جامعـة اكلـــي محنـــد اولحاج-البويـــرة
كليـة الحقـوق والعلـــوم السياسيـــة
القـسم العـــــــــام

قسم الحقوق **تخصص قانون جنائي**

الحماية الجنائية للمستهلك الإلكتروني

مذكرة مقدمة لنيل شهادة الماستر في القانون

إعداد الطالب:
مسلم آدم

تحت إشراف الأستاذة:
بوترعة سهيلة

تشكيل لجنة المناقشة

- د. حوت فيروز .....رئيسا
- د. بوترعة سهيلة.....مشرفا ومقررا
-أ.مزهود حكيم.....ممتحنا

السنة الجامعية:2023/2022

بسم الله الرحمن الرحيم

إهداء

أهدي هذا العمل إلى :

إلى الذي لن تكفيه حروف الدنيا لذكر فضله (أبي)، وإلى منبع الحب والحنان (أمي)

وإلى اللذان لن تغلا عنهما حبات عيني أخي وأختي (عزير، تسنيم)

وإلى كل الأصدقاء الذين قبلو بي انا بكل حالاتي وأحوالي دون تكليف التغيير والتصنع

وإلى الذين لولاهم لما نلت شرف الوصول إلى هنا إلى كل أساتذة الطور التربوي من الإبتدائي للمتوسطة للثانوية واساذة التعليم العالي كل بسمه كل بمقاتمه

وإلى كل كريم مر بحياتنا وعلمنا حرفا فيما يرضي الله

الشكر والتقدير

الحمد لله الذي بنعمه وعظمته تتم الصالحات، والصلاة والسلام على الحبيب المصطفى خاتم الأنبياء والمرسلين، أما بعد:

نحمد الله الذي وفقنا لتثمين هذه الخطوة في مسيرتنا الدراسية بمذكرتنا هذه.

نود أن نعبر عن خالص الشكر والامتنان لجميع الأشخاص الذين ساعدونا ودعمونا في إتمام هذا البحث، سواء كانوا قريبين أو بعيدين. نود أن نشكر بشكل خاص الأستاذة المشرفة **بوترعة سهيلة** على توجيهاتها القيمة ونصائحها والمعلومات التي قدمتها لنا، والتي كانت ذات مساعدة كبيرة في إتمام هذا البحث. نود أيضًا أن نشكرها على حسن معاملتها لنا وقبولها أن تكون مشرفة على هذه الرسالة.

كما نود أن نعبر عن خالص التقدير لجميع أعضاء لجنة المناقشة الأفاضل الذين أكرمونا بمعرفتهم وتقييمهم لجهودنا في هذا العمل. نود أيضًا أن نشكر كل الأشخاص الذين قدموا لنا الدعم المادي والمعنوي، سواء كانوا قريبين أو بعيدين، حتى لو كانت مساهمتهم بكلمة طيبة، فقد كانت لها دور كبير في إنجاز هذا العمل.

قائمة المختصرات

ق.إ.ج = قانون الإجراءات الجزائية

ق.إ.ج.ف = قانون الإجراءات الجزائية الفرنسي

ق.ع = قانون العقوبات

ج. ر. ج = الجريدة الرسمية الجزائرية

مقدمة

في ضوء الأوضاع العالمية الراهنة، يشهد العالم تحولًا جذريًا في قطاع المعلومات والاتصالات، مما أدى إلى تحقيق تغيرات عميقة في مجالات متعددة. ومن بين هذه المجالات التي تأثرت بشكل كبير، نجد التجارة والمعاملات التجارية. ظهرت التجارة الإلكترونية كبديل حديث للتجارة التقليدية، حيث عرفت المادة 06 من القانون 18-05 المتعلق بالتجارة الالكترونية المستهلك الالكتروني بأنه: كل شخص طبيعي أو معنوي يقتني بعوض أو بصفة مجانية سلعة أو خدمة عن طريق الاتصالات الالكترونية من المورد الالكتروني بغرض الاستخدام النهائي"[1]، كما عرفه بعض الفقهاء الفرنسيين بأنه: " الشخص الطبيعي أو الاعتباري الذي يحصل أو يستعمل المال أو الخدمة لغرض غير المزود [2]، وأصبحت تعتبر واحدة من أهم أشكال المعاملات الاقتصادية التي تتم عبر الإنترنت في هذا العصر، الذي شهد اندماجًا يكاد يلغي الحدود الجغرافية والمسافات بين الدول والشعوب.

رغم أن بعض المستهلكين يعبرون عن رفضهم للتعامل بواسطة التكنولوجيا الحديثة بسبب مخاوفهم من التعرض للغش أو الاحتيال، إلا أن حجم التجارة الإلكترونية بين الشركات لم يعد يمكن إيقافه، خاصة فيما يتعلق بالأنشطة التجارية والحكومية. وبالتالي، يصبح المستهلكون في هذه القطاعات هم الأكثر تعرضًا لأشكال الغش التجاري المعتادة، بالإضافة إلى ظهور أشكال جديدة من الغش التجاري الإلكتروني.

ردًا على التحديات المترتبة على المعاملات الإلكترونية، سارعت العديد من الدول إلى إصدار قوانين مخصصة لتنظيم هذا النوع من العمليات. تهدف هذه التشريعات إلى الاستفادة من فوائد المعاملات الإلكترونية، مثل السرعة والكفاءة وتقليل التكاليف، في حين تسعى في الوقت نفسه لحماية المستهلكين من المخاطر المحتملة.

---

[1] قانون رقم 18-05 مؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يتعلق بالتجارة الالكترونية، ج.ر. عدد 28 صادر في 30 شعبان عام ه1439 الموافق 16 مايو 2018.

[2] JEAN Clais, AULONY Frank steinmetz, droit de la consommation, 5eme ed, DOLLAZ p07 ,Montpellier, France, 2003

تشتمل أهداف هذه القوانين على تعزيز الثقة في المعاملات الإلكترونية، وتوفير بيئة آمنة للتجارة الإلكترونية، وتعزيز حقوق وحماية المستهلكين. تُنظَّم من خلالها جوانب مثل التعاقد الإلكتروني، والمسؤولية الجنائية، وحماية البيانات الشخصية والخصوصية، وتوفير آليات للتحكيم وتسوية المنازعات في البيئة الإلكترونية..

فتحت شبكة الإنترنت آفاقًا واسعة وحرة للممارسات الاستهلاكية الجديدة وتوقيع العقود بين الأفراد دون قيود. ومع ذلك، تظهر بعض المشكلات المعاصرة التي تواجه المستهلكين اليوم في سياق المعاملات الإلكترونية والعقود الإلكترونية. يعتبر المستهلك كطرف ضعيف في هذه العلاقة التعاقدية، وبالتالي يتعرض لسلوكيات غير نزيهة من قِبَل التجار، الذين يسعون إلى الغش والتلاعب بالمستهلك.

تسبب عدم التوازن في القوة بين التجار والمستهلكين في وجود تحديات ومشكلات مثل عدم الوضوح في العروض التجارية، وتضليل المعلومات، وتجاوز الشروط والأحكام المعقدة والغامضة، وسوء الخدمة أو التسليم غير الملائم للمنتجات المطلوبة. تلك السلوكيات غير النزيهة تؤثر سلبًا على المستهلكين وتتسبب في فقدان الثقة في التجارة الإلكترونية.

ومن أجل مواجهة تلك التحديات، نريد التطرق لقضية الحماية الجنائية للمستهلك الالكتروني تعمل الحكومات والمنظمات الدولية على وضع قوانين ولوائح لحماية حقوق المستهلكين في المعاملات الإلكترونية وضمان نزاهة العقود الإلكترونية. تشمل تلك الإجراءات تنظيم المعلومات والإعلانات، وضمان وضوح الشروط والأحكام، وإعطاء حقوق الاسترداد والتعويض عند الحاجة. يهدف ذلك إلى تعزيز الثقة في التجارة الإلكترونية وتحقيق تجارة إلكترونية عادلة وموثوقة للمستهلكين.

تواجه المستهلكون في المجالات الإلكترونية تحديات ومخاطر متعددة. يعتبر استهداف الشبكات الإلكترونية وسرقة المعلومات من أبرز هذه التحديات. يتمثل الهدف الرئيسي للمهاجمين في الحصول على معلومات شخصية للاستفادة منها بطرق غير قانونية، مثل سرقة بيانات البطاقات الائتمانية أو الهوية الشخصية. قد يؤدي ذلك إلى تعرض المستهلك للضرر المالي والاستغلال الاحتيالي.

بالإضافة إلى ذلك، تلعب الدعاية والإعلان دورًا هامًا في تعزيز وعي المستهلك وتثقيفه حول أساليب التعاقد الآمنة. يجب أن تعمل الشركات على توفير معلومات شافية وشفافة حول سياساتها الأمنية وخدماتها الإلكترونية، وتوضيح المخاطر المحتملة والتدابير التي تتخذها لحماية المستهلكين.

لذلك، ينبغي وضع قوانين تجرم السلوكيات التي تؤثر سلبًا في مصلحة المستهلك في نظام التجارة الإلكترونية. يتعين أن تكون هذه النصوص القانونية فعّالة في مكافحة الأعمال غير القانونية التي تضر بالمستهلك وتنتهك قوانين العقوبات. بالإضافة إلى ذلك، ينبغي وضع آليات لمراقبة الأنشطة التجارية وتطبيق العقوبات على المخالفين، وذلك لضمان تحقيق الحماية الجنائية للمستهلك في المعاملات الإلكترونية.

حيث تكمن أهمية هذا الموضوع في دور المستهلك كطرف ضعيف في العلاقة الاستهلاكية والتحديات الكبيرة التي يواجهها، وذلك بسبب عقود التجارة الإلكترونية التي يتعاقد عليها والتي تكون في الغالب خارج نطاق سيطرة الدولة. هذا الوضع يجعل المستهلك عُرضة للمخاطر المتعلقة بالتجارة الإلكترونية. بالإضافة إلى ذلك، فإن المستهلك غالبًا يفتقر إلى الخبرة والمعرفة الكافية في عقود التجارة الإلكترونية، ويكون قوته التفاوضية أقل في المعاملات الاقتصادية.

لعل من الأسباب التي دفعت بي لدراسة الموضوع الرغبة الذاتية في دراسة هذا الموضوع من خلال بيان أساليب مكافحة جريمة جرائم التجارة الالكترونية الماسة بالمستهلك الالكتروني من خلال التطرق الى سياسة المشرع الجزائري في التصدي لهذه الجريمة المستجدة . الاهتمام الشخصي بمجال التجارة الالكترونية. تفشي ظاهرة وقوع الكثير من المستهلكين في شباك هذه الجرائم و تأثيراتها السلبية على المجتمع . قلة الدراسات العربية التي تناولت موضوع هذا البحث.الآثار السلبية التي تخلفها الجرائم التي ترتكب ضد المستهلك الإلكتروني في عقود التجارة الإلكترونية، محاولة البحث عن الحماية الجنائية التي

يوفرها التشريع الجزائري في عقود التجارة الإلكترونية للمستهلك و مدى كفايتها للحد من الجرائم التي يقع ضحيتها

إن هذا البحث يهدف إلى تسليط الضوء على حماية المستهلك في مجال عقود التجارة الإلكترونية من الناحية الجنائية. يتم ذلك من خلال دراسة مختلف أنواع الجرائم التي يمكن ارتكابها ضد المستهلك، وتحليل الحماية الجنائية المتاحة للمستهلك في قوانين التشريع الجزائري. كما يهدف البحث إلى تحديد النواقص الموجودة في هذه الحماية وإشارتها للمشرع لتجنبها في المستقبل.

لذا نطرح الإشكالية التالية: **كيف جسد المشرع الجزائري الحماية الجنائية للمستهلك الالكتروني؟**.بمعنى البحث في الآليات القانونية الموضوعية والإجرائية تكريسا وحماية للمستهلك الإلكتروني، ومساس مواطن القوة والضعف فيها

للإجابة عن الإشكالية إتبعنا المنهج الإستدلالي بالتحليل والتأصيل القانوني في ، وذلك من خلال تحليل النصوص القانونية. بالإضافة إلى ذلك، تم استخدام المنهج الوصفي لشرح وتوضيح المفاهيم المتعلقة بالموضوع المطروح في الحديث. مما يساهم في توضيحها وفهمها بشكل أفضل.

وعليه قسمنا هذه الدراسة إلى فصلين رئيسيين. في **الفصل الأول**، تم التركيز على حماية المستهلك الإلكتروني بشكل عام، واشتمل على مبحثين رئيسيين. في المبحث الأول، تم التركيز على حماية المستهلك الإلكتروني من الجرائم الإلكترونية، حيث تمت مناقشة التحديات والمخاطر التي يتعرض لها المستهلك في البيئة الإلكترونية، وتم استعراض الإجراءات والسياسات التي يمكن اتخاذها للحد من هذه الجرائم وحماية المستهلك. أما المبحث الثاني، فتم التركيز على حماية المستهلك الإلكتروني في إطار التعاقد الإلكتروني، حيث تمت مناقشة حقوق وواجبات المستهلك في التعاقد الإلكتروني، وكذلك التحديات والمشكلات التي قد يواجهها في هذا السياق، وتمت استعراض الآليات والتدابير المتاحة لحماية حقوق المستهلك في عمليات التعاقد الإلكتروني.

في **الفصل الثاني** تم التركيز على الحماية الإجرائية للمستهلك الإلكتروني، وتم تقسيمه إلى مبحثين رئيسيين. في المبحث الأول، تم التطرق إلى الإجراءات القضائية المتبعة في حماية المستهلك الإلكتروني. تمت مناقشة السبل التي يمكن أن يلتجأ إليها في حالة وقوع انتهاك لحقوقه، بما في ذلك رفع دعوى قضائية. كما تم استعراض الإجراءات القانونية والقضائية المتاحة للمستهلك للحصول على تعويضات. أما المبحث الثاني، فقد تم التركيز على إثبات. تمت مناقشة أساليب جمع الأدلة وتوثيقها لدعم في المحاكمات وإثبات التجاوزات أو الجرائم التي تعرض لها. كما تم استعراض القوانين والأنظمة المتعلقة بإثبات الجرائم الإلكترونية وكيفية تطبيقها على حماية المستهلك الإلكتروني.

في ختام هذه الدراسة، سنلقي الضوء على النقاط الرئيسية والأبعاد المهمة التي تمت مناقشتها، والتي يجب إيلاء اهتمام خاص لها. سنقوم بتلخيص أهم المحتويات التي تمت معالجتها، ونسلط الضوء على المواضيع والمفاهيم التي يتعين على القراء الانتباه إليها.

الفصل الأول

الحماية القانونية الموضوعية للمستهلك الالكتروني

الفصل الأول

الحماية القانونية الموضوعية للمستهلك الالكتروني

تم تحديد الحماية الجنائية الموضوعية للمستهلك الإلكتروني من خلال مجموعة من النصوص التي تم إضافتها إلى تعديل قانون العقوبات عام 2004، والتي تغطي الجرائم المعلوماتية التي تهدد التجارة الإلكترونية. ويتعين حماية النظم المعلوماتية التي تستخدم بيانات المستهلكين والتجار الإلكترونيين من الجرائم المعلوماتية، حيث يعد المستهلك الطرف الأضعف في هذه العلاقات التجارية. ولم يكن القانون الجنائي القديم كافيًا لحماية معاملات التجارة الإلكترونية ضد الجرائم المعلوماتية، ولذلك تم تعديله بشكل يغطي جميع أنواع الجرائم المعلوماتية. ومع ذلك، تظهر أزمة القانون الجنائي في مواجهة الواقع الرقمي، حيث تتعرض الدعاوى الجنائية لمشكلات متعددة وخاصة بسبب مبدأ شرعية الجرائم.

تتسبب التعاملات الإلكترونية في العديد من المشكلات القانونية، بما في ذلك جرائم الاعتداء على المستهلك الإلكتروني، والتي ستتم مناقشتها في المبحث الأول. كما يشكل الاعتداء على بيانات المستهلك الإلكتروني، مثل بطاقات الائتمان والتوقيع الإلكتروني، مشكلة أخرى، وسيتم مناقشتها في المبحث الثاني.

المبحث الأول

حماية المستهلك الإلكتروني من الجرائم الإلكترونية

لا يمكن تحقيق الحماية الجنائية للمستهلك الإلكتروني وتعاملاته التجارية إلا من خلال حماية المواقع والأنظمة المعلوماتية التي يعتمد عليها في تلك التعاملات. لذلك، قام المشرع الجزائري وغيره من التشريعات المقارنة بتجريم انتهاك حق الدخول إلى هذه المواقع أو البقاء فيها بواسطة الاحتيال أو بدون تصريح. إذ تعتبر هذه الجريمة الفنية الأساسية التي تشكل أول خطر في ارتكاب باقي الجرائم المعلوماتية ذات الغرض من انتهاك بيانات المستهلك ووسائل الدفع الإلكترونية أو التوقيع الإلكتروني.

بالتالي، يتعين على المستهلك الإلكتروني أن يعتمد على نظم وتقنيات آمنة لحماية تعاملاته ومعلوماته الشخصية، بالإضافة إلى توفر قوانين فعالة تعاقب من يرتكب الجرائم الإلكترونية التي تستهدف المستهلك الإلكتروني وحقوقه.

وقد تم إدخال قوانين وجرائم جديدة تتعلق بحماية المستهلك، وهذا ما سنتناوله في هذا المبحث. تم تقسيم المبحث إلى مطلبين، حيث تم تخصيص المطلب الأول لدراسة الجرائم المنصوص عليها في قانون العقوبات. أما المطلب الثاني، فسنركز فيه على الجرائم المنصوص عليها في التشريعات الخاصة.

المطلب الأول

الجرائم المنصوص عليها في قانون العقوبات

لا يمكن إنكار أهمية الحاسوب وأنه أصبح ضرورة لا غنى عنها في حياة الأفراد والمؤسسات العامة والخاصة على حد سواء. فقد ساهم الحاسوب بشكل كبير في تسهيل الأعمال الإدارية والخدمات المتنوعة. ومع ذلك، تسبب الحاسوب بشكل غير مباشر في فتح الباب أمام وجود سلوكيات جرمية متنوعة.

واستجاب المشرع الجزائري لهذا التحدي بوضع حماية جنائية للمستهلك الإلكتروني من خلال إضافة القسم السابع المكرر ضمن قانون العقوبات، والذي يتعامل مع انتهاك أنظمة معالجة البيانات وجريمة النصب على المستهلك الإلكتروني. وقد تم تحديد عقوبات صارمة لمثل هذه الجرائم.

وبهذا، يؤكد المشرع على أهمية حماية الأنظمة المعلوماتية ومعالجة البيانات من أجل حماية المستهلك الإلكتروني وحقوقه. يُعتبر هذا القسم السابع المكرر من قانون العقوبات آلية قانونية فعالة لمكافحة الجرائم الإلكترونية وتأمين الحماية الجنائية للمستهلك الإلكتروني في البيئة الرقمية.

وعموما فإن الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري تشمل جريمة الدخول عن طريق الغش إلى النظام الآلي (الفرع الأول)، وجريمة البقاء غير المصرح به في النظام المعلوماتي (الفرع الثاني) وأخيرا جريمة إتلاف نظام المعالجة الآلية للمعطيات (الفرع الثالث).

الفرع الأول: جريمة الدخول عن طريق الغش إلى النظام الآلي

تضمن قانون العقوبات الجزائري هذه الصورة من الجرائم حيث تنص المادة 394 مكرر « يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 100,000 دج

كل من يدخل عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات او يحاول ذلك[1]».

من المتفق عليه بشكل عام أن الجريمة تقوم على ركنين مادي ومعنوي ، ويعتبر الركن المادي واحدًا من المبادئ الأساسية في النظام القانوني الجنائي. ففي جميع الجرائم، يشترط وجود حدث أو واقعة مادية تسبب ضررًا ملموسًا أو تشكل خطرًا على المصالح المحمية قانونًا[2].

إضافةً إلى ذلك، لا يكفي لوقوع الجريمة وتحديد عقوبتها أن يتوفر فقط الركن المادي، بل يجب أيضًا أن يتحقق الركن المعنوي الذي يعكس النية الخاطئة التي يتم من خلالها تنفيذ الفعل. يستنتج منها الحالة النفسية للمجرم أثناء ارتكابه للجريمة[3].

وبالتالي، فإن تحقق الركن المعنوي في الجريمة يلقي الضوء على العزم السلبي الذي تتخذه الشخصية المذنبة أثناء ارتكابها للفعل. يساهم هذا الركن في تشخيص العمل الجرمي وتحديد المسؤولية الجنائية للفاعل، إذ يعكس حالته النفسية والنية السيئة التي تدفعه للقيام بالفعل المخالف للقانون.

بالرجوع إلى نص المادة 394 مكرر من قانون العقوبات الجزائري يتضح لنا أن جريمة الدخول إلى نظام المعالجة الآلية للمعطيات[4]، تقوم كسائر الجرائم الأخرى على ركتين الركن المادي والذي يشمل السلوك الإجرامي الذي يترتب عنه الدخول غير المشروع إلى النظام (أولا) والركن المعنوي المتمثل في القصد الجنائي (ثانيا)

---

[1] أمر رقم 66-156 مؤرخ في 8 جوان 1966 يتضمن قانون العقوبات ج.ر عدد ،49، صادر في 11 جوان 1966، معدل و متمم.

[2] أحسن بوصقيعة ، الوجيز في القانون الجنائي العام الديوان الوطني للأشغال التربوية ، الجزائر 2002، ص 47

[3] محمد حماد مرهج الهيتي ، جرائم الحاسوب، دار المناهج للنشر و التوزيع ، عمان 2006، ص 182

[4] راجع المادة 394 مكرر، قانون العقوبات، مرجع سابق

أولا: الركن المادي جريمة الدخول عن طريق الغش إلى النظام الآلي

يتكون الركن المادي في هذه الجريمة من نشاط إجرامي يتمثل في القيام بفعل الدخول، ويمكن للسلوك الإجرامي أن يكون إيجابيًا أو سلبيًا. يتطلب هذا النشاط إجراءً إيجابيًا من الفاعل، ولا يمكن تنفيذ الجريمة بشكل سلبي. يجدر بالذكر أن هذا النوع من الجرائم لا يندرج تحت تصنيف الجرائم ذات الصفة المميزة مثل الرشوة أو الاختلاس أو الاحتيال. يمكن أن يرتكب أي شخص، بغض النظر عن صفته أو مهنته، هذه الجرائم سواء كان يفهم طريقة عمل النظام أو لا، وسواء كان يستفيد من الدخول أو لا[1]. يجب أيضًا الإشارة إلى أن مصطلح "فعل الدخول" يشمل جميع الأعمال التي تسمح بالوصول إلى النظام المعلوماتي أو التحكم في البيانات والمعلومات المتواجدة فيه[2]. بالإضافة إلى ذلك، فإن فعل الدخول إلى النظام المعلوماتي بحد ذاته لا يعد سلوكًا غير قانوني، ولكن يصبح غير قانوني عندما يتم القيام به بدون سبب مشروع

ثانيا: الركن المعنوي جريمة الدخول عن طريق الغش إلى النظام الآلي

في التشريع الجزائري، يتطلب ارتكاب جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للبيانات عن طريق الغش توفر ركن القصد الجنائي[3].

يعد الدخول إلى نظام المعالجة الآلية جريمة عمدية في القانون الجزائري، حيث يشكل الركن المعنوي جزءًا أساسيًا من القصد الجنائي، والذي يتكون من العلم والإرادة[4].

وفقًا لذلك، إذا توفر القصد الجنائي بوجود عنصري العلم والإرادة، فإنه لا يتأثر بالباعث الذي يحفز الشخص على الدخول أو البقاء في النظام. بمعنى آخر، حتى لو كان الباعث

---

[1] قورة نائلة جرائم الحاسب الاقتصادية ، دار النهضة العربية القاهرة 2004 , ص 343

[2] محمد حماد مرهج الهيتي ، المرجع السابق ، 183

[3] - كوثر فرام ، المرجع السابق، ص 73

[4] قارة أمال الجريمة المعلوماتية ، رسالة ماجستير ، كلية الحقوق بن عكنون ، الجزائر 2002 ص 60

هو الفضول أو إثبات القدرة على المهارة أو الانتصار على النظام[1]، فإن القصد الجنائي مازال قائمًا ويحتفظ بصحته.

عند الرجوع إلى المادة 394 المكررة من قانون العقوبات الجزائري، يُلاحظ أن القصد الجنائي وحده غير كافٍ، وإنما يجب أيضًا توافر قصد جنائي خاص وهو الغش. وبناءً على ذلك، يُعتبر الدخول غير المشروع إلى النظام الآلي جريمة.[2]

الفرع الثاني : جريمة البقاء غير المصرح به في النظام المعلوماتي

تناول المشرع الجزائري هذه الصورة من الجرائم كذلك في المادة 394 مكرر من قانون العقوبات والتي تنص .. أو يبقى عن طريق العش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات ...[3]

بناءً على هذا النص، يمكن تعريف الاحتيال الالكتروني في نظام المعلوماتية على أنه: أي تواجد غير عادي مثل الدخول والوصول إلى النظام المعلوماتي عبر الشبكة، والاطلاع على المعطيات المخزنة فيه، والقيام بأي تصرف غير مسموح به، والذي يشكل بقاءً احتياليًا[4]. يشير هذا البقاء إلى التواجد داخل نظام معالجة البيانات ضد إرادة صاحب الحق في السيطرة على هذا النظام[5]. يجب أن نلاحظ أن البقاء المعاقب عليه داخل النظام المعلوماتي يمكن أن يتحقق بشكل مستقل عن الدخول إلى النظام، أو يمكن أن يتواجد البقاء ويتم معاقبته بشكل مستقل عندما يكون الدخول إلى النظام مصرحًا به. يمكن أن يكون مثالًا على ذلك الدخول إلى النظام عن طريق الخطأ. او الصدفة، فيتوجب عليه قطع الاتصال والانسحاب على الفور. وإذا استمر في البقاء داخل النظام بعد انقضاء المدة المحددة له،

---

[1] محمد حماد مرهج الهيني . المرجع السابق ص 187 .

[2] راجع المادة 394 مكرر، قانون العقوبات، مرجع سابق

[3] راجع المادة 394 مكرر، قانون العقوبات، مرجع سابق

[4] عبد الفتاح حجازي. الدليل الجنائي والتزوير في جرائم الكمبيوتر و الإنترنت ، دار الكتب القانونية القاهرة ، 2002، ص 235

[5] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1999،ص601

فيتعرض لعقوبة جريمة الاستمرار في البقاء داخل النظام.[1] في حالة دخول الشخص إلى النظام ضد إرادة صاحب السيطرة عليه، وبقاءه داخل النظام بعد ذلك، يُعتبر في هذه الحالة أنه قد ارتكب جريمة الاقتحام غير المصرح به والاستمرار غير المشروع داخل النظام.[2]

وعلاوة على ذلك فأنه يتبين من النص السالف الذكر أن المشرع يفرض التزاما على من يتحقق الإتصال عنده يتمثل في عدم البقاء داخل النظام الذي حصل به الإتصال.

أولا: الركن المادي جريمة البقاء غير المصرح به في النظام المعلوماتي

يتحقق الركن المادي لجريمة الإبقاء على الاتصال غير المشروع مع النظام الآلي عندما يجد الفرد نفسه بطريقة غير مقصودة داخل النظام، وعلى الرغم من ذلك يقرر البقاء داخل النظام وعدم قطع الاتصال به[3].

ببساطة، جريمة البقاء غير المشروع في النظام الآلي تحدث عندما يستمر الفاعل في استخدام النظام لفترة زمنية محددة. يتم قياس غير المشروعية بناءً على المدة التي يستخدمها الشخص الذي ارتكب الجريمة في النظام، وبالتالي تكتمل هذه الجريمة عند استمراره في استخدام النظام لفترة زمنية. يتناقض ذلك مع جريمة الدخول غير المشروع حيث لا يتعلق الأمر بالبقاء في النظام، بل يتعلق بالدخول غير المشروع إليه[4].

ثانيا: الركن المعنوي جريمة البقاء غير المصرح به في النظام المعلوماتي

تعد جريمة البقاء غير المشروع داخل النظام من الجرائم العمدية التي تتطلب وجود القصد الجنائي العام، والذي يتضمن عنصري العلم والإرادة. يجب على الجاني أن يكون على علم بأنه يتجول داخل نظام معلوماتي بطريقة غير مشروعة، وفي الوقت نفسه يجب أن تكون إرادته موجهة نحو البقاء في النظام وعدم قطع الاتصال به

---

[1] نفس المرجع ص 602.

[2] محمد حماد مرهج الهيتي، المرجع السابق،ص 190.

[3] دردور نسيم . المرجع السابق ، ص 34

[4] نهلا عبد القادر المومني، المرجع السابق ، ص 162 .

ثالثا: العقوبة المقررة جريمة البقاء غير المصرح به في النظام المعلوماتي

جريمة البقاء في النظام الآلي لمعالجة المعطيات تعتبر جريمة شكلية، حيث لا يتطلب القانون نتيجة معينة لتحقيقها. إنها جريمة مستمرة تتطلب تدخلا مستمرًا من الفاعل. وبالنظر إلى المادة 394 مكرر الفقرة الثانية في قانون العقوبات الجزائري، يلاحظ أن المشرع الجزائري قد مشدد في العقوبة المفروضة على جريمتي الدخول والبقاء في النظام المعلوماتي، خاصة إذا تسببت في حذف أو تغيير المعطيات الموجودة في النظام، حيث يتم ضمان مضاعفة العقوبة. كما يشدد العقوبة أيضًا في حالة تعرض نظام النظام للتخريب. وبالإضافة إلى ذلك، يتم مضاعفة العقوبة إذا كانت الجريمة تستهدف الدفاع الوطني أو البيئة أو المؤسسات التي تخضع للقانون العام، وفقًا للمادة 394 مكرر 3 من قانون العقوبات الجزائري.[1]

الفرع الثالث: جريمة إتلاف نظام المعالجة الآلية

عالج المشرع الجزائري هذا النمط من الجرائم من خلال نص المادة 394 مكرر من قانون العقوبات والتي تنص على أنه : يعاقب بالحبس من سنة (6) أشير إلى ثلاث (3) سنوات وبغرامة مالية من 5000.00 دج إلى 20,000,00 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق العش المعطيات التي ينضمتها .. من خلال هذا النص ومن أجل معالجة عناصر هذه الجريمة يتوجب تحديد معنى الإتلاف الفرع الأول) ثم الوسائل التي يتحقق بها الإتلاف (الفرع الثاني)

الأول: مدلول الإتلاف

مدلول الإتلاف هو جعل الشيء غير صالح للاستعمال أو تعطيله جزئيًا أو كليًا، مما يؤدي إلى تقليل قيمته الاقتصادية والتأثير على مالكه. يمكن تجريم الإتلاف بسبب الفقدان المالي الذي يسببه أو الاستفادة المالية المتوقعة. فيما يخص تدمير نظم المعلومات والبرامج في الحواسيب، يشير إلى تدمير تعليمات البرامج والبيانات المخزنة بهدف إعاقة وتعطيل

[1] راجع المادة 394 مكرر قانون العقوبات، مرجع سابق

النظام، ولا يهدف عادةً للحصول على فائدة مالية شخصية. يمكن أن يشمل مفهوم الإتلاف تأثيرات أخرى تتجاوز تدمير نظم المعلومات، ويعتمد ذلك على الجوانب المنطقية والأخلاقية للأنظمة والكائنات المعنية. على سبيل المثال، يمكن أن يشمل الإتلاف فقدان الفائدة المادية أو المعنوية لجهاز الحاسوب نفسه، الذي يحمل قيمة اقتصادية عالية..[1]

ومن الجدير بالذكر أنه على الرغم من الاستخدام المتعلق بتدمير نظم المعلومات في الحواسيب كمثال، إلا أنه يمكن تطبيق مفهوم الإتلاف بطرق أخرى غير تلك التي يذكرها القانون الجزائري في قانون العقوبات.[2] يُقصد هنا أن المدلول العام للإتلاف يمكن أن يتضمن تأثيرات أخرى تتجاوز ما ذكره المشرع الجزائري، وذلك يعتمد على الجانب المنطقي والأخلاقي للأنظمة والكائنات المعنية. على سبيل المثال، يمكن أن يُعرَف الإتلاف في سياق آخر على أنه خسارة لفائدة مادية أو معنوية لجهاز الحاسوب نفسه، والذي أصبح يحمل قيمة اقتصادية عالية[3].

الثاني: اركان جريمة إتلاف نظام المعالجة الآلية

تعد هذه الجريمة من بين الجرائم التي تتطلب تنفيذ سلسلة من الأفعال التي تمثل الركن المادي للجريمة، بالإضافة إلى إرادة المرتكب لارتكاب الجريمة وتمثيل الركن المعنوي لها.

1: الركن المادي جريمة إتلاف نظام المعالجة الآلية

يتكون الركن المادي لجريمة الإتلاف العمدي للمعطيات من ثلاثة عناصر أساسية التي تمثل الأفعال التي يقوم بها المرتكب. وهذه العناصر هي:

أ. **إدخال معطيات غير موجودة في النظام:** يعني ذلك إضافة معلومات جديدة إلى البيانات التي كانت موجودة بالفعل. يتم تغيير المعطيات والمعلومات الموجودة في النظام المعلوماتي، ويمكن أن يؤدي هذا إلى تغيير النظام بشكل كامل. يمكن للشخص المعني بالإتلاف أن

---

[1] محمد أمين الشوابكة ، الجريمة المعلوماتية ، دار الثقافة للنشر و التوزيع ، عمان ،2004 ص216.

[2] محمد حماد مرهج الهيتي . المرجع السابق، ص 198 .

[3] محمد احمد عبابنة المرجع السابق . ص 100

يدخل معطيات أو معلومات زائفة تمكنه من الوصول إلى بيانات شخصية، وعادة ما تكون متعلقة بالمعلومات المالية للأفراد، بهدف تحقيق مكاسب مالية لنفسه.[1]

ب. **محو أو إلغاء المعلومات:** يعني ذلك إزالة أو حذف المعلومات الموجودة داخل النظام بشكل كلي أو جزئي. من الأمثلة الواقعية على هذا الفعل، قام أحد الموظفين في شركة سمسرة وتأمين الحياة في فورت ورث في تكساس في عام 1985، بعد فصله من العمل، بتسلل إلى النظام المعلوماتي للشركة بهدف الانتقام. تمكن من محو أكثر من 168 ألف سجل للشركة عن طريق زرع فيروس معلوماتي. وقد حُكم عليه بالمراقبة لمدة سبع سنوات ودفع تعويض قدره 11,800 دولار[2].

ج. **تعديل المعلومات:** يعني ذلك تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى. هذه العملية لا تتطلب تغييرًا في المعلومات الفعلية أو استبدالها بمعلومات جديدة. يتحقق الجانب المادي لهذه الجريمة من خلال إجراء تعديل داخلي. من الأمثلة الواقعية على هذا النوع من الإتلاف، قام صبي ألماني يبلغ من العمر 16 سنة بزرع فيروس معلوماتي في شبكة معلومات المستخدمين لنظام فيديو ونص، وكانت مهمته جمع البيانات الشخصية، بالإضافة إلى تلاعب هذا الفيروس في تلك البيانات من خلال تعديلها وتغييرها وحذفها وتغيير مفاتيح الوصول إليها[3].

2: الركن المعنوي جريمة إتلاف نظام المعالجة الآلية

يتميز الإتلاف العمدي للمعطيات عن جرائم الدخول أو البقاء في أنه يعكس إرادة الجاني في إلحاق الضرر بالآخرين. يتم تطبيق قواعد العمد الجنائي حيث يكون الجاني يقصد ويعلم بصلاحية نشاطه وأنه سيؤدي إلى النتيجة المحظورة قانونًا. بالتالي، يتم إتلاف أو تعديل المعطيات بصورة عمدية.[4]

---

[1] بوخلفة حدة، مرجع سابق، ص149.

[2] بوخلفة حدة، مرجع سابق، ص149.

[3] رامي حليم، مرجع سابق، ص351.352

[4] طباش عز الدين مرجع سابق، ص261

قواعد العمد في القصد الجنائي تعني أن الشخص يكون قد اتخذ القرار المتعمد بالقيام بالإتلاف العمدي للمعطيات، وأنه يكون على علم تام بصحة وصلاحية النشاط الذي يمارسه والتأثيرات السلبية التي ستحدث نتيجة لذلك. بالتالي، يكون للشخص المسؤولية القانونية عن جريمته وتعرضه للعقوبة بناءً على هذا العمد والعلم المتعمد بالأضرار التي ستنجم عن أفعاله.

ثالثا: العقوبة المقررة لجريمة الإتلاف العمدي للمعطيات

تخضع لتنظيم قوانين الدول المختلفة. وعلى سبيل المثال، في النظام الجزائري، يتم تحديد عقوبة قابلة للتطبيق لهذه الجريمة. فباستقراء النصوص المتعلقة بالجرائم المتعلقة بالأنظمة المعلوماتية في القانون الجزائري، نجد أن الشرع قد وضع عقوبة تتمثل في الحبس لمدة تتراوح بين ستة أشهر وثلاث سنوات، بالإضافة إلى فرض غرامة مالية تتراوح بين 500.000 دينار جزائري و2.000.000 دينار جزائري.[1]

إن هذه العقوبة السجنية تهدف إلى تأديب وردع الجناة، وتعكس جدية الجريمة وتأثيرها السلبي على المجتمع والأفراد. فالحكم بالحبس يشير إلى أن الشخص المدان سيفقد حريته لفترة محددة، مما يعاقبه ويحظر عليه ممارسة حقوقه الشخصية بينما يقضي فترة العقوبة في السجن.

بالإضافة إلى العقوبة السجنية، يتم فرض غرامة مالية على الجاني. تكون قيمة هذه الغرامة بين 500.000 دج و2.000.000 دج، وتعتبر هذه الغرامة مصدرًا للتعويض عن الأضرار التي لحقت بالضحايا أو المنظومة المعلوماتية المتضررة. إن فرض الغرامة المالية يعزز الجانب الرادع ويعمل على تحقيق التعويض المادي للخسائر الناجمة عن الجريمة. تهدف هذه العقوبات المقررة لجريمة الإتلاف العمدي للمعطيات إلى حماية البيانات والنظم المعلوماتية وتعزيز الأمن الرقمي[2]

[1] أنظر المادة 394 مكرر 1 من الأمر رقم 66-156 المتضمن قانون العقوبات، مرجع سابق

[2] أنظر المادة 394 مكرر 1 من الأمر رقم 66-156 المتضمن قانون العقوبات، مرجع سابق.

الفرع الرابع: جريمة النصب

تُعَدّ جريمة النصب واحدة من أكثر الجرائم انتشاراً وإلحاقاً بالأذى بالمستهلكين في مجال التجارة الإلكترونية. ويعود ذلك إلى تعامل المتعاملين عن بُعد عبر وسائل الاتصال الإلكترونية، والتي تخضع للقواعد العامة. وتُحدّد المادة 372 (قانون العقوبات) ركنها المادي لتحديد أشكال هذه الجريمة.

أولا: تعريف جريمة النصب

جريمة النصب تشمل استيلاء شخص عمدًا على ملكية أو ممتلكات آخر عن طريق الاحتيال والخداع، وتكون شائعة وخطيرة عبر الحواسيب والإنترنت. الهدف من النصب هو الحصول على فوائد مالية غير قانونية على حساب الضحية. يشمل النصب استيلاء الجاني على كل ممتلكات الضحية، سواء كانت نقودًا، أصولًا ثابتة، معلومات سرية، أو حقوق ملكية فكرية، بهدف تحقيق مكاسب غير مشروعة.[1]

جريمة النصب عبر الحواسيب والإنترنت يتطلب مهارات تقنية واستغلال ضعف الحماية الأمنية وعدم الوعي التقني للضحايا. يستخدم الجاني وسائل احتيالية جديدة ومتطورة لتنفيذ جريمته. من المهم توعية الأفراد والمؤسسات بأنواع الاحتيال الإلكتروني وتعزيز وعيهم التقني لحماية أنفسهم من هذه الجريمة الخطيرة[2]

ثانيا: أركان جريمة النصب

جريمة النصب تحتاج إلى تجسيد مادي وأن تتخذ شكلًا محددًا، ويُعرف هذا الجانب المادي باسم "الركن المادي" للجريمة. يمثل الركن المادي الجانب الظاهري والخارجي لنشاط الجاني، وهو العنصر الذي يجعله قابلاً للمساءلة والمحاسبة. ومع ذلك، فإن الركن المادي وحده غير كافٍ، بل يجب أن يكون الجاني قد انتهج النية وبمعرفة كاملة لارتكاب الجريمة.[3]

---

[1] مطر عصام عبد الفتاح، التجارة الالكترونية العربية والاجنبية،دار الجامعة الجديدة،مصر،2015،ص320.

[2] مطر عصام عبد الفتاح، التجارة الالكترونية العربية والاجنبية،دار الجامعة الجديدة،مصر،2015،ص320.

[3] بوسقيعة احسن، الوجيز في القانون الجزائي العام ، الطبعة 14، دار هومة،الجزائر، 2014،ص63.

1 الركن المادي لجريمة النصب:

تتكون جريمة النصب من مجموعة عناصر تشكل أساسها، وتتضمن هذه العناصر:

أ- استعمال وسائل احتيالية

جريمة النصب تشتمل على استخدام وسائل احتيالية التي تهدف إلى إيقاع الضحية في الخطأ[1]. وقد حدد القانون بعض هذه الوسائل، وتشمل استخدام أسماء وهمية أو صفات كاذبة، واستخدام سلطة وهمية، والاعتماد على مبالغ مالية وهمية، وإيهام الضحية بالفوز بجوائز أو مكاسب غير حقيقية، أو خلق توقعات بوقوع حوادث أو أحداث وهمية، أو إثارة خوف الضحية من وقوع مشكلة معينة.[2]

ب- لاتسليم القيم

توجد شروط محددة يجب توافرها لاعتبار فعل الاستعمال الكاذب لأسماء أو صفات أو الوسائل الاحتيالية الأخرى في إطار المادة 372 من قانون العقوبات جريمة النصب. يجب أن يتحصل الفاعل جراء استخدام هذه الوسائل على قيم أو أموال غرير شرعية إضرارا بالغير.[3]

بمعنى آخر، لا يكفي أن يستخدم الفاعل أسماء أو صفات كاذبة أو وسائل احتيالية أخرى فحسب، بل يجب أن يكون الهدف النهائي من هذا الاستخدام هو تحقيق تحصيل قيم أو أموال غير شرعية وتسلمها. ويجب أن يكون هناك أضرار كبيرة للطرف الآخر نتيجة لهذا التحصيل غير الشرعي. بالتالي، إذا تم استخدام أسماء أو صفات كاذبة أو وسائل احتيالية أخرى دون أن يكون الهدف النهائي من ذلك هو تسلم قيم أو أموال غرير شرعية، فإن هذا الفعل لا يعتبر نصبًا بموجب القانون.[4]

---

[1] لحسين بن شيخ، مذكرات في القانون الجزائي الخاص، الطبعة 5، دار هومة ، الجزائر، 2006، ص 189.

[2] لحسين بن شيخ،مرجع سابق ، ص 189.

[3] المرجع نفسه،ص198.

[4] أنظر المادة 372 مكرر 1 من الأمر رقم 66-156 المتضمن قانون العقوبات، مرجع سابق.

ت - سلب كل ثروة الغير أو البعض منها أو الشروع في ذلك

بالإضافة إلى التأكد من توافر العناصر المذكورة سابقاً، ينبغي أن يتم استيلاء على ثروة الآخرين بشكل جزئي أو كلي، أو القيام بمحاولة لذلك، أي يجب تسبب أضرار للشخص المتضرر.[1]

يمكن أن تشمل جريمة النصب على المستهلك الإلكتروني عدة أشكال، ومن بينها:

. عدم تسليم السلعة المطلوبة عبر الإنترنت رغم أن المستهلك قد أنفق مبلغًا ماليًا لشرائها.

. استخدام موقع مشابه لأحد المواقع التجارية الشهيرة وتقليد اسمها، بهدف خداع المستهلك الإلكتروني والاحتيال عليه.

. الترويج لسلع مقلدة ومشابهة للمنتجات العالمية المعروفة التي تتمتع بجودة عالية، بهدف تضليل المستهلك.

. الإعلان عن سلع وخدمات غير معروفة باستخدام إعلانات زائفة، وذلك بهدف الاحتيال والتلاعب بالمستهلك ليتعاقد دون معرفة حقيقة الأمر والتحقق منه.[2]

2 الركن المعنوي جريمة النصب

يعتبر الاحتيال جريمة عمدية تتطلب وجود نية جنائية عامة ونية خاصة. يتمثل القصد الجنائي العام في معرفة المتهم بأن الأفعال التي يقوم بها، والتي تشمل أساليب الاحتيال، تهدف إلى خداع المستهلكين وإقناعهم بالتسليم. يعاقب القانون على هذه الأفعال. أما القصد الخاص فيتمثل في نية المتهم للاستيلاء على أموال المستهلكين.[3]

---

[1] العايب سامية، عرابة منال، الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني، مجلة هيرودوت للعلوم الانسانية والاجتماعية. العدد 5، كلية الحقوق والعلوم السياسية،جامعة 8 ماي 1945،الجزائر، 2021،

[2] بلارو كمال، ص80

[3] خلوي عنان نصيرة،الحماية القانونية للمستهلك عبر الانترنات، رسالة ماجستير، جامعة مولوج معمري، تيزي وزو، 2013 ص148

ثالثا: العقوبة المقررة لجريمة النصب

يعاقب مرتكب الجريمة بالحبس من سنة على الاقل إلى 5سنوات على الأكثر وغرامة مالية من 5.000 دج إلى 20.000 دج (المادة 372 من قانون العقوبات)[1]. قد يتم تشديد العقوبة إذا قام الفاعل بتوجيه النصب للجمهور عبر إصدار أسهم أو سندات أو أذونات أو حصص أو أي أوراق مالية للشركات أو المشروعات التجارية أو الصناعية، وفي هذه الحالة قد يصل حكم الحبس إلى 10 سنوات والغرامة إلى 200.000 دج.[2] بالإضافة إلى العقوبات الرئيسية، يمكن فرض عقوبات تكميلية تتمثل في حرمان المدان من بعض الحقوق المذكورة في المادة 14، وقد يتم منعه أيضًا من الإقامة لمدة تتراوح بين سنة وخمس سنوات[3]

المطلب الثاني

الجرائم المنصوص عليها في قوانين خاصة

تواجه المستهلك الإلكتروني تهديدات جرائم الكترونية المتنوعة، مثل الاحتيال والغش والتلاعب. وبناءً على ذلك، وضعت المشرع الجزائري قوانين خاصة لحماية المستهلك في مثل هذه الحالات. يشمل ذلك قانون رقم 09-03 الذي يركز على حماية المستهلك ومكافحة الغش، وكذلك قانون رقم 18-05 المتعلق بالتجارة الإلكترونية.

الفرع الأول : الجرائم المنصوص عليها في القانون 09-03 المتعلق بحماية المستهلك وقمع الغش

يعتبر قانون رقم 09-03 المتعلق بحماية المستهلك ومكافحة الغش في الجزائر، مصدرًا للحماية القانونية للمستهلك الإلكتروني في مواجهة مجموعة متنوعة من الجرائم التي تؤثر على مصلحته. هذه الجرائم تشمل:

[1] أنظر المادة 372 من الأمر رقم 66-156 المتضمن قانون العقوبات، مرجع سابق

[2] العايب سامية، عرابة منال، مرجع سابق، ص80

[3] المرجع نفسه،ص80

أولا: جريمة الخداع

يُعتبر الخداع من بين الجرائم الاجتماعية المعاصرة التي تنتشر في مختلف مجالات الحياة. ومن أجل مكافحة هذه الظاهرة المدمرة وضمان أمن وسلامة المستهلك، قام المشرع بتنظيم هذه الجريمة من خلال المادة 68 في قانون رقم 09-03 المتعلق بحماية المستهلك ومكافحة الغش.

1- **تعريف جريمة الخداع:** لم يعرف المشرع الجزائري جريمة الخداع وترك ذلك للفقه و الذي عرفه على أنه : الباس أمر من الأمور مظهر يخالف ما هو عليه "[1] كما يعرفه البعض الآخر بأنه القيام ببعض للتصرفات كالأكاذيب أو بعض الحيل البسيطة التي من شأنها التأثير على المستهلك وايقاعه في غلط حول الشيء موضوع العقد على نحو مخالف للمحقيقة[2]

يجب أن يتسبب الخداع في التأثير على المستهلك وتضليله بشأن المنتج، وهذا يختلف عن جريمتي النصب والغش.

2- **أركان جريمة الخداع**

تتضمن جريمة خداع المستهلك الإلكتروني أو المتعاقد عمومًا عنصرين أساسيين، الركن المادي والركن المعنوي. يستند الركن المادي إلى سلوكيات ملموسة ومتعلقة بإرادة شخصية متعمدة تهدف إلى خداع المستهلك واختراق الثقة والمصداقية التي يعتمد عليها المستهلك في المعاملات التجارية.

أ- **الركن المادي جريمة الخداع:**

نص القانون رقم 09/03 المتعلق بحماية المستهلك وقمع الغش في المادة 68 منه على جريمة الخداع

[1] شعباني نوال، التزام المتدخل بضمان سلامة المستهلك في ضوء قانون حماية المستهلك وقمع الغش، رسالة ماجيستير، جامعة مولود معمري، تيزي وزو، 2012، ص137

[2] منال بوروح، ضمانات حماية المتهم في ظل القانون 09-03، اطروحة لنيل شهادة الماجستير، فرع قانون حماية المستهلك والمنافسة، كلية الحقوق، جامعة يوسف بن خدة، الجزائر 1، 2015،ص176

الركن المادي بجريمة الخداع يتمثل في محاولة المورد الالكتروني بأي وسيلة أو طريقة لخداع المستهلك، ويشمل عدة جوانب مهمة. أحد هذه الجوانب هو تلاعب بكمية المنتجات المقدمة، حيث يقوم الجاني بتقديم كمية أقل مما تم الاتفاق عليه أو ترويج منتجات ذات جودة منخفضة. علاوة على ذلك، قد يقوم الجاني بتسليم منتجات غير تلك المعينة مسبقاً، مما يؤدي إلى خداع المستهلك وإفساد صفقته.[1]

بالإضافة إلى ذلك، يتضمن الركن المادي أيضًا عدم قابلية استعمال المنتجات المقدمة. يعني هذا أن المستهلك لا يستطيع استخدام المنتج بالشكل المناسب أو لا تفي المنتجات بالاحتياطات اللازمة لاستخدامها بأمان.[2]

يتوقع من المنتجات أن توفر نتائج معينة وتلبي احتياجات المستهلك. ومن خلال الركن المادي للخداع، يمكن أن يقوم الجاني بتضليل المستهلك بشأن قدرة المنتج على تحقيق تلك النتائج المنتظرة. قد يعدل الجاني خصائص المنتج أو يوفر معلومات زائفة بشأنه، مما يجعل المستهلك يتعرض للخداع ويشتري منتجًا لا يفي بالأداء المتوقع.[3]

ينص القانون الجزائري في المادة 429 من قانون العقوبات على أن الركن المادي في جريمة الخداع يتحقق في كل فعل يصدر عن الجاني يخدع أو يحاول أن يخدع المستهلك في الطبيعة أو الصفات الجوهرية للسلعة أو التركيب أو نسبة المقومات اللازمة للسلعة.[4]

---

[1] مجدوب نوال،حماية المستهلك جنائيا من جريمة الخداع في عملية تسويق المواد الغذائية، مجلة دفاتر السياسية والقانون، العدد15،كلية الحقوق والعلوم السياسية،جامعة ابو بكر بلقايدن تلمسان،2016، ص271

[2] بودالي محمد، حماية المستهلك في القانون المقارن دراسة مقارنة مع القانون الفرنسي، دارالكتاب الحديث، الجزائر، 2006، ص213

[3] بودالي محمد، شرح جرائم الغش في بيع السلع والتدليس في المواد الغذائية والطبية ،ديوان المطبوعات الجامعية، الجزائر ،2006، ص20

[4] أنظر المادة 429 من الأمر رقم 66-156 المتضمن قانون العقوبات، مرجع سابق

ب- الركن المعنوي جريمة الخداع:

في جريمة الخداع. تُعتبر جريمة الخداع جريمة عمدية، ويُشترط لتحقيقها القصد الجنائي من قِبل الجاني، وهذا يعني أنه يجب أن يكون الجاني على علم بأركان جريمته ويقصد القيام بها. بشكل عام، تعتبر جريمة الخداع جريمة جنائية وفقًا للقانون الجزائري.

كما تجدر الإشارة إلى أن المادة 68 من القانون 09/03 المتعلق حماية المستهلك وقمع الغش لم تشترط إلحاق الضرر بالمستهلك، ولهذا صنفها البعض ضمن جرائم الخطر وليست من جرائم الضرر.

3- عقوبة جريمة الخداع:

أحالت المادة 68 من 09/03 المتعلق حماية المستهلك وقمع الغش فيما يخص العقوبة إلى المادة 429 من قانون العقوبات، فيعاقب بالحبس من شهرين إلى 3 سنوات وغرامة من 2.000 دج إلى 20.000 دج أو بإحدى هاتين العقوبتين فقط

تنص المادة 68 من قانون حماية المستهلك وقمع الغش والمادة 430 من قانون العقوبات على زيادة صرامة العقوبة في حالة ارتكاب أو محاولة ارتكاب جريمة باستخدام وسائل محددة في تلك المواد. وتشمل هذه العقوبة الحبس لمدة خمس سنوات ودفع غرامة تصل إلى 500,000 دينار جزائري. ويُعاقب الشخص المعنوي وفقًا للمادة 431 من قانون العقوبات الجزائري، وتتم محاسبته على أساس المعايير المنصوص عليها في المادة 18 المكررة من قانون العقوبات، بالإضافة إلى تطبيق عقوبات تكميلية. يتم أيضًا حجز المنتجات والأدوات وأي وسيلة أخرى استُخدمت في ارتكاب الجريمة.[1]

[1] انظر المادة 429 من الأمر 66-156 المتضمن قانون العقوبات ، مرجع سابق

ثانيا : جريمة الغش التجاري الالكتروني

1-تعريف الغش التجاري الالكتروني:

ان للغش عدة تعريفات نذكر منها التعريف التقليدي هو إظهار المبيع على خلاف ما هو على حقيقته سواء كان ذلك بالقيام بعمل أو بقول أو بكتمان[1]

في الجانب التشريعي، قانون حماية المستهلك وقمع الغش لم يتضمن تعريفًا محددًا للغش في التجارة الإلكترونية. بدلاً من ذلك، تم استبدال مصطلح "الغش" بمصطلح "التزوير"، على الرغم من أنهما يحملان نفس المعنى. ويتعلق الغش، وفقًا لقانون حماية المستهلك وقمع الغش، بجميع المنتجات سواء كانت مواد استهلاكية أو معدات، ويُطبق أيضًا على الخدمات نظرًا لأنها تُعتبر منتجات. ويمتد تطبيق هذا القانون أيضًا ليشمل المنتجات التي تستهدف الاستهلاك الحيواني.[2]

2-اركان جريمة الغش التجاري الإلكتروني:

تتطلب جريمة الغش ركنان اساسيان ، الركن المادي والركن المعنوي، وهذا ما سنبينه تاليا:

أ- الركن مادي الغش التجاري الالكتروني:

تنص المادة 70 من قانون حماية المستهلك وقمع الغش، وكذا المادة 431 من قانون العقوبات الجزائري على مجموعة من الأفعال المحظورة التي تعتبر جرائم، كما يلي :

يعاقب بالعقوبات المنصوص عليها فيً المادة 431 من قانون العقوبات كل من:

-يزور أي منتج موجه للاستهلاك أو للاستعمال البشري أو الحيواني

[1] ابراهيم احمد،البسطويسي،المسؤولية عن الغش في السلع، دراسة بين الفقه الاسلامي والقانون التجاري، دار الكتب القانونية، القاهرة،2011،ص18

[2] المرجع نفسه،ص67

- يعرض أو يضع للبيع أو يبيع، مع علمه بوجهتها مواد أو أدوات أو أجهزة أو كل مادة خاصة من شانها أن تؤدي إلى تزوير أي منتج موجه للاستعمال البشري أو الحيواني.[1]

ومع ذلك، يُلاحظ أن المادة 70 استخدمت مصطلح "التزوير" بدلاً من مصطلح "الغش" الذي ذُكر في المادة 431 من قانون العقوبات. وبالإضافة إلى ذلك، تم استخدام المادة 82 من قانون حماية المستهلك وقمع الغش أيضًا لاستخدام مصطلح "الغش"، وقد تم إحالتها إلى المادة 432 من قانون العقوبات الجزائري.

على سبيل المثال، يمكن تحقيق جريمة الغش في ثلاثة أنشطة، وهي تصنيع أو ترويج سلع مغشوشة. ويعني "الغش" في هذا السياق أي تغيير أو تشويه يتعرض لجوهر المادة، سواءً كان ذلك من خلال تغيير عناصر السلعة نفسها أو خلطها بمنتجات أخرى أو إضافة مواد غريبة أو إنقاص مكوناتها النافعة.[2]

أما عرض السلع المغشوشة للبيع، فيعتبر كافيًا لارتكاب الجريمة، فقط يكفي أن تكون السلعة المغشوشة مُعروضة أو معروضة للبيع.

وتنص المادة 431/3 من قانون العقوبات الجزائري على تجريم التعامل في مواد وأجهزة خاصة تستخدم في الغش، وذلك بهدف حماية الصحة العامة. وتجدر الإشارة إلى أن هذه الممارسات منتشرة بشكل خاص في المواقع الإلكترونية، خاصةً في ظل غياب رقابة صارمة على المنتجات المُعروضة[3].

[1] قانون رقم 09-03، المتضمن حماية المستهلك وقمع الغش، مرجع سابق

[2] بلارو كمال الحماية الجنائية للمستهلك الالكتروني في ظل التشريع الجزائري، مجلة البحوث في العقود وقانون الأعمال، العدد السابع،جامعة الاخوة منتوري ، قسنطينة1، 2019، ص78، تم الاطلاع عليه من الموقع التالي https://www.asjp.cerist.dz/en/article/69292

[3] أنظر المادة 3 من قانون العقوبات ، مرجع سابق

ب- الركن المعنوي الغش التجاري الالكتروني:

جريمة الغش هي جريمة عمدية تتطلب وجود قصد جنائي عام، وذلك يتحقق عندما يكون لدى المتهم نية واضحة لارتكاب الغش وعلمه به. بمعنى آخر، يجب أن يكون المتهم على علم بأنه يقوم بتزوير وتزييف المنتج في القصد الجنائي العام.[1]

لذلك، يتعين توافر القصد الجنائي وعلم المتهم بالغش في الوقت الذي يقوم فيه بالفعل الجنائي ليكون مسؤولًا جنائيًا عن جريمة الغش.[2]

3-عقوبة الغش التجاري الالكتروني:

تعتبر جريمة الغش جنحة يعاقب عليها بالحبس لمدة تتراوح بين سنتين وخمس سنوات، وفقًا للمادة 431 من قانون العقوبات الجزائري. وتشمل العقوبة أيضًا غرامة تتراوح بين 10,000 دج و50,000 دج. وفي حالة تعرض الأشخاص الذين استهلكوا المواد الغذائية المغشوشة أو الفاسدة للأذى أو الإعاقة أو عدم القدرة على العمل، يتم زيادة عقوبة الحبس إلى 5-10 سنوات والغرامة من 500,000 دج إلى 1,000,000 دج.

وفي حالة تسبب تلك المواد في أمراض غير قابلة للشفاء أو فقدان عضو أو إعاقة دائمة، يعاقب الجناة بالسجن المؤقت لمدة 10-20 سنة، إضافة إلى غرامة تتراوح بين 1,000,000 دج و2,000,000 دج. وفي حالة وفاة شخص بسبب تلك المواد، يعاقب الجناة بالسجن المؤبد.[3]

بالإضافة إلى العقوبات المذكورة، تنص المادة 82 من قانون حماية المستهلك وقمع الغش على عقوبات تكميلية تشمل مصادرة المنتجات والأدوات وأي وسيلة أخرى استخدمت في ارتكاب الغش.

---

[1] عبد الله حسين محمود، حماية المستهللك من الغش التجاري او الصناعي، دار النهضو العربية،االقاهرة،2002،ص10و11

[2] خلوي عنان نصيرة، المرجع السابق، ص99

[3] أنظر المادة 431 من الأمر رقم 66-156 المتضمن قانون العقوبات، مرجع سابق

وبالتالي، تُفرض عقوبات قانونية صارمة على جرائم الغش، بما في ذلك عقوبات سجنية وغرامات مالية، وإجراءات تكميلية مثل مصادرة المنتجات المغشوشة والأدوات المستخدمة في الغش.

4-التفرقة بين الغش التقليدي والغش الالكتروني

فيما يتعلق بالتفرقة بين الغش التجاري التقليدي والغش التجاري الإلكتروني، يمكن تلخيص الاختلافات على النحو التالي[1]:

أ- الغش التجاري التقليدي:

يشمل غشًا في كمية البضائع، ويعني زيادة أو نقصان في الوزن أو الحجم المعلن للمنتج.و يشمل غشًا في نوع السلعة، حيث يمكن استبدال المنتج بآخر ذو جودة أقل أو أقل قيمة. كما يشمل غشًا في الخصائص الجوهرية للبضاعة، مثل الاختلاط بين منتجات مختلفة أو تغيير في مواصفات المنتج. وايضا يشمل غشًا في طبيعة البضاعة، مثل تزييف المنتج أو بيع منتج ذو جودة منخفضة وادعاء أنه منتج عالي الجودة.

ب- الغش التجاري الإلكتروني:

يشمل غشًا في نقل الأموال إلكترونيًا، مثل احتيالات البنوك عبر الإنترنت أو الاحتيال في عمليات الدفع الإلكتروني.و يشمل غشًا في الأسهم والاستثمار، مثل احتيالات الأسهم عبر الإنترنت أو تلاعب الأسعار.وايضا يشمل غشًا في بطاقات الائتمان، مثل سرقة معلومات البطاقات أو استخدامها بشكل غير مصرح به.كما يشمل غشًا في خدمات الوصول إلى الإنترنت، مثل تقديم خدمات وهمية أو استخدام تقنيات احتيالية لاستدراج المستخدمين.بالإضافة الى انه يشمل غشًا في المزادات الإلكترونية، مثل زيادة الأسعار بشكل اصطناعي أو عرض منتجات غير حقيقية للبيع.[2]

---

[1] محكوف اسماء، مرجع سابق، ص68

[2] ابراهيم احمد،البسطويسي،المسؤولية عن الغش في السلع، دراسة بين الفقه الاسلامي والقانون التجاري، دار الكتب القانونية، القاهرة،2011،ص18

تتمثل أشكال الغش التجاري الإلكتروني في استخدام الإنترنت في عمليات الاحتيال التجاري، وقد تشمل عدم توفير السلع والخدمات المعلن عنها أو تقديم منتجات أو خدمات ذات جودة سيئة. وقد أصبحت هذه الأشكال أكثر انتشارًا في بيئة الأعمال التي تعتمد على منتجات وخدمات الكمبيوتر والخدمات المالية.

الفرع الثاني: الجرائم المنصوص عليها في القانون 2018 المتعلق بالتجارة الالكترونية

تم اعتماد قانون جديد رقم 18- يتعلق بالتجارة الإلكترونية، وذلك استجابةً للتطورات الحاصلة في العالم التجاري الذي أصبح يشبه قرية رقمية. يحدد هذا القانون القواعد العامة المتعلقة بالتجارة الإلكترونية للسلع والخدمات. ويهدف هذا القانون إلى إعادة التوازن بين الطرف الضعيف، وهو المستهلك الإلكتروني، والطرف القوي الذي يفرض بنوده وشروطه بشكل يخدم مصلحته(المورد). ويأتي ذلك نتيجة الحاجة الملحة لتلبية احتياجات المستهلك في هذه البيئة الرقمية.[1]

أولا: جريمة الترويج الالكتروني لسلع ممنوعة التسويق يُعاقب بموجب المادة 34 من القانون رقم 18/05، الذي يُشار إليه سابقًا، كل شخص يروج أو يعلن عن منتج أو خدمة محظورة من خلال وسائل الاتصال الإلكتروني.[2]

وتتمثل العقوبة في تغريمه مبلغًا يتراوح بين 50.000 دج و 500.000 دج وفقًا لما ينص عليه المادة 40 من القانون رقم 18/05.

1-الركن مادي جريمة الترويج الالكتروني لسلع ممنوعة التسويق

يتحقق الركن المادي سواء بعرض للبيع أو البيع عبر الوسائط الالكترونية ما يلي :

تشمل المنتجات والخدمات المحددة في المادة 03 من القانون 18-05 ما يلي:

- ألعاب القمار والرهان واليانصيب.

[1] بلارو كمال ،مرجع سابق ،ص81

[2] مجدوب نوال، الحماية الجنائية للمستهلك الالكتروني وفكرة الأمن الاقانوني، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 7، العدد1، ،2022،ص642

- المشروبات الكحولية ومنتجات التبغ.

- المنتجات الصيدلانية.

- المنتجات التي تنتهك حقوق الملكية الفكرية أو الصناعية أو التجارية.

- أي سلعة أو خدمة محظورة وفقًا للتشريعات السارية، مثل الألعاب النارية والمفرقات الممنوعة من البيع داخل البلاد.

- أي سلعة أو خدمة تتطلب عقدًا رسميًا وتتطلب إجراءات قانونية محددة، مثل شراء وبيع السيارات.

المنتوجات والخدمات المنصوص عليها في المادة 05 من القانون 18-05 وهي:

- العتاد والتجهيزات والمنتجات الحساسة المحددة قانونا بموجب نص خاص

- الخدمات التي تمس بمصالح الدفاع الوطني والنظام العام والأمن العمومي

كما يمنع كذلك بيع المواد الأولية في حالتها الأصلية إذا كانت موجهة [1]

2- الركن معنوي جريمة الترويج الالكتروني لسلع ممنوعة التسويق

هذه الجريمة جريمة عمدية تتطلب وجود قصد جنائي عام، حيث يتم تحقيق هذا القصد العام من خلال معرفة المخالف بأن القانون يحظر عرض أو بيع هذه الخدمات والسلع، والتي لا تقتصر على غيرها، ومع ذلك، يقوم المخالف بالقيام بتلك الأعمال.[2]

3- عقوبة جريمة منع التعامل عن طريق الاتصالات الالكترونية في بعض السلع والخدمات

إذا نظرنا إلى النص القانوني المتعلق بالتجارة الإلكترونية، نجد أن المشرع قد أقر جرائم تتراوح عقوبتها بين 3 أشهر و 6 أشهر. وفيما يتعلق ببيع أو عرض السلع والخدمات المحظورة وفقًا للمادة 05 عبر وسائل الاتصال الإلكترونية، يتم فرض غرامة تتراوح بين 200,000 دج و 1,000,000 دج، ويحق للقاضي أن يأمر بإغلاق الموقع الإلكتروني

[1] بلارو كمال، مرجع سابق،ص89

[2] بلارو كمال ، مرجع سابق ، ص83

وشطبه من السجل التجاري[1]. بالإضافة إلى ذلك، يمكن توقيع عقوبات أخرى مثل حجز البضائع المخالفة والأدوات ومعدات استخدمت في ارتكاب الجرائم.

بالنسبة للعقوبات المتعلقة بطبيعة السلع والخدمات، تتمثل جميعها في فرض غرامات كما يلي: يتم فرض غرامة تتراوح بين 200,000 دج و 1,000,000 دج على من يقوم ببيع أو عرض السلع والخدمات المحظورة وفقًا للمادة 03 عبر وسائل الاتصال الإلكترونية، ويحق للقاضي أن يأمر بإغلاق الموقع الإلكتروني لفترة تتراوح بين شهر واحد و6 اشهر.[2]

وبالنسبة إلى المادة 35 من القانون رقم 04-02 التي تحدد القواعد المطبقة على الممارسات التجارية المعدل والمتمم، يتم تغريم أي شخص يخالف المادة 20 من القانون رقم 18-05 بغرامة تتراوح بين 100,000 دج و 3,000,000 دج[3].

ثانيا: جريمة الإشهار الالكتروني الكاذب و المضلل:

تنص المادتان 31 و 32 في قانون التجارة الإلكترونية على الالتزامات التي يجب على الموردين الإلكترونيين الالتزام بها، وتهدف هذه الالتزامات إلى حماية المستهلك الإلكتروني من الإعلانات الكاذبة والمضللة. وتشمل هذه الالتزامات تقديم معلومات صحيحة ودقيقة عن المنتجات أو الخدمات المقدمة، وتوضيح الشروط والأحكام المتعلقة بالعمليات التجارية والمبيعات.أما المادة 40 في القانون، فتنص على أن الإعلان الذي ينتهك المورد الإلكتروني قوانين الإعلان والترويج يعتبر إعلانًا غير مرغوب فيه ويعاقب عليه. ويتم تحديد جريمة الإعلان بناءً على اركان مادية ومعنوية لتحديد المسؤولية القانونية للمورد الإلكتروني.هذه التدابير التشريعية تهدف إلى ضمان نزاهة وشفافية العروض والإعلانات على الإنترنت، وحماية حقوق ومصالح المستهلكين الإلكترونيين.[4]

---

[1] راجع المادة 38 من القانون رقم 18-05 المتعلق بالتجارة الالكترونية،مرجع سابقذ

[2] راجع المادة 37 من المرجع نفسه

[3] القانون رقم 04-02 المؤرخ في 23 يونيو سنة سنة 2004، يحدد القواعد المطبقة على الممارسات التجارية،المعدل والمتمم،ج.ر،عدد41، 2004

[4] قليل زوبيدة، الاشهار الإلكتروني في ظل قانون 18-05، مذكرة مكملة لنيل شهادة الماستر، تخصص قانون اعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي،2020،ص48

1-تعريف الاشهار الالكتروني

يعتبر الإعلان التجاري وسيلة فعالة للتعريف بالمنتجات وتعزيز التعاقدات التجارية. إنه عنصر أساسي في استراتيجية التسويق ويشكل جزءًا لا يتجزأ من المنافسة الشرعية. يمثل الإعلان التجاري كل ما يستخدمه التاجر لتحفيز العملاء وجذبهم لشراء منتجاته، سواء كان ذلك من خلال وسائط بصرية أو سمعية أو مكتوبة.[1]

قد تم التطرق إلى الجانب التشريعي في القانون الجزائري من خلال المادة الثانية، الفقرة الأولى من المرسوم التنفيذي 90-39 الذي يتعامل مع مسائل الجودة ومكافحة الغش. يتم تعريفه على أنه يشمل جميع الاقتراحات أو الإعلانات أو البيانات أو العروض التي يتم نشرها بواسطة وسائط بصرية أو سمعية بصرية من قبل الأفراد أو الشركات.[2]

كما تم تعريف الإعلان بواسطة المادة الثالثة، الفقرة الثالثة من القانون 04-02 الذي يحدد قواعد الممارسات التجارية، وذلك على أنه أي إعلان يهدف مباشرة أو غير مباشرة إلى تعزيز بيع السلع أو الخدمات، بغض النظر عن المكان أو وسائل الاتصال المستخدمة في ذلك[3]

تم تعريف الإعلان الإلكتروني في قانون التجارة الإلكترونية 18-05 من خلال المادة السادسة، الفقرة السادسة بأنه "أي إعلان يهدف بشكل مباشر أو غير مباشر إلى تعزيز بيع سلع أو خدمات من خلال وسائط الاتصال الإلكترونية."[4]

---

[1] زوبة سميرة، حماية المستهلك من الخداع الاعلاني الالكتروني،مجلة الدراسات القانونية، عدد25،مركز البصرة للبحوث والاستشارات والخدمات التعليمية،2017،ص29

[2] المرسوم التفيذي رقم 90-39 المتعلق برقابة الجودة وقمع الغش،مؤرخ في 03 رجب 1410 الموافق ل30 جانفي 1990،ج.ر،عدد05،الصادرة بتاريخ 31 جانفي 1990

[3] القانون رقم 04-02 المؤرخ في 23 يونيو سنة سنة 2004، يحدد القواعد المطبقة على الممارسات التجارية،المعدل والمتمم،ج.ر،عدد41، 2004

[4] قانون رقم 18-05، المؤرخ في 24 شعبان عام 1439 الموافق ل 10 ماي 2018، المتعلق بالتجارة الالكترونية،ج.ر،عدد28

2-تعريف الاشهار الالكتروني الكاذب المظلل

لم يقم المشرع الجزائري بتعريف الإشهار الإلكتروني الكاذب بشكل مباشر، إلا أنه تناول هذا الموضوع ضمن مشروع القانون المتعلق بممارسة النشاط الإشهاري في المادة 09. وفي هذه المادة، تم تعريف الإشهار الكاذب على أنه يشمل الادعاءات الكاذبة، والوعود الكاذبة، والإشارات الكاذبة، والعروض الكاذبة أو الغامضة، التي قد تضلل المستهلك أو المستخدم أو مستعمل الأملاك والخدمات.هذا التعريف يهدف إلى حماية المستهلك وضمان نزاهة الإعلانات، ويعتبر الإشهار الكاذب في السياق الإلكتروني من الممارسات غير المرغوبة والتي يمكن أن تتسبب في تضليل المتلقي وتؤثر سلباً على قراراته واختياراته.[1]

3- أركان جريمة الإشهار الالكتروني الكاذب و المضلل:

سنتناول الآن أهمية وجود ركنين أساسيين لجريمة الإعلان الكاذب والمضلل في الوسط الإلكتروني. سنستكشف كل من هذين الركنين بالتفصيل لفهم طبيعة الجريمة وتداعياتها.

أ- الركن المادي جريمة الإشهار الالكتروني الكاذب و المضلل:

لتنفيذ الجانب المادي في جريمة الإعلان الكاذب والمضلل في الوسط الإلكتروني، يجب على المورد الإلكتروني استخدام طرق وأساليب احتيالية. على الرغم من عدم تحديد التشريعات بشكل محدد لتلك الأساليب، إلا أنها تم ذكرها في المادة 37 من قانون العقوبات والمادة 31 من قانون التجارة الإلكترونية لعام 2018. وفقًا لهذه القوانين، يجب أن يقوم الفاعل بالحصول على تسليم مبلغ مالي أو أية قيمة منقولة عبر تلك الوسائل، بالإضافة إلى تسببه في تسليم شيء يتسبب في الحد من قيمة مالكه. وفي النهاية، يجب أن يكون هناك قصد الغش، حتى يمكن أن يُصنف هذا الإعلان ضمن نطاق الإعلان التضليلي الإلكتروني.[2]

---

[1] قليل زبيدة، مرجع سابق، ص40

[2] جافلي حسين، الحماية الجنائية للمستهلك من الاشهار الالكتروني في التجارة الالكترونية، الملتقى الوطني حول" الاطار القانوني لممارسة التجارة الالكترونية على ضوء قانون 10-05 "، يوم 8 اكتوبر 2019، جامعة العربي التبسي، تبسة، ص567

ب- ركن معنوي جريمة الإشهار الالكتروني الكاذب و المضلل:

في القانون الجزائري، يُعتبر الكذب في الإعلان الإلكتروني بشأن المواد الغذائية والخدمات خداعًا للمستهلك أو محاولة للخداع، ويعد ذلك جريمة يتطلب ثبوت القصد الجنائي. يُعتبر القصد الجنائي توجه المتهم بالعمل الجرمي ونية إدخال الغش على الأشخاص الذين يتعاملون معه. ونظرًا لأن الإعلان الكاذب هنا يُعتبر جريمة خداع، فإن المشرع يعتبرها جريمة عمدية تتطلب وجود القصد الجنائي كأحد عناصرها[1].

3- عقوبة الإشهار الالكتروني الكاذب و المضلل:

تم تحديد العقوبات المترتبة على جريمة الإشهار الإلكتروني الكاذب والمضلل في القانون 2018 المتعلق بالتجارة الإلكترونية. وتنص المادة 40 من القانون على أنه، بدون المساس بحقوق الضحايا في التعويض، يجب معاقبة المخالفين لأحكام المواد 30 و 31 و 32 و 33 و 34 من القانون بغرامة تتراوح بين 50,000 دج و 500,000 دج.[2] وفي المادة 39 من نفس القانون، تم تحديد أيضًا عقوبة بغرامة تتراوح بين 50,000 دج و 500,000 دج لأي مورد إلكتروني يخالف أحد الالتزامات المنصوص عليها في المادتين 11 و 12 من القانون. وبهذا، يتم تطبيق عقوبات محددة ومناسبة على الأفراد والمؤسسات التي يتم إدانتها بارتكاب جرائم الإشهار الإلكتروني الكاذب والمضلل والتجاوز عن الالتزامات المنصوص عليها في القوانين ذات الصلة.[3]

---

[1] غربوج حسام الدين، حماية المستهلك من الممارسات التجارية غير النزيهة في التشريع الجزائري، اطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون الاعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2017-2018، ص103

[2] قانون رقم 18-05، مؤرخ في 24 شعبان عام 1439 الموافق ل 10 مايو سنة 2018، يتعلق بالتجارة الالكترونية، مرجع سابق.

[3] قانون رقم 18-05، يتعلق بالتجارة الالكترونية، لمرجع سابق.

المبحث الثاني

حماية المستهلك الالكتروني في إطار التعاقد الالكتروني

في عالم التعاقد الإلكتروني، يستند العمل على التكنولوجيا الحديثة في الإنترنت كوسيلة رئيسية، وهي تفرض بشكل لازم تبني إجراءات حماية إضافية ومخصصة خصيصًا للمستهلك الإلكتروني، نظرًا لأن المستهلك يُعَدّ الطرف الضعيف في هذا النوع من العقود. علاوة على ذلك، يُلاحَظ أن استخدام هذه التكنولوجيا قد زاد من اتساع الفجوة العقدية التي ظهرت مع ظهور هذه العقود.

يتعين علينا أن ندرك أن وسيلة التعاقد الإلكتروني، التي تعتمد على التكنولوجيا الحديثة في عالم الإنترنت، تفرض بشدة الحاجة إلى تطوير آليات حماية إضافية ومتخصصة خصيصًا للمستهلك الإلكتروني، وذلك بناءً على حقيقة أن المستهلك يعد الطرف الضعيف في هذا النوع من العقود. علاوة على ذلك، يجب الإشارة إلى أن استخدام هذه التكنولوجيا قد زاد من حدة عدم التوازن العقدي الذي ظهر في ظل وجود هذه العقود.

ومن بين هذه المشاكل البارزة، تأتي في المقام الأول الاعتداء على المستهلك الإلكتروني، وخاصة فيما يتعلق ببياناته الشخصية (المطلب الأول)، بالإضافة إلى زيادة وسائل الدفع الخاصة به التي تشهد نموًا مستمرًا (المطلب الثاني). ولذا، من الضروري التوقيع حماية جنائية لهذه الوسائل، نظرًا للخسائر المحتملة المترتبة على الاعتداء عليها في المستقبل

المطلب الأول

الحماية الجنائية للبيانات الشخصية للمستهلك الالكتروني

ظهور الإنترنت وانتشاره في جميع جوانب الحياة أدى إلى زيادة المخاطر التي يتعرض لها خصوصية المستهلك. ولهذا السبب، ظهرت حاجة ملحة لحماية البيانات الشخصية، حيث كاد انتهاك تلك البيانات الرسمية للمستهلك الإلكتروني أن يصبح جزءًا من سمات العصر الرقمي. ووفقًا لتقرير غير رسمي، يتعرض اثنان من كل ثلاثة مستهلكين لمخاطر سوء استخدام معلوماتهم الشخصية من قِبَل مشغلي مواقع الإنترنت.[1]

في هذا السياق، سنتناول في هذا المطلب تعريف البيانات الشخصية للمستهلك وسنسلط الضوء على أشكال الاعتداء على تلك البيانات الشخصية. بالإضافة إلى ذلك، سنناقش أيضًا الإجراءات المتاحة لحماية هذه البيانات وضمان سلامتها.

الفرع الأول: تعريف البيانات الشخصية للمستهلك الالكتروني:

لقد أصبحت البيانات الإلكترونية ذات أهمية هائلة في عصرنا، إذ تُعَدُّ هذه البيانات سلعة ذات قيمة فائقة تُقَدَّر بملايين الدولارات لدى أولئك الذين يمتلكونها. ومن بين هذه البيانات، تتصدّر تلك التي تتعلق برغبات المستهلك وميولاته الشخصية. فعلى سبيل المثال، بيانات التصفح والتفاعل على وسائل التواصل الاجتماعي، والتفضيلات الشرائية، وتاريخ التصفح على الإنترنت تُعَدُّ جوهرية للشركات والمنظمات التي تسعى للاستفادة منها في استهداف المستهلكين وتوجيه عروضها وإعلاناتها بشكل مخصص لكل فرد.[2]

أولا: التعريف الفقهي

في الفقه، يُناقش بشكل شامل مسألة البيانات الشخصية الإلكترونية، ويُعرَفُها بأنها "تلك البيانات التي تتعلق بحرمة الحياة الخاصة للإنسان. ومن ضمن هذه البيانات، تتضمن بعضها ما يسمح بتشكيل صورة مفصلة عن توجهاته وميولاته الشخصية، بينما يتعلق

[1] عمارة ليندة، افنان عبد الغاني، مرجع سابق، ص 24

[2] عمارة ليندة، افنان عبد الغاني، مرجع سابق، ص 24

البعض الآخر باتجاهاته السياسية ومعتقداته الدينية، وتعاملاته المالية والبنكية، وحتى جنسيته وهواياته".[1]

تلك البيانات الشخصية تُعَدُّ جزءًا حساسًا من خصوصية الفرد وحياته الشخصية، وبالتالي تتطلب حمايةً خاصة. إذ ينبغي أن يتم التعامل معها بكل دقة وحذر لضمان عدم انتهاك حقوق الأفراد وتعرضهم للإساءة أو الاستغلال.

ثانيا التعريف التشريعي

أحدثت التشريعات المقارنة، بما في ذلك التوجيه الأوروبي رقم CE/95/46 الصادر عن البرلمان الأوروبي والمجلس في 24 أكتوبر 1995، تعريفًا للبيانات الشخصية ووضعت إطارًا لحماية الأفراد فيما يتعلق بمعالجة تلك البيانات وحرية تداولها. وفقًا لهذا التعريف، يتم اعتبار البيانات الشخصية على أنها "المعلومات المتعلقة بشخص محدد أو قابل للتعرف، سواء كانت تتعلق بخصائصه الجسدية أو العقلية أو الاقتصادية والثقافية، أو بالهوية الاجتماعية أو بالسجلات المحفوظة عنه".[2]

يشمل التعريف القانوني للبيانات الشخصية أيضًا مجموعة واسعة من المعلومات التي تساهم في تحديد هوية الفرد وتعكس جوانب مختلفة من حياته الشخصية. تشمل هذه البيانات الشخصية على سبيل المثال لا الحصر الاسم الكامل للفرد، ورقم الضمان الاجتماعي الذي يعتبر معرفًا فريدًا يتعلق بالشخص، ورقم تسجيل السيارة الخاصة به الذي يعطي معلومات عن ملكية السيارة والشخص المرتبط بها، ورقم الهاتف الثابت،الجوال الذي يتيح وسيلة اتصال مباشرة بالفرد، ورقم بطاقة الائتمان الذي يكشف وسيلة دفع وتعامل مالي يستخدمها الشخص، بالإضافة إلى العنوان الإلكتروني الذي يمثل موقعه الرقمي في العالم الافتراضي.[3]

---

[1] بيومي حجازي عبد الفتاح، التجارة الالكترونية وحمايتها القانونية، الكتاب الثاني، دار الكتب القانونية، مصر، 2007، ص64

[2] لعمريوي ليلى، الحماية الجنائية للمستهلك الالكتروني، مذكرة لنيل شهادة الماستر في القانون، قسم القانون، تخصص قانون جنائي وعلوم جنائيية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018،ص42

[3] المرجع نفسه، ص42

الفرع الثاني: صور الاعتداء على البيانات الشخصية للمستهلك الالكتروني:

يشهد الاستهلاك الإلكتروني تعددًا في حوادث انتهاك البيانات الشخصية، حينما يقوم المستهلك بشراء سلع أو طلب خدمات عبر الإنترنت. ويمكن تلخيص هذه الحوادث في النقاط التالية:

أولا: جمع البيانات الشخصية الخاصة بالمستهلك الالكتروني دون موافقة:

عترض الكثير من الاعتداءات على بيانات المستهلك الإلكتروني أثناء عملية شراء السلع وطلب الخدمات عبر الإنترنت. يتم ذلك من خلال أنشطة مثل مراقبة، اعتراض، تفريغ، وقراءة الرسائل التي يتبادلها المستهلك مع الأطراف المشاركة عن طريق البريد الإلكتروني. يتم تحقيق ذلك من خلال اختراق المواقع الإلكترونية والأجهزة الشخصية، أو باستخدام أساليب أخرى لجمع البيانات بطرق غير قانونية. على سبيل المثال، يتم استخدام برامج خبيثة مثل ملفات تعريف الارتباط (الكوكيز) وبرامج التجسس الإلكتروني (سبايوير)[1] لجمع البيانات الشخصية بدون موافقة المستهلك الإلكتروني. وتشمل هذه البيانات المسروقة معلومات حول المستهلك، بما في ذلك المكالمات التي تتم عبر الإنترنت وتحتوي على بيانات شخصية عنه.

ثانيا: الاطلاع و الإفشاء غير المشروع للبيانات الشخصية للمستهلك الالكتروني:

يتجلى هذا النوع من الاعتداء في قدرة الجاني على الاطلاع التام على معلومات وبيانات المستهلك الإلكتروني بطريقة غير قانونية، حيث يتم الاطلاع على هذه البيانات من قِبَل شخص غير مخول بالولوج إليها بشكل قانوني. ويشمل ذلك انتهاك الخصوصية والحصول على البيانات الشخصية للمستهلك في إطار عقود التجارة الإلكترونية، سواء من خلال اختراق المواقع الإلكترونية أو اختراق شبكات الاتصال للوصول إلى قواعد البيانات. يتجلى هذا الاعتداء في إفشاء غير قانوني للبيانات الشخصية للمستهلك الإلكتروني، حيث يحتفظ الجاني بالبيانات الشخصية سواء بطرق قانونية، مثل تصنيفها أو معالجتها، أو بطرق

[1] بن عقون حمزة، السلوك الاجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجيستر في علم الاجرام وعلم العقاب، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2011-2012، ص103

غير قانونية عن طريق اختراق المواقع الإلكترونية، ومن ثم يكشف تلك البيانات الشخصية ومحتواها السري للجمهور عبر شبكة الإنترنت، مما يتيح لأي شخص الاطلاع عليها بشكل عام.[1]

ثالثا: التعرض لحرمة الحياة الخاصة:

مع تطور وسائل الاتصال واستخدام أجهزة الكمبيوتر في هذا المجال، يزداد تداول المعلومات عبر الشبكات بشكل متسارع. ورغم الفوائد والتحسينات التي أحدثها هذا التطور، إلا أنه ينطوي أيضًا على مساوئ، خاصة عندما يتعلق الأمر بمعلومات شخصية تتعلق بالمستهلك الإلكتروني. لقد بدأ الوعي بخطورة استخدام الكمبيوتر على خصوصية الحياة الشخصية في الدول الغربية منذ أكثر من ثلاثين عامًا، وارتفعت مطالب حماية الحياة الشخصية لمواجهة خطر معالجة البيانات الشخصية بشكل آلي. ومن بين أكثر الاعتداءات التي تتعرض لها الحياة الشخصية للمستهلك الإلكتروني، نجد معالجة البيانات الشخصية دون الحصول على ترخيص من الجهة المختصة، وهي اللجنة الوطنية للمعلوماتية. كما تشمل هذه الاعتداءات الانحراف عن الغرض الذي يؤدي إلى سوء استخدام تلك المعلومات، فضلاً عن تخزين بيانات شخصية يمكن أن يكون الكشف عنها مساسًا بالشرف والسمعة أو خصوصية الحياة الشخصية دون موافقة الشخص ذاته.[2]

الفرع الثالث: أوجه حماية البيانات الشخصية للمستهلك الالكتروني:

نظرًا للتأثير الخاص بالخصوصية في البيئة الافتراضية التي تتم فيها عقود التجارة الإلكترونية بين المستهلك الإلكتروني والمورد، فقد تم تبني وسائل فعالة لضمان حماية هذه البيانات الشخصية.تم توفير آليات متقدمة لحماية بيانات المستهلك الشخصية في البيئة الافتراضية للتجارة الإلكترونية. تشمل هذه الآليات:

[1] لعمريوي ليلى، مرجع سابق، ص44

[2] علي جبار الحسيناوي، جرائم الحاسوب والانترنات، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009، ص78.79

أولا: تقنية التأكد من شخصية المستخدم:

تقنية التحقق من الهوية والحماية الشخصية تستخدم آليات متنوعة مثل كلمات المرور، والبطاقات الذكية، وتقنيات التعرف البيولوجي للتأكد من هوية المستخدمين. تعتمد على أدوات ومميزات تكنولوجية متقدمة لضمان الأمان في الوصول إلى النظام أو الشبكة. تهدف إلى تحقيق حماية فعالة للبيانات الحساسة وضمان أن يكون الوصول مقتصرًا على الأشخاص المصرح لهم فقط. تحقق توازنًا بين الوصول السهل للنظام والحماية الشخصية للمستخدمين والبيانات. تعتبر كلمات المرور والبطاقات الذكية وتقنيات التعرف البيولوجي أدوات فعالة لتحقيق هذا التوازن وتوفير بيئة آمنة للمستخدمين والبيانات[1].

ثانيا: تقنية كشف مضاد الفيروسات

تعتبر تقنية مكافحة الفيروسات واحدة من أهم وسائل الأمان التقني، وهي تعتبر برنامجًا يتم استخدامه للوقاية والكشف والتخلص من البرمجيات الخبيثة، بما في ذلك الفيروسات وبرامج الاختراق غير المرغوب فيها التي تسبب أضرارًا على أجهزة الكمبيوتر. يهدف برنامج مكافحة الفيروسات إلى حماية الأنظمة والشبكات من التهديدات الإلكترونية، وذلك عن طريق التعرف على الأنماط السلوكية والتوقيعات المميزة للبرامج الضارة وتحليلها. يتم استخدام تقنيات متقدمة مثل التحليل السلوكي وتحليل الشفرات للكشف عن البرامج الضارة وإزالتها من الأنظمة. تعتبر تقنية مكافحة الفيروسات ضرورية للحفاظ على سلامة وأمان الأجهزة والبيانات، حيث تقوم بمراقبة الأنشطة الضارة ومنعها قبل أن تتسبب في أي ضرر. كما تتيح أدوات إزالة الفيروسات تنظيف الأجهزة وإصلاح التلف الناجم عن البرامج الضارة.[2]

[1] العمريوي ليلى، مرجع سابق، ص48

[2] لعمريوي ليلى، مرجع سابق، ص 48

المطلب الثاني

الحماية الجنائية لوسائل الدفع الخاصة بالمستهلك الالكتروني

ترتب التزامات قانونية متبادلة نتيجة عقود التجارة الإلكترونية التي تبرم بين المستهلك والمورد، وتتضمن هذه التزامات العديد من الجوانب، منها الالتزام بسداد قيمة السلع والخدمات المتفق عليها. يتم تحقيق ذلك من خلال استخدام وسائل الدفع الإلكترونية التي تتيح إمكانية تسوية قيمة السلع والخدمات عبر الإنترنت.

نص المشرع الجزائري على وسائل الدفع الالكتروني من خلال الأمر رقم 03-11 و المتعلق بالنقد و القرض و التي نصت على :" تعتبر وسائل الدفع كل الأدوات التي تمكن كل شخص من تحويل الأموال مهما يكن السند أو الأسلوب التقني المستعمل"[1]

تم تسجيل الاعتراف بوسائل الدفع الإلكتروني من قبل المشرع الجزائري، والتي تتيح للأفراد تحويل الأموال، ويتم الاحتفاظ بالباب مفتوحًا لاستيعاب وسائل دفع إلكترونية جديدة قد تظهر في المستقبل، مثل بطاقات الوفاء الإلكترونية، وتحويل الأموال الإلكتروني، والنقود الإلكترونية، والاعتماد المستندي الإلكتروني، والأوراق التجارية الإلكترونية، ،التوقيع الإلكتروني، وأي وسيلة دفع إلكترونية أخرى. وتعتبر وسائل الدفع الإلكتروني من بين التدابير والإجراءات الوقائية المعتمدة من قبل المشرع الجزائري لمكافحة التهريب، وهذا وفقًا للأمر رقم 05-06 الصادر في 23 أغسطس 2005 المتعلق بمكافحة التهريب.[2]

الفرع الأول : الحماية الجنائية لبطاقة الائتمان :

يشكل استخدام بطاقة الائتمان موضوعًا جديدًا في المجالين التجاري والقانوني، حيث يتطلب متابعة ورعاية كبيرة للتأكد من سلامة استخدامها. يتطلب إصدار بطاقة الائتمان حماية جنائية خاصة نظرًا لأهميتها وتأثيرها على الأفراد والجهات المعنية. المشرع الجزائري

---

[1] عمارة ليندة، افنان عبد الغاني، مرجع سابق، ص 27

[2] امر رقم 05-06، المؤرخ في 23-08-2005، المتعلق بمكافحة التهريب،ج.ر،عدد 59، الصادرة في 28-08-2005

قد أعطى تعريفًا لبطاقات الائتمان في المادة 543 مكرر 23 من القانون التجاري، حيث يعتبرها بطاقة الدفع التي تصدرها البنوك والمؤسسات المالية المؤهلة قانونًا وتسمح لحاملها بسحب الأموال أو تحويلها.[1]

يتضمن الجانب الفقهي لتعريف بطاقة الائتمان أنها "عقد يلتزم بموجبه مصدر البطاقة بفتح اعتماد بمبلغ محدد لصالح شخص آخر هو حامل البطاقة، ويمكن لحامل البطاقة الوفاء بمشترياته لدى المحلات التجارية التي ترتبط مع مصدر البطاقة بعقد يلتزم فيه بقبول وفاء حاملي البطاقات الصادرة عنه، على أن يتم التسوية النهائية في فترة زمنية محددة"[2]، وهناك أيضًا وجهات فقهية تعتبر بطاقة الائتمان نوعًا من النقود الإلكترونية[3]، وآراء أخرى تعتبرها آلية وكالة حيث يفوض حامل البطاقة البنك بدفع ثمن السلعة أو الخدمة التي يحصل عليها من حسابه المصرفي، وهناك أيضًا رأي يعتبرها أداة دفع تمتاز بخصوصيتها مثل الشيك[4].

لذلك، سنناقش الآن الحماية الجنائية لبطاقة الائتمان بالنسبة لحاملها وبالنسبة للآخرين.

أولا : الاستعمال غير المشروع لبطاقة الائتمان من قبل حاملها :

يتحقق الاستعمال غير المشروع لبطاقة الائتمان من قبل حاملها، بتجاوز رصيده المسموح به خلال فترة صلاحيتها بعد انتهاء مدة صلاحيتها أو إلغائها: يتسبب تجاوز حامل البطاقة الائتمانية للرصيد في حدوث مشكلة، حيث يقوم الحامل الشرعي للبطاقة خلال فترة صلاحيتها بالقيام بشراء سلع وخدمات على الرغم من علمه بأن رصيده في البنك لا يكفي لتغطية تلك المبالغ.[5]

---

[1] قانون رقم 05-02 المؤرخ في 06 فيفري 2005، المعدل والمتمم للأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون التجاري،ج.ر،عدد 11، المؤرخة في 09-02-2005

[2] جهاد رضا الحبشة، الحماية الجزائية لبطاقة الوفاء، دار اثقافة، عمان، 2008، ص23

[3] لعمريوي ليلى، مرجع سابق، ص50

[4] لعمريوي ليلى، مرجع سابق، ص50

[5] المرجع نفسه، ص50

عندما يقوم الحامل الشرعي للبطاقة بالاستخدام بعد إلغاء البطاقة أو انتهاء صلاحيتها، فإنه يرتكب جريمة استخدام غير مشروع لبطاقة الائتمان الملغاة. يعد ذلك انتهاكًا للشروط والقوانين المتعلقة بالاستخدام الصحيح لبطاقة الائتمان.

عندما يتم إلغاء البطاقة من قبل البنك المصدر نتيجة سوء استخدامها أو لأي سبب آخر، فإن العميل مطالب بإعادة البطاقة إلى البنك. يجب أن يلتزم العميل بهذا الإجراء وعدم استخدام البطاقة الملغاة. إذا استخدمت البطاقة الملغاة بعد إلغائها، يُعتبر ذلك مخالفة قانونية تعرض الحامل للمسائلة القانونية.[1] في حالة عدم امتثال الحامل للبطاقة الملغاة وعدم إعادتها للبنك، يعتبر ذلك اختلاسًا وجريمة خيانة الأمانة. يتم تنفيذ هذه الجريمة عن طريق إنكار الحامل لحيازته البطاقة ورفض تسليمها للبنك. وعند استخدام البطاقة الملغاة للدفع في عمليات تجارية، يصبح ذلك عملاً احتياليًا يعرف بجريمة النصب.[2]

عندما يقدم الحامل الملغاة إلى التاجر في عملية شراء، يهدف إلى التلاعب بالتاجر عن طريق استخدام بطاقة ائتمان غير صالحة وتقديمها بشكل مكرر للتجار الذين يعتقدون أن لديه رصيد كافٍ لإتمام الصفقة. وهذا يعد جريمة نصب لأن البطاقة الملغاة ليست لديها رصيد حقيقي، وبالتالي يتسبب في تحميل البنك مسؤولية تسديد قيمة السلع والخدمات للتاجر.[3]

ثانيا : الاستخدام غير المشروع لبطاقة الائتمان من قبل الغير :

يحدث الاستخدام غير القانوني لبطاقة الائتمان عندما يتم استخدامها بدون إذن من صاحب البطاقة أو من أي شخص آخر يمتلك الرصيد. ويحدث ذلك عادة في حالات سرقة البطاقة أو فقدانها، أو عند تزوير البطاقة.

لكي يتم تحقيق استخدام غير قانوني للبطاقة المسروقة أو المفقودة بواسطة الغير، يجب أن يتم إدخال الرقم السري أو الشفرة الخاصة بالبطاقة، وهي معلومات عادة ما يكون على

---

[1] جهاد رضا الحباشة،مرجع سابق، ص129

[2] لعمريوي ليلى، مرجع سابق، ص51

[3] جهاد رضا الحبشة، مرجع سابق، ص 129

علم بها فقط صاحب البطاقة الشرعي. بالتالي، لا يكفي فقط أن يحتوي الشخص على البطاقة بشكل غير قانوني ليتمكن من سحب النقود، بل يجب أن يكون لديه أيضًا الرمز السري أو الشفرة السرية المتعلقة بالبطاقة.[1]

في حالة استخدام بطاقة مسروقة أو مفقودة للوفاء بالمعاملات، غالبًا ما لا يتطلب الأمر معرفة الرقم السري للبطاقة. بدلاً من ذلك، يتم تنفيذ المعاملات عن طريق توقيع حامل البطاقة على فاتورة الشراء. وفي بعض الحالات، قد لا يكتشف البائع تزوير التوقيع بسبب عدم خبرته في هذا الأمر.[2]

ثالثا - تزوير بطاقة الائتمان

تزوير بطاقة الائتمان يُعَدُّ من بين أخطر أنواع التزوير في المجال الإلكتروني، وقد تباينت الآراء الفقهية بشأن تحميل المسؤولية الجنائية للمزورين والاحتيال على البطاقات الائتمانية. بين المؤيدين والمعارضين.

والرأي السائد بشأن تزوير بطاقة الائتمان هو أنه يعاقب عن جريمة استخدام بطاقة مزورة. حتى في حالة محاولة استخدام بطاقة مزورة أو مقلدة، حيث يتنكر الجاني باستخدام اسم وصفة غير صحيحة لحامل البطاقة الأصلي، بهدف الحصول على فوائد مادية. تعتمد هذه الجريمة على ثلاثة أركان، وهي: الركن القانوني والركن المادي، والركن الأخلاقي. حيث يتمثل الركن القانوني في فعل استخدام بطاقة مزورة أو مقلدة، ويتمثل الركن المادي في تحقق العملية الجنائية من خلال تنفيذ الفعل المحظور. ويتمثل الركن الأخلاقي في وجود النية العمدية لدى الجاني بمعرفة أن البطاقة التي يستخدمها هي مزورة أو مقلدة، وتوجه إرادته نحو ارتكاب هذا الفعل الجنائي.[3]

---

[1] لعمريوي ليلى، مرجع سابق، ص 51-52

[2] المرجع نفسه،ص 52

[3] لعمريوي ليلى، مرجع سابق، ص 52

الفرع الثاني: الحماية الجنائية للتوقيع الالكتروني:

لا يُعتبر الكتابة دليلاً كاملاً للإثبات إلا عندما يتم تزويدها بالتوقيع، الذي يُعد العنصر الثاني في عناصر الدليل الكتابي المعد للإثبات. يُنسب التوقيع إلى الشخص الذي قام بتوقيع الوثيقة، حتى لو كانت النص مكتوبًا بخط يختلف عن خطه. على الرغم من تزايد استخدام تقنيات الاتصال الحديثة في إبرام العقود عن بُعد، فإن التوقيع التقليدي يعتبر أحد أهم التحديات التي تعيق تلك العملية. يهدف ذلك إلى حل المشكلات القانونية التي تنشأ في مجال إثبات العقود الإلكترونية، والتي تظهر بشكل متزايد.[1]

مع تطور التكنولوجيا في وسائل الاتصال والمعلومات، أصبح التوقيع التقليدي غير مناسب للمعاملات الإلكترونية. ولهذا السبب، ظهر التوقيع الإلكتروني كأحد الوسائل الرئيسية في تنظيم الخدمات المصرفية الإلكترونية، حيث يعتمد على التوقيع الإلكتروني.[2]

أولا: تعريف التوقيع الالكتروني:

يمكن أن نعرف التوقيع الالكتروني بأنه " كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع و مرتبطا ارتباطا وثيقا بالتصرف القانوني و يسمح بتميز صاحبها و تحديد هويته و يتم دون غموض عن رضائه بهذا التصرف " القانوني[3]

أثناء تعديل القانون المدني في الجزائر بواسطة القانون رقم 05/10 الصادر في 20 - 06 - 2005، كان من الضروري على المشرع الجزائري تضمين تعريف للتوقيع الإلكتروني بعد تعريف الكتابة الإلكترونية. وبالرجوع إلى الفقرة الثانية من المادة 327 من ذات القانون نجدها قد نصت على أنه " يعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر 1 و هي الشروط المتعلقة بإمكانية التأكد من هوية الشخص الذي أصدرها و أن تكون

---

[1] بن سعيد لزهر، النظام القانوني لعقود التجارة الالكترونية، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014، ص152

[2] افنان عبد الغني، عماري ليندة، الحماية الجنائية للمستهلك الالكتروني، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي وعلوم جنائية، جامعة عبد الرحمان ميرة، بجاية، 2021-2022، ص30

[3] ثروت عبد الحميّد، التوقّيع الاكترونيً، دار الاسكندرية، مصر، ،2007 ص50.

معدة ومحفوظة في ظروف تضمن سلامتها "[1]، و هو ما يعني مساواة حجيته للتوقيع الالكتروني. يمكن الاستنتاج من المعلومات التي تم ذكرها أن المشرع الجزائري قد أقر بشكل صريح واعترف بالتوقيع الإلكتروني وجعله متساويًا في جميع جوانبه للتوقيع الكتابي. ولضمان صحة التوقيع الإلكتروني، فإن المشرع اشترط استخدام وسيلة موثوقة تمكن من التعرف على هوية صاحب التوقيع وتضمن صلته القانونية بالتصرف الذي يتم إجراؤه. هذا يعني أنه يجب أن يتوفر وسيلة تحقق الأمان والمصداقية للتوقيع الإلكتروني، مما يضمن أن يكون له نفس القوة القانونية والتأثير القانوني مثل التوقيع الكتابي التقليدي. فتحت الفقرة الأخيرة من المادة 327 الباب أمام المشرع الجزائري للخوض في مسألة تنظيم التوقيع الالكتروني، وذلك بموجب المادة 3 من المرسوم التنفيذي رقم07 - 162 الصادر بتاريخ 30 05 -،2007. نضمنت الفقرة الثانية من نفس المادة مجموعة من الشروط الواجب توافرها في التوقيع الإلكتروني المؤمن. ومن بين هذه الشروط، يجب أن يكون شخصيا أي خاصا بالموقع و اتصال التوقيع بالمحدد. كما يجب أن يتمكن من كشف وتحديد أي تعديل يمكن أن يطرأ على التوقيع الإلكتروني بعد إجراء التوقيع نفسه. بالإضافة إلى ذلك، ينبغي أن يكون التوقيع ذو صلة مباشرة بالعمل المرتبط به، حيث يجب أن يكون أي تعديل غير مشروع قابلًا للاكتشاف والكشف عنه.[2]

حددت الفقرة الثانية من ذات المادة شروط التوقيع االالكترونًي المؤمن، وهًي أن يكون شخصًيا أي خاصا بالموقع، و اتصال التوقيع بالمحدد، و إمكانية كشف و معرفة أي تغيير قد يحصل للتوقيع الالكتروني بعد وضع هذا التوقيع، وأن يتضمن مع العمل المرتبط به صلة بحيث يكون كل تعديل لاحق للفعل قابلا للكشف عنه[3]

---

[1]امر رقم ،75-58 مؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، من القانون المدني،ج.ر، عدد78 ،صادر في 24 رمضان 1935 الموافق ل 30 سبتمبر ،1975 معدل و متمم

[2] مرسوم تنفّذي رقم ،162/07 المؤرخ في ،2007/05/30 يعدل و يتمم المرسوم التنفّذي رقم 01-123 المؤرخ في،2001/05/09 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فّها الاسلاك الكهربائية و على مختلف المواصلات السلكية و اللاسيكية، ج.ر، عدد ،37 الصادرة بتارّخ ،2007/06/07 ص.12

[3] قطاف إسماعيل، العقود الإلكترونية و حماية المستهلك، بحث لنيل شهادة الماجّستر، فرع عقود و مسؤولّية، كلّية الحقوق، جامعة الجزائر، الجزائر، ،2006/2005 ، ص36

ثانيا : صور التوقيع الالكتروني :

تتوفر أشكال متعددة للتوقيع الإلكتروني، وتختلف هذه الأشكال وفقًا للوسيلة أو التقنية المستخدمة. ومن الجدير بالذكر أن القوانين التي تنظم التوقيع الإلكتروني عادةً لا تحدد شكلًا محددًا له. وفيما يلي يمكن ذكر بعض الأشكال المشتركة للتوقيع الإلكتروني:

1- التوقيع البيومتري :

بواسطة التوقيع البيومتري، يتم استخدام الخواص الذاتية للشخص للتحقق من هويته[1]. يعتمد هذا النوع من التوقيع على خصائص فيزيائية وطبيعية فردية، بالإضافة إلى سلوك الأفراد. ويمكن استخدام طرق مختلفة للتوقيع البيومتري، مثل[2]:

التوقيع بالعين: حيث يتم التحقق من هوية الشخص باستخدام صورة دقيقة للعين البشرية. يتم تحليل ملامح العين، مثل القزحية والشبكية، ومقارنتها مع البيانات المخزنة مسبقًا للتحقق من الشخصية. التوقيع ببصمة الأصابع: يستخدم هذا النوع من التوقيع بصمة الأصابع للتحقق من هوية الشخص. تُلتقط صورة عالية الدقة لبصمة الأصابع وتخزن في قاعدة البيانات، ثم يتم استخدامها للتحقق من الشخص في المرات اللاحقة. التوقيع بملامح الوجه: يعتمد هذا النوع من التوقيع على تحليل ملامح الوجه الفريدة للشخص. يتم استخدام تقنيات التعرف على الوجه لاستخراج معالم وملامح الوجه وتخزينها لاستخدامها في التحقق من الشخص فيما بعد. تخزن البيانات الخاصة بالتوقيع البيومتري في الحاسوب، ويتم استرجاعها عند الحاجة للتحقق من شخصية الفرد والسماح له بالدخول إلى نظام الحاسوب.

2 التوقيع باستخدام القلم الالكتروني :

بواسطة التوقيع باستخدام القلم الإلكتروني، يتم نقل التوقيع الإلكتروني المكتوب بخط اليد إلى الملف المراد نقله عن طريق المحرر. يتم ذلك باستخدام الماسح الضوئي، المعروف

---

[1] فادي محمد عماد الديّن توكل، عقد التجارة الالكترونّية، منشورات حلبً الحقوقّية، لبنان، ،2010 ص161-162

[2] شين صالح، الحماية الجنائية للتجارة الالكترونية،رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة ابي بكر بلقايد، تلمسان، 2012،ص132

أيضًا باسم "السكانر"[1]، الذي يقوم بتحويل المستند المكتوب إلى صورة رقمية. عند استخدام القلم الإلكتروني، يمكن للشخص كتابة توقيعه على سطح خاص يتعرف على الضغط والحركة، وتُحفظ البيانات الخاصة بهذا التوقيع. ثم يتم استخدام الماسح الضوئي لالتقاط الصورة الرقمية للتوقيع وتحويلها إلى ملف إلكتروني. بعد ذلك، يتم نقل الملف الذي يحتوي على التوقيع الإلكتروني عبر الإنترنت إلى الشخص الآخر الذي يحتاج إلى رؤية التوقيع. يمكن أن يتم إرسال الملف عبر البريد الإلكتروني أو تحميله على منصة مشتركة أو استخدام أي وسيلة للتواصل عبر الإنترنت. باستلام الملف الذي يحتوي على التوقيع الإلكتروني، يمكن للشخص الآخر التحقق من صحة وأصالة التوقيع واستخدامه كما يلزم[2].

3 - البصمة الالكترونية :

على هذا الحساب، يجب أن يتم التحقق من الخصائص الكيميائية والطبيعية للأفراد قبل السماح لهم بالدخول إلى الحاسوب واستخدام المعلومات والبيانات الموجودة فيه. يتم استخدام خصائص مثل بصمة الأصابع، وخواص اليد البشرية، ونبرة الصوت، والتوقيع الشخصي، وخصائص العين للتحقق من هوية الأفراد.[3] في كل حالة، يتم تخزين بيانات الخصائص الفردية في الحاسوب الآلي، وعند الحاجة إلى الدخول إلى النظام، يتم مقارنة البيانات التي يقدمها الشخص مع تلك المخزنة في الحاسوب. إذا تم العثور على اتفاق بينهما، يسمح للشخص بالدخول واستخدام المعلومات. أما إذا وجد اختلاف بين البيانات المقدمة والبيانات المخزنة، فلا يُسمح للشخص بالدخول إلى النظام. هذا النوع من التوقيع يعزز الأمان والحماية، حيث لا يمكن لأي شخص عادي الدخول إلى الحاسوب واستخدام المعلومات الموجودة فيه إلا إذا تم التحقق من مطابقته للبيانات المخزنة، سواء كانت بصمة الأصابع أو خواص اليد البشرية أو نبرة الصوت أو التوقيع الشخصي أو خواص العين.

---

[1] قطاف حمزة، مرجع سابق، ص37

[2] بن سعيد لزهر، مرجع سابق، ص .158

[3] منيرمحمد الحنبيهي ، ممدوح محمد الحنبيهي ، جرايم الأنترنت و الحاسب آلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، ،2005، ص195

4- التوقيع المفتاحي :

تقنية التوقيع المفتاحي توفر وثيقة إلكترونية مزودة بتوقيع مشفر فريد يحدد هوية الشخص الذي قام بتوقيع الوثيقة والوقت الذي تم فيه التوقيع. يتم أيضًا استخراج معلومات حول صاحب التوقيع من هذا التوقيع الرقمي. وتُسجِّل التوقيع الرقمي بشكل رسمي عند جهات تسمى "سلطات التصديق"، ومهمتها التحقق من صحة وملكية التوقيع الرقمي للأشخاص الذين يقومون بتوقيع الوثائق الإلكترونية.[1]

عندما يتم فحص الوثيقة الإلكترونية التي تحتوي على التوقيع الرقمي، يمكن للجهات المختصة التحقق من سلامة وصحة التوقيع وملكيته باستخدام الشهادة الرقمية. السلطات المعترف بها، مثل سلطات التصديق، تقوم بإصدار الشهادات الرقمية للأشخاص بعد التحقق من هويتهم وصحة التوقيع الرقمي الخاص بهم.[2]

بهذه الطريقة، يتم ضمان صحة ومصداقية التوقيع الرقمي، ويتم تسجيله رسميًا لضمان الأمان وملكية التوقيع على الوثائق الإلكترونية.

ثالثا : وظيفة التوقيع الالكتروني :

التوقيع الإلكتروني أو الرقمي يُعَد رموزًا وأرقامًا تساهم في تحديد هوية الشخص الذي يصدر هذا التوقيع. يتم تمثيله على شاشة الحاسوب على شكل صورة، ولا يشبه توقيعًا واقعيًا بواسطة قلم على ورقة تُختم بعد ذلك بالحبر وتترك أثرًا ماديًا. إنه تشكيلة جديدة من أشكال التوقيع نشأت نتيجة استخدام الوسائط الإلكترونية في إجراء المعاملات عبر الحاسوب.[3]بهذه الطريقة، يعزز التوقيع الإلكتروني مصداقية وحجية التوقيع، ويسمح بالتحقق الفوري من

[1] منيرمحمد الحنبيهي ، ممدوح محمد الحنبيهي، مرجع سابق، ص 196

[2] قطاف حمزة، مرجع سابق، ص38

[3] عرب يونس، جرائم الكمبيوتر والانترنات، منشورات اتحاد المصارف العربية، النادي العربي لتقنية المعلومات والاعلام، 2001، ص176

صحة هوية صاحب التوقيع عند استخدام الرمز السري أو المفتاح الخاص، وهذا يجعله أكثر كفاءة وسهولة في الاستخدام مقارنة بالتوقيعات المكتوبة بخط اليد.[1]

ينص المشرع الجزائري على أن الإثبات في الشكل الإلكتروني يتمتع بنفس قوة الإثبات للكتابة على الورقة. يُشترط أن يكون من الممكن التحقق من هوية الشخص الذي أصدر الوثيقة الإلكترونية، وأن تُعد وتُحفظ في ظروف تضمن سلامتها. يُنص على ذلك في المادة 323 المكرر 1 من القانون المدني الجزائري.[2]

رابعا: جريمة تزوير التوقيع الالكتروني :

صحيح أن المشرع الجزائري لم ينص صراحة على جريمة التزوير المعلوماتي في القوانين الخاصة بالتوقيع الإلكتروني. ومع ذلك، يمكن الاستدلال على جريمة التزوير المعلوماتي من خلال بعض المواد في قانون العقوبات الجزائري.

تنص المادة 197 مكرر على جريمة التزوير، حيث يعاقب أي شخص يقوم بتغيير الحقيقة في وثيقة رسمية أو خاصة بطرق مادية أو معنوية بهدف تحقيق ضرر.

بالإضافة، المادة 253 مكرر تتعامل مع جريمة التوقيع الإلكتروني، حيث يعاقب أي شخص يستخدم التوقيع الإلكتروني بقصد جنائي عام واستعماله في أغراض محظورة، على الرغم من عدم ذكر تفصيلات واضحة حول جريمة التزوير المعلوماتي الإلكتروني. بالتالي، يمكن استنتاج أنه في حالة قيام شخص بتغيير الحقيقة في بيانات التوقيع الإلكتروني أو استخدام لتوقيع الإلكتروني بقصد جنائي أو لأغراض محظورة، يمكن اعتبار ذلك تزويرًا معلوماتيًا ومعاقبته وفقًا للمادتين المذكورتين وغيرها من الأحكام الجزائية ذات الصلة.[3]

---

[1] مخلوفي عبد الوهاب، مرجع سابق، ص 206

[2] أمر رقم 75-58، مؤرخ في 20 رمضان عام 1935 الموافق ل 26 سبتمبر 1975 يتضمن القانون المدني، المعدل والمتمم بالأمر رقم 05-10 المؤرخ في 20 يونيو 2005

[3] لعمريوي ليلى، مرجع سابق ، ص 57

الفصل الثاني

الحماية الإجرائية للمستهلك الالكتروني

الفصل الثاني

الحماية الإجرائية للمستهلك الالكتروني

قدّمت السلطات التشريعية الجزائرية حماية قانونية للمستهلك الإلكتروني للحدّ من جرائم الغش والتدليس التي قد تؤثر سلبًا على مصالحه المادية والمعنوية. وأُلحق بهذا الدور الوقائي مجموعة من ضباط الشرطة القضائية وأعضاء آخرين مرخص لهم بموجب تشريعات خاصة، فضلاً عن وجود جهاز مكافحة الغش الذي تم تنصيبه بموجب قانون رقم 09/03 الخاص بحماية المستهلك ومكافحة الغش.

ومنحت السلطات التشريعية الجزائرية القضاء سلطة متابعة جرائم تعرض المستهلك الإلكتروني لها، نظرًا لأنه يُعتبر الجهة المختصة في متابعة جميع انتهاكات القانون بصفة عامة، نظرًا لطبيعة هذه الجرائم المرتبطة بأجهزة الكمبيوتر، حيث تتميز بأساليبها الحديثة وسرعة تنفيذها وحذف أثرها بسرعة. تستدعي هذه الخصائص العامة معرفة شاملة بأنظمة الكمبيوتر وأساليب ارتكاب الجرائم المتعلقة بها أو التي تستخدمها، بالإضافة إلى قدرة تتيح الكشف عن غموض هذه الجرائم وسرعة التعامل معها، سواء في كشفها أو حجز الأدوات المستخدمة في ارتكابها أو الاحتفاظ بالبيانات أو الأجهزة التي تعد مصدرًا للجريمة.

تتزايد أهمية هذه الحماية الإجرائية في مواجهة مجموعة متنوعة من الجرائم التي تهدد مصالح المستهلك الإلكتروني المادية والمعنوية، مما دفع السلطات التشريعية إلى سعيها لتوفير حماية جنائية إجرائية للمستهلك الإلكتروني بهدف مكافحة هذه الجرائم المؤذية لمصالحه.

سنناقش هذا الموضوع في هذا الفصل، حيث قمنا بتقسيمه إلى مبحثين. في المبحث الأول، سنتطرق إلى الإجراءات القضائية التي يتم اتخاذها لحماية المستهلك الإلكتروني. أما في المبحث الثاني، سنتناول إثبات الجرائم التي يتعرض لها المستهلك الإلكتروني.

المبحث الأول

الحماية الجنائية الاجرائية للمستهلك الالكتروني

تطورت جرائم الحاسوب بشكل كبير في السنوات الأخيرة، وأصبحت أكثر تعقيدًا وتطورًا في أساليب ارتكابها. لذا، فإن جهات التحقيق والتحري والمحاكم يجب أن تكون ملمة بمستوى عالٍ من المعرفة في مجال أنظمة الحاسوب وأساليب ارتكاب هذه الجرائم.

أحد التحديات الرئيسية في التحقيق في جرائم الحاسوب هو تحديد الجريمة ذاتها وجمع الأدلة الرقمية اللازمة لإثباتها. قد تتطلب هذه العملية فهمًا عميقًا لأنظمة التشغيل وبرامج التشفير والشبكات والبرمجة والأمان السيبراني. لذلك، يتعين على الجهات ذوات الاختصاص أن يكونوا ملمين بأحدث التطورات التكنولوجية والأدوات المستخدمة في ارتكاب الجرائم الإلكترونية.

علاوة على ذلك، يجب أن تتمتع هذه الجهات بالقدرة على كشف الغموض المحيط بجرائم الحاسوب وتحليل البيانات الرقمية بشكل سريع وفعال. يمكن أن تكون المعرفة بتقنيات استرداد البيانات المحذوفة وتحليل سجلات النشاط وتتبع الشبكات مفيدة جدًا في هذا الصدد.

علاوة على ذلك، يجب على جهات التحقيق والتحري والمحاكم أن تتبنى إجراءات وسياسات فعالة لضبط الأدوات والأجهزة التي تم استخدامها في ارتكاب الجرائم. يتعين أيضًا عليهم القدرة على الاحتفاظ بالبيانات ذات الصلة والأجهزة التي قد تكون دليلاً ماديًا على الجريمة أو تحتوي على أدلة قيمة.

باختصار، تواجه جرائم الحاسوب تحديات فريدة تتطلب مستوى عالٍ من الخبرة والمعرفة فهناك إجراءات سابقة للمحاكمة (مطلب أول) و إجراءات لاحقة للمحاكمة (مطلب الثاني).

المطلب الأول

الإجراءات قبل مرحلة المحاكمة

تُعنى بالإجراءات الجنائية السابقة لمرحلة المحاكمة تلك التي وضعها المشرع الجزائري وتتم في مرحلة جمع الأدلة والتحقيق قبل إحالة المتهم للمحاكمة[1]. تشمل هذه الإجراءات:

تواجه أجهزة الضبط القضائي صعوبات وتحديات في مكافحة الجرائم الإلكترونية، ويعود ذلك إلى قلة خبرتهم في هذا المجال. هذا الواقع دفع العديد من الدول الأجنبية وبعض الدول العربية إلى إنشاء هيئات قضائية متخصصة في مجال الجرائم المعلوماتية، وتم تخويلها صلاحيات وسلطات عادية واستثنائية، وتشمل ذلك جرائم التجارة الإلكترونية. بالإضافة إلى ذلك، تم إنشاء منظمة الأنتربول على المستوى الدولي بهدف مكافحة الجرائم الإلكترونية وتعزيز التعاون الدولي في هذا الصدد. ، وعليه يمكن القول أن مرحلة قبل المحاكمة تمر بمرحلتين أساسية

مرحلة البحث والتحري (فرع أول) و مرحلة من خلال الضبطية القضائية بمكافحة جرائم التجارة الالكترونية التحقيق الابتدائي (فرع ثاني).

الفرع الأول : في مرحلة البحث والتحري :

يمنح القانون لأجهزة الضبط القضائي صلاحية البحث والتحقيق الأولي، المعروفة أيضًا بمرحلة جمع الأدلة. ويُمنح لهم مجموعة متنوعة من الاختصاصات والسلطات لتنفيذ هذه المهمة. يقوم أعضاء الضبط القضائي بدور فعال في جمع أدلة الجريمة وتحديد الجاني، بهدف مساعدة أجهزة التحقيق القضائي في الوصول إلى أدلة الجريمة وتحديد المشتبه به. يهدف ذلك إلى تمكين عملية العدالة وضمان توفير الأدلة اللازمة لإثبات التهم وإحالة

[1] عبد الله ماجد العكايلة، الوجيز في الضبطّية القضائية، دار الثقافة للنشر و التوزّيع، ألاردن، ،2010 ، ص 85

القضية للمحاكمة.[1] لذلك تطلب الأمر إنشاء ضبطية قضائية متخصصة في الجرائم المعلوماتية (أولا) وتخويلها اختصاصات و سلطات (ثانيا).

أولا : تحديد الضبطية القضائية المختصة بانتشار جرائم الانترنت:

تبذل الدول جهودًا كبيرة لمواجهة جرائم الإنترنت بمختلف الطرق المتاحة، ومنها إنشاء هيئات متخصصة، بما في ذلك إنشاء شرطة متخصصة على المستوى الوطني والدولي. تحث الاتفاقية الأوروبية لجرائم الإنترنت على هذا الإجراء، وتشجع على تأسيس وحدات شرطة متخصصة في مكافحة جرائم الإنترنت. بالإضافة إلى ذلك، ناقش المؤتمر الذي عقد في باريس بتاريخ 19 يناير 2005 بعنوان "الشرطة والإنترنت"[2] على المستوى الوطني والدولي" سبل تعزيز التعاون في هذا المجال ودور الشرطة في مكافحة جرائم الإنترنت.

1 على المستوى الوطني :

تم إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها في الجزائر بموجب القانون رقم 09-04. يهدف هذا القانون إلى تعزيز الوقاية من جرائم الاتصال والمعلومات ومكافحتها، ويعد استجابة للتطورات السريعة في مجال التكنولوجيا والاتصالات.

وفقًا لمواد القانون 13 و 14، يتم تحديد اختصاصات وصلاحيات الهيئة الوطنية. تعمل الهيئة على مكافحة جرائم تكنولوجيا الإعلام والاتصال، مثل الاحتيال الإلكتروني، وتعاون مع الجهات الأخرى ذات العلاقة لمكافحة جرائم الإنترنت والاعتداءات على الأمان السيبراني.[3]

---

[1] شنين صالح، الحماية الجنائية للتجارة الإلكترونية(دراسة مقارنة)، رسالة لنيل شهادة دكتوراه في القانون الخاص، كلّة الحقوق، جامعة أبو بكر بلقايد، تلمسان، ،2013/2012، ص.214

[2] شنين صالح، نفس المرجع، 214

[3] قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها، ج.ر،عدد45،صادر في 25 شعبان1430الموافق ل16غشت2009.

تشمل اختصاصات الهيئة الوطنية توفير التوعية والتثقيف للمجتمع بشأن أخطار جرائم تكنولوجيا الإعلام والاتصال، وتشجيع استخدام تكنولوجيا المعلومات بشكل آمن ومسؤول. كما تقوم الهيئة بالتحقيق في الجرائم التكنولوجية وجمع الأدلة، وتنفيذ إجراءات الضبط القضائي وتقديم المساعدة الفنية للجهات القضائية.

وبصفة عامة، يهدف إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحتها إلى تعزيز الأمن الإلكتروني والحماية السيبرانية في الجزائر، والحد من التهديدات والجرائم التي ترتبط بالتكنولوجيا والاتصالات.[1]

تتولى الهيئة المشار إليها وفقًا للمادة 14 من القانون المذكور تعزيز وتنسيق جهود الوقاية من جرائم الاتصال والمعلومات ومكافحتها، وتقديم الدعم للسلطات القضائية وأجهزة الشرطة القضائية في التحقيقات المتعلقة بهذه الجرائم. تشمل مهامها جمع المعلومات وتوفير الخبرات القضائية، وكذلك تبادل المعلومات مع هيئات مماثلة في الخارج بهدف تجميع جميع البيانات المفيدة لتحديد هوية المتهمين ومكان تواجدهم في جرائم تكنولوجيا الإعلام والاتصال.

استجابةً للتطور التكنولوجي وزيادة جرائم الإنترنت، قامت الجزائر بإنشاء مركز لمكافحة جرائم الإنترنت ضمن إطار الدرك الوطني. يهدف هذا المركز إلى التصدي لمختلف أشكال جرائم الإنترنت التي تشكل تهديدًا للأمن السيبراني والمجتمع بشكل عام.

يعمل المركز على عدة جوانب في مجال مكافحة جرائم الإنترنت. أولاً، يقوم بجمع المعلومات والاستخبارات المتعلقة بالتهديدات الرقمية وجرائم الإنترنت. ثم، يقوم بتحليل هذه البيانات وتقييمها لفهم الأنماط والاتجاهات وتحديد الأهداف المحتملة للجرائم الإلكترونية.

بالإضافة إلى ذلك، يعمل المركز على التحقيق في الجرائم الإلكترونية ومتابعة المشتبه بهم والمجرمين الذين يقومون بأعمال غير قانونية عبر الإنترنت. يستخدم المركز التقنيات

[1] انظر المواد 13و14 من القانون 09-04 المتعلق بالوقاية من جرائم الاتصال والمعلومات ومكافحتها، مرجع سابق

المتقدمة والأدوات المتخصصة لجمع الأدلة الرقمية وتحليلها لتقديمها كدليل قانوني في المحاكم.

علاوة على ذلك، يقوم المركز بتطوير استراتيجيات وسياسات متقدمة لمكافحة جرائم الإنترنت وتعزيز الأمن السيبراني. يعمل المركز على التعاون مع الجهات المعنية الأخرى، مثل الشرطة والأجهزة الأمنية والمؤسسات الحكومية والقطاع الخاص، لتعزيز التعاون وتبادل المعلومات في مجال مكافحة جرائم الإنترنت.

بالإضافة إلى مهامه التحقيقية والتطبيقية، يلعب المركز دورًا هامًا في توعية الجمهور وتثقيفه حول آفاق التهديدات الرقمية وكيفية حماية أنفسهم منها. يقوم المركز بتوفير المشورة والتوجيه والموارد للمجتمع بشأن استخدام الإنترنت بطرق آمنة والتصدي للمخاطر السيبرانية.

باختصار، يعد إنشاء مركز مكافحة جرائم الإنترنت في الجزائر استجابة حكومية هامة لتزايد التهديدات السيبرانية، ويهدف إلى ضمان الأمن الإلكتروني وحماية المجتمع من جرائم الإنترنت.[1]

2 على المستوى الدولي :

في ظل تصاعد جرائم الإنترنت وتأثيرها العابر للحدود، أصبح التعاون الدولي أمرًا ضروريًا لمكافحة هذه الجرائم. لم يعد التعاون يُنظر إليه كخرق لسيادة الدول، بل يُعتبر اليوم وسيلة فعالة لتعزيز الأمن السيبراني ومكافحة جرائم الإنترنت.

تعد "المنظمة الدولية للشرطة الجنائية"، المعروفة أيضًا باسم الأنتربول، من بين الهيئات المكلفة بمكافحة الجريمة العابرة للحدود. تأسست الأنتربول بهدف تعزيز التعاون الدولي في مكافحة الجريمة وتبادل المعلومات بين الجهات الأمنية في مختلف دول العالم.

تتمتع الأنتربول بشبكة واسعة من الأعضاء، حيث تشارك فيها الدول الأعضاء بالمعلومات الجنائية والاستخباراتية المتعلقة بجرائم الإنترنت وغيرها من أشكال الجريمة العابرة للحدود.

[1] انظر المواد 13و14 من القانون 09-04 المتعلق بالوقاية من جرائم الاتصال والمعلومات ومكافحتها ،نفس المرجع

تعمل الأنتربول على تحليل المعلومات وتوفير الدعم والتعاون الفني للدول الأعضاء لمكافحة الجرائم الإلكترونية.[1]

تعتبر حالة التعاون الناجحة بين الأنتربول والمباحث الفيدرالية الأمريكية والشرطة الإنجليزية في عام 1998 من الإنجازات الملموسة للمنظمة الدولية للشرطة الجنائية. في تلك الحالة، تم التعاون بين هذه الجهات المختلفة للكشف وتفكيك موقع إلكتروني يحتوي على أكثر من 75,000 صورة سلبية تتعلق بدعارة الأطفال. تم تبادل المعلومات والاستخبارات والتنسيق القوي بين الجهات المشاركة، بما في ذلك الأنتربول، وتم تنفيذ عملية ناجحة للقبض على الجناة وتفكيك الشبكة الإجرامية. بالإضافة إلى ذلك، في نفس الوقت، تم القبض على شاب ألماني يواجه تهمة توزيع فيروس معين، وذلك بفضل التعاون المشترك بين الأنتربول والمباحث الفيدرالية الأمريكية والشرطة الألمانية. تم تبادل المعلومات والمساعدة المتبادلة لتحديد هويته وتحقيق الاعتقال.

هذه الحالتين تبرز أهمية التعاون الدولي في مجال مكافحة جرائم الإنترنت وتبادل المعلومات والاستخبارات الجنائية بين الجهات الأمنية المختلفة. من خلال تعزيز التعاون المشترك، يصبح من الممكن الكشف عن الجرائم وتقديم الجناة للعدالة بفاعلية أكبر.[2]

المؤتمرات والملتقيات الدولية التي تجمع منظمات دولية وعددًا من الدول تلعب دورًا هامًا في تعزيز أمن التكنولوجيا والمعلومات على المستوى الدولي. تهدف هذه المؤتمرات إلى تبادل المعلومات والخبرات وتطوير السياسات لضمان سلامة وأمان التكنولوجيا والمعلومات في ظل التحديات السيبرانية المتزايدة.

منظمة التعاون الاقتصادي والتنمية (OECD) هي إحدى المنظمات الدولية التي تعمل في هذا المجال. تجمع الOECD بين دول أعضاء من مختلف أنحاء العالم، بما في ذلك مصر والصين وغيرها، وتهدف إلى تعزيز التعاون والتنسيق بين الدول في مجال سياسات

[1] امين عبد الحميد، استراتيجية مكافحة جرائم الحاسوب الالي، دراسة مقارنة،رسالة لنيل شهادة الدكتورته، اكاديمية الشرطة،2012، ص455

[2] صالح شنين ، مرجع سابق، ص223

التكنولوجيا والمعلومات. تساهم OECD في تطوير مبادئ وإرشادات ومعايير حول أمن التكنولوجيا والمعلومات، وتوفير منصة للتبادل الدولي للممارسات الجيدة.

مجموعة الثمانية الاقتصادية (G8)، التي تتألف من الدول الصناعية المتقدمة، تعقد أيضًا مؤتمرات وقمم تتناول قضايا أمن التكنولوجيا والمعلومات. تجمع هذه القمم قادة الدول الأعضاء في G8 لبحث القضايا الهامة، بما في ذلك الأمن السيبراني والتهديدات الرقمية. يتم تبادل الآراء والمعلومات والتجارب المختلفة لتعزيز قدرة الدول على مواجهة التحديات التكنولوجية.

باختصار، هذه المؤتمرات والملتقيات الدولية تلعب دورًا حاسمًا في توحيد جهود الدول والمنظمات الدولية في مكافحة جرائم التكنولوجيا والمعلومات، وتطوير إطار عالمي للتعاون والتنسيق في هذا الصدد.[1]

بالإضافة إلى الأنتربول، هناك مكاتب متخصصة في مجال مكافحة جرائم الإنترنت على المستوى الأوروبي. يوجد مركز الشرطة الأوروبية المعروف بـ "الأريول"، وكذلك "الأورجست"، وهما جهات تساعد في التعاون القضائي والشرطي لمواجهة ومكافحة جميع أنواع الجرائم الخطيرة، بما في ذلك جرائم الانترنات.[2]

ثانيا : إختصاصات الضبطية القضائية :

يتمتع اعضاء الضبط القضائي بنطاق واسع من الصلاحيات التي تمكنهم من القيام بتحقيقات وتحريات حول الجرائم ومرتكبيها. يقوم أعضاء الضبط القضائي بتنفيذ إجراءات تحقيق اعتيادية، بالإضافة إلى بعض الإجراءات الاستثنائية.

[1] صالح شنين، نفس المرجع، 224ص

[2] محمد فتحي عيد،الانترنات ودوره في انتشار المخذرات،اكاديمية نايف العربية للعلوم الامنية، الرياض، 2003، ص202

1- اختصاصات شرطة الانترنت في الظروف العادية :

يقصد بالظروف العادية الظروف التي يتلقى فيه عضو الضبط القضائي الشكوى عن وقوع الجريمة وعليه يقوم بالتحريات و جمع الأدلة

تُمثِّل اختصاصات الضبطية القضائية في الظروف العادية، وفقًا لنصوص المادة 17 و 18 من قانون الإجراءات الجزائية الجزائري، استقبال البلاغات والشكاوى، سواء كانت شفهية أو كتابية، بغض النظر عما إذا كانت تتعلق بوقوع جريمة أو تهديد بها، وسواء تم ذلك بالطرق التقليدية أو الرقمية، والتي تشمل إرسال رسالة إلكترونية إلى البريد الإلكتروني المختص للجهات المعنية بالتحقيق والتحري. وعند استلام عضو الضبط القضائي أي بلاغ، سواء كان ذلك يتعلق بوجود مواقع أو صفحات خادعة مصممة للاحتيال على المستهلكين، يقوم بتسجيل البلاغ وتقديمه لضباط الشرطة وقضاة التحقيق والمحققين، وتزويدهم بالمعلومات المتوفرة وضبط المرتكبين وتسليمهم إلى السلطات المختصة. ويقوم أيضًا بالمراقبة الإلكترونية كأداة لجمع البيانات والمعلومات حول المشتبه بهم[1] ، دون المساس بأحكام تقديم الشكاوى في بعض الجرائم التي يتطلب القانون تقديم شكوى من قبل المجني عليه أو وكيله. وبالإضافة إلى هذه المهام، يقوم الضبط القضائي بجمع المعلومات التي تقيد التحقيق، حيث يقوم المحقق بإجراء مجموعة من الإجراءات باستخدام التقنية الرقمية الإلكترونية للحصول على معلومات إضافية حول الأشخاص أو الأماكن. وتُعد المراقبة الإلكترونية أيضًا وسيلة أخرى لجمع البيانات والمعلومات حول المشتبه بهم، ويقوم عضو الضبط القضائي، الذي يتمتع بكفاءة تقنية عالية، بمراقبة شخص معين قد قام باختراقجهاز الحاسوب الخاص بالمجني عليه، أو بإعداد صندوق بريد إلكتروني مزيف للمراقبة عند إرساله للمشتبه به.[2]

---

[1] نبيلة هبة هروال، جرائم الانترنات دراسة مقارنة، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، 2013-2014،ص 197

[2] نبيلة هبة هروال ،مرجع سابق،ص 197

2- اختصاصات شرطة الانترنت في الظروف الاستثنائية :

عضو الضبط القضائي يتولى مسؤوليات إضافية في ظروف استثنائية، حيث يتمكن من اتخاذ بعض إجراءات التحقيق في حالة الجريمة المتلبس بها. يشمل ذلك القبض على المتهم وتفتيشه وفقًا للمادة 41 من قانون العقوبات الجزائري. تُعرف الجريمة المتلبس بها عندما يتم اكتشاف الجريمة أثناء ارتكابها أو فور ارتكابها[1]، أو عندما يصدر أمر من قاضي التحقيق بذلك.

يقوم عضو الضبط القضائي بعدة مهام سنوضحها في النقاط التالية :

أ- المعاينة :

توثيق وجمع الأدلة المادية يلعب دورًا حاسمًا في عمليات التحقيق الجنائي وتحقيق العدالة. يعمل الضابط القضائي على معاينة المكان بعد وقوع الجريمة ويتأكد من سلامة الأدلة المادية وتوثيقها بحرص ودقة.

الضابط القضائي يقوم بمشاهدة الأدلة المادية المتعلقة بالجريمة ويضع جهوده في توثيقها بطرق متعددة. يهدف ذلك إلى ضمان سلامة الأدلة والحفاظ على صحتها لاستخدامها في عملية التحقيق وتقديمها كدليل في المحاكمة. بعض الطرق الشائعة لتوثيق الأدلة المادية [2]تشمل:

التصوير الفوتوغرافي: يتم استخدام الكاميرات الفوتوغرافية لالتقاط صور دقيقة للأدلة المادية. يتم توثيق الموقع الأصلي للأدلة وتفاصيلها بواسطة التصوير من زوايا مختلفة واستخدام التقنيات المناسبة لتسجيل حجم وموقع الأدلة بدقة.

التسجيل المرئي: يتم استخدام الكاميرات المراقبة أو كاميرات الفيديو لتسجيل فيديو لعملية توثيق الأدلة. يتم تسجيل الإجراءات المتخذة والتفاصيل المهمة التي تتعلق بالأدلة المادية.

---

[1] لعمريوي ليلى، مرجع سابق، ص62

[2] عماري ليندة، افنان عبد الغاني، مرجع سابق، ص 40

التسجيل الكتابي: يقوم الضابط القضائي بتوثيق الأدلة المادية وتفاصيلها في تقرير معاينة الجريمة. يشمل ذلك وصفًا مفصلاً للأدلة وموقعها والظروف المحيطة بها.

توثيق الأدلة المادية يعتبر جزءًا هامًا من عملية التحقيق الجنائي، حيث يساعد على توثيق الحقائق وتوجيه التحقيقات المستقبلية. كما يساعد في منع تلف الأدلة أو تغييرها، مما يضمن أن تكون الأدلة المقدمة قوية وموثوقة في سياق العدالة.

في حالة جرائم الكمبيوتر والتقنية، يمكن للضابط القضائي أن يقوم بتحليل وفحص الحواسيب والأجهزة الإلكترونية ذات الصلة كجزء من عملية التحقيق. يهدف ذلك إلى جمع المعلومات والبيانات ذات الصلة التي يمكن استخدامها كأدلة في جريمة الكمبيوتر.

عملية فحص الحواسيب والأجهزة الإلكترونية تتضمن استخدام تقنيات متقدمة لاستخراج البيانات المخزنة عليها. يمكن أن تشمل هذه التقنيات استرجاع البيانات المحذوفة أو الغير مرئية وتحليل محتوى القرص الصلب والملفات والبرامج الموجودة على الأجهزة.

بالإضافة إلى ذلك، يمكن للضابط القضائي جمع البصمات الضرورية من الأجهزة الإلكترونية والمكونات المرتبطة بها. يتم تحليل هذه البصمات للتأكد من صحتها واستخدامها كأدلة في التحقيق. قد تكون البصمات الضرورية عبارة عن بصمات أصابع على لوحة المفاتيح أو الفأرة أو أي جزء آخر من الجهاز يمكن أن يحتوي على بصمات ضرورية لتحديد هوية المستخدم.

تحقيق جرائم الكمبيوتر يتطلب القدرة على جمع البيانات الرقمية وفهمها بشكل صحيح. ومن ثم، يمكن للأدلة الرقمية المكتشفة أن تسهم بشكل كبير في تحديد المشتبه بهم وإثبات جرائمهم.

توثيق وجمع الأدلة الموثوقة والمادية بعناية واحترافية يساهم في بناء حالة قوية أمام المحكمة وتقديم المتهمين للمحاكمة العادلة. فاستنادًا إلى هذه الأدلة، يتم اتخاذ قرارات قضائية مبنية على أسس قوية وموثوقة لتحقيق العدالة.[1]

[1] عماري ليندة، افنان عبد الغاني، مرجع سابق، ص 40

ب التفتيش

التطور العلمي والتكنولوجي في العصر الحالي يعمل على زيادة تعقيدات الفكر القانوني ويطرح تحديات جديدة أمام نظم العدالة. واحدة من هذه التحديات هي التعامل مع الأدلة العلمية والتقنية التي تصبح أكثر انتشارًا وتأثيرًا في القضايا القانونية.

استخدام الأدلة العلمية والتقنية يعتبر تطورًا بارزًا في أنظمة القانون، حيث يساهم في تحقيق العدالة وتطويرها وتحقيق الحقيقة. فالأدلة العلمية والتقنية تعتمد على المعرفة والتقنيات الحديثة، وتمثل أدوات فعالة في تقييم الحقائق وفهم الظروف المحيطة بالجرائم.

قد تشمل الأدلة العلمية والتقنية عدة جوانب، مثل التحليل الجيني والبصمات الوراثية وتحليل الأدلة الكيميائية والفيزيائية والأدلة الرقمية. تستند هذه الأدلة إلى الأبحاث العلمية والتقنيات المتقدمة، وتوفر معلومات موثوقة ومحددة لدعم عملية التحقيق واتخاذ القرارات القضائية.

استخدام الأدلة العلمية والتقنية يساهم في زيادة دقة وموثوقية النتائج، ويساعد على تقليل التأويلات والاعتماد على الحقائق الملموسة. كما يمكن أن يسهم في كشف الأدلة المزيفة أو المضللة وتعزيز الثقة في عملية التحقيق والعدالة.

ومع ذلك، يجب أن يتم استخدام الأدلة العلمية والتقنية بحذر وفقًا للإرشادات القانونية والأخلاقية، مع مراعاة حقوق الأفراد وضمان الشفافية والعدالة في عملية التحقيق والمحاكمة.

عملية تفتيش الشخص المشتب ه به والأجهزة المحمولة التي يحملها تستهدف جمع الأدلة المتعلقة بالجريمة المشتبه بها. تعتبر الأجهزة المحمولة مصدرًا غنيًا بالمعلومات والأدلة المحتملة، وتشمل مجموعة واسعة من البيانات والملفات التي يمكن استخدامها في عملية التحقيق[1].

بعض الأدلة المشتركة التي يمكن العثور عليها في الأجهزة المحمولة تشمل:

[1] عماري ليندة، افنان عبد الغاني، مرجع سابق، ص 42

رسائل النص: يمكن أن تحتوي رسائل النص على محتوى مهم يتعلق بالجريمة المشتبه بها، بما في ذلك التخطيط أو التنسيق مع الآخرين.

سجل المكالمات: يسجل سجل المكالمات معلومات حول المكالمات الهاتفية الواردة والصادرة، وقد يكون لها صلة بالجريمة أو تقديم دليل على الاتصال بين المشتبه به وأطراف أخرى ذات صلة.

الصور والفيديوهات: يمكن أن تحتوي الأجهزة المحمولة على صور أو فيديوهات تسلط الضوء على النشاط المشتبه به أو توثق الحدث المرتبط بالجريمة.

التطبيقات المثبتة: يمكن أن توفر التطبيقات المثبتة معلومات عن تفاصيل الجريمة المحتملة أو تكشف عن أنشطة غير قانونية.

ملفات الوسائط المختلفة: تشمل ملفات الوسائط المختلفة مثل الملفات الصوتية والملفات الفيديو والمستندات، والتي يمكن أن تحتوي على أدلة مهمة.

عند إجراء تفتيش الأجهزة المحمولة، يجب أن يتم ذلك وفقًا للإجراءات القانونية المعمول بها وباحترام حق عملية التفتيش يجب أن تتم وفقًا للقوانين والإجراءات المعمول بها، مع احترام خصوصية الأفراد والالتزام بالضوابط القانونية المنصوص عليها. إذا تم العثور على أدلة قانونية خلال التفتيش، يمكن استخدامها في إطار التحقيق وتقديمها كأدلة في المحاكمة.

بعد إجراء التفتيش، يمكن لعضو الضبط القضائي توجيه الاتهام للشخص المشتبه به بناءً على الأدلة المكتشفة وإعداد محضر التفتيش الذي يوثق العملية والنتائج التي تم الوصول إليها.

يجب أن يتم تنفيذ عملية التفتيش بحرص ودقة لضمان الحصول على الأدلة المشروعة واحترام حقوق الأفراد المعنيين في العملية.[1]

[1] شنين صالح، مرجع سابق، ص230

في المادة 47 فقرة 3 من قانون الإجراءات الجزائية الجزائري، وفيما يتعلق بالجرائم المعلوماتية التي يتم اكتشافها عند ارتكابها، تم السماح بإجراء التفتيش والمعاينة والحجز. تنص المادة على أنه يجوز تنفيذ عمليات التفتيش والمعاينة والحجز في أي مكان سواء كان محل سكن أو غير سكني، في أي وقت من النهار أو الليل. ولكن يتطلب ذلك الحصول على إذن مسبق من وكيل الجمهورية المختص. يتضمن نطاق التفتيش والمعاينة هذا الأمر كل من الجرائم المتعلقة بالمخدرات، والجريمة المنظمة التي تتجاوز الحدود الوطنية، وجرائم انتهاك أنظمة معالجة البيانات، وجرائم غسيل الأموال[1].

يتم تنفيذ عمليات التفتيش في هذه الجرائم على المكونات الفعلية والافتراضية للحاسب الآلي، بالإضافة إلى شبكة الاتصالات المرتبطة به. يقوم المفتش بتحرير محضر يشتمل على جميع الإجراءات التي تم اتخاذها بشأن الوقائع التي تثبت وقوع الجريمة، ويشمل التاريخ وتوقيع المحرر. يعود لعضو الضبط القضائي مسؤولية ضبط جميع العناصر المتعلقة بالجريمة والتي تساهم في التحقيق، سواء كانت أدوات استخدمت في ارتكاب الجريمة أو العناصر التي نتجت عنها، وأيضًا المعلومات المفيدة للكشف عن الحقيقة. يتم ذلك من خلال جمع البيانات المعلوماتية وضبطها من شبكة المعلومات ذات الصلة[2].

ت- التسرب الالكتروني:

حرصاً على مكافحة هذه الجرائم، قام المشرع بتوسيع صلاحيات الضبطية القضائية العادية لتمنحها صلاحية حديثة. يتم ذلك عن طريق السماح باستخدام وسائل تقنية للكشف السريع عن هذه الجرائم ومرتكبيها. يتم تنفيذ هذه الصلاحية من خلال مفهوم التسرب الإلكتروني، وقد جاء ذكر التسرب الإلكتروني في المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري التي تنص على: "عندما تستدعي ضروة التحري أو التحقيق في إحدى الجرائم المشار إليها في المادة 65 أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد

[1] الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق ل2 يونيو 1966 ، الذيّ تضمن قانون الإجراءات الجزائية، ج.ر، عدد ،48 صادر في 10 يونيو ،1966 معدل و متمم.

[2] شنين صالح، مرجع سابق، ص 238

إبلاغ وكيل الجمهورية، أن يأذن بتنفيذ عملية التسرب تحت إشرافه، وفقًا للشروط المبينة في المواد التالية.[1]

تم إدراج المادة 65 مكرر 12 في قانون الإجراءات الجزائية للتعامل مع حالات التسرب الإلكتروني بالتعريف التالي: "يشمل مفهوم التسرب تصرف ضابط الشرطة القضائية أو أحد مساعديه، وذلك بموجب توجيهات من ضابط الشرطة القضائية المكلف بتنسيق العمليات، حيث يقوم بمراقبة الأفراد المشتبه فيهم بارتكاب جريمة أو مخالفة بطرق تجعلهم يعتقدون أنه شريك أو متواطئ معهم، أو يثير فيهم الريبة أو الخوف"[2]

توضح الفقرة المذكورة أعلاه أن التسرب الإلكتروني يشير إلى تقنية حديثة في مجال التحقيقات والاستدلال الجنائي، حيث يتمكن ضباط الشرطة القضائية من الوصول إلى أنظمة معلوماتية أو نظم اتصالات إلكترونية، ويقومون بذلك من خلال إنشاء صفحات متعددة على منصات التواصل الاجتماعي الشائعة مثل Facebook، بهدف رصد الأفراد المشتبه فيهم وكشف أنشطتهم الإجرامية، مع القدرة على إخفاء هويتهم الحقيقية وفقًا لما ينص عليه القانون[3].

بمفهوم اخر، يُعرف التسرب الإلكتروني بأنه نظام حديث يندرج ضمن أنظمة التحري والاستقصاء الخاصة. يُمكن لضابط الشرطة القضائية، وفقًا للقوانين المعمول بها، اختراق المنظومة المعلوماتية أو نظم الاتصالات السلكية، والتوغل فيها تحت إشراف ضابط الشرطة القضائية. يتم ذلك بعد إبلاغ وكيل النيابة العامة، الذي يقرر ما إذا كانت العملية ستستمر أو يتم إيقافها. يهدف ذلك إلى كشف الجرائم الإلكترونية التي تستهدف المستهلك الإلكتروني وملاحقة المتورطين فيها. يُمكن في هذا السياق إخفاء الهوية الحقيقية من خلال إنشاء حسابات مجهولة باستخدام أسماء مستعارة على منصات التواصل الاجتماعي[4].

---

[1] شنين صالح، مرجع سابق، ص 238

[2] رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966، الذي يتضمن قانون الإجراءات الجزائيّة، مرجع سابق

[3] المرجع نفسه.

[4] بن عودة نبيل، نوار محمد، مرجع سابق، ص .328.329

الفرع الثاني: مرحلة التحقيق الابتدائي:

يشمل التحقيق الابتدائي سلسلة إجراءات يقوم بها جهاز مختص للتحقيق في صحة الاتهام الموجه من قبل النيابة العامة. يعتبر هذا المرحلة مرحلة لاحقة لعمليات البحث والتحري التي يقوم بها أحد أفراد الشرطة القضائية وتسبق مرحلة المحاكمة.

يهدف التحقيق إلى إعداد الأرضية المناسبة لإصدار الحكم وكشف الحقيقة. ولتحقيق هذا الهدف، يتبع المحقق مجموعة من الإجراءات مثل التفتيش، الضبط، المعاينة، الشهادة الخبرة، والحبس المؤقت. يلعب التفتيش دورًا حاسمًا في إثبات الجرائم وتحديد الجناة. يقوم جهاز مختص بتنفيذ هذا التفتيش للوصول إلى نظام معالجة البيانات، والذي يحتوي على مدخلات وتخزين للمعلومات. ومن خلال ذلك، يتم العثور على الأدلة المؤكدة للجرائم ونسبها بالمتهم.[1]

تمكن المشرع الجزائري من خلال المادتين 45 و 47 من القانون 6-22 المعدل والمتمم لقانون الإجراءات الجزائية من إجازة تفتيش المنظومة المعلوماتية. وينص القانون على أنه في حالة توجيه التفتيش للتحقيق في جرائم معلوماتية، لا يشترط حضور صاحب المسكن أو المشتبه به. يتم تطبيق الأحكام المتعلقة بالحفاظ على السرية المهنية، بالإضافة إلى جرد الأشياء وحجز المستندات المتعلقة بالتحقيق[2].

وفقًا لقانون الإجراءات الجزائية المعمول به في الجزائر، أكد المشرع على إمكانية إجراء تفتيش في المنازل أو المكاتب، سواء كانت سكنية أو غير سكنية، عندما يتعلق الأمر بجرائم تتعلق بأنظمة المعالجة الآلية للبيانات. يمكن إجراء هذا التفتيش في أي وقت من النهار أو الليل، وذلك بناءً على إذن مسبق من وكيل الجمهورية المختص[3].

---

[1] افنان عبد الغاني، عماري ليندة، مرجع سابق، ص 42

[2] أنظر المادة 45 من القانون 06-22 المؤرخ في 20 ديسمبر ،2006 المتضمن قانون الإجراءات الجزائية،ج.ر، عدد 84، صادر في 02 ديسمبر ،2006 معدل و متمم للأمر رقم 66-155

[3] راجع المادة 47 فقرة 3 من الأمر رقم 66-155 ، المتضمن قانون الإجراءات الجزائية، مرجع سابق

وفقًا للمشرع الجزائري، يُسمح بالدخول إلى منظومة معلوماتية لأغراض التفتيش ولو عن بعد[1]. تحدد المادة 04 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الحالات التي يُسمح فيها بذلك. تتضمن هذه الحالات الوقاية من جرائم الإرهاب والتخريب والجرائم الماسة بأمن الدولة، وفي حالة وجود معلومات تشير إلى احتمالية الاعتداء على منظومة معلوماتية تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. يشترط في التفتيش المعلوماتي في الجرائم المعلوماتية وجود جريمة معلوماتية مشتبه في ارتكابها وتوجيه اتهام لشخص أو أشخاص معنيين بارتكابها أو المشاركة فيها، بالإضافة إلى وجود قرائن قوية تشير إلى الكشف عن الحقيقة. يجب أن يُجرى التفتيش بواسطة سلطة مختصة في التحقيق، وهي قاضي التحقيق. يتم تحرير محضر التفتيش المعلوماتي الذي يتضمن توقيت العملية وإذن التفتيش المكتوب الصادر عن وكيل الجمهورية أو قاضي التحقيق.[2]

المطلب الثاني

في مرحلة المحاكمة

تعد المحكمة المرحلة النهائية في دعاوى الجنح العامة، حيث تختص بنظر جميع القضايا المتعلقة بأفعال تعتبرها القانون جريمة، بغض النظر عن هوية الشخص المتهم بارتكابها. تنتهي مرحلة المحاكمة عندما يصدر الحكم الجنائي من الهيئة القضائية، سواء بالإدانة أو البراءة، ويكون هذا الحكم نهائياً في الدعوى العامة. وتشير النتائج التي تم الكشف عنها في المؤتمرات إلى أن هناك عددًا كبيرًا من القضايا المتنازع عليها والمشكوك في صحتها، وهذا أمر مقلق. فالعديد من أصحاب البطاقات يشكون من عدم التعرف على البائع ومن وقوع عمليات احتيال. كما تثار أيضًا مشكلة النزاعات في التجارة الإلكترونية بسبب وجود علاقات تجارية تجمع بين أطراف من جنسيات وأماكن إقامة مختلفة، مما يثير

[1] انظر المادة 5 من القانون 09-04 المتعلق بالوقاية من الجزائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها.

[2] لعمريوي ليلى، مرجع سابق، ص65

جدلاً حول تحديد القانون الذي يجب تطبيقه في حالة عدم التوافق بين الأطراف المتعاقدة. سنركز في هذا السياق على مناقشة الاختصاص الجنائي على المستوى الوطني والدولي .[1]

الفرع الأول: الاختصاص الجنائي الوطني للمحكمة في التشريع الجزائري

أولا الإختصاص الجنائي الوطني:

في حالة عدم تحديد الجهة القضائية المختصة لفصل في النزاعات بين المستهلك والمهني في قانون حماية المستهلك، يجب الرجوع إلى القواعد العامة المنصوص عليها في القانون المدني المعدل والمتمم بالقانون رقم 05-10 الصادر في تاريخ 10/06/2005.

وفقًا للمادة 12 المكررة من هذا القانون، ينص على أنه يجب تطبيق قواعد الاختصاص والإجراءات المنصوص عليها في قوانين الدولة التي تقدم فيها الدعوى أو تباشر فيها الإجراءات. وهذا يعني أنه يتعين الالتزام بقواعد الاختصاص والإجراءات المنصوص عليها في القوانين المدنية المعمول بها في الدولة التي تقدم فيها الدعوى.

بموجب هذه المادة، يتم تحديد الجهة المختصة والإجراءات القضائية وفقًا للقوانين المدنية المعمول بها في الدولة المعنية. لذلك، يلزم الرجوع إلى النصوص القانونية المعمول بها في الدولة ذات الاختصاص لتحديد الجهة القضائية المختصة والإجراءات اللازمة لفصل في النزاعات بين المستهلك والمهني.[2]

إذا انتقل الاختصاص إلى القانون الجزائري، فإن الأصل ينص عليه المادة 37 من قانون الإجراءات المدنية والإدارية التي تحدد اختصاص المحكمة وفقاً لمكان إقامة المدعى عليه. وإذا لم يكن للمدعى عليه مكان إقامة معروف أو محل معروف، فإن الاختصاص يعود إلى المحكمة التي تنتمي إليها آخر مكان معروف له. في حالة العقود الاستهلاكية الإلكترونية، فإن المحكمة المختصة هي تلك التي تقع في منطقة إقامة أحد الأطراف أو

[1] افنان عبد الغاني، عماري ليندة، مرجع سابق، ص 43

[2] قانون رقم 05-10 المؤرخ في 13 جمادى الأولى عام 1426 الموافق 20 يونيو ،2005 المعدل والمتمم للأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة ،1975 المتضمن القانون المدني، ج.ر، عدد ،44 صادر في 20 يونيو 2005

مسكنهم، وذلك وفقًا لاختيار المدعي. ولكن هناك استثناءات تطبق على هذا الاختصاص المحلي العام لعقود الاستهلاك، حيث تأخذ بعين الاعتبار محكمة مقر الشركة أو محكمة موقع العقار أو محكمة مقر تقديم العلاج أو محكمة مقر المرسل أو المرسل إليه أو محكمة أداء الأغذية والسكن. وبالتالي، يتم تحديد الاختصاص المحلي للمحاكم وفقًا لمكان وقوع الجريمة أو مكان إقامة أحد الأشخاص المشتبه فيهم، أو مكان القبض عليهم. ونظرًا لأن جرائم الإنترنت يمكن أن تحدث في مكان معين، فإن المشرع يسمح بتمديد الاختصاص المحلي لوكيل النيابة العامة وقاضي التحقيق إلى دوائر اختصاص المحاكم الأخرى. ومع ذلك، يتم تنظيم تطبيق ذلك عن طريق التنظيم[1].

ثانيا : الاختصاص الجنائي الدولي

في قانون العقوبات الجزائري وقانون الإجراءات الجزائية، تتم تنظيم الاختصاص الجنائي الدولي وفقًا للمبادئ العالمية المعروفة. وتشمل هذه المبادئ:

مبدأ الإقليمية: وفقًا لهذا المبدأ، يكون للدولة السيادة والاختصاص في محاسبة المشتبه بهم على أفعالهم التي ترتكب داخل إقليمها الجغرافي. ويعني ذلك أن الدولة تحقق وتحاكم الأفراد المتهمين بارتكاب جرائم داخل حدودها الوطنية.

مبدأ الشخصية: ينص على أن الاختصاص الجنائي يتعلق بالشخص وليس بالجنسية أو الجنس أو الدين أو أي عوامل أخرى. وبموجب هذا المبدأ، يمكن محاكمة المتهمين بجرائم في الدولة التي تقوم فيها الجريمة بغض النظر عن جنسيتهم.

مبدأ العالمية: يسمح للدول بمحاكمة المتهمين بجرائم خطيرة ومن الطابع العالمي، بغض النظر عن مكان ارتكاب الجريمة أو جنسية المتهم أو الضحية. ويكون ذلك استنادًا إلى مبادئ القانون الدولي والمعاهدات والاتفاقيات المتعلقة بحقوق الإنسان.

[1] قطاف إسماعيل، مرجع سابق، ص100

تلك المبادئ تهدف إلى توفير نظام عادل لمحاكمة الجرائم الجنائية وضمان تحقيق العدالة الدولية. ويستند التطبيق الفعلي لهذه المبادئ إلى القوانين والاتفاقيات الدولية التي تحكم الاختصاص الجنائي على المستوى الوطني والدولي.

وتنص المادة 582 من قانون الإجراءات الجزائية الجزائري على أنه يجوز متابعة ومحاكمة الجزائري الذي ارتكب جريمة خارج إقليم الجمهورية وتُعتبر جريمة جنائية معاقب عليها وفقًا للقانون الجزائري في الجزائر[1]. ووفقًا لمبدأ الإقليمية المنصوص عليه في المادة 3 من قانون العقوبات الجزائري، يُطبق القانون الجزائري على الجرائم المرتكبة داخل إقليم الجزائر بغض النظر عن جنسية المرتكب أو المجني عليه. وتحدد دولة التطبيق للقانون من خلال وقوع الجريمة كاملة أو جزء منها على إقليم الدولة.وبموجب مبدأ الشخصية، يكون القانون الجزائري هو القانون المطبق إذا ارتكب جزائري جريمة من جرائم الإنترنت، أو إذا كان المجني عليه جزائري الجنسية لحظة وقوع الجريمة. وبناءً على مبدأ العينية، يتولى الاختصاص المحاكم إذا وقعت جريمة من جرائم الإنترنت وتتعلق بمصالح الدولة الأساسية والجوهرية، حتى وإن وقعت خارج الدولة، بغض النظر عن جنسية المرتكب.[2]

[1] أمر رقم 66-155 مؤرخ في 8 يونيو ،1996 المتضمن قانون الإجراءات الجزائية، مرجع سابق.

[2] راجع المادة 588 من قانون الإجراءات الجزائية

المبحث الثاني

إثبات الجرائم الواقعة على المستهلك الالكتروني

من الواضح أن إثبات الجريمة يحمل أهمية كبيرة، حيث يهدف إلى كشف الحقيقة. إذ يعتبر من الصعب معاينة الجريمة التي وقعت في الماضي وتحديد حقيقتها وتوجيه الاتهامات واتخاذ قرار قضائي دون الاعتماد على وسائل تجسد سير وتفاصيل الجريمة. تُعرف هذه الوسائل بوسائل الإثبات.

وبالتحديد، فإن أدلة الإثبات في الجرائم الإلكترونية تتمتع بأهمية خاصة وتختلف عن الجرائم التقليدية، حيث تتطلب طبيعتها الخاصة أساليب وأدوات مختلفة. سنناقش هذا الموضوع في قسمنا هذا، الذي قمنا بتقسيمه إلى مطلبين. سيتم التطرق في المطلب الأول إلى أدلة الإثبات التقليدية والحديثة، حيث سنستعرض تطور تلك الأدلة وتقنياتها المتنوعة. أما في المطلب الثاني، سنتناول حدود قبول الدليل الجنائي، أي الشروط التي يجب توافرها لاعتبار الدليل صالحًا وقابلاً للقبول في المحاكمة الجنائية.

المطلب الأول

وسائل الإثبات الجنائي

إن الإثبات يتمثل في تقديم الدليل الذي يثبت وقوع الجريمة ويربطها بالمتهم. يمكن القول بثقة أن القاضي الجنائي يصل إلى حكم يعكس الواقعية في الواقعة المطروحة عليه. يعتمد القاضي في ذلك على وسائل الإثبات التي تمكنه من بلوغ اليقين بشأن هوية المتهم الفعلي للجريمة. تعد الأدلة الرقمية واحدة من التطورات الهامة في العصر الحديث، وتأتي تلك الأدلة لتتلاءم مع التقدم العلمي والتكنولوجي في العصر الحالي. بالتالي، أصبحت وسائل الإثبات متجاوزة.[1]

لذا في هذه المطلب سنتناول فيه أدلة الإثبات التقليدية و الحديثة و ذلك كما يلي:

[1] افنان عبد الغاني، عماري ليندة، مرجع سابق، ص46

الفرع الأول: الإثبات بالوسائل التقليدية:

يعتبر الاعتماد على الوسائل التقليدية في جمع الأدلة من العمليات الأساسية في نظام العدالة الجنائية. فلكل وسيلة من هذه الوسائل قواعد وإجراءات تتم اتباعها لضمان صحة الأدلة وقبولها أمام المحكمة. ومع ذلك، فقد تثار تساؤلات حول جدوى هذه الوسائل التقليدية في جمع الأدلة الإلكترونية.

مع تطور التكنولوجيا، أصبحت الأدلة الرقمية تلعب دورًا مهمًا في الجرائم الإلكترونية والجرائم التقنية. ومن أمثلة هذه الأدلة الرقمية تسجيلات الفيديو والصور والرسائل الإلكترونية وسجلات الاتصالات والملفات الرقمية الأخرى. يمكن استخدام هذه الأدلة لتتبع أنشطة المشتبه بهم وتأكيد تورطهم في الجرائم.

ومع ذلك، فإن جمع الأدلة الإلكترونية يتطلب تقنيات وأساليب جديدة. يجب على القضاة والمحققين التحقق من صحة هذه الأدلة وموثوقيتها وسلامتها من التلاعب. يتطلب ذلك توفر الخبرة والتدريب المتخصص في مجال الأدلة الرقمية.

و هذه الوسائل التقليدية هي:

أولا: الشهادة

يشير مصطلح "الشهادة" إلى تقرير يقدمه الشخص بشأن ما رآه أو سمعه بنفسه أو شعر به بواسطة حواسه. وفيما يتعلق بجرائم المعلوماتية، يُشير مصطلح "الشاهد" إلى الشخص الذي يتمتع بالخبرة المعلوماتية والتخصص في تقنية وعلوم الحاسب الآلي وشبكاته. يُطلق على هذا النوع من الشهود مصطلح "الشاهد المعلوماتي" لتمييزه عن الشهود التقليديين.[1]

الشهادة تعتبر وسيلة أساسية لتقديم الأدلة في المحاكم، حيث يتم استدعاء الشاهد للإدلاء بمعلومات وملاحظاته المتعلقة بالجريمة أو الحدث المطروح على المحك. وفي جرائم المعلوماتية، يكون الشاهد المعلوماتي هو الشخص الذي يمتلك المعرفة الفنية والخبرة في

[1] سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، 2012، ص 118

مجال التكنولوجيا وأمن المعلومات، ويمكنه تقديم تحليلات وشهادات تتعلق بالأنشطة الإلكترونية والتهديدات والاختراقات. يعتبر الشاهد المعلوماتي جزءًا هامًا من عملية الإثبات في جرائم المعلوماتية، حيث يمكنه توضيح التفاصيل التقنية المعقدة أمام القضاء وتفسير الأدلة الرقمية والتقنية بشكل مفهوم. يستند القضاة والمحامون إلى خبرة الشاهد المعلوماتي لفهم تفاصيل التكنولوجيا وتقييم قوة الأدلة الرقمية المقدمة. بالتالي، يمكن اعتبار الشاهد المعلوماتي كمورد قيم في جرائم المعلوماتية، حيث يساهم في تحقيق العدالة والحقيقة من خلال تقديم الأدلة الفنية والتوضيحات المتعلقة بالتقنية والأمان السيبراني.[1]

فيما يتعلق بمعنى الشهادة في حالات الجرائم الإلكترونية، فإنها لا تختلف كثيرًا عن الشهادات المتعلقة بالجرائم التقليدية. يتعلق الأمر بسماع الشهود واستماعهم إلى ما لديهم من معلومات وشهادات حول الحادثة أو الجريمة المعلوماتية. ومع ذلك، يبقى أمر استدعاء الشهود وسماعهم يعتمد على تقدير المحقق ويرتبط بظروف التحقيق والمتطلبات المحددة لكل قضية. في نظام العدالة الجنائية، يتيح الأصل أن يطلب الخصوم استدعاء أي شاهد يرون أن لديه معلومات مهمة للقضية. وللمحقق أن يدعو إلى الشهادة أي شخص يرى أن لشهادته أهمية في كشف الحقيقة وتقديم الأدلة المهمة. بالإضافة إلى ذلك، يحق لأي شخص يتقدم من تلقاء نفسه ويمتلك معلومات ذات صلة أن يعرض شهادته.

بالتالي، يتم الاعتماد على مبدأ[2] استدعاء الشهود وسماعهم في جرائم المعلوماتية على نفس المبادئ الأساسية للعدالة الجنائية، مع التركيز على أهمية الشهادات التقنية والمعلوماتية من الأشخاص ذوي الخبرة في هذا المجال لكشف الحقيقة وتقديم الأدلة الملائمة.

ثانيا: الخبرة

الخبرة هي عملية تتطلب معرفة متخصصة في موضوع محدد يمكن من خلالها استخلاص الدليل والتوصل إلى رأي مؤهل. تتعلق الخبرة بفن أو معرفة تمكن الخبير من

[1] أبوديار مليكة، الإثبات الجنائي في الجرائم الالكترونية، المجلة القانونية للابحاث القانونية، عدد2، تونس، 2018، ص106

[2] افنان عبد الغاني، عماري ليندة، مرجع سابق، ص47

تحليل المعلومات وتفسيرها بطريقة متخصصة، وتتطلب التفاعل مع أدوات ومصادر معينة. تُعد الخبرة واحدة من وسائل الإثبات المباشرة التي يعتمد عليها القاضي للحصول على معلومات من الخبراء في المجالات التقنية والعلمية. يقوم القاضي باللجوء إلى الخبراء للاستعانة بهم في توضيح الأمور التقنية أو العلمية التي تتعلق بالقضية، وذلك للوصول إلى الحقيقة وتقديم الأدلة اللازمة. فيما يتعلق بالمسائل التقنية، فإنه قد يكون من الصعب على القاضي أن يكون ملمًا بكل التفاصيل التقنية المعقدة التي تتعلق بالجرائم الإلكترونية أو التقنيات الحديثة. لذا، فإن الخبراء المعنيين بتلك المجالات يقدمون رأيهم المؤهل والمدروس بشأن الأمور التقنية والعلمية المرتبطة بالقضية.[1]

بالتالي، يمثل استخدام الخبراء والاعتماد على خبراتهم واحدة من السبل التي يلجأ إليها القاضي للوصول إلى اكتشاف الحقيقة في المسائل التقنية التي تتعذر فهمها بوساطة المحكمة. يساعد ذلك في ضمان استناد القرارات القضائية إلى معرفة متخصصة وخبرات تقنية لتحقيق العدالة.

الفرع الثاني: الإثبات بالأدلة الالكترونية الحديثة

التطور العلمي والتكنولوجي في العصر الحالي يطرح تحديات جديدة أمام الفكر القانوني ويزيد من تعقيداته. يشهد الدليل العلمي اهتمامًا متزايدًا في الوقت الحاضر، ويُعتبر استخدام الأدلة العلمية والتقنية وسيلة تطورية بارزة في أنظمة القانون. فهي تتمتع بصفة الحداثة وتسهم في تطوير العدالة وتحقيق الحقيقة.

تواجه النظم القانونية تحديات جديدة نتيجة التطورات التكنولوجية والعلمية المستمرة. فمع التقدم في مجالات مثل علوم الحاسوب، والتحليل الجيني، والتقنيات الرقمية الأخرى، أصبح بإمكان الجهات القانونية الاستناد إلى الأدلة العلمية لتقديم البراهين وتحقيق العدالة.

يتضمن الدليل العلمي العديد من الوسائل المتقدمة مثل التحليلات المعملية، والتحقيقات الجينية، والتحليل الرقمي، والمحاكاة الحاسوبية، وغيرها. تستخدم هذه الوسائل

[1] سامي جلالي فقي حسين، مرجع سابق، ص114

لتحليل البيانات، واستنتاج النتائج العلمية، وإنتاج الأدلة القوية التي تدعم قضية الادعاء أو الدفاع.

بفضل استخدام الدليل العلمي والوسائل الحديثة، يتم تعزيز قدرة القضاء على الوصول إلى الحقيقة واتخاذ قرارات مستنيرة. يعزز استخدام الأدلة العلمية الشفافية والموضوعية في العملية القضائية، ويقدم حلولًا متقدمة للمشكلات القانونية المعقدة.

بهذه الطريقة، يمكن القول إن الإثبات الجنائي بالوسائل الحديثة يعتبر من أبرز تطورات العصر الحديث في المجال ال

قانوني. يمنح النظام القانوني القدرة على التأكد من الحقيقة من خلال الأدلة العلمية المبنية على المعرفة والتكنولوجيا الحديثة، وهو يساهم في تعزيز العدالة وتحقيق المساواة أمام القانون.

و من الأدلة المستحدثة في مجال الإثبات و المخصصة للإثبات الالكتروني هي:

أولا: الإثبات بواسطة البريد الالكتروني

البريد الإلكتروني هو وسيلة فعالة للتواصل عن بعد، حيث يوفر القدرة على إرسال واستقبال الرسائل بسرعة وتكلفة منخفضة عبر شبكة الإنترنت. يتم استخدام البريد الإلكتروني عن طريق برامج خاصة تسمح بكتابة وإرسال الرسائل، وكذلك استعراض وقراءة الرسائل الواردة. يعد البريد الإلكتروني وسيلة مرنة ومتاحة للأفراد والمؤسسات في جميع أنحاء العالم. بفضل توفر الإنترنت، يمكن للأشخاص التواصل بسهولة مع بعضهم البعض بغض النظر عن المسافات الجغرافية. من الجوانب الأمنية، يحتاج استخدام البريد الإلكتروني إلى وسائل حماية للحفاظ على السرية والأمان. على سبيل المثال، يتطلب حساب البريد الإلكتروني كلمة مرور قوية لمنع وصول غير المصرح به. كما يتم توفير خيارات أخرى مثل التحقق بخطوتين لزيادة الحماية. يوفر البريد الإلكتروني مزايا إضافية مثل القدرة على الرد وحفظ الرسائل وإعادة إرسالها بسهولة. يمكن للمستخدمين الاحتفاظ بالرسائل في صندوق الوارد للرجوع إليها في وقت لاحق، أو تخزينها في ملفات إلكترونية على أجهزتهم، أو حتى

طباعتها وحفظها كملفات ورقية. بالإضافة إلى ذلك، يمكن أن يكون البريد الإلكتروني قابلاً للاعتراف كدليل قانوني في النظم القانونية، شريطة التأكد من صحة وجوازية الرسالة وفقًا للتشريعات المعمول بها في البلدان المختلفة. تختلف التشريعات المتعلقة بالأدلة الإلكترونية من بلد لآخر، حيث توجد بعض البلدان التي وضعت تشريعات خاصة بهذا الشأن بناءً على التقنيات الحديثة، في حين تستند دول أخرى إلى المبادئ والقواعد العامة للإثبات في النظام القانوني العام. في النهاية، يمكن القول إن البريد الإلكتروني يعد وسيلة موثوقة وفعالة للتواصل عن بعد، وله القدرة على توفير السرعة والكفاءة في التواصل بين الأفراد والمؤسسات في جميع أنحاء العالم، بالإضافة إلى إمكانية استخدامه كدليل قانوني في النظم القانونية المناسبة[1].

ثانيا: الإثبات بواسطة المستندات الالكترونية

تطور مفهوم المستندات بفعل التقدم التكنولوجي الحديث، حيث تغيرت طبيعتها بشكل جذري عن المستندات التقليدية. المستند الإلكتروني يمثل أي وسيلة تعبير مكتوبة بواسطة وسائل إلكترونية تحمل فكرة معينة أو تعبير محدد. حلت المستندات الإلكترونية محل المستندات الورقية التقليدية، وبالتالي أصبحت المستندات الإلكترونية تُعتبر مستنداتٍ بحق. تم اعتماد حجية المستندات الإلكترونية واعتبارها قابلة للإثبات في أغلب التشريعات، حيث تعد سهلة التلاعب بها وتعرضها للتزوير. المحتوى المكتوب في المستندات الإلكترونية يتم تعبيره بواسطة لغة رقمية، وبالتالي تحل هذه اللغة محل الكتابة التقليدية. ونتيجةً لذلك، فإن المستند الإلكتروني يحمل نفس الحجية في الإثبات. طالما يُمكن قراءة المستند وفهم مضمونه ومعناه، فإنه يُعتبر محررًا يُعتد به ويكون دليلاً على منشئه. لذلك، يُمكن تطبيق ما نص عليه قانون الإجراءات الجزائية فيما يتعلق بالمحررات وحجيتها في الإثبات الجنائي على المستندات الإلكترونية. ومع ذلك، ينبغي أن نميز بين المستندات التي يتم إعدادها إلكترونيًا وتخرجها في شكل مادي، وبين الاعتراف بالمستند الإلكتروني ككيان معنوي مستقل

[1] هلال عبد الله أحمد، تفتيش نظام الحاسب الآلي و ضمانات المتهم المعلوماتي، الطبعة الثانية، دار النهضة العربية، القاهرة، ،2008 ص121

ذو حجية خاصة. من الأنسب الاعتراف بالمستندات الإلكترونية ككيان معنوي يحمل حجية خاصة كدليل في الأدلة الجنائية. وبناءعلى ذلك، ينبغي إضافة نص خاص للمستندات والمحررات المتعلقة بها، للتأكيد على هذه الحقيقة وتحديد حجيتها في سياق الإثبات.[1]

ثالثا: الإثبات بالعقد الإلكتروني:

يُعتبر العقد الإلكتروني واحدًا من الأدوات الحديثة المستخدمة في تبادل الأعمال في مجال التجارة الإلكترونية. يُعد العقد الإلكتروني وسيلة للتفاهم والقبول عبر شبكة اتصال دولية، حيث يتم تبادل البيانات الإلكترونية لإنشاء التزامات تعاقدية. يتم إبرام العقد الإلكتروني بشكل كامل أو جزئي عبر الإنترنت، حيث يتم توقيع الطرف الآخر على الوثيقة الرقمية أو إبداء الموافقة عليها بالطريقة المتفق عليها بين الأطراف.[2]

من المهم أن نناقش مدى اعتبار العقد الإلكتروني كدليل قابل للاعتماد في جرائم الإنترنت. يمكن تطبيق ذلك في بعض الجرائم التي تتطلب وجود شرط مفترض لارتكابها، على سبيل المثال، جريمة خيانة الأمانة. في حالة جريمة خيانة الأمانة، يشترط المشرع وجود عقد أمانة مثل عقد الوديعة أو الإيجار كشرط مفترض لارتكاب الجريمة. وبالتالي، يُعتبر إثبات وجود مثل هذا العقد الإلكتروني في جريمة خيانة الأمانة، حيث تم إبرام العقد الأمانة عبر الوسائل الإلكترونية، مقبولًا وقابلاً للاعتماد من قبل القضاء الجنائي. ويتم ذلك وفقًا للمعايير المنصوص عليها في إثبات العقود المدنية، أي أساليب الإثبات المتعلقة بالشهادات الشخصية والوثائق. تعترف قوانين المعاملات الإلكترونية بالعقد الإلكتروني كدليل قابل للاعتماد، مما يجعله مقبولًا للاعتبار من قبل القاضي الجنائي في إثبات وقوع جريمة خيانة الأمانة باستخدام وسائل الاتصال الإلكترونية الحديثة والاعتراف بوجود العقد الإلكتروني كشرط مفترض لوقوع تلك الجريمة[3]

---

[1] أمجد خليل حمودة، "الوسائل الحديثة لاثبات الجرائم التي ترتكب بواسطة الأجهزة الإلكترونية"، مجلة جامعة الأزهر، العدد 19، غزة، 2016، ص6-7

[2] أبو الديار مليكة، مرجع سابق، 106

[3] أمجد خليل حمودة، مرجع سابق، ص9

رابعا: الإثبات بالبصمة الرقمية أو الآثار المعلوماتية

تُعد البصمة الرقمية أدلة تترك أثرًا بدون أن يكون الشخص مقصودًا وجودها، وتُطلق عليها أيضًا مصطلح الآثار المعلوماتية الرقمية. يُترك آثر المستخدم في النظام المعلوماتي نتيجة تسجيل الرسائل المرسلة منه أو المرسلة إليه، بالإضافة إلى جميع الاتصالات التي تتم عبر النظام المعلوماتي وشبكة الاتصالات. ومع ذلك، فإن هذا النوع من الأدلة لم يعد أساسيًا للحفاظ على الخصوصية، نظرًا لأن التقنيات الحديثة تسمح بمراقبته وتتبعه على الرغم من بعض التأخير الزمني. يمكن ضبط الاتصالات التي تتم عبر الأنظمة المعلوماتية المتصلة بشبكة الاتصالات، وكذلك المراسلات الصادرة والواردة للشخص، باستخدام تقنيات خاصة بهذا الغرض. على سبيل المثال، يُمكن لشخص التواصل مع شخص آخر عبر البريد الإلكتروني لتحريضه غير مباشرة على تنفيذ أعمال تخريبية في بلد معين، وذلك من خلال تزويده بصور تخريبية لتُسجل عرضيًا على الكمبيوتر. ويُبرز الأهمية في التمييز بين هذين النوعين من الأدلة، حيث يتعمد النوع الأول حفظه للاحتفاظ به كدليل في المستقبل، وبالتالي يعتبر وسيلة لإثبات بعض الوقائع نظرًا لصعوبة فقدانه، كما أنه سهل الوصول إليه[1].

المطلب الثاني

القيمة القانونية للدليل الالكتروني

صحيح، الأدلة الإلكترونية تلعب دورًا مهمًا في إثبات الجرائم الإلكترونية. يمكن أن تكون الأدلة الإلكترونية في صورة مستندات ورقية تم إنتاجها بواسطة الطابعات أو الراسم، أو في صورة غير ورقية مثل الأقراص الممغنطة والأشرطة وغيرها من الأشكال الإلكترونية.

مع ذلك، يجب أن يتم الحصول على الأدلة الإلكترونية وفقًا للإجراءات والشروط المنصوص عليها قانونًا. يجب أن تكون الحصول على هذه الأدلة قانونيًا ولا يجب أن يتم انتهاك حقوق الأفراد أو تجاوز القوانين المعمول بها. إذا تم الحصول على الأدلة الإلكترونية عن طريق مخالفة القانون، فإن هذا الدليل يعتبر باطلاً وغير قانوني ولا يمكن استخدامه لإثبات الجرائم.

[1] أبوديار مليكة، مرجع سابق، ص106

بشكل عام، تعتمد حجية الأدلة الإلكترونية على عدة عوامل مثل طريقة الحصول عليها، ومصدرها، وتحقق صحتها التقنية، ووجود أي شهادات أو شهود يمكن التحقق منهم. يتطلب الاعتراف بالأدلة الإلكترونية توافر الضمانات القانونية والتقنية المناسبة لضمان أمانها وموثوقيتها.

لذلك، يجب على المحققين والنيابة العامة والمحاكم الالتزام بالإجراءات والشروط القانونية المناسبة عند جمع واستخدام الأدلة الإلكترونية، وذلك لضمان أن تكون هذه الأدلة صحيحة ومقبولة قانونًا في إثبات الجرائم الإلكترونية.

و لنبين ذلك سنتطرق في هذا المطلب إلى شروط الدليل الالكتروني (الفرع الأول)، ثم حجية الدليل الالكتروني (الفرع الثاني)، و أخيرا سلطة القاضي الجنائي في تقدير الأدلة الرقمية (الفرع الثالث).

الفرع الأول: شروط الدليل الالكتروني:

لصحة قبول الدليل الالكتروني في إثبات الجرائم المعلوماتية التي يقع المستهلك الالكتروني ضحية فيها لابد من توفر جملة من الشروط التالية:

أولا مشروعية الدليل الالكتروني

لضمان مشروعية الدليل الإلكتروني واستخدامه بشكل قانوني، يتعين الالتزام بأحكام الدستور وقوانين العقوبات. ينص الدستور على حماية كرامة الإنسان وحقوقه، وبالتالي يجب أن يتم استخلاص الدليل الإلكتروني بطرق تتوافق مع القوانين ومبادئ الدستور، خاصة فيما يتعلق بحماية الحريات الأساسية.

تشير الآراء القانونية في الدول المتقدمة في أوروبا وأمريكا إلى أهمية مبدأ المشروعية في الحصول على الدليل الإلكتروني، حيث يجب أن يتم بطرق شرعية ونزيهة ويبتعد عن الغش والتلاعب. ويجب أن تكون الأدلة القانونية الصحيحة دقيقة وصحيحة ومشتقة بشكل قانوني.

بالنسبة للعقوبات المترتبة على انتهاك القانون في الحصول على الأدلة، فقد يشمل ذلك عقوبات جنائية أو إدارية، بالإضافة إلى تعويضات مالية. يعتبر الموظف الذي ينتهك القانون في أداء واجباته ويتصرف بشكل غير قانوني مخالفًا لواجباته مستحقًا للمساءلة القانونية.

بالتالي، يجب الالتزام بالقوانين والإجراءات المنصوص عليها في النظام القانوني للحصول على الأدلة، وعدم ارتكاب جرائم أثناء الحصول عليها، حيث يعتبر الحصول على دليل بارتكاب جريمة باطلاً وغير قانوني لأنه يتعلق بالنظام العا.[1]

ثانيا يقينية الدليل الالكتروني

تمامًا، لكي يتم قبول الأدلة المستخرجة من الحاسوب والإنترنت واستخدامها في التحقيقات الجنائية، يجب أن تكون خالية من أي شك وتوفر قناعة القاضي بدرجة اليقين والثقة التامة. يعد الشكل والصحة القانونية للأدلة مهمة جدًا للحكم بالإدانة.

يقوم القاضي بفحص الدليل الإلكتروني كقاعدة عامة، ويتطلب ذلك مناقشته مع الأطراف المعنية لتوضيحه وفهمه بشكل صحيح. يمكن للقاضي عرض الأدلة الإلكترونية المحصلة مباشرة، سواء على الشاشة الخاصة بالحاسوب أو أجهزة أخرى، أو عرض النتائج المعالجة بواسطة الحاسوب.

من خلال استناده إلى المعلومات الإلكترونية المقدمة وتصوراته المحتملة، يمكن للقاضي تقييم قوة استدلال هذه الأدلة بشأن ارتكاب الجريمة الإلكترونية من عدمها بواسطة شخص محدد. يعتمد ذلك على قدرة الأدلة على تأكيد الروابط الضرورية بين الجريمة والمتهم، وتوفر المعلومات اللازمة للحكم بالإدانة.

يجب على القاضي أن يتبع إجراءات قانونية صارمة لضمان شرعية وصحة الأدلة الإلكترونية وتجنب أي انتهاكات للحقوق الأساسية للمتهم. يتطلب ذلك استنادًا إلى النظام

[1] زيدان زبيخة، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، الجزائر، ،2011 ص173

القانوني ومبادئ العدالة، بحيث يتم ضمان حق المتهم في الدفاع وتقديم أدلته والتحقيق في الأدلة بطريقة عادلة وشفافة[1].

ثالثا: مناقشة الدليل الالكتروني:

يعتمد هذا المبدأ على أن القاضي لا يمكنه الاعتماد على أي أدلة تثبت ارتكاب الجريمة إلا إذا تم طرحها ونقاشها بحرية في جلسات المحاكمة أمام جميع الأطراف المعنية. وبناءً على ذلك، فإن الأدلة المتعلقة بجرائم الحاسوب والإنترنت، سواء كانت مطبوعة أو عُرضت على شاشة الحاسوب أو كانت في شكل وسائط تخزين مثل الأشرطة الممغنطة أو الأقراص الضوئية أو الأفلام المصغرة، يتم مناقشتها ومنازعتها خلال جلسات المحاكمة كأدلة قابلة للاعتماد أمام المحكمة. وبناءً على ذلك، يجب أن يتم عرض كل دليل تم الحصول عليه من خلال تكنولوجيا المعلومات مباشرة أمام القاضي خلال الجلسة، وليس من خلال الملف القضائي في مرحلة التحقيق الأولية. وتُطبق هذه القواعد على جميع الأدلة التي تنشأ عن طريق أجهزة الحاسوب.

تهدف هذه القواعد إلى ضمان أن يتم تقديم الأدلة الرقمية بشكل شفاف ومفهوم في سياق المحاكمة وأمام الأطراف المعنية، وبهذا يمكن للمدافعين والمدعين العامين أن يقدموا حججهم ومنازعاتهم ويساهموا في تقدير صحة تلك الأدلة. يتم ضمان حقوق الدفاع والمحاكمة العادلة من خلال توفير الفرصة للطرفين للتعامل مع الأدلة ومنازعتها بشكل كامل.

هذه القواعد تعكس التحديات التي تواجه المحاكم في التعامل مع الأدلة الرقمية وتحديد صحتها وقيمتها الإقناعية، فمع التكنولوجيا المتقدمة وتعقيد الأنظمة الرقمية، يصبح من الضروري أن تتبنى القوانين والإجراءات القضائية اللازمة لتأمين الاعتمادية والموثوقية للأدلة الرقمية ولحماية حقوق الأفراد في العدالة الجنائية.[2]

---

[1] زبيحة نور الهدى، الإثبات الجنائي في الجرائم الإلكترونية، مذكرة تكميلية لنيل شهادة الماستر، شعبة الحقوق، تخصص قانون جنائي للأعمال، قسم الحقوق، كلية الحقوق و العلوم السياسية، جامعة العربي بن مهيدي، أم البواقي، 2015-2016، ص55

[2] لعمريوي ليلى، مرجع سابق، ص69

الفرع الثاني حجية الدليل الالكتروني في الإثبات

تشهد أنظمة الإثبات اختلافًا بالنسبة لقبول وتقدير الأدلة الرقمية في القوانين. في النظام اللاتيني، تُعتبر حرية الإثبات والاقتناع مبدأًا هامًا، وبالتالي لا تثير سلطة القاضي الجنائي صعوبات في قبول الأدلة الرقمية لإثبات الجرائم الإلكترونية. يُسمح للقاضي الجنائي في هذه الأنظمة باستخدام الأدلة الرقمية لإثبات الجريمة بشكل عام، وخاصة في التشريع الفرنسي.

أما في النظم الأنجلوسكسونية، فإن المشرع يحدد أدلة الإثبات وقيمتها الإقناعية. ونتيجة لذلك، يقتصر دور القاضي في هذه الأنظمة على الاعتماد على أنواع محددة من الأدلة المنصوص عليها في النظام، دون الحاجة إلى إقناع القاضي بصحة تلك الأدلة. تتبع بلدان مثل إنجلترا وبريطانيا هذا النظام.

أما في الأنظمة ذات الاتجاه المختلط، التي تجمع بين النظامين اللاتيني والأنجلوسكسوني، فإن القانون يحدد أدلة معينة لإثبات بعض الوقائع، أو يشترط شروطًا للدليل في بعض الحالات، أو يمنح القاضي حرية في تقدير الأدلة القانونية. مثال على ذلك هو القانون الإجرائي الياباني.

يتنوع نهج التعامل مع الأدلة الرقمية بين هذه الأنظمة المختلفة، ويرجع ذلك إلى اختلاف القوانين والتشريعات التي تنظمها. ومع تزايد الجرائم الإلكترونية واعتماد التكنولوجيا في حياتنا اليومية، فإنه من المهم أن تستمر الأنظمة القانونية في مواكبة التطورات وتحديث تشريعاتها لتمكين قبول وتقدير الأدلة الرقمية بطرق عادلة وموضوعية.[1]

الفرع الثالث: موقف المشرع الجزائري من الدليل الالكتروني

نظام الإثبات في القانون الجزائري يتبع مبدأ الإثبات الحر، وفقًا للمادة 212 من قانون الإجراءات الجزائية الجزائري. تنص هذه المادة على أنه يُسمح بإثبات الجرائم باستخدام أي

[1] هلال عبد الله أحمد، حجية المخرجات الكمبيوترية في الإثبات الجنائي، الطبعة الثانية، دار النهضة العربية، مصر، 2007،ص 62

وسيلة من وسائل الإثبات، ما لم ينص القانون على خلاف ذلك. وبالتالي، يتم ترك قرار قبول الأدلة وتقديرها لتقدير القاضي الجزائري بناءً على اقتناعه الخاص[1].

ويعني هذا أن القاضي لديه حرية واسعة في تقدير قوة الأدلة المقدمة أمامه واستناده إلى اقتناعه الشخصي في صدور حكمه. ولكن يجب أن يتم الالتزام بالقواعد القانونية وإجراءات المحاكمة العادلة أثناء تقدير الأدلة واتخاذ القرارات[2].

بالفعل، استنادًا إلى نص المادة 212 التي ذكرتها، يتضح أن المشرع الجزائري قد أذن بإثبات الجرائم باستخدام جميع وسائل الإثبات القانونية المشروعة، بما في ذلك الدليل الإلكتروني. ومنح القاضي الجزائي حرية تقدير الدليل وفقًا لاقتناعه الشخصي. ويمكننا أن نقول إذاً أن المشرع الجزائري اتبع نهج المشرع الفرنسي في الاعتراف بالدليل الإلكتروني كأدلة أخرى للإثبات الجنائي. وبناءً على ذلك، يمتلك القاضي الجنائي سلطة تقديرية تشمل الأدلة العلمية الحديثة، بما في ذلك الدليل الإلكتروني[3]. ومن الجدير بالذكر أنه يجب أن يتم احترام متطلبات المحاكمة العادلة وحقوق المتهم في جميع الأحوال، بما في ذلك توفير الفرصة المناسبة للدفاع وتقديم الأدلة المناسبة. وينبغي أن يتم التعامل مع الدليل الإلكتروني بنفس الاحترام والموضوعية التي يتم التعامل بها مع الأدلة الأخرى في إطار المحاكمة الجنائية.

بناءً على النظام القضائي الجزائري الذي يتبع النظام الحر، يمكن القول إن الدليل الرقمي لا يثير أي شكوك بشأن مشروعيته في النظام القضائي الجزائري. في هذا النظام، يتعين على القاضي الجزائي الامتثال للقواعد العامة المتعلقة بقبول الأدلة الجنائية، سواء كانت تلك الأدلة عبارة عن محاضر، أو نتيجة تفتيش، أو اعتراض على المراسلات، أو

---

[1] أمر رقم 66-156 المؤرخ في 18 صفر 1836 الموافق ل08 يونيو ،1966 المتضمن قانون الإجراءات الجزائية، مرجع سابق

[2] الخال إبراهيم، بن مالك أحمد، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، العدد ،01 جامعة تمنراست، الجزائر، ،2021 ص111.

[3] الخال إبراهيم، بن مالك أحمد، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، العدد ،01 جامعة تمنراست، الجزائر، ،2021 ص111-112.

خبرات فنية تتعلق بمعاينة أو فحص الأدلة الجنائية الرقمية المتعلقة بأجهزة الحاسوب وملحقاتها.

وبموجب هذه القواعد العامة، يتعين على القاضي الجنائي أن يحترم حقوق المتهم ويمنحه فرصة مناسبة للدفاع وتقديم الأدلة الملائمة. وبالمثل، يجب أن يتم التعامل مع الأدلة الجنائية الرقمية بشكل موضوعي وفقًا للمعايير القانونية المعمول بها في المحاكمة الجنائية.

بصفة عامة، يمكننا أن نستنتج أن النظام القضائي الجزائري يقبل ويعترف بالدليل الرقمي ويتعامل معه بنفس الطريقة التي يتعامل بها مع الأدلة الأخرى في سياق المحاكمة الجنائية. وذلك يؤكد التزام النظام القضائي الجزائري بالعدالة والمبادئ القانونية في معالجة الأدلة الجنائية المتعلقة بالتكنولوجيا الرقمية.

خاتمة

خاتمة

لقد سعينا من خلال هذه الدراسة إلى استكشاف موضوع حديث ومهم، وهو الحماية الجنائية للمستهلك الإلكتروني. ومن خلال التحليل والبحث الذي أجريناه في هذه المذكرة، تبين لنا أهمية هذا الموضوع في مجال الدراسات القانونية. فقد بدأت الدول الأوروبية والأمريكية توليه اهتمامًا كبيرًا، وتكرس له عناية خاصة. وقد سعى المشرع الجزائري جاهدًا لتحقيق الحماية الجنائية للمستهلك الإلكتروني في قدر المستطاع.

التشريع الجزائري يهتم بتوفير حماية للمستهلك الإلكتروني في إطار التجارة الإلكترونية. يتضمن التشريع تعريفًا للمستهلك الإلكتروني والتجارة الإلكترونية، ويحدد نطاق الحماية المطلوبة للمستهلك الإلكتروني في مجال الجرائم التي تؤثر على سلامته وأمانه.

في الفصل الأول، يتم دراسة العديد من الجرائم التي تستهدف المستهلك الإلكتروني وسلامته، مثل جرائم الاعتداء على نظام معالجة البيانات الآلية. يتم التركيز على حماية سلامة البيانات وضمان عدم تعرضها للاختراق أو الاستغلال غير المشروع.

بالإضافة إلى ذلك، يتم دراسة بعض الجرائم المحددة في قوانين خاصة تتعلق بالتجارة الإلكترونية والمستهلك الإلكتروني. يهدف ذلك إلى توفير إطار قانوني لمكافحة الجرائم المرتكبة ضد المستهلك الإلكتروني وتحميل المرتكبين المسؤولية القانونية.

وفي سياق حماية المستهلك الإلكتروني في إطار التعاقد الإلكتروني، تُدرس بيانات المستهلك الشخصية ونطاق حمايتها من الاعتداءات. يعتبر انتهاك حرمة الحياة الخاصة للمستهلك واختراق خصوصيته في استخدام البيانات الشخصية جريمة تستحق الحماية والمساءلة القانونية.

تهدف هذه الدراسات والتشريعات إلى تعزيز الثقة في التجارة الإلكترونية وضمان حماية المستهلك الإلكتروني من الاحتيال والاعتداءات وسرقة الهوية. تهدف السياسات والتشريعات إلى توفير بيئة

آمنة وموثوقة للمستهلكين الإلكترونيين وتعزيز التعاملات الإلكترونية في الجزائر.

تم التركيز على تعزيز الحماية والسلامة فيما يتعلق بالبيانات المتعلقة بالتوقيع الإلكتروني، وذلك بهدف منع استخدامها في أغراض غير مشروعة أو التلاعب بها. تم تطوير آليات فعالة للتحقق من صحة التوقيعات الإلكترونية، مثل تقنيات التشفير والتوثيق القوية. وبموجب التشريعات الجزائرية، يعتبر تزوير التوقيع الإلكتروني أو استخدامه بطرق غير قانونية جرائم يعاقب عليها القانون.

يتجلى الأهمية البالغة للتوقيع الإلكتروني بالنسبة للمستهلك الإلكتروني في ضمان صحة وموثوقية المعاملات الإلكترونية وتأمين بياناته الشخصية. فهو يعد وسيلة فعالة للتحقق من هوية الأطراف المشاركة والتأكد من صحة التوقيعات والتزامها بالتعاقدات الإلكترونية. بالتالي، فإن تعزيز الحماية للبيانات المتعلقة بالتوقيع الإلكتروني يسهم في بناء الثقة والمصداقية في التجارة الإلكترونية ويعزز حقوق ومصالح المستهلك الإلكتروني.

في الفصل الثاني، قمنا بمناقشة الحماية الإجرائية للمستهلك الإلكتروني. تم التركيز في هذا الفصل على وسائل الإثبات الإلكترونية، سواء كانت تقليدية أو حديثة، ودرس قيمتها وأهميتها في عملية الإثبات.

تم استعراض وسائل الإثبات الإلكترونية التقليدية، مثل البريد الإلكتروني والمستندات الرقمية، وتم مناقشة كيفية استخدامها كأدلة قانونية في الإثبات. كما تم تناول الوسائل الإثباتية الحديثة، مثل تسجيلات الشبكة وسجلات الدخول والمعلومات المتعلقة بالمعاملات الإلكترونية.

تم تسليط الضوء على قيمة هذه الوسائل الإثباتية الإلكترونية في تقديم الدليل وإثبات الحقائق المتعلقة بالمستهلك الإلكتروني. حيث تعزز هذه الوسائل القدرة على توثيق التفاصيل الهامة وتسجيل البيانات وتقديمها كدليل قوي وقابل للتحقق في النزاعات والمنازعات القانونية.

بالتالي، فإن دراسة وسائل الإثبات الإلكترونية في هذا الفصل تعزز حماية المستهلك الإلكتروني وتسهم في توفير آليات فعالة لإثبات حقوقه ومطالبه في بيئة الاتصالات الإلكترونية.

ومن خلال دراستنا، نستطيع القول بأن المشرع الجزائري قد أحرز تقدمًا كبيرًا في حماية المستهلك الإلكتروني وتعزيز خدمات التجارة الإلكترونية من خلال القانون الأخير رقم 18-05. وإلى جانب القواعد التي تنظم المستهلك بشكل عام، فإن هذا القانون يعد خطوة هامة في تعزيز الحماية وتحسين البيئة القانونية للتجارة الإلكترونية.

ومع ذلك، فإنه يجب أن نلاحظ أن هذه الإجراءات لا تزال غير كافية لمعالجة جميع انتهاكات المستهلك الإلكتروني، وخاصة في ظل انتشار واسع للتجارة الإلكترونية عبر وسائط الإنترنت. فالتجارة الإلكترونية تعتبر مجالًا غير متحكم فيه بسبب تعقيداتها وتطوراتها السريعة، وبالتالي فإن آليات المراقبة والرقابة الحالية قد تكون غير كافية للتعامل مع تلك التحديات.

على الرغم من وجود قواعد موضوعية وإجرائية وضعها المشرع الجزائري، إلا أن فعاليتها في حماية المستهلك الإلكتروني تعاني من العديد من النقائص. وعلى إثر ذلك، توصلنا إلى مجموعة من النتائج التي تستحق الانتباه.وهي

1- بظهور التجارة الالكترونية أصبح لدينا ما يسمى بالمستهلك الالكتروني، الذي أوجب حمايته من الاعتداء الواقع عليه
2- يمكن تعريف المستهلك الإلكتروني على أنه أي شخص طبيعي أو معنوي يقوم بشراء سلعة عبر وسائل الاتصال الإلكترونية، وذلك للاستخدام النهائي.
3- تتضمن مجموعة الجرائم التي يتعرض لها المستهلك الإلكتروني عدة أنواع، ومن بينها جرائم النصب والغش والاحتيال، فضلاً عن جرائم الاعتداء على بياناته الشخصية.
4- للكشف عن الجرائم التي تُرتكب ضد المستهلك الإلكتروني، هناك إجراءات يجب اتخاذها للكشف عن الحقائق المتعلقة بهذه الجرائم. ومن بين هذه الإجراءات، نجد التفتيش والمعاينة، التي يقوم بها سلطة مختصة وهي الضبطية القضائية. تكون هذه السلطة مسؤولة عن مباشرة التحقيقات وجمع الأدلة المادية والمعلوماتية لكشف الجرائم وتحديد المسؤولين عنها.

5- للكشف عن الجرائم التي تُرتكب ضد المستهلك الإلكتروني، يتوفر العديد من وسائل الإثبات، بما في ذلك الدليل الإلكتروني، الذي يُعتبر دليلاً علميًا يساعد في كشف الحقيقة. بالإضافة إلى ذلك، يمكن الاستفادة من الوسائل التقليدية الأخرى المتاحة للتحقق وجمع الأدلة، مثل التحقيقات الشرطية والشهادات والشهود والتفتيش وغيرها. يجب استخدام هذه الوسائل بشكل متكامل لضمان كشف الجرائم وتأمين العدالة.

بناءً على النتائج التي توصلنا إليها، لدينا مجموعة من الاقتراحات التي يمكن أن تساهم في تعزيز حماية المستهلك الإلكتروني وهي :

- يتطلب تعزيز حماية المستهلك الإلكتروني ضرورة تدخل المشرع لإصدار وتنفيذ قوانين جديدة تغطي جميع السلع والخدمات دون استثناء عبر وسائط الاتصال الإلكترونية.
- يُوصى بإجراء تعديلات على قانون حماية المستهلك، تُخصص نصوصًا خاصة لحماية المستهلك الإلكتروني من مخاطر التعاقد الإلكتروني التي قد يتعرض لها.
- إنشاء جهاز أمني متخصص مهتم بالتحقيق والتحري في مجال الجرائم الإلكترونية.
- تعديل نصوص الإثبات الجنائي لاستحداث طرق جديدة للبحث المعلوماتي، بهدف تعقب المجرمين الذين ينتهكون قواعد النزاهة التجارية. يجب أيضًا ابتكار طرق تتماشى مع الطبيعة الخاصة لهذا النوع من الجرائم. بالإضافة إلى ذلك، يُنصح بتعزيز استخدام التصديق الإلكتروني كوسيلة لضمان سلامة المستهلك وحمايته.
- تشديد العقوبات نظرًا للطبيعة المتزايدة للمخاطر التي يتعرض لها المستهلك الإلكتروني يوميًا، وخاصة في حالات الاعتداء المتكررة. يُلاحظ أن المجرمين الإلكترونيين يستخدمون أدوات تكنولوجية متقدمة، مما يتطلب وجود آليات رقابية متطورة لمراقبة تصرفاتهم في الفضاء الإلكتروني الذي لا يعرف حدودًا.

ولهذا السبب، يجب وضع نصوص قانونية جديدة تضمن حماية أكثر فعالية للمستهلك الإلكتروني.

تواجه حماية المستهلك بشكل عام، وحمايته من الجانب الجنائي بشكل خاص، تحديات كبيرة في تحقيق أهدافها المطلوبة. يعود ذلك إلى نقص الوعي لدى المستهلكين وعدم كفاية الآليات القانونية الحالية في توفير حماية فعالة للمستهلك الإلكتروني. بالإضافة إلى ذلك، فإن التطور التكنولوجي السريع والعصر الرقمي يتجاوز قدرة القوانين الحالية على مواكبة التحديات المتعلقة بحماية المستهلك الإلكتروني.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

1-باللغة العربية:

أولا: الكتب

1- ابراهيم احمد،البسطويسي،المسؤولية عن الغش في السلع، دراسة بين الفقه الاسلامي والقانون التجاري، دار الكتب القانونية، القاهرة،2011.

2- لحسين بن شيخ، مذكرات في القانون الجزائي الخاص، الطبعة 5، دار هومة ، الجزائر، 2006.

3- بن سعيد لزهر، النظام القانوني لعقود التجارة الالكترونية، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014.

4- بودالي محمد، حماية المستهلك في القانون المقارن دراسة مقارنة مع القانون الفرنسي، دارالكتاب الحديث، الجزائر، 2006.

5- بودالي محمد، شرح جرائم الغش في بيع السلع والتدليس في المواد الغذائية والطبية ،ديوان المطبوعات الجامعية، الجزائر،2006.

6- بوسقيعة احسن، الوجيز في القانون الجزائي العام ، الطبعة 14، دار هومة،الجزائر، 2014.

7- أحسن بوصقيعة ، الوجيز في القانون الجنائي العام الديوان الوطني للأشغال التربوية ، الجزائر 2002.

8- عبد الفتاح حجازي. الدليل الجنائي والتزوير في جرائم الكمبيوتر و الإنترنت ، دار الكتب القانونية القاهرة ، 2002.

9- بيومي حجازي عبد الفتاح، التجارة الالكترونية وحمايتها القانونية، الكتاب الثاني، دار الكتب القانونية، مصر، 2007.

10- ثروت عبد الحميِّد، التوقِّيع الاكتروني، دار الاسكندرية، مصر، ،2007.

11- جهاد رضا الحبشة، الحماية الجزائية لبطاقة الوفاء، دار اثقافة، عمان، 2008.

12- رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، جامعة سعد حلب ، البليدة، (د،س)

13- سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، 2012.
14- عبد الله ماجد العكايلة، الوجيز في الضبطٌية القضائية، دار الثقافة للنشر و التوزٌيع، ألاردن، ،2010.
15- علي جبار الحسيناوي، جرائم الحاسوب والانترنات، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009.
16- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية، القاهرة، 1999.
17- فادي محمد عماد الديٌن توكل، عقد التجارة الالكترونٌية، منشورات حلبً الحقوقٌية، لبنان، ،2010.
18- مطر عصام عبد الفتاح، التجارة الالكترونية العربية والاجنبية،دار الجامعة الجديدة،مصر ،2015.
19- منيرمحمد الحنبيهي ،منير محمد الجنبيهي، ممدوح محمد الحنبيهي ، جرابم الأنترنت و الحاسب آلي ووسائل مكافحتها، دار الفكر الجامعي، الاسكندرية، ،2005.
20- هلال عبد الله أحمد عبد الله ، حجية المخرجات الكمبيوترية في الإثبات الجنائي، الطبعة الثانية، دار النهضة العربية، مصر، 2007.

ثانيا: الأطروحات والمذكرات الجامعية

أ- الاطروحات

1- امين عبد الحميد، استراتيجية مكافحة جرائم الحاسوب الالي، دراسة مقارنة،رسالة لنيل شهادة الدكتورته، اكاديمية الشرطة،2012.
2- محمد فتحي عيد،الانترنات ودوره في انتشار المخذرات،اكاديمية نايف العربية للعلوم الامنية، الرياض، 2003.

3-نبيلة هبة هروال، جرائم الانترنات دراسة مقارنة، رسالة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، 2013-2014.
4- شنين صالح، الحماية الجنائية للتجارة الإلكترونية(دراسة مقارنة)، رسالة لنيل شهادة دكتوراه في القانون الخاص، كلّة الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2012/2013.
5-قطاف إسماعيل، العقود الإلكترونية و حماية المستهلك، بحث لنيل شهادة الماجُستر، فرع عقود و مسؤولُية، كلّية الحقوق، جامعة الجزائر، الجزائر، 2005/2006.
6-مخلوفي عبد الوهاب، التجارة الالكترونية عبر الانترنات، أطروحة لنيل شهادة دكتوراه في الحقوق، تخصص قانون الأعمال ، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة.

ب- مذكرات

أولا: مذكرات المتاجستير

1- بن عقون حمزة، السلوك الاجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجيستر في علم الاجرام وعلم العقاب، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2011-2012.

2- منال بوروح، ضمانات حماية المتهم في ظل القانون 09-03، اطروحة لنيل شهادة الماجستير، فرع قانون حماية المستهلك والمنافسة، كلية الحقوق، جامعة يوسف بن خدة، الجزائر 1، 2015.
3- خلوي عنان نصيرة،الحماية القانونية للمستهلك عبر الانترنات، رسالة ماجستير، جامعة مولوج معمري، تيزي وزو، 2013.
4- غربوج حسام الدين، حماية المستهلك من الممارسات التجارية غير النزيهة في التشريع الجزائري، اطروحة مقدمة لنيل شهادة الدكتوراه في الحقوق تخصص قانون الاعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2017-2018.

ثانيا: مذكرات الماستر

1- زبيحة نور الهدى، الإلثبات الجنائي في الجرائم الإلكترونية، مذكرة تكميلية لنيل شهادة الماستر، شعبة الحقوق، تخصص قانون جنائي للأعمال، قسم الحقوق، كلية الحقوق و العلوم السياسية، جامعة العربي بن مهيدي، أم البواقي ،2015-2016.

2- قليل زوبيدة، الاشهار الإلكتروني في ظل قانون 18-05، مذكرة مكملة لنيل شهادة الماستر، تخصص قانون اعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي،2020.

3- لعمريوي ليلى، الحماية الجنائية للمستهلك الالكتروني، مذكرة لنيل شهادة الماستر في القانون، قسم القانون، تخصص قانون جنائي وعلوم جنائيبة، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.

ثالثا: المقلات والمجلات

1- أبوديار مليكة، الإثبات الجنائي في الجرائم الالكترونية، المجلة القانونية للابحاث القانونية، عدد2، تونس، 2018.

2- الخال إبراهيم، بن مالك أحمد، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، العدد ،01 جامعة تمنراست، الجزائر، ،2021.

3- العايب سامية، عرابة منال، الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني، مجلة هيرودوت للعلوم الانسانية والاجتماعية. العدد 5، كلية الحقوق والعلوم السياسية،جامعة 8 ماي 1945،الجزائر، 2021.

4- امجد خليل حمودة، الوسائل الحديثة لاثبات الجرائم التي ترتكب بواسطة الاجهزة الالكترونية، مجلة جامعة الإزهر، العدد 19، غزة، 2016.

5- بن عودة نبيل نوار ،محمد "الصلاحيات الحديثة للضبطية القضائية للكشف ملاحقة مرتكبي الجرائم المتعلقة بالتمييز و خطاب الكراهية" التسرب الالكتروني نموذجا"، مجلة الأكاديمية للبحوث في العلوم الاجتماعية، العدد 03، مستغانم،2020

6- مجدوب نوال،حماية المستهلك جنائيا من جريمة الخداع في عملية تسويق المواد الغذائية، مجلة دفاتر السياسية والقانون، العدد15،كلية الحقوق والعلوم السياسية،جامعة ابو بكر بلقايدن تلمسان،2016.

7- مجدوب نوال، الحماية الجنائية للمستهلك الالكتروني وفكرة الأمن الاقانوني، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 7، العدد1، ،2022.

8- معكوف أسماء، "الحماية الجنائية للمستهلك أثناء التعاقد الالكتروني"، مجلة البحوث في العقود و قانون الأعمال العدد الرابع، قسنطينة 2018.

رابعا: المقالات الإلكترونية

1- بلارو كمال الحماية الجنائية للمستهلك الالكتروني في ظل التشريع الجزائري، مجلة البحوث في العقود وقانون الأعمال، العدد السابع،جامعة الاخوة منتوري ، قسنطينة1، 2019، تم الاطلاع عليه من الموقع التالي https://www.asjp.cerist.dz/en/article/69292 يوم 11 جوان 2023

خامسا: المطبوعات الجامعية

1- طباش عز الدين، شرح القسم الخاص من قانون العقوبات (جرائم ضد الأشخاص والأموال، السنة أولى ماستر تخصص قانون جنائي و علوم جنائية، قسم القانون الخاص كلية الحقوق و العلوم السياسية، جامعة عبد الرحمان ميرة بجاية، 2020-2021.

سادسا: أشغال الملتقيات

1- جافلي حسين، الحماية الجنائية للمستهلك من الاشهار الالكتروني في التجارة الالكترونية، الملتقى الوطني حول" الاطار القانوني لممارسة التجارة الالكترونية على ضوء قانون 10-05 "، يوم 8 اكتوبر 2019، جامعة العربي التبسي، تبسة.

سابعا: النصوص القانونية

أ- النصوص التشريعية:

1-أمر رقم 6-5 المؤرخ في 18 صفر 1836 الموافق ل08 يونيو 1966، الذي يتضمن قانون الإجراءات الجزائية، ج.ر، عدد48، صادر في 10 يونيو 1966،معدل و متمم.

2- أمر رقم 66-15 مؤرخ في 08 جوان ،1966 بتضمن قانون العقوبات، ج.ر، عدد 49 ، صادر في 11 جوان 1966 معدل و متمم.

3- أمر رقم 75 مؤرخ في 20 رمضان 1396 الموافق ل 26 سبتمبر سنة 1975، يتضمن القانون المدني، ج . ر ، عدد 78 ، صادر في 24 رمضان 1395 الموافق ل 30 سبتمبر 1975 معدل و متمم.

4- أمر رقم 03-211 المؤرخ في 25-08-2003 ، يتعلق بالنقد و القرض، ج.ر عدد 2 صادر في 26-08-2003، معدل و متمم -52 قانون رقم 05-02 مؤرخ في 06 فبراير 2005.

5- قانون رقم 05-02 مؤرخ في 06 فبراير 2005 معدل و متمم للأمر رقم 75-59 المؤرخ في 26 سبتمبر 1975 المتضمن القانون التجاري، ج.ر عدد 11، المؤرخة في 09-02-2005.

6- قانون رقم 09-03 مؤرخ في 29 صفر 1430 الموافق ل 25 فبراير 2009 يتعلق بحماية المستهلك وقمع الغش ج.ر عدد 15 مؤرخ في 08 مارس 2009

7- قانون رقم 05-01 المؤرخ في 13 جمادى الأولى عام 1426 الموافق ل 20 يونيو 2005 المعدل والمتمم للأمر رقم 75-8 المؤرخ في 26 سبتمبر 1975، المتضمن القانون المدني، ج.ر عدد 44 ، صادر في 20 يونيو 2005.

8- قانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها، ج.ر،عدد45،صادر في 25 شعبان1430الموافق ل16غشت2009.

ب- التصوص التنفيذية:

1- مرسوم تنفيذي رقم 07/162 المؤرخ في 30-05-2007، يعدل و يتمم المرسوم التنفيذي رقم 01-123 المؤرخ في 09-05-2001 المتعلق بنظام الاستغلال المطابق على كل نوع من أنواع الشبكات بما فيها الأسلاك الكهربائية و على مختلف

المواصلات السلكية و اللاسلكية، ج.ر عدد 37 ، صادر بتاريخ 07-06-2007

2- باللغة الفرنسية:

1- GEAN Clais, AULOY Frank steinmetz, droit de la consommation, 5ém éd, DOLLAZ Montpellier, France, 2003, p.07.

فهرس المحتويات

إهداء

الشكر والتقدير

قائمة المختصرات

العنوان الصفحة

ملخص

تسبب التطور التكنولوجي والتبادلات التجارية في ظهور مفهوم المستهلك الإلكتروني كجزء أساسي في عملية التعاقد. وعلى الرغم من أن المستهلك الإلكتروني غالبًا ما يكون غير متمرس في هذا المجال، إلا أن هذا التطور ترافق معه زيادة في حوادث الاعتداءات على المستهلك الإلكتروني وتعرضه للأذى. لمواجهة هذا الوضع، قام المشرع الجزائري بتدخل ووضع قوانين جديدة، مثل قانون حماية المستهلك ومكافحة الغش رقم 09-03 وقانون التجارة الإلكترونية رقم 18-05. وقد ساهمت هذه القوانين في تعزيز الحماية الجنائية للمستهلك الإلكتروني، حيث يتم تجريم أعمال الاحتيال والتلاعب التي تستهدف المستهلك الإلكتروني، مثل الغش والاعتداء على بياناته الشخصية. بالإضافة إلى ذلك، تم توفير إجراءات قانونية للحماية تتمثل في إجراءات يتخذها الجهاز القضائي المختص، مثل الضبطية القضائية، التي تتابع وتكافح هذه الجرائم وتقوم بإثباتها باستخدام جميع الوسائل المتاحة لتحديد المتسبب فيها.

Le résumé

Le développement technologique et les échanges commerciaux ont entraîné l'émergence du concept de consommateur électronique en tant qu'élément essentiel du processus contractuel. Bien que le consommateur électronique soit souvent inexpérimenté dans ce domaine, cette évolution s'accompagne d'une augmentation des attaques et des préjudices subis par les consommateurs électroniques. Pour faire face à cette situation, le législateur algérien est intervenu en promulguant de nouvelles lois, telles que la Loi 09-03 sur la protection du consommateur et la répression des fraudes, ainsi que la Loi 18-05 sur le commerce électronique. Ces lois ont contribué à renforcer la protection pénale des consommateurs électroniques en criminalisant les actes de fraude et de manipulation qui ciblent ces consommateurs, tels que la fraude et les atteintes à leurs données personnelles. De plus, des mesures légales de protection ont été mises en place, notamment par le biais de procédures engagées par l'autorité compétente, telle que la police judiciaire. Celle-ci enquête sur ces crimes, le combat et les prouve en utilisant tous les moyens disponibles pour identifier les auteurs.