وزارة التعليم العالي والبحث العلمي

جامعة عمار ثليجي – الأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

العنوان:

الاحتيال في التجارة الالكترونية

مذكرة في اطار مقتضيات نيل شهادة الماستر تخصص قانون أعمال

من إعداد الطلبة:

جليخ خيرة

بومقواس مريم

الأستاذ المشرف:

أ.د/لحاق عيسى

لجنة المناقشة:

-الاستاذ:.....أ.د/رزق الله العربي.....رئيسا

-الاستاذ:..... أ.د/لحاق عيسى.....مشرفا ومقررا

-الأستاذ:.....د/بن جلول مصطفى.....عضوا مناقشا

السنة الجامعية 2026/2025

شكر وعرفان

الحمد لله حبا وشكرا وامتنانا

ماكنت أفعلها لول فضل الله عز وجل فالحمد لله عند البدء والحمد لله عند الختام قال رسول الله صلى الله عليه وسلم "من لا يشكر الناس لا يشكر الله" نتقدم بخالص الشكر وعظيم الامتنان الى

الاستاذ الدكتور المشرف عيسى لحاق

لقبوله الاشراف على هذا العمل والذي كان خير مرشد طوال انجاز هذا العمل ولم يبخل علينا بعلمه وتوجيهاته.

الى جميع اعضاء اللجنة كل باسمه ومقامه

الى كل من كان بجانبنا الى من قدم لنا كلمة طيبة او دعوة في ظهر غيب أو لمسة دعم خفية لكم جميعا منا كل الِامتنان .

الإهداء

بسم الله الرحمن الرحيم

ما سلكنا البدايات إلا بتسييره، وما بلغنا النهايات إلا بتوفيقه، وما حققنا الغاية إلا بفضله...

فالحمد لله الذي وفّقني لتثمين هذه الخطوة في مسيرتي الدراسية.

إلى نفسي الطموحة جداً التي لم تخذلني...

إلى مَن تمنّيتُ أن تشهد يوم تخرّجي، إلى مَن كان دعاؤها سرّ نجاح وحنانها بلسم جراحي،

داعمتي الأولى ووجهتي التي استمددتُ منها القوّة...

إلى روح أمّي الغالية — رحمها الله وأسكنها فسيح جنّاته—

يا أمّاه، لو كنتِ تعلمين كم مرّة ناديتكِ في سرّي حين اشتدّ عليّ الأمر،

وكم مرّة تخيلتُ يديكِ تمسحان رأسي وتقولان: ستنجحين يا حبيبتي.

اليوم تحقّق ما كنتِ تدعين له في كل سجدة...

أرجو أن يبلّغك الله نجاحي، كما كان يبلّغك دعاؤكِ إليّ.

إلى مَن أحمل اسمه بكل فخر واعتزاز...

إلى روح والدي الحبيب — رحمه الله رحمةً واسعة وأعلى درجته—

الرجل الذي علّمني أنّ الكرامة لا تُباع، وأنّ العلم هو أشرف ما يسعى إليه الإنسان...

إلى زوجي العزيز—

شكراً لأنّك لم تكتفِ بالوقوف إلى جانبي، بل حملتَ معي ما لم أستطع حمله،

وتجاوزتَ عمّا قصّرتُ فيه بسبب انشغالي دون أن تُشعرني يوماً بثقل ما تتحمّله.

هذا النجاح نصفه لك، وربما أكثر.

إلى أبنائي الأحبّة — يا بهجة الروح ونور الأيام—

لكم كنتُ أكمل ما بدأتُ حين تعبتُ، ولكم كنتُ أقول لنفسي: لا يجوز أن أستسلم وعيونهم تنظر إليّ.

إلى إخوتي الأعزّاء وكل الأصدقاء الذين لم يتّسع المقام لذكرهم—

إلى أساتذتي الكرام — يا بنّاة العقول وصنّاع الأجيال—

ما من فكرة في هذه المذكرة إلا وفيها أثر من علمكم ونورٌ من توجيهاتكم.

وإلى كل من استحضرته أو لم تستحضره الذاكرة في هذه اللحظات...

أُهدي هذا العمل المتواضع.

"رَبِّ اشْرَحْ لِي صَدْرِي ✦ وَيَسِّرْ لِي أَمْرِي"

صدق الله العظيم

جلـــــــيخ خيـــــــــــــرة

اهداء

اهدي ثمرة هذا العمل المتواضع، وبعون الله وتوفيقه، إلى كل من كان له فضل في مسيرتي العلمية وساعدني ولو بالكلمة الطيبة أو بالنصح والتوجيه.

إلى زهرتي البستان ووردة الريحان، إلى من أوصى بها الرحمن،

إلى أغلى ما في الوجود، إلى امي العزيزة، بارك الله في عمرها وأدام عليها الصحة والعافية.

إلى من ربّاني على الفضيلة والأخلاق، وكان لي سندًا وعونًا في مواجهة صعوبات الحياة، وتحمل أعباءها حتى لا نشعر بالحرمان، إلى ابي العزيز، حفظه الله وأطال في عمره.

الى زوجي العزيز اهدي لك هذا العمل عربون امتنان لك

إلى إخوتنا وأخواتنا الذين تقاسموا معنا أفراح الحياة وأحزانها، وكانوا خير داعم وسند.

وإلى جميع أهلنا وأقاربنا وأصدقائنا، وكل من ساهم من قريب أو بعيد في إنجاز هذا العمل.

اهدي هذا الجهد المتواضع عربون محبة وتقدير ووفاء، راجين من الله تعالى أن يجعله في ميزان حسنات الجميع.

بومقواس مريم

مقدمة

أدت العولمة بمختلف اتجاهاتها وأفكارها ونظرياتها، إلى ربط دول العالم في إطار إقتصادي ومالي واحد، وبالتالي أثر على أوضاعها السياسية والاجتماعية والثقافية وظهر ذلك في الأزمة المالية العالمية التي ضربت بقواها كل المصارف والأسواق المالية العالمية، وتأثرت بها كل أرجاء المعمورة.

كل ذلك كان أرضا خصبة لظهور أنواع جديدة من الجرائم والمجرمين، يستغلون ثمار التقدم العلمي، ويستفيدون من إنهيار المصارف، وإهتزاز الأسواق المالية، وينتهزون فرصة الخوف الطبيعي للأفراد من إيداع أموالهم في المصارف خشية إفلاسها، وترددهم في الإستثمار في أسواق الأوراق المالية تجنبا لخسائر إنهيارها. ولقد أصبح الاحتيال والمحتالون سمة هذا العصر، وأصبح المحتالون من كبار رجال الأعمال ومن أصحاب الشركات الذين يتنقلون بين دول العالم بسهولة ويسر وتفتح لهم الأبواب وتعقد لهم المؤتمرات والندوات ويستقبلون بكل ود وترحاب.

رافق هذا التطور في المعاملات التجارية الإلكترونية الكثير من المفاهيم الجديدة التي لم تكن معروفة من قبل في الممارسات التجارية التقليدية، الأمر الذي إستلزم وضع الأحكام والقواعد التي تنظم هذا النوع الجديد من العقود التجارية الإلكترونية.

وكان الاحتيال الإلكتروني هو الأداة المساعدة في إرتكاب جرائم الاحتيال المستجدة عن طريق إستخدام الحاسبات الآلية والإنترنت، وآلات الدفع الآلي، حتى الهاتف المتحرك إما باستعمالها كأداة أساسية في إرتكاب الجريمة كحالة تزوير بطاقات الائتمان، بإرسال رسائل نصية مضللة، أو كأداة مساعدة لإختراق شبكات الإنترنت ونشر بيانات مضللة، أو باستخدام برامج خبيثة تجمع كلمات السر المصرفية وأرقام البطاقات الائتمانية واستغلالها في السحب من أرصدة العملاء، أو للتشويش على المعلومات المخزونة بما يحقق أهداف المحتال. ويترتب على جرائم الاحتيال إرتكاب جريمة أخرى، هي جريمة غسل أو تبييض الأموال، لإخفاء الأموال المتحصلة من جرائم الاحتيال، وإعطائها مظهر الأموال الشرعية

1 – أهمية الموضوع

تكتسي دراسة موضوع الاحتيال في التجارة الإلكترونية أهمية بالغة في ظل التحول الرقمي الذي يشهده العالم، حيث أصبحت المعاملات التجارية تتم بشكل متزايد عبر الوسائط الإلكترونية. وقد أدى هذا التطور إلى بروز أنماط جديدة من الجرائم، من بينها الاحتيال الإلكتروني، الذي يستهدف المستهلكين والمتعاملين عبر الإنترنت بطرق متطورة يصعب أحياناً إكتشافها.

وتبرز أهمية هذا الموضوع من الناحية العملية في حماية المستهلك الإلكتروني وتعزيز الثقة في المعاملات الرقمية، خاصة في الجزائر التي تسعى إلى تطوير الاقتصاد الرقمي وتشجيع التجارة الإلكترونية. كما يساهم البحث في هذا المجال في الكشف عن الثغرات القانونية التي قد يستغلها المحتالون، وتقييم مدى فعالية النصوص التشريعية الوطنية في التصدي لهذه الجرائم.

أما من الناحية العلمية، فإن هذا الموضوع يُثري الدراسات القانونية الحديثة المرتبطة بـــ"القانون الرقمي"، ويُبرز الحاجة إلى تكييف القواعد التقليدية للقانون الجنائي والتجاري مع البيئة الإلكترونية. كما يتيح الفرصة لتحليل التشريعات المقارنة والإستفادة من التجارب الدولية في مكافحة الاحتيال الإلكتروني.

ومن الناحية الاجتماعية والاقتصادية، فإن الحد من الاحتيال في التجارة الإلكترونية يساهم في حماية الاقتصاد الوطني وتقليل الخسائر المالية، فضلاً عن حماية الأفراد من الوقوع ضحايا لممارسات احتيالية قد تمس بأمنهم المالي والشخصي.

2 – أهداف الموضوع

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف العلمية والعملية، من أبرزها:

- ✓ تحديد مفهوم الاحتيال في التجارة الإلكترونية وبيان خصائصه وتمييزه عن غيره من الجرائم المشابهة في البيئة الرقمية.

- ✓ تحليل صور وأساليب الاحتيال الإلكتروني الأكثر انتشارًا في المعاملات التجارية عبر الإنترنت، مع إبراز تطورها في ظل التكنولوجيا الحديثة.
- ✓ دراسة الإطار القانوني الجزائري المنظم للتجارة الإلكترونية وجرائم الاحتيال، وتقييم مدى كفايته وفعاليته في مواجهة هذه الجرائم.
- ✓ تسليط الضوء على آليات حماية المستهلك الإلكتروني وبيان دور التشريعات الوطنية في تعزيز الثقة في المعاملات الرقمية.
- ✓ الكشف عن الثغرات القانونية والتطبيقية التي قد يستغلها المحتالون في البيئة الإلكترونية.
- ✓ الإستفادة من التجارب والتشريعات المقارنة في مجال مكافحة الاحتيال الإلكتروني، ومحاولة إسقاطها على الواقع الجزائري.
- ✓ اقتراح حلول وتوصيات قانونية وعملية من شأنها الحد من ظاهرة الاحتيال في التجارة الإلكترونية وتعزيز الأمن القانوني الرقمي.

3 –أسباب اختيار الموضوع

الأسباب الذاتية لاختيار الموضوع

ارتباط موضوع الاحتيال الإلكتروني باهتماماتنا الشخصية والبحثية في مجال الجريمة الرقمية وتقنيات المعلومات.

رغبتنا في تعميق الفهم القانوني والتقني لهذه الظاهرة التي تتسم بالتطور السريع والتعقيد.

شعورنا بأهمية هذا الموضوع في حياتنا اليومية، خاصة مع الاعتماد المتزايد على الخدمات الإلكترونية والتعاملات الرقمية.

حرصنا على المساهمة في رفع مستوى الوعي المجتمعي تجاه الأخطار المترتبة على هذه الجريمة، خصوصا في ظل قلة المعلومات المتوفرة باللغة العربية.

4 –المنهج المتبع :

المنهج الوصفي و المنهج التحليلي .

5– الاشكالية : مامدى نجاعة النصوص القانونية الوطنية والدولية في محاربة الاحتيال الإلكتروني ؟

الفصل الأول:
مفهوم الاحتيال في التجارة الالكترونية

تمهيد

شهد العالم في العقود الأخيرة تطورًا تكنولوجيًا متسارعًا انعكس بشكل مباشر على مختلف مجالات الحياة، لاسيما المجال الاقتصادي، حيث ظهرت التجارة الإلكترونية كأحد أبرز مظاهر هذا التحول الرقمي.

فقد أتاحت هذه الأخيرة إمكانية إبرام المعاملات التجارية عن بُعد باستخدام الوسائط الإلكترونية، مما ساهم في تسهيل المبادلات وتقليص التكاليف والوقت.

غير أن هذا التطور لم يخلُ من التحديات، إذ أفرزت البيئة الرقمية أنماطًا جديدة من الجرائم، وفي مقدمتها الاحتيال الإلكتروني، الذي بات يشكل تهديدًا حقيقيًا لأمن المعاملات وثقة المتعاملين. ويتميز هذا النوع من الاحتيال بتعدد صوره وتطوره المستمر، مستفيدًا من الخصائص التقنية التي تميز الفضاء الإلكتروني، كسهولة إخفاء الهوية وسرعة تنفيذ العمليات.

وعليه، يهدف هذا الفصل إلى وضع الإطار المفاهيمي لكل من التجارة الإلكترونية والاحتيال الإلكتروني، من خلال تحديد المفاهيم الأساسية وبيان الخصائص المميزة لهما، إضافة إلى استعراض أهم الصور والأساليب المعتمدة في هذا النوع من الجرائم، بما يمهد لدراسة الإطار القانوني وآليات المكافحة في الفصول اللاحقة.

المبحث الأول: مفهوم التجارة الالكترونية

يعد موضوع التجارة الإلكترونية من أكثر المواضيع المثيرة للجدل في وقتنا الحالي، وهذا لحداثة مصطلح التجارة الإلكترونية، كذلك تعدد مفاهيمها لإختلاف وجهات النظر عند تفسيرها بسبب تعدد مجالاتها، وهذا دفع العديد من الباحثين والخبراء ومنظمات العالمية إلى الإختلاف حول إحاطتها بمفهوم شامل وجامع يميزها عن غيرها من المفاهيم المشابهة.

المطلب الأول : تعريف التجارة الالكترونية

من حيث اللغة ينقسم مصطلح التجارة الإلكترونية إلى كلمتين:

التجارة: وتعني ممارسة البيع والشراء وهي حرفة التاجر الذي يمارس الأعمال التجارية على وجه الاحتراف .

أما الإلكترونية: يقصد بها القيام بالنشاط الإقتصادي باستخدام تكنولوجيا الاتصالات الحديثة[1].

نظرا للإهتمام العالمي والدولي سواء على مستوى الأفراد أو الشركات أو المنظمات الدولية بهذا النوع الجديد من التجارة عمدت اللجنة المنبثقة عن الأمم المتحدة والمتخصصة في القانون التجاري الدولي المعروفة بإسم Unictral إلى وضع تعريف للتجارة الإلكترونية في قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية، الصادرة في 16 ديسمبر 1996 حيث نص في المادة الثانية الفقرة "أ" منه على أنه: يراد بمصطلح" رسالة البيانات" المعلومات التي يتم إنشاءها أو إرسالها أو إستلامها أو تخزينها بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية، أو البريد الإلكتروني،أو البرق، أو التلكس، أو النسخ البرقي، كما عرفت الفقرة "ب" المقصود

[1]–حورية لشهب، " النظام القانوني للتجارة الإلكترونية، دراسة مقارنة "، مجلة العلوم الانسانية، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، الجزائر، العدد 2011 ،23، ص 28.

بمصطلح تبادل البيانات الإلكترونية بأنه: " نقل المعلومات إلكترونيا من حاسوب إلى حاسوب آخر باستخدام معيار متفق عليه لتكوين المعلومات."

أولا: التعريف الفقهي للتجارة الإلكترونية

وضعت العديد من التعريفات الفقهية للتجارة الإلكترونية لكل منها زاوية نظر في بناء تعريف لها، ونورد بعضا منها على سبيل المثال: عرف بعض الفقهاء التجارة الإلكترونية أنها : "نوع من عمليات البيع والشراء ما بين المستهلكين والمنتجين أو بين الشركات بعضهم وبعض بإستخدام تكنولوجيا المعلومات والإتصالات[1]."

وكذلك عرفها البعض بأنها هي كل معاملة تجارية تتم باستعمال وسيلة إلكترونية وذلك حتى إتمام العقد.

وعرفها جانب آخر من الفقه بأنها " عرض للسلع والخدمات على موقع الإنترنت ليحصل على طلبات من العملاء.[2]

من هذه التعريفات الفقهية المختلفة يمكننا أن نعرف التجارة الإلكترونية على أنها نظام إلكتروني يتيح التعامل في السلع و الخدمات في صيغة إفتراضية أو رقمية،وتنفيذ العقود المتعلقة بهذه السلع والخدمات.

ثانيا : تعريف التجارة الإلكترونية وفقا للمنظمات الدولية

لقد حاولت مختلف الهيئات والمنظمات الدولية وضع تعريف قانوني للتجارة الإلكترونية بعد تضارب آراء الفقهاء وتعددها، وأهمها:

1-عصام عبد الفتاح مطر، التجارة الالكترونية في التشريعات العربية والاجنبية، دار الجامعة الجديدة للنشر، الاسكندرية، 2009، ص17.

2- عصام عبد الفتاح، مرجع سابق، ص 18 وما بعدها.

أ – تعريف منظمة التعاون والتنمية الاقتصادية للتجارة الإلكترونية

عرفتها المنظمة على أنها جميع أشكال المعاملات المتعلقة بالنشاطات التجارية للمنظمة والفردية التي تتم بالاستناد على تبادل ونقل البيانات الرقمية " بما فيها النصوص والأصوات والصور الضوئية.

ومن خلال هذا التعريف يظهر لنا أن التجارة الإلكترونية شملت جميع الأنشطة التجارية.

ب– تعريف منظمة التجارة العالمية للتجارة الإلكترونية

قد عرفت التجارة الإلكترونية على أنها : " إنتاج وتسويق وتوزيع منتجات من خلال شبكات الاتصال.

ج – تعريف التجارة الإلكترونية وفقا لبعض التشريعات الأجنبية

فيما يتعلق بتعريف التجارة الإلكترونية في مشروعات وقوانين عربية فقد قامت كذلك بإعطائها تعريف فالمثال على ذلك: عرفها المشرع المصري في المادة 2 من مشروع قانون التجارة الإلكترونية على أنها: المعاملات الإلكترونية : هي كل معاملة تجارية تتم عن بعد باستخدام وسيلة إلكترونية.[1]

وفقا للمادة الثانية من قانون المبادلات والتجارة الإلكترونية التونسي رقم 53 لسنة 2000 فإن التجارة الإلكترونية: هي العمليات التجارية التي تتم عبر المبادلات الإلكترونية ."نجد المشرع الفرنسي عرفها على النحو التالي: مجموعة من المعاملات الرقمية المرتبطة بأنشطة تجارية بين المشروعات فيما بينها وبين المشروعات والأفراد، وبين المشروعات والإدارة . [2]

[1]– قانون المعاملات الإلكترونية المؤقت رقم 85 لسنة 2001 المنشور على الصفحة 2010 من عدد الجريدة الرسمية رقم 4524 لجمهورية مصر العربية بتاريخ 03 ديسمبر 2001، المادة (2).

[2]– عصام عبد الفتاح مطر، مرجع سابق، ص 23.

أما التشريع الأمريكي: كانت الولايات المتحدة الأمريكية من الدول السباقة والرائدة في مجال دعم وتشجيع استخدام أسلوب التجارة الإلكترونية في عقد الصفقات التجارية حيث أصدر المشرع الأمريكي سنة 1999 قانون المعاملات التجارية الإلكترونية، وما يلاحظ على هذا القانون الذي جاء مقسم إلى 21 جزء أنه لم يعرف التجارة الإلكترونية ولكنه عرف في المقابل ماهية الأعمال التجارية الإلكترونية وهذا من خلال الفقرة الثانية من المادة الثانية منه. [1]

كما عرفت **المادة 26 من الجزء 02** اللفظ "الكتروني" بأنه كل ما يتصل بالتكنولوجيا بوسيط إلكتروني له قدرات كهربائية أو رقمية أو مغناطيسية أو لا سلكية أو بصرية أو كهرومغناطيسية أو أي قدرات مماثلة.

وعلى الرغم من أن النظام القانوني للولايات المتحدة الأمريكية يتضمن عشرات التشريعات المنظمة للشؤون الثقافية والكمبيوتر والشبكات، إلا أن المشرع الأمريكي لم يضع تعريفا للتجارة الكترونية في قوانينه.

ثالثا : تعريف المشرع الجزائري للتجارة الإلكترونية

نظم المشرع الجزائري، ولأول مرة الإنترنت كنشاط إقتصادي متقن بموجب المرسوم التنفيذي رقم 98-257 المؤرخ في 25 غشت 1998، المتضمن ضبط شروط وكيفيات إقامة خدمات "انترنت" واستغلالها، المعدل والمتمم.

ولقد تزامنت عدة مراسيم وبعدها تعديل القانون المدني سنة 2005 بموجب القانون رقم 05-10 [2]في نصي المادتين 323 مكرر و 323 مكرر 1، وبهذا يكون قد أقر بالمعاملات الإلكترونية، وإن كان في قوانين متفرقة إلا أنه قام بوضع قانون مهم يتعلق بالتوقيع الإلكتروني، والتصديق الإلكتروني سنة 2015 وبعدها جاء تعديل قانون العقوبات

[1]- خالد ممدوح ابراهيم، لوجستيات التجارة الإلكترونية، دار الفكر الجامعي، مصر، 2008، ص 137.

[2]- قانون رقم 10-05 مؤرخ في 20 يونيو 2005، المتضمن القانون المدني المعدل والمتمم، ج.ر.ج.ج عدد 44،الصادر في 26 يونيو 2005 .

حيث أدخل الجرائم المستحدثة تحت فصل الجرائم الماسة بالأنظمة المعالجة للمعطيات،بموجب القانون رقم 04-15[1] المؤرخ في 10 نوفمبر 2004، ويتضمن المواد من 394 مكرر إلى 394 مكرر 7.

في سنة 2018 تيقن المشرع الجزائري بضرورة إصدار قانون التجارة الإلكترونية الذي جاء لحماية المستهلك الإلكتروني، وذلك وفقا للقانون رقم 18-05 المؤرخ في 10 مايو 2018 المتعلق بالتجارة الإلكترونية، حيث عرف هذا الأخير التجارة الإلكترونية في المادة 6 فقرة 1 على أنها : "النشاط الذي يقوم بموجبه مورد الإلكتروني بإقتراح أو ضمان توفير سلع وخدمات عن بعد لمستهلك إلكتروني عن طريق الإتصالات الإلكترونية.[2]

يلاحظ من خلال هذا التعريف أن المشرع لم يحدد الوسيلة التي يتم بها هذا النوع من المعاملات وبالتالي لم يحصرها في إطار شبكة الإنترنت هذا ما تتفق عليه جل التشريعات كنقطة الأولى، أما النقطة الثانية، لم يبين الطابع التجاري بل إكتفى بذكر مصطلح "نشاط" مع الإشارة إلى المقابل المالي لتوفير أو إقتناء السلع والخدمات حيث أشار أنه يمكن أن يكون مجاني، أي أنه وسع من هذا التعريف وترك المجال مفتوحا.

المطلب الثاني: خصائص التجارة الالكترونية

للتجارة الإلكترونية عدة مميزات تختلف عن التجارة التقليدية من أهمها ما يلي:

أولا: غياب العلاقة المباشرة بين الأطراف المتعاملة فيما بينها

يتم الاتفاق بين البائع والمشتري على العقد المبرم بينهما بكافة تفاصيله الدقيقة دون تواجدهما في مكان واحد فالرابط بينهما هو وجود جهاز إتصال يربط بينهما وهذا دليل

[1] -قانون رقم 15-04 مؤرخ في 10 نوفمبر 2004، معدل ومتمم الأمر رقم 156-66، المؤرخ في 8 يونيو سنة 1966، المتضمن قانون العقوبات، ج.ر.ج.ج العدد 71، الصادر في 10 نوفمبر 2004.

[2]- المادة 6/1 من قانون رقم 05-18، المؤرخ في 10 مايو 2018، المتعلق بالتجارة الإلكترونية، ج.ر.ج.ج عدد 28، الصادر في 16 مايو 2018.

على عدم وجود العنصر البشري، أي أن العملية التجارية تتم من خلال إستخدام تكنولوجيا المعلومات وشبكة الإتصالات في مواقع و أوقات مختلفة، وهذا خلافا للتجارة التقليدية[1].

ثانيا : تسليم المنتوجات إلكترونيا

لقد أتاحت التجارة الإلكترونية إمكانية تسليم بعض المنتوجات إلكترونيا، أي هناك تسليم قانوني و تسليم فعلي للمنتوجات .

مثل التقارير الإلكترونية إلى جانب بعض الخدمات مثل الإستشارات الطبية والهندسية، وهو ما يشكل تحدي حقيقي أمام السلطات المختصة، حيث لا يوجد حتى الآن آليات متفق عليها لإخضاع المنتجات الرقمية للجمارك أو للضرائب لغياب هذه المعاملات عن دفاتر المحاسبة الرقمية.[2]

ثالثا : كثافة المعلومات

إن كثافة المعلومات هي النتيجة المترتبة عن تطوير شبكة الإنترنت وهذه الكثافة تعبر عن كمية المعلومات المتاحة للمشتركين في السوق من زبائن وتجار، ومن الآثار الإيجابية لتطبيق التجارة الإلكترونية تخفيض تكلفة جميع البيانات ومعالجتها، وتوثيق هذه المعلومات وجعلها أكثر فائدة، وإتاحة الفرصة للزبائن للتعرف على مختلف الأسعار السائدة في السوق، والتكلفة الحقيقية للمنتوجات هذا من جهة ومن جهة أخرى تسمح هذه المعلومات التجارية بمعرفة الزبائن.

[1]– محمد منير جنيبهي، ممدوح محمد جنيبهي، الشركات التجارية، دار الفكر الجامعي، مصر، 2002، ص 09.

[2]– خالد ممدوح إبراهيم، لوجستيات التجارة الإلكترونية، مرجع سابق، ص 151.

رابعا : سرعة الأعمال التجارية

تتسم التجارة الإلكترونية بالسرعة الفائقة أي سرعة التعاقد وسرعة التسليم لكثير من الصفقات ومن ثم فهي تختزل عنهم الوقت، فقد إعتدنا أن نذكر عند التفرقة بين التجارة المحلية والدولية عاملي المسافة والوقت، والواقع أن التجارة الإلكترونية الدولية جاءت لتختزل هذين العاملين إذ هي تختزل الحدود وتتم في وقت قصير للغاية، إضافة إلى ذلك فهي توفر المال.

خامسا: العلاقات في التجارة الإلكترونية ذات طبيعة دولية

إن شبكة الإنترنت هي شبكة دولية تتسم بالحرية فلا تخضع لحدود أي دولة من ناحية الإقليم الجغرافي أو السياسة المتبعة وهي شبكة عالمية أي مفتوحة لكل شعوب العالم دون إستثناء وهو ما يجعل التجارة الإلكترونية، تمارس بكل حرية دون أن تكون مقيدة من طرف الدول بعد إزالة كل العقبات القانونية والمادة التي تكون حاجزا أمامها.

سادسا: التجارة الإلكترونية آدات لزيادة القدرة التنافسية

تعمل التجارة الإلكترونية على زيادة القدرة التنافسية وزيادة الصادرات نظرا لسهولة الوصول إلى مراكز الإستهلاك،و إمكانية تسويق السلع والخدمات عالميا، كما تتميز بطابع السرعة في إبرام العقود وإنهاء الصفقات، حسب متطلبات المستهلكين، وهي وسيلة تحقق المشاركة في مشروعات التجارة العالمية وبالتالي تتيح للمنتج إجراء المعاملات التجارية في مختلف دول العالم بفاعلية من خلال حفظ تكاليف السوق والدعاية والإعلان وتوفير الوقت مما يؤثر إيجابيا على تنشيط المشروعات[1].

[1]-أحمد أمداح، التجارة الإلكترونية من منظور الفقه الإسلامي، مذكرة مقدمة لنيل درجة الماجستير في الفقه، وأصوله، كلية العلوم الاجتماعية والإسلامية، قسم الشريعة، جامعة الحاج لخضر، باتنة، 2005، ص 29.

سابعا : وجود الوسيط الإلكتروني

وهو جهاز الحاسوب (الكمبيوتر) المتصل بشبكة الإنترنت لدى كل من أطراف التعاقد والتي تقوم بنقل التعبير عن الإرادة لكل من المتعاقدين بذات اللحظة على الرغم من تباعد الأمكنة.

المطلب الثالث: التنظيم القانوني للتجارة الالكترونية في الجزائر

يخضع تنظيم التجارة الإلكترونية في الجزائر لإطار قانوني حديث نسبيًا يهدف إلى مواكبة التطورات التكنولوجية وضمان حماية مختلف الأطراف المتعاملة عبر الوسائط الرقمية، وقد كرس المشرع هذا التوجه من خلال إصدار القانون رقم 18-05[1] المتعلق بالتجارة الإلكترونية، الذي يحدد القواعد العامة لممارسة هذا النوع من التجارة، بما في ذلك شروط إبرام العقود الإلكترونية، وواجبات المورد الإلكتروني، وحقوق المستهلك، خاصة ما يتعلق بالإعلام المسبق وحق العدول. كما يتكامل هذا القانون مع أحكام القانون المدني الجزائري التي تنظم القواعد العامة للعقود، بالإضافة إلى قانون حماية المستهلك وقمع الغش الذي يوفر حماية إضافية للمستهلك في البيئة الرقمية. ويعكس هذا الإطار القانوني سعي الدولة إلى تحقيق التوازن بين تشجيع الاقتصاد الرقمي وضمان الأمن القانوني للمعاملات الإلكترونية.

[1] .- القانون رقم 18-05 المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 28، سنة 2018، ص. 4-12

المبحث الثاني: مفهوم الاحتيال الالكتروني

يعد الاحتيال الالكتروني صورة من صور الاحتيال بوجه عام، ومع ذلك فهو يتميز ببعض الخصائص التي تميزه وتجعل له طبيعة قانونية خاصة نظرا لارتباطه بالحاسبات الآلية وتكنولوجيا المعلومات، لذا سوف نتناول من خلال هذا المبحث إستعراض المقصود بجريمة الإحتيال الإلكتروني ؟

المطلب الأول: تعريف الاحتيال الالكتروني

يتسم الاحتيال الإلكتروني ببعض الصفات التي تميزه عن غيره من الجرائم، وتجعل له طبيعة خاصة، نظرا لارتباطه بالحاسب الآلي وبرامج تكنولوجيا المعلومات، وسنتطرق في هذا المطلب إلى تعريف جريمة الاحتيال الإلكتروني، وإلى خصائصها وذلك في الفروع التالية:

الفرع الأول: تعريف الاحتيال الإلكتروني

يتطلب تحديد مفهوم جريمة الاحتيال الإلكتروني، الإشارة إلى الاحتيال في إطاره العام وفقا لمختلف التعاريف التي تضمنته كما سنوضحه في النقاط التالية:

أولا: تعريف جريمة الاحتيال الالكتروني لغة

الاحتيال هو الحذق وجودة النظر، والقدرة على دقة التصرف، والاحتيال هومحاولة المطالبتك الشيء بالحيل، والحيلة هي المكر والخديعة والكيد لكل فعل يقصد فاعله به خلاف ما يقتضيه ظاهره[1].

يذكر أيضا أن الاحتيال من الحيلة و أحال) الرجل أتى بالمحال وتكلم به و (المحالة) بالفتح الحيلة وقولهم لإحالة، أي لابد وهو (أحول) منه أي أكثر منه حيلة وهو أحوله رجل (حول) بوزن سكر أي بصير وهو حول قلب احتال من الحيلة. وتم الإشارة له باللغة

1-بولحية، شهيرة. سويح، دنيا زاد. الإحتيال الالكترونية، مجلة الدراسات القانونية والاقتصادية، جامعة سي الحواس بريكة،20191.ص37

الأجنبية الإنجليزية يسمى الاحتيال بكلمة fraud وتعني حيلة، خداع، غش وتسمى باللغة الفرنسية وهي الغش أو النصب وهي مرادفة كلمة fraude.

كما نجد ان مصطلح الاحتيال استخدم في العديد من الايات القرانية او الاحاديث النبوية لقوله تعالى: ﴿ يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُم بَيْنَكُم بِالْبَاطِلِ إِلَّا أَن تَكُونَ تِجَارَةً عَن تَرَاضٍ مِّنكُمْ ۚ وَلَا تَقْتُلُوا أَنفُسَكُمْ ۚ إِنَّ اللَّهَ كَانَ بِكُمْ رَحِيمًا﴾. [1]

ثانيا : تعريف جريمة الاحتيال الإلكتروني اصطلاحا

يقصد بالاحتيال بصفة عامة الغش والخداع الذي يعمد إليه الجاني للحصول من الغير ، بدون وجه حق على فائدة أو ميزة، كما أن الاحتيال كصورة مستحدثه تقوم على إساءة إستخدام الحاسب الآلي في نظم المعالجة الإلكترونية للبيانات بهدف الحصول بغير حق على أموال أو أصول أو خدمات، وهي صورة يتميز الاحتيال فيها عن صور وأنماط ما يسمى بالاحتيال التقليدي العادي وله سمات عدة أهمها التعقيد الناجم عن إستخدام المفاتيح والشفرات والدلائل الالكترونية في إرتكابه للجريمة[2].

إن جريمة الاحتيال بصفة عامة من الجرائم التي تقع على المال، غير أنه إلى حد الآن لا يوجد تعريف عام لجريمة الاحتيال الإلكتروني يمكن للباحثين الرجوع اليه لذلك تعددت المفاهيم التي وضعها الفقه واختلفت فيما بينها من حيث العناصر التي ينبغي توافرها لتحقيقه، ولقد توسعت غالبية التعريفات في مفهوم الاحتيال أو كما يطلقون عليه بالاحتيال المعلوماتي حيث تربط بين الاستخدام غير المشروع للحاسبات الآلية لتحقيق ربح مادي غير مشروع بصفة عامة وبينل الاحتيال الإلكتروني .

وقد عرف على أنه الإستلاء و الحيازة الكاملة على مال الغير بوسيلة يشوبها الخداع تسفر عن تسليم ذلك المال ، وعرفها آخر بأنها استعمال وسيلة من وسائل التدليس

---

[1]– سورة النساء، الاية 29

[2]–رستم، هشام محمد فريد. قانون العقوبات ومخاطر تقنية المعلومات. مكتبة الالات الحديثة. القاهرة: 1992، ص44.

التي نص عليها القانون على سبيل الحصر لحمل المجني عليه على تسليم الجاني مالا مملوكا لغيره نتيجة الوقوع في الغلط [1]، واختلفت القوانين في تسمية هذه الجريمة، كما هو الحال بالنسبة للقانون الفرنسي الذي تناول لأول مرة عبارة طرق احتيالية، واعتبر الاحتيال جريمة قائمة بذاتها في نص المادة (405)، التي نصت على أنه كل من يتوصل الى أن يسلب، أو يشرع في سلب مال أو بعض ثروة الغير، وأضاف ظرفا مشددا لجريمة الاحتيال أو الشروع فيها، يتحقق عندما ترتكب إما بانتحال صفة ضابط في الشرطة القضائية، أو مأمور الضبط في دائرة الدولة المدنية، أو في الجيش الفرنسي الأجنبي.

ثالثا : تعريف جريمة الاحتيال الإلكتروني فقهيا

أما فقهيا فقد جرى الاختلاف في المفهوم لدى البعض فمنهم من أطلق التعريف ومنهم من قيده، فبعض التعريفات لهذه الجريمة جاءت كالتالي: يقصد بها الاستيلاء بطريقة الحيلة أو الخداع على مال مملوك للغير بنية تملكه."

وقيل أيضا هي الغش والخداع الذي يعتمد إليه شخص للحصول من الغير دون حق على فائدة أو ميزة وهي سلوك ينطوي على خداع المجني عليه.

و قد عرف بعض الفقهاء الاحتيال الإلكتروني بأنه التلاعب العمدي بمعلومات وبيانات تمثل قيما مادية يختزنها نظام الحاسب الآلي، أو الإدخال غير المصرح به للمعلومات والبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أية وسيلة أخرى

من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملياته بناء على هذه البيانات أو الأوامر أو التعليمات، من أجل الحصول على ربح غير مشروع والحاق الضرر بالغير.

[1] بولحية، شهيرة. سويح، دنيا زاد. المرجع السابق، ص38.

رابعا : تعريف جريمة الاحتيال الإلكتروني في القانون الجزائري

بالرجوع للمشرع الجزائري نجد أنه يتناول جريمة الاحتيال الإلكتروني بشكل موحد، وكل ما يمكن قوله هو أن الطرق الاحتيالية التقليدية التي تضمنتها المادة 372 من قانون العقوبات على أنه كل من توصل إلى استلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبرام 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 أي شيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر وبغرامة مالية من 20.000 إلى 100.000 دينار جزائري[1].

كما ربط المشرع الجزائري مفهوم هذه الجريمة بانتحال الوظائف والألقاب أو الأسماء وإساءة استعمالها واعتبرت من قبيل جريمة الإحتيال، لأن الاحتيال لا يكون الغرض منه العائد المالي فقط، بل قد يعود إلى إعتبارات أخرى كالانتقام، ويأخذ أشكالا متعددة مثل ما أشارت اليه المواد (243) الى (246) من قانون العقوبات الجزائري

مثل التدخل بغير صفة في الوظائف العمومية والمدنية والعسكرية، أو القيام بعمل من أعمال هذه الوظائف.

أو إستعمال شخص لقبا متصلا بمهنة منظمة قانونا أو شهادة رسمية أو صفة حددت السلطة العمومية شروط منحها أو إدعى لنفسه شيئا من ذلك بغير أن يستوفي الشروط المفروضة لحملها.

[1] – قانون رقم 06–24 مؤرخ في 19 شوال 1445 الموافق 28 ابريل 2024 ، يعدل ويتمم الامر رقم 156–66 المؤرخ في 18 صفر 1386 الموافق 8 يونيو 1966 والمتضمن قانون العقوبات.

أو من إنتحل لنفسه بصورة عادية أو في عمل رسمي لقبا أو رتبة شرفية

الفرع الثاني: خصائص جريمة الاحتيال الإلكتروني

يقوم الاحتيال الإلكتروني على مجموعة من الخصائص تمثل فيما يلي:

1 – الاحتيال الإلكتروني من الجرائم العابرة للحدود

يعني ذلك أنها تمثل شكلا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كلها، مع وجود أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية دون أن تخضع لحدود الزمان والمكان، لذلك كان من السهولة إرتكاب الاحتيال مع عدم القدرة على كشفه، وهذه الخاصية خلقت العديد من المشاكل حول تحديد الدولة التي تكون صاحبة الإختصاص القضائي في حالة ما اذا كان المجرم من دولة والضحية من دولة أخرى، وكذا الإشكالية في القانون الواجب التطبيق وإجراءات الملاحقة القضائية، وبالنظر إلى الطبيعة الخاصة لهذه الجريمة وخطورتها على المستوى الدولي، كان من الضروري التعاون الدولي في المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء من أجل التكفل بالإيقاع بالمجرم المعلوماتي ومحاكمته[1].

2 – جريمة الاحتيال الإلكتروني جريمة ذات طابع ذهني

ومن الخصائص المميزة لجريمة الاحتيال أيضا أنها جريمة ذات طابع ذهني، باستعمال طرق احتيالية حيث تقوم هذه الجريمة على استخدام الجاني ذكاءه ودهاءه في ارتكابها، دون ان يستخدم وسائل العنف والقسوة، لذلك يتسم مرتكبي هذه الجريمة بتمتعهم بنسبة عالية من الفطنة والحيلة والدهاء، فمن المستلزمات الأساسية لهذه الجريمة أن تكون لدى مرتكب الجريمة مقدرة ذهنية على كشف الثغرات في نظام التعامل كي يصل الى

[1]– بولحية، شهيرة. سويح، دنيا زاد. المر جع نفسه، ص4

خداع ضحاياه، ويكون لديه القدرة على إختيار الظروف المناسبة ووسيلة الخداع التي تتناسب وشخص المجني عليه[1].

3 – الاحتيال الإلكتروني من الجرائم التي يصعب إكتشافها

توصف الجرائم الإلكترونية بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات، وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم وبالتالي فإن هذه الجرائم وفي الغالب لا تترك اثر لها بعد إرتكابها، كما يصعب الإحتفاظ الفني بأثارها إن وجدت، وهذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه الجريمة إلى خبرة فنية عالية متخصصة لإثباتها[2].

تقع جريمة الاحتيال الالكتروني في بيئة إفتراضية لا تترك أية أثار على مرتكبيها، لأن الضحية لا يلاحظها رغم أنها تقع أثناء وجوده على الشبكة، وهذا بفضل القدرات الفنية والتقنية التي يتمتع بها الجاني والتي تمكنه من إرتكاب جريمته بدقة[3].

4 – الاحتيال الإلكتروني من الجرائم التي لا تقوم على العنف

يعتمد إرتكاب هذا النوع من الجريمة لأسلوب لا يحتاج فيه الى مجهود عضلي كجرائم القتل والسرقة التقليدية، فتنفذ بأقل جهد ولا تتطلب نوعا من الإيذاء أو الاختطاف أو التكسير، بل تعتمد فقط على المعرفة الواسعة بتقنية المعلوماتية وشبكة الأنترنت

---

[1]– حسني. محمود نجيب. دروس في علم الجرائم والعقاب. القاهرة: دار النهضة العر بية، 1982، ص54.

[2]–الكعيبي. محمد عبيد. الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت. القاهرة: دار النهضة العربية،2009 ، ص 31.

[3]–بن الصغير. عبد المومن. الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن، الملتقى الوطني حول الجريمة المعلوماتية بين الو قاية والمكافحة، جامعة محمد خيضر بسكرة، 2015، ص5.

والإحاطة ببعض البرامج التشغيلية، لذلك يطلق على هذا النوع من الجرائم بالجرائم الناعمة.[1]

تتم عملية الاحتيال الإلكتروني أو كما تسمى بالجرائم الناعمة دون بذل جهد عضلي كجرائم السرقة التقليدية، فهي جريمة لا تعتمد على العنف بل يعتمد تنفيذها على الإلمام بالتقنيات المعلوماتية وتشغيل برامج الحاسوب والشكة العنكبوتية.[2]

المطلب الثاني: اركان جريمة الاحتيال الالكتروني

جريمة الاحتيال الإلكتروني هي جريمة مقصودة (عمدية)، وعليه فإن الركن المعنوي فيها يتطلب توافر القصد الجنائي بعنصريه العلم والإرادة، والقصد الجنائي الواجب توافره لقيام جريمة الاحتيال الإلكتروني ينطوي على قصد عام، يتحقق حين تنصرف إرادة الجاني إلى التلاعب بالمعلومات من أجل الإستيلاء على مال الغير مع علمه بذلك، فضلا عن توفر قصدا خاصا يتمثل في نية تملك مال الغير، وبناء على ذلك سنتعرض القصد الجنائي العام، ومدى وجوب توفر القصد الجنائي الخاص في هذه الجريمة.

الفرع الأول: الركن المادي

يعرف الركن المادي بصورة عامة بأنه سلوك إجرامي يتمثل في إرتكاب فعل جرمه القانون أو الإمتناع عن فعل أمر به القانون، ويستهدف الإعتداء على مصلحة يحميها القانون، ويقوم الركن المادي لجريمة الاحتيال الإلكتروني على سلوك إجرامي يستخدم فيه الجاني وسائل أو أساليب كاذبة عبر أي أداة إلكترونية يترتب عليها أن يسلم المجني عليه ماله رضاء وطواعية للجاني معتقدا بصدقه.

---

[1]– بولحية، شهيرة. سويح، دنيا زاد. المرجع السابق، ص42.

[2]–هراكي، حياة. واقع جريمة الإحتيال الإلكتروني في التجارة الإلكترونية، مجلة التغيير الاجتماعي، م8.، ع.، الاجتماعي الجزائر: 2023، ص52.

أولا : النشاط الإجرامي في جريمة الاحتيال الإلكتروني

يعرف النشاط الإجرامي بأنه: "السلوك المادي الخارجي الذي يصدر عن الجاني ليحقق النتيجة الإجرامية التي يعاقب عليها القانون وهو عنصر ضروري لكل جريمة، ولا يتدخل المشرع الجزائي بالعقاب قبل صدور النشاط المادي الخارجي المكون للجريمة وبالعودة إلى النصوص القانونية المتعلقة بجريمة الاحتيال الإلكتروني في التشريعين الاتحادي والسعودي فقد جاء في نص المادة 40 من المرسوم بقانون اتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية الاتحادي أنه: .... كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند، وذلك بالاستعانة بأي طريقة من الطرق الإحتيالية أو باتخاذ إسم كاذب أو إنتحال صفة غير صحيحة عن طريق الشبكة المعلوماتية أو نظام معلوماتي إلكتروني أو إحدى وسائل تقنية المعلومات."

1 –السلوك

حسب نص المادة 372 من قانون العقوبات الجزائري حصر المشرع الجزائري الأفعال التي تعتبر سلوك إجرامي لجريمة الاحتيال التي عرفها البعض أنها الأكاذيب مدعمة بمظاهر خارجية من بينها:

أ– 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 تغيير الواقعة وتقديم معلومات زائفة للآخرين على سبيل المثال: يمكن لشخص أن يدعى أنه يملك قدرات خارقة مثل قدرته على شفاء الأمراض وتحديد الإيماءات وحركات للإقناع الآخرين بصحة هذا ، ونتيجة لذلك يمكن أن يقع الآخرون في خطأ بتعرضهم للاحتيال وفقدان أموالهم.

وكل ما يؤدي إلى الخداع يمكن أن يعد طريقة احتيالية، ومن ثم فإن مجرد الكذب ومهما كان منمقا مرتبا يوحي بتصديقه لا يكفي لوحده لتحقق الطريقة الاحتيالية، ما لم يكن مصحوبا بمظاهر خارجية أو أعمال مادية يتعمد المحتال حبكها لحمل المجني عليه على تصديقه والإعتقاد بصحته، ولتحقق الاحتيال في إتخاذ إسم كاذب؛ يكفي أن يتخذ الجاني إسما غير إسمه الحقيقي، بشرط أن يؤدي إتخاذ الإسم الكاذب إلى خداع المجني عليه وإيقاعه في دائرة الاحتيال. مثال ذلك : أن يتخذ الجاني إسما كاذبا بهدف خداع المجني عليه عبر الشبكة المعلوماتية، كان يعرف نفسه للمجني عليه باسم شخص آخر صاحب شركة توريد أجهزة حاسوب، ومن ثم يخدع المجني عليه ويقوم بإبرام صفقة معه على أساس أنه صاحب الشركة ويقوم بعدها المجني عليه بإرسال الأموال إلى الجاني معتقدا أنه صاحب الشركة، فيتحقق هنا الاحتيال الإلكتروني.

ب –المظاهر الخارجية لجريمة الاحتيال الطرق الاحتيالية :

الطرق الاحتيالية عبارة عن مظاهر خارجية يلجا إليها الجاني لتأييد كذبه وخداعه وحمل المجني عليه على تصديقه، سواء كانت هذه المظاهر أفعالا صادرة عن الجاني أو عن شخص سواه، أو كانت ظروفا واقعية هيأها الجاني،[1] أو تهيأت بشكل عارض، فأحسن إستغلالها، والنشاط الإجرامي في الاحتيال الإلكتروني يبنى في أساسه على الخداع والغش والكذب، فيلجا الجاني إلى إستخدام الطرق الاحتيالية، وتغيير الحقيقة باستغلال الشبكة المعلوماتية أو النظام المعلوماتي الإلكتروني أو أية وسيلة من الوسائل التقنية للمعلومات لكي يستولي على مال منقول أو منفعة أو على سند أو توقيع هذا السند المملوك للمجني عليه دون وجه حق، مثال ذلك عندما يدعي الجاني أنه مستورد لأجهزة الحاسب الآلي من خلال شركة يملكها، فيقوم بمراسلة عدد من الشركات المعروفة لتزوده ببعض

[1]–محمد، وائل. نصيرات، عبد الرحمن. جريمة الإحتيال عبر شبكة المعلومات الدولية، دراسة مقارنة النظام السعودي والقانون الاردني،2018،ص33

هذه الأجهزة، فإن مجرد كذبه وإدعائه لا يشكل جريمة إحتيال، بل يتوجب عليه أن يدعم هذه الأكاذيب ببعض المظاهر الخداعة، والتي من شأنها، إيهام المجني عليه بصدق الجاني، وهذا ما أكدته المحكمة الاتحادية العليا بقولها: أن مجرد الأقوال والادعاءات الكاذبة مهما بالغ قائلها في توكيد صحتها لا تكفي وحدها لتكوين الطرق الاحتيالية، بل يجب لتحقيق هذه الطرق في جريمة الاحتيال أن يكون الكذب مصحوبا بأعمال مادية أو مظاهر خارجية تحمل المجني عليه علي الاعتقاد بصحته[1] .

لا يمكن أن تتوفر طرق احتيالية إلا في حالة تأييد الكذب الظاهر خارجيا وهو ما يقوم به الجاني من أجل تحقيق مبتغاه والإيقاع بالمجني عليه، ويتحقق ذلك في صور معينة:

- استعانة الجاني بشخص آخر.
-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.
-إستغلال الجاني وقائع ناقصة للتأييد أكاذيبه.

إتهام المجني عليه بأمر من الأمور المحددة قانونيا، يتم فيه التلاعب بعقول الناس من خلال نشر أكاذيب أو إذاعة أحداث مزيفة بهدف خداعهم سواء عن طريق إيداع مشروع غير حقيقي، أو تصوير حادثة وهمية بهدف إقناعهم بوجود أرباح وهمية أو إستعادة مبالغ خيالية سلبت بواسطة أساليب غير أخلاقية. كما يمكن إتهامهم بوجود سند

[1]- محمد، وائل. نصيرات، عبد الرحمن،مرجع سابق،ص35

دين غير صحيح أو وثيقة تسوية مزورة، 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 الاحتيال.
- اتهام بوجود سند دين غير صحيح أو سند مخالصة مزور[1].

2 - النتيجة الإجرامية

الشيء الذي يسعى الجاني إلى تحقيقه هو تسليم المجني عليه مال أو منقول للجاني وهو عنصر أساسي لقيام الجريمة ، أما عنصر التسليم في هذه الحالة فهو ما يميز جريمة الاحتيال عن جريمة السرقة، وفي هذا المقام تكون برضى المجني عليه، لكن في حالة السرقة يكون الإستيلاء عن الشيء خفية ودون علم المجني عليه أو دون رضاه.

ثانيا: الركن المادي للجريمة المعلوماتية

يتكون الركن المادي للجريمة المعلوماتية من:

1 - السلوك

ينقسم السلوك إلى صورتين فقد يكون بفعل إيجابي إذ يفترض فيه قيام الجاني بفعل إرادي بغية إحداث النتيجة معينة كما يمكن إن يكون بفعل سلبي، يأخذ وصف الإمتناع عن إتيان أمر يوجبه المشرع، بينما في الجريمة المعلوماتية يمكن أن نجده بنوعيه ومن جهة أخرى لا يمكننا أن نغفل التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي واكب تقدم الوسائل الحديثة. هذه الأخيرة التي ساعدت الجاني في الإبتكار والتي نجحت في الإنتقال من تقليدية السلوك الإجرامي إلى مجالات أكثر تعقيدا مما أوجد العديد

[1]-حمدان الرقب. أسامة. المرجع السابق، ص40

من الصعوبات وتتمثل هذه السلوكيات في الإعتداء على الإعلام الآلي ويتضمن أيضا التلاعب والتعديل في المعطيات بصورة غير قانونية[1].

2-النتيجة

تتمثل نتيجة الجريمة في الضرر الذي يلحق بشخص المجني عليه نتيجة الفعل المرتكب، وعلى سبيل المثال إذا قام الشخص بدخول موقع بشكل غير قانوني وقام بتهكيره أو تغيير تصاميمه مما يتسبب في إلحاق ضرر كبير بصاحب الموقع، فإن النتيجة الإجرامية تكون قد تحققت على الجانب الآخر إذا ما قام شخص بدخول موقع بشكل غير قانوني وقام بحذف البيانات وتسريبها أو إيقاف عمل الشبكة المعلوماتية أو تعطيلها فإن النتيجة الإجرامية تكون قد تحققت بمجرد تحقيق الفاعل لهدفه.

3- العلاقة السببية

تعني العلاقة السببية ذلك النشاط الذي يكون السبب وراء حدوث النتيجة وهي جزء من الركن المادي للجريمة، ومن الواضح أن النتيجة المقصودة هنا هي النتيجة المادية التي ترتبط بالنشاط والسلوك المعمول به إذا ما كان حذف أو تعديل للبيانات أو الدخول الغير مشروع والبقاء أو العرقلة وهذا ما تطرقنا له في سلوك الجريمة المعلوماتية[2].

الفرع الثاني: الركن المعنوي لجريمة الاحتيال الإلكتروني

جريمة الاحتيال الإلكتروني هي جريمة مقصودة (عمدية)، وعليه فإن الركن المعنوي فيها يتطلب توافر القصد الجنائي بعنصريه العلم والإرادة والقصد الجنائي الواجب توافره لقيام جريمة الاحتيال الإلكتروني ينطوي على قصد عام، يتحقق حين تنصرف إرادة الجاني إلى التلاعب بالمعلومات من أجل الاستيلاء على مال الغير مع علمه بذلك، فضلا عن توفر قصدا خاصا المتمثل في نية تملك مال الغير، وبناء على ذلك سنتعرض القصد الجنائي العام، ومدى وجوب توفر القصد الجنائي الخاص في هذه الجريمة.

---

[1]– قهوجي، علي عبد القادر. الحماية الجنائية لبرامج الحاسوب، بحث منشور في مجلة الحقوق للبحوث والدراسات القانونية،القاهرة: جامعة إلسكندرية ، 1992، ص 120.

[2]–بن دراج. علي إبراهيم. محاضرات في الجرائم المعلوماتية. المركز الجامعي أفلو الاغواط: 2021 ص15.

أولا : القصد الجنائي العام في جريمة الاحتيال الإلكتروني

يقوم القصد الجنائي العام في جريمة الاحتيال الإلكتروني بتوفر عنصرين، أولهما العلم، وثانيهما الإرادة، ويتوفر القصد العام بعلم الجاني بأن الأفعال التي يأتيها يعدها القانون وسائل إحتيال من شأنها خداع المجني عليه وحمله على تسليم المال، وإنصراف نية الجاني إلى الإستيلاء على الحيازة الكاملة لمال المجني عليه، فالقصد العام في جريمة الاحتيال الإلكتروني يتطلب أن يعلم المتهم أن التلاعب الذي تحدثه المعلومات التي يحتوي عليها نظام الحاسوب الآلي أو المعلومات التي يقوم بإدخالها إلى هذا النظام من شأنها أن تجعل الحاسوب الآلي يستجيب وفقا لهذه المعلومات، فيقوم بتنفيذ ما يصل إليه من تعليمات، فالفاعل يعلم أن ما يقوم بإدخاله من معلومات إلى نظام الحاسوب الآلي يعد من قبيل التلاعب بهذه المعلومات فمن يعتقد أن التعديل الذي يلحقه بالمعلومات داخل نظام

الحاسوب الآلي ضروري حتى تقوم هذه المعلومات بعملها على نحو صحيح داخل هذا النظام لا يتوافر لديه القصد المطلوب لقيام الجريمة، ويجب أن يعلم الجاني أن المال الذي يستولي عليه مملوك لغيره، ويستوي أن يكون مملوكا للمجني عليه أو لشخص آخر، وهو الوضع الغالب في الاحتيال الإلكتروني، وبصفة خاصة في الحالات التي تنطوي على تحويل إلكتروني غير مشروع للأموال حيث لا يعلم الفاعل في كثير من الأحيان شخصية المجني عليه[1].

ولا يتطلب في جريمة الاحتيال الإلكتروني أن يكون الفاعل على دراية وعلم بأن هذه الوسائل التي يستخدمها من الوسائل التي أشار إليها القانون وجرمها، ما دام أن إرادته إتجهت إلى القيام بهذا العمل، وأنه يعلم أن القيام به بحد ذاته مجرم بغض النظر عن الوسيلة المستخدمة، خصوصا أن مثل هذه الوسائل غالبا ما تكون قائمة على الابتكار

[1]– قورة. نائلة. المرجع سابق، ص 489.

والتطور وليس على سبيل الحصر، بل يكفي أن تكون هذه الوسيلة المستخدمة تنطوي على التلاعب غير المشروع بالبيانات والمعلومات[1].

ثانيا : القصد الجنائي الخاص في جريمة الاحتيال الإلكتروني

القصد الخاص هو الغاية التي يبتغيها فاعل الجريمة من وراء فعله المقصود، أي اتجاه نيته إلى إحداث أثر معين، ويتمثل في جريمة الاحتيال في إنصراف نية الفاعل إلى تملك المال المستولى عليه.

وقد إختلفت الآراء حول مدى إشتراط القصد الجنائي الخاص في جريمة الاحتيال الإلكتروني، فالبعض ذهب إلى وجوب تحققه، وأنه يلزم في الاحتيال إلى جانب القصد العام، وجوب تحقق القصد الخاص، أي نية محددة، وهي نية تملك الجاني للمنفعة أو المال من المجني عليه، وهو ذاته المتطلب في السرقة، وعليه لا تقوم الجريمة إذا كانت نية الجاني هي الاطلاع على السلعة المسلمة، أو الانتفاع بها وردها ثانية، ولا يقوم الاحتيال إذا كان الاستيلاء على المال بقصد المزاح.[2]

ووفقا لهذا الرأي يراد بنية التملك أن يباشر الجاني على الشيء الذي تسلمه مظاهر السيطرة التي ينطوي عليها حق الملكية، وأن يحرم المجني عليه من مباشرتها، كما أن القصد الخاص لا يستلزم أن تتجه إرادة الجاني إلى الإضرار بالمجني عليه، أو إلى الإثراء، فبمجرد اتجاه الجاني إلى التملك فهذا وحده كاف، [3]كمن يقوم بالاستيلاء على مال المجني عليه بالطرق الاحتيالية لسداد دين مدين به المجني عليه لصالحه.

وهناك رأي آخر يرى بأنه لا يلزم القصد الخاص لقيام جريمة الاحتيال الإلكتروني باعتبار أن نية التملك تدخل في عناصر القصد العام الذي تتجه الإرادة فيه إلى النشاط الإجرامي والنتيجة، والنتيجة كما هو معلوم تتمثل في تسليم المجني عليه للمال أو المنفعة

---

[1]– ممدوح. خالد إبراهيم. حوكمة الانترنت. الاسكندرية: دار الفكر الجامعي، 2011، ص391.

[2]–إبراهيم. عبد الخالق. الموسوعة الشاملة في جرائم الاشخاص والاموال، المكتب الفني للموسوعات القانونية، الاسكندرية2009ص 232

[3]– حسني. محمود نجيب. شرح قانون العقوبات. ط4.، القاهرة: دار النهضة العربية، 2012، ص118 .

للجاني، وهذا من شأنه تمكين المحتال من السيطرة على القصد محل الجريمة والظهور عليه بمظهر المالك، ومن ثم فلا حاجة لجعل نية التملك مستقلة ضمن القصد الخاص.

ثالثا : الركن الشرعي

يقصد بالركن الشرعي وجود نص قانوني يُجرّم الفعل المرتكب، انسجاما مع مبدأ لا جريمة ولا عقوبة إلا بنص"، وقد نظم المشرع الجزائري جريمة الاحتيال الإلكتروني من خلال المادة 394 مكرر من قانون العقوبات الجزائري، المعدل بموجب القانون رقم 23-06 المؤرخ في 20 ديسمبر 2006، والتي تنص على:

يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج كل من استخدم خداعاً إلكترونياً للاستيلاء على شيء مملوك للغير .[1]

كما جاء في الأمر رقم 09-01 المؤرخ في 23 يوليو 2009 ، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، نصوص مهمة تدعم الجانب الوقائي لهذه الجريمة.

وعليه، فإن الركن الشرعي في جريمة الاحتيال الإلكتروني يتحقق بوجود نصوص صريحة تجرم الأفعال الاحتيالية التي ترتكب بواسطة تقنيات الاتصال الحديثة، وهو ما يُعتبر شرطاً ضرورياً لقيام المسؤولية الجنائية

المطلب الثالث:أنواع الاحتيال الالكتروني و خصائصها في البيئة الرقمية

أصبحت الجرائم في عصر التقنية الحديثة أربعة أنواع، جرائم الاعتداء على النفس جرائم الاعتداء على المال، جرائم الاعتداء على المصلحة العامة، والجرائم الإلكترونية بعد أن كانت ثلاثة أنواع فقط[2]. وعلى هذا الأساس قسمت الأجهزة التي تتولى التحقيق في هذه الجرائم إلى:

---

[1]- المادة 394 الامر رقم 23-06 المؤرخ في 20 ديسمبر 2006، المتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية، العدد 84، سنة 2006.

[2]- مصطفى. محمد موسى. التحقيق في الجرائم الالكترونية. القاهرة: مطابع الشرطة، 20ص 286

أولا: أجهزة الأمن العام

وتختص بالتحقيق في جرائم الاعتداء على النفس والمال.

أ الجرائم الواقعة على الأشخاص

إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، ومثال على ذلك الاعتداء على المعلومات الإلكترونية الخاصة بالمحامين أو الأطباء أو المحاسبين أو غيرهم من المهنيين، وقد تتم هذه الجريمة من خلال الإطلاع على البيانات والمعلومات الخاصة.

ويتمثل الركن المادي في جريمة نشر مواد إباحية بالسلوك الذي يتخذه الفاعل بتهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة، ويقوم بنشرها على الانترنت، أما الركن المعنوي وهو الحالة النفسية للجاني أي أنه كان يقصد نشر الصور ولديه العلم والإرادة بذلك[1].

ب – الجرائم الواقعة على الأموال

لقد صاحب ظهور شبكة الانترنت تطورات في شتى المجالات، حيث أصبحت بعض المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء، مما إنجر عنه تطور وسائل الدفع والوفاء وأصبحت جزء لا يتجزأ من هذه المعاملات

وفي ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الإلكترونية وما أنجر عنه من تطور خاصة في وسائل الدفع والوفاء، وفي خضم التداول المالي عبر الانترنت أصبحت هذه المعاملات عرضة لأنواع شتى من الجرائم ومنها:

-السطو على بطاقات الائتمان والتحويل الإلكتروني غير المشروع.

- القمار وغسل الأموال عبر الانترنت.

-جريمة السرقة والسطو على أموال البنوك.

-تجارة المخدرات عبر الانترنت[2].

---

[1]- مصطفى. محمد موسى. المرجع نفسه، ص 289

[2]- صغير. يوسف. الجريمة الاكترونية عبر الانترنت. الجزائر: 2013، ص44.

ثانيا: جهاز التحقيق في الجرائم الإلكترونية.

وهذا النوع من الأجهزة لم ينشأ بعد في كل الدول العربية وإن كانت بعض الدول قد أنشأته منذ أن إستخدمت الحاسوب الآلي وشبكات المعلومات، ويرجع السبب الرئيسي لإنشاء جهاز متخصص للتحقيق الجنائي في الجرائم الإلكترونية إلى تحقيق الضبط الاجتماعي الإلكتروني لحماية للمجتمع من الجرائم الإلكترونية وذلك للحد منها وضبطها بعد وقوعها، وذلك بالعمل على الحصول على الدليل الإلكتروني من أجل إثبات الجريمة.

ويضاف إلى هذا السبب زيادة تفاعل المجرمين مع تقنية المعلومات، فقد إتضح أن المعلومات ستزيد التفاعل بين الإرهابيين ومهربي المخدرات والأسلحة وجماعات الجريمة المنظمة، فمن خلال عالم مرتبط شكليا سيكون هناك مدخل للمعلومات والتقنية والتمويل والخداع المعقد وتقنيات الأفكار الهدامة، وإذا تم إستخدام تلك الأجهزة سواء عن طريق الدول أو فاعلين غير دوليين سيصبح ذلك بمثابة الخاصية الرئيسية لمعظم التهديدات من الداخل للدول.[1]

ثالثا: أجهزة التحقيق في الجرائم المخلة بأمن الدولة

أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الداخل وتتولها أجهزة متخصصة مثل مباحث أمن الدولة في مصر، فرنسا والكويت. أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الخارج وتتولاها أجهزة متخصصة مثل المخابرات العامة في مصر[2].

وقد اشتغل الكثير من الجماعات المتطرفة الطبعة الاتصالية للأنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا معنى آخر في استعمال الانترنت التي

---

[1]–مصطفى. محمد موسى. المرجع السابق، ص291.

[2]– بوضياف، إسمهان. الجريمة الالكترونية والاجراءات التشر يعية لمواجهتها في الجزائر، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، ع11، سبتمبر2018، ص258.

لهم في ارتكاب جرائم غاية الشلك في حق المجتمعات والدول، بل الأخطر من ذلك أتاحت الانترنت الكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية الاقتصادية لهذه الأخيرة، خاصة فيما يتعلق بالدول التي يكون فيها نزاعات ويبقى المساس بالأمن الفكري من بين أخطر الجرائم المرتكبة عبر الانترنت.[1]

الفرع الثاني: خصائص الدليل الرقمي

يتميز الدليل الرقمي عن غيره من الأدلة الجنائية الأخرى بعدة خصائص أهمها:

-الطابع العلمي للدليل الرقمي أي أن عملية البحث عن الدليل الرقمي تتم في نطاق جغرافي داخل النظام الافتراضي.

-**الطابع التقني للدليل الرقمي:** إن الطبيعة العلمية للدليل الرقمي تقتضي التعامل مع هذا النوع من الأدلة الجنائية العلمية من قبل تقنيين في البيئة الافتراضية، فالطبيعة التقنية تقتضي أن يكون هناك توافق بين الدليل المستخلص والبيئة التي يكون فيها، لأن التقنية لا تنتج لنا سكين يتم به الكشف عن القاتل وانما تنتج نبضات أو مجالات مغناطيسية أو كهربائية.[2].

-**الدليل الرقمي دليل متطور** : وخاصية التطور التي يتمتع بها الدليل الرقمي ناتجة عن تزايد استخدام تقنية المعلومات الرقمية، بعد أن أصبحت أجهزة الحاسب الآلي وشبكة الانترنيت تشكل مستودعا هاما للمعلومات والبيانات الرقمية..

- **صعوبة ازالة أو تحطيم الدليل الرقمي :** ففي حالة محاولة اصدار أمر بإزالة ذلك الدليل فمن الممكن اعادة اظهاره من خلال ذاكرة الآلة التي تحتوي ذلك الدليل، بل أن محاولة محو الدليل تعد في حد ذاتها دليل، لأنه في حالة القيام بتلك العملية يتم تسجيلها في ذاكرة الآلة ويمكن استخراجه كدليل ضد من قام بالفعل، ويمكن ايضا عرض الدليل الرقمي على برامج وتطبيقات المعرفة اذا كان قد تعرض للعبث أو التحريف .[3]

---

[1]- بوضياف، إسمهان. المرجع نفسه، ص258.

[2]- بن يونس. عمر محمد. الدليل الرقمي. مصر: دون دار نشر، 2006، ص8.

[3]- اوشن، حنان. وادي، عماد الدين. االثبات الجنائي والوسائل العلمية الحديثة، الجزائر: دار الخلدونية للنشر والتوزيع، 2015، ص98،99.

خلاصة الفصل الاول :

من خلال ما تم التطرق إليه في هذا الفصل، يتضح أن التجارة الإلكترونية تمثل نمطًا حديثًا من المعاملات التجارية يقوم على استخدام الوسائل الإلكترونية، وقد ساهمت بشكل كبير في تطوير النشاط الاقتصادي وتوسيع نطاقه. غير أن هذه البيئة الرقمية، رغم مزاياها، أفرزت مخاطر متعددة، من أبرزها ظاهرة الاحتيال الإلكتروني.

كما تبين أن الاحتيال في التجارة الإلكترونية يتميز بخصائص خاصة تجعله أكثر تعقيدًا من الاحتيال التقليدي، سواء من حيث الوسائل المستعملة أو من حيث صعوبة اكتشافه وإثباته. وتعددت صوره وأساليبه، مما يستدعي تدخلًا قانونيًا فعالًا لمواجهته والحد من آثاره.

وعليه، فإن الإحاطة بالجوانب المفاهيمية لهذا الموضوع تشكل خطوة أساسية لفهم أبعاده القانونية، وهو ما سيتم التعمق فيه في الفصل الموالي من خلال دراسة الإطار القانوني وآليات مكافحة الاحتيال في التجارة الإلكترونية في التشريع الجزائري.

الفصل الثاني:
الآثار المترتبة على جريمة الاحتيال الإلكتروني

.تمهيـــد:

بعد التطرق في الفصل الأول إلى الإطار المفاهيمي للتجارة الإلكترونية والاحتيال الإلكتروني، من خلال تحديد المفاهيم الأساسية وبيان أهم الصور والأساليب المستعملة، تبرز أهمية الوقوف على الآثار التي تنجم عن هذه الجريمة، لما لها من انعكاسات متعددة تمس مختلف الجوانب القانونية والاقتصادية والاجتماعية.

فالاحتيال الإلكتروني لا يقتصر أثره على إلحاق الضرر بالمجني عليه من الناحية المالية فحسب، بل يمتد ليؤثر على الثقة في المعاملات الإلكترونية، ويعرقل تطور التجارة الرقمية، خاصة في الدول التي تسعى إلى ترسيخ الاقتصاد الرقمي، على غرار الجزائر. كما قد يترتب عنه آثار قانونية تتمثل في قيام المسؤولية الجزائية والمدنية، وما يستتبع ذلك من جزاءات وعقوبات تهدف إلى ردع الجناة وحماية الضحايا.

وعليه، يهدف هذا الفصل إلى دراسة مختلف الآثار المترتبة على جريمة الاحتيال الإلكتروني، من خلال تحليل الأضرار التي تصيب الأفراد والاقتصاد، إضافة إلى بيان النتائج القانونية المترتبة عنها، بما يساهم في إبراز خطورة هذه الجريمة وضرورة تعزيز آليات مكافحتها.

المبحث الأول: المسؤولية المترتبة عن الجريمة الاحتيال الإلكتروني

تُعدّ جريمة الاحتيال الإلكتروني من أبرز صور الجرائم المستحدثة التي أفرزها التطور التكنولوجي المتسارع، حيث أصبحت الوسائط الرقمية بيئة خصبة لارتكاب أفعال احتيالية تمسّ بالأموال والمعاملات الإلكترونية. وقد أثار هذا النوع من الجرائم إشكالات قانونية متعددة، خاصة فيما يتعلق بتحديد المسؤولية المترتبة عنها، سواء كانت مسؤولية جزائية تقع على عاتق الجاني، أو مسؤولية مدنية تهدف إلى جبر الضرر اللاحق بالضحية. وعليه، يقتضي الأمر دراسة مختلف أوجه المسؤولية الناشئة عن جريمة الاحتيال الإلكتروني، في ظل التشريعات الوطنية، لاسيما القانون الجزائري، ومدى كفايتها في مواجهة هذه الجرائم المستحدثة.

المطلب الأول: المسؤولية المدنية

تعد المسؤولية المدنية أحد الأعمدة الأساسية التي يقوم عليها النظام القانوني في أي مجتمع، إذ تهدف إلى حماية الحقوق الفردية وتنظيم العلاقات بين الأفراد، من خلال إلزام من يخل بهذه الحقوق بتعويض الضرر الناتج عن فعله، سواء كان ذلك الفعل عمدا أم إهمالا.

يقصد بالمسؤولية المدنية إخلال الفرد بالتزاماته القانونية التي تلحق الضرر بالغير، وتعرف كذلك أنها التزام بتعويض الضرر الناتج عن عدم تنفيذ الدائن الإلتزامه تجاه المدين، فالمضمون هنا هو الإلتزام بتعويض الأضرار التي لحقت بالغير، فالمسؤولية المدنية تهدف إلى إصلاح الضرر الذي لحق بالمضرور ، ويتم ذلك بمنحه تعويض مالي في أغلب الأحيان.[1]

تعد المسؤولية المدنية في إطار المعاملات الإلكترونية أمرا بالغ الأهمية، نظرا لما يشهده العالم من تحول تكنولوجي في مختلف مجالات الحياة، خاصة في ميادين التجارة

[1]-زروق عبد الحفيظ، ملخص المسؤولية القانونية في القانون الجزائري، المكتبة القانونية الجزائرية، 2022.ص 45.

الإلكترونية والخدمات، فقد أصبحت المعاملات الإلكترونية بديلا فعليا عن المعاملات التقليدية، مما أفرز أنماطا جديدة من العلاقات القانونية التي تبرم عبر الوسائط الإلكترونية، كالعقود المبرمة عن بعد، والتوقيعات الرقمية وتداول البيانات، والمعلومات الشخصية عبر الأنترنت.

وتعرف المسؤولية المدنية بأنها الإلتزام القانوني الذي يقع على عاتق الشخص نتيجة الإخلال بالتزامه مما يؤدي إلى إحداث ضرر بالغير، مما يستوجب جبر هذا الضرر عن طريق التعويض،[1] وعليه تنقسم المسؤولية المدنية الإلكترونية إلى نوعين المسؤولية العقدية الإلكترونية، والمسؤولية التقصيرية الإلكترونية.

الأول: المسؤولية العقدية للمعاملات الإلكترونية.

المسؤولية العقدية هي نوع من المسؤولية المدنية تنشأ نتيجة إخلال أحد أطراف العقد بالإلتزامات التي يرتبها عليه العقد، سواء بعدم التنفيذ كليا أو جزئيا، أو بتنفيذ الإلتزام على نحو معيب أو متأخر، ولا يشترط في هذه الحالة أن يكون العقد مكتوبا، يكفي أن يكون العقد صحيحا من الناحية القانونية، سواء كان العقد كتابة أو شفاهة.

لا تقوم امسؤولية العقدية في إطار المعاملات الإلكترونية إلا بتوافر ثلاثة أركان أساسية وهي الخطأ، والضرر، والعلاقة السببية بينهما، ولا يمكن أن يحكم بمسؤولية أحد المتعاقدين تجاه الآخر، إلا إذا ثبت توافر هذه الأركان الأساسية المتمثلة فيما يلي:

1-الخطأ العقدي الإلكتروني: ويتمثل الخطأ العقدي في إخلال أحد أطراف العقد الإلكتروني بتنفيذ التزام تعاقدي محمول عليه، سواء تمثل هذا الإخلال في عدم تنفيذ الإلتزام كليا، أو تنفيذه بشكل جزئي، أو التأخر في تنفيذه، أو غير مطابق للشروط الإلكترونية، وقد يكون هذا الخطأ في عدم تسليم الخدمة الإلكترونية، أو إرسال منتج إلكتروني معيب، أو تعطيل الولوج إلى المنصة الإلكترونية المتفق على إستخدامها،

[1]- عبد الرزاق السنهوري،المرجع السابق، ص 682

ويفترض أن المدين يتحمل تنفيذ التزاماته كما إتفق عليها وقت إبرام العقد إلكترونيا، طبقا لمبدأ – العقد شريعة المتعاقدين، وإذا لم يثبت وجود سبب أجنبي كقوة قاهرة أوحادث مفاجئ أو خطأ المضرور أو الغير يحول دون التنفيذ، فإن الخطأ يفترض بحقه دون حاجة لإثباته في بعض أنواع الإلتزامات، خاصة تلك التي تهدف إلى تحقيق نتيجة محددة[1].

وللخطأ العقدي الإلكتروني عدة صور ، تتمثل في تبادل المعلومات الإلكترونية والبيانات الشخصية، أو يكون الخطأ نتيجة لمعلومات مغلوطة أو ناقصة، و من بين هذه الصور:

الإمتناع عن تنفيذ التزام إلكتروني، وتتحقق هذه الصورة عندما يرفض أحد أطراف العقد تنفيذ ما تم الإتفاق عليه، كعدم تسليم الخدمة الإلكترونية، أو عدم تفعيل الإشتراك المتفق عليه، أو التوقف عن

تقديم الدعم الفني دون مبرر مشروع، و يعد هذا الخطأ من أكثر صور الإخلال الشائعة في العقود الإلكترونية.

من بين صوره أيضا التنفيذ غير المطابق لشروط العقد الإلكتروني، كأن يتم تسليم منتج إلكتروني لا يتوافق مع المواصفات المنصوص عليها في العقد، أو التأخر في تنفيذ الإلتزام الإلكتروني، وهو ما يحصل عندما يلتزم الطرف بتسليم منتج، أو أداء خدمة في موعد معين ضمن العقد الإلكتروني، ثم يتأخر في ذلك دون مبررات تقنية مقبولة، ما يؤدي إلى ضرر للطرف الآخر، مثل خسارة العملاء، أو توقف خدمة حيوية[2].

2 – **الضرر العقدي الإلكتروني:** كما في المادة 164 من قانون العقوبات الجزائري: "الا يكفي وقوع الخطأ بمفرده، بل من تحقق ضرر فعلي أصاب الدائن نتيجة لذلك الخطأ، ويشترط أن يكون هذا الضرر محققا، أو على الأقل محتمل الوقوع بطريقة

[1]– محمد حاتم، البيانات المسؤولية العقدية، الموسوعة القانونية المتخصصة هيئة الموسوعة العربية، دمشق المجلد القانون الخاص.ص121/106

[2]– نوال السعدي.المسؤولية المدنية في العقود الالكترونية.دار الجامعة الجديدة.الاسكندرية .2019.ص158.

مباشرة، ويشمل الضرر ما يصيب الذمة المالية كالخسارة أو فوات الفرصة، أو الضرر الأدبي كالمساس بالسمعة أو المشاعر شريطة أن يكون قابلا للتعويض قانونا".[1]

الضرر في المسؤولية العقدية والذي نقصد به ذلك الأثر لخطأ ما إرتكبه أحد الأطراف المتعاقدة، حيث يظهر لنا في عدة صور من بينها الضرر الذي يمس السلامة الجسدية، والضرر الذي ينقص من الذمة المالية والذي يسمى بالضرر المادي، أما الضرر الذي يمس كرامة الشخص وشعوره و أحاسيسه فنقصد به الضرر المعنوي.

3- العلاقة السببية بين الخطأ والضرر الإلكترونيين: وهي الركن الذي يربط بين الخطأ والضرر الذي أصاب المتعاقد الآخر، بحيث يكون الضرر نتيجة مباشرة للإخلال بالإلتزام، فإذا ثبت أن الضرر كان نتيجة سبب أجنبي لا دخل للمدين فيه إنتفت علاقة السببية، وبالتالي لا تقوم المسؤولية العقدية، كما قد تتعدد الأسباب المؤدية إلى الضرر، وهنا يتعين على القاضي تقدير السبب الأكثر ترجيحا وتأثيرا في وقوع الضرر.[2]

الخطأ التقصيري الإلكتروني: يعتبر الخطأ أحد الأركان الجوهرية التي لا تقوم المسؤولية التقصيرية بدونها، سواء في مجال المعاملات التقليدية، أو تلك التي تتم عن طريق الوسائل الإلكترونية، وعلى الرغم من إختلاف النظم القانونية في تحديد الأساس الذي تبنى عليه المسؤولية، إلا أن المشرع الجزائري قد تبنى كقاعدة عامة مبدأ الخطأ الواجب الإثبات كأساس لقيام المسؤولية، بإستثناء بعض الحالات الخاصة التي يعتد فيها بالضرر، أو بحالة الخطر كمبرر لتحمل المسؤولية[3]

---

[1]- المادة 164 من قانون العقوبات الجزائري.

[2]- عبد الرزاق السنهوري. المرجع السابق.ص928

[3]- فارس بوبكر . المسؤولية المدنية في مجال المعاملات الاكترونية.رسالة لنيل شهادة دكتوراه في العلوم تخصص عقود ومسؤولية مدنية. كلية الحقوق والعلوم السياسية.جامعة الحاج لخضر .باتنة1.2020.2021.ص13

الإختراق غير المشروع للأنظمة المعلوماتية، كقيام شخص بإختراق قاعدة بيانات شركة، أو موقع إلكتروني دون إذن، مما يؤدي إلى تسريب، أو تعديل، أو إتلاف معلومات حساسة.

نشر برامج خبيثة أو فيروسات إلكترونية، سواء بقصد تعطيل أنظمة الغير، أو التسبب بأضرار مالية، أو تشغيل المواقع أو أجهزة.

المطلب الثاني: المسؤولية الجزائية

المسؤولية تعني في أبسط معانيها تحمل التبعية (أو) المؤاخذة، فهي تدل على التزام شخص لتحمل عواقب فعله الذي أخل بقاعدة أو بنص جزائي[1]. وتعرف المسؤولية الجزائية بوجه عام بأنها عبارة عن التزام بتحمل الجزاء الذي ترتبه القواعد القانونية كأثر للفعل الذي يرتكب خروجاً على أحكامها[2]."

وبناء على ذلك يمكن القول بأن المسؤولية الجزائية هي التزام قانوني بتحمل العقوبة، فمتى ثبتت هذه المسؤولية بقرار قضائي صادر من محكمة جزائية مختصة ترتب عليها جزاء جنائي على فاعلها ومن اشترك فيها، كما وأن الجريمة التي يعنيها المشرع هي التي صدرت من الإنسان نتيجة خطئه ويسأل جزائيا عنها ويتحمل العقاب المقرر لها.

إذ أن هناك ارتباط وثيق بين المسؤولية الجزائية وبين الجريمة كواقعة أو حقيقة قانونية، ذلك لا يمكن تحقق الأولى في حال تخلف الثانية، إذ لا قيام لتلك المسؤولية دون مرتكب الجريمة والمسؤول عنها، وأن المجرم لا يأخذ هذه الصفة إلا بعد ثبوت ارتكابه الجريمة المنصوص عليها في قانون العقوبات.

المطلب الثالث: صعوبات تحرير المسؤولية في البيئة الرقمية

الجريمة الإلكترونية ظاهرة اجرامية مستجدة تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الاجرامي المجسدة للركن المادي لكل جريمة

[1]– خلفي عبد الرحمان، الاجراءات الجزائية في التشريع الجزائري.دار بلقيس.2015.ص91.

[2]–الحيدري جمال إبراهيم. احكام المسؤولية الجزائية.ط1.مكتبة السنهوري.2019.ص61

على حدى ، مع تطور أنماطها يوما بعد يوم وما أتاحته الشبكة من فرص جديدة لارتكابها،مما جعل إثباتها من العقبات التي يعمل الخبراء على كسرها من أجل إيجاد وسائل إثبات ناجعة على أساس أنها تتطلب خبرة فنية عالية واعتماد أسلوب واضح في التحقيق[1].

1-أسباب صعوبة اكتشاف وإثبات الجرائم الإلكترونية.

أ- تمتاز الجرائم المعلوماتية بصعوبة الإكتشاف وإثباتها وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز و الأرقام ، هي رمـــوز دقيقة ويصعب اكتشافها وإثباتها لهذا عـــادة ما يتم اكتشافها بالصدفة.

ب- فالجريمة المعلوماتية لا تترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية،يتم فيها نقل المعلومات وتناولها بواسطة نبضات إلكترونية غير مرئية.

ت-كذلك وسيلة التنفيذ فيها تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها ، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات

ث- يصعب العثور على دليل مادي للجريمة وذلك راجع إلى إستخـــدام الجـــاني وسائل فنية وتقنية معقدة لا يستغرق إلا ثواني معدودة يتـــم فيهـــا محو الدليل والتلاعب به .

ج – تتطلب خبـــرة وتحكما فـــي التكنولوجيا المعلوماتية عنـــد متابعتها، ولذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري، لابد أن يكون المحقق متخصص حتى لا يتسبب في إتلاف الدليل الإلكتروني.

1- د/عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي ، دار الكتب والوثائق المصرية،2006 ص 46.

ح- عدم وجود تعاون دولي، فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين و لكن النتيجة تحدث في بلد أخر ليس بالضرورة أن ينتج هذا السلوك أثاره في بلد المجرمين.[1]

خ- إختلاف النظم القانونية، و بالتالي عدم الإتفاق على الفعل المجرم ، فما هو محظور في الجزائر من الناحية الأخلاقية مباح في غيرها من الدول .

د- التطور السريع للجريمة و المعالجة البطيئة لقضايا ،أستفادة المجرم من هذه العقبات للعبث والتخريب و الإستمرار في الجريمة. ولهذه الأسباب وكذا الطبيعة الخاصة التي تتسم بها الجريمة أدى ببعض التشريعات الى تبنى الخبرة و المعاينة كأسلوبين للإثبات و التحقيق وكشف الجريمة.

2-**الخبـــرة والمعاينة:**

أ-**الخبرة:** يجب أن تكون الخبرة في هذا المجال من نوع خاص يتماشى وخصوصية الجريمة الإلكترونية،و قد تعمل بعض الدول على إعادة تأهيل بعض القراصنة من أجل الإستفادة من خبراتهم في الاختراق.وفي هذا الصدد يجب أن يتحلى الخبير بمؤهلات و مقدرة فنية عالية ،معرف تركيب الكمبيوتر،معرفة شاملة لشبكة الأنترنت، كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف[2] .

ب- **المعاينـــة:** قد تكون المعاينة حلا كإجراء لكشف بعض الجرائم الإلكترونية

ولتكون المعاينة لا بد من وجود مسرحا للجريمة، و هذا ما يصعب تحديده و بالتالي صعوبة الحفاظ على الآثار المادية إن وجدت ،و كما قد يحدث أن الفارق الزمني بين حدوث الجريمة و إكتشافها واسعا مما يؤثر سلبا في اكتشاف الدليل المادي و لإجراء

[1]-د/عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي ، دار الكتب والوثائق المصرية،2006 ص 46 .

[2]-محمد السعيد رشدى ، الانترنت والجوانب القانونية لنظم المعلومات ، بحث مقدم إلى المؤتمر العلمي الثاني لكلية الحقوق ،جامعة حلوان

المعاينة لا بد من تبليغ الجهة المؤهلة عالميا بتقنية خاصة من أجل التحفظ على الأدلة الموجودة وحتى أن تكون معاينة محكمة يجب توافر عدة تدابير منها، ضمان عدم إنقطاع التيار الكهربائي، العمل ضمن فريق.

و خلاصة القول فإن تأهيل الضبطية القضائية و إعادة النظر في التشريع الذي يحكمها أضحى ضرورة لا بد منها من أجل فتح المجال للعمل الإستدلالي.[1]

المبحث الثاني: آليات الحماية و الوقاية من جريمة الإحتيال الإلكتروني

في ظل الانتشار الواسع للتكنولوجيا الرقمية وتزايد الإعتماد على الوسائط الإلكترونية في مختلف المعاملات، برزت الحاجة الملحّة إلى وضع آليات فعّالة للحماية والوقاية من جريمة الاحتيال الإلكتروني، التي أصبحت تشكل تهديدًا حقيقيًا للأفراد والمؤسسات على حدّ سواء. ولا يقتصر التصدي لهذه الجريمة على الجانب الردعي فقط، بل يتعداه إلى تبني تدابير وقائية تشمل الإطار القانوني، والتقني، إضافة إلى نشر الوعي المعلوماتي لدى المستخدمين. ومن هذا المنطلق، يهدف هذا المبحث إلى تسليط الضوء على أهم الآليات المعتمدة للحدّ من جريمة الاحتيال الإلكتروني، ومدى فعاليتها في تحقيق الأمن الرقمي في ظل التشريع الجزائري.

المطلب الأول: ضوابط مشروعية الدليل الرقمي

إن الدليل الرقمي يجب أن يكون مشروعا أي أن إجراءات جمع الأدلة الرقمية المتحصلة من الحاسب الآلي إذا خالفت القواعد الإجراءات التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تبنى علها الإدانة في المواد الجزائية.

فإجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة في الدستور يكون

[1]– محمد السعيد رشدى ، الانترنت والجوانب القانونية لنظم المعلومات ، مرجع سبق ذكره.

باطلا بطلانا مطلقا لتعلقه بالنظام العام، ويجوز لكل ذي مصلحة التمسك به كما أن للمحكمة أن تقضي به من تلقاء نفسها.[1]

كأن يستخدم أعضاء الضبطية القضائية طرقا معلوماتية في أعمال التنصت على المحادثات الهاتفية، ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن الجرائم الإلكترونية، الإكراه المادي والمعنوي في مواجهة المتهم الإلكتروني من أجل فك شفرة نظام من النظم الإلكترونية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة، أو التحريض على ارتكاب الجريمة الإلكترونية من قبل أعضاء الضبطية القضائية، كالتحريض على الغش أو التزوير المعلوماتي أو التجسس المعلوماتي والاستخدام غير المصرح به للحاسوب، والتنصت والمراقبة الإلكترونية عن بعد.

يعد التشريع الجزائري من التشريعات التي تبنت نظام الإثبات الحر في مجال الإثبات الجنائي، مسايرة في ذلك النظم اللاتينية كفرنسا وبلجيكا، وهو الأمر الذي كرسته المادة 212 من قانون الإجراءات الجزائية والتي تنص على أنه: " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ولا يسوغ للقاضي يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه والملاحظ من خلال المادة أعلاه أن المشرع الجزائري فتح باب الحرية في وجه تقديم الأدلة وتركها لمعيار القناعة الشخصية لقاضي الموضوع تعزيزا لمبدأ إثبات قرنية البراءة ولمجال ممارسة حقوق الدفاع الفردية.

-**منظومة معلوماتية:** أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذ البرنامج معين

[1]-محمود، نور الهدى. حجية الدليل الرقمي في إثبات الجرمة المعلوماتية، مجلة الباحث للدراسات ألكاديمية، جامعة باتنة، ع11، جوان 2017، ص920.

معطيات معلوماتية أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

فالمشرع الجزائري في خلال النصين القانونيين السابقين لم يعرف الجريمة الإلكترونية وإنما تبنى الدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة .

وبالتالي وأمام صعوبة تتبع والكشف عن الجرائم الإلكترونية التي تعرف على أنها كل فعل أو امتناع من شأنها الإعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة في تدخل التقنية المعلوماتية، وأمام قصور القواعد التقليدية في مواجهة الجريمة كان لزاما على المشرع الجزائري التدخل بنصوص آمرة لتجريم الظاهرة من جهة وإصدار قوانين خاصة تتلاءم وطبيعة الجريمة ومستلزمات المكافحة التي تستدعي التعاون بين الجهات القانونية والمختصين في المعلوماتية زيادة على التعاون الدولي.

تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات بنص المواد 394 مكرر إلى المادة 394 مكرر 7، وباستقراء هذه المواد يتضح لنا أن المشرع قسم الجرائم الإلكترونية إلى أربع طوائف تتعدد بحسب المصالح المحمية التي تتمثل أساسا في سرية هذه المعطيات أو تكاملها وفي وفرتها وفي تكاملها هي:

-الطائفة الأولى: وتتضمن جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير وكذا جريمة الحذف والتغيير والتخريب في هذه المعطيات.

-الطائفة الثانية : الجرائم الإلكترونية بواسطة النظام المعلوماتي وأهمها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزنة في نظام معلوماتي.

-الطائفة الثالثة: الجرائم الإلكترونية المتعلقة بأمن الدولة ومؤسساتها كجرائم التجسس والإرهاب.

-الطائفة الرابعة: الجرائم الإلكترونية للشخص المعنوي والتي تعادل عقوبتها خمس مرات عقوبة الشخص الطبيعي المادة 394 مكرر 4 من قانون العقوبات. [1]في سنة 2006 قام المشرع بإدخال تعديلات جديدة مست القسم السابع مكرر منها، حيث تم تشديد العقوبة على كل الجرائم الواردة في هذا القسم دون المساس بالجرائم الواردة فيها، ويعود ذلك بالتأكيد إلى إقرار المشرع بأن الظاهرة جديدة ومستحدثة متميزة عن الجرائم التقليدية من حيث محلها وأشخاص مرتكبيها، وسعيا منها في ضمان المكافحة لم يميز بين نوعية المعلومات التي تطالها الحماية سواء كانت مادية أو اقتصادية أو مسائل أمنية غرضها في ذلك هو حتما تحقيق الردع العام على إثر التزايد الخطير النسب الجرائم المرتكبة وتنوعها وخطورتها على الأفراد من جهة وعلى الاقتصاد الوطني من جهة أخرى[2].

إجراءات جديدة للمواجهة تضمنت إصدار القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وهو القانون المنظم للفضاءات المعلوماتية بصفة عامة ومكافحة المجال الإجرامي المتصل بها من خلال قواعد تسمح بمتابعة هذا النوع من الجرائم ومرتكبيها بشكل يضمن شرعية الإجراءات المتخذة.[3]

---

[1] -تمديلي رحيمه. خصوصية الجريمة الالكترونية في القانون الجزائري و القوانين المقارنة.كتاب اعمال مؤتمر الجرائم الالكترونيةة ,ص 105

[2]- القانون06/23 المؤرخ في 20/12/2006 المعدل و المتمم لقانون العقوبات

2- ربيعي حسين , اليات البحث و التحقيق في الجرائم المعلوماتية. رسالة نيل شهادة دكتورى. كلية الحقوق . جامعة باتنة. 2015.2016. ص170.

يتكون القانون من ست فصول تتضمن تعريفا للجريمة المعلوماتية والتي لم تختلف كثيرا عما ورد في قانون العقوبات، أيضا بعض الأحكام المتعلقة بمراقبة الاتصالات الإلكترونية وأيضا القواعد الإجرائية لتفتيش المنظومات المعلوماتية، إضافة إلى إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ولعل أهم ما يثيره هذا القانون بالرغم من أنها جاءت لتكملة سلسلة الترسانة القانونية المواجهة الإشكالات القانونية التي ترتبط بتنوع الجريمة الإلكترونية وتطورها المستمر، بالرغم من ذلك يبقى الفصل الثاني من هذا القانون يقلق الحقوقيين بدعوى أن هذا القانون يجيز مراقبة الاتصالات الفردية من دون علمهم ومن دون أن يرتكبوا أي نوع من الإجرام المادي أو المعنوي وهو ما يشكل خرقا للحق في الخصوصية وانتهاكا لحقوق الإنسان وقرينة البراءة المكفولة دستوريا[1].

أولا: أساليب التحري الخاصة

إن أهمية جهاز الشرطة القضائية في الكشف عن الجريمة الإلكترونية والتعرف على المجرم الالكتروني تبعها استحداث المشرع الجزائري أساليب التحري الخاصة المستعملة بما تتناسب ومتطلبات ضبط الوجه الجديد للإجرام حتى يسمح للقضاء والشرطة أن تتكيف بدورها في مهامها مع الإجرام الجديد مستمدة شرعيتها من المواثيق الدولية التي صادقت عليها الجزائر وخاصة المادة 20 من اتفاقية باليرمو لمكافحة الجريمة المنظمة عبر الحدود الوطنية التي أدرجت الجريمة الإلكترونية كشكل من أشكال الجريمة المنظمة[2].

[1]–امحمدي بوزينة امنة. إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية. (دراسة تحليلية. الاحكام قانون االجراءات الجزائية وقانون الوقاية من جرائم الاعلام). كتاب اعمال ملتقى اليات مكافحة الجرائم الالكترونية في التشريع الجزائري.29/03/2017.الجزائر. ص 57.

[2]– عزز المشرع الجزائري بموجب القانون 06/22 نشاط ضبطية القضائية باجراءات لمواجهة بعض الجرائم المتضمن القانون الفساد بمقتضى المادة 56 منه الصورة التالة اذا تعلق الامر بجرائم الفساد و التسليم المراقب و الترصد الالكتروني والاختراق.

ما تجدر الإشارة إليه، أن هذه الأساليب لا يرخص بها إلا في بعض الجرائم المعينة من طرف المشرع الجزائري على سبيل الحصر لا المثال بما فيها الجريمة الإلكترونية استدركها المشرع بموجب تعديل قانون الإجراءات الجزائية القانون رقم:22-06 والتي تتمثل في:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

- وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

- جواز التسرب أو الاختراق للكشف عن الجريمة الإلكترونية بمقتضى المادة 65 مكرر 12 من القانون 06-22 المتضمن قانون العقوبات، ولأنه إجراء غير مألوف وخطير في عمل سلطات الضبط القضائي أحاطه المشرع بجملة من الضوابط أهمها: الإذن القضائي بالتسرب من وكيل الجمهورية أو قاضي التحقيق المادة 65 مكرر 11 وأيضا احترام المدة القانونية للتسرب.

ثانيا /التفتيش :

تتميز الجريمة الإلكترونية عن غيرها من الجرائم كونها من الجرائم التي يصعب إثباتها، لذلك يجيز المشرع الجزائري التفتيش في المنظومة المعلوماتية ضد كل جريمة يحتمل وقوعها وتتقلص معها الضمانات التي يشترطها المشرع عادة في الجرائم الأخرى نظرا لسرعة ارتكابها ومحو آثارها وتخطيها الحدود الوطنية.

وعن شروط إجراء عملية التفتيش في الجريمة الإلكترونية، فإنه وفي سبيل مكافحتها سمحت العديد من القوانين التبين عن هذه الجريمة والحصول على دليل الكتروني يمكن من خلاله إثبات أو نفي هذه الأخيرة عن المتهم أو المتهمين بها، ففي

التشريع الجزائري كانت بعض مواد القانون رقم 09-04 [1]المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مصدر مشروعية لهذا الإجراء فقد جاء في المادتين 03 [2]و 05 منه أنه "في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو المقتضيات التحريات والتحقيقات. وفي إطار قانون الإجراءات الجزائية يجور للمسلمات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بعرض التفتيش إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، أو الدخول وتفتيش منظومة تخزين معلوماتية. ولأن التفتيش يمس بخصوصية الأفراد ومستودع أسرارهم، خص هذا الإجراء بمجموعة من الضمانات التي تسمح بإيجاد توازن بين المصلحة العامة والخاصة.

والمادة 44 من قانون الإجراءات الجزائية الجزائري تضمنت مجموعة من هذه الضمانات؛ إذ لا يمكن القيام بعملية تفتيش مساكن الأشخاص الذين يظهر أنهم ساهموا في جناية أو جنحة متلبس بها أو التحقيق في الجرائم الإلكترونية، أو تفتيش مساكن أشخاص يتبين أنهم يحوزون أوراق أو أشياء لها علاقة بالأفعال الجرمية المرتكبة إلا بإذن مكتوب صادر من وكيل الجمهورية أو من قاضي التحقيق مع التأكيد على ضرورة إظهار ذلك الإذن قبل الدخول والشروع في التفتيش، كما أكدت فقرات تلك المادة على أن يتضمن الإذن وصفا للجرم المرتكب وكذا عنوان الأماكن التي سيتم زيارتها والتفتيش فيها، وكل ذلك تحت طائلة البطلان وذات الأمر نجده في المادة 91 من قانون الإجراءات الجنائية المصري، والتي قضت بأنه: "لا يجوز القيام بالتفتيش إلا بمقتضي أمر من قاضي التحقيق

[1]-القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، الصادر بتاريخ 16 أوت 2009 .

[2]- نص المادة 03 من القانون رقم 09-04 على إمكانية اتخاذ تدابير وقائية في حال وجود معلومات حول احتمال المساس بالمنظومات المعلوماتية.

بناء على اتهام موجه إلى شخص بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن تدل على أنه حائز لأشياء ما تتعلق بالجريمة المرتكبة[1]

المطلب الثاني: التدابير الوقائية و التعاون الدولي

إن الإستراتيجية الجزائرية اتجاه الجرائم الالكترونية تعتمد على مجموعة من الإجراءات يهدف حماية النظام العام في الدولة وفقا لقوانين الدولة مع وضع ترتيبات المراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها، والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية[2] وتمارس عمليات المراقبة من قبل الجهات المختصة في حالات عديدة أهمها:

-الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته إذن لمدة ستة أشهر قابلة للتجديد على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها توضع الترتيبات التقنية وتوجه حصريا لتجميع وتسجيل معطيات ذات صلة بالوقاية من الأفعال الإرهابية والاعتداءات على أمن الدولة ومكافحتها في حال توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني أو في حال صعوبة الوصول إلى نتيجة تهم الأبحاث الجارية متعلقة بمقتضيات التحريات والتحقيقات القضائية.

-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة حيث يمكن للسلطات. المختصة الجزائرية تبادل المساعدة القضائية في إطار التحريات أو التحقيقات القضائية

---

[1]- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 2006، ص 387.

[2]- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تقارير رسمية حول آليات الوقاية من الجرائم الإلكترونية في الجزائر.

الجارية لمعاينة الجرائم وكشف مرتكبها ولجمع الأدلة الخاصة بالجريمة الالكترونية تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية بناء على الاتفاقيات الدولية ذات الصلة والاتفاقيات الثنائية وحسب مبدأ المعاملة بالمثل بينما يتم رفض طلبات المساعدة الدولية إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام، وتضطلع هيئات وطنية وقضائية متخصصة والمعهد الوطني للأدلة الجنائية وعلم الجرائم لهذه المهام.

-باستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات، لاحظنا أن التسارع في مواكبة ومسايرة التطور تشهده التشريعات العالمية بات من السهولة إجراء التحويلات المالية عن الطريق الإلكتروني ذلك ما نصت عليه المادة 87 ، كما نصت المادة 84/2 منه على استعمال حوالات دفع عادية أو الكترونية أو برقية.

ثالثا :القوانين الخاصة للتصدي للجرائم الالكترونية

أ -قانون التأمينات:

تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي في نصوص قانونية عديدة تخص البطاقة الالكترونية التي تسلم المؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني وكذا للجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 92 مكرر.

ب- القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]

[1]-المواد من المادة الثانية حتى 14 من القانون رقم 09/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها.

جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكل ما يتعلق بالمنظومة المعلوماتية والمعطيات المعلوماتية ومقدمو الخدمات والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية من مراقبة وتفتيش المنظومات المعلوماتية عند الضرورة وحجز المعطيات المعلوماتية، وحفظ المعطيات المتعلقة بحركة السير على الالتزامات الخاصة بمقدمي خدمة الإنترنت، وأخيرا على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ج- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

في إطار الإصلاحات التي تنتهجها الجزائر مؤخراً ذات الطابع القانوني والأمني والسياسي، وإصلاح العدالة لتعزيز دولة القانون ولمكافحة الجريمة الإلكترونية. أصدرت عدة نصوص قانونية، والتي تم من خلالها إنشاء مصالح وهيئات، تضم عملية البحث مجموعة من الموارد البشرية والإمكانات المادية والتقنية التي تسهل البحث عن مرتكبي الجرائم الإلكترونية، وتمكن من القبض عليهم، وتسليمهم للجهات القضائية المختصة، الوطنية منها أو الدولية، ومن بينها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

وأنشئت بموجب القانون رقم 09/04 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق عمليات الوقاية والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالحالإستراتيجية للاقتصاد الوطني.

فبموجب المادة 13 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، نص المشرع الجزائري على

إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والتي كانت محط أنظار العديد من وسائل الإعلام التي تحدثت عنها، ولكن بعدها اختفت أخبارها، حتى اعتقد الجميع أنها ستبقى حبراً على ورق كغيرها من الكيانات القانونية التي كان مصيرها البقاء حبيسة المواد والنصوص القانونية، إلا أنه وفي الثامن من شهر أكتوبر سنة 2015 تم إصدار المرسوم الرئاسي رقم 15-261 والذي تم من خلاله تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[1]

وعلى غير العادة قام المشرع الجزائري بعدها بأربع سنوات تقريباً بإصدار مرسوم رئاسي آخر تحت رقم 19-172 والخاص بتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، والذي يتكون من خمس وعشرين مادة نصت المادة 24 منه على إلغاء المرسوم الرئاسي 15-261 الصادر سنة 2015 السالف الذكر، ثم بعد حوالي (13) شهراً قام المشرع بإصدار مرسوم رئاسي تحت رقم 20-183، والمتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، متكون من (38) مادة، ألغت المادة (37) منه المرسوم الرئاسي رقم 19-172 السالف الذكر.

أ- تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

[1]-المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية .

حسب المادة الأولى من المرسوم الرئاسي رقم 20-183[1]، فإن هذا المرسوم جاء ليعيد تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فمن خلاله يمكن معرفة تشكيلة هذه الهيئة وكذا طريقة وكيفية سيرها.

وبمقتضى المادة 02 و 03 من ذات المرسوم تعد الهيئة: "سلطة إدارية مستقلة تمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة رئيس الجمهورية"، "يحدد مقر الهيئة بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني بموجب مرسوم رئاسي"، وبمقارنة هاتين المادتين بالمادتين الثانية والثالثة من المرسوم الرئاسي رقم 19-172 الملغي والذي كان يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، وكذا المرسوم الرئاسي 15-261 الذي سبقه، يتبين أن هناك تغيير جوهري يستوجب الوقوف عنده، فمن خلال المادة الثانية من المرسوم الرئاسي رقم 19-172[2] جرد المشرع الجزائري الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من صفتين مهمتين كانتا موجودتين في المرسوم الذي سبقه ألا وهما الاستقلالية الإدارية والسلطة الإدارية التي تخضع لها الهيئة.

ح- الهيئات القضائية الجزائية المتخصصة:

[1]- المرسوم الرئاسي رقم 20-183 المؤرخ في 22 جويلية 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، يتضمن 38 مادة.

[2]- المرسوم الرئاسي رقم 19-172 المؤرخ في 10 جوان 2019، المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها (ملغى).

أنشئت بموجب القانون 14-04 المؤرخ في 10/01/2004 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 32/38/40 من ق ا ج ج تتمتع باختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 06-348 المؤرخ في 05/10/2006 بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09-04 .[1]

خ -المعهد الوطني للأدلة الجنائية وعلم الجرائم.

يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة التكوين والتعليم وتقديم المساعدات التقنية ودائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات.

د -المديرية العامة للأمن الوطني

تتصدى هذه المديرية للجريمة الإلكترونية من عدة جوانب ومنها الجانب التوعوي بحيث لم تفضل المديرية العامة للأمن الوطني عن الوقاية التوعية وهذا من خلال برمجتها التنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها نوعية المواطن حول خطورة الجرائم

[1]- عياش هواري . مداخلة بعنوان . مسار التحقيقات الجمالية في مجال الجريمة المعلوماتية

الالكترونية ودائما في إطار مكافحة الجريمة الالكترونية. ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم، فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية (INTER) القضائية.[1]

خلاصة الفصل الثاني:

من خلال ما تم تناوله في هذا الفصل، يتضح أن جريمة الاحتيال الإلكتروني تُخلّف آثارًا متعددة ومتداخلة، لا تقتصر على الجانب المالي فحسب، بل تمتد لتشمل أبعادًا قانونية واقتصادية واجتماعية. فقد تبين أن هذه الجريمة تؤدي إلى إلحاق أضرار مباشرة بالضحايا، تتمثل أساسًا في الخسائر المالية وانتهاك البيانات الشخصية، وهو ما ينعكس سلبًا على شعور الأفراد بالأمن والثقة في البيئة الرقمية.

كما أن انتشار الاحتيال الإلكتروني من شأنه أن يُضعف الثقة في التجارة الإلكترونية، ويُعيق نمو الاقتصاد الرقمي، خاصة في الدول التي تسعى إلى تطوير هذا المجال، الأمر الذي يستدعي اتخاذ تدابير فعالة لتعزيز الحماية القانونية للمستهلكين والمتعاملين عبر الإنترنت.

[1]– المنظمة الدولية للشرطة الجنائية (INTERPOL)، إطار دولي للتعاون الأمني في مجال مكافحة الجرائم العابرة للحدود، بما فيها الجرائم الإلكترونية.ص1

ومن الناحية القانونية، يترتب عن هذه الجريمة قيام المسؤولية الجزائيـــة للجاني إلى جانب إمكانية قيام المسؤولية المدنية لجبر الضرر وتعويض الضحايا، وهو ما يعكس حرص المشرّع على مواجهة هذه الظاهرة وردع مرتكبيها. غير أن فعالية هذه الآليات تبقى رهينة بمدى تطورها ومواكبتها للتغيرات التكنولوجية المتسارعة.

وعليه، فإن الحد من الآثار السلبية لجريمة الاحتيال الإلكتروني يقتضي تعزيز المنظومة القانونية، وتكثيف الجهود التوعوية، إلى جانب تطوير الوسائل التقنية والأمنية بما يضمن تحقيق بيئة رقمية آمنة تدعم نمو التجارة الإلكترونية وتحمي مختلف المتعاملين فيها.

خاتمة

خاتمة:

في ختام هذا البحث نستنتج أن جريمة الاحتيال الإلكتروني تعد من أبرز الجرائم التي شهدها العصر الحديث نتيجة لتطور التكنولوجيا وانتشار استخدام الإنترنت في مختلف جوانب الحياة اليومية، مع تزايد الاعتماد على الوسائل الرقمية في التواصل والتعاملات المالية والتجارية، أصبحت فرص وقوع الأفراد والشركات ضحايا لهذه الجرائم كبيرة ومتنوعة. حيث يستخدم المجرمون طرقاً متطورة ومبتكرة لخداع الضحايا، مثل انتحال الشخصيات، ورسائل التصيد الاحتيالي، والبرمجيات الخبيثة التي تهدف إلى سرقة البيانات الحساسة والمعلومات البنكية. وما يزيد الأمر خطورة هو أن هذا النوع من الجرائم يتصف بالسرعة العالية والتخفي مما يصعب على الأجهزة الأمنية تتبع الجناة والقبض عليهم بسهولة.

-وأسفر عن هذا العديد من النتائج أهمها:

إنتشار واسع لجرائم الاحتيال الإلكتروني بسبب الاعتماد المتزايد على الإنترنت والتقنيات الرقمية في الحياة اليومية.

ضعف الوعي الأمني عند المستخدمين يشكل عاملا رئيسيا في نجاح عمليات الاحتيال.

-أهمية تطوير الحلول التقنية لتعزيز الحماية والكشف المبكر عن محاولات الاحتيال.

ضعف التنسيق بين الجهات الأمنية والقطاع الخاص يؤثر سلباً على فعالية المكافحة.

تراجع ثقة المستخدمين في التعاملات الرقمية نتيجة تعرضهم للاحتيال.

-وجود فجوة بين التطور التكنولوجي السريع وقدرة المؤسسات على التصدي للجرائم الإلكترونية.

-ومن هذه النتائج اقترحنا مجموعة توصيات:

رفع مستوى الوعي الأمني لدى جميع مستخدمي الإنترنت من خلال حملات تعليمية وتثقيفية مستمرة.

خاتمة:

تحديث القوانين والتشريعات لتشمل جميع أشكال الاحتيال الإلكتروني وتوفير عقوبات رادعة. تعزيز التعاون الدولي بين الدول لتبادل المعلومات والتنسيق في ملاحقة المجرمين.

تشجيع البحث والتطوير في مجال الأمن السيبراني لتطوير تقنيات جديدة لرصد ومنع الاحتيال.

تفعيل دور القطاع الخاص في تبني أنظمة حماية قوية وتحسين نظم الكشف المبكر عن الهجمات الإلكترونية.

توفير دعم نفسي ومالي للضحايا لمساعدتهم على التعافي واستعادة ثقتهم.

توجيه المستخدمين لتبني ممارسات أمنية سليمة مثل تحديث البرامج، وعدم مشاركة البيانات الشخصية عبر قنوات غير آمنة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

1. القرآن الكريم

أولاً: الكتب

1. أحمد فتحي سرور، **الوسيط في قانون الإجراءات الجنائية**، دار النهضة العربية، القاهرة، 2006.
2. أوشن، حنان؛ وادي، عماد الدين، **الإثبات الجنائي والوسائل العلمية الحديثة**، دار الخلدونية للنشر والتوزيع، الجزائر، 2015.
3. إبراهيم، عبد الخالق، **الموسوعة الشاملة في جرائم الأشخاص والأموال**، المكتب الفني للموسوعات القانونية، الإسكندرية، 2009.
4. بن يونس، عمر محمد، **الدليل الرقمي**، (دون دار نشر)، مصر، 2006.
5. بن دراج، علي إبراهيم، **محاضرات في الجرائم المعلوماتية**، المركز الجامعي أفلو الأغواط، 2021.
6. الحيدري، جمال إبراهيم، **أحكام المسؤولية الجزائية**، الطبعة الأولى، مكتبة السنهوري، 2019.
7. حسني محمود نجيب، **شرح قانون العقوبات**، الطبعة الرابعة، دار النهضة العربية، القاهرة، 2012.
8. حسني محمود نجيب، **دروس في علم الجرائم والعقاب**، دار النهضة العربية، القاهرة، 1982.
9. خالد ممدوح إبراهيم، **لوجستيات التجارة الإلكترونية**، دار الفكر الجامعي، مصر، 2008.
10. خلفي عبد الرحمان، **الإجراءات الجزائية في التشريع الجزائري**، دار بلقيس، 2015.

11.رستم، هشام محمد فريد، **قانون العقوبات ومخاطر تقنية المعلومات**، مكتبة الآلات الحديثة، القاهرة، 1992.

12.زروق عبد الحفيظ، **ملخص المسؤولية القانونية في القانون الجزائري**، المكتبة القانونية الجزائرية، 2022.

13.صغير، يوسف، **الجريمة الإلكترونية عبر الإنترنت**، الجزائر، 2013.

14.عصام عبد الفتاح مطر، **التجارة الإلكترونية في التشريعات العربية والأجنبية**، دار الجامعة الجديدة للنشر، الإسكندرية، 2009.

15.عبد الفتاح مراد، **شرح التحقيق الجنائي الفني والبحث الجنائي**، دار الكتب والوثائق المصرية، 2006.

16.عبد الرزاق السنهوري، **الوسيط في شرح القانون المدني**،)دون ذكر بيانات النشر.(

17.الكعيبي محمد عبيد، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت**، دار النهضة العربية، القاهرة، 2009.

18.ممدوح خالد إبراهيم، **حوكمة الإنترنت**، دار الفكر الجامعي، الإسكندرية، 2011.

19.محمد حاتم، **المسؤولية العقدية**، الموسوعة القانونية المتخصصة، هيئة الموسوعة العربية، دمشق.

20.محمد منير جنيبهي، ممدوح محمد جنيبهي، **الشركات التجارية**، دار الفكر الجامعي، مصر، 2002.

21.مصطفى محمد موسى، **التحقيق في الجرائم الإلكترونية**، مطابع الشرطة، القاهرة.

22.نوال السعدي، **المسؤولية المدنية في العقود الإلكترونية**، دار الجامعة الجديدة، الإسكندرية، 2019.

ثانياً: الرسائل والأطروحات الجامعية

1. أحمد أمداح، **التجارة الإلكترونية من منظور الفقه الإسلامي**، مذكرة مقدمة لنيل درجة الماجستير في الفقه وأصوله، كلية العلوم الاجتماعية والإسلامية، قسم الشريعة، جامعة الحاج لخضر، باتنة، 2005.
2. ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، رسالة لنيل شهادة الدكتوراه، كلية الحقوق، جامعة باتنة، 2015-2016.
3. فارس بوبكر، **المسؤولية المدنية في مجال المعاملات الإلكترونية**، رسالة لنيل شهادة الدكتوراه في العلوم، تخصص عقود ومسؤولية مدنية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة 1، 2020-2021.

ثالثاً: المقالات العلمية

1. بوضياف، إسمهان، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، **مجلة الأستاذ الباحث للدراسات القانونية والسياسية**، العدد 11، سبتمبر 2018، ص258.
2. بولحية، شهيرة؛ سويح، دنيا زاد، "الاحتيال الإلكتروني"، **مجلة الدراسات القانونية والاقتصادية**، جامعة سي الحواس، بريكة، 2019.
3. حورية لشهب، "النظام القانوني للتجارة الإلكترونية (دراسة مقارنة)، **مجلة العلوم الإنسانية**، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، الجزائر، العدد 23، 2011.
4. حمدان الرقب، أسامة، "الجرائم الإلكترونية"، **مجلة الحقوق للبحوث والدراسات القانونية**، جامعة الإسكندرية.
5. قهوجي، علي عبد القادر، "الحماية الجنائية لبرامج الحاسوب"، **مجلة الحقوق للبحوث والدراسات القانونية**، جامعة الإسكندرية، 1992.

6. محمود، نور الهدى، "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية"، **مجلة الباحث للدراسات الأكاديمية**، جامعة باتنة، العدد 11، جوان 2017، ص920.
7. هراكي، حياة، "واقع جريمة الاحتيال الإلكتروني في التجارة الإلكترونية"، **مجلة التغيير الاجتماعي**، المجلد 8، الجزائر، 2023..

رابعاً: القوانين والتشريعات

أ- القوانين الجزائرية:

1. دستور الجزائر 2020.
2. قانون الإجراءات الجزائية الجزائري (القانون رقم 25-14)
3. قانون العقوبات الجزائري (الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المعدل والمتمم)
4. الأمر رقم 23-06 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون العقوبات.
5. القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات.
6. القانون رقم 06-24 المؤرخ في 19 شوال 1445 الموافق 28 أبريل 2024، المعدل والمتمم لقانون العقوبات.
7. القانون المدني الجزائري (القانون رقم 05-10 المؤرخ في 20 يونيو 2005، المعدل والمتمم)
8. القانون رقم 18-05 المؤرخ في 10 مايو 2018، المتعلق بالتجارة الإلكترونية.
9. القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ب- القوانين المصرية:

1. قانون المعاملات الإلكترونية المؤقت رقم 85 لسنة 2001، المنشور على الصفحة 2010 من عدد الجريدة الرسمية رقم 4524 لجمهورية مصر العربية، بتاريخ 03 ديسمبر 2001، المادة (2)

خامساً: المراسيم والتنظيمات

1. المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
2. المرسوم الرئاسي رقم 19-172 المؤرخ في 10 جوان 2019، المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها.
3. المرسوم الرئاسي رقم 20-183 المؤرخ في 22 جويلية 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

سادساً: المصادر الأخرى

أ- مداخلات وملتقيات علمية:

1. امحمدي بوزينة أمنة، "إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام) كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، 29مارس 2017، الجزائر.

2. بن الصغير، عبد المومن، "الطبيعة الخاصة للجريمة المرتكبة عبر الإنترنت في التشريع الجزائري والتشريع المقارن"، **الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة**، جامعة محمد خيضر، بسكرة، 2015.

3. تمديلي رحيمة، "خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة"، **كتاب أعمال مؤتمر الجرائم الإلكترونية**.

4. عياش هواري، "مسار التحقيقات الجمالية في مجال الجريمة المعلوماتية" (مداخلة علمية)

5. محمد السعيد رشدي، "الإنترنت والجوانب القانونية لنظم المعلومات"، **بحث مقدم إلى المؤتمر العلمي الثاني**، كلية الحقوق، جامعة حلوان.

ب- تقارير:

1. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تقارير رسمية حول آليات الوقاية من الجرائم الإلكترونية في الجزائر.

2. المنظمة الدولية للشرطة الجنائية(INTERPOL) ، إطار دولي للتعاون الأمني في مجال مكافحة الجرائم العابرة للحدود، بما فيها الجرائم الإلكترونية.

فهرس
المحتويات

العنوان	الصفحة
الشكر	
الإهداء	
مقدمة	
الفصل الأول: الاطار مفهوم الاحتيال في التجارة الالكترونية	
تمهيد	08
المبحث الأول: مفهوم التجارة الالكترونية	09
المطلب الأول : تعريف التجارة الالكترونية	09
المطلب الثاني: خصائص التجارة الالكترونية	13
المطلب الثالث: التنظيم القانوني التجارة الالكترونية في الجزائر	16
المبحث الثاني: مفهوم الاحتيال الالكتروني	17
المطلب الأول: تعريف الاحتيال الالكتروني و خصائصه	17
المطلب الثاني: اركان جريمة الاحتيال الالكتروني	23
المطلب الثالث: أنواع الاحتيال الالكتروني و خصائصها في البيئة الرقمية	31
خلاصة الفصل	35
الفصل الثاني: الاثار المترتبة على جريمة الاحتيال الالكتروني	
تمهيد	37
المبحث الأول: المسؤولية المترتبة عن الجريمة الاحتيال الالكتروني	38
المطلب الأول : المسؤولية المدنية	38
المطلب الثاني : المسؤولية الجزائية	42
المطلب الثالث: صعوبات تحرير المسؤولية في البيئة الرقمية	43
المبحث الثاني : اليات الحماية و الوقائية من جريمة الاحتيال الالكتروني	46
المطلب الأول : آليات الحماية التشريعة و العلمية	46
المطلب الثاني: التدابير الوقائية و التعاون الدولي	52
خلاصة الفصل	59
خاتمـــــة	61
قائمـــة المصادر والمراجع	64