال المعطيات الشخصية للمستهلكين في الاشهار الإلكتروني غير المرغوب فيه بدون موافقة المستهلك الإلكتروني، أو عدم تمكنه من الاعتراض على الرسائل الاشهارية الموجهة اليه، أو الاستمرار في ارسال رسائل الاستبيان المباشر رغم معارضة المستهلك (المادة 40).

3-الجزاءات المنصوص عليها في القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

نص القانون 18-07 في الفصل الثالث بعنوان الاحكام الجزائية، من الباب السادس المتعلق بالأحكام الإدارية والجزائية، على عدة انتهاكات يمكن أن ترتب عقوبة الحبس الذي قد يصل الى 5 سنوات، والغرامة التي قد تصل إلى 1.000.000 دج، مع إمكانية تطبيق العقوبات التكميلية التي ينص عليها قانون العقوبات، والحكم بمصادرة محل الجريمة، كما يعاقب على محاولة ارتكاب إحدى الجنح المنصوص عليها في هذا القانون بنفس العقوبة للجريمة التامة، وفي حالة العود تضاعف العقوبات وذلك نذكر اهمها فيما يلي:

يعاقب المسؤول عن معالجة المعطيات الشخصية بالحبس من سنتين الى خمس سنوات وبغرامة من 200.000 إلى 500.000دج في حالة معالجة المعطيات الشخصية بدون احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، أو المساس بحقوق الأشخاص وشرفهم وسمعتهم (المادة 54).

[1] انظر المادة 47،46،45 من القانون 18-05، السالف الذكر.

ويعاقب على القيام بمعالجة المعطيات الشخصية بدون الحصول على الموافقة المسبقة والصريحة للشخص المعني أو المعالجة رغم المعارضة أو الرجوع عن الموافقة، أو في حال استهداف المعالجة الاشهار التجاري رغم اعتراض الشخص المعني، بالحبس من سنة الى ثلاث سنوات وبغرامة من 100.000دج الى 300.000دج (المادة55) .

ويعاقب على معالجة المعطيات الشخصية دون الحصول على تصريح أو ترخيص أو مواصلة المعالجة رغم اعتراض السلطة الوطنية او بعد سحب وصل التصريح او الترخيص من طرف السلطة الوطنية بالحبس من سنتين الى خمس سنوات وبغرامة من 200.000 الى 500.000دج (المادة 56) .

كما يعاقب على المعالجة لأغراض غير مصرح بها بغرامة قد تصل الى 300.000دج وبالحبس من سنة الى ثلاث سنوات (58).

وكما يعاقب على جمع المعطيات الشخصية بطرق تدليسيه او غير نزيهة او غير مشروعة، بالحبس من سنة من ثلاث سنوات وبغرامة من 100.000 الى 300.000دج (المادة 59).

ويعاقب على عدم وضع التدابير التقنية والتنظيمية والتقنية الملائمة لحماية المعطيات من التلف او الإتلاف او النشر او الولوج غبر المرخصين، بغرامة من 200.000 الى 500.000دج (المادة 65).[1]

الفرع الثاني: حماية المستهلك من الإعلانات التجارية الكاذبة والمضللة

للغش طرق وأساليب كثيرة، لكن اخطرها على الاطلاق ذلك الذي يتم بواسطة الإعلانات الكاذبة والمضللة خاصة ذلك الذي يبث عبر الانترنت، لأنه كثيرا ما يشمل فيها الكذب والتضليل مصحوب بأساليب إبهار وإغواء ومؤثرات، ولذا سنقوم بتعريف الإعلان الكاذب أو المضلل .

أولا: تعريف الإعلان الكاذب أو المضلل

الإعلان الكاذب او المضلل فهو الذي: "يتضمن معلومات مغلوطة تجعل المستهلك يحصل على معلومات خاطئة فيما يتعلق بعناصر أو أوصاف أو خصائص أو آثار المنتج المعلن عنه، وذلك من خلال أساليب الخداع في الرسالة الاعلانية لغرض تضليل المستهلك والعمل على إقناعه بشراء منتج ما، وهذا بالتركيز على مختلف أساليب الاغراء الموجودة في الإعلان، واثارة التصرفات الانفعالية غير الرشيدة التي تؤثر على اذواق المستهلكين".

[1] انظر المادة 65،59،58،56،55 من القانون 18-07، السالف الذكر.

كما عرق الإعلان التجاري المضلل بأنه: "الإعلان الذي يكون من شأنه خداع المستهلك، أو يمكن أن يؤدي الى ذلك".

وفي تعريف آخر: "الاعلام المتضمن معلومات تهدف الى الوقوع في خلط او خداع، فيما يتعلق بعناصر أو اوصاف جوهرية للمنتج".

فالإعلان التجاري المضلل هو الذي يؤدي الى خداع المستهلك من خلال تضمنه معلومات مغلوطة حول عناصر أو اوصاف جوهرية في المبيع .

وهو أيضا" ذلك الذي وبأي وسيلة كانت يتناول سلعة أو خدمة، يتضمن عرضا أو بيانا أو ادعاء كاذبا، او انه مصاغ بعبارات من شأنها أن تؤدي بطريقة مباشرة أو غير مباشرة الى خداع أو تضليل المستهلك". [1]

غير أن التضليل ليس حتما مرادفا للكذب، فالكذب يؤدي الى تضليل الضحية، لكن التضليل قد يحدث حتى دون كذب، فالكذب هو تزييف للحقيقة، وذل بالإخبار عن شيء بخلاف ما هو عليه في الواقع، والأصل في الكذب أنه فعل عمدي يقوم على إخفاء الحقيقة أو تزييفها بهدف تضليل الضحية وهو هذا المعنى يتألف من عنصرين، مادي بتزييف الحقيقة، أي المضمون الكاذب، ومعنوي هو نية الغش [2].

أما التضليل فهو خداع المستهلك دون ذكر معلومات كاذبة، فالإعلان صادق من حيث البيانات التي يذكرها، لكنه يصاغ في عبارات أو يقدم بطريقة من شأنها أن تخدا المستهلك .

وقد يلجأ القضاء غالبا إلى التسوية بين الإعلان المضلل في خد ذاته والاعلان الذي يؤدي الى التضليل، علما ان التفرقة بينها أمر في غاية الصعوبة، والعلة هي أن الإعلان المضلل يمكن اسناد تقديره الى معيار موضوعي، في حين ان الإعلان الذي يؤدي الى التضليل يقوم على معيار ذاتي أو شخصي[3] .

[1] هلال شعوة، (حماية المستهلك من جريمة الإعلان التجاري المضلل أو الكاذب)، دراسات قانونية، كلية الحقوق جامعة عنابة، الجزائر، العدد1, مجلد1 ، ص12.
[2] المرجع نفسه، ص 13.
[3] محمد عبد القدوس المصري، (الإعلان الكاذب والمضلل -الماهية والاركان القانونية-)، مجلة البحوث الفقهية والقانونية، جامعة الأزهر،القاهرة, مصر, العدد 42، يوليو 2023، ص 2424 .

ثانيا: العقوبات المقررة للحماية من الإعلان الكاذب والمضلل

الاشهار التضليلي أو الإعلان الكاذب من الممارسات التجارية الغير نزيهة وتأخذ وصف جنحة، ويعاقب على جريمة العلان الكاذب أو المضلل بنص المادة 38 من القانون 04-02 بغرامة مالية التي قدرها من خمسين الف دينار (50000) إلى خمس ملايين دينار (5.000.000) كعقوبة أصلية [1].

وتنص المادة 69 من قانون المستهلك الجديد: "ترفع العقوبات المنصوص عليها في المادة 68 أعلاه إلى خمس سنوات (5) وغرامة قدرها خمس مائة ألف دج (500000) إذا كان الخداع أو محاولة الخداع قد ارتكبت سواء بواسطة:

- إشارات تدليسيه أو ادعاءات تدليسيه .
- كتيبات او منشورات أو نشرات أو معلقات أو إعلانات أو بطاقات أو أية تعليمات أخرى".

كما أضاف المشرع إمكانية أن يحكم القاضي بمصادرة السلع المحجوزة حيث أنه إذا كانت المصادرة تتعلق سلع كانت موضوع حجز عيني حيث بينت الفقرة 02 من المادة 44 من القانون 04-02 السلع التي تسلم الى إدارة أملاك الدولة التي تقوم ببيعها وفق الشروط المنصوص عليها في التشريع والتنظيم المعمول به .

وكعقوبة تكميلية أخرى لجريمة الاشهار التضليلي أضاف المشرع إمكانية أن يأمر القاضي المحكوم عليه نهائيا في هذه الجريمة بنشر القرار القضائي كاملا، وخلاصة منه في الصحافة الوطنية أو لصقه بأحرف بارزة في الأماكن التي يحددها، وذلك علة نفقة مرتكب جريمة الاشهار التضليلي، وفقا لنص المادة 48 من القانون 04-02 .[2]

ولقد كيّف أيضا قانون التجارة الإلكترونية رقم 18-05 جريمة الاشهار الالكتروني الغير مرغوب فيه على أساس جنحة وذلك بموجب المادة 40 منه، وأفرد له عقوبة مالية تتراوح بين 50.000دج إلى 500.000 دج، أما في حالة العود فتضاعف العقوبة حيث تصبح غرامة من 100.000 دج إلى 1.000.000دج .[3]

كما أجاز قانون التجارة الإلكترونية المصالحة في الجرائم المتعلقة بالإشهار الإلكتروني غير المشروع عامة والتي من بين صورها الاشهار الالكتروني غير المرغوب فيه، حيث ان القاعدة العامة

[1] انظر المادة 38 من القانون رقم 02.04 المؤرخ في 23يونيو 2004، المحدد للقواعد المطبقة على الممارسات التجارية، المعدل والمتمم.
[2] انظر المواد 44 و48 من القانون 04-02، المحدد للقواعد المطبقة على الممارسات التجارية المعدل والمتمم.
[3] انظر المادة 40، من القانون 18-05، المتعلق بالتجارة الالكترونية .

في تحديد غرامة الصلح في قانون التجارة الإلكترونية هي الحد الأدنى لعقوبة الغرامة المقررة للجريمة، وهو ما نصت عليه المادة 46 من نفس القانون، وعليه فإن غرامة الصلح في جريمة الاشهار الإلكتروني غير المرغوب فيه تساوي 50.000دج. [1]

كما منح المشرع الوطني للمورد الإلكتروني الذي قبل بغرامة الصلح المقترحة من طرف الإدارة المعنية (مصالح التجارة) بتخفيض في غرامة الصلح قدره 10 بالمئة .

[1] انظر المادة 46 من القانون 18-05، المتعلق بالتجارة الالكترونية .

المبحث الثاني: الإجراءات الردعية للاحتيال في التجارة الإلكترونية

بعد التطرق في المبحث الأول إلى الإجراءات الوقائية التي تهدف إلى الحد من الاحتيال في التجارة الإلكترونية، من خلال حماية وسائل الدفع والبيانات والمستهلك، يأتي هذا المبحث ليتناول الجانب الردعي من خلال الآليات القانونية التي تهدف إلى التصدي الفعلي لهذه الجرائم، فمكافحة الاحتيال لا تكتمل دون إجراءات فعالة للتصدي لهذه الجريمة، وعليه سيتم التطرق في هذا المبحث إلى أهم الآليات الإجرائية لمكافحة جرائم الاحتيال المتعلقة بالتجارة الإلكترونية **(المطلب الأول)** تليها الحماية الجزائية للتجارة الإلكترونية في مرحلة المحاكمة **(المطلب الثاني)** .

المطلب الأول: الآليات الإجرائية لمكافحة جريمة الاحتيال في بالتجارة الإلكترونية

تعد الآليات الإجرائية من أهم الأسس في مكافحة الاحتيال في التجارة الإلكترونية، بحيث تتطلب طبيعة هذه الجرائم التقنية إلى تبني إجراءات فعالة ومتطورة، بالإضافة إلى تحديثها بما يتناسب مع تطور وسائل الاحتيال الإلكتروني .

سنتناول في هذا المطلب أهم الإجراءات التي تم اعتمادها لمكافحة الاحتيال الإلكتروني في التجارة الإلكترونية، بدءا بإجراءات البحث والتحري (الفرع الأول)، يليها مرحلة التحقيق الابتدائي

(الفرع الثاني)، وبعدها ننتقل إلى مرحلة التحقيق الابتدائي (الفرع الثالث) .

الفرع الأول: إجراءات البحث والتحري

تعد مرحلة البحث والتحري هي مرحلة جمع الاستدلالات، والتي هي موكلة إلى ضباط الشرطة القضائية، وفي مجال جرائم التجارة الإلكترونية منحهم القانون عدة سلطات واختصاصات متنوعة للتحري عن الحقيقة، ونظرًا لما تحدثه هذه الجرائم من إشكالات قانونية، يصعب على أعوان الشرطة القضائية التعامل معها ومواجهتها، وذلك راجع إلى نقص خبرتهم في هذا المجال، مما أدى إلى إنشاء ضباط شرطة قضائية متخصصة .

أولا/- الأشخاص المؤهلون لمكافحة الاحتيال في التجارة الإلكترونية:

مع تزايد الجرائم الإلكترونية، وخاصة في مجال التجارة الإلكترونية وما يترتب عنها من خسائر فادحة، قررت العديد من الدول تكوين أجهزة لمكافحة هذا النوع من الجرائم، ومن بينها إنشاء شرطة[1]

[1] رزيقة بودودة، (الحماية الجنائية للتجارة الإلكترونية)، مذكرة تكميلية لنيل شهادة الماستر، شعبة الحقوق، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي –ام البواقي-، الجزائر، كلية الحقوق والعلوم السياسية، السنة الجامعية 2015/2014، ص 44، ص45 .

متخصصة سواء على المستوى الوطني أو الدولي، وهذا حسب ما نصت عليه الاتفاقية الأوروبية لجرائم الأنترنت، والمؤتمر المنعقد في السوربون بباريس في 2005/01/19 .

وهذه الأجهزة تسمى "بشرطة الأنترنت" وهي عبارة عن ضبطية قضائية من مهامها جمع الاستدلالات والتحري في العالم الافتراضي عن الجريمة الإلكترونية .

ولذا قررت بعض التشريعات على ضرورة تكوين أجهزة متخصصة لمكافحة جرائم التجارة الإلكترونية، ومن بين هذه التشريعات الأجنبية والعربية نجد الجزائر .

1/- التشريع الجزائري:

نجد أن المشرع الجزائري لم يقم بإنشاء هيئات خاصة لمكافحة جرائم التجارة الإلكترونية وإنما استحدث هيئة وطنية للوقاية من الجرائم الإلكترونية فقط، وذلك بموجب القانون رقم 04/09 المتعلق بجرائم الاتصال والمعلومات ومكافحتها طبقا لما نصت عليه المادة 13 و14 منه، ومن مهام هذه الهيئة تنشيط وتنسيق عمليات الوقاية من جرائم الاتصال والمعلومات ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات عن هذه الجرائم، بما فيها تجميع المعلومات وإنجاز الخبرات القضائية بهدف كشف مرتكبي هذه الجرائم الإلكترونية .

ثانيا/- السلطات المخولة للضبطية القضائية لمكافحة جرائم التجارة الإلكترونية:

تمارس الضبطية القضائية عدة اختصاصات في حدود الصلاحيات المخولة لها قانونا للكشف عن وقوع الجريمة، وجمع الاستدلالات المتعلقة بها، وملاحقة مرتكبيها سواء كانوا فاعلين أصليين أم شركاء فيها، وذلك بمجرد تلقي أعوان الضبط القضائي بلاغا بشأن وقوع هذا النوع من الجرائم، بحيث يعد التبليغ هو أساس تحريك الدعوى العمومية، ويقصد به إعلام السلطات المختصة بوقوع الجريمة .

لقد شهد الضبط القضائي عبر الأنترنت قد تطورا بشكل هائل، حيث أصبح بإمكان مقدم البلاغ التوجه إلى موقع إلكتروني مخصص لتلقي البلاغات وكتابتها حول الجرائم ثم إرسالها إلى الجهات المختصة، مثال ذلك موقع حماية برمجيات الأوروبية، ويطلق على هذا النوع من الإبلاغ عبر شبكة الأنترنت "بالإبلاغ الرقمي"، حيث يتم ذلك بواسطة إرسال رسالة إلكترونية إلى عنوان البريد الإلكتروني، أو عن طريق ملء استمارة إلكترونية متاحة في موقع البلاغات والشكاوى الرسمية، وبذلك منح الحاسب صلاحيات أكبر في الاستدلال عن الجرائم برصد تحريات كاملة عن الواقعة ومرتكبيها[1] والمجني عليه، وبذلك يعد البلاغ محلا للبحث والتحري في حد ذاته ولا بد التأكد من صحته، ولا يشترط البلاغ أن يكون المبلغ معروف الهوية .

[1] راجع رزيقة بودودة، المرجع السابق، ص 45، ص 48، ص 50 .

كما يتلقى ضابط الشرطة القضائية الشكاوى عن بعض الجرائم المحددة حصرا والتي لا يجوز فيها تحريك الدعوى الجزائية إلا بعد تقديم شكوى من طرف المجني عليه، وتجدر الإشارة إلى أنه لا تختلف أحكام الشكوى في الجرائم التقليدية عن تلك المرتكبة بواسطة شبكة الأنترنت .

بعد الإبلاغ أو تقديم شكوى إلى الجهات المختصة عن وقوع الجريمة هنا تبدأ مرحلة جمع الأدلة، ويكمن دور الضبطية القضائية بجمع المعلومات التي تفيد التحقيق، فمرحلة التحري هي مرحلة تحضيرية تسبق مرحلة التحقيق، ويمكن اعتبار الأدلة من الإجراءات الضرورية في الجرائم المتعلقة بالتجارة الإلكترونية، وهي من صلاحيات المتحري عبر الأنترنت بواسطة التقنية الإلكترونية الرقمية، ولرجال الضبط القضائي كامل الحرية في اختيار الوسيلة الملائمة لإجراء التحري لجمع المعلومات وكشف الجريمة، ومن أهمها نظام الإرشاد الجبائي عبر الأنترنت، والذي يعد من أهم المصادر المعتمدة في التحري وجمع الأدلة، بالإضافة إلى مراقبة شبكة الأنترنت .

بالإضافة للاختصاص الأصيل للضبطية القضائية المتمثل في البحث والتحري توجد ظروف تستدعي تدخلا مباشرا وسريعا بغرض الحفاظ على الأدلة، لذلك أعطى المشرع لأعضاء الضبط القضائي صلاحية القيام ببعض إجراءات التحقيق، وذلك طبقا للحالات المنصوص عليها في المادة 14 من قانون الإجراءات الجزائية .

تجدر الإشارة إلى أن المشرع الجزائري قد أجاز إجراء المعاينة في الجرائم المعلوماتية المتلبس فيها طبقا لنص المادة 47 الفقرة 3 من قانون العقوبات الجزائية، والتي تنص على أنه عندما يتعلق الأمر بالجرائم الماسة بأنظمة معالجة الآلية للمعطيات فإنه يجوز إجراء معاينة في أي محل سكني في كل ساعة من ساعات النهار والليل بشرط الحصول على إذن مسبق من وكيل الجمهورية المختص لإثبات حالته، وضبط كل ما من شأنه كشف الحقيقة، فهي تتطلب الانتقال إلى محل واقعة إجرامية لمباشرتها أو الأصل في المعاينة أنها إجراء من الإجراءات .

إن حالات التلبس المنصوص عليها قانونا من الحالات التي يمكن لسلطة التحقيق القيام بها بنفسها أو بانتداب ضباط الشرطة القضائية للقيام بها، وبمقتضى ذلك تحرير محضر لها عن طريق كاتب، أما فيما يتعلق بكيفية إجراء المعاينة التقنية لمسرح الجريمة الإلكترونية، يكون عند العلم بوقوع الجريمة أول خطوة يقوم بها رجال الضبط القضائي الانتقال لمسرح الجريمة، ويمكن التعامل معه على أساس أنه[1] مسرحان، مسرح تقليدي ومسرح افتراضي يقع داخل بيئة إلكترونية، ومن الجدير بالذكر أنه يمكن لرجل الضبط القضائي القيام بالمعاينة وهو جالس في مكتبه من خلال الحاسوب الموضوع في المحكمة مثلا .

[1] رزيقة بودودة، المرجع السابق، ص 50، ص 51، ص 52 .

الفرع الثاني: مرحلة التحقيق الابتدائي

مرحلة التحقيق الابتدائي هي مرحلة لاحقة لمرحلة البحث والتحري ومجمل الإجراءات المتخذة في هذه المرحلة مخولة لقاضي التحقيق بهدف الحصول على الأدلة اللازمة التي من شأنا الكشف عن الحقيقة، وتسمى بإجراءات جمع الدليل، ومن بينها التفتيش والضبط والخبرة .

1/- التفتيش في مجال التجارة الإلكترونية:

يقصد بالتفتيش في إطار الجرائم الإلكترونية إجراء من الإجراءات التحقيق تباشره سلطة مختصة بقصد الدخول إلى أنظمة المعالجة الآلية للبيانات بما تشمله من تخزين ومخرجات، بهدف البحث فيها عن أفعال غير مشروعة تكون مرتكبة، وقد تشكل جناية أو جنحة أو التوصل من خلال ذلك إلى أدلة تساعد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها .

إن إجراءات التفتيش في جرائم الحاسوب تحتاج إلى مهارات وتقنيات خاصة لابد أن يتحلى بها قاضي التحقيق، فهي تختلف تماما عن حالات التفتيش العامة، لأن نظم المعلومات يصعب إجراء التفتيش فيها، الأمر الذي يفرض استخدام تقنيات خاصة، كما أن التفتيش المتعلق بمكونات الحاسوب يسهل إجرائه على المكونات المادية، وبالتالي نطبق عليه القواعد العامة للتفتيش، أما عندما يتعلق الأمر بالتفتيش عن المكونات الغير مادية للحاسوب فالتعامل معها يحتاج إلى معرفة كيفية تطبيق القواعد التقليدية عليها، ويرى البعض أن القواعد التقليدية للتفتيش تطبق على أدلة الجرائم التي يكون محلها برامج الحاسوب كالسرقة والإتلاف، واستعمال هذه الرامج كوسيلة لارتكاب هذه الجرائم، فهو من الأمور الصعبة لأنه يتم التخلص من البيانات المستهدفة للتفتيش من طرف الجاني بإرسالها لمكان آخر .

ما يمكن ملاحظته من نص المادة 45 من قانون الإجراءات الجزائية أن المشرع الجزائري قد أقر إمكانية تفتيش المنظومة المعلوماتية، كما نجد أن إجراءات التفتيش عن الجرائم الإلكترونية تختلف نوعا ما عن الجرائم التقليدية، حيث لا يستلزم حضور المشتبه فيه صاحب المسكن أثناء إجراء التفتيش عن الجرائم الإلكترونية، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني، وكذا جرد الأشياء وحجز المستندات، كما أجاز المشرع الجزائري بموجب القانون 09/04 حسب ما هو وارد في المادة 05 الدخول إلى منظومة معلوماتية أو منظومة تخزين كلها أو جزء منها، متى كان الهدف من ذلك تفتيش[1] المعطيات التي تم الاعتداء عليها متخذا جميع التدابير لحمايتها، طبقا للحالات المنصوص عليها في المادة 04 من نفس القانون .

[1] رزيقة بودودة، المرجع السابق، ص 53، ص 54 .

كما نجد المشرع الجزائري نص في المادة 06 من القانون 09-04 أنه قد خول للسلطات صلاحيات التفتيش عن معطيات مخزنة إذا كان من شأنها الكشف عن الجريمة، وليس شرط حجز كامل المنظومة المعلوماتية بل يكفي نسخ بعض المعطيات محل البحث فقط .

إن تفتيش نظم الحاسوب والأنترنت له عدة قواعد تحكمه منها القواعد الموضوعية، والقواعد الشكلية، ولتبيان القواعد الموضوعية لا بد ممن تحديد السبب الذي صدر من أجله أمر التفتيش، ومحل التفتيش، كما أن السبب في تفتيش نظم الحاسوب والأنترنت هو وقوع جريمة إلكترونية، والتي هي: "كل فعل غير مشروع مرتبط باستخدام الحاسوب لتحقيق أغراض غير مشروعة" .

أما محل التفتيش في مجال الجرائم الإلكترونية قد تشمل الشخص المتهم أو منزله أو شخص غير المتهم، وهو ويتم تنفيذ هذا الإجراء من طرف النيابة العامة أو قاضي التحقيق أو بتفويض منهم لأحد ضباط الشرطة القضائية، وذلك في حالة وجود أدلة تفيد بإدانة الشخص المراد تفتيشه بأنه قد ساهم في ارتكاب الجريمة بوصفه فاعلا أصليا أو شريكا، فضلا عن توفر قرائن كافية لوجود أشياء أو معدات معلوماتية يمكن أن تؤدي للكشف عن الحقيقة لدى المتهم، ويتمحور محل التفتيش على الحاسوب بكل مكوناته المادية والمعنوية، حيث يتمثل هدفه في ضبط هذه المكونات، والتي توجد حوة الشخص أو في مسكنه .

أما بخصوص الضوابط الشكلية لإجراء عملية التفتيش، فيستلزم تحديد أولا السلطة المختصة بالتحقيق، حيث اختلفت مجمل التشريعات العربية والأجنبية على تحديد هذه السلطة، فمثلا نجد في القانون المصري تعد النيابة العامة هي الجهة الأصلية المختصة بإجراء التفتيش، ويمنح لقاضي التحقيق هذا الاختصاص في حالات خاصة .

فضلا على إجراء التفتيش يستوجب الحضور الضروري لبعض الأشخاص المعنيين، وبالنسبة للميعاد الزمني لتنفيذ تفتيش نظم الحاسوب والأنترنت فقد اختلفت مجمل التشريعات بشأن التوقيت الزمني لتفتيش المسكن ليلا فبعض الدول سمحت بذلك، في حين منعت أخرى ذلك، أما المشرع الجزائري فقد سمح بإجراء التفتيش على المنظومة المعلوماتية في أي وقت طبقا للمادة 47 الفقرة الثالثة من قانون الإجراءات الجزائية .[1]

كما أن تفتيش نظم الحاسوب والأنترنت يشترط إذن قضائي، نظرا لما تحمله من قواعد تهدف لحماية الخصوصية وحقوق الأفراد، مع ضرورة أن يكون الإذن مكتوبا ومحدد التاريخ وموقعا من جهة إصداره، ولكي يكون التفتيش صحيحا لا بد أن يكون مصدر الإذن مختصا بالتحقيق في الجريمة، كما أن

[1] رزيقة بودودة، المرجع السابق، ص 54، ص 55 .

المعطيات الخاصة بالتجارة الإلكترونية تتطلب أيضا اتخاذ نفس إجراءات تفتيش نظم الحاسوب والأنترنت بهدف حمايتها .

2/- ضبط أدلة جرائم التجارة الإلكترونية:

حتى يتسنى لقاضي التحقيق من تنفيذ إجراء التفتيش لا بد من ضبط الأدلة، والتي يقصد بها التحفظ عليها وحجزها، إذ يمنح القانون لقاضي التحقيق صلاحية ضبط وحجز الأدلة والأشياء ووضعها في أحراز مختومة، إذا كانت هذه الأدلة من شأنها كشف الحقيقة، وعادة ما يكون الضبط مقترنا بالتفتيش الذي يسعى إلى ضبط ما يمكن أن يفيد في إظهار الحقيقة وكشفها، والهدف الرئيسي من ضبط الأشياء هو دعم التحقيق الجاري سواء كان هذا الشيء متعلق بأدوات استعملت في الجريمة أو شيئا نتج عنها قد يفيد في كشف الجريمة .

يرتبط ضبط الأدلة الإلكتروني غالبا بضبط المكونات المادية لأنظمة الحاسوب، وضبط المكونات المعنوية والبرمجيات، إضافة إلى ضبط المعطيات المتناقلة في نطاق شبكة المعلومات التي تساعد على ربط الحاسبات معا، ويجوز ضبط مكونات الحاسوب المادية كونها تعتبر من الأشياء، حيث يرى البعض أن اجراء الضبط لا يعد من إجراءات الاستدلال فقط، بل يشمل الضبط على الأشياء المادية والغير مادية، كما هو الحال في مراقبات المحادثات الهاتفية وتسجيل المحادثات الخاصة، إلى جانب ما هو مخزن في أجهزة الحاسوب ومحل الضبط بطبيعته يرد على الأشياء .

ولقد أثار خلاف فقهي حول مدى قابلية الأدلة الرقمية للضبط بين معارض ومؤيد، حيث يرى البعض أن بيانات الحاسوب لا تصلح لأن تكون محلا للضبط لانتفاء الكيان المادي عنها ولا سبيل لضبطها، إلا بعد نقلها على دعامة مادية أو غيرها من الوسائل المادية، ويستند هذا الرأي بأن النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة .

في حين يرى الاتجاه الثاني بأنه يمكن ضبط المكونات المعنوية كالبرامج والمعلومات، لأنها ذبذبات الكترونية أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية وبالإمكان نقلها واستقبالها المادي لا يمكن إنكاره، حيث يرى الفقه الكندي أنه يمكن ضبط المكونات المادية، والتي تمنح سلطة الضبط أي شيء طالما توافر أسباب معقولة بأن الجريمة ارتكبت، ولا يجوز للسلطات[1] استعمال المعلومات المتحصل عليها عن طريق المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات تحت طائلة قانون العقوبات .

[1] رزيقة بودودة، المرجع السابق، ص 55، ص 56، ص 57 .

ونظرا لما تتميز به الجريمة التجارية الإلكترونية من خصائص، بإمكان سلطة التحقيق الاستعانة بخبراء مختصين للفحص وإبداء الرأي الفني في المسائل المعقدة التي يصعب فهمها، وذلك تفاديا لأي شك في صحة الأدلة المستخلصة، وبالتالي فالخبرة في مجال المساعدة القضائية هي أحد أهم وسائل جمع الأدلة تعتمد عليها سلطة التحقيق خصوصا عند وجود واقعة مادية لا يمكن التعرف عليها إلا بحكم الخبير المتخصص، باعتبار أن مجال دراسات الحاسوب والانترنت لا ترتبط بمنهج دراسي معين وإنما بمهارات خاصة .[1]

الفرع الثالث: إجراءات التحري المستحدثة

في إطار تعديل من قانون الإجراءات الجزائية الجزائري بالقانون 22/06 المؤرخ في 2006/12/20 الذي جاء فيه إجراءات مستحدثة للكشف عن الجرائم الماسة بأنظمة المعالجة للمعطيات وهي:

أولا/- الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

خول المشرع الجزائري لضابط الشرطة القضائية من صلاحية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، للكشف عن الجرائم المعلوماتية، حيث تباشر هذه الإجراءات بشكل سري، على الرغم من تناقضها مع النصوص المقررة لحماية الحق في الحياة الخاصة .

إن ما يهم هو أن مثل هذا الإجراءات يمكن لها المساس بالحرية الشخصية، خصوصا إذا علمنا أن سرية المراسلات هي حق دستوري، فقد جاء في المادة 03 من القانون رقم 04/09 المؤرخ في 05 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها .

ويعد هذا الإجراء المستحدث من أبرز إجراءات التحقيق، حيث خول المشرع ضابط الشرطة القضائية صلاحية تنفيذه للكشف عن الجرائم المنصوص عليها حصرا في المادة 65 مكرر 5 بموجب قانون الإجراءات الجزائية، ويباشر هذا الإجراء من قبل الجهة القضائية في بعض الجنايات والجنح التي ارتكبت أو التي قد يتم ارتكابها في القريب العاجل، بمعنى أنها إجراء للتحري والتحقيق، وكما يعتمد عنها كدليل ضد كل شخص توفرت بشأنه تحريات جدية على ضلوعه في ارتكاب هذه الجريمة أو[2] لديه

[1] رزيقة بودودة، المرجع السابق، ص 57 .

[2] عمار حشمان، (الجريمة المعلوماتية في التشريع الجزائري)، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر المهني الطور الثاني، المبدان العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، تخصص إدراة التحقيقات الاقتصادية والمالية، جامعة قاصدي مرياح-ورقلة-، الجزائر، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم علوم التسيير، السنة الجامعية 2019/2018، ص 53، ص 54، ص 55 .

أدلة تتعلق بها، وأن في مراقبة أحاديثه الهاتفية ما يفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية .

ورغم ذلك، نجد أن المشرع سعى للتوفيق بين هذه المتعارضات، حيث أجاز اللجوء إلى هذه الأساليب، ضمن بضوابط خاصة وهي مباشرة التحري بإذن من وكيل الجمهورية المختص، إلى جانب التزام أعوان وضباط الشرطة القضائية القائمين بالإجراء السر المهني، وسنقوم فيما يلي بتوضيح كلا الضابطين، فالمشرع على الرغم من إقراره أساليب تحري خاصة قد تمس بحرمة الحياة الخاصة إلا أنه شدد على معاقبة استعمالها بطرق غير مشروعة، وهو ما سنشير إليه على النحو التالي:

1/- مباشرة التحري بإذن من وكيل الجمهورية:

لم يجز المشرع اللجوء إلى اجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه الإجراءات تحت مراقبته، وهذا ما قررته المادة 04 من القانون 04/09 التي جاء فيها أنه: "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة" .

ويجب أن يتضمن الإذن بدقة البيانات التي تسمح بالتعرف على الاتصالات المطلوب التقاطها كما يجب أن يتضمن نوع الجريمة التي تبرر اللجوء إلى هذه التدابير ومدة هذه التدابير، لذلك فإن الإذن الممنوح من قبل وكيل الجمهورية يشأن التحقيق في جريمة ما لا يصلح للتحقيق في جريمة أخرى، بل يستلزم الحصول على إذن جديد، كذلك ينبغي أن يتضمن الإذن كل الأماكن التي توضع فيها الترتيبات التقنية من أجل التقاط وتسجيل وتثبيت الكلام الصادر من شخص أو عدة أشخاص محددين .

وخلال مباشرة التحريات والتحقيقات، يقوم ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص، بتحرير محضر مفصل لكل عملية اعتراض المراسلات وتسجيل الأصوات والتقاط للصور، وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها بشكل دقيق، بحيث يشتمل المحضر على كل البيانات المذكورة سابقا وتكون محددة تحديدا نافيا للجهالة، ويجب أن يشتمل المحضر على توقيع محرره في نهايته، بعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب، المراسلات أو الصور أو المحادثات المسجلة المفيدة في إظهار الحقيقة، ضمن محضر[1]

[1] عمار حشمان، المرجع السابق، ص 55، ص 56 .

يودع بملف المتهم، وكما تنسخ وتترجم المكالمات التي جرت باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم يكلف لهذا الغرض .

2/- التزام السر المهني:

تكون إجراءات التحري والتحقيق ذات طابع سري، ومن ثم فإن بحثها ضمن الضمانات الممنوحة للمتهم، والمقصود بالسرية هو التزام كل من هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وبالتالي لم تعد السرية تهدف كما كان عليه من قبل إلى تسهيل قمع المتهم، بل صارت وسيلة لضمان الحريات الشخصية .

فقد نص المشرع بشكل صريح على أن هذه العمليات تتم بمراعاة السر المهني ودون المساس به، إذ يلزم القانون الضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور بكتمان السر المهني، مع اتخاذه مسبقا التدابير اللازمة لضمان احترام ذلك السر، وقد نص قانون الإجراءات الجزائية على أن تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع، وبموجب قانون العقوبات فإن كل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة وتحت طائلة العقوبات المنصوص عليها فيه، لذلك فعملية التحري عن جرائم المساس بأنظمة المعالجة الألية للمعطيات تتم بسرية مطلقة، فيمنع منعا باتا ابلاغ المشتبه فيه أو أي شخص آخر بهذه التحريات، كما يمنع على ضابط الشرطة المأذون له أو المناب الإفشاء عن مضمون محضر التحريات لأي شخص كان، وإلا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضباط الشرطة القضائية ومرؤوسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين لا يجوز أن تظل مهددة ببيانات لم تثبت صحتها.[1]

ثانيا/- أسلوب التسرب أو الاختراق:

لغة: التسرب في اللغة يُقصد به الدخول بشكل خفي أو التسلل إلى مكان أو جماعة ما، مع إيهامهم بأن المتسرب ينتمي إليهم وليس غريبًا عنهم.

اصطلاحا: أما من هذه الناحية، فهناك عدة ألفاظ تُعبر عن نفس المعنى، مثل "الاختراق" أو "التوغل". ويُعتبر التسرب تقنية تمكن من الدخول إلى وسط مغلق، كمنظمة إجرامية أو شبكة تهريب ممنوعات كالمخدرات أو الأسلحة، فعملية التسرب تقوم على فكرة إقحام عنصر أجنبي عن الجماعة المراد[2]

[1] عمار حشمان، المرجع السابق، ص 56 ص 57 .

[2] حطاب كمال، (الحماية الجزائية للتجارة الالكترونية)، أطروحة دكتوراه في العلوم، تخصص علوم قانونية فرع علوم جنائية، جامعة جيلالي ليابس سيدي بلعباس، الجزائر، كلية الحقوق والعلوم السياسية، السنة الجامعية 2016/2015، الصفحة 313 .

اختراقها داخلها ليكون عينا عليها ويطلق عليها أيضا "الزرع"، أي زرع عنصر من أعوان أو ضباط الشرطة القضائية تتوفر فيه صفات خاصة وسط مجموعة إجرامية، ليراقب تحركات المجموعة من الداخل، ومعرفة أنشطتها ويجمع معلومات حول الإمكانات المادية والبشرية والتنظيمية، وطرق التواصل والتنقل لديها، بهدف تمكين المصالح الأمنية من مكافحة جرائمهم، وتقديم أفرادها إلى العدالة، مع إثبات الاتهامات الموجهة إليهم .[1]

يعتبر التسرب تقنية مستحدثة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5، ولوكيل الجمهورية الصلاحية بأن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة ويشترط حصول الضابط المكلف بالتسرب على الإذن من وكيل الجمهورية المختص، ويجب أن تتم العملية تحت اشراف ومراقبته، فيشترط على ضابط الشرطة القضائية إذا قرر مباشرة هذا الإجراءات أولا إخطار وكيل الجمهورية بذلك، ليقوم بمنحه إذنا كتابيا لتتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه، وهذا تحت طائلة البطلان المطلق، فيجب أن يكون الإذن مكتوبا يتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب .[2]

يرى بعض الفقهاء أنه يجب التقيد الصارم بالنص القانوني فيما يتعلق بهوية الشخص المتسرب، بحيث يُشترط أن يكون من بين ضباط أو أعوان الشرطة القضائية دون غيرهم، في المقابل، هناك رأي فقهي آخر إلى تفسير النص بشكل أكثر توسعا، ويجيز أنه لا يوجد ما يمنع من إسناد مهمة التسرب إلى أي شخص تتوفر فيه المواصفات، حتى وإن كان مواطنا عاديا، ويُعد هذا الرأي الأخير أكثر واقعية، خصوصًا في ميدان الجريمة الإلكترونية، التي تتطلب توفر مواصفات فنية دقيقة قد لا تتوافر لدى أعوان أو ضباط الشرطة القضائية .

يمكن تصور تنفيذ عملية التسرب في الجرائم الإلكترونية في اشتراك ضابط أو عون الشرطة القضائية، أو غيرهما، في محادثات تدور داخل غرف الدردشة حول مواضيع مثل اختراق الشبكات أو تقليد المصنفات، حيث يعتمد المتسرب اسماً مستعاراً، ويظهر كما لو كان واحد من المشاركين الحقيقيين في هذه الأنشطة، ويحاول الاستفادة من قدراتهم ومهاراتهم حول عمليات الاقتحام "الهاكر" لموقع ما .[3]

[1] حطاب كمال، المرجع السابق، ص 313 .
[2] عمار حشمان، المرجع السابق، ص 56 .
[3] حطاب كمال، المرجع السابق، ص 314 .

لما كان التسرب إجراء غير عادي قد يمس بحرمة الحياة الخاصة للغير، أحاطه المشرع بسياج من الضمانات تتمثل فيما يلي:

- صدور إذن التسرب من وكيل الجمهورية أو قاضي التحقيق، بعد إخطار وكيل الجمهورية .
- وجوب أن يكون الإذن مكتوبا، ومسببا .
- ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته .
- تحديد مدة عملية التسرب في الإذن، وحسب القانون لا يجوز أن تتجاوز أربعة أشهر قابلة للتجديد بحسب مقتضيات التحري أو التحقيق ضمن الشروط ذاتها، مع جواز أن يأمر القاضي الذي رخص بإجرائها بوقفها في أي وقت قبل انقضاء المدة المحددة .[1]

ورغم أن المشرع أجاز مثل هذه الأفعال التي تعتبر في حقيقة الأمر جرائم من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم والنجاح في إيهامهم بأنهم شركاء أو فاعلون، مع ذلك منع المشرع هؤلاء الضباط أو الأعوان من أن يحرّضوا المشتبه فيهم على ارتكاب الجريمة، بمعنى أنه يمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ودفعه لارتكاب الجريمة، فهذا الفعل ممنوع تحت طائلة بطلان الإجراء .

وحسب نص المادة 65 مكرر 14 أنه يجوز لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا القيام بما يلي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها .
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم، الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخريب أو الإيواء أو الحفظ أو الاتصال .[2]

ويحظر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب إلا لرؤسائهم السلميين، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر، وهو ما أكده المشرع بموجب المادة 65 مكرر 16 بأن

[1] حطاب كمال، المرجع السابق، ص 314 .
[2] راجع عمار حشمان، المرجع السابق، ص 59، ص 60 .

نصت صراحة أنه: " لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات ."

كما عاقب المشرع كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة مالية تقدر ب 50.000 دج إلى 2.000.000 دج، واذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس لمدة من خمس سنوات إلى عشر سنوات وبغرامة مالية تتراوح من 200.000 دج إلى 500.000 دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من 10 إلى 20 سنة وغرامة من 500.000 دج إلى 1.000.000 دج .[1]

المطلب الثاني: الحماية الجزائية للتجارة الإلكترونية في مرحلة المحاكمة

تكفل النصوص العامة إضافة إلى النصوص الخاصة في الإجراءات الجزائية حماية قانونية للتجارة الإلكترونية غي مرحلة المحاكمة فهي مرحلة قضائية من اختصاص قضاء الحكم، وتعد مرحلة نهائية كون التحقيق نهائي، وبما أن جرائم التجارة الإلكترونية جرائم دولية لا تتقيد بحدود جغرافية لدولة معينة الأمر الذي يشكل صعوبة في تحديد القانون الواجب التطبيق على مرتكبي هذه الجريمة لذا سنتطرق إلى تحديد المحكمة الجزائية الفاصلة في جريمة الاحتيال في التجارة الإلكترونية (الفرع الأول) وسلطة القاضي في تقدير الأدلة الرقمية (الفرع الثاني).

الفرع الأول: تحديد المحكمة الجزائية الفاصلة في جريمة الاحتيال في التجارة الإلكترونية

إن جرائم التجارة الإلكترونية لها نوع من الخصوصية من حيث القانون الواجب التطبيق لأن الركن المادي فيها لا يتجسد على إقليم دولة معينة، فقد يقع سلوكها الإجرامي في دولة أخرى، وهو ما نتج عنه اختلاف فقهي وقضائي حول تحديد المحكمة الجزائية المختصة[2] .

أولا: موقف الفقه والقضاء من تنازع الاختصاص الجزائي المعلوماتي

حاول كل من الفقه والقضاء اقتراح حلولا لحل مشكلة تنازع الاختصاص، وانقسم الفقه الى مذهب النشاط الإجرامي، ومذهب تحقق النتيجة، والمذهب المختلط.

[1] راجع عمار حشمان، المرجع السابق، ص 59، ص 60 .
[2] رزيقة بودودة، المرجع السابق، ص57.

1- مذهب النشاط الاجرامي بوصفه معيارا لتحديد مكان وقوع الجريمة

حيث يرى فقهاء مذهب النشاط الاجرامي ووفقا لهذا المعيار ينعقد الاختصاص للمحكمة التي يقع في نطاقها النشاط الاجرامي وليس مكان حصول النتيجة أو الآثار المترتبة عليه، بدعوى اتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات، يمكن اجمالها في أنه معيار مرن وفضفاض فضلا عن أن معيار حصول النشاط أدعى إلى تيسير عملية الإثبات وجمع الأدلة، وأن المحكمة التي لها ولاية نظر الدعوى تكون قريبة من مسرح الجريمة، ناهيك عن أن الحكم الذي يصدر في الواقعة يكون اكثر فعالية ويسهل معه ملاحقة الجناة، وقد حظي هذا الاتجاه بتأييد جانب كبير من الفقه سواء في فرنسا أو مصر ليس هذا فحسب، بل اتجهت لعض التشريعات المقارنة إلى تبنييه، ومن هذا القبيل القانون النمساوي الصادر سنة 1979 والمجري الصادر في السنة ذاتها .[1]

2-مذهب تحقق مكان النتيجة كمعيار لتحديد الاختصاص

على الرغم من الحجج التي ساقها مؤيدو المذهب الأول، فإن هذا الاتجاه تعرض لجملة من الانتقادات من جانب آخر من الفقه، وقد انصبت هذه الانتقادات على أن هذا المذهب لا يعير اهتماما للمكان الذي تحقق فيه الضرر أو أثر النشاط الاجرامي الذي كان الجاني يسعى الى تحقيقه فيه، فالآثار الضارة هي التي تبعث الفزع في نفوس الناس، في حال أن مكان وقوع السلوك لا يعدو أن يكون مصدر الضرر ليس إلاّ، كما أن تمام الجريمة لا يكون إلاّ في المكان الذي ظهرت فيه آثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيقها [2].

يضاف الى ذلك أن تقادم الجريمة يتم احتسابه من الوقت الذي تحققت فيه النتيجة، كما يؤخذ في الحسبان جسامة الضرر كأساس لتقدير التعويض ولا عبرة بخطورة الفعل أو درجة الخطأ، كذلك يعد حصول الضرر شرطا أساسيا لقيام المسؤولية المدنية، فتنفى هذه المسؤولية متى ما انتفى الضرر، ومن ثم لا مصلحة للمدعي في الدعوى، ما يجعلها غير مقبولة .

فقد لقي هذا الاتجاه ترحيبا من بعض الفقه إلى جانب ذلك تم تبنيه من بعض التشريعات المقارنة، ومنها القانون الألماني الصادر سنة 1975، والقانون الدولي الخاص التركي الصادر سنة 1982، كما أقرته اتفاقيه بروكسل لسنة 1969 بشأن المسؤولية عن اضرار التلوث بالبترول.

[1] حطاب كمال، المرجع السابق، ص325.
[2] حطاب كمال، المرجع نفسه، ص325.

ومع ذلك، فإن هذا الاتجاه لم يكن بمنأى هو الآخر عن النقد، الذي يتركز في أن الاخذ به يفضي به في نهاية المطاف إلى عدم تجريم المشروع إذا لم تتحقق النتيجة، وكذلك عدم العقاب على ما يُعرف بالسلوك المجرد (جرائم السلوك المجرد).

3-المذهب المختلط

أمام الانتقادات التي تعرض لها كلا من الاتجاهين السابقين، برز اتجاه ثالث مفاده أن الجريمة تعد واقعة في مكان حصول النشاط، وكذلك المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققها فيه، ويجد مبرره أن الركن المادي للجريمة يقوم على ثلاث عناصر وهي: الفعل (النشاط) والنتيجة، والعلاقة السببية، ما يعني ان الجريمة تعد واقعة في كل مكان تحقق فيه عنصر من عناصر الركن المادي، أي في مكان النشاط ومكان النتيجة .[1]

وهذا التشريع أخذت به التشريعات المقارنة، كما تبنته المحاكم في بعض الدول ومنها فرنسا في عدد من الأحكام، إذ ذهبت إلى أن اختصاصها يتسع ليشمل كل الأمكنة التي كانت مسرحا للجريمة عند وقوعها .

ثانيا: موقف التشريعات من تنازع الاختصاص الجزائي المعلوماتي

لقد أبدت التشريعات مواقف مختلفة اتجاه تنازع الاختصاص الجزائي المعلوماتي، ومن بينها التشريع الجزائري، وذلك راجع لعدم تجسيد الركن المادي كاملا للجريمة المعلوماتية في دولة واحدة، وهو ما أدى إلى صعوبة كبيرة في تحديد القانون الواجب التطبيق لهذه الجريمة .

بالنسبة للتشريع الجزائري، ووفقا لمبدأ الإقليمية يطبق القانون الجزائري على الجرائم المرتكبة على التراب الوطني بغض النظر عن جنسية الجاني أو المجني عليه، وبالتالي إذا تمت جريمة الأنترنت، وتحققت النتيجة في الجزائر يطبق القانون الوطني الجزائري، فالعبرة في تحديد دولة القانون المطبق بوقوع الجريمة كاملة أو جزء منها على إقليم الدولة[2]، وطبقا لمبدأ شخصية القوانين يطبق أيضا القانون الجزائري في حالة ارتكاب جزائري احدى جرائم التجارة الالكترونية، أو كان الضحية جزائري الجنسية أثناء وقوع الجريمة، والاخذ بها المبدأ صعب التطبيق في الجرائم الالكترونية لان محاكمة المتهم الأجنبي تحتاج إلى إجراءات طويلة، بالإضافة الى عدو وجود اتفاقيات لتسليم المجرمين .

أما مبدأ العينية فيعود الاختصاص فيه للمحاكم إذا وقعت جريمة من جرائم التجارة الإلكترونية بصفة خاصة تمس بالمصالح الأساسية للدولة، وإن وقعت خارج الدولة، ولا يهم جنسية مرتكبيها، وهو

[1] كمال حطاب ,المرجع السابق, ص 326.
[2] انظر المادة 3 من قانون العقوبات الجزائري .

ما أشار إليه المشرع الجزائري طبقا لنص المادة 588 من قانون الإجراءات الجزائية حيث حصر الاختصاص للمحاكم الجزائرية الجرائم التي ترتكب من طرف أجنبي خارج الإقليم الجزائري، بغض النظر إن كانت جناية أو جنحة ماسة بسلامة وأمن الدولة الجزائرية أو تزييف النقود أو أوراق مصرفية وطنية متداولة قانونا، وهذا ينطبق على الجريمة التجارية الإلكترونية في حالة مساسها بأمن الدولة الجزائرية، وهنا يمكن محاكمة مرتكبيها وفقا لأحكام القانون الجزائري في حالة القبض عليهم بالجزائر[1].

أما بالنسبة للاختصاص الجزائي الوطني للجهات القضائية يتحدد بمكان وقوع الجريمة ومحل إقامة المتهم، أو المكان الذي تم القبض فيه على الأشخاص المشتبه فيهم ارتكاب الجريمة والمشرع الجزائري قد وسع من نطاق الاختصاص القضائي لهؤلاء الأشخاص .[2]

طبقا لنص المادة 37 من قانون الإجراءات الجزائية يتحدد الاختصاص الإقليمي للنيابة العامة بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم في لجريمة أو المكان الذي تم بدائرته القبض على أحد هؤلاء الأشخاص [3]، وبما أن جرائم التجارة الإلكترونية يتحقق سلوكها الإجرامي في دولة والنتيجة المترتبة عنها في دولة أخرى، فقد وسع المشرع الجزائري من دائرة الاختصاص الإقليمي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى طبقا لما نص عليه في المادة 37 من قانون الإجراءات الجزائية .

كما يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في ارتكابها، أو بمحل القبض على أحد هؤلاء الأشخاص، ولو كان القبض لسبب أخر طبقا لنص المادة 40 من قانون الإجراءات الجزائية .

وفي حالة ارتكاب جريمة من جرائم الإلكترونية، فقد أجاز المشرع الجزائري تمديد الاختصاص المحلي لقاضي التحقيق الى محاكم أخرى، تاركا كيفية تحديد تلك الإجراءات عن طريق التنظيم حسب ما هو وارد في المادة 40 الفقرة 2 من قانون الإجراءات الجزائية، ويتحدد أيضا الاختصاص المحلي لمحاكم الجنح طبقا للمادة 329 من قانون الإجراءات الجزائية، كما نجد أن المشرع الجزائري قد نص طبقا لنص المادة 329 فقرة 4 على تمديد الاختصاص المحلي للمحكمة في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى دائرة اختصاص محاكم أخرى بموجب التنظيم[4] .

[1] انظر المادة 588 من قانون الإجراءات الجزائية.
[2] انظر المادة 37 فقرة 2 من قانون الإجراءات الجزائية .
[3] انظر المادة 37 من قانون الإجراءات الجزائية .
[4] رزيقة بودودة، المرجع السابق، ص 60.

كما وسع المشرع الجزائري نطاق اختصاص وكيل الجمهورية وقاضي التحقيق واختصاص محاكم الجنح في حالة ارتكاب جريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بموجب المرسوم التنفيذي رقم 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق . [1]

الفرع الثاني: سلطة القاضي في تقدير الأدلة الرقمية

الدليل الإلكتروني من الأدلة الجنائية المستحدثة في نطاق الاثبات الجنائي، جاء بغرض التصدي لنوع مستحدث من الجرائم ألا وهي الجرائم الإلكترونية .

أولا: أساس قبول الدليل الإلكتروني في الإثبات الجزائي

يخضع هذا الأساس الى طبيعة نظام الاثبات السائد في الدولة، والاثبات في المواد الجزائية يخضع لقواعد تختلف عن تلك التي تحكم الاثبات في المواد المدنية، وذلك لاعتبارات قد ترجع إلى اختلاف موضوع الاثبات بين تلك المواد ومنها ما يرجع الى أهمية الدعوى الجزائية، وإن القواعد التي تحكم المسائل الجزائية تدور كلها حول غاية واحدة وهي الكشف عن حقيقة جريمة تمثل اعتداء على الجماعة وتهم المجتمع.

ومن القواعد التي تحكم الاثبات في المسائل الجنائية ثلاثة : أولها حرية القاضي في تكوين عقيدته بمعنى أن له ان يوجه تحقيقه في الجلسة بالشكل الذي يراه مناسبا وملائما للوصول إلى الحقيقة والكشف عنها دون أن يتقيد في ذلك باتباع وسائل معينة للكشف عن الحقيقة، كما ان له مطلق الحرية في تقدير أدلة الدعوى، فله ان يأخذ بها وله أن يطرحها كل ذلك بناء على تقييمه لها وقناعته بما ينتهي إليه من مجموع ما طرح من أدلة في الجلسة، وذلك راجع الى أن الاثبات الجنائي يتعلق بوقائع مادية، أو معنوية لها طابع استثنائي وليس متعلقا بإثبات تصرفات قانونية، ومن جهة ثانية كي يكون ذلك مقابل قرينة البراءة، وثاني القواعد التي تحكم لأثبات في المسائل الجزائية الدور الإيجابي للقاضي الجزائي في البحث عن الحقيقة، فإنه ليس مجرد موازن للأدلة المثبتة للإدانة أو البراءة، وإنما عليه التحري عن الحقيقة والكشف عنها، وآخر القواعد التي تحكم الإثبات في المسائل الجزائية قاعدة عبء الإثبات في المواد الجزائية يقع على سلطة الادعاء من منطلق أن الأصل في الانسان البراءة، وعلى من يدعي عكس ذلك اثباته. [2]

[1] الجمهورية الجزائرية الديمقراطية الشعبية، المرسوم التنفيذي رقم 06-348 المؤرخ في 05 أكتوبر 2006، المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية 'عدد63، مؤرخة في 2006-08-08 .

[2] كمال حطاب، المرجع السابق، الصفحة 339.

ثانيا: الضوابط التي تحكم اقتناع القاضي الجزائي بالدليل الإلكتروني

للقاضي الجزائي سلطة واسعة في تقدير الأدلة والدليل الإلكتروني ليس مستثنى من هذه القاعدة العامة، غير أن المشرع وضع ضوابط كي لا ينحرف القاضي عن الصواب عند ممارسته لهاته السلطة، وبالنسبة للدليل الإلكتروني فلا بد أن يكون هذا الدليل مقبولا، أي يحصل به اليقين في ضمير القاضي، بحيث تتطابق حالة الذهن والعقل مع حالة الواقع والحقيقة، ذلك أنه من مقتضيات مبدأ أو قرينة البراءة أن يبنى الحكم الجزائي على الجزم واليقين لا على مجرد تخمين او اتباع الظن (وإن الحق لا يغني من الحق شيئا)، لذلك ليس معنى القول أن القاضي يملك حرية تقدير الأدلة بما فيها الأدلة الإلكترونية أو الرقية أنه يملك الحكم بالإدانة على غير أساس من التثبيت والتيقن[1] .

لكن هذا لا يمنع القاضي أن يؤسس حكمه بإدانة المتهم بترجيح فرض على آخر، إذ يكون هنا اقتناع القاضي بوقوع الجريمة ونسبها الى المتهم يقينا.

غير أن محكمة النقض الفرنسية لا تأخذ بمبدأ الشك يفسر لصالح المتهم إلا في اضيق نطاق، إذ أنها تعتبر ان مجرد وجود شك في الإدانة لا يكفي لتبرئة ساحة المتهم، بل يجب أن يستند هذا الشك على أدلة قاطعة، وبالنسبة للأدلة الإلكترونية لا مجل لتطبيق ما توصلت إليه محكمة النقض الفرنسية فلا بد من أن تكون الأدلة الإلكترونية يقينية.[2]

كما يجب أيضا مناقشة الأدلة الرقمية بطريقة شفوية أمام اطراف الدعوى وبحضورهم، ويجب على الخبير المعين من قبل المحكمة الحضور وتلاوة تقريره في الجلسة، فكل دليل مهما كان لابد أن يخضع للمناقشة العلنية، وعليه فإن القاضي لا يجوز له ان يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى ونصت على هذه القاعدة القوانين الإجرائية المقارنة[3] .

[1] كمال حطاب, المرجع السابق ، ص 340.
[2] رزيقة بودودة، المرجع السابق، ص 63.
[3] كمال حطاب المرجع السابق، ص346.

خلاصة الفصل :

من خلال دراستنا لهذا الفصل حاولنا تسليط الضوء على أهم أساليب الحماية من جرائم التجارة الإلكترونية خاصة وسائل الدفع الإلكترونية وحمايتها القانونية وحماية بيانات المستهلك كما خصص جزء من الدراسة لمسألة الحماية من الإعلانات الكاذبة والمضللة باعتبارها أحد الأساليب الاحتيالية الشائعة في البيئة الرقمية .

كما تطرقنا إلى الإجراءات الردعية المتمثلة في إجراءات البحث والتحري والتي تبدأ بإجراءات التحقيق الابتدائي ثم إجراءات البحث و التحري المستحدثة وصولا إلى إجراءات المحاكمة مع الإشارة إلى ضرورة تأهيل القضاة للتعامل مع الأدلة الرقمية بطريقة دقيقة تحفظ حقوق الأطراف .

الـــــــــخاتمة

الخاتمة:

في ختام هذه الدراسة، وبعد التطرق لموضوع الاحتيال في التجارة الإلكترونية من مختلف جوانبه القانونية، يتّضح أن هذا النوع من الجرائم يُمثل أحد أبرز التحديات الناتجة عن التقدم التكنولوجي في المجال التجاري، بالنظر إلى ما يتسم به من مرونة، وسرعة في التطور، وتعدد في الأساليب المستخدمة فيه، الأمر الذي مكّننا من الوقوف على وجود آليات قانونية وتنظيمية اعتمدها المشرّع الجزائري في سبيل مكافحة هذه الجريمة، وذلك في إطار مجهودات واضحة تبذلها أجهزة الدولة المختصة للحد من انتشارها والتصدي لمخاطرها المتنامية .

وقد أظهرت الدراسة أن جريمة الاحتيال الإلكتروني تُعد من العوامل الأساسية التي تضعف الثقة في التعاملات الرقمية، وتُهدد استقرار البيئة التجارية الحديثة، بما فيها من منصات الكترونية، ووسائل دفع رقمية، وعقود إلكترونية، فانتشار هذا النوع من الجرائم يؤدي إلى تراجع ثقة المستهلك في التعامل مع الوسائط التكنولوجية، ويفتح المجال لخلق بيئة غير آمنة للاستثمار الرقمي والتبادل التجاري عبر الإنترنت .

كما كشفت الدراسة عن أهمية تحديد أركان الجريمة بدقة، وضرورة تجريم الأفعال الاحتيالية بصيغ واضحة وشاملة، مع التشديد على العقوبات الرادعة للحد من انتشارها .

ولقد أبرزت هذه الدراسة أن الاحتيال في التجارة الإلكترونية ليس مجرد تصرف فردي مخالف للقانون، بل هو ظاهرة متطورة تعكس واقعًا رقميًا جديدًا، يشهد تحوّلًا سريعًا في أساليب التعامل والتبادل التجاري، فهذه الجريمة تمسّ الحياة اليومية للناس، وتؤثر بشكل مباشر على ثقتهم في استخدام الوسائل الإلكترونية، سواء في البيع أو الشراء أو حتى في مجرد تصفح المنصات التجارية .

ولهذا، فإن معالجة هذه الظاهرة لا تقتصر فقط على النصوص القانونية، بل تحتاج إلى وعي مجتمعي شامل، وجهد جماعي يُشارك فيه كل من الدولة، والمؤسسات، والأفراد، من أجل حماية هذا الفضاء الجديد الذي أصبح جزءًا من حياتنا .

كما أن تطور هذه الجريمة من حيث الأساليب والأدوات، يجعل منها تحديًا حقيقيًا يفرض على الجميع أن يواكب هذا التطور، سواء من خلال التحديث المستمر للقوانين، أو عبر دعم التكوين والتخصص في مجالات التحقيق الرقمي، والقضاء الإلكتروني فمواجهة الاحتيال في التجارة الإلكترونية ليست مسؤولية المشرّع وحده، بل هي مهمة تتطلب تكامل الأدوار بين القانون، والتقنية، والإعلام، والتربية، حتى نتمكن من خلق بيئة رقمية أكثر أمانًا وثقة .

ومن خلال دراستنا لموضوع الاحتيال في التجارة الإلكترونية، توصلنا إلى عدة نتائج، نعرض أبرزها كما يلي :

- التجارة الالكترونية مثل أي نشاط تقليدي يمكن أن تتم داخليا أو خارجيا، تختلف عن التجارة التقليدية في الطريقة لأنها تتم بالوسائط الإلكترونية .
- يُسجل غياب نص خاص بتجريم الاحتيال التجاري الإلكتروني كمفهوم مستقل، حيث يتم غالبًا تكييف الأفعال وفق قواعد الاحتيال الكلاسيكي، وهو ما يُحدث صعوبات على مستوى التطبيق القضائي.
- ظهرت الدراسة أن الاتفاقيات الدولية، خصوصًا اتفاقية بودابست المتعلقة بالجرائم السيبرانية لسنة 2001، تُعد من أبرز الجهود العالمية في سبيل وضع إطار قانوني لمكافحة الجرائم المعلوماتية، بما فيها الاحتيال الإلكتروني، لكنها تبقى غير مفعّلة في الجزائر نظرًا لعدم المصادقة عليها رسميًا، وهو ما يُضعف إمكانية التعاون الدولي في تتبع مرتكبي هذه الجرائم.
- يتبيّن أن المشرّع الجزائري حاول مواكبة التطور الرقمي، من خلال إدراج بعض صور الاحتيال الإلكتروني ضمن قانون العقوبات، وقانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إلا أن النصوص تبقى عامة وغير مفصّلة بما يكفي لتغطية كل مظاهر الاحتيال التجاري الحديث.
- أهمية التزام المورد الإلكتروني بضمان احترام مبادئ معالجة المعطيات الشخصية .
- نستنتج أن القاضي الجزائي له سلطة واسعة في تقدير الأدلة والدليل الإلكتروني ليس مستثنى من هذه القاعدة العامة .

استنادا لما توصلنا إليه من نتائج، نرى أنه من الضروري تقديم الاقتراحات الآتية :

- إعادة النظر في حماية المواقع والحماية الجنائية للبيانات الشخصية في التشريع الجزائري بتوسيع نطاقها من حيث الجرائم وتقري عقوبات مناسبة وردعية ،وذلك بتشديد العقوبات على من يقوم بحمع أو نشر البيانات الشخصية دون ترخيص أو رضا المعني .
- وضع أحكام خاصة وآليات الرقابة على المورد الإلكتروني، ما يتماشى مع خصوصية هذا الأخير عوض الإحالة إلى النصوص التنظيمية .
- على المشرع الجزائري تفعيل آليات جديدة لحماية حق المستهلك الإلكتروني في الخصوصية، كآلية الرقابة التي اعتمدها قانون التجارة الإلكترونية .

- ضرورة مراجعة بعض مواد القانون 18-05 لما يتضمن توفير حماية أكثر شمولية وفاعلية ضد الاحتيال الإلكتروني بالإضافة إلى دمج جهود المؤسسات القضائية والأمنية والرقابية ضمن سياسة وطنية متكاملة للأمن الرقمي في الجزائر .

قـــــــائمة المراجع

قائمة المصادر والمراجع .

المراجع باللغة العربية

أولاً: الكتب

1. العيسوي، إبراهيم، **التجارة الإلكترونية**، المكتبة الأكاديمية، ط.1، الإسكندرية، مصر، 2003.

2. قورة، نائلة عادل محمد فريد، **جرائم الحاسب الآلي الاقتصادية**، منشورات الحلبي الحقوقية، ط.1، بيروت، لبنان، 2005.

3. إسماعيل، محمد سعيد أحمد، **أساليب الحماية القانونية لمعاملات التجارة الإلكترونية (دراسة مقارنة)**، منشورات الحلبي الحقوقية، ط.1، دمشق، سوريا، 2009.

4. الشلبي، هيثم حمود، **إدارة مخاطر الاحتيال في قطاع الاتصالات**، دار صفاء للنشر والتوزيع، ط.1، عمان، الأردن، 2009.

5. مطر، عصام عبد الفتاح، **التجارة الإلكترونية في التشريعات العربية والأجنبية**، دار الجامعة الجديدة، (د.ط)، الإسكندرية، مصر، 2015.

6. كيلاني، عبد الراضي محمود، **المسؤولية عن الاستعمال غير المشروع لبطاقات الوفاء والضمان**، دار النهضة العربية، (د.ط)، القاهرة، مصر، 2001.

7. حجاج، مصطفى، **التجارة الإلكترونية**، مطبوعة موجهة لطلبة السنة أولى ماستر، جامعة ابن خلدون تيارت، الجزائر، 2022-2023.

ثانياً: المقالات والمداخلات العلمية

1. عبد الرحمان، محمد قدري حسن، "جرائم الاحتيال الإلكتروني"، **دار المنظومة**، المجلد 20، العدد 79، الإمارات العربية المتحدة، 2016.

2. بوضياف، إسمهان، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، المجلد 03، العدد 11، جامعة محمد بوضياف المسيلة، الجزائر، سبتمبر 2018.

3. بولحية، شهيرة، "الاحتيال الإلكتروني"، **مجلة الدراسات القانونية والاقتصادية**، العدد 04، المركز الجامعي سي الحواس بريكة، باتنة، الجزائر، ديسمبر 2019.

4. قارون، سهام، "التزام المورد الإلكتروني بحماية المعطيات الشخصية للمستهلك"، **مجلة الباحث للدراسات الأكاديمية**، المجلد 07، سوق أهراس، الجزائر، 2020.

5. عبد الباقي، حياة وعبدوس، عبد العزيز، "آليات التصدي للجرائم المعلوماتية الواقعة على التجارة الإلكترونية"، **مجلة البصائر للدراسات القانونية الاقتصادية**، المجلد 01، العدد 01، جامعة بلحاج بوشعيب عين تموشنت، الجزائر، مارس 2021.

6. غبش، عز الدين، "حماية المستهلك الإلكتروني في ظل الجرائم السيبرانية"، **المجلة الدولية للتحولات القانونية والسياسية**، المجلد 01، العدد 01، جامعة الشهيد حمة لخضر الوادي، الجزائر، أفريل 2022.

7. الفليح، محمد طه إبراهيم، "جريمة الاحتيال الإلكتروني في إطار التجارة الإلكترونية ضمن التشريعات الأردنية"، **مجلة جامعة الزيتونة الأردنية للدراسات القانونية**، المجلد 03، العدد 03، الأردن، 2022.

8. علال، نزيهة وعاشور، فاطمة، "الحماية القانونية للمعطيات الشخصية في معاملات التجارة الإلكترونية"، **دائرة البحوث والدراسات القانونية والسياسية**، المجلد 06، العدد 02، المركز الجامعي عبد الله مرسلي تيبازة، الجزائر، 2022.

9. المصري، محمد عبد القدوس، "الإعلان الكاذب والمضلل (الماهية والأركان القانونية)"، **مجلة البحوث الفقهية والقانونية**، العدد 42، جامعة الأزهر، القاهرة، مصر، يوليو 2023.

10. هراكي، حياة، "واقع جريمة الاحتيال الإلكتروني في التجارة الإلكترونية"، **مجلة التغيير الاجتماعي**، المجلد 08، العدد 02، جامعة محمد خيضر بسكرة، الجزائر، 31 ديسمبر 2023.

11. العمري، سليمة، "مدخل مفاهيمي للتجارة الإلكترونية متطلباتها ومعوقاتها"، **مجلة الدراسات الإنسانية والاجتماعية**، المجلد 16، العدد 01، جامعة وهران، الجزائر، 16 يناير 2024.

12. الشبلي، حسين محمد، "صور الاحتيال والتزوير في البطاقات الائتمانية"، **المجلة العربية للدراسات الأمنية والتدريب**، المجلد 29، العدد 58، المملكة الأردنية الهاشمية، (د.س.ن.(

13. شعوة، هلال، "حماية المستهلك من جريمة الإعلان التجاري المضلل أو الكاذب"، **مجلة دراسات قانونية**، المجلد 01، العدد 01، كلية الحقوق جامعة عنابة، الجزائر، (د.س.ن.(

14. شرابشة، ليندة، **السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية**، مداخلة، المركز الجامعي سوق أهراس، الجزائر، (د.س.ن.(

15. عبيد، علي وناصر، موفق وآخرون، "ماهية جريمة الاحتيال الإلكتروني"، **مجلة كلية القانون للعلوم القانونية والسياسية**، جامعة تكريت، العراق، (د.س.ن.(

16. علاوة، محمد لحسن ومولاي لخضر، عبد الرزاق، **آليات التجارة الإلكترونية كأداة لتفعيل التجارة العربية البينية**، مداخلة بالملتقى الرابع حول عصرنة نظام الدفع في البنوك الجزائرية، جامعة قاصدي مرباح ورقلة، الجزائر، (د.س.ن.(

17. مشري، فريد وقاجة، آمنة والمزاودة، رياض، **الحماية القانونية لوسائل الدفع الإلكتروني (الجزائر نموذجا(**، مداخلة بالملتقى الوطني الثالث حول المستهلك والاقتصاد الرقمي، المركز الجامعي عبد الحفيظ بوالصوف ميلة، الجزائر، (د.س.ن.(

ثالثاً: أطروحات ورسائل الجامعية

أ- أطروحات الدكتوراه

1. حطاب، كمال، **الحماية الجزائية للتجارة الإلكترونية**، أطروحة دكتوراه في العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس سيدي بلعباس، الجزائر، 2015-2016.

ب- رسائل الماجستير

1. واقد، يوسف، **النظام القانوني للدفع الإلكتروني**، مذكرة ماجستير في القانون العام، كلية الحقوق، جامعة مولود معمري تيزي وزو، الجزائر، 2011.

2. صراع، كريمة، **واقع وآفاق التجارة الإلكترونية في الجزائر**، مذكرة ماجستير في الاستراتيجية، كلية العلوم الاقتصادية وعلوم التسيير والعلوم التجارية، جامعة وهران، الجزائر، 2013-2014.

ج- مذكرات الماستر

1. بودودة، رزيقة، **الحماية الجنائية للتجارة الإلكترونية**، مذكرة ماستر في القانون الجنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي، الجزائر، 2014-2015.

2. حشمان، عمار، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة ماستر مهني في إدارة التحقيقات الاقتصادية والمالية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرباح ورقلة، الجزائر، 2018-2019.

3. السايس، إبتسام ونيلي، صفاء، **وسائل الدفع في التجارة الإلكترونية**، مذكرة ماستر أكاديمي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، 2019-2020.

4. بن حميدة، هجيرة وعتيق، ستي، **النظام القانوني لوسائل الدفع الإلكتروني في التشريع الجزائري**، مذكرة ماستر في قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر السعيدة، الجزائر، 2020-2021.

5. شرفي، كميليلة وفريفرة، دنيا، **الحماية القانونية لوسائل الدفع الإلكتروني**، مذكرة ماستر في القانون الخاص، كلية الحقوق، جامعة بلحاج بوشعيب عين تموشنت، الجزائر، 2022-2023.

6. العالية، ختام وحجاج، درة، **جريمة الاحتيال المعلوماتي في التشريع الجزائري**، مذكرة ماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أم البواقي، الجزائر، 2023-2024.

رابعاً: النصوص القانونية

أ- الأوامر

1. الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، يتضمن قانون العقوبات، المعدل والمتمم،ج.ر عدد 49 الصادر بتاريخ 8 يونيو 1966 .

ب- القوانين الوطنية

1. القانون رقم 04-02، المؤرخ في 5 جمادى الأولى عام 1425 الموافق 23 يونيو سنة 2004، يحدد القواعد المطبقة على الممارسات التجارية، المعدل والمتمم،ج.ر عدد 41، الصادر ب 27 يونيو 2004.

2. القانون رقم 18-04، المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج.ر عدد 34 ،الصادر ب10 يونيو 2018 .

3. القانون رقم 18-05، المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يتعلق بالتجارة الإلكترونية، ج.ر عدد 34، الصادر بتاريخ 10 مايو 2018.

4. القانون رقم 18-07، المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي،ج،ر عدد 34 الصادر بتاريخ 10 يونيو 2018.

ج- القوانين الأجنبية

5. القانون المصري رقم 181 لسنة 2018، بشأن حماية المستهلك.

د- المراسيم التنفيذية

1. المرسوم التنفيذي رقم 06-348، المؤرخ في 9 رمضان عام 1427 الموافق 2 أكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

المراجع الإلكترونية

لجنة الأمم المتحدة للقانون التجاري الدولي (الأونسيترال)، الموقع الرسمي، https://uncitral.un.org/ar،

الفـــــهرس

الفهرس

مقدمة .....ب
الفصل الاول: الاطار المفاهيمي للاحتيال في التجارة الالكترونية..... 6
المبحث الأول: مفهوم الإحتيال في التجارة الإلكترونية 7
المطلب الأول: مدلول التجارة الإلكترونية..... 7
الفرع الأول: تعريف التجارة الإلكترونية..... 7
الفرع الثاني: خصائص التجارة الإلكترونية وأهميتها 9
المطلب الثاني: المقصود بالإحتيال في التجارة الإلكترونية 12
الفرع الاول: مفهوم الاحتيال في التجارة الإلكترونية 12
الفرع الثاني: أشكال وأساليب الاحتيال في التجارة الإلكترونية 13
المبحث الثاني: الإطار القانوني لتجريم الاحتيال في التجارة الإلكترونية..... 18
المطلب الأول: تجريم الاحتيال في التجارة الإلكترونية 18
الفرع الأول: دور الاتفاقيات الدولية في تجريم الاحتيال الالكتروني في التجارة الإلكترونية..... 18
الفرع الثاني: موقف المشرع الجزائري في تجريم الاحتيال الإلكتروني 21
المطلب الثاني: أركان جريمة الاحتيال في المجال الإلكتروني..... 23
الفرع الأول: الركن المادي لجريمة الاحتيال الإلكتروني 23
الفرع الثاني: الركن المعنوي لجريمة الاحتيال الإلكتروني 26
الفرع الثالث: الركن الشرعي لجريمة الاحتيال الإلكتروني..... 27
خلاصة الفصل..... 29
الفصـــل الثاني حماية التـــجارة الإلكترونية من جـــريمة الاحتـــيال الإلكتروني 31
المبحث الأول: الإجراءات الوقائية للحماية من الاحتيال في التجارة الإلكترونية 32
المطلب الأول: أساليب الحماية للتجارة الإلكترونية 32
الفرع الأول: وسائل الدفع الالكتروني وأساسها القانوني في مكافحة الاحتيال 32
الفرع الثاني: وسائل الحماية من جريمة الاحتيال في التجارة الإلكترونية..... 36
المطلب الثاني: حماية البيانات والمستهلك في التجارة الإلكترونية..... 39
الفرع الأول: حماية البيانات الشخصية في التجارة الإلكترونية:..... 39
الفرع الثاني: حماية المستهلك من الإعلانات التجارية الكاذبة والمضللة..... 44
المبحث الثاني: الإجراءات الردعية للاحتيال في التجارة الإلكترونية 48
المطلب الأول: الآليات الإجرائية لمكافحة جريمة الاحتيال في التجارة الإلكترونية..... 48

الفرع الأول: إجراءات البحث والتحري 48
الفرع الثاني: مرحلة التحقيق الابتدائي 51
الفرع الثالث: إجراءات التحري المستحدثة 54
المطلب الثاني: الحماية الجزائية للتجارة الإلكترونية في مرحلة المحاكمة 59
الفرع الأول: تحديد المحكمة الجزائية الفاصة في جريمة الاحتيال في التجارة الإلكترونية..... 59
الفرع الثاني: سلطة القاضي في تقدير الأدلة الرقمية 63
خلاصة الفصل : 65
الخاتمة:..... 67
قائمة المصادر والمراجع 71