الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة سعيدة الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم الحقوق

الجرائم الالكترونية الماسة بالمعاملات التجارية في ضوء التشريع الجزائري والاتفاقيات الدولية

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص قانون الاعمال

من إعداد الطالبة:

بوعوج فاطمة الزهراء

تحت إشراف الأستاذ(ة):

أ.د عز الدين غالية

الدكتور بوشنتوف بوزيان	أستاذ(ة): التعليم العالي	جامعة سعيدة_الدكتور مولاي الطاهر	رئيساً
الدكتور عز الدين غالية	أستاذ(ة): التعليم العالي	جامعة سعيدة _ الدكتور مولاي الطاهر	مشرفاً ومقرراً
الدكتور حمادو فاطيمة	أستاذ(ة): محاضر	جامعة سعيدة_الدكتور مولاي الطاهر	عضواً

السنة الجامعية: 2025-2026

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة سعيدة الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم الحقوق

الجرائم الالكترونية الماسة بالمعاملات التجارية في ضوء التشريع الجزائري والاتفاقيات الدولية

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص قانون الاعمال

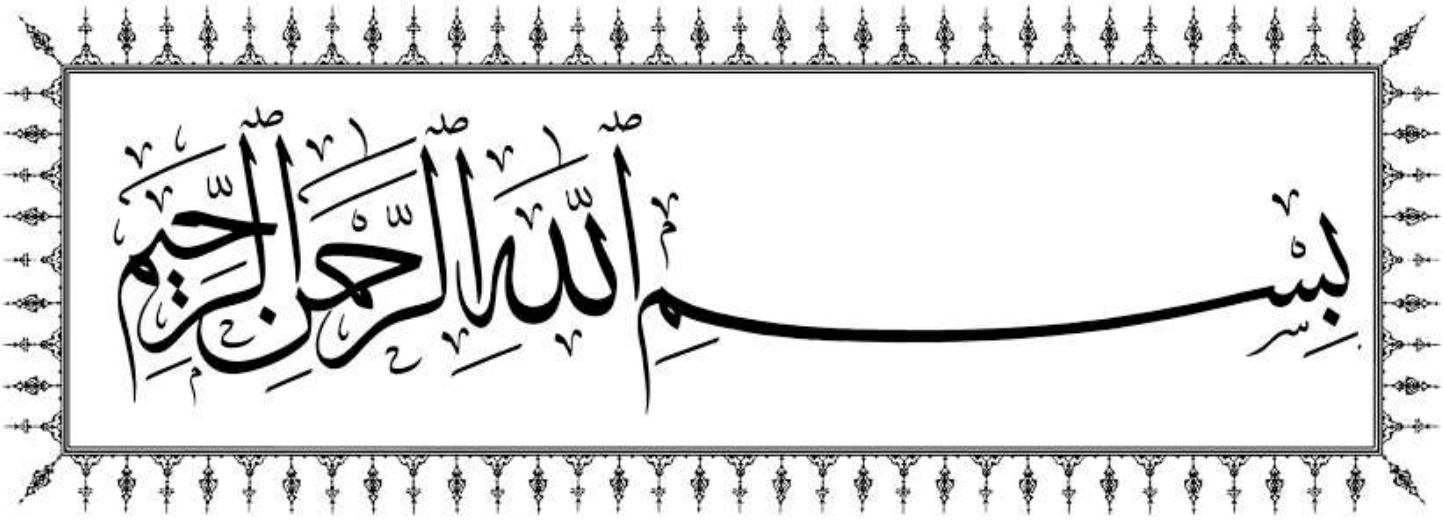
من إعداد الطالبة:

بوعوج فاطمة الزهراء

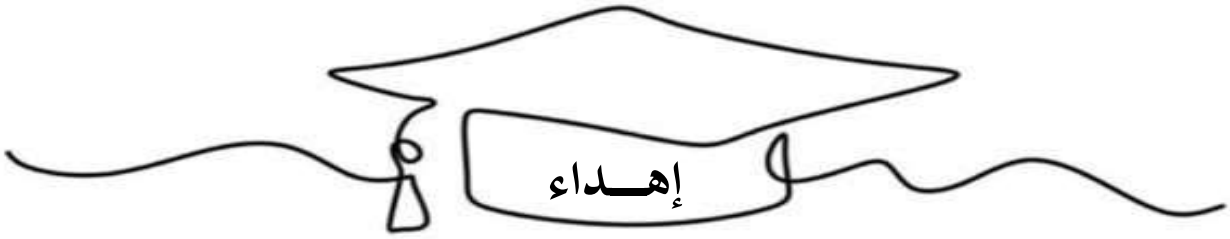
تحت إشراف الأستاذ(ة):

أ.د عز الدين غالية

السنة الجامعية: 2025-2026



(فَرِحِينَ بِمَا آتَاهُمُ اللَّهُ مِنْ فَضْلِهِ)



إلى روح أبي إلى ذلك الغائب الحاضر في كل خطوة إلى من تمنيت لو كان هنا ليرى ثمرة تعبي رحلت يا أبي، لكنك لم ترحل من قلبي فكل نجاح أصل إليه أبحث فيه عن نظرة فخر من عينيك فلا أجدها، رحمك الله رحمةً واسعة، وجعل هذا العمل نورًا لك في قبرك.

إلى جدي الحبيب

إلى من أخذ بيدي حين فقدت أبي، إلى من عوضني حنانًا وسندا وقوة، وكان لي الأب بعد رحيل الأب

وقفت بجانبي حين ضعفت، وحملت عني ما عجزت عنه

رحمك الله يا جدي، وجعل كل ما قدمته لي في ميزان حسناتك

هذا العمل بعض من جميلك الذي لا يوفى.

إلى أمي

إلى تلك التي أخفت ألمها لتقويني إلى من حملت عني ثقل الحياة وأنا أعجز إلى قلب لم يعرف الراحة لانه لم يبخل علي يوما بالحب والصبر

إلى أختي الوحيدة أمينة إلى من كانت لي أختا وسندا وأمانًا، شاركتني لحظات الانكسار قبل الفرح، وكانت دائما اليد التي ترفعني حين أتعب وجودك في حياتي نعمة لا أستطيع وصفها.

إلى صديقاتي أحلام ،إكرام،وئام اللواتي لم يتركني إلى من بقين معي حين ضاقت بي الدنيا حين خذلتني الأيام، وجدتهن سندًا لا يميل كنتن الضوء في عتمتي، والدفء في قسوة أيامي.

إلى كل من كان لي دعاء في الغيب

أهدي هذا العمل، ليس كإنجاز فقط بل كحكاية تعب، وصبر، ودموع لم ترى،راجيةً من الله أن يجعل فيه جبرًا لما انكسر في داخلي، وتوفيقا لي

شكر وتقدير

الحمد لله عز وجل حمدًا كثيرًا طيبًا مباركًا فيه، الحمد لله الذي بنعمته تتم الصالحات، والذي وفقني ومنحني القوة والصبر لإتمام هذا العمل، فما كان لي أن أصل إلى هذه اللحظة لولا فضله ورحمته وتوفيقه

أتقدم بخالص الشكر والامتنان إلى أمي الغالية، التي كانت النور الذي يضيء طريقي، والسند الذي أستند عليه في كل تعثر، فجزاها الله عني خير الجزاء

كما أتوجه بجزيل الشكر والتقدير إلى أستاذتي الفاضلة، على توجيهاتها القيمة ونصائحها التي كان لها أثر كبير في إنجاز هذا العمل

وأخص بالشكر أختي أحلام العزيزة، التي تعبت معي كثيرًا، وشاركتني لحظات التعب والقلق قبل الفرح، وكانت تؤمن بأحلامي وتساندني دائمًا حتى أصبحت أحلامها مرتبطة بنجاحي، فوجودها كان نعمة عظيمة في حياتي

كما أتقدم بالشكر إلى عائلتي الكريمة، وكل من ساندني بدعوة صادقة، أو كلمة طيبة، أوموقف جميل خفف عني عناء الطريق

وإلى كل من لم تسعهم قلمي ولم ينساهم قلبي، لكم مني كل المحبة والتقدير والامتنان.

قائمة المختصرات

ج.ر : الجريدة الرسمية.

دج : الدينار الجزائري.

ص : الصفحة.

ص ص : من الصفحة إلى الصفحة.

ط : الطبعة.

د.ط : دون طبعة.

د.س.ن : دون سنة نشر.

د.ب.ن : دون بلد نشر.

ق.ع : قانون العقوبات.

ق.إ.ج : قانون الإجراءات الجزائية.

ق.ت : القانون التجاري.

ق.ت.إ : قانون التجارة الإلكترونية.

ق.م.ت : قانون الممارسات التجارية.

ج.إ : الجريمة الإلكترونية.

ج.م : الجريمة المعلوماتية.

ن.م : نظام معلوماتي.

ن.م.آ.م : نظام المعالجة الآلية للمعطيات.

ت.إ.إ : تكنولوجيات الإعلام والاتصال.

OECD : منظمة التعاون الاقتصادي والتنمية.

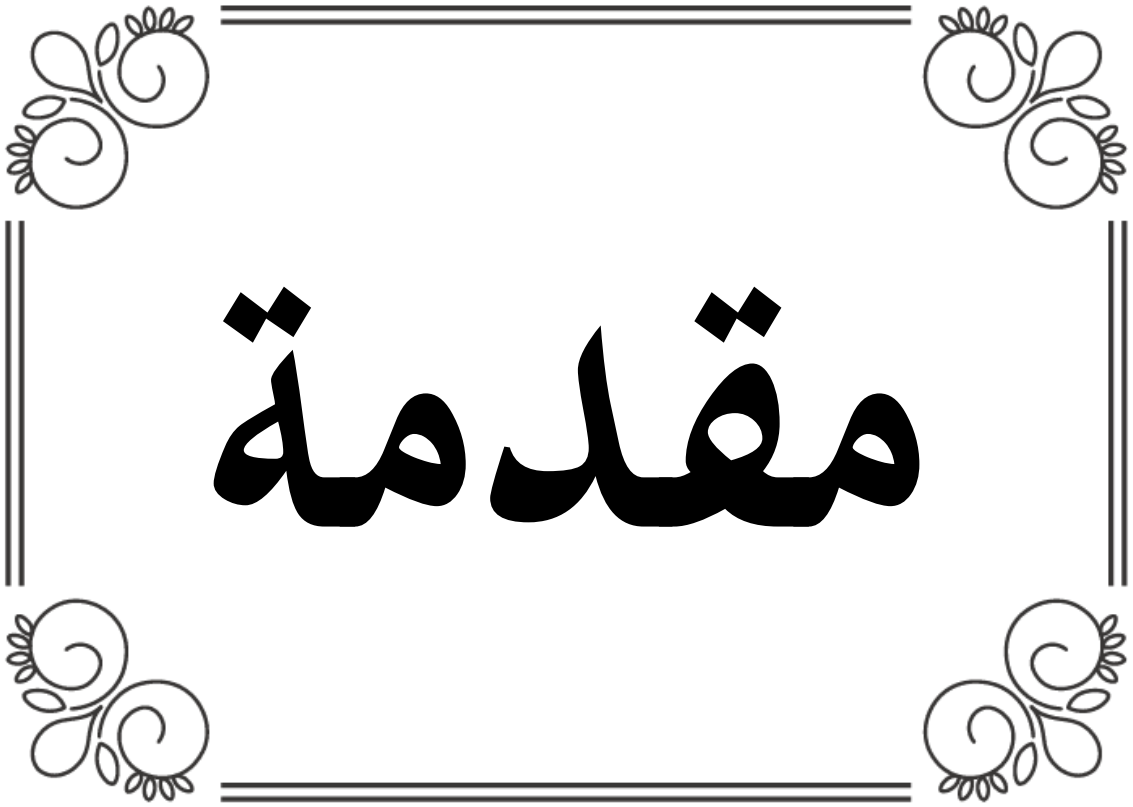
UN : منظمة الأمم المتحدة.

Cyber terrorism : الإرهاب الإلكتروني.

Cyber Extortion : الابتزاز الإلكتروني.

Interpol : المنظمة الدولية للشرطة الجنائية (الإنتربول).

CPU : وحدة المعالجة المركزية.


مقدمة

تعرف الجرائم الإلكترونية الماسة بالمعاملات التجارية،بأنها تلك السلوكيات الإجرامية المستحدثة التي تتخذ من الأنظمة المعلوماتية والشبكات الرقمية وسيلةً،أو هدفاً لتقويض سلامة النشاط الاقتصادي.

وهي تؤدي في جوهرها إلى المساس بالثقة القانونية والتجارية التي تقوم عليها المعاملات التجارية،الذي يربط بين أطراف العلاقة التجارية في الفضاء الافتراضي يتجاوز هذا الموضوع التوصيف التقني الجاف للاعتداءات الرقمية ،ليمسَّ في عمقه بيانات الشخصية والحقوق المالية للمتعامين إلكترونيا في بيئة تجارية آمنة ونزيهة.

فالجريمة المعلوماتية في السياق التجاري لم تعد مجرد اختراق لأنظمة صماء، بل هي اعتداءٌ مباشر على حقوق المستهلكين في حماية بياناتهم وأموالهم وتقويضٌ لجهود الأعوان الاقتصاديين في بناء بيئة تنافسية شريفة قائمة على الجدارة لا على التدليس.

وينبثق عن هذا الموضوع تحليلٌ معمق للعلاقة الجدلية بين التطور التكنولوجي المتسارع والقيم الأخلاقية الراسخة، حيث يتم التركيز على إرساء مبادئ الشفافية والنزاهة كضمانات جوهرية تفوق في أهميتها النصوص الردعية ذاتها.

إذ يتم تبيان كيف سعى المشرع إلى تهذيب السلوك التجاري في الفضاء الافتراضي وحمايته من الأنماط الإجرامية المستحدثة كالنصب المعلوماتي، والقرصنة المالية، وتزوير المحررات الإلكترونية، وانتحال الصفات التجارية الرقمية،إن هذه الممارسات لا تخلُّ فقط بالتوازن الاقتصادي للسوق بل تزرع حالة من عدم الثقة والقلق الاجتماعيمما يستوجب صياغة سياسة جنائية توفق بين صرامة العقاب وبينالروح الإنسانية التي تتوخى العدالة المطلقة وحماية الطرف الضعيف في العلاقة التعاقدية الرقمية.

وعلى صعيد التحليل التشريعي،يمتد الموضوع ليشمل فحص كفاءة المنظومة القانونية الجزائرية في ثوبها الجديد، لاسيما التحولات الجذرية التي أحدثها القانون رقم 24-06[1]،

[1]قاانون رقم 24-06مؤرخ في 20 شوال عام1445 الموافق 28 أبريل 2024،يعدل ويتمم الامر رقم 66-156 والمتضمن قانون العقوبات،الجريدة الرسمية للجمهورية الجزائرية،العدد ثلاثون،الصادر بتاريخ 30أفريل 2024،ص4.

والقانون 09-04[2]واللذان يعكسان يقظة المشرع تجاه السيادة الرقمية وحماية المعطيات الحساسة من العبث ولا يتوقف الأمر عند حدود النص الجامد،بل يمتد ليشمل أنسنة الإجراءات الجزائية،من خلال إيجاد توازن دقيق ومقدس بين فعالية التحري الرقمي والبحث عن الأدلة المتطايرة في الخوادم والشبكات،وبين صون الحرمات والحريات الشخصية للأفرادوهو ما يتجسد في الدور المحوري للقطب الجزائي الوطني المتخصص والهيئات الرقابية المستحدثة التي تمثل ذراع الدولة في تأمين المعاملات.

أما في بعدها الكوني، فإن هذا الموضوع يكرس مفهوم التضامن القانوني الدولي، فبما أن الجريمة الإلكترونية لا تعترف بالحدود الجغرافية ولا بالسيادات التقليدية، فإنه ينفتح بالضرورة على دراسة آليات التعاون القضائي والأمني العابر للقارات وتحليل الاتفاقيات الدولية والإقليمية التي تهدف إلى توحيد الجبهة القانونية لملاحقة الجناة أينما وجدوا.

ومن خلال إجراء مقاربات نقدية مع تشريعات مقارنة رائدة يتم تقديم رؤية استشرافية تضمن حماية متكاملة للمعاملات التجارية تزاوج بين مقتضيات الحداثة التقنية،وبين المبادئ القانونية الراسخة التي تضع الإنسان،وأمنه الاقتصادي في المقام الأول.

تكتسب دراسة "الجرائم الإلكترونية الماسة بالمعاملات التجارية" أهمية بالغة تتجاوز الأطر الأكاديمية الصرفة لتلامس الواقع المعاش في ظل التحول الرقمي الشامل، حيث تبرز أولاً من الناحية القانونية والتشريعية،من خلال رصد اليقظة التشريعية للمشرع الجزائري،لاسيما مع صدور التعديلات الجوهرية في قانون العقوبات,

إذ يتيح هذا الموضوع فهم كيفية تطويع النصوص الكلاسيكية واستحداث قواعد جديدة لمواجهة الذكاء الإجرامي الرقمي، مما يضمن مبدأ الشرعية ويحقق الأمان القانوني للأعوان الاقتصاديين.

[2] قانون رقم 09-04 مؤرخ في 14 شعبان 1430الموافق 05 غشت سنة 2009،يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها،الجريدة الرسمية للجمهورية الجزائرية ،العدد سبعة وأربعون ،الصادر بتاريخ 16 أوت 2009 ص7.

وتتجلى الأهمية الاقتصادية والتقنية،في كونها تمس عصب الائتمان في التجارة المعاصرة،فحماية المعاملات من القرصنة والاحتيال والتزوير الإلكتروني ليست مجرد ترف قانوني،بل هي ضرورة حتمية لبناء اقتصاد رقمي مستدام قائم على الثقة المطلقة، وهو ما يسهم بشكل مباشر في تشجيع الاستثمار الرقمي وحماية التدفقات المالية من الهزات الناجمة عن الاختراقات الأمنية.

وتتجلى خطورة الجرائم الإلكترونية بشكل خاص في المجال التجاري،لما يترتب عنها من تهديد لوسائل الدفع الإلكتروني والعقود المبرمة عبر الإنترنت ،وقواعد بيانات الزبائن الأمر الذي يؤدي إلى زعزعة الثقة في البيئة التجارية الرقمية ويؤثر سلبا على الاستثمار والتبادل الإلكتروني.

كما تكمن الأهمية القانونية لدراسة حماية الممارسات التجارة الإلكترونية في التشريع الجزائري[3] في حماية المستهلك إلكترونيا، بإعتباره الطرف الأضعف عقديا لغياب المعاينة المادية عبر كافة حقوقه الآمرة،كالإعلام المسبق والعدول لمواجهة التدليس،وفي إرساء النظام العام الرقمي لضمان أمان المعاملات وإستقرارها،من خلال التنظيم التشريعي لحماية البيانات والتنظيم القانوني لتقنيات التشفير والتوقيع الإلكتروني منعا للعبث بها وتعزيزا للثقة الإئتمانية الرقمية.

وعلى الصعيد الإنساني والاجتماعي ينطوي الموضوع على بعد أخلاقي عميق يتمثل في صون كرامة الإنسان وحماية خصوصيته من التغول المعلوماتي، فالبحث يسعى لتبيان آليات حماية المستهلك باعتباره الطرف الضعيف في العلاقة التعاقدية الرقميةمن ممارسات النصب والابتزاز،مما يعزز الاستقرار الاجتماعي ويحفظ طمأنينة الأفراد في تعاملاتهم اليومية.

كما تبرز الأهمية المؤسساتية والإجرائية في تقييم فاعلية الهيئات المستحدثة ،كالقطب الجزائي الوطني المتخصص،ومدى قدرة أجهزة العدالة على التعامل مع الدليل الرقمي المتطايربمهنية توازن بين سرعة التحري وبين صون الحريات الفردية وصولاً إلى الأهمية الدوليةالتي تفرضها الطبيعة العابرة للحدود لهذه الجرائم.

مما يبرز حتمية التعاون القضائي والأمني العالمي وتجسير المسافات القانونية بين الدول لملاحقة الجناة أينما وجدوا التزاماً بروح العدالة والأمانة العلمية في بناء مجتمع رقمي آمن.

[3] بسمة صيشي،الحماية القانونية للممارسات التجارية الإلكترونية،رسالة دكتوراه(غير منشورة)،شعبة القانون الخاص،تخصص قانون الأعمال،قسم الحقوق،كلية الحقوق الحقوق والعلوم السياسية،جامعة الوادي،2024-2025،ص أ.

نبع مبررات اختيار هذا الموضوع من تقاطعٍ حرج بين المسؤولية الأخلاقية والضرورة القانونية في ظل عصرٍ باتت فيه التكنولوجيا تُهيكل حياة المجتمعات وتصيغ مستقبل اقتصادها، فالاختيار لم يكن وليد الصدفة،بل أملاه التنامي المتسارع لظاهرة "الجرائم الإلكترونية الماسة بالمعاملات التجارية" وما تسببه من طعناتٍ في خاصرة الثقة الرقمية التي يُفترض أن تجمع بين الإنسان وأمنه المالي.

إن الرغبة في سبر أغوار هذا الموضوع،تأتي مدفوعةً بهاجس إنساني يسعى لحماية المستهلك والعون الاقتصاديمن تغوّل الذكاء الإجرامي ،الذي استحلّ الحقوق وسلب الأموال تحت ستار العوالم الافتراضية،مما يجعل البحث في هذا المجال واجباً أخلاقياً يهدف إلى إرساء قيم الشفافية والنزاهة كحصنٍ منيع ضد ممارسات التدليس والاحتيال والقرصنة.

وعلى الصعيد القانوني الأكاديمي يبرز مبررٌ جوهري ،يتمثل في الرغبة العميقة في رصد وتحليل اليقظة التشريعية الاستثنائية التي أبداها المشرع الجزائري لاسيما مع صدور التعديلات الحاسمة في قانون العقوبات بموجب القانون 24-06 [4].

حيث يفرض الواقع البحثي ضرورة تقييم كفاءة هذه النصوص المستحدثة وقدرتها على احتواء الجريمة المعلوماتية بمعادلةٍ توازن بين زجر الجناة وصون الحريات الفردية،كما أن الطبيعة العابرة للحدود لهذه الجرائم شكّلت حافزاً قوياً لاستكشاف آليات التعاون الدولي والاتفاقيات الإقليمية، رغبةً في فهم كيفية بناء جبهة قانونية عالمية موحدة لا تترك للمجرمين ثغرةً للإفلات من العقاب.

علاوة على ذلك، فإن الميل الشخصي والأكاديمي نحو التخصص في القضايا القانونية المرتبطة بالتقنيات الحديثةوالوقوف على الدور المحوري للهيئات المتخصصة ،كالقطب الجزائي الوطني يُعد مبرراً أصيلاً لتقديم دراسة تزاوج بين عمق النظرية ودقة التطبيق الإجرائي.

إن الهدف الأسمى من هذا الاختيار هو المساهمة في بناء منظومة قانونية متكاملة تضمن سيادة القانون في الفضاء الرقمي،وتحمي كرامة الإنسان وأمانه الاقتصادي التزاماً بالأمانة

[4] القانون 24-06،المرجع نفسه،ص4.

العلمية ووفاءً لمقتضيات الحداثة،التي تتطلب باحثين يدركون أن حماية المعاملة التجارية هي في جوهرها حمايةٌ للإنسان الذي يقف خلف الشاشة.

في ظل التسارع المتزايد للتطور التكنولوجي، لم تعد المعاملات التجارية بمنأى عن المخاطر المستحدثة،إذ أضحت الجرائم الإلكترونية تطال وتمس مختلف مراحلها سواء عند إبرامها أو أثناء تنفيذها،الأمر الذي من شأنه المساس بعنصري الثقة والاستقرار اللذين يقوم عليهما النشاط التجاري، وأمام هذا الواقع يواجه النظام القانوني تحديات حقيقية تتعلق بمدى قدرته على استيعاب هذه الأشكال الجديدة من الإجرام خاصة في ظل ما تتسم به من تعقيد تقني وطابع عابر للحدود.

كما تتزايد وتتفاقم هذه التحديات مع تنامي دور الاتفاقيات الدولية ،في إرساء معايير مشتركة لمكافحة الجرائم الإلكترونية وتعزيز التعاون بين الدول،وعلى هذا الأساس تبرز إشكالية جوهرية مفادها إلى أي حد يمكن للإطار القانوني الوطني أن يحقق حماية فعالة للمعاملات التجارية من الجرائم الإلكترونية، وأن يواكب في الوقت ذاته المعايير والتوجهات التي كرّستها الاتفاقيات الدولية في هذا المجال؟

وتتفرع عن هذه الإشكالية تساؤلات تبحث في ماهية الجرائم الإلكترونية الماسة بالمعاملات التجارية وكيفية التمييز بين الممارسات النزيهة والأنماط الإجرامية التي تستهدف كرامة الإنسان وأمنه المالي في الفضاء الرقمي؟.

ومدى كفاية الأركان القانونية والسياسة العقابية في التشريع الجزائري،لاسيما بعد تعديلات أفريل2024في توفير حماية إجرائية وموضوعية توازن بين ردع الجناة وصون الحريات الفردية وخصوصية البيانات؟وصولاً إلى فحص فاعلية الأجهزة القضائية المتخصصة،في ملاحقة الأدلة الرقمية المتطايرة ومدى نجاعة التعاون الدولي العابر للحدود في بناء بيئة تجارية عالمية آمنة تصون الحقوق الاقتصادية وتلتزم بمقتضيات الأمانة العلمية وروح العدالة؟.

تتمحور فرضيات البحث حول التصور، بأن المنظومة القانونية الجزائرية،رغم حداثة نصوصها لاسيما تعديلات 2024تسعى جاهدة لتطويع القواعد الجنائية التقليدية لمجابهة الطبيعة المعقدة للجرائم الإلكترونية الماسة بالمعاملات التجارية مع افتراض أن فاعلية هذه الحماية

تظل رهينة التوازن الدقيق بين صرامة الردع العقابي وبين صون الحقوق والحريات الأساسية وحرمة الحياة الخاصة.

كما يُفترض أن تبني المشرع لآليات إجرائيةوقضائيةمتخصصة،كالقطب الجزائي الوطني يمثل ركيزة أساسية لضمان الأمن القانوني والمالي للأعوان الاقتصاديين والمستهلكين في الفضاء الرقمي ،شريطة تعزيزها بتعاون دولي وقضائي فاعل يتجاوز العقبات السيادية والتقنية،بما يضمن بناء بيئة تجارية نزيهة تحمي كرامة الإنسان وتصون الأمانة العلمية في ملاحقة الدليل الرقمي العابر للحدود.

يتحدد نطاق هذه الدراسة،في أبعادٍ ثلاثية متكاملة تضمن الإحاطة بموضوع "الجرائم الإلكترونية الماسة بالمعاملات التجارية" من منظور قانوني وإنساني رصين فعلى المستوى الموضوعي،يرتكز البحث على تحليل الأنماط الإجرامية التي تستهدف نزاهة المعاملات الاقتصادية الرقمية مع التركيز بشكل خاص ،على السياسة الجنائية الموضوعية والإجرائية التي استحدثها المشرع الجزائري لضمان الأمن القانوني والائتمان التجاري.

أما زمانياً فتكتسب الدراسة راهنيتها ،من خلال مواكبة أحدث التطورات التشريعية لاسيما التعديلات المفصلية في قانون العقوبات بموجب القانون 24-06 [5]وما تلاه من نصوص منظمة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في حين ،يمتد النطاق المكانيليشمل الممارسات القضائية داخل الدولة الجزائرية ،من خلال أجهزتها المتخصصة مع الانفتاح الضروري على الفضاء الدولي والإقليمي الذي تفرضه طبيعة الجريمة العابرة للحدود.

إن هذا التحديد، يهدف في جوهره إلى تقديم رؤية علمية دقيقة توازن بين مقتضيات الردع القانوني وبين صون الحريات الفردية ،وكرامة الإنسان في المحيط الرقمي التزاماً بالأمانة العلمية وبمنهجية بحثية واضحة المعالم تبتعد عن التشتت المعرفي.

[5]القانون 24-06،المرجع نفسه،ص4.

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، لتشريح النصوص القانونية،لاسيما تعديلات قانون العقوبات لعام2024 واستجلاء قدرتها على حماية الائتمان التجاريوكرامة المستهلك .

كما يُستعان بالمنهج المقارن لربط التشريع الوطني بالمعايير الدولية والاتفاقيات الإقليمية، بهدف استنباط حلول توازن بين فعالية الردع الرقمي وبين صون الحريات الفردية ،ومن منطلق الأمانة العلمية،يتم توظيف المنهج الاستنباطي لإيجاد حلول قانونية للقضايا التقنية المستحدثة، مما يضمن تقديم رؤية شاملة تزاوج بين دقة التحليل الفقهي والروح الإنسانية للعدالة في الفضاء الرقمي.

واجهت هذه الدراسة جملة من التحديات والمصاعب التي تفرضها طبيعة الموضوع المتجددة تتقدمها الحداثة التشريعية،المتمثلة في صدور تعديلات قانون العقوبات لعام 2024 مما جعل من الصعب العثور على مراجع فقهية كافية أو اجتهادات قضائية مستقرة تواكب هذه النصوص المستحدثة، وهو ما تطلب مجهوداً مضاعفاً لتحري الدقة والأمانة العلمية في التفسير.

كما برزت صعوبة التعقيد التقني للجريمة الإلكترونية وتداخلها مع المفاهيم التجارية،مما فرض تحدي الموازنة بين المصطلحات القانونية الجامدة،وبين الواقع الرقمي المتسارع الذي لا يعترف بالحدود، فضلاً عن صعوبة الحصول على إحصائيات دقيقة أو قضايا واقعية تعكس البعد الإنساني المتضرر من هذه الجرائم بسبب طابع السرية الذي يغلف المعاملات المالية.

ورغم هذه العقبات،كان الإصرار على تقديم دراسة رصينة تخدم العدالة وتحمي كرامة الإنسان في الفضاء الرقمي هو الدافع لتجاوز شح المصادر الميدانية،والاعتماد على التحليل العميق للنصوص والاتفاقيات الدولية كبديل منهجي موثوق.

للإحاطة بهذا الموضوع في أبعاده القانونية والإنسانية، والتزاماً بمقتضيات الأمانة العلمية التي تفرض تسلسلاً منطقياً يخدم غايات البحث،تم رسم معالم هذه الدراسة وفق خطة ثنائية متكاملةنستهلّها.

في الفصل الأول بوضع الأسس المفاهيمية والقانونية للجرائم الإلكترونية الماسة بالمعاملات التجارية،حيث نسعى من خلاله إلى تكييف هذه الأنماط المستحدثة ،وتبيان أركانها التي تمس

جوهر الثقة الرقمية، مع التركيز على حماية الإنسان من التضليل والاعتداء على بياناته المالية في ظل البيئة الافتراضية.

أما الفصل الثاني فقد خُصص لاستقراء السياسة العقابية والآليات الإجرائية التي اعتمدها المشرع الجزائري،لاسيما في ظل التعديلات المفصلية لعام 2024 لتقييم مدى نجاعة التدابير الموضوعية والأجهزة القضائية المتخصصة،في ردع الجناة وتكريس العدالة مع الانفتاح على أطر التعاون الدولي والاتفاقيات الإقليمية،كضرورة حتمية لمواجهة الإجرام العابر للحدود وصولاً إلى صياغة رؤية قانونية شاملة تضمن استقرار المعاملات التجارية،وتصون كرامة الأفراد وحقوقهم في ظل دولة القانون الرقمية.

الفصل الأول

الإطار المفاهيمي للجرائم الإلكترونية الماسة بالمعاملات التجارية

أحدثت الثورة التكنولوجية والرقمنة تحولاً جذرياً في نمط الحياة البشرية،وانتقل النشاط الاقتصادي من حيزه المادي التقليدي إلى فضاء سيبراني افتراضي لا يعترف بالحدود الجغرافية، وبالرغم من المزايا الهائلة التي وفرتها معاملات التجارية من سرعة وكفاءة، إلا أنها أفرزت في المقابل بيئة خصبة لظهور أنماط مستحدثة من الإجرام تُعرف بالجرائم الإلكترونية.

تعد هذه الجرائم من أخطر التحديات التي تواجه استقرار المعاملات التجارية في العصر الحديث، كونها تستهدف الثقة والائتمان ،اللذين يقومان عليهما النشاط التجاري و لأجل الإحاطة بهذا الموضوع كان لزاماً علينا أولاً ضبط المفاهيم وتحديد الماهية القانونية والتقنية لهذه الجرائم، وكذا فهم طبيعة المعاملات التجارية التي تقع ضحية لها.

و عليه، سيتم تقسيم هذا الفصل إلى مبحثين أساسيين،المبحث الأول ماهية الجرائم الإلكترونية أما المبحث الثاني ماهية المعاملات التجارية.

المبحث الأول :ماهية الجرائم الإلكترونية الماسة بالمعاملات التجارية :

يعد تحديد ماهية الجرائم الإلكترونية الركيزة الأساسية لفهم الأخطار التي تهدد الفضاء الرقمي،فهي ليست مجرد تطور للجريمة التقليدية،بل هي نمط إجرامي مستحدث يتميز بتعقيده التقني وطابعه العابر للحدود، يسعى هذا المبحث إلى ضبط المفاهيم المتداخلة لهذه الجرائم من خلال استعراض تعريفاتها الاصطلاحية والقانونية والدولية مع تسليط الضوء على أنواعها المختلفة وأبرز الخصائص والأركان التي تميزها ككيان قانوني مستقل بذاته،حيث سيتم تطرق لمفهوم وأنواع الجرائم الإلكترونية في المطلب الأول،وإلى خصائص وأركان الجريمة الإلكترونية في المطلب الثاني.

المطلب الأول:مفهوم الجرائم الإلكترونية

يشكل تحديد مفهوم الجرائم الإلكترونية، وتصنيف أنواعها حجر الزاوية في فهم التهديدات السيبرانية المعاصرة،إذ لا يمكن مواجهة هذا الإجرام دون الإحاطة بأبعاده التعريفية المختلفة وتعدد صوره التي تمس الأفراد والدول والمصالح التجارية على حد سواء.

لذاسنتناول في هذا المطلب ضبط المصطلحات القانونية والدولية المؤطرة لهذه الجرائم مع استعراض تصنيفاتها المتنوعة التي تعكس شمولية وخطورة هذا النشاط الإجرامي في البيئة الرقمية، وعليه سيتم تناول في الفرع الأول تعريف الجرائم الإلكترونية، أما في الفرع الثاني أنواع الجرائم الإلكترونية.

الفرع الأول: تعريف الجرائم الإلكترونية

لم يحسم الفقه القانوني أمر بشأن إقرار تعريف جامع مانع للجريمة الإلكترونية و يرجع ذلك إلى الإختلاف في تحديد نطاقها ومجال إنطباقها،وعليه سيتم وبيان [1]:

أولا:التعريف الفقهي للجريمة الإلكترونية يقصد بالجريمة الإلكترونية إصطلاحا كل سلوك إجرامي يرتكب بإستخدام وسيلة تقنية معلوماتية،كالحاسوب أو شبكات الإنترنتويأخذ صور متعددة،من بينها الأفعال التي تتم عبر غرف الدردشة أو احتراق البريد الإلكترونيأ و التعدي على حسابات مواقع التواصل الإجتماعي،بقصد الإضرار بشخص معين أو مجموعة من الأفراد،وقد يمتد اثره ليشمل دولة من الدول في إطار إستهداف ذي طابع حربي أو إقتصادي أو بقصد المساس بسمعتها،وفي جميع هذه الصوريضل الهدف متمثلا في الوصول إلى معلومات محجوبة أو الكشف عنها أو تسريبها لفائدة جهة معينة.[2]

[1] آية بن ميسية، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة ضمن متطلبات شهادة الماستر، قسم حقوق، كلية الحقوق والعلوم السياسية، جامعة عبد الحفيظ بوالصوف، ميلة، 2024-2025، ص05.

[2] آية بن ميسية،المرجع نفسه، ص06.

وقد أشار مجلس أوروبي،في تقاريره المتعلقة بجرائم الحاسوب إلى قيام الجريمة ،كلما تم التدخل غير المشروع في البيانات أو البرامج،سواء عن طريق تغييرها أو محوها أو إدخال تعديلات عليها أو عرقلة معالجتهامتى ترتب عن ذلك ضرر إقتصاديأو مساس بحقوق الملكية أو تحقيق منفعة مالية غير مشروعة للجاني أو لغيره.

ويرى أنصار أحد الإتجاهات الفقهية، أن الجريمة الإلكترونية تتمثل في كل فعل ضار يصدر عن شخص ذي إلمام تقني يستخدم نظاما معلوماتيا أو شبكة حاسوبية ،للوصول إلى البيانات أو البرامج بقصد نسخها أو تعديلها أو حذفها أو تزويرها أو إتلافها أو تعطيلها أو الإستلاء عليها أو نشرها بغير سند قانوني ،في حين يذهب إتجاه فقهي آخر إلى توسيع المفهوم ليشمل كل نشاط إجرامي تستخدم فيه الوسائل الإلكترونية أو الرقميةسواء بصورة مباشرة أو غير مباشرةكأداة لتنفيذ الفعل الإجرامي.

غير أن هذا التوسع في المفهوم ،يثير إشكالا من الناحية القانونية،إذ لايكفي مجرد وجود الحاسوب أو إحدى وسائطه ضمن محل الجريمة ،لإضفاء وصف الجريمة الإلكترونية عليه،كما هو الحال في سرقة جهاز الحاسوب ذاته أو وسائط التخزين،كذلك لا يعد الفعل جريمة إلكترونية لمجرد استعمال الحاسوب كوسيلة اتصال بين الجناة لارتكاب جريمة تقليدية،كالتخطيط لعملية سطوما لم يكن النظام المعلوماتي أو البيانات محل إعتداء مباشر أو عنصراً جوهرياً في تكوين الركن المادي للجريمة.[1]

ثانيا:التعريف القانوني للجريمة الإلكترونية

1_**التعريف الوطني** ثبت قانونا بفعل الثورة المعلوماتية المتسارعة ظهور أنماط مستحدثة من الإجرام[2]، لم تكن مألوفة من قبل الأمر الذي دفع العديد من الدول ،ومن بينها الجزائر إلى التدخل التشريعي العاجل لمواكبة هذه التحولات العميقة وسد الفراغ القانوني الذي أحدثته التكنولوجيا ،وفي هذا السياق قام المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 04-15،وذلك بإدراج قسم سابع مكرر تحت عنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات والممتد من المادة 394 مكرر إلى المادة 394 مكرر 7.

حيث استهدف هذا التعديل، توفير حماية جزائية متكاملة للأنظمة المعلوماتية وأساليب المعالجة الآليةمواجهاً بذلك بروز أشكال جديدة من الإجرام تتخذ من الفضاء الرقمي مسرحاً لها،كما أقرّ المشرع

[1] آية بن ميسية، المرجع السابق،ص06.

[2] يزيد بوحليط،الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقيات العربية لمكافحة جرائم التقنية المعلومات قانون العقوبات قانون إجراءات الجزائية قوانين خاصة،دار الجامعة الجديدة،الجزائر،ص54_60.

في هذه المرحلة بمسؤولية الشخص المعنوي ووسع من نطاق التجريم ،ليشمل الشروع والاتفاق الجنائي مع تشديد العقوبات في الجرائم ذات الصلة.[1]

ولم يتوقف المشرع عند هذا الحد، بل سارع إلى تدعيم المنظومة القانونية بإصدار القانون رقم 09-04،الذي اعتمد من خلاله مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال،كدلالة شاملة على الجريمة الإلكترونية،حيث عرفها في مادته الثانية الفقرة أ،بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وكل جريمة أخرى تُرتكب أو يُسهل ارتكابها عن طريق منظومة معلوماتية أونظام للاتصالات الإلكترونية وهو ما سمح بتصنيف هذه الجرائم إلى ثلاثة أنواع رئيسية تشمل الجرائم الواقعة على الأنظمة،والجرائم المرتكبة بواسطة المنظومات المعلوماتية والجرائم التيتتم عبر أنظمة الاتصالات الإلكترونية.[2]

تبرز أهمية هذه المنظومة في اعتمادها على عدة معايير، أولها معيار الوسيلة نظام الاتصالاتوثانيها [3]معيار الموضوع المساس بالمعالجة الآلية،وثالثها المعيار الشرعي المستمد من قانون العقوبات،ورغم أن تعبير نظام المعالجة الآلية للمعطيات هو تعبير فني تقني قد يصعب إدراك حقيقته بسهولة.

إلا أنه يعكس رغبة المشرع في الإحاطة بكل الجوانب الرقمية المتطورةومع تعدد المصطلحات الفقهية والتشريعية بين الجريمة الإلكترونية وجرائم التقنية العالية، فإن التشريع الجزائري تبنى مفهوماً مرناً يجمع بين هذه المسميات متجاوزاً الجدل الفقهي حول ضرورة الاتصال بين جهازين،ليجعل من المنظومة المعلوماتية سواء كانت منفردة أو مرتبطة بالشبكة محلاللحماية أو أداة للجريمة.

وعلى ضوء التعديلات الجوهرية الأخيرة التي طرأت بموجب القانون رقم 24-06 لقانون العقوبات[4]،فقد انتقلت السياسة الجنائية في الجزائر إلى مرحلة الردع المشدد،حيث تم رفع سقف العقوبات الأصلية والتكميلية بشكل كبير وتشديد الغرامات المالية المفروضة على مرتكبي جرائم المساس بالمعطيات خاصة تلك التي تستهدف المؤسسات السيادية أو تهدف إلى المساس بالأمن القومي والوحدة الوطنية عبر الفضاء السيبراني.

وبذلك تكون السياسة الجنائية الجزائرية ،قد استكملت بناء مقاربة شاملة تأخذ بعين الاعتبار الطابع المتطور لهذه الجرائم وتضمن حماية متكاملة للبيئة الرقمية معتبرة أن التطور التكنولوجي يستوجب يقظة

[1] يزيد بوحليط،المرجع السابق،ص54 _60.

[2] عفاف لعقون، جميلة فشار،"الجريمة الالكترونية: المقاربة المفاهيمية القانونية"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تمنراست، جامعة الجلفة،المجلد15،العدد واحد،جانفي 2021،ص259-260.

[3] عفاف لعقون،جميلة فشار،المرجع السابق،ص261.

[4] قانون رقم 24-06 ،المرجع السابق،ص4.

تشريعية مستمرة توازن بين حماية الحقوق والحريات وبين ضرورة ردع الأنماط الإجرامية الحديثة،حيث تأخذ الجرائم الإلكترونية خطورة أكبر عندما تستهدف المعاملات التجارية الإلكترونية ،إذ لايقتصر أثرها على المساس بالأنظمة المعلوماتية فقط،بل يمتد إلى الإضرار بالمصالح المالية للأعوان الإقتصاديين والمستهلكين خاصة في ظل الاعتماد المتزايد على وسائل الدفع والعقود الإلكترونية.

2:التعريف الدولي للجريمة الإلكترونية

حددالمشرع مفهوم المنظومة المعلوماتية، بأنها كل نظام منفصل أو مجموعة أنظمة مترابطة تقوم بمعالجة [1]آلية للمعطيات تنفيذاً لبرنامج معين، وهو تعريف يتوافق مع المعايير الدولية الواردة في اتفاقية بودابست و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات التي صادقت عليها الجزائر سنة2014 كما عرّف الاتصالات الإلكترونية،بأنها كل عملية إرسال أو استقبال للعلامات أو الإشارات أو البيانات أو الصور أو الأصوات عبر مختلف الوسائط التقنية كالحاسوب والهاتف النقال والأجهزة اللاسلكية.

وبالرجوع إلى أحكام قانون العقوبات، يتضح أن المشرع انتهج سياسة جنائية موسعة حيث جرم الأفعال التي تتم عبر الوسائل الإلكترونية، مثلا لإساءة إلى رئيس الجمهورية المادة 144 مكرر والجرائم ضد الهيئات الرسمية المادة 146[2]مع تعزيز الحماية الجزائية لوسائل الدفع الإلكتروني وبطاقات الضمان الاجتماعي ونصوص تجرم إساءة استخدام وسائل الاتصال الحديثة في قانون البريد و المواصلات الإلكترونية.

اعتمدت الاتفاقيات الدولية المتعلقة بالجريمة الإلكترونية ،وعلى رأسها اتفاقية بودابست مقاربة تقنية لتعريف الجريمة المعلوماتية ،من خلال ضبط المصطلحات المرتبطة بها،حيث نصت المادة الأولى منها على... التعريفات لأغراض هذه الإتفاقية:

أ:يقصد بمنظومة الكومبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلةوالتي يقوم واحد منها أو أكثر وفقا لبرنامج بالمعالجة الآلية للبيانات.[3]

ب: يقصد ببيانات الكومبيوتر أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر،بما في ذلك برنامج مناسب يساعد نظام كومبيوتر في أداء وظيفة معينة

[1] يزيد بوحليط،المرجع السابق،ص60_61.

[2]يزيد بوحليط،المرجع نفسه،61.

[3] اتفاقية مجلس اروبا المتعلقة بالجريمة الالكترونية (بودابست)،المبرمة بتاريخ 23 نوفمبر 2001، لم تصادق عليها الجزائر،مجموعة المعاهدات الاروبية رقم 185، ص3.

ج: يقصد بمقدم الخدمة: أي كيان عام أو خاص يقدم المستخدمي الخدمة التي يوفرها القدرة على الاتصال عن طريق نظام الكومبيوترو أي كيان آخر يقوم بمعالجة بيانات الكومبيوتر أو تخزينها نيابة عن مزود خدمة الاتصالات أو مستخدمي هذه الخدمة.

د:يقصد بيانات حركة الاتصالات ،أي بيانات كومبيوتر متعلقة باتصال عن طريق نظام الكومبيوتر والتي تنشأ عن نظام كومبيوتر يشكل جزءاً في سلسلة الاتصالات توضح المنشأ والوجهة والمسار والزمنوالتاريخ والحجموالمدة أو نوع الخدمة الأساسية.[1]

وبناءا على ماسبق تم إشارة إلى تعريف المنظمات الدولية للجريمة الإلكترونية:

- ✓ منظور منظمة التعاون الاقتصادي والتنمية(OECD) :تبنت لجنة الخبراء التابعة للمنظمة في عام 1983 رؤية موسعة للجريمة المعلوماتية، حيث لم تحصرها في الشق الجنائي الفج فحسب،بل مدّت نطاقها ليشمل أي ممارسة تتعارض مع القواعد الأخلاقية أو الأطر القانونية أو الصلاحيات الممنوحة ويركز هذا التعريف على أن الجريمة تقع بمجرد المساس بسلامة المعالجة الآلية للبيانات أواعتراض مسار نقلها بطرق غير مشروعة.[2]
- ✓ منظور المجلس الأوروبي(Council of Europe) :وفقاً للتقرير الصادر عن المجلس الأوروبي حول جرائم الحاسوب يتمحور التعريف حول الاعتداء المادي والمنطقي على المحتوى الرقمي،فالجريمة هنا تتمثل في أي تدخل غير قانونيسواء بالحذف أو التعديل أو الإضافةيستهدف المعطيات والبرمجيات،ويشترط هذا التعريف في شقه الاقتصاديترتب ضرر مادي أو معنوي أو السعي لتحقيق كسب مالي غير مشروع عبر سلب ملكية الآخرين أو التلاعب بمسار معالجة البيانات.
- ✓ منظور منظمة الأمم المتحدة (UN):اتسم تعريف مؤتمر الأمم المتحدة العاشر لمنع الجريمة 2000[3]بالشمولية والمرونة،حيث اعتبر الجريمة المعلوماتية وعاءً لكل الأفعال الجرمية التي تُتخذ من الأنظمة الحاسوبية وسيلة أو مسرحاً لارتكابها ،وبموجب هذا المنظور فإن أي نشاط مخالف للقانون

[1] اتفاقية مجلس اروبا المتعلقة بالجريمة الالكترونية (بودابست)،المرجع السابق، ص3.

[2] سليمان أبونمر،يوسف بوكريدة ، مكافحة الجريمة المعلوماتية في ايطار القانون الدولي ، مذكرة لنيل شهادة الماستر ،" غيرمنشور" ، قسم الحقوق ،كلية الحقوق و العلوم السياسية ،جامعة محمد خيضر،بسكرة، 2020-2021،ص07.

[3] سليمان أبو نمر،يوسف بوكريدة،المرجع نفسه،ص07.

يتم تنفيذه ضمن البيئة الرقمية يندرج تحت طائلة هذا التصنيف مما يفتح الباب لاستيعاب كافة الجرائم التقليدية عند انتقالها إلى الفضاء الإلكتروني.[1]

الفرع الثاني:أنواع الجرائم الإلكترونية

تعتبر الجرائم الإلكترونية وجهاً حديثاً للنشاط الإجرامي،حيث انتقلت فيه النوايا الجرمية من الواقع الملموس إلى الفضاء الرقمي لتستهدف كل مفاصل الحياة المعاصرةفهي لا تكتفي بتهديد أمن الدول وسيادتها عبر اختراق أنظمتها الحساسة،بل تمتد لتطال أدق تفاصيل حياة الأفراد وخصوصياتهم وصولاً إلى استغلال الثغرات التقنية للاستيلاء على الأموال والممتلكات،وبذلك أصبحت هذه الجرائم خطراً عابراً للحدود يستغل بذكاء وسرية التطور التكنولوجي لزعزعة الاستقرار المادي والمعنوي للمجتمعات،فمن خلال هذا المبحث سيتم ذكر أهم أنواع الجرائم الإلكترونية:

أولا:جرائم الإلكترونية ضد الجكومات:تُعد الجرائم الإلكترونية الموجهة ضد الدول والسيادة الوطنية من أخطر التحديات القانونية والأمنية في العصر الرقمي،حيث تتجاوز في آثارها مجرد اختراق الأنظمة لتصل[2]إلى تهديد السلم المجتمعي والاستقرار العالمي ويمكن صياغة هذا المفهوم من منظور إنساني وقانوني شامل على النحو التالي:تستهدف هذه الجرائم في جوهرها البنى التحتية الحيوية والمواقع الرسمية للحكومات والمنظمات الدولية.

حيث يسعى مرتكبوها الذين يُصطلح على تسميتهم بالمنفذين السيبرانيين أو القراصنةإلى تقويض أركان الدولة من خلال تدمير الأنظمة الشبكية،أو تعطيل الخدمات العامةوتتخذ هذه الأفعال أبعاداً أشد خطورة حين تتوجه نحو المنشآت العسكرية والأمنية،بقصد الاستيلاء على الأسرار القومية والمعلومات الحساسة التي تمس كيان الدولة وأمن مواطنيها ثم إعادة تداولها ونشرها عبر طرق غير مشروعة تفتقر إلى أدنى معايير المسؤولية القانونية.[3]

وفي هذا السياق يبرز مصطلح الإرهاب الإلكتروني (Cyber terrorism) كأحد أبشع صور الاعتداء التقني، وهو نشاط منظم تقوده جماعات تسعى لاستغلال الثغرات البرمجية للوصول إلى المواقع

[1]سليمان أبو نمر،يوسف بوكريدة،المرجع السابق،ص07.

[2]الطاهر ياكر،"مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية"،مجلة الصدى للدراسات القانونية والسياسية،جامعة الجيلالي بونعامة، خميس مليانة،الجزائر،المجلد 04،العدد الرابع،ديسمبر 2022، ص06.

[3]الطاهر ياكر،المرجع نفسه، ص06.

المشفرة والمحجوبة ولا تقتصر أهداف هذا الإرهاب على الجوانب العسكرية فحسب،بل تمتد لتشمل زعزعة الأمن الاقتصادي والمالي للدول مما يؤثر بشكل مباشر على حياة الأفراد ورفاهيتهم.[1]

ثانيا: جرائم الإلكترونية ضد الأفراد: تُمثل الجرائم الإلكترونية الموجهة ضد الأفراد انتهاكاً صارخاً للخصوصية الإنسانية والكيان المعنوي للشخص، حيث تقوم هذه الجرائم في جوهرها على اختراق الهوية الرقمية والوصول غير المشروع إلى البيانات الشخصية مثل حسابات البريد الإلكتروني وكلمات المرور وتتجاوز هذه الأفعال مجرد التعدي التقني لتصل إلى انتحال الشخصية، حيث يستولي الجاني على ملفات وصور الضحية الخاصة لاستخدامها كأداة ضغط وابتزاز، مما يضع الفرد تحت وطأة التهديد النفسي والمادي لإجباره على الامتثال لإرادة المجرم وهو ما يُعرف قانونياً وإنسانياً بجرائم الإنترنت الشخصية[2].

ومن المنظور القانوني والأخلاق يتسع نطاق هذه الجرائم ليشمل عمليات التشهير ونشر المعلومات المضللة أو المغلوطة سواء كان المستهدف فرداً أو كياناً تجارياً بهدف النيل من مكانته الاجتماعية أو الاقتصادية وتتعدد الوسائل التقنية المستخدمة، في هذا الصدد بدءاً من تدشين منصات رقمية مخصصة لنشر المحتوى المسيء وصولاً إلى استغلال القوائم البريدية لبث الشائعات على نطاق واسع.

كما تبرز في هذا الإطار حملات تشويه السمعة الممنهجة التي تستهدف الرموز الفكرية والسياسية والدينيةسعياً لزعزعة ثقة المجتمع في مصداقيتهم،وغالباً ما يكون المحرك الأساسي لهذه الأفعال هو الرغبة في الابتزاز أو تحقيق مآرب نفعية غير مشروعة مما يجعلها جرائم مركبة تمس الحق في الكرامة والحق في حماية الحياة الخاصة التي كفلتها المواثيق الدولية والقوانين الوطنية.[3]

ثالثا:جرائم الإحتيال والإعتداء على الأموال: تُصنف جرائم الاحتيال والاعتداء الرقمي على الأموال كأحد أخطر الانتهاكات المالية المعاصرة،إذ تقوم قانوناً على التلاعب بالبيانات وتجاوز صلاحيات الوصول بطرق غير مشروعة، وتتجلى خطورتها الإنسانية والمهنية في خيانة الأمانة التي قد يرتكبها موظفون داخل المؤسسات عبر إدخال بيانات زائفة أو تعديل السجلات المحفوظة أو إساءة استخدام البرمجيات والأنظمة لاختلاس الأصول،إن هذا السلوك الإجرامي لا يهدف فقط للسرقة المادية.

[1] الطاهر ياكر،المرجع السابق، ص06.

[2] الطاهر ياكر،المرجع نفسه،ص06.

[3] الطاهر ياكر،المرجع نفسه،ص06.

بل يمتد أثره لزعزعة الثقة في النظم الاقتصادية وضرب قيم النزاهة المؤسسية مما يستوجب حماية قانونية صارمة للأمن المالي.[1]

وقد تتعرض المؤسسات التجارية لهذا النوع من الجرائم ،من خلال تهديدها بنشر بياناتها المالية أو تعطيل منصاتها الإلكترونية مقابل دفع مبالغ مالية،الأمر الذي يؤثر على استمرارية النشاط التجاري وثقة المتعاملين.

رابعا:جرائم الإبتزاز الإلكتروني:تُمثل جرائم الابتزاز الإلكتروني (Cyber Extortion) صورةً عصرية من صور الإكراه المادي والمعنوي،حيث تعتمد قانوناً على توجيه هجمات تقنية منظمة مثل هجمات حرمان الخدمة[2] لتعطيل الأنظمة الحاسوبية أو المواقع الإلكترونية ومنعها من أداء وظائفها الحيوية،ويقوم هذا الجرم على استراتيجية الضغط المتكرر التي يمارسها قراصنة محترفون ضد الأفراد أو المؤسسا،بهدف إخضاع الضحية ومطالبتها بمقابل مادي أو فدية مالية مقابل كف الأذى التقني وإعادة النظام لحالته الطبيعية.

من المنظور الإنساني والقانونيلا يُعد هذا الفعل مجرد اختراق تقني،بل هو اعتداء مباشر على حق الملكية الرقمية وحرية العمل واستغلال غير مشروع للقدرات البرمجية لتحقيق كسب مادي تحت وطأة التهديد، مما يستدعي تدخلاً تشريعياً حازماً لتجريم هذه الممارسات وحماية الفضاء الرقمي من الاستغلال القسري.

خامسا:جرائم الإلكترونية ضد الملكية:تُعد الجرائم الإلكترونية الموجهة ضد الملكية اعتداءً مباشراً على الأصول المعنوية والرقمية للمؤسسات سواء كانت حكومية،[3] خاصة أو فردية، حيث تنطوي قانوناً على استهداف عمدي لإتلاف الوثائق الحيوية أو تخريب البرمجيات والأنظمة الجوهرية التي تعتمد عليها تلك الجهات.

وتتجسد الخطورة الإنسانية والمهنية لهذه الأفعال ،في سعي الجناة لتعطيل المصالح العامة والخاصة عبر حقن الأنظمة ببرمجيات ضارة وتخريبية مستغلين وسائل الاتصال الرقمي،مثل الرسائل الإلكترونية المفخخة كقنوات لتنفيذ هذا التعدي ومن منظور الأمانة العلمية والقانونية يُصنف هذا السلوك ،كجريمة إتلاف عمدي للممتلكات الفكرية والبيانات، حيث يتجاوز ضررها الخسارة المادية ليصل إلى تقويض الثقة في أمن

[1] الطاهر ياكر،المرجع السابق،ص07.

[2] الطاهر ياكر،المرجع نفسه،ص07.

[3] الطاهر ياكر،المرجع نفسه،ص07.

المعلومات واستقرار المؤسسات،مما يفرض ضرورة توفير حماية قانونية صارمة تصون حق الملكية في الفضاء الرقمي وتضمن سلامة المحتوى المعلوماتي من العبث أو التدمير الممنهج.[1]

كما تمتد هذه الجرائم إلى سرقة الأسرار التجارية والبيانات الاقتصادية الخاصة بالمؤسسات ،وهو مايشكل إعتداء على المنافسة المشروعة ويهدد الأمن الاقتصادي للمؤسسة التجارية.

سادسا:مجموعة أخرى من الجرائم الإلكترونية العديدة:تشمل هذه الحزمة من الانتهاكات الرقمية اعتداءات مباشرة على الكرامة الإنسانية والحق في الخصوصية، حيث تبرز جرائم التشهير والسب والقدح كأدوات لتشويه السمعة وتزييف الحقائقويتزامن ذلك مع المطاردة الإلكترونية،التي تعتمد على تتبع الضحايا وجمع بياناتهم الشخصية من منصات التواصل بغرض التحرش أو الابتزاز المالي.

بالإضافة إلى التصيد الاحتياليالذي يستهدف استدراج الأفراد تقنياً والجرائم ذات الأبعاد الأخلاقية وقانونياً تُعد هذه الممارسات انتهاكاً جسيماً للحريات الشخصية والأمن النفسي، إذ تحول الوسائل التكنولوجية إلى أدوات للقمع والإحراج العام،مما يستوجب حماية قانونية تصون الحرمات وتكافح الاستغلال الرقمي بكافة صوره.[2]

المطلب الثاني:خصائص وأركان الجريمة الإلكترونية

تتطلب الإحاطة بالجريمة الإلكترونية الماسة بالمعاملات التجارية تفكيك طابعها القانوني،فالنص العقابي يهدف أساسا إلى حماية المراكز القانونية لأطراف التعامل ،وبناءا على ذلك ينقسم هذا المكلب إلى فرعين،الفرع الأول خصائص هذه الجريمة والفرع الثاني أركانها.

الفرع الأول:خصائص الجريمة الإلكترونية

تأخذ الجريمة الإلكترونية أبعاداً تتجاوز الأطر التقليدية التي ألفها الفقه القانوني، فهي ليست مجرد فعل مادي يترك أثراً ظاهراً في الواقع الملموس،بل هي سلوك إجرامي معقد ينسج خيوطه في ثنايا البيئة الرقمية وشبكات الاتصالهذا الانتقال من العالم المادي إلى الفضاء الافتراضي،يمنح هذه الجرائم طبيعة مراوغة.

حيث يختبئ الجاني خلف ستار التقنية مما يجعل من رصد النشاط الإجرامي أو تتبع أثره الرقمي مهمة شاقة للغاية،إن ما يميز هذا النمط من الانتهاكات هو افتقاره للعناصر المادية التقليدية واعتماده

[1] الطاهر ياكر، المرجع السابق، ص07.

[2] الطاهر ياكر،المرجع نفسه، ص06.

الكلي على الوسائط التكنولوجية وهو ما يضفي عليها خصوصية بنيوية ،تجعل من آليات اكتشافها والتصدي لها أمراً يتطلب مقاربات قانونية وتقنية مغايرة تماماً لما هو سائد في الجرائم الكلاسيكية،وهو مايظهر، من خلال خصائصها المميزة لها عن باقي الجرائم التقليدية.

أولا:الجريمة الإلكترونية من الجرائم العابرة للحدود

تُعد الجريمة الإلكترونية نموذجاً حداثياً للجرائم العبر وطنية، حيث تخلت الجريمة في ثوبها الرقمي عن مفهوم الحدود الجغرافية التقليدي،فمتى ما انصرف السلوك إلجرامي إيجاباً أو سلباً عبر وسيط معلوماتي للاعتداء على الحقوق والمصالح التي يسبغ عليها القانون حمايته أو استهدف المكونات المنطقية للحاسوب ،ونظم الشبكات وتمددت آثاره لتشمل سيادة أكثر من دولة نكون بصدد جريمة عابرة للحدود بامتياز.[1]

إن الصفة الدولية هي السمة الملازمة لهذا النوع من الإجرام،إذ تتيح الشبكة المعلوماتية للجاني تجاوز العوائق المكانية بيسر شديد ويبرز الواقع العملي خطورة هذا البعد في حوادث شهيرة، كتمكن مخترق من أوروبا من كسر شفرات مراكز بيانات حساسة في وزارة الدفاع الأمريكية (البنتاغون)، مما مكنه من العبث ببيانات استراتيجية، ناهيك عن الانتشار العالمي للفيروسات البرمجية التي لا تعترف بالحدود السياسية.

تثير هذه الطبيعة العابرة للقارات معضلات قانونية وإدارية وفنية معقدة،لعل أبرزها إشكالية تنازع الاختصاص القضائي وتحديد الدولة الأحق بمحاكمة الجاني، بالإضافة إلى التحديات السياسية المرتبطة بإجراءات الملاحقة الجنائية وجمع الأدلة الرقميةولأجل ذلك تعالت الأصوات المنادية بضرورة إرساء قواعد للتعاون الدولي المكثف،يهدف إلى التوفيق بين التشريعات الوطنية المتباينة وضمان انسيابية تبادل المعلومات وتسهيل تسليم المجرمينواعتراف المحاكم بالأدلة الرقمية المستخلصة في دول أخرى.[2]

وفي هذا السياق تبرز الجهود المحورية لمنظمة "الإنتربول" عبر ضباط الارتباط وقواعد البيانات الضخمة التي تشكل حجر الزاوية في ملاحقة الجناة دولياً.

وعلى صعيد التشريع الجزائري فقد أبدى المشرع استجابة استباقية وفعالة من خلال المنظومة القانونية المتكاملة لاسيما القانون رقم 09-04 [3]المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

---

[1]عفاف لعقون، مرجع سابق،ص262.

[2]عفاف لعقون، مرجع نفسه،ص262.

[3]قانون رقم 09-04،المرجع السابق،ص03.

والذي استحدث قواعد إجرائية مرنة تتعلق بالتفتيش والحجز الرقمي وأسس الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،كما تضمن هذا القانون أحكاماً صريحة للتعاون والمساعدة القضائية الدولية،ويؤازر ذلك التعديل الجوهري في قانون العقوبات بموجب القانون رقم 04-15 الذي أفرد حماية جنائية خاصة للأنظمة المعلوماتية المواد 394 مكرر إلى 394 مكرر 7،مما يعكس وعي المشرع الجزائري بخصوصية هذا الإجرام وضرورة ملاحقته وطنياً ودولياً.

ثانيا:الجريمة الإلكترونية جريمة خفية

تنفرد الجريمة الإلكترونية بخصيصة الخفاء التي تميزها عن الأنماط الإجرامية التقليدية، فهي تُعد من الجرائم الذهنية التي تتطلب مهارات تقنية وفكراً علمياً دقيقاً، عوضاً عن القوة البدنية فبينما يعتمد الإجرام التقليدي،كالسرقة والقتلعلى القوة المادية التي تخلف ضجيجاً وآثاراً ملموسة تُرتكب الجريمة الإلكترونية في صمت مطبق ،ومن خلال نقرات يسيرة على لوحة المفاتيح،مما يمنحها وصف الجرائم الناعمة أو الجرائم النظيفة.[1]

وتكمن التحديات القانونية لهذا النوع من الإجرام في صعوبة إثباته مادياً إذ تفتقر مسارح الجريمة الإلكترونية إلى الأدلة المادية التقليدية ،مثل بقع الدماء أو آثار الكسر مما يجعل وسائل الإثبات الكلاسيكية غير كافية لملاحقة الجناة،هذا الواقع يفرض على الأنظمة القانونية والجهات التحقيقية الانتقال من أساليب التحقيق التقليدية إلى البحث عن الأدلة الرقمية و التقنيات البيومترية المتطورة، كالبصمات الصوتية والبصرية لضمان الكفاءة في الإثبات الجنائي ومواكبة التطور التقني الذي يستغله المجرمون للتخفي وراء شاشاتهم.[2]

ثالثا:صعوبة إكتشاف وإثبات الجريمة الإلكترونية

تُعد إشكاليةعسر الاكتشاف وصعوبة الإثبات الجنائي حجر الزاوية في دراسة الجريمة الإلكترونية،إذ يواجه النظام القضائي تحدياً جسيماً في ملاحقة أفعال جرمية تدور رحاها في فضاء افتراضي، يتسم بالسرعة الفائقة والتبدل المستمر و بخلاف الجرائم التقليدية التي تترك بصمات مادية يعتمد الجاني الرقمي على التخفي خلف ترسانة من الرموز المشفرة والأساليب التقنية التي تجعل من العثور على الدليل الرقمي عملية معقدة.

[1] عفاف لعقون،المرجع السابق،ص262.

[2] عفاف لعقون، المرجع نفسه،ص263.

مما يؤدي في كثير من الأحيان إلى اكتشاف هذه الجرائم إما عن طريق المصادفة المحضة أو بعد انقضاء زمن طويل على حدوثها وهو ما يفسر اتساع الفجوة بين الجرائم المرتكبة فعلياً وتلك التي يتم [1]كشفها،ويمكن حصر العوامل التي تكرس هذه الصعوبات في ثلاثة أبعاد رئيسية البعد الأول والعامل النفسي والمصلحي للمجني عليه، حيث يميل الضحايا سواء كانوا أفراداً أو مؤسسات مالية ضخمة إلى الصمت وعدم التبليغ خشية تضرر سمعتهم الائتمانية أو فقدان ثقة الجمهور في أمن بياناتهم فضلاً عن جهل البعض أصلاً بوقوع الاختراق.

البعد الثاني يتمثل في طبيعة الدليل الرقمي القابل للمحو إذ يمتلك المجرم المعلوماتي القدرة على طمس معالم [2]جريمته في لحظات خاطفة مستخدماً أدوات تقنية لمسح البيانات أو برمجيات انتحارية تدمر المحتوى المعلوماتي بمجرد استشعار أي محاولة دخول غير مصرح بها من جهات التحقيق مما يجعل الدليل يتطاير قبل تثبيته قانوناً أما البعد الثالث فيتعلق بـ الفجوة التقنية لدى جهاز العدالة الجنائية، حيث تتطلب عملية الإثبات كفاءة فنية استثنائية وإلماماً عميقاً بآليات المعالجة الآلية للمعطيات وأنظمة فك التشفير فالمحقق الذي لا يمتلك أدوات تكنولوجية تضاهي تلك المستخدمة في عمليات السطو الرقمي على الحسابات البنكية أو الدخول الاحتيالي للنظم المحمية سيجد نفسه أمام عائق فني يحول دون صياغة دليل إدانة متماسك مما يستدعي بالضرورة صقل الخبرات القضائية والأمنية لتتلاءم مع الطبيعة العلمية لهذه الجرائم[3].

وتزداد خطورة هذا الأمر في البيئة التجارية الإلكترونية،حيث يؤدي التأخر في اكتشاف الجريمة إلى خسائر مالية معتبرة وإلى المساس بثقة الزبائن في المعاملات الإلكترونية.

رابعا:الجريمة الإلكترونية تتم بواسطة الأجهزة الإلكترونية

تتمحور الجريمة الإلكترونية في جوهرها حول استخدام الوسيط التكنولوجي كأداة رئيسية للتنفيذ، حيث يمثل الحاسب الآلي وشبكة الإنترنت البيئة الخصبة التي تمنح الجاني نافذة مفتوحة على العالمإن الارتباط الوثيق بالمنظومة المعلوماتية العالمية جعل من ارتكاب الجريمة فعلاً عابراً للمسافات لا يتطلب من الفاعل سوى المهارة التقنية والذكاء والقدرة على توظيف البرمجيات عبر نقرات معدودة على لوحة المفاتيح.

[1] عفاف لعقون،مرجع سابق،ص263.

[2]عفاف لعقون، مرجع نفسه،ص264.

[3]عفاف لعقون، مرجع نفسه،ص264.

وعليه فإن الركن المادي في هذه الجرائم يعتمد بشكل أساسي على القوة الذهنية والعلمية بدلاً من المجهود العضلي، حيث يستغل الجاني انفتاح الشبكة الدولية لتنفيذ مخططاته الإجرامية في وقت قياسي وبأقل قدر من المخاطرة الجسدية وتعد هذه الخاصية التقنية هي المحدِد الأساسي لطبيعة الجريمة كونها لا تقع إلا من خلال استغلال الأنظمة الإلكترونية مما يضع العالم بأسره في حالة اتصال دائم ومخاطرة مستمرة تستوجب اليقظة القانونية والتقنية.[1]

الفرع الثاني:أركان الجريمة الإلكترونية

تقوم الجريمة الإلكترونية في جوهرها على ذات الأركان التي لا تكتمل أي جريمة بدونها وهي الركن القانوني الذي يحدد النص المجرم والركن المادي المتمثل في السلوك الخارجي والركن المعنوي القائم على العلم والإرادة إلا أن ما يمنحها طابعها الإنساني والتقني الخاص هو ضرورة وجود نظام المعالجة الآلية للمعطيات كشرط أولي وركن خاص، حيث لا يمكن تصور وقوع الاعتداء أو البحث في اكتمال أركانه إلا إذا استهدف هذا النظام الرقمي الذي بات يشكل مسرحاً جديداً للحياة والحقوق.

أولا:الركن الشرعي

يستند الركن الشرعي للجريمة الإلكترونية إلى المبدأ القانوني الراسخ الذي يحمي حقوق الإنسان وحرياته[2]وهو مبدأ شرعية الجرائم والعقوبات ،فلا يمكن إدانة شخص أو معاقبته إلا بناءً على نص تشريعي مسبق وواضح يضعه المشرع ليحدد السلوكيات المجرمة والعقوبات المقابلة لها وفي هذا الإطار وبموجب التعديلات القانونية أفرد المشرع الجزائري حماية قانونية خاصة للأنظمة المعلوماتية ضمن قانون العقوبات وتحديداً في القسم السابع مكرر الذي يضم المواد القانونية التي تُفصّل صور الاعتداء على أنظمة المعالجة الآلية للمعطيات، وتُعد هذه النصوص هي الضابط القانوني الذي يوازن بين زجر الاعتداءات الإلكترونية وبين ضمان العدالة، بحيث يضمن ألا يُعامل أي فعل بوصفه جريمة ما لم يرد فيه نص صريح يحمي الفضاء الرقمي للمجتمع[3].

---

[1] عفاف لعقون،مرجع سابق،ص264.

[2] مهداوي حنان،" التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري"،مجلة الفكر القانوني والسياسي،جامعة لمين دباغين،سطيف02،المجلد 06،العدد الثاني، 2022، ص1064.

[3] مهداوي حنان،المرجع نفسه، ص1064.

ثانيا:الركن المادي للجريمة الإلكترونية

يتجسد الركن المادي للجريمة الإلكترونية في التعدي الفعلي على حرمة الأنظمة المعلوماتية وسلامة معطياتها، حيث لم يعد الاعتداء يتطلب حضوراً مادياً،بل يكفي فيه الدخول أو البقاءعن طريق الغش في نظام المعالجة الآلية للمعطيات دون وجه حق وقد رسم المشرع الجزائري في المادة 394 مكرر من قانون العقوبات حدود هذا السلوك معتبراً أن مجرد التواجد غير المرخص داخل النظام أو الاستمرار فيه حتى لو كان الدخول الأول قد تم صدفة يشكل جريمة تستوجب العقاب.

كما شدد المشرع الجزائي العقوبة في ذات المادة لتصل إلى الحبس لمدة سنتين والغرامة المالية إذا ما اقترن هذا السلوك بمحو البيانات أو تعديلها أو أدى إلى تخريب نظام اشتغال المنظومة وإعاقتها عن أداء وظيفتها.

[1]وتمتد الحماية القانونية لتشمل المعطيات ذاتها في صور أوسع من الاعتداء، حيث تضمنت المادة 394 مكرر 1 [2]تعديل وأهم ماجاء فيهايعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها حيث تضمنت هذه المادة عقوبات رادعة لكل من يقوم بإدخال معطيات وهمية أو تعديل البيانات الأصلية بطرق احتيالية وهو ما يعرف بجريمة التلاعب بالمعطيات.

وفي سياق تعزيز الأمن الرقمي جرمت المادة 394 مكرر 2 كل أشكال التعامل غير المشروع في المعطيات سواء ،من خلال تصميم وتجميع أدوات برمجية تسهل ارتكاب الجرائم الإلكترونية، أو عبر حيازة ونشر معطيات تم الحصول عليها أصلاً من فعل إجرامي سابق إن هذه المنظومة القانونية بموادها المعدلة 394 مكرر، 394 مكرر 1، 394 مكرر 2تعكس حرص المشرع على تطويق الأساليب التقنية المتطورة التي تمس بكيان البيانات وحقوق أصحابها في بيئة رقمية آمنة.[3]

[1]مهداوي حنان ،مرجع سابق، ص1065.

[2] المادة 394 مكرر1 من الامر 66-156 المتضمن قانون العقوبات،المعدل والمتمم بالقانون 04-15 المؤرخ في 10نوفمبر 2004 والمعدل بموجب القانون 24-06.

[3]مهداوي حنان،المرجع السابق،ص1065_1066.

ثالثا:الركن المعنوي للجريمة الإلكترونية

يُعد الركن المعنوي الجوهر الذي يربط الفعل المادي بنية الجاني، حيث أجمع الفقه والتشريع على أن الجريمة الإلكترونية،وفي مقدمتها جريمة الدخول غير المشروع،هي جريمة عمدية بامتياز فلكي تكتمل أركان الجريمة قانونًالا بد أن تتجه إرادة الفاعل إلى اقتحام النظام المعلوماتي مع علمه اليقيني بأن هذا الفعل محظور قانوناً، مما ينفي المسؤولية الجنائية في حالات الدخول العرضي أو الذي يقع نتيجة خطأ تقني غير مقصود وهو ما أيدته توجهات قضائية دولية كمحكمة استئناف باريس ويقوم هذا الركن على ركيزتي العلم بمكونات الجريمة والإرادة التي تتجه لتحقيق النتيجة الإجرامية أو قبولها وهو ما يعكس نية الجاني المبيتة لحظة الاعتداء.[1]

وفي حين يتطلب القانون توافر القصد الجنائي العام في كافة صور الجرائم الإلكترونية،إلا أن بعضها كجريمة تشويه السمعة عبر الإنترنت يستلزم قصداً جنائياً خاصاً يتجاوز مجرد الفعل إلى نية تحقيق غاية محددة ومن الناحية العملية ينبغي أن يحيط علم الجاني بكافة العناصر المادية للجريمة وعلى رأسها موضوع الحق المعتدى.

عليه فالمجرم المعلوماتي يجب أن يدرك أن فعله ينصب على مستند إلكتروني أو نظام محمي قانوناً، ورغم أن انتفاء العلم يؤدي قانوناً إلى انتفاء القصد الجنائي، إلا أن هذا الفرض يظلنادراً في الواقع العملي نظراً لما يتمتع به مرتكبو هذه الجرائم من خبرة تقنية عالية تجعل من الصعب التسليم بوقوع الدخول دون إدراك أو معرفة مسبقة.[2]

تتطابق الجريمة المعلوماتية مع القواعد العامة للتشريع الجنائي في ضرورة اقتران السلوك المادي بنية جرمية واضحة لتحديد المسؤولية القانونية، حيث لا يمكن تصور قيام قصد جنائي خاص بمعزل عن وجود القصد العام أولاً.

ويقوم الركن المعنوي في هذا الفضاء الرقمي على ثنائية العلم الذي يعكس إدراك الجاني لطبيعة نشاطه غير المشروع و الإرادة،التي توجه هذا النشاط نحو تحقيق نتيجة إجرامية محددة،وبينما يكتفي القصد الجنائي العام بالرغبة في ارتكاب الفعل المجرم بحد ذاته يتطلب القصد الخاص في بعض الجرائم الإلكترونية،مثل تشويه السمعة أو نشر الفيروساتسعي الجاني الحثيث لضمان وقوع النتيجة الضارة وتأكيد أثرها وبموجب

[1] شهاب بن عبد الرحمن بن حامد المسعود،"أركان الجريمة الإلكترونية"،المجلة الدولية والدراسات القانونية،،جامعة الملك عبد العزيز،الإصدار الرابع،العدد الرابع،سنة 2025،ص52.

[2] شهاب بن عبد الرحمان بن حامد المسعود،مرجع نفسه،ص52.

التطورات التشريعية الأخيرة يظل القصد العام ركيزة ثابتة في كل الجرائم المعلوماتية ،دون استثناءفي حين يقع عبء إثبات هذا القصد واستخلاص سوء النية على عاتق النيابة العامة والمحكمة المختصة التي تنفرد بسلطة تقدير الوقائع،وتحديد مدى توافر النية الجرمية بناءً على المعطيات التقنية والقانونية المعروضة أمامها.[1]

المبحث الثاني:ماهية المعاملات التجارية

تعد المعاملات التجارية الركيزة الأساسية التي يقوم عليها النشاط الاقتصادي،وهي تشهد تطوراً مستمراً يواكب التحولات الرقمية والتقنية المعاصرة و لتحديد نطاق الحماية القانونية ضد الجرائم الإلكترونية يبرز البحث في ماهية هذه المعاملات كضرورة حتمية،وذلك من خلال ضبط مفهومها وتحديد دلالاتها الاصطلاحية والقانونية بدقة.

كما يستوجب الأمر التمييز بين المسارات التي تتخذها هذه المعاملات عبر تصنيف ممارساتها من حيث المشروعية،صوناً للأنشطة القائمة على النزاهة والشفافية وكشفاً للممارسات التدليسية وغير النزيهة التي تشكل ثغرة للإجرام المعلوماتي،وهو ما سيتم تفصيله من خلال المطلبين الآتيين،المطلب الأول ماهية المعاملات التجارية أما المطلب الثاني تصنيف الممارسات التجارية من حيث المشروعية.

المطلب الأول:مفهوم المعاملات التجارية

يمثل تحديد مفهوم المعاملات التجارية ،المدخل الأساسي لفهم طبيعة العلاقات المالية والتبادلية التي تتم في السوق، خاصة في ظل تداخل الأنشطة الاقتصادية الحديثة،ويهدف هذا المطلب إلى تأصيل هذا المفهوم من خلال ضبط دلالاته المختلفة بدءاً من التعريف العام للمعاملة التجارية وصولاً إلى التدقيق في معانيها من الناحيتين الاصطلاحية و القانونية و ذلك لرسم حدود واضحة تميز النشاط التجاري وتحدد القواعد والقوانين الناظمة له،وعليه سيتم تناول في الفرع الأول التعريف الإصطلاحي للمعاملات التجارية أما في الفرع الثاني لتعريفها القانوني.

[1] شهاب بن عبد الرحمان بن حامد المسعود،مرجع سابق،ص53.

الفرع الأول:التعريف الإصطلاحي للمعاملات التجارية

لم يضع الفقهاء تعريفاً واحداً متفقاً عليه للمعاملة التجارية بل انقسمت آراؤهم بناءً على الزاوية التي ينظرون منها إلى النشاط التجاري، ويمكن حصر هذا المفهوم في اتجاهين أساسيين:[1]

أولا_المفهوم الاقتصادي :ينظر هذا الاتجاه للمعاملة التجارية على أنها نشاط [2]يتوسط بين مرحلة الإنتاج ومرحلة الاستهلاك،فالمعاملة تكون تجارية اصطلاحا عندما تهدف إلى تداول الثروات أي انتقال السلعة من يد بقصد الربحوبناء عليه،فإن الأنشطة التي لاتتضمن وساطة كالفلاحة أو المهن الحرةت خرج اصطلاحا من المفهوم الضيق.[3]

ثانيا_المفهوم الفقهي:توسع هذا التعريف ليشمل كل نشاط إلى المضاربة وهي وراء العمل وترى الدكتورة نادية فضيل أن المعاملة التجارية اصطلاحا هيتلك الأنشطة التي تتجاوز مجرد توزيع السلع لتشمل العمليات التحويلية والصناعية وإنتاج الخدمات،حيث يصبح عنصر المخاطرة وتحمل التبعات المالية جزءا لايتجزأ من تعريف المعاملة،وعليه المعاملة التجارية اصطلاحا هي مزيج بين الوساطة في التداول وقصد المضاربة تحقيقا للربح،وهو مايميزها جوهرها عن الأعمال المدنية التي تفتقد لأحد هذين الركنين.

الفرع الثاني:التعريف القانوني للمعاملات التجارية

على خلاف الفقه، نجد أن المشرع الجزائري لم يعتمد تعريفاً نظرياً واحداً، بل اعتمد مقاربة واقعية تتجلى في ثلاثة نصوص قانونية أساسية تحدد ماهية المعاملة من زوايا مختلفة

أولا:تعريف المعاملات التجارية في القانون التجاري:

يُعرف القانون الجزائري المعاملة التجارية بناءً على طبيعة العمل،فكل تصرف يندرج تحت نص المادة 2 من القانون التجاري (مثل: شراء العقارات أو المنقولات لإعادة بيعها، أعمال البنوك، السمسرة، التأمين) يعتبر معاملة تجارية قانونية بقوة القانون، بغض النظر عن صفة القائم بها سواء كان تاجراً أو غير تاجر.[4]

---

[1]نادية فضيل،القانون التجاري الجزائرري (الاعمال التجارية–التاجر– المحل التجاري)،ديوان المطبوعات الجامعية،الجزائر،الطبعة 06، 2024،ص11.

[2] نادية فضيل،المرجع نفسه،ص11.

[3]نادية فضيل ،مرجع نفسه، ص11.

[4]المادة 02 من الامر رقم 75–59،المؤرخ في 26 سبتمبر 1975، المتضمن القانون التجاري الجزائري،المعدل والمتمم.

ثانيا_تعريف المعاملات التجارية في قانون التجارة الالكترونية: بسبب التطور التكنولوجي وضع المشرع تعريفاً حديثاً للمعاملة في المادة 06 من القانون 18-05، حيث عرفها بأنها: "النشاط الذي يتم من خلاله قيام مورد إلكتروني بعرض أو توفير سلع وخدمات لزبون إلكترونيعبر اتصالات إلكترونية"،وهذا التعريف القانوني يركز على الوسيلة الاتصال الإلكتروني والظرف المكاني عن بُعد كمعيار لتحديد قانونية المعاملة التجارية الحديثة.[1]

ثالثا_تعريف المعاملات التجارية في قانون الممارسات التجارية: يعرّف القانون المعاملة من منظور الممارسة في المادة 03، بأنها كل نشاط يمارسه عون اقتصادي بصفة مهنية يتعلق ببيع السلع أو تقديم الخدماتهذا التعريف يوسع نطاق المعاملة التجارية لتشمل حتى الأنشطة التي يقوم بها أشخاص معنويون عامون إذا كانت تكتسي طابعاً تجارياً.[2]

المطلب الثاني:تصنيف الممارسات التجارية من حيث المشروعية

لا تكتمل الصورة المفاهيمية للمعاملات التجارية إلا بفحص طبيعة السلوكيات التي تمارس في إطارها وتقييمها بميزان المشروعية والقانون، فالمعاملة التجارية ليست مجرد تبادل للمنافع،بل هي سلوك محكوم بضوابط أخلاقية وقانونية تضمن استقرار السوق.

وسنحاول من خلال هذا المطلب تسليط الضوء على الانقسام الجوهري في هذه الممارسات،وذلك بالتمييز بين الممارسات المشروعة ،التي تتخذ من النزاهة والشفافية ركيزة لها في الفرع الأول وبين الممارسات غير المشروعة القائمة على التدليس وعدم النزاهة، والتي تعد المدخل الأول والبيئة الخصبة لوقوع الجرائم الإلكترونية الماسة بالمعاملات التجارية.

الفرع الأول:الممارسات التجارية المشروعة القائمة على النزاهة والشفافية

تعد الأخلاق الركيزة الجوهرية التي تُصاغ من خلالها القيم الفاضلة داخل المجتمع،فهي تهدف في جوهرها الإنساني إلى حماية التعاملات من الأنانية والاستغلال معززةً مبادئ الصدق ،وحسن النية كمعايير واجبة

[1] المادة 06 من القانون رقم 18-05 المؤرخ في 10 مايو 2018،يتعلق بالتجارة الالكترونية، الجريدة الرسمية، العدد ثمانية وعشرون، 2018.

[2] المادة 03 من القانون رقم 04-02 المؤرخ في 23 جوان 2004،المحدد للقواعد المطبقة على الممارسات التجارية، الجريدة الرسمية،العدد واحد واربعون، سنة 2004.

الاحترام لتحقيق العدل والمساواة، وقد امتد هذا المفهوم الأخلاقي ليشمل صلب الحياة الاقتصادية،حيث حدد فلاسفة الاقتصاد الحديث فضائل أساسية تحكم سلوك السوق، من أبرزها النزاهة والعدالة والشجاعة والتحوط القائم على المعرفة والبصيرة[1].

واستجابةً لهذه الضرورات الأخلاقية حرص المشرع على تكريس مبدأي الشفافية والنزاهة كركيزتين أساسيتين في قانون الممارسات التجارية فبعد أن كان الأمر الملغى 95-06 يدمج بين أحكام المنافسة والممارسات التجارية، خطى المشرع خطوة نوعية بصدور القانون 04-02 المتعلق بالممارسات التجارية والأمر 03-03 [2]المتعلق بالمنافسة.

ومن خلال هذا الفصل نجح المشرع في إخضاع الأفعال التجارية لمعايير دقيقة تضمن شفافية الممارسة ونزاهتها مما يعكس توجهاً تشريعياً حديثاً ،يهدف إلى ضبط السوق عبر موازنة النصوص القانونية بالقيم الأخلاقية المتأصلة وهو تقسيم وُفق فيه المشرع لضمان استقرار المعاملات وحماية المتدخلين الاقتصاديين.

أولا:الممارسات التجارية المشروعة القائمة على النزاهة

تتجلى النزاهة في قانون الممارسات التجارية كقيمة معنوية وفضيلة أخلاقية كرسها المشرع الجزائري كأداة لضبط سلوك السوق والارتقاء بالمعاملات التجارية،وقد أولى المشرع أهمية بالغة لهذا المبدأ في القانون رقم 04-02، [3]حيث خصص له الباب الثالث تحت عنوان نزاهة الممارسات التجارية، والملاحظ أن المشرع اعتمد في صياغته لهذا الباب منهجاً سلبياً أو عكسياً.

إذ لم يضع تعريفاً مباشراً وجامعاً للنزاهة،بل حدد معالمها من خلال حصر الأفعال المناقضة لها والمنهية عنها في خمسة فصول،فشمل الفصل الأول الممارسات التجارية غير الشرعية وتلاه الفصل الثاني بممارسة أسعار غير شرعيةثم الممارسات التدليسية وغير النزيهة، وصولاً إلى الفصل الخامس الذي ضبط الممارسات

[1] بن شيخ راضية، نساخ فطيمة، " الشفافية وعلاقتها بالنزاهة الممارسات التجارية"، المجلة الجزائرية للعلوم القانونية السياسية، كلية الحقوق جامعة الجزائر، المجلد57،العدد الخامس،ديسمبر2020، ص412.

[2] الأمر 03-03 المتعلق بالمنافسة المؤرخ في 19 جمادى الأولى عام 1424 الموافق ل19 يوليو سنة 2003،الجريدة الرسمية للجمهورية الجزائرية، العدد ثلاثة واربعون، الصادر بتاريخ 20 يوليو2003، ص23.

[3] بن شيخ راضية, نساخ فطيمة, مرجع سابق, ص411.

التعاقدية التعسفية هذا التحديد بالضد، يعكس رغبة المشرع في محاصرة كافة صور الخروج عن السلوك القويم لضمان التزام الأعوان الاقتصاديين بالنزاهة في كافة تعاملاتهم.

وفي ظل غياب تعريف نصي مباشر للنزاهة في قانون الممارسات التجارية بخلاف مصطلحات أخرى [1]كالعون الاقتصادي والمستهلك يبرز الدور الفقهي في تحديد مفهومها،فالنزاهة لغةً واصطلاحاً تعني البعد عن الظلم والتعسف وتتمثل في منظومة قيمية تهدف للمحافظة على الموارد واستئصال الفساد عبر الصدق والأمانة وعدم الإضرار بالغير،وتتلاقى هذه الرؤية مع مبادئ الفكر الإسلامي التي تفرض الوفاء بالعقود والعهود وتنفيذ ما تم الالتزام به بحسن نية مع ربط العدالة بالإحسان والأخلاق.

مما ينتج عنه قواعد شرعية وقانونية تمنع الغش وتجرم الاستغلال والتعسف في استعمال الحق وتتميز النزاهة بكونها مفهوماً أوسع من مجرد الأمانة، فهي تشمل الكفاءة واحترام الالتزامات خاصة عندما تصطدم مصلحة الفرد بقراراته وأفعاله.

وعلى الصعيد العقدي تبرز النزاهة كمكمل ضروري للعدالة العقدية، حيث يفرض واجب النزاهة تنفيذ [2]الالتزامات بطريقة مفيدة وأمينة ويستند هذا الواجب إلى نظرية توابع العقد القائمة على حسن النية والتي ترسم حدود التصرف بين المتعاقدين ،وتمنع الطرف الذي ينفرد بتحرير العقد من فرض شروط خفية أوتعسفية لم يقبلها الطرف الآخر.

وقد تبنى القضاء الحديث هذا التوجه بفرض سلوك نزيه وشرعي على المتعاقدين متجاوزاً النظرة الفردية الضيقة للعلاقات العقدية،وهو ما كرسه المشرع الجزائري في المادة الأولى من القانون 04-02 بجعل النزاهة أساساً للعلاقة بين العون الاقتصادي ومنافسيه من جهة وبينه وبين المستهلك من جهة أخرى.

أما بخصوص كيفية قياس هذه النزاهة في الواقع العملي، فقد اعتمد المشرع في المادة 26 من القانون 04-02[3]معيار الأعراف التجارية النظيفة والنزيهة، وبالرغم من أن العرف التجاري يتميز بالمرونة والسرعة في التغير ،وفقاً لمستجدات العصر إلا أنه يظل القاعدة التي استقرت عليها المعاملات وساد الاعتقاد بإلزاميتها

[1] بن شيخ راضية،نساخ فطيمة،المرجع السابق،ص411.

[2] بن شيخ راضية،نساخ فطيمة،المرجع نفسه،ص411.

[3] المادة 26 من القانون 04-02،الذي يحدد القواعد المطبقة على الممارسات التجارية،المؤرخ في23يونيو سنة 2004،المعدل والمتمم،الجريدة الرسمية 41،ص23.

ما لم تخالف القانون ويتم تقدير هذه النزاهة قضائياً إما بمعيار سلبي عبر البحث عن مظاهر سوء النية كالخطأ الجسيم والتدليس والتعسف أو بمعيار إيجابي.

يستند إلى نموذج الرجل العادي، الذي يضمن تنفيذ التزاماته بصدق وأمانة في ظل الظروف المتاحة و بذلك تظل النزاهة قاعدة سلوك أخلاقية وقانونية تفرض على المتعامل الاقتصادي الالتزام بمسار مهني نزيه يحمي استقرار السوق وحقوق جميع أطرافه.

ثانيا:الممارسات التجارية المشروعة القائمة على الشفافية

تُعد الشفافية ركيزة جوهرية ضمن منظومة واجب الاستقامة والنزاهة، وهي المبدأ الأصيل الذي يحكم قانون الممارسات التجارية ،ويجد في مبدأ النزاهة سنداً مكملاً له وبالرغم من أن المشرع الجزائري لم يضع تعريفاً اصطلاحياً محدداً للشفافية ضمن نصوص قانون الممارسات التجارية.

إلا أن الفقه القانوني والاقتصادي يجمع على أنها تتمثل في إتاحة المعرفة الشاملة بكل ظروف السوق وهذا يقتضي تمكين كل طرف، سواء كان بائعاً أو مشتراً، من الوقوف بدقة على أثمان السلع والخدمات وكافة تفاصيل العروض والطلبات داخل الأسواق[1].

ويتجلى البعد الإنساني والقانوني لهذا المبدأ في كونه يضمن توفير تدفق مستمر للمعلومات الأساسية للزبون بخصوص الأسعار والكميات والنوعية مما يجعل قراره بالتعاقد نابعاً من إدراك حقيقي للواقع، حيث إن غياب هذا الوضوح يؤدي حتماً إلى زعزعة استقرار السوق وإحداث اختلالات تضر بالعدالة التجارية وفي مقابل ذلك تظهر السريةكلفظ مناقض تماماً للشفافية فهي تعبر عن حجب المعارف والسكوت الذي قد يؤدي إلى تضليل الأطراف الضعيفة في العلاقة التجارية[2].

وقد كرس المشرع الجزائري سمو مبدأ الشفافية على السرية من خلال المادة الأولى من القانون 04-02[3]،التي تهدف إلى ضبط قواعد الشفافية والنزاهة في الممارسات التي تتم بين الأعوان الاقتصاديين أنفسهم، أو في علاقتهم مع المستهلكين مع التركيز بشكل خاص على حماية المستهلك وإعلامه.

[1] بن شيخ راضية،نساخ فطيمة، مرجع سابق،ص411.

[2] بن شيخ راضية،نساخ فطيمة،مرجع نفسه،ص411.

[3] المادة 1 من القانون04-02،مرجع السابق،ص23,

إن هذه الأهمية القانونية للشفافية تتجاوز مجرد التنظيم التقني لتصل إلى بناء جسور الثقة،فهي تمنح المستهلك حرية الاختيار و تضمن للعون الاقتصادي الحصول على معاملة عادلة ومكافئة ،لما يحظى به غيره من المتدخلين، مما يساهم في الارتقاء بسلوكيات السوق والحد من الممارسات السلبية التي قد يعتقد البعض خطأً أنها اعتيادية في ظل غياب الرقابة والشفافية المطلوبة.[1]

الفرع الثاني:الممارسات التجارية الغير المشروعة التدليسية وغير النزيهة

يسعى القانون رقم 04-02 المتعلق بالممارسات التجارية إلى إرساء ميثاق أخلاقي يضبط العلاقة بين الأعوان الاقتصاديين والمستهلكين ،بناءً على مبدأي الشفافية والنزاهة ويهدف هذا التوجه التشريعي إلى حماية المستهلك وصون كرامته الاقتصادية ،من خلال فرض بيئة قائمة على الثقة والوضوح التام في المعاملات.

ومن هذا المنطلق حظر المشرع الجزائري كافة السلوكيات التدليسية والأساليب الاحتيالية التي تخرج عن[2]إطار الأعراف التجارية النظيفة فاعتبر الممارسات غير الشرعية، مثل ممارسة أسعار غير قانونية أو التلاعب بمواصفات الأماكن التجارية جرائم تستوجب الردع لحماية حق المستهلك في الاختيار الحر والآمن،وضمن هذا السياق يأتي هذا الفرع لتسليط الضوء على كيفية تنظيم المشرع لهذه الممارسات في المواد من 14 إلى 20 بهدف محاصرة كل أشكال التعسف وضبط حدود المنافسة المشروعة.

أولا:الممارسات التجارية التدليسية

تعتبر الممارسات التجارية التدليسية من أخطر السلوكيات التي يلجأ إليها بعض الأعوان الاقتصاديين، حيث تعتمد في جوهرها على استخدام وسائل احتيالية ،تهدف إلى تحقيق أرباح طائلة حتى وإن كان ذلك على حساب المصالح الاقتصادية للمستهلكين.[3]

وبناءً على ذلك تدخل المشرع الجزائري بموجب القانون رقم 04-02 لحماية إرادة المستهلك، من أي تضليل قد يدفعه للتعاقد بناءً على معطيات تخالف الحقيقة،وقد حظر المشرع هذه الممارسات صراحةً في المادتين 24 و25 فارضاً على العون الاقتصادي الالتزام بأمانة المعاملة والابتعاد عن كل ما من شأنه تزييف الواقع التجاري.

---

[1] بن شيخ راضية،نساخ فطيمة، مرجع سابق، ص412.

[2] نواصر الطاهر وغزالي نصيرة،" ممارسات التجارية التدليسية وغير النزيهة في قانون رقم 04-02 المعدل والمتمم"، مجلة الفكر القانوني والسياسي،جامعة الحاج موسى،تمنراست،جامعة ثليجي بالاغواط،المجلد 06،العدد الأول، 2022، ص1214.

[3] نواصر الطاهر وغزالي نصيرة،المرجع نفسه، ص1214.

وتتجلى صور تزييف المعاملات التجارية، كما نصت عليها المادة 24، في عدة أفعال تهدف في مجملها إلى إخفاء الشروط الحقيقية للتعامل[1]:

دفع أو استلام فوارق مخفية للقيمة: وتتمثل في لجوء العون الاقتصادي لطرق ملتوية لإخفاء القيمة الحقيقية لصفقاته، كأن يُصرح بمعاملة واحدة من أصل اثنتين لإخفاء رقم أعماله الحقيقي وتشمل هذه الفوارق كافة المبالغ غير المصرح بها في وثائق الإثبات كأن يضطر المستهلك لدفع مبلغ يفوق المدون في الفاتورة، وهو سلوك يهدف غالباً للتهرب الضريبي ويشكل جريمة غش جبائي[2].

تحرير فواتير وهمية أو مزيفة: تُعد الفاتورة أداة الضبط الجوهرية لضمان شفافية السوق، فهي التي تُعلم المستهلك بالسعر الحقيقي وشروط البيع،لذا فإن أي تلاعب بها يُعد جريمة طبقا للمادة 25 حيث تُعتبر الفواتير الوهميةأو فواتير المجاملة وثائق لا وجود حقيقي لمعاملاتها وتُحرر فقط لإيهام الرقابة بسلامة النشاط أو لاختلاس أموال المؤسسات ،أما الفواتير المزيفة فهي فواتير لمعاملات حقيقية لكنها تعرضت للتزوير في بياناتها مثل السعر أو الكمية بهدف تخفيض القاعدة الضريبية، تبييض الأموال، أو الحصول غير المشروع على قروض واستردادات ضريبية.[3]

إتلاف الوثائق التجارية والمحاسبية وإخفاؤها: جرم المشرع فعل إتلاف أو إخفاء الدفاتر والوثائق ،لا سيما الفواتير قبل انقضاء المدة القانونية المقررة بعشر سنوات، ويأخذ التزوير هنا صورتين إما مادياً بالزيادة أو الحذف أو التعديل الذي يترك أثراً ملموساً، أو معنوياً بتغيير مضمون الوثيقة وظروفها بشكل لا يدركه البصر ويُعد هذا التلاعب المحاسبي من أكثر وسائل الغش الجبائي شيوعاً،حيث يهدف لتغيير محتوى التصريحات المقدمة للإدارة الجبائية.

ولردع هذه الممارسات أقر المشرع في المادة 37 عقوبات مالية صارمة تتراوح بين 300.000 دجو10.000.000،كما أضاف القرار المؤرخ في أوت 2013 جزاءات جبائية إضافية تصل إلى غرامة تساوي 50% من قيمة الفواتير المزورة تُطبق على من حررها ومن استلمها مع استرجاع كافة مبالغ الرسوم

[1] نواصر الطاهر وغزالي نصيرة،المرجع السابق، ص1214.

[2] نواصر الطاهر،غزالي نصيرة،مرجع نفسه،ص1214.

[3] نواصر الطاهر،غزالي نصيرة،مرجع نفسه،ص1215.

التي تم التهرب منها إن هذه المنظومة تهدف في كليتها إلى ضمان نزاهة السوق وصون حقوق المستهلك من أي تلاعبات تمس سلامة تعاملاته المالية.[1]

ومن زاوية أخرى تشكل المضاربة غير المشروعة مظهراً آخر من مظاهر الممارسات التدليسية التي تمس بنزاهة السوق، وقد أفرد لها المشرع الجزائري في المادة 25 من القانون رقم 04-02 المعدل والمتمم نصوصاً صريحة تحظر كل سلوك ،يهدف إلى التلاعب بوفرة المنتجات أو أسعارها،وتتجلى أولى صور هذه الممارسة في حيازة منتجات مستوردة أو مصنعة بصفة غير شرعية و هي المنتجات التي تفتقر للمشروعية القانونية لكونها مقلدة أو مزورة للعلامات التجارية.

مما يجعل حيازتها جنحة تقليد مكتملة الأركان وفقاً للأمر رقم 03-06 [2]المتعلق بالعلامات ويمتد هذا التجريم ليشمل الجرائم الجمركية [3]في حال كانت البضائع مستوردة دون وثائق ثبوتية أو منتهكة لحقوق الملكية الفكرية وبراءات الاختراع.

حيث تقوم الجريمة هنا على ركن مادي متمثل في الحيازة الفعلية، وركن معنوي يتجسد في علم العون الاقتصادي الصريح بحظر تداول هذه المنتجاتولا تقف الحماية عند العقوبات الجزائية التي تبدأ من 300,000 دج وتصل إلى 10,000,000 دج، بل تمتد لتمنح المستهلك حق إبطال العقد استناداً لعيب الغلط، مع حقه في طلب التعويض عن أي ضرر يلحق به جراء استهلاك هذه السلع المقلدة.

أما الصورة الثانية والأكثر تأثيراً على القدرة الشرائية للمواطن،فهي حيازة مخزون من المنتجات بهدف تحفيز الارتفاع غير المبرر للأسعار وهو ما يُعرف قانوناً بالاحتكار،يهدف المشرع من خلال حظر هذا السلوك إلى منع انفراد العون الاقتصادي بالسيطرة على سلعة ما أو احتباسها عن التداول الطبيعي بقصد إحداث ندرة مصطنعة ترفع قيمتها السوقية، وهو ما يتوافق مع روح المادة 06 [4]من الأمر رقم 03-03 المتعلق بالمنافسة أهم ماتناولت مايلي :"تحظر الممارسات و الأعمال المدبرة والاتفاقات الصريحة والضمنية.....الممارسات المقيدة" التي تجرم الأعمال الرامية لعرقلة حرية التنافس ويتطلب قيام هذه الجريمة أن تنصب على سلع تخضع لقانون العرض والطلب،حيث يقوم الجاني بتخزينها عمداً وعدم

[1] نواصر الطاهر،غزالي نصيرة،مرجع سابق،ص1216.

[2] الامر 03-06 المؤرخ في 19 جمادى الثانية 1427 الموافق ل15يوليو سنة 2006، المتعلق بالعلامات،الجريدة الرسمية،الجمهورية الجزائرية، العدد سبعة واربعون،الصادر بتاريخ 19 يوليو 2006،ص33.

[3] نواصر الطاهر،غزالي نصيرة،مرجع سابق،ص1217.

[4] المادة 6 من الأمر رقم 03-03،المرجع السابق،ص5.

عرضها للبيع بصفة عادية،كما يحدث في تخزين المواد الأساسية قبيل المناسبات كشهر رمضان بقصد جنائي خاص ،يتمثل في نية التحكم في السوق والتأثير على الأسعار وتخضع هذه الممارسة لذات العقوبات المالية الصارمة الواردة في المادة 37 من قانون الممارسات التجارية تأكيداً من المشرع على حماية استقرار الاقتصاد الوطني وضمان وصول السلع للمستهلكين بأسعار عادلة وشرعية[1].

تكتمل منظومة الحماية من الممارسات التدليسية ،بحظر المشرع الجزائري حيازة الأعوان الاقتصاديين لمنتوجات تخرج عن نطاق تخصصهم التجاري الشرعي بقصد بيعها إذ يفرض القانون على كل تاجر الالتزام الصارم بالنشاطات المحددة في سجله التجاري حمايةً للنظام العام الاقتصادي ومنعاً للفوضى في تداول السلع وتجسيداً لهذا الحرص.

أقر المشرع عقوبات مالية رادعة تتراوح بين ثلاثمائة ألف دينار وعشرة ملايين دينار لكل من يتجاوز موضوع تجارته المعتمد،ولم يتوقف الردع عند الغرامات المالية، بل منحت المواد 39 وما بعدها للقاضي سلطة تقديرية واسعة لفرض عقوبات تكميلية تمس كيان النشاط التجاري المخالف، بدءاً من الحجز العيني أو الاعتباري للبضائع، وصولاً إلى المصادرة والغلق الإداري للمحلات، ونشر الأحكام القضائية ليكون ذلك زجراً للمخالف وعبرة لغيره مع تشديد هذه الجزاءات في حال العود لضمان استقامة السلوك التجاري ونزاهة التعاملات داخل السوق.

ثانيا:الممارسات التجارية الغير نزيهة

تعد الممارسات التجارية غير النزيهة أفعالاً يحظرها القانون لما تنطوي عليه من أساليب تنافسية غير شريفةوقد نظمها المشرع الجزائري في المادتين 26 و27 من القانون رقم 04-02 المعدل والمتمم وتتجسد هذه الممارسات في التعدي على حقوق المنافسين عبر سلوكيات تخالف الأعراف التجارية النظيفة.

مثل تشويه السمعة والتشبيه المؤدي للبس واستغلال الأسرار المهنية وإحداث الاضطراب في السوق[2] أو في تنظيم مؤسسة المنافس ويشكل تشويه سمعة المنافس إحدى أكثر الصور شيوعاً، حيث يعمد العون الاقتصادي إلى نشر معلومات مسيئةسواء كانت صادقة أو كاذبة تستهدف النيل من شخص المنافس أو

[1] نواصر الطاهر ،غزالي نصيرة، مرجع سابق، ص1216.

[2] نواصر الطاهر ،غزالي نصيرة، مرجع نفسه، ص1216.

جودة منتجاته لزعزعة ثقة المستهلكين ودفعه للعزوف عن التعامل معه ويأخذ هذا التشويه شكلاً مباشراً ،يسهل إثباته أو شكلاً غير مباشر يتخفى غالباً في قوالب الإشهار المقارن الذي يسيء لمنتجات الغير.[1]

كما تمتد هذه الممارسات لتشمل إغراء المستخدمين، حيث يقوم العون الاقتصادي بجذب عمال المنافس ذوي الخبرة العالية عبر وعود ومزايا مادية مخالفة لتشريع العمل،مما يلحق ضرراً جسيماً برب العمل الأصلي ويخل بقواعد المنافسة الحرة وفي سياق حماية المعرفة الفنية، حظر المشرع الاستفادة من الأسرار المهنيةالتي يحوزها الأجراء أو الشركاء القدامى بما في ذلك أسرار الصنع وقوائم الزبائن معتبراً إفشاءها أو استغلالها دون إذن تطفلاً غير مشروع يهدف للإضرار بصاحب السر[2].

وعلى صعيد التنظيم العام جرم القانون إحداث ،أي خلل في تنظيم مؤسسة المنافس سواء عبر تخريب وسائله الإشهارية أو اختلاس طلبياته أو ممارسة السمسرة غير القانونية لتحويل زبائنه بطرق غير نزيهة ويتسع نطاق الحماية ليشمل نظام السوق بوجه عام،حيث يُمنع العون الاقتصادي من إحداث اضطرابات سوقية عبر التهرب من الالتزامات القانونية أو ممارسة نشاطات تخالف ما هو مدون في سجله التجاري.

كأن يمارس تجارة الجملة بصفة تاجر تجزئة للتهرب من الأعباء الضريبية المرتفعة المرتبطة برقم الأعمال الحقيقي،إن هذه المنظومة القانونية تهدف في جوهرها الإنساني والمهني إلى ترسيخ أخلاقيات المهنة وضمان أن يكون النجاح الاقتصادي ثمرة للتميز والكفاءة لا ثمرة للاعتداء على مجهودات الآخرين أو تضليل الرأي العام.[3]

[1] نواصر الطاهر ،غزالي نصيرة،مرجع السابق،ص1219.

[2] نواصر الطاهر،غزالي نصيرة،مرجع نفسه،ص1220.

[3] نواصر الطاهر،غزالي نصيرة، مرجع نفسه،ص1221.

الفصل الثاني

النظام القانوني للجرائم الإلكترونية الماسة بالمعاملات التجاري

يعد النظام القانوني للجرائم الإلكترونية الماسة بالمعاملات التجارية حجر الزاوية في حماية الثقة الائتمانية والنمو الاقتصادي الرقمي،فمع التحول المتسارع نحو التجارة الإلكترونية برزت أنماط مستحدثة من الإجرام تتجاوز الحدود التقليدية ،وتستهدف بنية المعاملات التجارية في جوهرها ولم تعد القوانين التقليدية قادرة بمفردها على استيعاب خصوصية هذه الجرائم، مما استوجب إيجاد نظام قانوني متكامل يجمع بين القواعد الموضوعية التي تجرم هذه الأفعال والقواعد الإجرائية ،التي تتيح ملاحقتها وتفتيش الأنظمة المعلوماتية المعقدة.

وعليه سيتم في هذا الفصل تسليط الضوء على القواعد والأسس التي يقوم عليها هذا النظام القانوني،وذلك من خلال مبحثين متكاملين المبحث الأول، يتناول الأساس القانوني لتجريم هذه الجرائم في التشريع الجزائري، حيث سنبحث في القواعد الموضوعية والإجرائية التي استحدثها المشرع الجزائري لضبط الجريمة الإلكترونية وتوفير الحماية القانونية اللازمة للتكنولوجيا .

مع التطرق لسلطات التحقيق والتدقيق في هذا المجال،أما المبحث الثانيفينتقل بنا إلى الأساس القانوني لمواجهة هذه الجرائم في الاتفاقيات الدولية والمنظور المقارن،ذلك أن الجريمة الإلكترونية بطبيعتها عابرة للحدود مما يتطلب إطاراً اتفاقياً دولياً وعربياً موحداً وجهوداً قضائية وأمنية مشتركة ،ومن هذا المنطلق سيتم سعي لاستعراض أهم الاتفاقيات الدولية والمبادرات الأممية، ومقارنة التوجه التشريعي الجزائري ببعض التشريعات العربية الرائدة (الإماراتية، الكويتية، الأردنية، المصريةوالسعودية)، لنخلص في النهاية إلى آليات التعاون القضائي والأمني الدولي التي تشكل الدرع الواقي للمجتمع الرقمي.

المبحث الأول :الأساس القانوني لتجريم الجرائم الإلكترونية الماسة بالمعاملات التجارية في التشريع الجزائري

لاتقتصر السياسة الجنائية في مجال الجرائم الإلكترونية عللا تجريم الأفعال ومعاقبة مرتكبيها،وإنما تهدف أساسا إلى حماية المعاملات التجارية الإلكترونية وضمان الثقة في وسائل الدفع والتبادل الرقمي،بما يكفل استقرار النشاط الاقتصادي وحماية مصالح الأعوان الإقتصاديين والمستهلكين.

تعتبر الثقة والأمان الركيزة الأساسية لنمو التجارة الإلكتروني،وبما أن هذا الفضاء الرقمي أصبح عرضة لانتهاكات تهدد استقرار المعاملات المالية وحقوق المستهلكين، كان لزاماً على المشرع الجزائري التدخل لإيجاد غطاء قانوني يحمي هذه البيئة الافتراضية ولم يكتفِ المشرع بالنصوص التقليدية،بل استحدث قواعد موضوعية، تتماشى مع خصوصية الجريمة المعلوماتية لضمان ردع المخالفين وحماية الاقتصاد الوطني.

يهدف هذا المبحث إلى تبيان المظلة القانونية التي تحكم هذا النوع من الجرائم، وذلك من خلال محورين أساسيين يعكسان التوجه التشريعي الجزائري والدولي ،حيث المطلب الأول نخصصه لدراسة الأسس القانونية والقواعد الموضوعية للجريمة الإلكترونية مع التركيز على الحماية المقررة في قانون العقوبات وقانون الإجراءات الجزائية.

بالإضافة إلى القوانين المتصلة بتكنولوجيات الإعلام والاتصال،وحرصا على الحماية المقررة في القانون التجاري وقانون التجارة الإلكترونية 18-05[1] الذي جاء ليوازن بين الاستثمار الرقمي وتطوير المعاملات التجارية 04-02[2] إلى القانون التجاري ،والمطلب الثاني نتناول فيه القواعد الموضوعية الخاصة بالجرائم الإلكترونية مع التمييز بين القواعد الموجهة للشخص الطبيعي وتلك المتعلقة بالشخص المعنوي، نظراً للدور المحوري الذي تلعبه الشركات والمؤسسات في بيئة التجارة الرقمية.

[1] القانون رقم18-05،المؤرخ في 1ماي 2018،يتعلق بالتجارة الإلكترونية،ج-ر،العدد 28،الصادر في 16 ماي 2018.

[2] القانون 04-02،يحدد القواعد المطبقة على الممارسلت التجارية،المرجع السابق.

المطلب الأول:الأسس القانونية والقواعد الموضوعية للجريمة الإلكترونية

إن مواجهة الجرائم الإلكترونية الماسة بالمعاملات التجارية تطلبت من المشرع صياغة منظومة قانونية متكاملة توازن بين القواعد التقليدية والاحتياجات التقنية الحديثة فلا يمكن حماية التجارة الرقمية دون وجود نصوص واضحة تحدد الأفعال المجرمة والعقوبات المقررة لها.

وهو ما يجسد المبدأ القانوني "لا جريمة ولا عقوبة إلا بنص"وللإحاطة بهذه الأسس سنقوم بتفصيل هذا المطلب من خلال فرعين أساسيين،الفرع الأول سنبحث فيه عن الأساس القانوني للجرائم الإلكترونية في التشريع الجزائري، حيث سنسلط الضوء على الحماية الجنائية التي كفلها قانون العقوبات المعدلرقم24-06[1]وقانون الإجراءات الجزائية25_14[2].

بالإضافة إلى القوانين المتخصصة المتعلقة بتكنولوجيات الإعلام والاتصال، والتي تشكل معاً الدرع القانوني للمعاملات التجارية،أما في الفرع الثاني سيتم تخصيصه لدراسة القواعد الموضوعية للجريمة الإلكترونية مع التركيز على تكييف هذه القواعد بما يتناسب مع طبيعة الجرائم التي تستهدف البيانات والأنظمة المعلوماتية التجارية.

الفرع الأول:الأسس القانونية المنظمة للجرائم الإلكترونية في الجزائر

يتمثل التحدي الأكبر في حماية المعاملات التجارية الرقمية في إيجاد نص قانوني صريح يستوعب الأساليب الإجرامية المتطورةوقد سعى المشرع الجزائري إلى مواكبة هذا التحول من خلال دمج نصوص عقابية خاصة ضمن المنظومة القانونية العامة تهدف إلى إضفاء الصبغة الشرعية على ملاحقة المعتدين في الفضاء السيبراني.

سيتم تناول في هذا الفرع مرتكزات هذه الحماية من خلال نقطتين جوهريتين،أولاً الحماية بموجب قانون العقوبات وقانون الإجراءات الجزائيةحيث سيتم إستعراض كيف كيّف المشرع النصوص الجزائية التقليدية لتشمل الجرائم المعلوماتية التي تمس سلامة التجارة،ثانياً الحماية المتصلة بتكنولوجيات الإعلام والاتصال لإستيضاح دور القوانين الخاصة في حماية البيانات التجارية والابتكارات الرقمية من القرصنة والاعتداء.

[1] قانون رقم 24-06،المرجع السابق،ص4.

[2]القانون رقم 25-24 المؤرخ في 15 اوت 2025 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية،العدد ثمانية وخمسون،الصادر في اوت 2025.

أولا:الحماية في قانون العقوبات والإجراءات الجزائية

تعد حماية المعاملات التجارية في الفضاء الرقمي تحدياً قانونياً استدعى من المشرع الجزائري تحديث ترسانته القانونية التقليدية لتستوعب خصوصية الجريمة الإلكترونية[1]،فقبل بروز النصوص المتخصصة كان القضاء يستند إلى القواعد العامة في قانون العقوبات ،لاسيما تلك المتعلقة بالاعتداء على الأموال والأشخاص غير أن الطبيعة التقنية العابرة للحدود والهشاشة ،التي تتسم بها الأدلة الرقمية كشفت عن قصور في تلك النصوص الكلاسيكية،مما استوجب تدخلاً تشريعياً نوعياً يزاوج بين الصرامة العقابية والمرونة الإجرائية.[2]

لقد شكل القانون رقم 04-15 المنعطف الأساسي في هذا المسار،حيث استحدث القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وهو القسم الذي شهد تنقيحاً مستمراً ،كان آخره التعديل الهام والحديث بموجب القانون رقم 24-06 وبناءً على هذه المنظومة العقابية أصبحت الأفعال التي تمس سلامة المعاملات التجارية مجرمة بوضوحمثل الدخول غير المشروع أو البقاء في أنظمة المعطيات المادة 394 مكرر1[3].

وكذا إتلاف أو تعديل البيانات التجارية بطرق غير مشروعة المادة 394 مكرر 1حيت نصت على" يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج ، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها" وصولاً إلى تجريم إنتاج أو نشر البرمجيات المعدة للاعتداء على الأنظمة المادة 394 مكرر2. وقد شدد المشرع العقوبات بشكل لافت ،حينما تتعلق الجريمة بمؤسسات القانون العام أو مصالح الدفاع الوطني مع الإبقاء على إمكانية تطبيق النصوص العامة في حالات النصب أو التزوير الإلكتروني إذا ما استوفت أركانها القانونية[4]،ويبرز تشديد العقوبات خطورة الأضرار الاقتصادية التي قد تلحق بالمؤسسات التجارية والمتعاملين الاقتصاديين نتيجة الإعنداء على الأنظمة المعلوماتية.

---

[1] شريف خالد، " الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في التشريع الجزائري" ،مجلة البيان للدراسات القانونية، جامعة محمد خيضر بسكرة،الجزائر، المجلد 10،العدد واحد،جوان 2025،ص128.

[2]شريف خالد،مرجع نفسه،ص128.

[3]المادة 394 مكرر 1،من الامر 66-156 المعدل والمتمم من قانون 04-15 المؤرخ في 10 نوفمبر2004 والمعدل بموجب قامون 24-06.

[4]شريف خالد،مرجع سابق، ص133.

وفي مقابل هذا الزخم الموضوعي لم يغفل المشرع الجانب الإجرائي إدراكاً منه بأن النص العقابي يظل عديم الأثر دون آليات فعالة للبحث والتحري، ومن ثم شهد قانون الإجراءات الجزائية تحولات عميقة لاسيما بموجب القانون رقم 06-22[1]، الذي أرسى قواعد خاصة للتفتيش المعلوماتي ومراقبة الاتصالات فقد مكنت النصوص الإجرائية السلطات القضائية من تفتيش المنظومات المعلوماتية ودعامات تخزين البيانات المادة 45،بل وسعت نطاق ذلك ليشمل اعتراض المراسلات الإلكترونية وتسجيل الأصوات والتقاط الصور المادة 65 مكرر 5 وما يليها بناءً على أوامر قضائية.

ويهدف هذا التوجه، كما تؤكد الدراسات المتخصصة كدراسات الباحثين "مراد مشوش" و"راضية عيمور" إلى تمكين الضبطية القضائية من وضع اليد على الأدلة الرقمية المتطايرة وضمان عدم إتلافها في معادلة دقيقة تسعى للتوفيق بين الفعالية الأمنية في حماية الاقتصاد الرقمي وبين صون الحقوق والحريات الفردية مع الإحالة الدائمة إلى الجريدة الرسمية باعتبارها المرجع النهائي لتحيين هذه النصوص والتأكد من سريانها في ظل التعديلات المتلاحقة.[2]

إن حماية المستهلك في العصر الرقمي لمتعد مجرد خيار تشريعي بل أضحت ضرورة ملحة فرضتها التحولات العميقة في بنية الاقتصاد العالمي و تنامي ظاهرة العولمة ،فالمستهلك اليوم يجد نفسه الطرف الأضعف في مواجهة ترسانة من الإعلانات الإلكترونية المغرية وسيطرة الشركات الكبرى التي تستثمر أموالاً طائلة في الدعاية المكثفة للتأثير على إرادته ،و من هنا يبرز التفاوت الواضح في العلاقة التعاقدية عبر الإنترنت حيث يفتقد المستهلك القدرة على التفاوض بشأن شروط العقد التي غالباً ماتتضمن مصطلحات تحد بشكل غير عادل من حقوقه[3].

وقد استدرك المشرع الجزائري خطورة هذه السلوكات المنافية لمصالح المستهلك، فعمد إلى تجريم الأفعال الضارة بصحته وسلامته ليس فقط عبر القواعد العامة في قانون العقوبات، بل و من خلا لترسانة قانونية متخصصة و محدثة.

[1] قانون رقم 06-22، مؤرخ في 20 ديسمبر 2006،يعدل ويتمم الأمر رقم 03-03 المؤرخ في 19جويلية 2003 ،المتعلق بالمنافسة،الجريدة الرسمية العدد 84،الصادر بتاريخ 24 ديسمبر 2006.

[2] شريف خالد،مرجع سابق، ص133.

[3] كاملة بوعكة،"حماية المستهلك الإلكتروني جزائيا في ذل التجارة الإلكترونية"،مجلة الدراسات والبحوث القانونية،كلية الحقوق والعلوم السياسية،جامعة المسيلة-الجزائر-،المجلد10،العدد واحد جانفي 2025،ص334.

وتتجلى هذه الحماية في القانون رقم 04-02 المتعلق بالممارسات التجارية و الذي يفرض شفافية كاملة في إعلام المستهلك و نزاهة المعاملات وامتدت هذه الحماية لتشمل الفضاء الرقمي بموجب القانون رقم 18-05 المتعلق بالتجارة الإلكترونية ،الذي وضع أطراً قانونية صارمة لحماية المستهلك الإلكتروني من الغش و الاحتيال، ومنحه حقوقاً جوهرية مثل حق العدول لضمان عدم تضرره من المعلومات المضللة[1].

وعلاوة على ذلك ونظراً لأن عمليات الشراء عبر المواقع تتطلب الإفصاح عن بيانات حساسة، فقد تقررت حماية خاصة للبيانات الشخصية كآلية قانونية لتعزيز الثقة الرقمية وبموازاة ذلك حرص المشرع على مواكبة التطور التقني بمكافحة الجرائم السيبرانية التي قد تمس بسلامة البرامج والمعلومات.

وهو ماتجسد في المصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بموجب المرسوم الرئاسي رقم 14-252[2] و لضمان فعالية هذه الحماية تم تعزيز المنظومة الردعية بموجب الأمر 21-11 المعدل لقانون العقوبات، الذي شدد العقوبات على الجرائم الماسة بالاقتصاد الوطني والوحدة الوطنية و أمن المعلومات تماشياً مع استراتيجية الدولة في حماية الأمن السيبراني و المستهلك من التلاعب و الضرر بمضامين الحاسبات الإلكترونية ،بما يضمن صيانة الحلقة النهائية في العملية الاقتصادية و هي الاستهلاك[3]،كما تهدف السياسة العقابية في مجال الجرائم الإلكترونية إلى حماية الثقة في المعاملات التجارية الإلكترونية وضمان سلامة المبادلات المالية.

ثانيا:الحماية المنظمة للجرائم المتصلة بتكنولوجيا الإعلام والإتصال

تجسيداً لوعي المشرع الجزائري بأن القواعد العامة قد لا توفر الإحاطة الكاملة بجوانب الجريمة المعلوماتية المتشعبةبادر إلى تعزيز المنظومة التشريعية بسن قوانين خاصة ترسم إطاراً أكثر شمولاً وفعالية للمواجهة[4] ويبرز في طليعة هذه النصوص القانون رقم 09-04 المؤرخ في 05 أوت 2009المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، و الذي يُعد كما يصفه الباحث "مراد مشوش"حجر الزاوية والركيزة الأساسية في هذا المجال لقد قدم هذا القانون تعريفاً جامعاً في مادته الثانية، لم يقتصر فيه على المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات فحسبل

[1] كاملة بوعكة،المرجع السابق،ص334.

[2] مرسوم رئاسي رقم 14-252،مؤرخ في 13ذي القعدة عام 1435الموافق 8 سبتمبر سنة 2014،يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،المعتمدة بالقاهرة في 21 ديسمبر سنة 2010،الجريدة الرسمية للجمهورية الجزائرية،العدد54،الصادر في 17 سبتمبر2014،ص4.

[3] كاملة بوعكة،المرجع السابق،ص335.

[4] شريف خالد،مرجع سابق،ص127.

مد نطاقه ليشمل أي جريمة أخرى يُسهل ارتكابها عبر الوسائط الرقمية مما يعكس مرونة تشريعية تستوعب الجرائم التقليدية حينما تتخذ من الفضاء السيبراني مسرحاً لها.

وقد استحدث هذا القانون آليات إجرائية وقائية متطورة تتناسب مع الطبيعة التقنية للأدلة الرقمية، حيث [1]أجازت المادة الخامسة منه إجراء التفتيش والدخول للمنظومات المعلوماتية حتى عن بُعد تحت إشراف قضائي وهو ما اعتبره الباحث عبد الصديق شيخ تحكماً جيداً في أساليب المكافحة الحديثة كما فرض القانون التزامات صارمة على مقدمي الخدمات للتعاون مع السلطات القضائية وحفظ بيانات حركة المرور موازاة مع تأسيس الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كجهاز مؤسساتي متخصص يضطلع بمهام استشارية وتقنية حيوية.

وفي خطوة نوعية لتعزيز التخصص القضائي جاء الأمر رقم 21-11[2] المؤرخ في 25 أوت 2021 ليعدل قانون الإجراءات الجزائية ويستحدث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ،ويهدف هذا القطب حسب ما أشارت إليه الباحثة "أمينة بصافة" إلى تركيز الخبرة القضائية في جهة واحدة متخصصة ،مما يرفع من جودة التحقيقات والمحاكمات في القضايا ذات التعقيد التقني العالي إن هذا التكامل بين النصوص الموضوعية المتخصصة والتنظيم القضائي المستحدث يعكس استراتيجية المشرع الجزائري في بناء جدار حماية قانوني متين، قادر على مواكبة التحولات المتسارعة في عالم تكنولوجيا المعلومات والاتصال وضمان أمن المعاملات الرقمية.

وفي نفس الصدد تتجلى الحماية القانونية للجرائم الإلكترونية الماسة بالمعاملات التجارية في التشريع [3]الجزائري من خلال منظومة متكاملة تجمع بين القواعد العامة والنصوص المتخصصة ،حيث يمثل القانون رقم 24-06 أحدث قفزة تشريعية في قانون العقوبات لتجريم المساس بأنظمة المعالجة الآلية للمعطيات بما في ذلك الدخول غير المشروع أو التلاعب بالبيانات التجارية،وتتكامل هذه الحماية مع القانون رقم 09-04الذي وضع الإطار الوقائي والإجرائيمعززاً بـ الأمر رقم 21-11الذي استحدث القطب الجزائي الوطني لضمان تخصص القضاء في ملاحقة هذه الجرائم المعقدة تقنياً.

---

[1] شريف خالد،مرجع سابق،ص128.

[2] الأمر رقم 21-11 ،مؤرخ في 14 ذي القعدة عام 1442 الموافق 25 يونيو 2021،يعدل ويتمم الأمر رقم 66-156،المتضمن قانون العقوبات، الجريدة الرسمية للجمهوريةالجزائرية،العدد50،الصادر في27يونيو2021.

[3] شريف خالد،مرجع نفسه،ص133.

ثالثا.الحماية المنظمة في قانون التجاري وقانون التجارة الإلكترونية:

تعد حماية المعاملات التجارية ركيزة الاستقرار الاقتصادي،لذا أرسى المشرع الجزائري قواعد تقليدية بموجب القانون التجاري حيث يمثل الأمر 75-59[1] الإطار التشريعي التقليدي الذي يضبط الأنشطة التجارية واستقرار المعاملات ومع التحول الرقمي وتوفير الحماية خاصة للمستهلك تواكب سرعة وطبيعة المعاملات الرقمي حيث أن يُمثل القانون رقم 18-05 المتعلق بالتجارة الإلكترونية في الجزائر ركيزة أساسية لتأمين الفضاء الرقمي و بناء جسور الثقة بين المورد و المستهلك.

إذ ألزم المشرع المورد الإلكتروني بالقيد في السجل التجاري و إنشاء اسم نطاق بالامتداد الوطني و التسجيل في البطاقية الوطنية بهدف إضفاء الشفافية وتسهيل المساءلة القانونية[2].

وفي إطار ضبط هذا النشاط جرم المشرع ممارسته دون قيد معاقباً على النشاط الدائم بغرامة من 10,000[3]إلى 100,000 دج مع غلق المحل حتى تسويةالوضع وعلى النشاط غير الدائم بغرامة من 5,000 إلى 50,000 دج مع إمكانية حجز البضائع ويُعاب على هذا المقتضى التخلي عن عقوبة الحبس في حالة العود والمساواة في الغرامة بين الشخص الطبيعي والمعنوي رغم تاوت ملاءتهما المالية.

كما جرم المشرع استخدام مستخرج سجل منتهي الصلاحية بغرامة تصل إلى 500,000 دج وغلق إداري مع منح مهلة ثلاثة أشهر للتسوية قبل الشطب القضائي،ولحماية مصداقية المحررات الرقمية عوقب على تزوير السجل الإلكتروني بالحبس من ستة أشهر إلى سنة وغرامة تصل إلى مليون دينار مع الغلق الوجوبي وهي عقوبة يراها الفقه مخففة مقارنة بالقواعد العامة للتزوير في قانون العقوبات وامتداداً لمبدأ علانية البيانات فرض المشرع غرامة من 50,000 إلى 500,000 دج على التصريح ببيانات ناقصة أو كاذبة دون النص على الحبس أو الحظر المؤقت من النشاط، وهو نقص تشريعي يؤثر على الردع.

كما عوقب على عدم الإشهار القانوني للبيانات بغرامة تفرق بين الشخص الطبيعي والمعنوي ،في حين عوقب على عدم تعديل البيانات كالمقر أو العنوان خلال ثلاثة أشهر بغرامة تصل إلى 500,000 دج والشطب في حال عدم التسوية.

---

[1] الأمر رقم 75-59 المؤرخ في 20رمضان عام 1395،الموافق 26 سبتمبر سنة 1975،المتضمن القانون التجاري،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد101،الصادر بتاريخ 19 ديسمبر 1975،المعدل والمتمم،ص1118.

[2] بسمة صيشي،المرجع السابق،ص211.

[3] بسمةصيشي،نفس المرجع،ص212.

وأخيراً واجه المشرع الاعتداءات المستحدثة على أسماء النطاق كالقرصنة والانتحال الرقمي بتنظيم حجزها وتشغيلها تحت الامتداد الوطني حمايةً للمستهلك من التضليل وضماناً لنزاهة المنافسة واستقرار الاقتصاد الرقمي[1] يُبرم العقد الإلكتروني عن بُعد دون الحضور المادي لأطرافه بالاعتماد على الوسائط الرقمية ولضمان سلامة الرضا أوجبت المادة 11 من القانون رقم 18-05 المتعلق بالتجارة الإلكترونية أن تسبق المعاملة عرضاً تجارياً يتضمن البيانات الجوهرية للمنتج .

كما أُلزم المورد بالإشهار الرقمي المنضبط وفق شروط محددة كالقيد في السجل التجاري والانتساب للنطاق الوطني وقد فرض المشرع حماية جزائية استباقية بتجريم أي إخلال بهذه الشروط أو توجيه إشهار يتضمن بيانات كاذبة أو مغرضة وهو ما عززته السياسة الجنائية الحديثة بموجب الأمر 21-11 المعدل لقانون العقوبات لحماية المستهلك والاقتصاد الوطني من الممارسات الاحتيالية السيبرانية.

وتبرز الجرائم المتعلقة بالإشهار الإلكتروني كأحد أخطر التحديات التي تواجه سلامة إرادة المستهلك فلئن كان الإشهار أداة تسويقية حيوية[2] إلا أن بعض الموردين استغلوا الخصائص التقنية للبيئة الرقمية والتي تحجب الرؤية المباشرة للسلعة لتوجيه رسائل إعلانية مخادعة تفسد الرضا وتوقع في الغلط وتصدى التشريع الجزائري لهذا النمط السلوكي عبر قمع جريمة التضليل الإشهاري، حيث يُعرّف فقهياً بأنه كل صياغة مبهمة أو زعم من شأنه إيقاع المتلقي في الغلط حول حقيقة المنتج أو سعره دون كذب صريح.

فالإشهار المضلل يمثل منزلةً بين الإعلان الصادق والكاذب تماماً كونه يعتمد على توليد انطباع زائف وقد جُرّم هذا السلوك بموجب المادة 28 من القانون رقم 04-02 المحدد للقواعد المطبقة على الممارسات[3] التجارية المعدل والمتمم والتي حظرت كل إشهار يتضمن تصريحات أو بيانات تضلل بخصوص تعريف المنتج أو مميزاته أو تؤدي للبس مع عون اقتصادي آخر وجاء القانون رقم 18-05 ليؤكد خلو العروض الإلكترونية من العبارات الغامضة والمضللة متماشياً مع الرؤية التشريعية للأمر 21-11 التي وسعت نطاق التتبع الجزائي لمكافحة بث الاضطراب في الأسعار عبر معلومات كاذبة أو مضللة موجهة للجمهور[4].

[1] بسمة صيشي،المرجع السابق،ص212.

[2] بسمة صيشي،المرجع نفسه،ص201.

[3] بسمة صيشي،المرجع نفسه،ص202-203.

[4] بسمة صيشي،المرجع نفسه،ص203.

وتتخذ هذه الجريمة صورتين رئيسيتين:

أولاهما الإشهار الإلكتروني الكاذب وهو سلوك عمدي يقوم على تقديم ادعاءات زائفة ومخالفة للحقيقة كلياً بنية الغش في العناصر الأساسية للمنتج وهو ما حظرته صراحة الأحكام المنظمة لقمع الغش مثل المرسوم التنفيذي رقم 90-39[1] المتعلق بمراقبة الجودة وقمع الغش والذي يمنع استعمال أي إشارة تدون في ذهن المستهلك اللبس حول طبيعة السلعة أو تركيبتها أو تاريخ صلاحيتها.

أما الصورة الثانية فهي الإشهار الإلكتروني المقارن وهو الأسلوب الذي يوازن فيه المعلن بين خصائص سلعته وعلامة تجارية منافسة ورغم تنظيم هذا الأسلوب في بعض التشريعات المقارنة كالقانون الفرنسي الذي يشترط بقاء المقارنة موضوعية ودون تلميح مسيء إلا أنه يتحول إلى فعل مجرّم ومنافسة غير مشروعة في القانون الجزائري إذا انطوى على تشويه لسمعة المورد المنافس أو الحط من قيمة منتجاته لحظر المنافسة الشريفة حمايةً للمستهلك واستقراراً للسوق الرقمي والوطني ككل.

كما تتجلى خطورة الجرائم المعلوماتية في نطاق التجارة الإلكترونية في استهدافها أمن المعاملات واستقرارها حيث تقع الاعتداءات عبر اختراق المواقع التجارية وتدمير بياناتها بالفيروسات أو بانتهاك سرية البيانات الشخصية للمتعاقدين وهي الخصوصية اللازمة لبناء الثقة الرقمي وفيما يتعلق بوسائل الدفع نظّم القانون الجزائري رقم 18-05 البطاقات البنكية كأداة دفع إلكترونية [2]إلا أنها تواجه مخاطر جرمية سواء من الحامل نفسه كاستعمالها بوثائق مزورة أو بعد إلغائها أو عقب انتهاء صلاحيتها القانونية أو من قِبل الغير عن طريق القرصنة والسرقة لاستغلالها دون وجه حق[3].

أما لتأمين وتوثيق هذه المعاملات يبرز التوقيع الإلكتروني كأداة لإثبات الهوية والتعبير عن الرضا وهو ما أطّره المشرع في القانون رقم 15-04 تماشياً مع المعايير الدولية كقانون اليونسيترال النموذجي ولإضفاء الحجية عليه يُشترط تصديقه من جهة محايدة ورغم ذلك يظل عرضة للانتهاك والتقليد مما يستدعي دعم

[1] المرسوم التنفيذي رقم 90-39 ،المتعلق بمراقبة الجودة وقمع الغش،ا،لمؤرخ في 3 رجب عام 1410 الموافق 30 يناير سنة 1990،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد05،الصادر بتاريخ 31 يناير،ص214.

[2] موزالي نور الدين،"الجرائم المعلوماتية في إطار التجارة الإلكترونية وسبل مكافحتها"،مجلة الدراسات القانونية،مخبر السيادة والعولمة،جامعة يحيى فارس بالمدية،الجزائر،المجلد 09،العدد الثاني،جوان 2023،ص182.

[3] موزالي نو الدين،المرجع نفسه،ص183.

الحماية القانونية بآليات تقنية متطورة أبرزها التشفير الذي يحوّل البيانات إلى نصوص مبهمة لمنع أي اختراق معلوماتي.[1]

الفرع الثاني:آليات الحماية الموضوعية للمعاملات التجارية من للجريمة الإلكترونية

تعتبر القواعد الموضوعية حجر الزاوية في تحديد الأركان القانونية للجرائم الإلكترونية وضبط حدود المسؤولية الجزائية المترتبة عنها خاصة في ظل الطبيعة الافتراضية للمعاملات التجاريةوقد حرص المشرع [2]الجزائري على صياغة أطر عقابية متطورة تتناسب مع هوية الجاني ونوع الاعتداء الرقمي، ولتفصيل هذه القواعد سنرتكز على نقطتين التاليين الاولى القواعد الموضوعية للشخص الطبيعي؛ عبر تبيان كيفية مساءلة الأفراد عن الأفعال الإجرامية الإلكترونية وتحديد العقوبات المقررة لكل جرم،والنقطة الثانية القواعد الموضوعية للشخص المعنوي بالنظر إلى الدور المتزايد للشركات في التجارة الإلكترونية، وما يترتب على كياناتها من مسؤولية جنائية خاصة عن الجرائم المرتكبة باسمها أو لحسابها.

أولا:القواعد الموضوعية للشخص الطبيعي

تقوم المسؤولية الجزائية للشخص الطبيعي في مجال الإجرام الإلكتروني على مواءمة النصوص القانونية لاستيعاب الطبيعة الرقمية للأفعال المجرمة حيث يعامل المشرع الجزائري هذه الجرائم بصرامة تماثل الجرائم التقليدية لضمان أمن المعاملات، وتتجسد هذه الحماية الموضوعية في المادة 59 من القانون رقم 18-07، التي أقرت" عقوبة الحبس من سنة إلى ثلاث سنوات وغرامة مالية تصل إلى 300,000 دج لكل من يجمع معطيات ذات طابع شخصي بطرق تدليسية أو غير مشروعة أو غير نزيهة ".

ويتطلب قيام هذه الجريمة توافر ركن مادي يتمثل في سلوك إجرامي يستخدم الاحتيال والخداع للتأثير على إرادة الضحية وركن معنوي يستند إلى القصد الجنائي العام حيث تُصنف كجريمة عمدية تنصرف فيها إرادة الفاعل وعلمه إلى ارتكاب الفعل المجرم والمساس بخصوصية البيانات.[3]

---

[1] موزالي نور الدين،المرجع السابق،ص184 .

[2] شاكر سليمان، " القواعد الإجرائية والموضوعية للجريمة المعلوماتية في التشريع الجزائري"،المجلة الجزئرية للحقوق والعلوم السياسية،جامعة تيسمسيلت، المجلد9،العدد واحد، 2004، ص12.

[3] شاكرسليمان،المرجع نفسه،ص12.

ثانيا: القواعد الموضوعية للشخص المعنوي

أقر المشرع الجزائري مسؤولية جزائية صريحة على الشخص المعنوي عن الجرائم الإلكترونية التي تُرتكب لحسابه بواسطة أجهزته أو ممثليه القانونيين وذلك بموجب المادة 51 مكرر من قانون العقوبات المستحدثة بالقانون 04-15 وتتجسد هذه المسؤولية في نظام عقابي رادع يستند إلى المواد 18 مكرر وما يليها من قانون العقوبات المعدل حيث تُفرض على الشخص المعنوي غرامات مالية تتراوح بين مرة وخمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعيبالإضافة إلى إمكانية تسليط عقوبات تكميلية أخربكما عزز القانون رقم 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي هذا التوجه في مادته 70مؤكداً على إحالة عقوبات الشخص المعنوي إلى القواعد العامة المنصوص عليها في قانون العقوبات وتجدر الإشارة إلى أن مساءلة الشخص المعنوي لا تعفي الشخص الطبيعي كفاعل أصلي أو شريك من المسؤولية الجزائية عن ذات الأفعال وهو ما يفرض على الشركات والمؤسسات الالتزام الصارم بمعايير الأمان الرقمي لحماية بيانات العملاء وتجنب التبعات القانونية الثقيلة.[1]

تُشكل القواعد الموضوعية الركيزة الأساسية والنواة التشريعية الصلبة التي أسسها المشرع الجزائري لحماية[2] بيئة المعاملات الرقمية، حيث ينصب جوهر هذه القواعد على تحديد الأفعال التي تشكل اعتداءً على التجارة الإلكترونية وبيان أركانها القانونية المادية والمعنوية ورسم الحدود الفاصلة بين الممارسات التجارية المشروعة والأنشطة الإجرامية المستحدثة وقد حرص المشرع على صياغة نصوص تجريمية خاصة تستوعب الأنماط الإجرامية الناشئة عن سوء استخدام تكنولوجيا المعلومات مثل التزوير الإلكتروني للمحررات التجارية، والقرصنة والاعتداء على نظم المعالجة الآلية للبيانات الخاصة بالموردين أو المستهلكين وسرقة الهوية الرقمية في المعاملات المالية وتتكامل هذه المنظومة الموضوعية بالاستناد إلى القواعد العامة الواردة في قانون العقوبات الجزائري بالإضافة إلى النصوص الخاصة المقررة في القانون رقم 18-05 المتعلق بالتجارة الإلكترونية والقانون رقم 04-02 المتعلق بالممارسات التجارية والتي تهدف جميعها إلى حماية الثقة الائتمانية والشفافية في السوق الافتراضية وبناءً على مبدأ شرعية الجرائم والعقوبات ترتّب المشرع الجزائري جزاءات جنائية صارمة تتناسب مع خطورة هذه الجرائم وطبيعتها العابرة للحدود حيث تختلف هذه العقوبات بحسب جسامة الفعل وتكييفه القانوني وتتنوع بين العقوبات.

[1] شاكر سليمان،المرجع سابق، ص13.

[2] بسمة صيشي،المرجع سابق،ص200 .

ذات الطابع المالي الغليظ كالغرامات المالية الموجهة للمخالفين أو الشركات التي تخرق قواعد التجارة الرقمية و العقوبات السالبة للحرية كالحبس والمصادرة بالإضافة إلى العقوبات التكميلية كغلق المواقع الإلكترونية وحظر النشاط التجاري الرقمي ويوفر هذا التأصيل الموضوعي إطاراً قانونياً واضحاً يُحدد السلوك الإجرامي ويقرر رادعاً حقيقياً يضمن استقرار المنظومة الاقتصادية والالكترونية الوطنية مما يمنح القضاء سلطة واضحة في تكييف الاعتداءات وتطبيق الجزاءات العادلة لحماية حقوق جميع أطراف الرابطة التجارية الرقمية.[1]

المطلب الثاني: جماية الإجرائية للمعاملات التجارية من الجريمة الإلكترونية

أدى التطور المتسارع للتجارة الإلكترونية إلى تعقيد مواجهة الاعتداءات التي تمس بالممارسات التجارية الرقمية[2] باستخدام القواعد القانونية التقليدية مما فرض الحاجة إلى تحديث المنظومة الإجرائية لضمان فاعلية الدليل الإلكتروني في إثبات الجرائم ومعاقبة مرتكبيها ولتفعيل هذه الرقابة منح المشرع بموجب القانون رقم 04-02 المتعلق بالقواعد المطبقة على الممارسات التجارية صلاحيات واسعة لموظفين مؤهلين للقيام بمهام التحقيق والتفتيش والمعاينة الإدارية والقضائية لحماية مصالح الموردين الإلكترونيين والمستهلكين على حد سواء وفي الجانب الإجرائي القضائي.

تبنى المشرع الجزائري الآليات التقليدية الواردة في قانون الإجراءات الجزائية ،مع إضفاء خصوصية تقنية عليها، لاسيما عبر القانون رقم 09-04 المتضمن قواعد الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بينما اكتفى قانون التجارة الإلكترونية رقم 18-05 بالإحالة إلى القواعد العامة المعمول بها وتتنوع إجراءات المتابعة هنا بين آليات بحث وتحري تقليدية وأخرى مستحدثة .

حيث تشمل الإجراءات التقليدية المعاينة الإلكترونية التي تمتد افتراضياً ومادياً للنظم والبيانات للكشف عن الآثار الرقمية واستعانة الضبطية القضائية بالخبراء المتخصصين لتوثيقها بالإضافة إلى التفتيش ،الذي ينصب على المكونات المادية والمعنوية للحاسوب وفق شروط موضوعية ترتبط بالسبب والمحل وتوافر القرائن الكافية وشروط شكلية صارمة تحمي البيانات الشخصية من المعالجة أو النشر دون أمر قضائي وقد منح المشرع الجزائري مرونة خاصة في تفتيش جرائم المعلوماتية تماشياً مع سرعة اختفاء الدليل الرقمي

[1] بسمة صيشي، المرجع السابق،ص200.

[2] بسمة صيشي،المرجع نفسه،ص223_224.

إذ أجاز إجراءه في أي وقت من النهار أو الليل [1]بناءً على إذن مكتوب ومسبق من وكيل الجمهورية أو قاضي التحقيق المختص، مع اشتراط الحضور الإلزامي لصاحب المسكن أثناء العملية تحت طائلة البطلان واستثناءً من ذلك إذا كان المتهم موقوفاً وهناك صعوبة في نقله أو خشية من ضياع الأدلة ألزم القانون حضور ممثل يعينه صاحب السكن أو شاهدين مسخرين لضمان سلامة الإجراء وضبطه الصحيح .

وتثير عملية ضبط الأدلة الإلكترونية صعوبة بالغة إذا تعلقت بالجانب المعنوي والنظم البرمجية غير المرئية مقارنة بالمكونات الصلبة للحاسوب مما يتطلب برمجيات حديثة وتدريباً فنياً عالياً لأجهزة القضاء والمحققين لضمان شرعية الدليل وحمايته من التلف ولتجاوز هذه العقبات التقنية أقر المشرع الجزائري إجراءات بحث وتحري مستحدثة بموجب قانون الإجراءات الجزائية والقانون 09-04 مثل تسجيل الأصوات والتقاط المحادثات الشفهية والسيبرانية في الأماكن العامة أو الخاصة دون موافقة المعنيين بناءً على ترخيص وإذن قضائي مسبق مما يسهم في تعزيز الحجية القانونية للدليل الرقمي ومواكبة التدابير التشريعية الحديثة لحماية بيئة المعاملات التجارية .

علاوة على ذلك تتمثل القواعد الإجرائية في مكافحة الجريمة الإلكترونية في تلك الآليات التقنية والقانونية التي استحدثها[2] المشرع الجزائري لضمان كفاءة التحقيق والبحث والتحري وقد تجسد ذلك في تعديلات قانون الإجراءات الجزائية لا سيما القانون رقم 06-22، الذي منح سلطات واسعة لوكيل الجمهورية وقاضي التحقيق للإشراف على معاينة وتفتيش أنظمة المعالجة الآلية للمعطيات كما أتاح هذا الإطار القانوني لضباط الشرطة القضائية بناءً على ترخيص قضائي مراقبة المشتبه فيهم واختراق حساباتهم الإلكترونية لضبط الأدلة الرقمية وتحليلها من قبل جهات مختصة.

بما يضمن تحديد المسؤولية الجزائية بدقة تتماشى مع التطورات التشريعية الحديثة ومن أجل الإحاطة بهذه الإجراءات سنفصل في آليات التفتيش التكنولوجي للحواسيب وسلطات تنفيذه وصولاً إلى إجراءات

[1] بسمة صيشي،المرجع السابق،ص225.

[2] شاكر سليمان، مرجع سابق، ص13.

التوثيق التقني لضمان سلامة الأدلة وللإحاطة بهذه الآليات سنقوم بدراسة القواعد الإجرائية من جانبين الاول التفتيش التكنولوجي للحواسيب والجانب الثاني توقيف النظر.[1]

الفرع الأول:التفتيش التكنولوجي للحواسيب

يُمثل التفتيش التكنولوجي للحواسيب عملية فنية وقانونية دقيقة تهدف إلى فحص الأنظمة والشبكات لكشف الثغرات والجائم الإلكترونية الماسة بسلامة البيانات والمعاملات وتتجلى خصوصية هذا الإجراء في كونه يتجاوز مفهوم التفتيش التقليدي للمساكن، فبينما ظل مضمون المادة 44 [2]من قانون الإجراءات الجزائية ثابتاً بوجوب الحصول على إذن مكتوب قبل دخول المسكن استحدث المشرع إطاراً خاصاً للتفتيش الإلكتروني بموجب القانون رقم 09-04وتستمد هذه العملية مشروعيتها من المواد 03 و04 و05 من القانون المذكور لاسيما عند وجود تهديد للنظام العام أو مقتضيات التحري، حيث أجاز المشرع لجهات التحقيق النيابة، قاضي التحقيق، وضباط الشرطة القضائية إجراء التفتيش حتى عن بُعد بناءً على ترخيص قضائي مع التمييز بين المنظومات المحلية وتلك المرتبطة بأنظمة خارج الإقليم الوطني التي تخضع للاتفاقيات الدولية.

وفيما يخص الجانب التنفيذي وبالرغم من أن القاعدة العامة في قانون الإجراءات الجزائية تحصر التفتيش في الفترة ما بين الخامسة صباحاً والثامنة مساءً صوناً للحرمات الدستورية، إلا أن طبيعة الجريمة المعلوماتية وما تتسم به من سهولة إتلاف الأدلة الرقمية جعلت المشرع يقر استثناءات تسمح بالتفتيش في أي ساعة نهاراً أو ليلاً لضمان عدم ضياع الدليل الرقمي وتكتسي سرعة جمع الدليل الرقمي أهمية خاصة في المجال التجاري إلى إمكانية ضياع البيانات المتعلقة بالتحويلات المالية والعقود الإلكترونية والمعاملات البنكية.

ويتطلب نجاح هذا الإجراء الاستعانة بخبراء يمتلكون المعرفة التقنية اللازمة للتعامل مع البيانات المخزنة وتحليلها بشكل صحيح، مع الالتزام التام بالضمانات القانونية التي تحمي حقوق الأفراد وتضمن سلامة الإجراءات من البطلان في ظل التعديلات التشريعية المستمرة[3].

---

[1] شاكر سليمان، مرجع سابق، ص13.

[2]المادة 44 من الأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية،المرجع السابق،ص504.

[3]شاكر سليمان،مرجع سابق، ص13.

الفرع الثاني:التوقيف النظر

يُعد إجراء التوقيف للنظر في سياق الجرائم الإلكترونية أحد أبرز التدابير الاحترازية التي تهدف إلى وضع الشخص المشتبه فيه تحت تصرف التحقيق لفترة زمنية محددة وذلك لضرورة جمع الأدلة الرقمية ومنع إتلافها أو التأثير على سير المعاينة الإلكترونية[1]، ورغم أن هذا الإجراء يستمد مشروعيته الدستورية من المادتين 47 و48 من دستور 1996، إلا أنه شهد تكريساً إجرائياً دقيقاً بموجب تعديلات قانون الإجراءات الجزائية، لا سيما القانون رقم 15-02 [2]المؤرخ في 23 جويلية 2015 الذي سمح لضباط الشرطة القضائية بالاحتفاظ بالأشخاص الذين تتوفر ضدهم دلائل قوية ومتوافقة من شأنها تدعيم الاتهام.

وتتحدد المدة الأصلية للتوقيف للنظر في الجرائم العادية بثماني وأربعين (48) ساعة غير أن طبيعة الجريمة المعلوماتية وخطورتها قد تستدعي تمديد هذه الفترة وفقاً للضوابط المنصوص عليها في المادة 51 من قانون الإجراءات الجزائية"يمكن وكيل الجمهورية تلقائيا أو بناء على طلب مسبب من ضابط الشرطة القضائية، خلال التحريات الأولية، أن يطلب من رئيس المحكمة.....ترسل لها نسخة منه"، شريطة الحصول على إذن كتابي مسبق من وكيل الجمهورية المختص إقليمياً ،الذي يمارس رقابة مباشرة على قانونية وصحة هذا الإجراء وفي ظل الخصوصية التقنية التي تتميز بها الاعتداءات الإلكترونية الماسة بالمعاملات التجارية.

يبرز دور وكيل الجمهورية في ضمان التوازن بين مقتضيات التحري في الفضاء الرقمي وبين حماية الحقوق والحريات الأساسية للموقوفين مع مراعاة أن إجراءات التوقيف والتمديد في هذا النوع من الجرائم تظل محكومة بقواعد صارمة تمنع التعسف وتضمن توثيق كافة مراحل الاحتجاز في محاضر رسمية تماشياً مع أحدث التعديلات التشريعية.[3]

---

[1] شاكر سليمان،مرجع السابق،ص13.

[2]القانون 15-02 المؤرخ في 11 ربيع الثاني 1436 الموافق ل 1فبراير 2015، المتعلق بتحصيل متبادل للمعلومات والوثائق بين الإدارات، الجريدة الرسمية للجمهورية الجزائرية،العدد السادس،الصادر بتاريخ 4 فبراير 2015، ص04.

[3] شاكر سليمان، مرجع سابق، ص13.

المبحث الثاني:الأساس القانوني لتجريم الجرائم الإلكترونية الماسة بالمعاملات التجارية في الإتفاقيات الدولية

نظراً للطبيعة العابرة للحدود التي تتسم بها الجرائم الإلكترونيةأدرك المجتمع الدولي أن المجهودات التشريعية الوطنية تظل قاصرة عن الإحاطة بكافة جوانب هذا الإجرام المتطور ما لم تستند إلى تعاون دولي وثيق وإطار قانوني موحد، فالمعاملات التجارية الرقمية لا تعترف بالحدود الجغرافية مما جعل من الضروري إيجاد توافق دولي وعربي يضمن ملاحقة الجناة وتوحيد المفاهيم القانونية،وللإحاطة بهذا الجانب، سنقوم بدراسة هذا عبر المطلبين التاليين ،المطلب الأول الإطار الاتفاقي الدولي والعربي في مواجهة الجريمة الإلكترونية.

سنتناول فيه المبادرات والاتفاقيات الدولية الكبرى مع تسليط الضوء على الجهود العربية المتمثلة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،أما المطلب الثاني سنتناول فيه أساليب التعاون الدولي في الفضاء الإلكتروني سنبحث فيه الآليات العملية والوسائل التقنية التي تعتمدها الدول لتبادل المعلومات والملاحقة القضائية، بما في ذلك المساعدة القانونية المتبادلة ودور المنظمات الدولية في تأمين الفضاء الرقمي وحماية المعاملات التجارية من الاعتداءات العابرة للحدود.

المطلب الأول:الإطار الإتفاقي الدولي والعربي لمكافحة الجريمة الإلكترونية

يستهدف هذا المطلب تبيان الأسس القانونية التي يستند إليها المجتمع الدولي في مجابهة الإجرام الإلكتروني العابر للحدود، وذلك لضمان بيئة رقمية آمنة للمعاملات التجارية، وسنتناول فيه نقطتين التاليين باختصار،الفرع الأول سنتناول الإطار الاتفاقي الدولي والعربي

ونستعرض فيه الجهود العالمية ك اتفاقية بودابست ودور منظمة الأمم المتحدة، بالإضافة إلى الاتفاقية العربيةلتنسيق الملاحقة القضائية اما بالنسبة للفرع الثاني سنشير لدور التشريعات المقارنة؛حيث نسلط الضوء على تجارب قانونية رائدة كالتشريع الإماراتي، الكويتي، الأردني، المصري، والسعودي.

الفرع الأول:الإتفاقيات والمعاهدات الدولية في مواجهة الجريمة الإلكترونية

تتمثل المواجهة القانونية للجريمة الإلكترونية في هذا الفرع عبر رصد وتحليل الإطار الاتفاقي والمبادرات الدولية، حيث استوجب الطابع العابر للحدود لهذه الجرائم إيجاد صيغ قانونية عالمية موحدة ويهدف هذا القسم إلى استعراض المجهودات الدولية التي صاغت معالم المواجهة الرقمية، وذلك من خلال النقاط التالية:[1]

[1] د. سعيداني سلامي، " تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية (وقائع ومقاربات)"،مجلة الأستاذ الباحث للدراسات القانونية والسياسية،جامعة محمد بوضياف،المسيلة،العدد العاشر، جوان 2018، ص199.

أولا:الجهود والإتفاقيات الدولية في مواجهة الجريمة الدولية وتتمثل في:

أ_إتفاقية بودابست:تُعتبر اتفاقية بودابست، التي أُبرمت في العاصمة المجرية أواخر عام 2001، حجر الزاوية وأول وثيقة دولية ملزمة تهدف إلى صياغة سياسة جنائية مشتركة لمواجهة جرائم الإنترنت وقد جاءت هذه المعاهدة كضرورة حتمية بعد أن انتقل الإجرام المعلوماتي من مجرد محاولات تسلل فردية بريئة يقوم بها الهواة إلى مرحلة الاحتراف الإجرامي المتخصص الذي يستهدف ممتلكات وحياة الأشخاص عبر عمليات الاحتيال والاختلاس الرقمي.[1]

و يمثل التوقيع على هذه الاتفاقية من قبل القوى الكبرى كأوروبا وأمريكا واليابان وكندا ثمرة مفاوضات تقنية وقانونية استمرت لأكثر من أربعة أعوام لضمان إيجاد صيغة توافقية تسمح بتوسيع دائرة التضامن الدولي وتوحيد الجهود التشريعية لمكافحة الاستخدام السيئ للشبكة المعلوماتية وتتجلى أهمية هذه المعاهدة في قدرتها على التطور المستمر، حيث تُعد اليوم المرجع الأساسي للتشريعات الوطنية الحديثة بما فيها التعديلات التي تتبناها الدول لتعزيز التعاون القضائي وتسهيل ضبط الأدلة الرقمية العابرة للحدود تماشياً مع الالتزامات الدولية المستجدة.[2]

ب_معاهدة تريبس:تعد اتفاقية الجوانب المتصلة بحقوق الملكية الفكرية من التجارة المعروفة بـ "معاهدة تريبس" والمبرمة عام 1994 تحت مظلة منظمة التجارة العالمية الجات سابقاً، إطاراً قانونياً دولياً حازماً للتصدي لعمليات السطو الإلكتروني التي تستهدف النتاج الفكري والمادي للمبدعين وتتجلى أهمية هذه المعاهدة في قدرتها على الموازنة بين المعايير الدولية والتشريعات المحلية.[3]

حيث تلزم الدول الأعضاء بتبني تدابير إجرائية وموضوعية فعالة لمواجهة الاعتداءات الرقمية وضمان الحقوق المعنوية والمادية ومن أبرز الأدوات الردعية التي أقرتها المعاهدة منح السلطات القضائية والأمنية صلاحية إصدار أوامر بالقيام بحملات ضبط وتفتيش فجائية وهو إجراء حيوي نظراً لسهولة إتلاف الأدلة الرقمية مع إتاحة التحفظ على الوسائل المستخدمة في الإجرام وفرض عقوبات جنائية رادعة ويساهم هذا

[1] د.سعيداني ،سلامي،المرجع السابق،ص199.

[2] د. سعيداني سلامي،المرجع انفسه،ص200.

[3] د. سعيذاني سلامي،المرجع نفسه،ص201.

المسعى في خلق بيئة تجارية دولية آمنة تمنع الاستغلال غير المشروع للأعمال الفنية والتقنية في الفضاء السيبراني.

ج_معاهدة برن:تعد اتفاقية الجوانب المتصلة بحقوق الملكية الفكرية من التجارة المعروفة بـ "معاهدة تريبس" [1]والمبرمة عام 1994 تحت مظلة منظمة التجارة العالمية الجات سابقاً إطاراً قانونياً دولياً حازما للتصدي لعمليات السطو الإلكتروني التي تستهدف النتاج الفكري والمادي للمبدعين وتتجلى أهميةهذه المعاهدة في قدرتها على الموازنة بين المعايير الدولية والتشريعات المحلية.

حيث تلزم الدول الأعضاء بتبني تدابير إجرائية وموضوعية فعالة لمواجهة الاعتداءات الرقمية وضمان الحقوق المعنوية والمادية ،ومن أبرز الأدوات الردعية التي أقرتها المعاهدة منح السلطات القضائية والأمنية صلاحية إصدار أوامر بالقيام بحملات ضبط وتفتيش فجائية، وهو إجراء حيوي نظراً لسهولة إتلاف الأدلة الرقميةمع إتاحة التحفظ على الوسائل المستخدمة في الإجرام وفرض عقوبات جنائية رادعة ،ويساهم هذا المسعى في خلق بيئة تجارية دولية آمنة تمنع الاستغلال غير المشروع للأعمال الفنية والتقنية في الفضاء السيبراني.

ثانيا:الإتفاقيات والمنظومات

سعت النظم القانونية العربية ومنظمة الأمم المتحدة جاهدة للحاق بركب التحول الرقمي العالمي حيث بادرت دول كالمملكة العربية السعودية، مصر، الإمارات، الأردن، تونس، منذ مطلع التسعينات إلى سن تشريعات تتقاطع [2]مع العصر الجديد الذي أصبحت فيه المعرفة والمعلومات المحدد الاستراتيجي لرأس المال إلا أن هذا التقاطع واجه تحديات قانونية جمّة فرضتها تقنية المعلومات مما استوجب ظهور موجات تشريعية مست عدة حقول بدءاً من حماية الخصوصية والبيانات الشخصية مروراً بجرائم الكمبيوتر والملكية الفكرية للمصنفات الرقمية وصولاً إلى القواعد الإجرائية الجزائية المتخصصة وتشريعات التجارة الإلكترونية والمعاملات التجارية والتواقيع الرقمية التي تعد ركيزة الحكومة الإلكترونية.

وبالرغم من تبني مبادرات تقنية رائدة مثل مدينة دبي للإنترنت في الإمارات والقرى الذكية في مصر إلا أن التجربة العربية في التعامل مع المتطلبات التشريعية لتقنية المعلومات لا تزال تعاني من حالة عدم وضوح

[1]–آمنة قريش، "مظاهر التعاون الدولي لمكافحة الجرائم المعلوماتية: الآليات والتحديات"، دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة خميس مليانة، المجلد 18، العدد 01، جانفي 2026،ص127.

[2] د. سعيداني سلامي،المرجع سابق،ص203.

الرؤية والاعتماد على حلول تشريعية جزئية أو مقتبسة دون مواءمة حقيقية مع البيئة المحلية إن الاكتفاء بمعالجات مبتسرة لبعض المسائل كالتواقيع الرقمية أو حجية المعاملات لا يعد حلاً كافياً للفضاء التشريعي الرحب الذي يتطلبه أمن المعلومات وحماية المستهلك والخصوصية ،فالواقع الرقمي يفرض حاجة ملحة لتدخل تشريعي شمولي يدرك التطور التاريخي لهذه التحديات ويستشرف آفاقها المستقبلية بدلاً من الركون إلى تقديرات خارجية قد تكون هي ذاتها محل تجربة وذلك لضمان فعالية النظم القانونية في حماية المجتمع وتذليل العوائق أمام خطط التنمية الرقمية الشاملة.[1]

الفرع الثاني:دور التشريعات المقارنة في مواجهة الجريمة الإلكترونية

وتثمثل في:

أولا:التشريع الإماراتي

تُعد دولة الإمارات العربية المتحدة رائدةً في البيئة التشريعية الرقمية على المستوى العربي؛ إذ كانت السبّاقة [2]في إفراد تشريع مستقل ومستدام لمواجهة المخاطر السيبرانية وحماية المعاملات الإلكترونية من القرصنة والتهديدات الخارجية وقد تجسد هذا الفكر القانوني الاستباقي في إصدار القانون الاتحادي رقم2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات والذي شكّل طفرة تشريعية تضمنت 28 مادة قانونية عُنِيت بتجريم الأنماط المستحدثة من السلوكيات المعلوماتية غير المشروعة وتحديد العقوبات الرادعة لها.

وفي سياق متصل واكبت الدولة التطور التكنولوجي السريع بتعزيز منظومتها الرقابية والوقائية عبر تطبيق نظام الرقيب (Proxy) لإحكام الحماية والرقابة الأمنية على شبكة الإنترنت وحجب المحتويات الضارة وامتداداً لهذه الرؤية الحمائية وتطويراً للنصوص التشريعية بما يتلاءم مع تسارع الجريمة الإلكترونية أصدر المشرع الإماراتي القانون الاتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات والذي خضع لاحقاً للتعديل بموجب المرسوم بقانون اتحادي رقم 12لسنة 2016 ليرسخ بذلك بيئة رقمية آمنة ومستقرة تدعم وثوقية المعاملات الإلكترونية وفق أعلى المعايير القانونية حيث بذل المشرع الإماراتي جهوداً حثيثة

[1] د. سعيذاني سلامي،المرجع السابق،ص204.

[2]نور الدين موزالي،المرجع السابق،ص193.

لتعزيز الحماية القانونية لقطاع الاتصالات وسرية المراسلات، حيث [1]كانت البداية بصدور قانون مؤسسة الإمارات للاتصالات رقم 1 لسنة 1991 الذي اتسم بالمرونة في ملاحقة المعتدين على تقنية المعلومات ومع تطور الجرائم وتزايد التحديات صدر المرسوم بقانون اتحادي رقم 3 لسنة 2003 بشأن تنظيم قطاع الاتصالات.

والذي جرم في مادتيه71 و72 أفعال الإساءة أو الإزعاج عبر أجهزة الاتصال وتوزيع الرسائل المؤذية للمشاعر واستجابة للمستجدات الرقمية انتقل المشرع إلى مرحلة التخصيص بإصدار القانون الاتحادي رقم 2 لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات بمواده الست وعشرين قبل أن يحل محله القانون الشامل رقم 5 لسنة 2012 وقد استحدث هذا القانون الأخير إطاراً تعريفياً دقيقاً لثمانية عشر مصطلحاً تقنياً مثل الموقع الإلكتروني والبيانات الحكومية لضمان وضوح النص العقابي كما أرسى منظومة جزائية رادعة تجمع بين الغرامات المالية الضخمة التي قد تصل إلى ثلاثة ملايين درهم، والعقوبات الجسدية التي تتنوع بين الحبس والسجن المؤقت، وتشتد لتصل إلى عشر سنوات في حالات التهديد بارتكاب جناية أو المساس بالشرف تأكيداً على التزام المشرع بحماية المنظومة الأخلاقية والأمنية في البيئة الافتراضية.[2]

ثانيا:التشريع الكويتي

وفي السياق التشريعي الخليجي حرص المشرع الكويتي على توفير الحماية القانونية اللازمة للمعاملات [3]الإلكترونية وضمان سلامة الفضاء الرقمي من خلال إرساء منظومة تشريعية رادعة،حيث توجت هذه الجهود بصدور القانون رقم 30 لسنة 2010 بشأن جرائم أنظمة المعلومات والذي تصدى لعدة سلوكيات مجرمة تعيق تدفق المعاملات الإلكترونية وتخترق خصوصيتها ،وقد شملت هذه التجريمات الدخول العمدي وغير المصرح به إلى المواقع الإلكترونية أو أنظمة المعلومات أو تجاوز حدود التصريح الممنوح ،بالإضافة إلى حظر إدخال أو نشر البرمجيات الخبيثة عبر الشبكة المعلوماتية بقصد التلاعب بالبيانات

أو تعديلها أو حذفها أو الاطلاع عليها دون وجه حق فضلاً عن تجريم عمليات تخريب المواقع الإلكترونية أو إلغائها وتعديل محتوياتها وتعزيزاً لهذه المنظومة التشريعية ومواكبةً للمستجدات التقنية المتسارعة أصدرت

[1]ط.د هاني مطر منصور أبو سعود، د.عباسة طاهر،"الأنظمة القانونية العربي وتحدي التعاون في مواجهة الجرائم المعلوماتية"،مجلة الاجتهاد القضائي،مخبر أثر الاجتهاد القضائي على حركة التشريع،جامعة محمد خيضر،المجلد،العدد الثاني،أكتوبر 2021،ص1347.

[2]ط.د هاني مطر منصور أبو سعود، د.عباسة طاهر، المرجع نفسه،ص1347.

[3]نور الدين موزالي،المرجع السابق،ص193.

دولة الكويت لاحقاً القانون رقم 63 لسنة 2015 بشأن [1]مكافحة جرائم تقنية المعلومات، والذي جاء ليتوج مساراً قانونياً بدأ بقانون المعاملات الإلكترونية وقانون إنشاء هيئة تنظيم الاتصالات وتقنية المعلومات لعام 2014 ويعد هذا القانون النص المتخصص الأول الذي عالج الجريمة المعلوماتية ببعديها الموضوعي والإجرائي من خلال 21 مادة قانونية[2].

حيث استهل المشرع الكويتي نصه بضبط المفاهيم التقنية وتحديد ستة عشر مصطلحاً أساسياً لضمان دقة التكييف القانوني، شملت مفاهيم الشبكة المعلوماتية والنظم المؤتمتة والمعالجة الإلكترونية للبيانات وفي شق العقوبات أرسى القانون منظومة جزائية متكاملة توازن بين الردع المالي والبدني حيث قرر غرامات مالية تتراوح بين 500 و50 ألف دينار كويتي وعقوبات سالبة للحرية تتدرج من الحبس لمدة ستة أشهر وتصل في جسامتها إلى عشر سنواتبما يكفل حماية الأفراد والمؤسسات من التعديات والسلوكيات غير المشروعة في البيئة الرقمية.

ثالثا:التشريع الأردني

أرسى المشرع الأردني دعائم المواجهة القانونية للإجرام الرقمي بصدور قانون جرائم أنظمة المعلومات المؤقت[3] رقم 30 لسنة 2010 والذي تضمن سبع عشرة مادة استهلت بضبط المفاهيم التقنية كالموقع الإلكتروني ونظام المعلومات لضمان دقة التكييف القانوني وقد حدد القانون صوراً شتى للسلوكيات المجرمة منها الدخول غير المشروع للمواقع وإفشاء البيانات أو حجبها والاعتداء على خصوصية المراسلات فضلاً عن استغلال الشبكة في أغراض مخلة بالآداب مقرراً منظومة عقابية تجمع بين الغرامات المالية والعقوبات السالبه للحرية كالحبس والأعمال الشاقة مع النص على تشديد الجزاء في حالات العود.

وبالنظر إلى التجربة العربية في عمومها، يلحظ اتجاه المشرعين نحو الاكتفاء أحياناً بتعديل القوانين العقابية التقليدية، فالمشرع العماني قبل إصداره قانوناً مستقلاً استحدث فصلاً خاصاً بجرائم الحاسب الآلي ضمن قانون الجزاء بموجب مرسوم سلطاني عام 2001 ليكون من أوائل المبادرات العربية في هذا الصدد، كما سلكت دول أخرى كالبحرين ومصر مسلكاً يقوم على تطبيق قانون العقوبات العام أو قوانين الصحافة

[1] ط.د هاني مطر منصور أبو سعود،المرجع السابق،ص 1348.

[2] ط.د هاني مطر منصور أبو سعود،المرجع نفسه،ص 1348.

[3] ط.د هاني مطر منصور أبو سعود،المرجع نفسه،ص 1348.

والنشر على الجرائم المعلوماتية بالقياس متى وجد تشابه بين الجرم التقليدي والمستحدث، وذلك كحل تشريعي لمواكبة التطورات التقنية السريعة وضمان عدم إفلات الجناة من العقاب في ظل غياب النصوص المتخصصة آنذاك.

رابعا:التشريع المصري

تعتبر التجربة المصرية في مكافحة الجريمة المعلوماتية نموذجاً يجمع بين الرقابة المؤسسية والمبادرات المدنية،[1]حيث أسست وزارة الداخلية إدارة متخصصة لمكافحة جرائم الحاسب الآلي تتبع تقنياً مرتكبي الجرائم التي تستهدف الأموال أو الملكية الفكرية أو أمن الدولة.

وتعتمد هذه الجهود على تفعيل القوانين القائمة كقانون العقوبات وقوانين الاتصالات والتوقيع الإلكتروني مع السعي المستمر لاستكمال المنظومة بمرونة تشريعية تشمل حماية البيانات الشخصية وتأمين الفضاء السيبراني كما تلعب مؤسسات المجتمع المدني دوراً محورياً في تأهيل الكوادر القانونية والقضائية للتعامل مع تحديات الدليل الرقمي والتعاقدات الإلكترونية بما يضمن مواكبة الدولة للتحولات الرقمية العالمية وحماية مواطنيها من مخاطر الإجرام المنظم عبر الإنترنت.

خامسا:التشريع السعودي

تتبنى المملكة العربية السعودية استراتيجية شاملة لمواجهة الجرائم المعلوماتية، بدأت بإصدار نظام مكافحة جرائم المعلوماتيةبموجب المرسوم الملكي رقم م/17 لعام 1428هـ وهو نص قانوني رائد يهدف إلى[2] تحقيق الأمن المعلوماتي وحماية المصلحة العامة والاقتصاد الوطني ،من خلال تجريم الأفعال الرقمية غير المشروعة ووضع عقوبات رادعة تشمل السجن والغرامات المالية وقد عززت المملكة هذا الإطار التشريعي بالانضمام والمصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 ،مما أتاح لها تعاوناً قضائياً وأمنياً واسعاً مع الدول العربية في مجالات تبادل المعلومات وملاحقة المجرمين وتسليمهم وعلى الصعيد المؤسسي تتكامل جهود وزارات الاتصالات والداخلية والعدل في رسم السياسات وتتبع

[1] شيماء بقدار، آليات مكافحة الجريمة الإلكترونية على المستويين الدولي والوطني، مذكرة نهاية الدراسة، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2022-2023،ص57.

[2] شيماء بقدار،المرجع نفسه،ص57.

الجناة وإرساء العدالة ويتوج هذا الدور بوجود الهيئة الوطنية للأمن السيبراني كمرجع وطني مختص بحماية البنى التحتية الحساسة والمصالح الحيوية للدولة في الفضاء السيبراني.[1]

سادسا:منظمة الأمم المتحدة: تضطلع منظمة الأمم المتحدة بدور ريادي في مكافحة الجريمة المعلوماتية وحماية فضاء المعاملات الرقمية؛ وتجلى ذلك في إقرار اتفاقية مكافحة الجريمة المنظمة عبر الوطنية لعام 2000، وتفعيل دور وكالاتها المتخصصة كمنظمة الملكية الفكرية (WIPO) واليونسكو التي رعت[2]الاتفاقية العالمية لحق المؤلف،وفي الشق التجاري صاغت لجنة القانون التجاري الدولي (الأونسيترال) القانون النموذجي للتجارة الإلكترونية لعام 1996 والقانون النموذجي للتوقيع الإلكتروني بهدف توفير مرجعية تشريعية للدول لتأمين التعاقد الرقمي والحد من الجرائم المعلوماتية التي تهدد مصالح أطراف العملية التجارية من بائع ومستهلك ومورد .

وقد حظيت هذه المبادئ الاسترشادية بقبول دولي واسع، حيث استندت إليها دول عدة في صياغة قوانينها الوطنية (مثل كولومبيا وكوريا الجنوبية وسنغافورة)، واقتبستها تشريعات إقليمية وفيدرالية كبرى كالقانون الكندي الموحد لعام 1999، وقانون المعاملات الإلكترونية الموحد (UETA) الأمريكي، والتوجيه الأوروبي للتجارة الإلكترونية.

المطلب الثاني:أساليب التعاون الدولي في محاربة الجرائم الإلكترونية

مع تحولا لمعاملات التجارية إلى الفضاء الرقمي أصبحت الجريمة الإلكترونية تهديداً عابراً للحدود لاتكفي القوانين المحلية وحدها لمواجهته ،إذ يمكن التخطيط للهجوم في دولة وتنفيذه في أخرى ضد مؤسسات اقتصادية ومالية من هنا غدا التعاون الدولي ركيزة أساسية لحماية الاقتصاد الرقمي وضمان بيئة استثمارية آمنة وموثوقة فلا يمكن تحصين المعاملات الإلكترونية وحماية بيانات المستهلكين إلا عبر آليات مشتركة تشمل تبادل المعلومات الأمنية وتوحيد الجهود القضائية وإبرام الاتفاقيات الدولية لتتبع القراصنة .

وبناءً على ذلك ،يستعرض هذا المحور أبرز أساليب التعاون الدولي في محاربة الجريمة الإلكترونية ودورها في تأمين المعاملات التجارية حول العالم حيث تفرض الجرائم الإلكترونية بطبيعتها العابرة للحدود ضرورة تكاتف الجهود الدولية لتجاوز عقبات السيادة الإقليمية وسد ثغرات الملاحقة الجنائيةلذايرتكز هذا

[1] شيماء بقدار،المرجع السابق،ص57.

[2] نور الدين موزالي،المرجع السابق،ص190_191.

المطلب على دراسة أساليب المواجهة من خلال مسارين متكاملين ،وتبرز أهمية التعاون الدولي خاصة في الجرائم التي تستهدف المعاملات التجارية العابرة للحدود،كاختراق المنصات التجارية الدولية أو الاحتيال في التحويلات المالية الالكترونية،حيث يتناول الفرع الأول آليات التعاون القضائي لضمان فاعلية المحاكمة وجمع الأدلة بينما يستعرض الفرع الثاني أدوات التعاون الأمني الدولي بوصفه الركيزة العملياتية والتقنية اللازمة للتصدي الفوري والمباشر لهذه الجرائم.

الفرع الأول:التعاون القضائي الدولي في مواجهة الجريمة الإلكترونية

يمثل التعاون القضائي الدولي الضمانة القانونية الأساسية لحماية المعاملات التجارية الإلكترونية من الجرائم السيبرانية العابرة للحدود فنظراً لطبيعة الإنترنت المتجاوزة للمجالات الجغرافية تبرز أهمية هذا التعاون عبر آليات تسليما لمجرمين وتبادلا لإنابات القضائية، ومشاركة الأدلة الرقمية و تساهم هذه الجهود المشتركة بشكل مباشر في ردع القراصنة، وبناء الثقة في الاقتصاد الرقمي وضمانا ستقرار بيئة الأعمال الدولية[1].

كما تعتبر الجريمة الإلكترونية اليوم واحدة من أعقد التحديات[2] القانونية التي تواجه المجتمع الدولي، فبسبب طبيعتها العابرة للحدود التي تتجاوز النطاق الجغرافي التقليدي تضع الدول أمام مأزق عملي ،يتمثل في اصطدام قوانينها الوطنية بمبدأ سيادة الدول الأخرى،ومن هنا يبرز التعاون القضائي الدولي أو المساعدة القضائية المتبادلةكحجر زاوية وآلية محورية لا غنى عنها لردم الفجوة بين حق الدولة في العقاب وتقييد سلطاتها بحدود إقليمها إذ يضمن هذا التنسيق ألا يتحول الفضاء السيبراني إلى ملاذ آمن يفلت فيه المجرمون من يد العدالة.

ويستند هذا التعاون إلى ضرورة التوفيق بين استقلال الدولة [3]وممارستها لاختصاصها الجنائي. وبين الفعالية المطلوبة لملاحقة إجرام تقني يتسم بالسرعة والسيولة متخذاً عدة صور قانونية تتكامل فيما بينها بروح من المرونة والدقةحيث تبدأ هذه المنظومة بـ تبادل المعلومات والبيانات وهي الخطوة الأكثر حيوية في مواجهة الجرائم الرقمية، حيث لا يقتصر الأمر على تقديم الوثائق والمواد الاستدلالية فحسب بل يمتد ليشمل البيانات الرقمية والسوابق القضائية التي تطلبها السلطات الأجنبية وقد تجسد هذا الالتزام في

[1]ليث علام سعيد موسى،إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية،رسالة ماجستير(غير منشور)،تخصص القانون العام،كلية الدراسات العليا،جامعة النجاح الوطنية،نابلس_فلسطين_،2025،ص25.

[2]ليث علام سعيد موسى، مرجع نفسه،ص 25.

[3]ليث علام،المرجع السابق،ص26.

معاهدات دولية وإقليمية مثل معاهدة الأمم المتحدة النموذجية، اتفاقية الرياض، اتفاقية شنغن رغم ما يواجهه هذا المسار من تحديات تتعلق بمحدودية الاتفاقيات المتخصصة تقنياً أو عزوف بعض الدول عن الانضمام إليها، [1]كما يتجلى التكامل الدولي في آلية نقل الإجراءات الجنائية ،حيث تشرع دولة ما بناءً على اتفاقات مسبقة في مباشرة التحقيق والمقاضاة في جريمة وقعت على إقليم دولة أخرى ولصالحها خاصة حين تكون أدلة الجريمة متوفرة في الدولة المطلوب إليها النقل ويظل الازدواج التجريمي شرطاً جوهرياً لتفعيل هذه الآلية مع ضمان أن يكون الإجراء المتخذ ذا دور محوري في كشف الحقيقة مع احتفاظ الدول بحق الرفض إذا تعارض الطلب مع التزاماتها القانونية أو السيادية.

أما الأداة الأكثر فعالية في كسر الحواجز الجغرافية فهي الإنابة القضائية الدولية، وهي طلب رسمي رفيع المستوى يتيح للدولة الطالبة ممارسة أعمال قضائية داخل إقليم أجنبي ،كسماع الشهود أو التفتيش الرقمي لتعذر القيام بها بنفسها، وقد طورت الاتفاقيات الحديثة مثل الاتفاقية الأمريكية الكندية وميثاق منظمة المؤتمر الإسلامي ،هذه الأداة لتشمل الاتصال المباشر والتبادل الشفوي في حالات الاستعجال مما يضمن اختصار الإجراءات البيروقراطية الجامدة وتدفق الأدلة الرقمية بالسرعة التي تسبق حركة الجريمة، وصولاً إلى صياغة عدالة جنائية دولية قادرة على حماية الأمن المعلوماتي العالمي.

الفرع الثاني:التعاون الأمني الدولي لمواجهة الجرائم الإلكترونية

يُمثل التعاون الأمني الدولي خط الدفاع الأول و الضربة الاستباقية لتأمين المعاملات التجارية الإلكترونية من الهجمات السيبرانية الخاطفة و القرصنة المالية العابرة للحدود ،و تتجلى أهمية هذا التعاون في التبادل الفوري للمعلومات حول الثغرات وتتبع الأموال المشبوهة والتنسيق المشتركيين الأجهزة الأمنية كالإنتربول .

مما يسهم في إحباط الجرائم قبل وقوعها وتوفير بيئة استثمارية رقمية آمنة تحمي الشركات و المستهلكين على حد سواء في التعاون الأمني الدولي يعتبر الركيزة الأساسية في الاستراتيجية العالمية لمواجهة الجرائم المعلوماتية فبالنظر إلى طبيعة هذا التعاون بمفهومه الواسع نجد أنه نسيج متكامل يجمع بين المسارات الشرطية والقانونية والقضائية فالأمن في الفضاء الرقمي لا يتحقق بمجرد ملاحقة المطلوبين للعدالة بل يمتد ليشمل

[1] ط.د عبد القدوس بوعزة،ط.د أيوب مخرمش،"أساليب التعاون الدولي في القضاء على الجرائم الإلكترونية"،المجلة الجزائرية للعلوم السياسية والعلاقات الدولية ،جامعة ورقلة،المجلد13،العدد ثمنية عشر،جوان 2022،ص167.

منظومة استباقية و وقائية وقمعية توازن بدقة بين فاعلية المكافحة من جهة، واحترام سيادة الدول وحقوق المتهمين والضحايا من جهة أخرى.[1]

ويمكن تعريف هذا التعاون بأنه حالة من تضافر الجهود وتبادل العون بين دولتين أو أكثر بهدف التصدي لمخاطر الإجرام المعلوماتي وما يتبعه من تحديات في مجالات العدالة الجنائية و تبرز أهميته كضرورة حتمية فرضها التطور المتسارع للجريمة التي باتت ظاهرة عابرة للحدود.

مما استوجب تجاوز قيود السيادة الإقليمية ،من خلال آليات قانونية وقضائية وشرطية مرنة تتيح ملاحقة الجناة وتعقب التهديدات أينما وجدت،وتتعدد صور هذا التعاون الدولي لتبدأ من المستويات التقنية عبر ربط شبكات الاتصال والمعلومات لضمان السرعة الفائقة في تبادل البيانات بين سلطات التحقيق والملاحقة ولا يتوقف الأمر عند تبادل المعلومات بل يمتد إلى تنفيذ عمليات شرطية وأمنية مشتركة تشمل تعقب الأدلة الرقمية وتفتيش النظم المعلوماتية والحواسب العابرة للحدودوهو ما يسهم في صقل خبرات الكوادر الأمنية ووضع حد للإجرام المعلوماتي المنظم.[2]

وفي قلب هذا الحراك الدولي تبرز منظمة الشرطة الجنائية الدولية الانتربول كأكبر كيان أمني عالمي منذ تأسيسها عام 1923وتعمل المنظمة من خلال هيكل تنظيمي متطور يضم الجمعية العامة والأمانة العامة والمكاتب المركزية الوطنية حيث تركز استراتيجيتها على تبادل المعلومات حول المجرمين الدوليين ومكافحة الأنشطة الإجرامية المعقدة كغسل الأموال والجرائم الإلكترونية وقد استحدثت المنظمة وحدة تحليل المعلومات الجنائية لاستخلاص البيانات وتحليل أنماط المنظمات الإجرامية ووضعها تحت تصرف الدول الأعضاء[3].

وتتجسد أهداف الانتربول ،في بناء جسور التعاون بين أجهزة الشرطة العالمية بدءاً من جمع وتحليل[4]المعلومات عبر شبكات اتصال حديثة ووصولاً إلى إصدار النشرات الدولية لضبط الهاربين ،كما

[1] قاضي خولة،جباس منال ،التعاون الدولي في مكافحة الجريمة المعلوماتية،مذكرة لنيل شهادة الماستر(غير منشورة)،تخصص قانون أعمال ،كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح ورقلة،2020_2021،ص22.

[2] قاضي خولة،جباس منال،مرجع نفسه،ص22.

[3]قاضي خولة،جباس منال،مرجع نفسه،ص22.

[4]قاضي خولة،جباس منال،مرجع نفسه،ص23.

تلعب المنظمة دوراً محورياً في دعم البحث الجنائي من خلال قواعد بيانات البصمات والحمض النووي (DNA) مع الالتزام التام بروح الإعلان العالمي لحقوق الإنسان والقوانين الوطنية للدول.

وفي إطار التخصص الدقيق لمواجهة التهديدات الرقمية استحدث الانتربول في عام 2004 وحدة خاصة لمكافحة جرائم التكنولوجيا وعمل بالتعاون مع مجموعة الثماني الكبرى (G8) على تطوير استراتيجيات شاملة.

شملت هذه الجهود إنشاء مركز اتصال أمني يعمل على مدار الساعة، واستخدام برامج متطورة للتحليل الآلي للصور وقواعد البيانات المركزية فضلاً عن تقديم الدعم المعرفي والتدريبي للشرطة الوطنية عبر أدلة إرشادية متخصصة في التحقيق الرقميإن هذا الدور الذي يلعبه الانتربول يمثل حلقة الوصل الحيوية التي تضمن تناغم الجهود الدولية وتكاملها في مواجهة الجرائم المعلوماتية المتشعبة.[1]

[1] قاضي خولة،جباس منال،مرجع سابق،ص23.

خـــــاتمة

تُعد الجرائم الإلكترونية في المعاملات التجارية من أخطر التحديات التي فرضها التطور التكنولوجي في العصر الحديث، لأنها لا تقتصر على الاعتداء على البيانات والأنظمة المعلوماتية فحسب، بل تمتد آثارها إلى المساس بالثقة والأمان اللذين يشكلان الأساس الذي تقوم عليه المعاملات التجارية في البيئة الرقمية ومن خلال هذه الدراسة، حاولنا الوقوف على الإطار القانوني المنظم لهذه الجرائم، وبيان مدى كفاية القواعد القانونية في توفير حماية فعالة للمعاملات التجارية من مختلف صور الاعتداء الإلكتروني.

وقد أظهرت الدراسة أن حماية المعاملات التجارية في الفضاء الرقمي لم تعد مسألة اختيارية، وإنما أصبحت ضرورة قانونية واقتصادية تفرضها طبيعة التجارة الإلكترونية وما يرتبط بها من مخاطر متزايدة. فكلما توفرت حماية قانونية فعالة، تعززت الثقة في المعاملات الإلكترونية واستقر النشاط التجاري، بما يضمن التوفيق بين متطلبات التطور التكنولوجي وضرورة تحقيق العدالة والأمن القانوني.

يمكن الإجابة عن الإشكالية المطروحة بالقول إن المشرع الجزائري سعى إلى توفير حماية قانونية للمعاملات التجارية من خطر الجريمة الالكترونية من خلال تجريم مختلف صور الاعتداء على الأنظمة المعلوماتية ووسائل الدفع الإلكتروني، إلى جانب استحداث آليات إجرائية خاصة تتلاءم مع طبيعة الدليل الرقمي غير أن فعالية هذه الحماية تبقى نسبية، بالنظر إلى التطور السريع للجريمة الإلكترونية والصعوبات التقنية والإجرائية التي تواجه أجهزة التحقيق والإثبات.

وقد خلصت الدراسة إلى مجموعة من النتائج الأساسية، يمكن إجمالها فيما يلي:

_تتميز الجرائم الإلكترونية في المعاملات التجارية بطابع تقني خاص، وبصعوبة اكتشافها، وسرعة ارتكابها، وقدرتها على تجاوز الحدود الجغرافية.

_تختلف هذه الجرائم عن الجرائم التقليدية من حيث وسائل التنفيذ وطبيعة الأدلة المعتمدة في إثباتها، والتي تتمثل أساسًا في الأدلة الرقمية.

_وفّر المشرع الجزائري حماية موضوعية للمعاملات التجارية من خلال أحكام قانون العقوبات، والقانون التجاري، والتشريعات الخاصة بالتجارة الإلكترونية.

_أسهمت النصوص القانونية المنظمة للتجارة الإلكترونية في تعزيز الثقة في البيئة الرقمية وحماية الحقوق المالية والمعلوماتية للمتعاملين.

_تتطلب مكافحة هذه الجرائم إجراءات تحرٍ وتحقيق خاصة تتلاءم مع طبيعة الدليل الرقمي وسهولة إتلافه أو تغييره.

_يقتضي التعامل مع الجرائم الإلكترونية تحقيق التوازن بين فعالية المتابعة الجزائية واحترام الحقوق والحريات الأساسية، ولا سيما الحق في الخصوصية.

_يواجه القضاء وأجهزة إنفاذ القانون تحديات تقنية وفنية تستوجب تكوينًا متخصصًا ومستمرًا.

_يُعد التعاون القضائي والأمني الدولي عنصرًا أساسيًا في مواجهة الجرائم الإلكترونية بالنظر إلى طابعها العابر للحدود.

_لا تكفي الحماية القانونية وحدها لمواجهة هذه الجرائم، بل يجب دعمها بنشر الوعي الرقمي والقانوني لدى المتعاملين الاقتصاديين.

_تمثل حماية المعاملات التجارية في البيئة الرقمية شرطًا أساسيًا لتعزيز الثقة في التجارة الإلكترونية وضمان استقرار المعاملات الاقتصادية.

بناءا على النتائج المتوصل إليها يمكن تقديم الإقترحات التالية :

_مواصلة تحديث التشريعات الوطنية بما يواكب التطور التقني المستمر.

_تكوين قضاة وأعوان ضبطية قضائية متخصصين في مجال الجرائم الإلكترونية.

_تعزيز آليات التعاون الدولي والإقليمي في مجال تبادل المعلومات وتسليم المجرمين.

_نشر الوعي الرقمي والقانوني لدى المتعاملين الاقتصاديين للحد من مخاطر الاحتيال والاعتداء الإلكتروني.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا/ المصادر

-الاتفاقيات الدولية

- اتفاقية مجلس اروبا المتعلقة بالجريمة الالكترونية (بودابست)،المبرمة بتاريخ 23 نوفمبر 2001،مجموعة المعاهدات الاروبية رقم 185.
- سليمان أبو نمر،يوسف بوكريدة،مكافحة الجريمة المعلوماتية في ايطار القانون الدولي،مذكرة لنيل شهادة الماست،"غير منشور"،قسم الحقوق، كلية الحقوق والعلوم السياسية،جامعة محمد خيضر،بسكرة، 2020-2021.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، القاهرة، 21 ديسمبر 2010 (المصادق عليها بالمرسوم الرئاسي 14-252 لسنة 2014).

-القوانين العادية:

- القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، 2009.
- القانون رقم 24-06 المؤرخ في 28 أفريل 2024، المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 30، 2024.
- القانون رقم 18-05 المؤرخ في 10 ماي 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية، العدد 28، 2018.
- القانون رقم 04-02 المؤرخ في 23 جوان 2004، المحدد للقواعد المطبقة على الممارسات التجارية، الجريدة الرسمية، العدد 41، 2004.
- القانون رقم 25-24 المؤرخ في 15 أوت 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد 58، 2025.

- القانون 15-02 المؤرخفي 11 ربيعالثاني 1436 الموافقل 1فبراير 2015،المتعلق بتحصيل متبادل للمعلومات والوثائق بين الإدارات، الجريدة الرسمية للجمهورية الجزائرية، العدد السادس، الصادر بتاريخ 4 فبراير 2015.
- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 03-03 المتعلق بالمنافسة، الجريدة الرسمية، العدد 84، 2006.

-الأوامر:

- الأمر رقم 66-156 المتضمن قانون العقوبات، المعدل والمتمم (قانون 21-11 لسنة 2021 وقانون 04-15 وقانون 24-06).
- الأمر رقم 75-59 المؤرخ في 20رمضان عام 1395،الموافق 26 سبتمبر سنة 1975،المتضمن القانون التجاري،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد101،الصادر بتاريخ 19 ديسمبر 1975،المعدل والمتمم.
- الأمر 03-03 المتعلق بالمنافسة المؤرخ في 19 جمادى الأولى عام 1424 الموافق ل19 يوليو سنة 2003،الجريدة الرسمية للجمهورية الجزائرية، العدد ثلاثة واربعون، الصادر بتاريخ 20 يوليو2003.
- الامر 03-06 المؤرخ في 19 جمادى الثانية 1427 الموافق ل15يوليو سنة 2006، المتعلق بالعلامات،الجريدة الرسمية،الجمهورية الجزائرية، العدد سبعة واربعون،الصادر بتاريخ 19 يوليو 2006.
- الأمر رقم 21-11 ،مؤرخ في 14 ذي القعدة عام 1442 الموافق 25 يونيو 2021،يعدل ويتمم الأمر رقم 66-156،المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية،العدد50،الصادر في27يونيو2021.

-المراسيم الرئاسية

- مرسوم رئاسي رقم 14-252،مؤرخ في 13ذي القعدة عام 1435الموافق 8 سبتمبر سنة 2014،يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،المعتمدة بالقاهرة

في 21 ديسمبر سنة 2010،الجريدة الرسمية للجمهورية الجزائرية،العدد54،الصادر في 17 سبتمبر2014.

-المراسيم التنفيذية

- المرسوم التنفيذي رقم 90-39 ،المتعلق بمراقبة الجودة وقمع الغش،ا،لمؤرخ في 3 رجب عام 1410 الموافق 30 يناير سنة 1990،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية،العدد05،الصادر بتاريخ 31 يناير.

ثانيا/ المراجع العامة

- يزيد بوحليط،الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقيات العربية لمكافحة جرائم التقنية المعلومات قانون العقوبات قانون إجراءات الجزائية قوانين خاصة،دار الجامعة الجديدة،الجزائر.
- نادية فضيل،القانون التجاري الجزائرري (الاعمال التجارية-التاجر- المحل التجاري)،ديوان المطبوعات الجامعية،الجزائر،الطبعة 06، 2024.

-الأطروحات والمذكرات

الأطروحات

- بسمة صيشي،الحماية القانونية للمارسات التجارية الإلكترونية،رسالة دكتوراه(غير منشورة)،شعبة القانون الخاص،تخصص قانون الأعمال،قسم الحقوق،كلية الحقوق الحقوق والعلوم السياسية،جامعة الوادي،2024-2025.

المذكرات

- آية بن ميسية، الجريمة الالكترونية والية مكافحتها في التشريع الجزائري، مذكرة ضمن متطلبات شهادة الماستر، قسم حقوق، كلية الحقوق والعلوم السياسية، جامعة عبد الحفيظ بوالصوف، ميلة، 2024-2025.

- سليمان أبو نمر،يوسف بوكريدة،مكافحة الجريمة المعلوماتية في ايطار القانون الدولي،مذكرة لنيل شهادة الماستر،"غير منشور"،قسم الحقوق، كلية الحقوق والعلوم السياسية،جامعة محمد خيضر،بسكرة، 2020-2021.

- شيماء بقدار، آليات مكافحة الجريمة الإلكترونية على المستويين الدولي والوطني، مذكرة نهاية الدراسة، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2022-2023.
- ليث علام سعيد موسى،إشكاليات التعاون الدولي في مواجهة الجرائم الإلكترونية،رسالة ماجستير(غير منشور)،تخصص القانون العام،كلية الدراسات العليا،جامعة النجاح الوطنية،نابلس_فلسطين_،2025.
- قاضي خولة،جباس منال ،التعاون الدولي في مكافحة الجريمة المعلوماتية،مذكرة لنيل شهادة الماستر(غير منشورة)،تخصص قانون أعمال ،كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح ورقلة،2020_2021.
- **-المقالات العلمية**

- عفاف لعقون، جميلة فشار،"الجريمة الالكترونية: المقاربة المفاهيمية القانونية"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تمنراست، جامعة الجلفة،المجلد15،العدد واحد،جانفي 2021
- الطاهر ياكر،"مكافحة الجرائم الالكترونية بين التشريعات الوطنية والاتفاقيات الدولية"،مجلة الصدى للدراسات القانونية والسياسية،جامعة الجيلالي بونعامة، خميس مليانة،الجزائر،المجلد 04،العدد الرابع،ديسمبر 2022.
- شريف خالد، " الجرائم المتصلة بتكنولوجيا الاعلام والاتصال في التشريع الجزائري" ،مجلة البيان للدراسات القانونية، جامعة محمد خيضر بسكرة،الجزائر، المجلد 10،العدد واحد،جوان 2025.
- بن شيخ راضية، نساخ فطيمة، " الشفافية وعلاقتها بالنزاهة الممارسات التجارية"، المجلة الجزائرية للعلوم القانونية السياسية، كلية الحقوق جامعة الجزائر، المجلد57،العدد الخامس،ديسمبر2020.

- نواصر الطاهر وغزالي نصيرة،" ممارسات التجارية التدليسية وغير النزيهة في قانون رقم 04-02 المعدل والمتمم"، مجلة الفكر القانوني والسياسي،جامعة الحاج موسى،تمنراست،جامعة ثليجي بالاغواط،المجلد 06،العدد الأول، 2022.
- مهداوي حنان،" التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري"،مجلة الفكر القانوني والسياسي،جامعة لمين دباغين،سطيف02،المجلد 06،العدد الثاني، 2022.
- شهاب بن عبد الرحمن بن حامد المسعود،"أركان الجريمة الإلكترونية"،المجلة الدولية والدراسات القانونية،جامعة الملك عبد العزيز،الإصدار الرابع،العدد الرابع،سنة 2025.
- كاملة بوعكة،"حماية المستهلك الإلكتروني جزائيا في ذل التجارة الإلكترونية"،مجلة الدراسات والبحوث القانونية،كلية الحقوق والعلوم السياسية،جامعة المسيلة-الجزائر-،المجلد10،العدد واحد جانفي 2025.
- موزالي نور الدين،"الجرائم المعلوماتية في إطار التجارة الإلكترونية وسبل مكافحتها"،مجلة الدراسات القانونية،مخبر السيادة والعولمة،جامعة يحي فارس بالمدية،الجزائر،المجلد 09،العدد الثاني،جوان 2023.
- شاكر سليمان، " القواعد الإجرائية والموضوعية للجريمة المعلوماتية في التشريع الجزائري"،المجلة الجزئرية للحقوق والعلوم السياسية،جامعة تيسمسيلت، المجلد9،العدد واحد، 2004.
- سعيداني سلامي، " تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية (وقائع ومقاربات)"،مجلة الأستاذ الباحث للدراسات القانونية والسياسية،جامعة محمد بوضياف،المسيلة،العدد العاشر، جوان 2018.
- آمنة قريش، "مظاهر التعاون الدولي لمكافحة الجرائم المعلوماتية: الآليات والتحديات"، دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة خميس مليانة، المجلد 18، العدد 01، جانفي 2026.
- ط.د هاني مطر منصور أبو سعود، د.عباسة طاهر،"الأنظمة القانونية العربي وتحدي التعاون في مواجهة الجرائم المعلوماتية"،مجلة الاجتهاد القضائي،مخبر أثر الاجتهاد القضائي على حركة التشريع،جامعة محمد خيضر،المجلد،العدد الثاني،أكتوبر 2021.

- ط.د عبد القدوس بوعزة،ط.د أيوب مخرمش،"أساليب التعاون الدولي في القضاء على الجرائم الإلكترونية"،المجلة الجزائرية للعلوم السياسية والعلاقات الدولية ،جامعة ورقلة،المجلد13،العدد ثمنية عشر،جوان 2022.

فهرس المحتويات

فهرس المحتويات

قائمة المختصرات .....-
مقدمة.....أ
الفصل الأول: الاطارالمفاهيمي للجرائم الإلكترونية الماسة بالمعاملات التجارية 1
المبحث الأول :ماهية الجرائم الإلكترونية الماسة بالمعاملات التجارية : 12
المطلب الأول:مفهوم الجرائم الإلكترونية.....12
الفرع الأول: تعريف الجرائم الإلكترونية 12
الفرع الثاني: أنواع الجرائم الإلكترونية 17
المطلب الثاني: خصائص وأركان الجريمة الإلكترونية 20
الفرع الأول: خصائص الجريمة الإلكترونية 20
الفرع الثاني:أركان الجريمة الإلكترونية.....24
المبحث الثاني: ماهية المعاملات التجارية.....27
المطلب الأول:مفهوم المعاملات التجارية 27
الفرع الأول:التعريف الإصطلاحي للمعاملات التجارية 28
الفرع الثاني:التعريف القانوني للمعاملات التجارية 28
المطلب الثاني:تصنيف الممارسات التجارية من حيث المشروعية 29
الفرع الأول:الممارسات التجارية المشروعة القائمة على النزاهة والشفافية.....29
الفرع الثاني:الممارسات التجارية الغير المشروعة التدليسية وغير النزيهة.....33
الفصل الثاني:المظام القانوني للجرائم الإلكترونية الماسة بالمعاملات التجاري 30
المبحث الأول :الأساس القانوني لتجريم الجرائم الإلكترونية الماسة بالمعاملات التجارية في التشريع الجزائري 40
المطلب الأول:الأسس القانونية والقواعد الموضوعية للجريمة الإلكترونية.....41

الفرع الأول:الأسس القانونية المنظمة للجرائم الإلكترونية في الجزائر.....41
الفرع الثاني:آليات الحماية الموضوعية للمعاملات التجارية من للجريمة الإلكترونية 49
المطلب الثاني: جماية الإجرائية للمعاملات التجارية من الجريمة الإلكترونية 50
الفرع الأول:التفتيش التكنولوجي للحواسيب 53
الفرع الثاني: التوقيف النظر.....54
المبحث الثاني:الأساس القانوني لتجريم الجرائم الإلكترونية الماسة بالمعاملات التجارية في الإتفاقيات الدولية.....55
المطلب الأول:الإطار الإتفاقي الدولي والعربي لمكافحة الجريمة الإلكترونية 55
الفرع الأول: الإتفاقيات والمعاهدات الدولية في مواجهة الجريمة الإلكترونية 55
الفرع الثاني:دور التشريعات المقارنة في مواجهة الجريمة الإلكترونية 58
المطلب الثاني:أساليب التعاون الدولي في محاربة الجرائم الإلكترونية 62
الفرع الأول:التعاون القضائي الدولي في مواجهة الجريمة الإلكترونية 63
الفرع الثاني:التعاون الأمني الدولي لمواجهة الجرائم الإلكترونية.....64
خـــاتمة 58
قائمة المصادر والمراجع 60
فهرس المحتويات 66
ملخص:. 71

ملخص:

تتمحور هذه الدراسة حول الآليات القانونية لمواجهة الجرائم الإلكترونية الماسة بالمعاملات التجارية، حيث تسعى لتقييم مدى نجاعة المنظومة التشريعية الجزائرية، لاسيما بعد تعديلات عام 2024، في خلق توازن معقد بين ضرورة الردع الجنائي وبين صون كرامة الإنسان وحقوقه في الفضاء الرقمي. وينصب التركيز، التزاماً بالأمانة العلمية، على تحليل القواعد الموضوعية والإجرائية المستحدثة لحماية الائتمان التجاري وتعزيز الثقة في السوق الافتراضي، مع تبيان كيف سعى المشرع لتطويع النصوص القانونية لملاحقة "الدليل الرقمي" العابر للحدود دون المساس بحرمة الحياة الخاصة. ويخلص البحث إلى أن بناء بيئة تجارية رقمية آمنة يتطلب تكاملاً بين صرامة القانون والتعاون الدولي الفاعل، بما يضمن سيادة العدالة وحماية الأفراد من التغول الإجرامي التقني، ترسيخاً لمبادئ دولة القانون التي تجعل من كرامة الإنسان غاية أسمى لكل تشريع.

كلمات مفتاحية: الجرائم الإلكترونية، الائتمان التجاري، التشريع الجزائري 2024، الردع الجنائي، الثقة الرقمية، الدليل الرقمي، السيادة القانونية، الحماية الإجرائية، التعاون الدولي

ABSTRACT This study centers on the **legal mechanisms for combating cybercrimes affecting commercial transactions**, seeking to evaluate the efficacy of the Algerian legislative framework—particularly following the **2024 amendments**—in establishing a complex balance between the necessity of criminal deterrence and the preservation of human dignity and rights within the digital sphere. Committed to scientific integrity, the focus is placed on analyzing the newly introduced substantive and procedural rules designed to protect commercial credit and bolster trust in the virtual market. Furthermore, it demonstrates how the legislator sought to adapt legal provisions to pursue transboundary "digital evidence" without infringing upon the sanctity of private life. The research concludes that building a secure digital commercial environment requires integration between legal rigor and effective international cooperation, thereby ensuring the rule of law and protecting individuals from technical criminal encroachment, in reinforcement of the principles of a constitutional state that regards human dignity as the ultimate goal of all legislation.

Keyword : Cybercrimes, Commercial Credit, Algerian Legislation 2024, Criminal Deterrence, Digital Trust, Digital Evidence, Legal Sovereignty, Procedural Protection, International Cooperation.