

جامعة سعيدة، الدكتور مولاي الطاهر



كلية الحقوق والعلوم السياسية

قسم القانون الخاص

مذكرة لاستكمال متطلبات الحصول على درجة ماستر الحقوق

تخصص: إدارة الكترونية

الجرائم الالكترونية في التشريع الجزائري

تحت إشراف الأستاذة

خادم حمزة

من إعداد الطالبان:

- زادي محمد ال سيد الشيخ

- بومدين صلاح الدين

أعضاء لجنة المناقشة

رئيساً	جامعة سعيدة	أستاذ التعليم العالي	الدكتورة مراح نعيمة
مشرفاً ومقرراً	جامعة سعيدة	أستاذ التعليم العالي	الدكتورة خادم حمزة
عضواً	جامعة سعيدة	أستاذ التعليم العالي	الدكتور عصموني خليفة

السنة الجامعية: 2026/2025

جامعة سعيدة، الدكتور مولاي الطاهر



كلية الحقوق والعلوم السياسية قسم القانون الخاص

مذكرة لاستكمال متطلبات الحصول على درجة ماستر الحقوق
تخصص: إدارة الكترونية

الجرائم الالكترونية في التشريع الجزائري

تحت إشراف الأستاذة
خادم حمزة

من إعداد الطالبان:

- زادي محمد ال سيد الشيخ
- بومدين صلاح الدين

أعضاء لجنة المناقشة

رئيساً	جامعة سعيدة	أستاذ التعليم العالي	الدكتورة مراح نعيمة
مشرفاً ومقرراً	جامعة سعيدة	أستاذ التعليم العالي	الدكتورة خادم حمزة
عضواً	جامعة سعيدة	أستاذ التعليم العالي	الدكتور عصموني خليفة

السنة الجامعية: 2026/2025

اهداء

إلى من كانا سندي في كل خطوة، ومن غرسا في قلبي حب العلم والطموح، إلى من كان دعاؤهما سر نجاحي، وتعبهما ثمرة كل إنجاز أصل إليه...

إلى والدي العزيز، الذي علمني الصبر والاجتهاد، وكان دائما مصدر قوة ودعم لي، وإلى والدتي الغالية، التي أحاطتني بدعائها وحنانها وتشجيعها، وكان وجودها في حياتي أعظم نعمة.

إليكما أهدي ثمره هذا العمل المتواضع، عرفانا وامتنانا لكل ما قدمتماه لي من حب ودعم وتضحيات، راجية من الله أن يحفظكما ويطيل في عمركما، وأن أكون دائما عند حسن ظنكما.

إلى والدي ووالدتي...
لكما كل الحب والامتنان.

زادي محمد ال سيد الشيخ

إهداء

إلى من كانا لي السند والعون في كل مراحل حياتي، إلى من زرعنا في قلبي حب العلم، وغرسا في نفسي الأمل والطموح، وكان دعائهما رفيقي في كل خطوة، وتضحياتهما أساس كل نجاح وصلت إليه...

إلى والدي العزيز، من علمني أن النجاح ثمرة للصبر والاجتهاد، وكان دائما مصدر ثقة وقوة ودعم، وإلى والدتي الغالية، من أحاطتني بحنانها ودعائها، وكانت كلماتها وتشجيعها دافعا لي لمواصلة الطريق مهما كانت الصعوبات.

إليكما أهدي هذا العمل المتواضع، تعبيرا عن خالص محبتي وامتناني لكل ما قدمتماه لي من حب وتضحيات ودعم لا حدود له، سائلا الله أن يحفظكما، ويمتلككما بالصحة والعافية، ويطيل في أعماركما، وأن يجعلني دائما مصدر فخر وسعادة لكما.

إلى والدي ووالدتي...

لكما أهدي ثمرة هذا الجهد، ولكما وحدكما يعود الفضل بعد الله في كل خطوة وصلت إليها.

لكما كل الحب والامتنان.

بومدين صلاح الدين

شكر وعرفان

الحمد لله الذي بنعمته تتم الصالحات، والحمد لله الذي وفقنا وأعاننا على إتمام هذا العمل، ويسر لنا سبل إنجازه، فله الحمد والشكر أولاً وآخراً.

نتقدم بخالص الشكر وعظيم الامتنان إلى الأستاذ المشرف حمزة، على ما قدمه لنا من توجيهات قيمة ونصائح سديدة وملاحظات بناءة، وعلى حرصه ومتابعته التي كان لها بالغ الأثر في إنجاز هذه المذكرة وإخراجها في صورتها النهائية.

كما نتوجه بجزيل الشكر والتقدير إلى جميع أساتذتنا الكرام الذين رافقونا خلال مسيرتنا الجامعية، وأسهموا بعلمهم وتوجيهاتهم في تكويننا العلمي والمعرفي، فلكم منا كل التقدير والاحترام.

ولا يفوتنا أن نعبر عن خالص امتناننا لكل من ساهم في إنجاز هذا العمل، سواء بالمساعدة أو التوجيه أو التشجيع، ولكل من قدم لنا دعماً من قريب أو بعيد، وكان له أثر في تجاوز الصعوبات والوصول إلى إتمام هذه المذكرة.

وفي الختام، نسأل الله أن يجزي الجميع عنا خير الجزاء، وأن يجعل ما قدموه لنا في ميزان حسناتهم، وأن يوفقنا لما فيه الخير والنجاح.

قائمة المختصرات

المختصر	الدلالة
ج.ر.ج.ج	الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية
ق.ع	قانون العقوبات
ق.إ.ج	قانون الإجراءات الجزائية
ق.م.ج	قانون مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
م.م.م.ب	منظومة المعالجة الآلية للمعطيات
ت.إ.إ	تكنولوجيات الإعلام والاتصال
م.إ.إ	منظومة معلوماتية
د.إ	الدليل الإلكتروني
م.ع.ش	المعطيات ذات الطابع الشخصي
ص	صفحة
ط	الطبعة

مقدمة

شهد العالم خلال العقود الأخيرة تطورا متسارعا في مجال تكنولوجيايات الإعلام والاتصال، أدى إلى إحداث تحولات عميقة في مختلف المجالات الاقتصادية والإدارية والاجتماعية، حيث أصبحت الأنظمة المعلوماتية والشبكات الإلكترونية من أهم الوسائل المعتمدة في تخزين المعلومات ومعالجتها وتبادلها، كما ساهم الانتشار الواسع لشبكة الإنترنت ووسائل الاتصال الحديثة في تسهيل الوصول إلى المعلومات وتسريع تداولها وتوسيع نطاق المعاملات الإلكترونية. غير أن هذا التطور التكنولوجي لم يقتصر على تحقيق مزايا إيجابية، وإنما أفرز في المقابل أنماطا إجرامية مستحدثة تستغل الوسائل التقنية والبيئة الرقمية لارتكاب أفعال تمس بالأشخاص والأموال والأنظمة المعلوماتية والبيانات الرقمية، وهو ما جعل الجريمة الإلكترونية من أبرز التحديات التي تواجه السياسة الجنائية المعاصرة¹

وتتميز الجريمة الإلكترونية عن الجريمة التقليدية بارتباطها المباشر بالتكنولوجيا، سواء من حيث الوسيلة المستعملة في ارتكابها أو محل الاعتداء عليها، كما تتميز بسرعة تنفيذها وصعوبة اكتشاف مرتكبيها وإخفاء آثارها الرقمية، فضلا عن إمكانية ارتكابها من أماكن مختلفة وعبر الحدود الإقليمية للدول. وقد أدى ذلك إلى بروز صعوبات أمام القواعد القانونية التقليدية، خاصة فيما يتعلق بتحديد الاختصاص، والكشف عن الجناة، وجمع الأدلة الإلكترونية والحفاظ عليها وإثباتها أمام القضاء، الأمر الذي فرض ضرورة تطوير التشريعات الوطنية وآليات البحث والتحري بما يتلاءم مع طبيعة البيئة الرقمية، مع مراعاة حماية الحقوق والحريات الفردية.

وفي هذا السياق، عمل المشرع الجزائري على وضع إطار قانوني لمواجهة الجرائم المرتبطة بتكنولوجيايات الإعلام والاتصال، من خلال مجموعة من النصوص القانونية التي تضمنت أحكاما موضوعية وإجرائية لمكافحة هذا النوع من الإجرام، وفي مقدمتها أحكام قانون العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، إلى جانب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيايات الإعلام والاتصال ومكافحتها²، فضلا عن النصوص القانونية المرتبطة بحماية المعطيات ذات الطابع الشخصي والملكية الفكرية والتوقيع والتصديق الإلكترونيين. ولم

¹ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 19-25.

² القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيايات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادرة في 16 غشت 2009.

يقتصر تدخل المشرع الجزائي على تحديد الأفعال المجرمة والعقوبات المقررة لها، وإنما امتد إلى تنظيم بعض إجراءات البحث والتحري والتفتيش وضبط الأدلة ذات الصلة بالجرائم الإلكترونية، بما يعكس محاولة تكييف المنظومة الجزائية مع خصوصية الإجرام المعلوماتي¹

وتنبع أهمية الدراسة من الأهمية المتزايدة التي أصبحت تكتسبها الجريمة الإلكترونية في ظل الاعتماد المتنامي على الوسائل الرقمية في مختلف مناحي الحياة. فمن الناحية العلمية، تساهم الدراسة في توضيح مفهوم الجريمة الإلكترونية وخصائصها وصورها، وبيان الإطار القانوني الذي اعتمده المشرع الجزائي لمواجهتها، مع إبراز خصوصية القواعد المتعلقة بالبحث والتحري والإثبات في البيئة الرقمية. أما من الناحية العملية، فتتجلى أهمية الموضوع في ارتباطه بحماية الأنظمة المعلوماتية والبيانات والأموال والحياة الخاصة للأفراد، ومدى فعالية الآليات القانونية في تمكين أجهزة العدالة من اكتشاف الجرائم الإلكترونية وتحديد مرتكبيها وإثبات مسؤوليتهم الجزائية.

وتهدف هذه الدراسة إلى بيان ماهية الجريمة الإلكترونية وخصائصها وصورها في التشريع الجزائي، وتحليل مظاهر الحماية القانونية المقررة للأنظمة المعلوماتية، مع الوقوف على أهم النصوص الموضوعية التي تجرم الأفعال المرتبطة بها وتحدد العقوبات المقررة لها. كما تهدف إلى دراسة الآليات الإجرائية المعتمدة لمكافحة الجريمة الإلكترونية، لا سيما إجراءات البحث والتحري والتفتيش وضبط الأدلة الإلكترونية وحجبتها وإجراءات الحفاظ عليها، بالإضافة إلى تقييم مدى قدرة المنظومة القانونية الجزائية على الاستجابة للخصوصية التي تتميز بها الجريمة الإلكترونية في ظل التطور المستمر للوسائل والتقنيات الرقمية.

أما مبررات اختيار الموضوع فتتوزع بين مبررات موضوعية وأخرى علمية؛ إذ تتمثل المبررات الموضوعية في الانتشار المتزايد لاستخدام تكنولوجيات الإعلام والاتصال وتنامي الاعتماد على الأنظمة الرقمية، وما ترتب عن ذلك من تعدد صور الاعتداءات الإلكترونية واتساع نطاق الأضرار الناجمة عنها. كما تتمثل في الأهمية التي أصبحت تحتلها حماية الأنظمة المعلوماتية والبيانات الرقمية والأموال والحياة الخاصة من الاعتداءات المرتكبة في البيئة الإلكترونية. أما المبررات العلمية فتتمثل في الرغبة في دراسة مدى قدرة التشريع الجزائي على مواجهة هذه الظاهرة الإجرامية، ومدى ملاءمة

¹ محمد أمين الشوابكة، جرائم الحاسوب والإنترنت: الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2007، ص 23-31.

القواعد القانونية الموضوعية والإجرائية المقررة مع طبيعة الجرائم الإلكترونية، خاصة في ظل التطور المتواصل للتكنولوجيا وظهور أساليب إجرامية جديدة.

وقد تناولت الدراسات السابقة موضوع الجريمة الإلكترونية في التشريع الجزائري من زوايا مختلفة، ومن أبرزها دراسة عيمور راضية بعنوان الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، المنشورة في المجلة الأكاديمية للبحوث القانونية والسياسية سنة 2022، حيث تناولت الباحثة مفهوم الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، من خلال التركيز على الجوانب الموضوعية والإجرائية، وانتهت إلى أن المشرع الجزائري اعتمد سياسة تجمع بين القواعد العامة الواردة في التشريع الجزائري والقواعد الخاصة المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

كما تناولت دراسة شيخ ناجية المعنونة حول مكافحة الجريمة الإلكترونية في التشريع الجزائري، المنشورة في مجلة العلوم القانونية والسياسية سنة 2018، مختلف التدابير التي اعتمدها المشرع الجزائري لمواجهة الجريمة الإلكترونية، مع التركيز على الأحكام التي تضمنها قانون العقوبات وقانون الإجراءات الجزائية والقانون رقم 09-04، وأبرزت توجه المشرع نحو الجمع بين القواعد العامة والأحكام الخاصة في مجال مكافحة الجرائم الإلكترونية¹

وفي السياق نفسه، جاءت دراسة معزوز ربيع وزروقي آسيا بعنوان الجريمة الإلكترونية وإجراءات مواجهتها في التشريع الجزائري، المنشورة في مجلة القانون والعلوم السياسية سنة 2021، حيث ركزت على خصوصية الجريمة الإلكترونية والإجراءات القانونية المعتمدة لمواجهتها، مع إبراز ضرورة تكييف وسائل المكافحة القانونية مع التطور التقني وطبيعة الجرائم المرتكبة باستعمال الوسائل الإلكترونية²

وتتميز الدراسة الحالية عن الدراسات السابقة بمحاولتها الجمع بين الجانب الموضوعي والجانب الإجرائي للجريمة الإلكترونية ضمن دراسة واحدة؛ فهي لا تقتصر على تحديد مفهوم الجريمة الإلكترونية وخصائصها وصورها، وإنما تمتد إلى تحليل الحماية القانونية المقررة للأنظمة المعلوماتية في

¹ ناجية شيخ، «حول مكافحة الجريمة الإلكترونية في التشريع الجزائري»، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 2، جامعة الشهيد حمه لخضر بالوادي، الجزائر، 2018، ص 701-688.

² ربيع معزوز، آسيا زروقي، «الجريمة الإلكترونية وإجراءات مواجهتها في التشريع الجزائري»، مجلة القانون والعلوم السياسية، المجلد 7، العدد 2، الجزائر، 2021، ص 370-358.

التشريع الجزائري، ودراسة العقوبات المقررة، إلى جانب بحث إجراءات البحث والتحري والتفتيش وضبط الأدلة الإلكترونية وحجيتها وطرق الحفاظ عليها، بما يسمح بالوقوف على مدى كفاية المنظومة القانونية الجزائرية في مواجهة خصوصية الجريمة الإلكترونية.

وبناء على ما سبق، يمكن طرح الإشكالية الرئيسية للدراسة على النحو الآتي:

إلى أي مدى وفق المشرع الجزائري في وضع منظومة قانونية فعالة لمكافحة الجريمة الإلكترونية، ومدى ملائمة الآليات الموضوعية والإجرائية المقررة لخصوصية هذا النوع من الجرائم؟

وتتفرع عن هذه الإشكالية مجموعة من الأسئلة الفرعية تتمثل فيما يأتي:

- ما المقصود بالجريمة الإلكترونية، وما أهم خصائصها وصورها؟
- ما هي أهم صور الجرائم الإلكترونية التي تناولها التشريع الجزائري؟
- ما مدى كفاية الحماية الجنائية التي أقرها المشرع الجزائري للأنظمة المعلوماتية؟
- ما هي العقوبات المقررة للجرائم الإلكترونية في التشريع الجزائري؟
- ما مدى فعالية إجراءات البحث والتحري والتفتيش في مكافحة الجريمة الإلكترونية؟
- كيف نظم المشرع الجزائري مسألة ضبط الأدلة الإلكترونية والحفاظ عليها وإثبات حجيتها أمام القضاء؟
- إلى أي مدى تستجيب المنظومة القانونية الجزائرية للتطور المستمر للجريمة الإلكترونية؟

وانطلاقاً من الإشكالية المطروحة والأسئلة المتفرعة عنها، يمكن صياغة فرضيات الدراسة على النحو الآتي:

الفرضية الرئيسية:

يفترض أن المشرع الجزائري وضع منظومة قانونية تجمع بين الأحكام الموضوعية والإجرائية لمكافحة الجريمة الإلكترونية، إلا أن فعالية هذه المنظومة قد تواجه بعض التحديات المرتبطة بالتطور المستمر للتكنولوجيا والطبيعة الخاصة للجرائم الإلكترونية.

وتتفرع عنها الفرضيات الآتية:

- يفترض أن خصوصية الجريمة الإلكترونية من حيث طبيعتها ووسائل ارتكابها ومحل الاعتداء عليها تفرض قواعد قانونية خاصة إلى جانب القواعد العامة.
- يفترض أن المشرع الجزائري وفر حماية جنائية للأنظمة المعلوماتية من خلال تجريم مجموعة من الأفعال المرتبطة بالمساس بأنظمة المعالجة الآلية للمعطيات وغيرها من الاعتداءات الإلكترونية.
- يفترض أن الإجراءات التقليدية للبحث والتحري لا تكفي بمفردها لمواجهة الجرائم الإلكترونية، مما يستوجب اعتماد إجراءات تتلاءم مع طبيعة الأدلة والبيئة الرقمية.
- يفترض أن الأدلة الإلكترونية تطرح إشكالات خاصة تتعلق بجمعها وحفظها وسلامة محتواها وحجيتها أمام القضاء.
- يفترض أن التطور السريع للوسائل التقنية وأساليب ارتكاب الجرائم الإلكترونية يفرض ضرورة المراجعة المستمرة للإطار القانوني والإجرائي لمكافحتها.

أما من حيث **حدود الدراسة**، فتتمثل الحدود الموضوعية في دراسة الجريمة الإلكترونية من الناحية القانونية، مع التركيز على مفهوميها وخصائصها وصورها وأحكامها الموضوعية والإجرائية، لاسيما ما يتعلق بالبحث والتحري والتفتيش وضبط الأدلة الإلكترونية وحجيتها والحفاظ عليها. وتتمثل الحدود المكانية في التشريع الجزائري، باعتباره الإطار القانوني الأساسي للدراسة، مع الاستعانة ببعض المقارنات عند الضرورة. أما الحدود الزمنية، فتتمثل في النصوص القانونية الجزائرية ذات الصلة بالموضوع إلى غاية الفترة التي تغطيها الدراسة، مع مراعاة التعديلات التشريعية ذات الصلة.

وللإجابة عن الإشكالية المطروحة واختبار الفرضيات، تم الاعتماد أساسا على **المنهج الوصفي** من خلال عرض مفهوم الجريمة الإلكترونية وخصائصها وتصنيفاتها وصورها، وعلى **المنهج التحليلي** لتحليل النصوص القانونية الجزائرية المتعلقة بالجريمة الإلكترونية وبيان الأحكام الموضوعية والإجرائية التي تضمنتها، كما تم الاستعانة بـ **المنهج المقارن** عند الحاجة، بهدف الاستفادة من بعض التجارب التشريعية المقارنة وتوضيح بعض المسائل التي تقتضي المقارنة.

وقد واجهت الدراسة جملة من **الصعوبات**، من أبرزها الطبيعة التقنية والمتغيرة للجريمة الإلكترونية، الأمر الذي يتطلب الجمع بين المفاهيم القانونية وبعض الجوانب التقنية المرتبطة بالأنظمة المعلوماتية والبيانات الرقمية. كما تمثلت الصعوبات في تعدد النصوص القانونية المنظمة للموضوع

وتوزعها بين قانون العقوبات والقوانين الخاصة، فضلا عن التطور المستمر في أساليب ارتكاب الجرائم الإلكترونية وظهور صور جديدة قد لا تكون محل تنظيم تشريعي صريح. ويضاف إلى ذلك ما تثيره الطبيعة العابرة للحدود لبعض الجرائم الإلكترونية من إشكالات تتعلق بالاختصاص القضائي والتعاون الدولي والحصول على الأدلة الإلكترونية الموجودة خارج الإقليم الوطني.

ولمعالجة الموضوع والإجابة عن الإشكالية المطروحة، تم تقسيم الدراسة إلى **فصلين**؛ تناول **الفصل الأول: الإطار المفاهيمي والتنظيمي للجريمة الإلكترونية**، حيث خصص لبيان مفهوم الجريمة الإلكترونية وخصائصها وتصنيفاتها، ثم دراسة أهم صور الجرائم الإلكترونية التي تناولها التشريع الجزائي، سواء تلك الواقعة على أنظمة المعالجة الآلية للمعطيات أو الواقعة على الأموال والأشخاص. أما **الفصل الثاني: آليات مكافحة الجريمة الإلكترونية في التشريع الجزائي**، فقد خصص لدراسة الحماية الموضوعية للأنظمة المعلوماتية من خلال النصوص القانونية ذات الصلة، لاسيما قانون العقوبات والقانون رقم 09-04، ثم تناول الآليات الجزائية والإجرائية لمكافحة الجريمة الإلكترونية، من خلال دراسة العقوبات المقررة وإجراءات البحث والتحري والتفتيش وضبط الأدلة الإلكترونية وحجبتها وإجراءات الحفاظ عليها.

الفصل الأول: ماهية الجريمة الإلكترونية وتنظيمها في التشريع الجزائري

أفرز التطور المتسارع في مجال تكنولوجيات الإعلام والاتصال أنماطاً جديدة من السلوك الإجرامي، نتيجة استغلال الوسائل والأنظمة المعلوماتية في ارتكاب أفعال تمس بالأشخاص والأموال والبيانات والأنظمة المعلوماتية، وهو ما أدى إلى بروز الجريمة الإلكترونية كصورة من صور الإجرام الحديث. وتتميز هذه الأخيرة بخصوصية تختلف بها عن الجرائم التقليدية، سواء من حيث طبيعة الوسيلة المستعملة أو محل الاعتداء أو صعوبة اكتشافها وإثباتها، الأمر الذي جعل تحديد مفهومها وخصائصها وتصنيف صورها من المسائل التي حظيت باهتمام الفقه والتشريع.

وقد سعى المشرع الجزائري إلى مواجهة هذه الظاهرة الإجرامية من خلال إقرار مجموعة من الأحكام القانونية التي توفر الحماية الجنائية للأنظمة المعلوماتية ومختلف المصالح التي يمكن أن تكون محل اعتداء في البيئة الإلكترونية، لا سيما من خلال أحكام قانون العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، إلى جانب القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وعليه، يقتضي الوقوف على ماهية الجريمة الإلكترونية تحديد مفهومها وخصائصها وأهم أنواعها في المبحث الأول، ثم بيان أبرز صورها التي نظمها التشريع الجزائري في المبحث الثاني

المبحث الأول: ماهية الجريمة الإلكترونية

تُعد الجريمة الإلكترونية من الظواهر الإجرامية المستحدثة التي فرضها التطور المتسارع لتكنولوجيات الإعلام والاتصال، والتي تتميز بخصوصية من حيث مفهومها وطبيعتها ووسائل ارتكابها. وعليه، يقتضي تحديد ماهية الجريمة الإلكترونية الوقوف على مختلف التعريفات الفقهية والقانونية لها، وبيان أهم خصائصها التي تميزها عن الجرائم التقليدية، فضلاً عن تحديد أبرز تصنيفاتها وصورها، وهو ما سيتم تناوله من خلال ثلاثة مطالب.

المطلب الأول: تعريف الجريمة الإلكترونية وتمييزها عن الجريمة التقليدية

يُعد تحديد مفهوم الجريمة الإلكترونية خطوة أساسية لفهم طبيعتها القانونية وحدود التجريم المقرر بشأنها، وذلك بالنظر إلى حداثة هذه الظاهرة وتعدد صورها. وعليه، سيتم تناول هذا المطلب من خلال بيان تعريف الجريمة الإلكترونية في الفرع الأول، ثم تمييز الجريمة الإلكترونية عن الجرائم التقليدية في الفرع الثاني.

الفرع الأول: تعريف الجريمة الإلكترونية

تعددت التعريفات الفقهية للجريمة الإلكترونية تبعاً لاختلاف المعايير المعتمدة في تحديدها، بين التركيز على محل الاعتداء أو وسيلة ارتكاب الجريمة أو الجمع بينهما. كما تناول المشرع الجزائري هذه الجريمة ضمن مفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهو ما يستدعي بيان مفهومها فقهاً وقانوناً.

أولاً: التعريف الفقهي للجريمة الإلكترونية

لم يستقر الفقه الجنائي على تسمية موحدة للجريمة الإلكترونية، فقد أطلقت عليها تسميات متعددة، من بينها الجريمة المعلوماتية، وجرائم الحاسوب والإنترنت، وجرائم إساءة استخدام تكنولوجيا المعلومات والاتصال.¹ ويرتبط هذا التعدد في التسمية بتعدد الزوايا التي تناول منها الفقه هذه الظاهرة،

¹ محمد أمين الشوابكة، جرائم الحاسوب والإنترنت: الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2007، ص 7.

فهناك من ربط مفهومها بموضوع الاعتداء، في حين ربطه اتجاه آخر بوسيلة ارتكاب الجريمة، بينما اتجه جانب ثالث إلى الجمع بين الوسيلة وموضوع الاعتداء في تعريف واحد.¹

وفي إطار التعريفات التي ركزت على موضوع الجريمة، عرّف خبراء منظمة التعاون والتنمية في الميدان الاقتصادي الجريمة المعلوماتية بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها. ويضيق هذا الاتجاه من نطاق الجريمة الإلكترونية، إذ يجعل النظام المعلوماتي أو البيانات محلاً مباشراً للاعتداء. كما عرّفها الدكتور محمود أحمد عبادة بأنها: «كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية (معطيات الحاسب) يكون ناتجاً بطريقة مباشرة أو غير مباشرة لتدخل التقنية المعلوماتية».²

أما الاتجاه الذي يركز على وسيلة ارتكاب الجريمة، فيتوسع في نطاقها ليشمل مختلف الجرائم التي تستخدم فيها التقنية المعلوماتية وسيلة لتنفيذ السلوك الإجرامي، حتى ولو لم يكن النظام المعلوماتي أو البيانات محلاً مباشراً للاعتداء. ومن هذا المنطلق، ارتبط مفهوم الجريمة الإلكترونية باستخدام الحاسوب وشبكات الاتصال في تنفيذ الفعل المجرّم، الأمر الذي يسمح بإدراج صور متعددة من الجرائم التقليدية متى ارتكبت بواسطة الوسائل الإلكترونية.³

وفي محاولة للجمع بين الاتجاهين، اتجه جانب من الفقه إلى صياغة مفهوم أوسع للجريمة الإلكترونية، يراعي الوسيلة والهدف معاً، ومن التعريفات البارزة في هذا الاتجاه تعريف الدكتور عبد الفتاح بيومي حجازي لها بأنها جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون يمتلكون أدوات المعرفة التقنية، وتوجه للاعتداء على الحق في المعلومات، وتمس معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات.⁴ ويكشف هذا الاتجاه عن خصوصية الجريمة الإلكترونية من خلال الجمع بين البيئة التقنية التي تقع فيها الجريمة والمصلحة التي يستهدفها الاعتداء.

¹ ربيع معزوز، آسيا زروقي، «الجريمة الإلكترونية وإجراءات مواجهتها في التشريع الجزائري»، مجلة القانون والعلوم السياسية، المجلد 7، العدد 2، جامعة الوادي، الجزائر، 2021، ص ص 358-370.

² محمود أحمد عبادة، «الجريمة الإلكترونية: مفهومها وصورها وسبل مكافحتها»، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 15، العدد 1، 2026، ص 256.

³ محمود أحمد عبادة، مرجع نفسه، ص 256.

⁴ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص 33.

وبناءً على ما سبق، فإن تعدد التعريفات الفقهية للجريمة الإلكترونية لا يرجع إلى اختلاف حول عدم مشروعية السلوك، وإنما إلى اختلاف الفقهاء حول المعيار المحدد لنطاقها؛ أهو محل الاعتداء، أم وسيلة ارتكاب الفعل، أم الجمع بينهما. ويبدو أن الاتجاه الجامع أكثر قدرة على الإحاطة بمظاهر الإجرام الإلكتروني، لأنه لا يحصر الجريمة في الاعتداء المباشر على النظام المعلوماتي، ولا يكتفي كذلك بمجرد استخدام الوسيلة الإلكترونية، وإنما يراعي طبيعة البيئة المعلوماتية والمصلحة محل الحماية الجنائية معاً.

ثانياً: التعريف القانوني للجريمة الإلكترونية

لم يضع المشرع الجزائري تعريفاً مستقلاً للجريمة الإلكترونية تحت هذه التسمية، وإنما تناولها ضمن مفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك من خلال القانون رقم 04-09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وقد نصت المادة 2، الفقرة (أ)، منه على أن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي: «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية».¹

ويستفاد من هذا التعريف أن المشرع الجزائري أخذ بالمفهوم الواسع للجريمة الإلكترونية، فلم يحددها في الجرائم التي يكون النظام المعلوماتي أو البيانات محلاً مباشراً للاعتداء، وإنما مد نطاقها إلى كل جريمة أخرى يتم ارتكابها أو تسهيل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية. وبذلك يجمع التعريف التشريعي بين الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات، وبين الجرائم التقليدية التي تستعمل فيها التكنولوجيا الحديثة كوسيلة للارتكاب أو التسهيل.²

¹ القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، 16 غشت سنة 2009، المادة 2، الفقرة (أ).

² المادة 2، الفقرة (أ)، القانون رقم 04-09، سالف الذكر.

كما أحال المشرع الجزائري، في تحديد الجانب الأول من مفهوم الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها في قانون العقوبات، ولا سيما المواد 394 مكرر إلى 394 مكرر 5، التي تجرم أفعال الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات، وإدخال المعطيات أو حذفها أو تعديلها بطريق الغش، إلى جانب صور أخرى من الاعتداء على هذه الأنظمة. ويكشف ذلك عن اعتماد المشرع على حماية جنائية متعددة المستويات للبيئة المعلوماتية، تجمع بين التجريم الموضوعي للأفعال الماسة بالأنظمة والمعطيات، والتنظيم الخاص للوقاية والتحري والمكافحة بموجب القانون رقم 04-09.¹

ويلاحظ كذلك أن المشرع لم يكتفِ باستعمال مصطلح «المنظومة المعلوماتية» وإنما عرّفها في المادة 2، الفقرة (ب)، من القانون رقم 04-09 بأنها «أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين»، كما عرّف «المعطيات المعلوماتية» و«الاتصالات الإلكترونية»، الأمر الذي يسمح بضبط النطاق المادي للأفعال الإجرامية التي تدخل ضمن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.²

وعليه، فإن المفهوم القانوني للجريمة الإلكترونية في التشريع الجزائري يقوم على ثنائية محل الاعتداء ووسيلة ارتكاب الجريمة؛ فهي تشمل من جهة الجرائم التي تمس أنظمة المعالجة الآلية للمعطيات، ومن جهة أخرى الجرائم التي ترتكب أو يسهل ارتكابها باستخدام منظومة معلوماتية أو نظام للاتصالات الإلكترونية. ويمنح هذا التصور نطاقاً واسعاً للحماية الجنائية، بما يسمح باستيعاب التطور المستمر للوسائل والتقنيات المستخدمة في ارتكاب الجرائم الإلكترونية.³

¹ المواد 3 إلى 14، القانون رقم 04-09، سالف الذكر.

² المادة 2، الفقرة (ب)، القانون رقم 04-09، سالف الذكر.

³ عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والجرائم المعلوماتية، الطبعة الأولى، الإسكندرية، مصر، منشأة المعارف، 2009، ص 33-34.

الفرع الثاني: تمييز الجريمة الإلكترونية عن الجريمة التقليدية

تختلف الجريمة الإلكترونية عن الجريمة التقليدية من حيث البيئة التي يتم فيها النشاط الإجرامي والوسائل المعتمدة في تنفيذه، رغم اشتراكهما في خضوعهما للقواعد العامة للتجريم والعقاب من حيث ضرورة توافر أركان الجريمة ومبدأ الشرعية الجنائية. فالجريمة التقليدية تقع غالبًا في العالم المادي وبوسائل محسوسة، في حين ترتبط الجريمة الإلكترونية بالبيئة الرقمية، ويستخدم الجاني فيها الحاسوب أو شبكة الإنترنت أو غيرها من وسائل تكنولوجيايات الإعلام والاتصال، سواء كان النظام المعلوماتي محلاً للاعتداء أو وسيلة لارتكاب الجريمة.¹

وتظهر خصوصية الجريمة الإلكترونية كذلك من خلال محل الاعتداء؛ إذ قد تنصب على أنظمة المعالجة الآلية للمعطيات أو البيانات والمعلومات الإلكترونية، كما قد تستهدف مصالح أخرى كالأموال أو الحياة الخاصة أو السمعة، بينما تنصب الجريمة التقليدية في صورها المعتادة على أموال أو أشخاص أو مصالح مادية بصورة مباشرة.² كما يختلف مرتكب الجريمة في البيئة الإلكترونية، إذ لا يتطلب تنفيذ بعض الأفعال الإجرامية حضوراً مادياً في مكان ارتكابها، وإنما قد يكفي امتلاك المعرفة والمهارات التقنية اللازمة للوصول إلى النظام أو البيانات المستهدفة.³

ويبرز الاختلاف بصورة أوضح في اكتشاف الجريمة وإثباتها، فالجريمة التقليدية قد تترك في الغالب آثاراً مادية يمكن معاينتها وضبطها، كآثار العنف أو أدوات الجريمة أو الأشياء محل الاعتداء، بينما تترك الجريمة الإلكترونية آثاراً رقمية قد تكون غير محسوسة وقابلة للتغيير أو المحو، مما يفرض على سلطات التحقيق التعامل مع أدلة ذات طبيعة تقنية تستلزم وسائل وإجراءات خاصة للمحافظة عليها وضمان سلامتها. وقد أخذ المشرع الجزائري بهذه الخصوصية عندما نظم، بموجب القانون رقم 09-04، إجراءات خاصة تتعلق بالتفتيش والحجز في المنظومات المعلوماتية والبيانات المخزنة فيها، فضلاً عن اللجوء إلى المراقبة الإلكترونية والاعتراض في الحالات التي حددها القانون.⁴

¹ محمد أمين الشوابكة، مرجع سابق، ص 7-8.

² محمد أمين الشوابكة، مرجع نفسه، ص 222-224.

³ عبد الفتاح بيومي حجازي، مرجع سابق، ص 50.

⁴ المواد 3 و5 و6، القانون رقم 09-04، سالف الذكر.

كما تتميز الجريمة الإلكترونية عن الجريمة التقليدية من حيث النطاق المكاني، إذ يمكن أن يتم الفعل الإجرامي في دولة، بينما يوجد النظام المعلوماتي أو البيانات المستهدفة في دولة أخرى، وقد تظهر آثار الجريمة في دولة ثالثة، وهو ما يمنح الجريمة الإلكترونية طابعاً عابراً للحدود ويطرح إشكالات تتعلق بالاختصاص القضائي والتعاون الدولي.¹ وقد أشار المشرع الجزائري إلى هذه الخصوصية ضمن القانون رقم 04-09 من خلال تنظيم التعاون والمساعدة القضائية الدوليين في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.²

وبذلك، فإن الفارق بين الجريمة الإلكترونية والجريمة التقليدية لا يكمن في خروج الأولى عن المبادئ العامة للقانون الجنائي، وإنما في خصوصية الوسيلة والبيئة ومحل الاعتداء وطرق اكتشاف وإثبات الفعل والنطاق المكاني؛ وهي خصوصيات فرضت على المشرع تطوير آليات قانونية وإجرائية تتلاءم مع الطبيعة التقنية لهذا النوع من الإجرام.

المطلب الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بمجموعة من الخصائص التي تفرضها طبيعة البيئة الرقمية والوسائل التقنية المستخدمة في ارتكابها، مما يمنحها خصوصية تميزها عن الجرائم التقليدية. ولبين هذه الخصائص، سيتم التطرق في الفرع الأول إلى الطابع التقني للجريمة الإلكترونية، ثم بيان صعوبة اكتشاف وإثبات الجريمة الإلكترونية في الفرع الثاني، وأخيراً دراسة الطابع العابر للحدود للجريمة الإلكترونية في الفرع الثالث.

الفرع الأول: الطابع التقني للجريمة الإلكترونية

ترتبط الجريمة الإلكترونية ارتباطاً مباشراً بالتطور التقني في مجال تكنولوجيات الإعلام والاتصال، إذ تتطلب في صورتها الأصلية وجود بيئة معلوماتية تسمح بتنفيذ السلوك الإجرامي أو تحقيق نتيجته. وتتمثل هذه البيئة في الحواسيب والأنظمة المعلوماتية وشبكات الاتصال والبرمجيات وقواعد البيانات، مما يجعل التقنية عنصراً محورياً في تكوين هذا النمط من الإجرام. ومن ثم، فإن الجريمة

¹ عبد الفتاح بيومي حجازي، المرجع السابق، ص ص 39-41.

² المادتان 15 و16، من القانون رقم 04-09، سالف الذكر.

الإلكترونية لا تُفهم بمعزل عن الوسائل التقنية التي أوجدت مجالها، إذ يمكن أن يكون النظام المعلوماتي محلاً للاعتداء، كما يمكن أن يستخدم كوسيلة لتنفيذ الاعتداء على مصالح أخرى.¹

ويظهر الطابع التقني كذلك في الوسائل والأساليب التي يعتمد عليها الجاني، حيث يمكن تنفيذ الأفعال الإجرامية باستعمال تقنيات الاختراق، أو البرمجيات الخبيثة، أو التلاعب بالبيانات، أو استغلال الثغرات الأمنية في الأنظمة والشبكات. ويمنح ذلك الجريمة الإلكترونية خصوصية من حيث طبيعة الفاعل، الذي يحتاج في العديد من صورها إلى قدر من المعرفة التقنية التي تمكنه من التعامل مع الأنظمة المعلوماتية وتجاوز وسائل الحماية الموضوعة لها. وقد أشارت الدراسات القانونية المتخصصة إلى أن ارتباط الجريمة المعلوماتية بالتقنية منحها خصائص مادية وإجرائية متميزة عن الجرائم التقليدية، سواء من حيث طريقة ارتكابها أو طبيعة آثارها أو أساليب البحث والتحقيق فيها.²

كما أن الطابع التقني للجريمة الإلكترونية ينعكس على مسرح الجريمة وآثارها؛ فمسرح الجريمة هنا قد يكون نظاماً معلوماتياً أو شبكة إلكترونية، ولا يشترط وجود مكان مادي يجتمع فيه الجاني والجاني عليه. وقد تكون البيانات محل الجريمة مخزنة على أجهزة متعددة أو موزعة عبر شبكة، الأمر الذي يجعل التعامل مع محل الجريمة وإثبات عناصرها مرتبطاً بفهم البنية التقنية للنظام المستهدف. ويتربط على ذلك حاجة جهات التحقيق إلى الاستعانة بالوسائل الفنية والخبرات المتخصصة من أجل تحديد كيفية وقوع الفعل، ومصدره، والبيانات التي تم الوصول إليها أو تغييرها أو حذفها.³

ويؤثر هذا الطابع التقني كذلك في طبيعة الحماية الجنائية التي أقرها المشرع الجزائري، إذ خصّص قانون العقوبات أحكاماً لتجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، كما وضع القانون رقم 04-09 قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو ما يعكس ارتباط التجريم ذاته بالبيئة التقنية التي تقع فيها هذه الأفعال.⁴ وبذلك،

¹ عبد الفتاح المرجع السابق، 2009، ص 27.

² شول بن شهرة، مراد ماشوش، «السمات الخاصة للجريمة المعلوماتية»، مجلة المستقبل للدراسات القانونية والسياسية، المجلد 4، العدد 1، 2020، ص 1-21.

³ عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، الجزائر، النشر الجامعي الجديد، 2021، ص 25-31.

⁴ المواد من 3 إلى 6 السالف الذكر.

فإن التقنية لا تمثل مجرد وسيلة عرضية في الجريمة الإلكترونية، وإنما تشكل عنصراً أساسياً في تحديد طبيعتها وتمييزها عن صور الإجرام التقليدي.

الفرع الثاني: صعوبة اكتشاف وإثبات الجريمة الإلكترونية

تطرح الجريمة الإلكترونية صعوبات خاصة أمام أجهزة البحث والتحري، بالنظر إلى طبيعة البيئة التي تقع فيها والأدوات التقنية التي تستخدم في تنفيذها. فهي لا ترتبط بالضرورة بمسرح مادي محسوس يمكن معاينته بالطرق التقليدية، وإنما قد تتم داخل منظومة معلوماتية أو عبر شبكة اتصال إلكترونية، كما يمكن أن تتم عن بُعد ودون حضور الجاني في المكان الذي تظهر فيه آثارها. ويضاف إلى ذلك إمكانية إخفاء هوية الفاعل باستعمال وسائل تقنية متعددة، الأمر الذي يجعل اكتشاف الجريمة وتحديد مصدر السلوك الإجرامي أكثر تعقيداً من كثير من الجرائم التقليدية.¹

وتزداد صعوبة اكتشاف الجريمة الإلكترونية بسبب ضعف الإبلاغ عنها في بعض الحالات، سواء لعدم اكتشاف الضحية وقوع الاعتداء في حينه، أو خشية المؤسسات والأشخاص من الآثار المترتبة على الكشف عن تعرض أنظمتهم للاختراق. كما أن الجاني يستطيع استغلال المعرفة التقنية لإخفاء آثاره أو تغيير البيانات التي يمكن أن تكشف عن نشاطه، وهو ما يؤدي إلى اتساع الفجوة بين العدد الفعلي للجرائم المرتكبة والجرائم التي تصل إلى علم السلطات المختصة.²

أما من ناحية الإثبات، فإن خصوصية الجريمة الإلكترونية تظهر بصورة أوضح في طبيعة الدليل الذي يمكن الاعتماد عليه، إذ قد لا تترك الجريمة آثاراً مادية تقليدية يمكن إدراكها بالحواس، وإنما تترك آثاراً رقمية داخل الأجهزة أو الأنظمة أو الشبكات. وتتميز هذه الآثار بقابليتها للمحو والتعديل والنسخ والنقل، مما يفرض على المحقق اتخاذ إجراءات فنية وقانونية دقيقة للمحافظة عليها منذ لحظة اكتشافها إلى غاية تقديمها أمام القضاء.³ ولذلك، فإن قيمة الدليل الإلكتروني لا ترتبط بمجرد

¹ عبد الفتاح بيومي حجازي، المرجع السابق، ص 78.

² عبد القادر عميمر، المرجع السابق، ص 25-32.

³ نعيمة بلكاوي، الدليل الإلكتروني في التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، جامعة عمار ثلجي بالأغواط، الجزائر، السنة الجامعية 2024/2025، ص 4

وجوده، وإنما كذلك بسلامة إجراءات الحصول عليه وحفظه وعدم العبث بمضمونه، بما يضمن إمكانية مناقشته وتقييمه قضائياً.

وتتطلب عملية إثبات الجريمة الإلكترونية كذلك معرفة تقنية متخصصة، لأن تحديد كيفية ارتكاب الفعل ومصدره وآثاره قد يتجاوز المعارف القانونية والفنية العادية لجهات التحقيق. ولهذا تبرز أهمية الاستعانة بالخبرة الفنية في فحص الأجهزة والأنظمة والبيانات الرقمية، وتحليل الآثار الإلكترونية المرتبطة بالجريمة. وقد أفرزت هذه الخصوصية حاجة المشرع الجزائري إلى وضع قواعد إجرائية تتلاءم مع طبيعة هذا النوع من الإجرام، إذ أقر القانون رقم 04-09 إجراءات خاصة تتعلق بالتفتيش والحجز في المنظومات المعلوماتية، وجمع البيانات وتسجيلها، فضلاً عن مراقبة الاتصالات الإلكترونية في الحالات والشروط التي حددها القانون.¹

كما تثير طبيعة الدليل الإلكتروني إشكالاً يتعلق بحجيته أمام القضاء، لاسيما من حيث مشروعية الحصول عليه وسلامته ونسبته إلى مرتكب الجريمة. وقد اعترف المشرع الجزائري بالدليل الإلكتروني ضمن منظومة الإثبات، مع إخضاعه للقواعد العامة للإثبات الجنائي والإجراءات القانونية الخاصة التي تتلاءم مع طبيعته التقنية.² ومن ثم، فإن صعوبة إثبات الجريمة الإلكترونية لا ترجع إلى انعدام وسائل الإثبات، وإنما إلى ضرورة الوصول إلى الدليل الرقمي بطريقة مشروعة، والمحافظة على سلامته، وإثبات علاقته بالفعل الإجرامي ومرتكبه، وهي مسائل تتطلب تكامل المعرفة القانونية والتقنية.

وبناءً عليه، فإن خصوصية الجريمة الإلكترونية تفرض تحدياً مزدوجاً على أجهزة العدالة الجنائية؛ يتمثل أولهما في اكتشاف الجريمة وتحديد مرتكبها، بينما يتعلق الثاني بجمع الدليل الإلكتروني والمحافظة عليه وإثبات حجته أمام القضاء، وهو ما يفسر اتجاه التشريع الجزائري إلى استحداث آليات إجرائية تتناسب مع الطبيعة التقنية لهذا النوع من الجرائم.

¹ المواد 3 و5 و6، القانون رقم 04-09، سالف الذكر.

² نعيمة بلكاوي، مرجع سابق، ص 11

الفرع الثالث: الطابع العابر للحدود للجريمة الإلكترونية

تتميز الجريمة الإلكترونية بإمكانية تجاوزها للحدود الإقليمية للدول، نتيجة اعتمادها على شبكات الاتصال الإلكترونية التي تسمح للجاني بتنفيذ الفعل الإجرامي من مكان يوجد فيه، في حين يكون المجني عليه أو النظام المعلوماتي أو البيانات محل الاعتداء في دولة أخرى. وقد تتوزع العناصر المرتبطة بالجريمة بين عدة دول، الأمر الذي يجعل تحديد مكان ارتكابها أكثر تعقيداً مقارنة بالجريمة التقليدية، ويطرح إشكالات قانونية تتعلق بالاختصاص القضائي والقانون الواجب التطبيق.¹

ويظهر الطابع العابر للحدود كذلك في إمكانية ارتكاب الجريمة دون انتقال الجاني بصورة مادية إلى الدولة التي ظهرت فيها النتيجة الإجرامية، إذ تكفيه إمكانية الوصول عن بعد إلى النظام أو الشبكة المستهدفة. وقد يؤدي ذلك إلى وجود أكثر من دولة تملك صلة بالفعل الإجرامي، سواء باعتبارها دولة ارتكاب السلوك، أو الدولة التي تحققت فيها النتيجة، أو الدولة التي يوجد فيها النظام المعلوماتي أو البيانات محل الاعتداء. ومن ثم، فإن القواعد التقليدية للاختصاص الإقليمي قد تواجه صعوبات في تحديد الدولة المختصة بالتحقيق والمتابعة والمحاكمة.²

وتزداد هذه الصعوبة بالنظر إلى أن الأدلة المتعلقة بالجريمة الإلكترونية قد تكون موجودة خارج إقليم الدولة التي تباشر التحقيق، فقد تكون البيانات المخزنة أو الخوادم أو الحسابات الإلكترونية مرتبطة بمقدم خدمة يوجد في دولة أجنبية. ويترتب على ذلك ارتباط عملية البحث عن الأدلة والحصول عليها بحدود السيادة الإقليمية للدول، إذ لا تستطيع سلطات دولة ما ممارسة إجراءات التحقيق داخل إقليم دولة أخرى بصورة مستقلة، مما يجعل التعاون القضائي الدولي ضرورة عملية لمواجهة هذا النوع من الإجرام.³

وقد أدرك المشرع الجزائري هذه الطبيعة العابرة للحدود، فأفرد القانون رقم 09-04 أحكاماً خاصة للتعاون والمساعدة القضائية الدولية في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث أجاز التعاون القضائي الدولي وفقاً للاتفاقيات الدولية ومبدأ المعاملة بالمثل، كما نظم بعض

¹ المواد 15 إلى 17، القانون رقم 09-04، سالف الذكر.

² عبد القادر عميمر، مرجع سابق، ص 25-29.

³ المادة 16، القانون رقم 09-04، سالف الذكر.

صور المساعدة المتعلقة بالحصول على البيانات والمعلومات ذات الصلة بالتحقيقات الجارية.¹ ويعكس ذلك إدراك المشرع لصعوبة مكافحة الجرائم الإلكترونية بالاعتماد على الوسائل الوطنية وحدها، بالنظر إلى إمكانية امتداد عناصر الجريمة وأدلتها إلى خارج الإقليم الجزائري.

كما يرتبط تجاوز الجريمة الإلكترونية للحدود بتعدد صور التعاون الدولي اللازمة لمواجهتها، سواء من خلال تبادل المعلومات، والمساعدة القضائية، وتسليم المجرمين، وتنفيذ الإنابات القضائية، وتبادل الأدلة الإلكترونية، فضلاً عن التنسيق بين أجهزة إنفاذ القانون.² وقد أصبح هذا التعاون أكثر أهمية بسبب سرعة انتقال البيانات الإلكترونية وإمكانية محوها أو تغييرها خلال فترة زمنية قصيرة، الأمر الذي يفرض سرعة الاستجابة بين السلطات المختصة في الدول المعنية.³

وعليه، فإن الطابع العابر للحدود للجريمة الإلكترونية لا يقتصر على إمكانية ارتكابها من دولة وإلحاق آثارها بدولة أخرى، وإنما يمتد إلى توزيع عناصرها وأدلتها وأطرافها عبر أقاليم متعددة، وهو ما يفرض تحديات أمام الاختصاص القضائي الوطني ويجعل التعاون الدولي أحد المتطلبات الأساسية للتحقيق فيها وملاحقة مرتكبيها.

المطلب الثالث: معايير تصنيف الجريمة الإلكترونية

تتعدد صور الجريمة الإلكترونية وتختلف باختلاف المصلحة محل الحماية الجنائية والوسائل التقنية المعتمدة في ارتكابها، الأمر الذي أفرز عدة تصنيفات فقهية لهذه الجرائم. ولتحديد أهم هذه التصنيفات والصور، سيتم التطرق في الفرع الأول إلى تصنيف الجرائم الإلكترونية بحسب محل الاعتداء، ثم بيان تصنيفها بحسب وسيلة ارتكابها في الفرع الثاني.

الفرع الأول: تصنيف الجرائم الإلكترونية بحسب محل الاعتداء

يسمح معيار محل الاعتداء بتقسيم الجرائم الإلكترونية بالنظر إلى المصلحة أو العنصر الذي ينصب عليه السلوك الإجرامي، إذ لا تتجه جميع الأفعال المرتكبة في البيئة الرقمية إلى غرض واحد،

¹ المواد 15 و16 و17، القانون رقم 09-04، سالف الذكر.

² المادتان 16 و17، من نفس القانون

³ عبد القادر عميمر، مرجع سابق، ص 25-29

وإنما قد تستهدف النظام المعلوماتي ذاته، أو البيانات والمعلومات، أو الأموال، أو الأشخاص وحقوقهم. ويأخذ هذا التصنيف أهمية قانونية بالنظر إلى اختلاف المصالح التي تتولى القواعد الجنائية حمايتها، واختلاف الأركان والجزاءات المقررة بحسب طبيعة الاعتداء.

أولاً: الجرائم الماسة بالأنظمة المعلوماتية

وتأتي في مقدمة هذه الجرائم الجرائم الماسة بالأنظمة المعلوماتية، وهي التي ينصب فيها الاعتداء على النظام المعلوماتي ذاته، كالدخول أو البقاء غير المشروع فيه، أو تعطيل عمله، أو إتلاف مكوناته، أو عرقلة تشغيله. وقد أفرد المشرع الجزائري لهذه الأفعال حماية جنائية خاصة ضمن أحكام قانون العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث جرم الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات، كما جرم أفعال إدخال أو حذف أو تعديل المعطيات بطريق الغش.¹

ثانياً: الجرائم الماسة بالبيانات والمعلومات الإلكترونية

وتشمل كذلك الجرائم الماسة بالبيانات والمعلومات الإلكترونية، حيث يكون محل الاعتداء المعطيات المخزنة أو المعالجة أو المنقولة إلكترونياً، سواء تعلق الأمر بإتلافها أو حذفها أو تغييرها أو الحصول عليها دون حق. وتكتسب هذه الفئة أهمية خاصة بالنظر إلى القيمة الاقتصادية والقانونية التي أصبحت تتمتع بها البيانات، إذ يمكن أن تكون محلاً مستقلاً للحماية الجنائية أو وسيلة للوصول إلى مصالح أخرى محمية قانوناً. وقد عرّف المشرع الجزائري «المعطيات المعلوماتية» ضمن القانون رقم 04-09، وأخضع الاعتداءات التي تستهدف الأنظمة والمعطيات لقواعد خاصة تتلاءم مع طبيعتها التقنية.²

¹ المواد 394 مكرر وما يليها، من القانون 06-24 المعدل والمتمم لقانون العقوبات.

² المادة 2، الفقرة (ج)، والمواد 3 إلى 6، القانون رقم 04-09، سالف الذكر.

ثالثا: الجرائم الإلكترونية الماسة بالأشخاص

ومن جهة أخرى، قد يكون الأشخاص محلاً للاعتداء الإلكتروني، وذلك من خلال استخدام الوسائط الرقمية للمساس بحقوقهم ومصالحهم المشروعة، كالحياة الخاصة والسمعة والشرف والاعتبار، أو من خلال التهديد والابتزاز الإلكتروني ونشر المعلومات الشخصية دون ترخيص. ولا تتوقف الحماية في هذه الحالة عند حماية النظام المعلوماتي، وإنما تمتد إلى الحقوق والحريات الفردية التي يمكن أن تتعرض للاعتداء بواسطة الوسائل الإلكترونية.¹

رابعا: الجرائم الماسة بالاموال

كما تستهدف الجريمة الإلكترونية الأموال والمصالح المالية، من خلال استعمال الأنظمة والشبكات الإلكترونية للاستيلاء على الأموال أو الحصول عليها بطرق احتيالية، أو الاعتداء على الحسابات والمعاملات المالية الإلكترونية. وقد أتاح التطور في وسائل الدفع والمعاملات الإلكترونية صورا جديدة للاعتداء على الذمة المالية، مما دفع التشريعات الحديثة إلى إخضاع هذه الأفعال للحماية الجنائية، سواء من خلال النصوص التقليدية التي تتوافر عناصرها في السلوك الإلكتروني أو من خلال النصوص الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.²

خامسا: الجرائم الماسة بالمصلحة العامة وأمن الدولة

كما يمكن أن ينصب الاعتداء على المصلحة العامة وأمن الدولة، متى استعملت الوسائل الإلكترونية لاستهداف مرافق أو أنظمة ذات أهمية حيوية، أو للحصول على معلومات ذات طبيعة حساسة، أو لتعطيل خدمات إلكترونية مرتبطة بمؤسسات الدولة. وتكتسب هذه الصورة خطورة خاصة بسبب ارتباط الأنظمة المعلوماتية بالبنية التحتية والخدمات الأساسية، الأمر الذي يجعل الاعتداء عليها يتجاوز نطاق الضرر الفردي إلى المساس بمصالح جماعية أو وطنية.³

¹ المواد المتعلقة بحماية الحياة الخاصة والشرف والاعتبار، الأمر رقم 66-156، سالف الذكر؛ والقانون رقم 09-04، سالف الذكر.

² المادة 2، القانون رقم 09-04، سالف الذكر؛ والأمر رقم 66-156، سالف الذكر، بحسب طبيعة الفعل المرتكب.

³ المادة 2، والمواد 13 و14، من القانون رقم 09-04، سالف الذكر.

ومن ثم، فإن تصنيف الجرائم الإلكترونية بحسب محل الاعتداء يكشف عن اتساع نطاق الحماية الجنائية في البيئة الرقمية، إذ يمكن أن يكون النظام المعلوماتي أو البيانات أو الأموال أو الأشخاص أو المصلحة العامة محلاً للفعل الإجرامي. ولا يعني اختلاف محل الاعتداء استقلال هذه الفئات بصورة مطلقة، فقد يجمع الفعل الإلكتروني الواحد بين أكثر من مصلحة محل حماية، كأن يؤدي اختراق نظام معلوماتي إلى الاستيلاء على بيانات شخصية ثم استعمالها للاستيلاء على أموال الضحية¹.

الفرع الثاني: تصنيف الجرائم الإلكترونية بحسب وسيلة ارتكابها

يسمح معيار وسيلة ارتكاب الجريمة بتصنيف الجرائم الإلكترونية وفق الأداة أو الوسيط التقني الذي يستعمله الجاني في تنفيذ السلوك الإجرامي، ذلك أن التطور المتواصل في تكنولوجيات الإعلام والاتصال أوجد وسائل متعددة يمكن استغلالها في ارتكاب الأفعال غير المشروعة. وبناءً على هذا المعيار، يمكن التمييز بين الجرائم المرتكبة بواسطة الحاسوب والأنظمة المعلوماتية، والجرائم المرتكبة عبر شبكات الاتصال والإنترنت، فضلاً عن الجرائم التي تستعمل فيها وسائل الاتصال الحديثة كالهاتف الذكي والبريد الإلكتروني والمنصات الرقمية.

أولاً: الجرائم الإلكترونية المرتكبة بواسطة الحاسوب والأنظمة المعلوماتية

وتشمل الفئة الأولى الجرائم المرتكبة بواسطة الحاسوب والأنظمة المعلوماتية، حيث يستخدم الجاني الحاسوب أو نظام المعالجة الآلية للمعطيات كأداة لتنفيذ السلوك الإجرامي، سواء تعلق الأمر بالدخول غير المشروع إلى النظام، أو التلاعب بالبيانات، أو إتلافها، أو تعطيل النظام. وقد نظم المشرع الجزائري هذه الأفعال ضمن الأحكام الخاصة بالمساس بأنظمة المعالجة الآلية للمعطيات، إذ جرم الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات، كما جرم الأفعال التي تؤدي إلى حذف أو تغيير المعطيات أو عرقلة عمل النظام.²

¹ شول بن شهرة، مراد ماشوش، المرجع السابق، ص 1-21.

² المواد 394 مكرر إلى 394 مكرر 5، من القانون 06-24 المعدل والمتمم لقانون العقوبات المعدل والمتمم الأمر رقم 66-156، سالف الذكر.

ثانيا: الجرائم الالكترونية المرتكبة عبر شبكات الإنترنت

أما الفئة الثانية فتتمثل في الجرائم المرتكبة عبر شبكات الإنترنت، حيث توفر الشبكة بيئة تسمح للجاني بالتواصل مع الضحية أو الوصول إلى أنظمة ومعلومات توجد في أماكن مختلفة، ومن صورها الاحتيال الإلكتروني، والاعتداء على المواقع والأنظمة، ونشر المحتويات غير المشروعة، وانتهاك الخصوصية، والتهديد والابتزاز عبر الشبكة. وتتميز هذه الجرائم باتساع نطاقها بالنظر إلى سهولة الوصول إلى الشبكة وإمكانية استعمالها في ارتكاب الفعل من مسافات بعيدة.¹

ثالثا: الجرائم الالكترونية المرتكبة بواسطة البريد الإلكتروني ووسائل الاتصال الرقمية

وتظهر كذلك الجرائم المرتكبة بواسطة البريد الإلكتروني ووسائل الاتصال الرقمية، حيث يستغل الجاني هذه الوسائل في إرسال رسائل احتيالية أو تهديدية، أو انتحال صفة الغير، أو الحصول على بيانات ومعلومات بطريقة تدليسية، أو نشر محتويات تمس بحقوق الأشخاص. وقد أدى انتشار هذه الوسائل إلى انتقال عدد من السلوكيات الإجرامية إلى البيئة الرقمية، مع احتفاظها في بعض الحالات بجوهر الأفعال التقليدية، بينما تختلف وسيلة التنفيذ وطريقة الوصول إلى الضحية.²

رابعا: الجرائم الالكترونية المرتكبة بواسطة الهواتف الذكية والمنصات والتطبيقات الرقمية

وتشمل وسائل ارتكاب الجريمة الإلكترونية أيضاً الهواتف الذكية والمنصات والتطبيقات الرقمية، بالنظر إلى قدرتها على الاتصال بالشبكات وتخزين البيانات وتبادلها، حيث يمكن استخدامها في الوصول غير المشروع إلى الحسابات، أو سرقة البيانات، أو نشر المحتويات غير المشروعة، أو ارتكاب أفعال تمس بالحياة الخاصة للأشخاص. ولا تقتصر الوسيلة في هذه الحالة على الجهاز المادي، وإنما تمتد إلى التطبيقات والمنصات والخدمات الرقمية التي تتيح تنفيذ السلوك الإجرامي أو تسهيله.³

¹ محمد أمين الشوابكة، جرائم الحاسوب والإنترنت: الجريمة المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2007، ص 75 وما بعدها.

² محمد أمين الشوابكة، مرجع سابق، ص 75 وما بعدها.

³ محمد أمين الشوابكة، المرجع السابق، ص 75 وما بعدها.

ويأخذ هذا التصنيف أهمية خاصة من الناحية القانونية، لأن الوسيلة الإلكترونية قد تكون محلاً للجريمة أو أداة لارتكابها أو عنصراً مساعداً في تنفيذها، وهو ما يتفق مع المفهوم الواسع الذي تبناه المشرع الجزائري في القانون رقم 09-04،¹ حين اعتبر من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تلك الجرائم التي ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.² ومن ثم، فإن تحديد وسيلة ارتكاب الجريمة يساعد على فهم طبيعة السلوك الإجرامي وآليات تنفيذه، دون أن يعني ذلك أن كل وسيلة تقنية تشكل في ذاتها جريمة، إذ تبقى الصفة الإجرامية مرتبطة بتوافر نص قانوني يجرم السلوك المرتكب.

وبذلك، فإن تصنيف الجرائم الإلكترونية بحسب وسيلة ارتكابها يكشف عن تعدد الأدوات التقنية التي يمكن أن توظف في النشاط الإجرامي، بدءاً من الحاسوب والأنظمة المعلوماتية، مروراً بالإنترنت والبريد الإلكتروني، وصولاً إلى الهواتف الذكية والمنصات والتطبيقات الرقمية، وهو تعدد يجعل نطاق الجريمة الإلكترونية متطوراً باستمرار تبعاً لتطور الوسائل التكنولوجية ذاتها.³

المبحث الثاني: تنظيم الجرائم الإلكترونية في التشريع الجزائري

أحاط المشرع الجزائري الجريمة الإلكترونية بمجموعة من النصوص القانونية التي تهدف إلى حماية الأنظمة المعلوماتية والأموال والأشخاص من مختلف صور الاعتداء المرتكبة باستعمال تكنولوجيات الإعلام والاتصال. وتتباين هذه الجرائم بحسب المصلحة محل الحماية وطبيعة السلوك الإجرامي، لذلك سيتم تناول جرائم التعدي على الأنظمة الآلية لمعالجة المعطيات في المطلب الأول، ثم دراسة الجرائم الإلكترونية الواقعة على الأموال في المطلب الثاني، وأخيراً بيان جرائم التعدي على الأشخاص في المطلب الثالث.

¹ المادة 2، الفقرة (أ)، القانون رقم 09-04، سالف الذكر.

² المادة 2، الفقرة (أ)، القانون رقم 09-04، سالف الذكر.

³ شول بن شهرة، مراد ماشوش، المرجع السابق، ص 1-21.

المطلب الأول: جرائم التعدي على الأنظمة الآلية لمعالجة المعطيات

أولى المشرع الجزائري حماية جنائية للأنظمة الآلية لمعالجة المعطيات بالنظر إلى ما يمكن أن تتعرض له من أفعال غير مشروعة تمس سريتها أو سلامتها أو حسن سيرها، وقد شملت هذه الحماية صوراً متعددة من الاعتداءات المعلوماتية. وعليه، سيتم تناول جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي في الفرع الأول، ثم دراسة جرائم المساس بسلامة النظام المعلوماتي ومعطياته في الفرع الثاني، وأخيراً التطرق إلى جرائم الاعتداء على البيانات والبرامج المعلوماتية في الفرع الثالث.

الفرع الأول: جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي

أولى المشرع الجزائري حماية جنائية خاصة للأنظمة المعالجة الآلية للمعطيات، وأدرج ضمن القسم السابع مكرر من قانون العقوبات الجرائم الماسة بهذه الأنظمة. وتتصدر هذه الجرائم جريمة الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات، وهي الجريمة التي نصت عليها المادة 394 مكرر من قانون العقوبات. ويستفاد من صياغة النص أن التجريم لا ينصرف إلى الدخول غير المشروع فحسب، وإنما يمتد كذلك إلى حالة البقاء غير المشروع داخل النظام، كما يشمل محاولة ارتكاب الفعل.¹

ويتطلب الركن المادي للجريمة تحقق أحد السلوكين المجرمين، وهما الدخول أو البقاء، في كل أو جزء من منظومة المعالجة الآلية للمعطيات، مع اقترانهما بطابع الغش الذي اشترطه المشرع صراحة. كما لم يشترط النص تحقق ضرر فعلي بالنظام حتى تقوم الجريمة في صورتها الأساسية، إذ يكفي تحقق الدخول أو البقاء عن طريق الغش، أو الشروع في ذلك، بينما رتب المشرع تشديداً للعقوبة عندما يترتب عن الفعل حذف أو تغيير لمعطيات المنظومة.²

ويتمثل الركن المعنوي في القصد الجنائي، إذ يتعين أن تتجه إرادة الجاني إلى الدخول أو البقاء في النظام مع علمه بعدم مشروعية فعله، فضلاً عن عنصر الغش الذي أورده المشرع في نص المادة 394 مكرر. ولا تتوقف المسؤولية على الغرض الذي دفع الجاني إلى ارتكاب الفعل، متى توافرت

¹ الأمر رقم 66-156، المرجع السابق.

² المادة 394 مكرر، الأمر رقم 66-156، سالف الذكر، المعدلة والمتمة بموجب القانون رقم 24-06، سالف الذكر.

العناصر التي يتطلبها النص، بحيث لا يغير من قيام الجريمة كون الباعث هو الفضول أو الرغبة في اختبار القدرة التقنية أو تحقيق منفعة معينة.¹

وقد شدد المشرع الجزائري العقوبة بحسب النتيجة المترتبة عن السلوك الإجرامي. فبعد تعديل قانون العقوبات بموجب القانون رقم 24-06 المؤرخ في 28 أبريل 2024، أصبحت المادة 394 مكرر تقرر بالنسبة للصورة الأساسية الحبس من ستة أشهر إلى سنتين وغرامة من 60.000 إلى 200.000 دج لكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. وتضاعف العقوبة إذا ترتب عن الفعل حذف أو تغيير لمعطيات المنظومة، بينما تصل العقوبة إلى الحبس من سنة إلى ثلاث سنوات وغرامة من 100.000 إلى 300.000 دج إذا ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة.²

وتبرز من خلال هذه الأحكام سياسة المشرع الجزائري في التدرج في التجريم والعقاب، إذ لم يربط الحماية الجنائية بوقوع اعتداء مادي على محتوى النظام فقط، وإنما تدخل منذ مرحلة الولوج أو البقاء غير المشروع، ثم شدد الجزاء كلما تجاوز الاعتداء مجرد الدخول إلى المساس بالمعطيات أو تخريب نظام اشتغال المنظومة. ويعكس ذلك رغبة المشرع في توفير حماية استباقية للأنظمة المعلوماتية بالنظر إلى خطورة إمكانية استغلال الولوج غير المشروع في ارتكاب اعتداءات أشد خطورة.

وبذلك، فإن جريمة الدخول أو البقاء غير المشروع تشكل إحدى الصور الأساسية للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، وتقوم على حماية حرمة النظام المعلوماتي وسلامة المجال المعلوماتي من الولوج غير المشروع، مع تدرج العقوبة تبعاً للنتائج التي تترتب عن هذا السلوك.³

¹ عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، المرجع السابق، ص 33-34.

² المادة 394 مكرر، من الأمر رقم 66-156، المعدل والمتمم.

³ عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، مرجع سابق، ص 33-34.

الفرع الثاني: جرائم المساس بسلامة النظام المعلوماتي ومعطياته

تتطلب الحماية الجنائية للأنظمة الآلية لمعالجة المعطيات عدم الاقتصار على منع الدخول أو البقاء غير المشروع فيها، وإنما تمتد إلى ضمان سلامة النظام والمعطيات التي يحتويها من كل سلوك من شأنه تغييرها أو حذفها أو إدخال بيانات غير صحيحة إليها أو التأثير في طريقة اشتغال النظام. وقد خص المشرع الجزائري هذه الأفعال بأحكام تجرمية مستقلة ضمن قانون العقوبات، بما يعكس أهمية سلامة المعطيات واستقرار النظام المعلوماتي بالنسبة للحماية الجنائية.¹

وتتحقق إحدى صور المساس بسلامة النظام عندما يترتب على الدخول أو البقاء غير المشروع حذف أو تغيير لمعطيات المنظومة. وقد نصت المادة 394 مكرر من قانون العقوبات على مضاعفة العقوبة المقررة لجريمة الدخول أو البقاء عن طريق الغش إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة. كما شدد المشرع الجزاء في حالة ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة، حيث قرر الحبس من سنة إلى ثلاث سنوات والغرامة من 100.000 إلى 300.000 دج.²

وتأخذ الجريمة صورة أكثر استقلالاً عندما يقوم الجاني بإدخال معطيات بطريق الغش في نظام المعالجة الآلية، أو إزالة أو تعديل المعطيات التي يتضمنها، وهي الأفعال التي نصت عليها المادة 394 مكرر 1 من قانون العقوبات. ويستوي في ذلك أن يكون التغيير متعلقاً بإضافة بيانات جديدة إلى النظام أو حذف بيانات موجودة فيه أو تعديل مضمونها، متى وقع السلوك بطريق الغش الذي يتطلبه النص. وقد رفع المشرع، بموجب القانون رقم 06-24، العقوبة المقررة لهذه الأفعال إلى الحبس من سنة إلى ثلاث سنوات والغرامة من 500.000 إلى 2.000.000 دج.³

وتستهدف هذه الحماية سلامة المعطيات من الناحية المادية والمضمونية؛ فإدخال بيانات غير مشروعة أو حذف بيانات صحيحة أو تعديل محتواها يمكن أن يؤدي إلى تغيير النتائج التي ينتجها النظام أو التأثير في القرارات التي تعتمد على المعلومات المعالجة داخله. ومن ثم، فإن الاعتداء لا

¹ المادتان 394 مكرر و394 مكرر 1، الأمر رقم 156-66، سالف الذكر، المعدل والمتمم بموجب القانون رقم 06-24، سالف الذكر.

² المادة 394 مكرر، الأمر رقم 156-66، سالف الذكر، المعدلة والمتممة بموجب القانون رقم 06-24، سالف الذكر.

³ المادة 394 مكرر 1، الأمر رقم 156-66، سالف الذكر، المعدلة والمتممة بموجب القانون رقم 06-24، سالف الذكر.

ينصب بالضرورة على الجهاز أو مكونات النظام المادية، وإنما قد ينصب مباشرة على المحتوى المعلوماتي الذي يقوم النظام بتخزينه أو معالجته. ويتربط على ذلك إمكانية قيام الجريمة بمجرد تحقق السلوك الذي حدده النص، متى توافرت بقية عناصرها القانونية.

كما أن المشرع لم يربط الحماية الجنائية لسلامة النظام المعلوماتي بتحقيق خسارة مالية بصورة مباشرة، إذ إن مجرد المساس بالمعطيات أو بنظام اشتغال المنظومة يمكن أن يشكل محلاً للتجريم متى استوفى الفعل العناصر المنصوص عليها قانوناً. ويكشف ذلك عن انتقال الحماية الجنائية من التركيز على النتيجة المالية أو المادية وحدها إلى حماية الوظيفة المعلوماتية ذاتها، بما في ذلك موثوقية البيانات واستمرارية عمل الأنظمة¹.

وتتضح أهمية هذه الحماية أيضاً بالنظر إلى إمكانية استعمال البيانات المعدلة أو المحذوفة في ارتكاب جرائم أخرى، إذ قد يكون تغيير معلومة داخل النظام خطوة تمهيدية للاستيلاء على أموال أو الحصول على منفعة غير مشروعة أو تعطيل خدمة إلكترونية. ولهذا، فإن تجريم المساس بسلامة المعطيات يؤدي وظيفة وقائية إلى جانب وظيفته العقابية، من خلال التدخل الجنائي لحماية النظام قبل أن يتطور الاعتداء إلى أضرار أكثر جسامة.

وقد عزز المشرع الجزائري هذه الحماية ضمن منظومة قانونية متكاملة، فلم يكتفِ بأحكام قانون العقوبات، بل أقر بموجب القانون رقم 09-04 قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو ما ينسجم مع الطبيعة التقنية لهذه الجرائم والحاجة إلى إجراءات تتلاءم مع طبيعة الأنظمة والبيانات الإلكترونية².

وعليه، فإن جرائم المساس بسلامة النظام المعلوماتي ومعطياته تنصرف أساساً إلى حماية موثوقية البيانات واستقرار النظام واستمرارية عمله، سواء تم الاعتداء من خلال حذف المعطيات أو

¹ عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والجرم المعلوماتي، مرجع سابق، ص 78 وما بعدها.

² المواد 3 إلى 6، من القانون رقم 09-04، سالف الذكر.

تغييرها أو إدخال معطيات بطريق الغش، أو من خلال تخريب نظام اشتغال المنظومة، مع تدرج الحماية والعقوبة بحسب طبيعة الفعل والنتيجة المترتبة عنه¹.

الفرع الثالث: جرائم الاعتداء على البيانات والبرامج المعلوماتية

تكتسب البيانات والبرامج المعلوماتية أهمية متزايدة في البيئة الرقمية، بالنظر إلى اعتماد مختلف الأنشطة الاقتصادية والإدارية والاجتماعية على تخزين المعلومات ومعالجتها بواسطة الأنظمة المعلوماتية. وقد أدى ذلك إلى ظهور صور إجرامية تستهدف البيانات والبرامج بصورة مباشرة، من خلال إتلافها أو حذفها أو تغييرها أو نسخها أو استعمالها دون ترخيص، بما يمكن أن يؤدي إلى تعطيل النظام أو المساس بمصالح أصحاب البيانات والبرامج. ولذلك امتدت الحماية الجنائية في التشريع الجزائري إلى هذه العناصر، سواء من خلال النصوص الخاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو من خلال القواعد المتعلقة بحماية المصنفات والحقوق الفكرية².

وتتمثل إحدى أهم صور الاعتداء على البيانات في حذفها أو تغييرها أو إدخال بيانات جديدة بطريق الغش، وهي الأفعال التي تناولها المشرع الجزائري في المادة 394 مكرر 1 من قانون العقوبات، حيث جرم كل من أدخل بطريق الغش معطيات في نظام للمعالجة الآلية أو أزال أو عدل المعطيات التي يتضمنها. وتقوم هذه الجريمة متى انصب السلوك على المعطيات الموجودة داخل النظام، دون اشتراط أن يؤدي الفعل بالضرورة إلى إتلاف الجهاز أو تعطيل النظام بأكمله³.

وقد يأخذ الاعتداء على البيانات صورة إتلافها أو تعطيل إمكانية الانتفاع بها، بحيث يفقد صاحبها القدرة على الوصول إليها أو استخدامها على النحو المعتاد. وتزداد خطورة هذا السلوك عندما يتعلق الأمر ببيانات ذات قيمة مالية أو إدارية أو شخصية، لأن فقدانها أو العبث بها قد يؤدي إلى أضرار تتجاوز مجرد الضرر التقني. ومن الناحية القانونية، يقتضي التكيف الدقيق للفعل تحديد

¹ المادة 394 مكرر 1، الأمر رقم 66-156، المعدل والمتمم سالف الذكر.

² المادة 2، القانون رقم 09-04، سالف الذكر؛ المواد 4 و 27 وما يليها، الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 44، 23 يوليو سنة 2003.

³ المادة 394 مكرر 1، الأمر رقم 66-156، المعدل والمتمم سالف الذكر.

طبيعة البيانات محل الاعتداء، وطريقة ارتكاب السلوك، والنتيجة التي ترتبت عنه، فضلاً عن توافر القصد الجنائي الذي يتطلبه النص المطبق.

أما البرامج المعلوماتية، فقد حظيت بحماية قانونية خاصة في التشريع الجزائري من خلال قواعد الملكية الفكرية، حيث أدرج المشرع برامج الحاسوب ضمن المصنفات المحمية بموجب الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة. وتترتب على ذلك حماية حقوق صاحب البرنامج من مختلف صور الاستغلال غير المرخص بها، ولا سيما النسخ أو التعديل أو الإتاحة أو الاستغلال خارج الحدود التي يسمح بها القانون.¹

ولا يقتصر الاعتداء على البرامج المعلوماتية على مجرد النسخ غير المشروع، وإنما قد يشمل تحوير البرنامج أو تكييفه أو استغلاله دون إذن صاحبه، متى توافرت الشروط القانونية للحماية. وقد قرر المشرع الجزائري حقوقاً أدبية ومالية للمؤلف، كما أخضع استغلال المصنفات المحمية لشروط وضوابط قانونية، الأمر الذي يوفر أساساً للحماية المدنية والجزائية عند وقوع الاعتداء على الحقوق المرتبطة بالبرامج.²

وتبرز صورة أخرى في الاستيلاء غير المشروع على البيانات أو الحصول عليها دون حق، لاسيما عندما تكون البيانات ذات طبيعة سرية أو شخصية أو اقتصادية. وقد ربط المشرع الجزائري حماية بعض هذه البيانات بأحكام خاصة، من بينها القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الذي وضع قواعد تتعلق بمعالجة البيانات وحمايتها، وأقر جزاءات على بعض الأفعال المخالفة لأحكامه.³

كما يمكن أن تتخذ الاعتداءات على البيانات والبرامج صورة البرمجيات الخبيثة التي يتم إدخالها إلى النظام بقصد إتلاف البيانات أو تعديلها أو تعطيل النظام أو تمكين الجاني من الوصول غير المشروع إليه. ولا تنحصر الخطورة القانونية في الأداة التقنية ذاتها، وإنما في السلوك والنتيجة التي

¹ المادة 4، الفقرة (أ)، الأمر رقم 03-05، سالف الذكر.

² المواد 27 و 41 و 52 و 53، الأمر رقم 03-05، سالف الذكر.

³ القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، 10 يونيو سنة 2018.

تستهدفها، إذ يمكن أن تستخدم البرمجيات الخبيثة كوسيلة لتنفيذ جرائم أخرى تمس سلامة البيانات أو الأنظمة أو الأموال¹.

وتتضح من ذلك الطبيعة المركبة للحماية المقررة للبيانات والبرامج المعلوماتية في التشريع الجزائري؛ فالبيانات قد تحظى بالحماية الجنائية باعتبارها عنصراً من عناصر منظومة المعالجة الآلية للمعطيات، كما قد تخضع لنظام خاص إذا كانت ذات طابع شخصي، بينما تتمتع البرامج المعلوماتية بحماية ضمن نظام حقوق المؤلف، إلى جانب إمكانية استفادتها من الحماية الجنائية عندما تكون محل اعتداء يدخل ضمن الجرائم التي نص عليها قانون العقوبات.²

وعليه، فإن الاعتداء على البيانات والبرامج المعلوماتية يشمل مجموعة من السلوكيات التي تمس سلامة البيانات أو سريتها أو إمكانية الانتفاع بها، أو تنتهك الحقوق المرتبطة بالبرامج المعلوماتية، وهو ما جعل المشرع الجزائري يعتمد أكثر من أساس قانوني لتوفير الحماية اللازمة لهذه العناصر بحسب طبيعتها والصورة التي اتخذها الاعتداء.

المطلب الثاني: الجرائم الإلكترونية الواقعة على الأموال

أدى التوسع في استخدام الوسائل الإلكترونية في المعاملات المالية إلى ظهور صور جديدة من الاعتداء على الأموال، حيث أصبحت التقنيات الرقمية وسيلة لارتكاب أفعال تستهدف الذمة المالية للأشخاص والمؤسسات. وتتعدد هذه الجرائم بحسب الأسلوب المتبع والمصلحة المالية محل الاعتداء، لذلك سيتم تناول الاحتيال الإلكتروني في الفرع الأول، ثم السرقة والاختلاس باستخدام الوسائل الإلكترونية في الفرع الثاني، وأخيراً دراسة جرائم المساس بالمعاملات والأموال الإلكترونية في الفرع الثالث.

الفرع الأول: جريمة الاحتيال الإلكتروني

أفرزت البيئة الإلكترونية صوراً جديدة من الاعتداء على الذمة المالية، من بينها الاحتيال الإلكتروني الذي يقوم على استغلال الوسائل والأنظمة المعلوماتية في تضليل المجني عليه أو التأثير في

¹ المادة 2، القانون رقم 04-09، سالف الذكر؛ والمادة من الأمر رقم 66-156، سالف الذكر، بحسب طبيعة السلوك المرتكب.

² المواد 4 و 27 و 52 و 53، الأمر رقم 03-05، سالف الذكر؛ والمادة رقم 18-07، سالف الذكر.

إرادته بقصد الحصول على منفعة مالية غير مشروعة. ولا تختلف الغاية الإجرامية في هذه الصورة عن الاحتيال في صورته التقليدية، وإنما تكمن خصوصيتها أساساً في الوسيلة الإلكترونية التي يتم من خلالها استعمال أساليب التدليس والوصول إلى الضحية أو إلى أموالها.

ويتحقق الاحتيال الإلكتروني من خلال مجموعة من الأساليب التقنية، من بينها انتحال الهوية الإلكترونية، وإنشاء مواقع أو حسابات وهمية، وإرسال رسائل احتيالية، والاستيلاء على بيانات الدخول إلى الحسابات، والتلاعب بالمعطيات المتعلقة بالمعاملات المالية. وقد يتمكن الجاني من إقناع الضحية بتقديم بياناتها المصرفية أو تحويل أموالها إليه، أو يستعمل البيانات التي حصل عليها دون رضا صاحبها لإجراء معاملات مالية غير مشروعة.¹

ومن الناحية القانونية، يطرح الاحتيال الإلكتروني إشكالية تحديد النص الجنائي الواجب التطبيق، لأن استعمال الوسيلة الإلكترونية لا يؤدي في حد ذاته إلى إنشاء جريمة مستقلة ما لم يوجد نص يجرّم السلوك، وإنما يتم البحث عن التكييف القانوني المناسب للفعل وفق العناصر التي تحققت في الواقعة. فإذا توافرت عناصر جريمة النصب المنصوص عليها في قانون العقوبات، أمكن تطبيق النص الخاص بها، ولو استعمل الجاني وسيلة إلكترونية في تنفيذ الأفعال التدليسية، مع إمكانية انطباق نصوص أخرى متى شكل السلوك في الوقت نفسه اعتداءً على نظام معلوماتي أو بيانات إلكترونية.²

ويقوم الاحتيال الإلكتروني، من حيث الأصل، على ركن مادي يتمثل في استعمال وسيلة تدليسية من شأنها التأثير في إرادة المجني عليه ودفعه إلى القيام بتصرف يؤدي إلى تسليم المال أو تحقيق المنفعة للجاني، وعلى قصد جنائي يتجه إلى استعمال التدليس والاستيلاء على مال الغير. غير أن خصوصية البيئة الإلكترونية قد تجعل الوسيلة التدليسية ذات طبيعة تقنية، كإنشاء منصة إلكترونية وهمية أو إرسال رسالة تنتحل صفة مؤسسة مالية أو شخص آخر، وهو ما يقتضي من جهات التحقيق إثبات العلاقة بين النشاط الإلكتروني والضرر المالي الناتج عنه.

¹ كليلي حسن، الطيب نجمة، «جريمة النصب الإلكتروني من منظور المشرع الجزائري»، مجلة المفكر، المجلد 20، العدد 1، جامعة محمد خيضر بسكرة، الجزائر، 2025، ص 64-84.

² نفسه، ص 64-84.

وقد تتداخل جريمة الاحتيال الإلكتروني مع جرائم أخرى، خصوصاً عندما يحصل الجاني، قبل الاستيلاء على المال، على بيانات الدخول إلى الحساب أو يخترق نظاماً معلوماتياً أو يغير بيانات إلكترونية. ففي هذه الحالة قد تعدد الأوصاف الجنائية بحسب الأفعال المرتكبة وتوافر عناصر كل جريمة، ولا يقتصر الأمر بالضرورة على جريمة الاحتيال وحدها. ويبرز هنا دور التكييف القضائي في تحديد النصوص التي تنطبق على الوقائع، مع احترام مبدأ الشرعية الجنائية المنصوص عليه في التشريع الجزائري¹.

كما تتسم جرائم الاحتيال الإلكتروني بسرعة انتشارها واتساع نطاقها، إذ يستطيع الجاني استهداف عدد كبير من الضحايا في وقت قصير، كما يمكن أن يستعمل حسابات أو مواقع إلكترونية يصعب التحقق من أصحابها الحقيقيين. ويؤدي ذلك إلى زيادة صعوبة تحديد الجاني وتتبع الأموال محل الجريمة، خاصة عندما تمر المعاملة عبر أكثر من نظام أو مؤسسة مالية أو دولة.

وقد دعم المشرع الجزائري حماية المعاملات والأموال في البيئة الرقمية من خلال مجموعة من النصوص، من بينها الأحكام المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فضلاً عن القانون رقم 04-09 الذي وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ويتيح هذا الإطار القانوني التعامل مع الحالات التي يتجاوز فيها السلوك مجرد التدليس المالي إلى الاعتداء على نظام معلوماتي أو بيانات إلكترونية مرتبطة بالمعاملة.²

وعليه، فإن الاحتيال الإلكتروني يمثل صورة من صور الاعتداء على الذمة المالية، تتمثل خصوصيته الأساسية في توظيف الوسائل الإلكترونية في تنفيذ الأساليب التدليسية، مع بقاء التكييف الجنائي مرتبطاً بتوافر العناصر التي يتطلبها النص القانوني المطبق. وقد يؤدي تعدد الأفعال المرتبطة بالواقعة الواحدة إلى قيام جرائم أخرى إلى جانب الاحتيال، بحسب طبيعة النظام أو البيانات أو الأموال التي استهدفها النشاط الإجرامي.³

¹ المادة 1، من الأمر رقم 66-المعدل والمتمم، مرجع سابق، ص 64-84.

² المادة 2، الفقرة (أ)، القانون رقم 09-المادتان 394 مكرر و394 مكرر 1، من الأمر رقم 66-156، المعدل والمتمم سالف الذكر، المعدل والمتمم بالقانون رقم 24-06، سالف الذكر.

³ كليلي حسن، الطيب نجمة، المرجع السابق، ص 64-84.

الفرع الثاني: السرقة والاختلاس باستخدام الوسائل الإلكترونية

أدى الاعتماد المتزايد على الوسائل الإلكترونية في حفظ الأموال وإدارتها وتحويلها إلى ظهور صور من الاعتداء على الذمة المالية تتم باستعمال الأنظمة المعلوماتية وشبكات الاتصال. وقد تتخذ هذه الاعتداءات صورة السرقة عندما يستولي الجاني على مال الغير دون رضاه، أو صورة الاختلاس عندما يكون المال قد عهد به إلى الجاني بحكم وظيفته أو صفته ثم يتجه إلى الاستيلاء عليه أو تبديده. وتكمن خصوصية هذه الأفعال في انتقال وسيلة التنفيذ من الوسائل المادية التقليدية إلى وسائل إلكترونية، مع بقاء التكييف الجنائي مرتبطاً بالعناصر التي حددها القانون لكل جريمة.

وتقوم السرقة في مفهومها الجنائي على اختلاس شيء غير مملوك للجاني، وقد نصت المادة 350 من قانون العقوبات الجزائري على معاقبة كل من اختلس شيئاً غير مملوك له.¹ ويمكن أن تستخدم الوسائل الإلكترونية في تنفيذ الاختلاس، كالوصول بطريقة غير مشروعة إلى حساب إلكتروني أو حساب مصرفي ثم تحويل الأموال الموجودة فيه إلى حساب آخر، أو الاستيلاء على أموال إلكترونية بواسطة بيانات الدخول التي حصل عليها الجاني بطرق غير مشروعة. غير أن استعمال النظام المعلوماتي أو الوسيلة الإلكترونية لا يغير وحده من طبيعة الجريمة، إذ يتعين تحديد ما إذا كان محل الفعل يدخل ضمن مفهوم «الشيء» محل السرقة وفقاً للقواعد الجنائية المطبقة.²

وتطرح السرقة المرتكبة باستعمال الوسائل الإلكترونية إشكالاً فقهيًا وقانونيًا يتعلق بمحل السرقة، خاصة عندما يتعلق الأمر ببيانات أو معلومات لا تتمتع بذات الطبيعة المادية للأموال التقليدية. فالاستيلاء على بيانات مصرفية مثلاً لا يعني بالضرورة الاستيلاء على المال ذاته، وإنما قد يكون وسيلة للوصول إليه أو إجراء تحويل غير مشروع. ومن ثم، ينبغي التمييز بين الاعتداء على البيانات باعتبارها محلاً مستقلاً للحماية، وبين الاستيلاء على المال الذي قد يتحقق باستعمال تلك

¹ المادة 350، الأمر رقم 66-156، سالف الذكر.

² المادة 350، من الأمر رقم 66-156 المعدل والمتمم، سالف الذكر.

البيانات. وقد يؤدي السلوك الواحد، بحسب ظروفه، إلى انطباق أكثر من نص جنائي متى توافرت أركان الجرائم المعنية¹.

أما الاختلاس، فيختلف عن السرقة من حيث صفة الجاني وعلاقته بالمال محل الجريمة. فالمشرع الجزائري نظم جريمة الاختلاس ضمن الجرائم المتعلقة بالفساد، ولا سيما بالنسبة للموظف العمومي أو من في حكمه، عندما يقوم باختلاس أو تبديد أو احتجاز عمدي ودون وجه حق، لصالحه أو لصالح شخص أو كيان آخر، أموالاً أو أوراقاً مالية عمومية أو خاصة أو أشياء أخرى ذات قيمة عهد بها إليه بحكم وظائفه أو بسببها². ويمكن أن تستخدم الوسائل الإلكترونية في تنفيذ الاختلاس، كالتلاعب بالسجلات المحاسبية الإلكترونية، أو تحويل الأموال التي تكون تحت إدارة الجاني بحكم وظيفته إلى حسابات أخرى، أو تغيير البيانات المتعلقة بالعمليات المالية لإخفاء واقعة الاستيلاء³.

وتتضح خصوصية الاختلاس الإلكتروني في إمكانية توظيف النظام المعلوماتي في مرحلتين مختلفتين؛ فقد يكون وسيلة مباشرة لتنفيذ الاستيلاء، وقد يستخدم بعد ارتكاب الفعل لإخفاء آثاره، من خلال تغيير القيود المحاسبية أو حذف البيانات المتعلقة بالمعاملة أو التلاعب بالسجلات الإلكترونية. وفي هذه الحالات، لا تقتصر الحماية الجنائية على المال محل الاختلاس، وإنما قد تمتد إلى سلامة النظام والمعطيات المعلوماتية إذا توافرت العناصر القانونية للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات⁴.

كما يمكن أن ترتبط هذه الجرائم بسرقة أو استعمال وسائل الدفع الإلكترونية بصورة غير مشروعة، خاصة عندما يحصل الجاني على بيانات البطاقة أو الحساب ويستخدمها لإجراء عمليات مالية دون موافقة صاحبها. وقد نظم المشرع الجزائري بعض صور المساس بوسائل الدفع في إطار

¹ المادتان 394 مكرر و 394 مكرر 1، الأمر رقم 66-156، سالف الذكر، المعدل والمتمم بالقانون رقم 24-06، سالف الذكر؛ والمادة 2، الفقرة (أ)، القانون رقم 09-04، سالف الذكر.

² المادة 29، القانون رقم 06-01 المؤرخ في 21 محرم عام 1427 الموافق 20 فبراير سنة 2006، المتعلق بالوقاية من الفساد ومكافحته، المعدل والمتمم.

³ المادة 29، القانون رقم 06-01، سالف الذكر؛ والمادة 394 مكرر 1، الأمر رقم 66-156، سالف الذكر، المعدل والمتمم بالقانون رقم 24-06، سالف الذكر.

⁴ المادتان 394 مكرر و 394 مكرر 1، الأمر رقم 66-156، سالف الذكر، المعدل والمتمم بالقانون رقم 24-06، سالف الذكر؛ والمواد 3 و 5 و 6، القانون رقم 09-04، سالف الذكر.

النصوص الخاصة، كما وفر حماية للمعاملات المالية الإلكترونية من خلال مجموعة من الأحكام المتعلقة بالأنظمة المعلوماتية والمعاملات المصرفية ووسائل الدفع.

وتزداد صعوبة كشف هذه الجرائم وإثباتها عندما تتم العمليات المالية بصورة إلكترونية، لأن عملية الاستيلاء قد لا تترك آثاراً مادية تقليدية، وإنما تظهر في شكل سجلات إلكترونية وبيانات معاملات وآثار رقمية. ولذلك يتطلب إثباتها تحديد العملية المالية محل الاعتداء، وتتبع مسار الأموال، وتحديد الحساب أو الوسيلة الإلكترونية التي استعملت في التنفيذ، وربط النشاط الإلكتروني بالشخص المسؤول عنه، مع احترام القواعد القانونية المتعلقة بجمع الدليل الإلكتروني والمحافظة عليه¹.

ويظهر من ذلك أن استعمال الوسائل الإلكترونية في السرقة والاختلاس لا يؤدي إلى إلغاء الأحكام العامة لهاتين الجريمتين، وإنما يمنح طريقة ارتكابهما خصوصية تقنية. فقد يستخدم الجاني التكنولوجيا للوصول إلى المال أو تحويله أو إخفاء آثار الاستيلاء، بينما يبقى التكييف القانوني رهيناً بطبيعة المال وصفة الجاني وكيفية وقوع الاستيلاء ومدى توافر العناصر التي يشترطها النص الجنائي.

وعليه، فإن السرقة والاختلاس باستخدام الوسائل الإلكترونية يمثلان صورتين من صور الاعتداء على الأموال في البيئة الرقمية، تتداخل فيهما القواعد التقليدية للقانون الجنائي مع الأحكام الخاصة بحماية الأنظمة والبيانات الإلكترونية. ويقتضي تحديد المسؤولية الجنائية في كل حالة الوقوف على طبيعة السلوك المرتكب ومحل الاعتداء وصفة الجاني والوسيلة المستعملة والنتيجة المترتبة عن الفعل.

الفرع الثالث: جرائم المساس بالمعاملات والأموال الإلكترونية

أدى الانتقال المتزايد من المعاملات المالية التقليدية إلى المعاملات الإلكترونية إلى ظهور مصالح مالية جديدة تستوجب الحماية الجنائية، خاصة مع اعتماد المؤسسات والأفراد على الحسابات الإلكترونية ووسائل الدفع الحديثة لإجراء عمليات التحويل والتسديد. وقد أوجد هذا التطور صوراً من السلوكيات الإجرامية التي تستهدف سلامة المعاملات المالية أو وسائل الدفع أو الأموال المتداولة

¹ المواد 3 و5 و6، القانون رقم 04-09، سالف الذكر؛ عبيزة منيرة، بوبكر مصطفى، «الدليل الإلكتروني والسلطة التقديرية للقاضي»، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 3، 2018، ص ص 560-587.

إلكترونيًا، سواء من خلال التلاعب بالبيانات المالية أو استعمال وسائل الدفع دون حق أو إجراء عمليات تحويل غير مشروعة¹.

وتتمثل إحدى أهم صور الاعتداء في الاستعمال غير المشروع لوسائل الدفع الإلكترونية، كاستعمال بطاقة الدفع أو بياناتها دون موافقة صاحبها، أو إجراء عمليات مالية باستعمال بيانات تم الحصول عليها بطرق غير مشروعة. وتزداد خطورة هذه الأفعال عندما يتمكن الجاني من استعمال وسيلة الدفع لإجراء عمليات متكررة أو تحويل مبالغ مالية إلى حسابات أخرى، مما يؤدي إلى إلحاق ضرر مباشر بالذمة المالية لصاحب الحساب أو المؤسسة المالية المعنية².

وقد وضع المشرع الجزائري إطارًا خاصًا لتنظيم وسائل الدفع الإلكترونية، لاسيما من خلال القانون رقم 09-23 المتضمن القانون النقدي والمصرفي، الذي نظم عمليات الدفع ووسائل الدفع والخدمات المرتبطة بها، وأخضع ممارسة النشاط المصرفي والعمليات المالية لضوابط قانونية ورقابية³. وتوفر هذه القواعد أساسًا قانونيًا لحماية الثقة في النظام المصرفي ووسائل الدفع، إلى جانب الأحكام الجزائية التي يمكن تطبيقها على الأفعال غير المشروعة بحسب طبيعتها⁴.

كما يمكن أن ينصب الاعتداء على التحويلات والمعاملات الإلكترونية من خلال إدخال بيانات غير صحيحة أو تغيير البيانات المتعلقة بالمستفيد أو قيمة العملية أو الحساب المراد تحويل الأموال إليه. وقد يستعمل الجاني في ذلك صلاحيات غير مشروعة داخل نظام معلوماتي، أو يستغل بيانات الدخول الخاصة بالضحية، أو يتدخل في عملية الدفع أثناء تنفيذها. وفي هذه الحالة قد تتداخل جريمة المساس بالمال مع الجرائم المتعلقة بالاعتداء على البيانات أو الأنظمة المعلوماتية، بحسب الوسيلة التي اتبعها الجاني لتحقيق النتيجة الإجرامية.

¹ القانون رقم 09-23 المؤرخ في 3 ذي الحجة عام 1444 الموافق 21 يونيو سنة 2023، المتضمن القانون النقدي والمصرفي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 43، 27 يونيو سنة 2023.

² المادة 372، الأمر رقم 66-156، سالف الذكر؛ والقانون رقم 09-23، سالف الذكر.

³ المواد 58 و59 و74، القانون رقم 09-23، سالف الذكر.

⁴ المادة 74، القانون رقم 09-23، سالف الذكر؛ والمادتان 394 مكرر و394 مكرر 1، الأمر رقم 66-156، سالف الذكر، المعدل والمتمم بالقانون رقم 06-24، سالف الذكر.

وتظهر صورة أخرى في التلاعب بالبيانات المصرفية والمحاسبية الإلكترونية، إذ يمكن للجاني تغيير البيانات المتعلقة بالأرصدة أو العمليات المالية أو حذف بعض القيود الإلكترونية بهدف إخفاء عملية تحويل أو إنشاء معاملة وهمية. وتستمد هذه الأفعال خطورتها من أن الأنظمة المصرفية تعتمد على دقة وسلامة البيانات في تحديد الحقوق والالتزامات المالية، وبالتالي فإن تغيير البيانات قد يؤدي إلى نتائج مالية غير مشروعة دون الحاجة إلى التعامل المباشر مع الأموال في صورتها المادية¹.

وقد تتصل هذه الأفعال أيضاً بالاعتداء على أنظمة المعالجة الآلية للمعطيات، خصوصاً عندما يتم الدخول إلى النظام المصرفي أو المالي دون ترخيص، أو تغيير البيانات الموجودة فيه، أو عرقلة سيره. وقد جرم المشرع الجزائري هذه السلوكيات ضمن أحكام قانون العقوبات الخاصة بالمساس بأنظمة المعالجة الآلية للمعطيات، وهو ما يسمح بتوفير حماية جنائية للنظام الذي تتم من خلاله المعاملة إلى جانب الحماية المقررة للمال محل العملية.²

وتأخذ المعاملات الإلكترونية أهمية خاصة من حيث الإثبات، لأن العملية المالية تتم في صورة بيانات إلكترونية يمكن تسجيلها وتخزينها وتبادلها بين عدة أنظمة. ولذلك فإن إثبات الاعتداء عليها يتطلب تحديد مسار العملية الإلكترونية، والتحقق من بيانات الحسابات والأوامر الإلكترونية وسجلات النظام، مع مراعاة القواعد المتعلقة بحجية الدليل الإلكتروني وسلامة إجراءات جمعه وحفظه.

كما يرتبط هذا النوع من الجرائم بالثقة التي تقوم عليها المعاملات المصرفية والمالية، إذ إن مجرد إمكانية التلاعب بالعمليات الإلكترونية أو وسائل الدفع قد تؤثر في ثقة المتعاملين في النظام المالي. ومن هنا تتجه السياسة التشريعية إلى الجمع بين التنظيم القانوني للمعاملات الإلكترونية والحماية الجزائية للمصالح المالية المرتبطة بها، مع إمكانية تطبيق أكثر من نص جنائي عندما يتضمن الفعل الواحد اعتداءً على المال ووسيلة الدفع والنظام المعلوماتي في الوقت نفسه³.

¹ المادة 394 مكرر 1، الأمر رقم 156-66، سالف الذكر، المعدل والمتمم بالقانون رقم 24-06، سالف الذكر؛ والمواد 58 و59 و74، القانون رقم 23-09، سالف الذكر.

² المادتان 394 مكرر و394 مكرر 1، الأمر رقم 156-66، سالف الذكر، المعدل والمتمم بالقانون رقم 24-06، سالف الذكر؛ والمواد 3 و5 و6، القانون رقم 09-04، سالف الذكر.

³ المادة 29، القانون رقم 06-01، سالف الذكر؛ والمادتان 58 و59، القانون رقم 23-09، سالف الذكر.

ويضاف إلى ذلك أن بعض الاعتداءات قد تقع على النقود الإلكترونية أو القيم المالية المخزنة إلكترونياً، من خلال الاستيلاء عليها أو تحويلها أو استعمالها دون حق. غير أن التكييف القانوني لهذه الأفعال يتوقف على طبيعة الأداة المالية محل الاعتداء والنظام القانوني الذي تخضع له، إذ لا يمكن مساواة جميع الأصول أو القيم الرقمية بالمال التقليدي دون التحقق من طبيعتها القانونية ومن النص الذي يوفر لها الحماية الجنائية¹.

وعليه، فإن جرائم المساس بالمعاملات والأموال الإلكترونية تشمل مجموعة من الأفعال التي تستهدف سلامة العمليات المالية ووسائل الدفع والقيم المالية المتداولة إلكترونياً، وقد تتخذ صورة الاستعمال غير المشروع لوسائل الدفع أو التلاعب بالتحويلات والبيانات المصرفية أو الاعتداء على الأنظمة التي تستضيف هذه العمليات. وبظل تحديد المسؤولية الجنائية مرتبطاً بالتكييف الدقيق لكل فعل وبمدى توافر أركان الجريمة المنصوص عليها قانوناً.

المطلب الثالث: الجرائم الإلكترونية الواقعة على الأشخاص

لم يقتصر أثر التطور التكنولوجي على المجال المالي والمعلوماتي، بل امتد إلى الحقوق والحريات المرتبطة بالأشخاص، مما أتاح ظهور أفعال إجرامية تستعمل الوسائط الإلكترونية للمساس بالحياة الخاصة والسمعة والأمن الشخصي. وتختلف هذه الاعتداءات بحسب الحق محل الحماية وطبيعة السلوك المرتكب، لذلك سيتم تناول الاعتداء على الحياة الخاصة والمعطيات الشخصية في الفرع الأول، ثم جرائم التشهير والسب والقذف عبر الوسائط الإلكترونية في الفرع الثاني، وأخيراً دراسة التهديد والابتزاز الإلكتروني في الفرع الثالث.

الفرع الأول: الاعتداء على الحياة الخاصة والمعطيات الشخصية الإلكترونية

أدى الانتشار الواسع لتكنولوجيات الإعلام والاتصال إلى اتساع نطاق تداول المعلومات المتعلقة بالأشخاص وإمكانية تخزينها ومعالجتها ونقلها بسرعة كبيرة، الأمر الذي زاد من احتمالات المساس بالحياة الخاصة والمعطيات الشخصية. وقد أصبح الاعتداء على هذه المعطيات ممكناً من خلال التصوير أو التسجيل أو النشر أو الجمع أو المعالجة أو الاستعمال غير المشروع للمعلومات التي

¹ المادة 74، القانون رقم 09-23، سالف الذكر.

تسمح بالتعرف على الشخص، مما دفع المشرع الجزائري إلى إقرار حماية قانونية خاصة لهذه الحقوق، إلى جانب الحماية المقررة للحياة الخاصة في قانون العقوبات.

وتستند حماية الحياة الخاصة في الجزائر إلى أساس دستوري، حيث نص التعديل الدستوري لسنة 2020 على حماية الحياة الخاصة وحرمة الشرف، كما أقر حماية المعطيات ذات الطابع الشخصي. ويشكل هذا الاعتراف الدستوري أساساً للحماية التشريعية التي جاءت بها النصوص القانونية المتعلقة بالخصوصية والمعطيات الشخصية.¹

وقد خص المشرع الجزائري المعطيات ذات الطابع الشخصي بنظام قانوني مستقل بموجب القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ويهدف هذا القانون إلى وضع قواعد لحماية الأشخاص الطبيعيين أثناء معالجة بياناتهم، وضمان احترام حقوقهم وحرمتهم الأساسية، ولا سيما الحق في الحياة الخاصة والشرف والكرامة.²

ويشترط القانون، كأصل عام، أن تتم معالجة المعطيات ذات الطابع الشخصي في إطار المشروعية والشفافية، وأن تكون المعالجة مرتبطة بأغراض محددة ومشروعة، مع احترام حقوق الشخص المعني. كما نظم المشرع مجموعة من الحقوق المرتبطة بالمعطيات الشخصية، من بينها حق الشخص في الإعلام بحقوقه، وحقه في الوصول إلى بياناته وتصحيحها، وفق الشروط والحدود التي يحددها القانون.³

ويأخذ الاعتداء على المعطيات الشخصية عدة صور، من بينها جمع البيانات أو معالجتها دون احترام الشروط القانونية، أو استعمالها لغرض غير مشروع، أو إفشاؤها أو إتاحتها للغير دون سند قانوني. وتزداد خطورة هذه الأفعال في البيئة الإلكترونية بسبب إمكانية نسخ البيانات وتداولها على نطاق واسع، وصعوبة التحكم في انتشارها بعد خروجها من نطاق صاحبها أو الجهة التي تقوم بمعالجتها.

¹ المادتان 47 و48، المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020، المتعلق بإصدار التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 82، 30 ديسمبر سنة 2020.

² المادة 1، القانون رقم 07-18 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، 10 يونيو سنة 2018.

³ المواد 7 إلى 12، القانون رقم 07-18، سالف الذكر.

وقد أحاط المشرع الجزائري هذه الحماية بجزاءات جنائية، إذ خصص القانون رقم 07-18 مجموعة من الأحكام العقابية للأفعال المخالفة لقواعد معالجة المعطيات ذات الطابع الشخصي. وتختلف العقوبة بحسب طبيعة المخالفة والحق المعتدى عليه والظروف التي ارتكب فيها الفعل، بما يعكس رغبة المشرع في ضمان احترام القواعد المنظمة لمعالجة البيانات الشخصية.¹

أما الحياة الخاصة، فقد حظيت هي الأخرى بحماية جنائية في قانون العقوبات، ولا سيما من خلال تجريم بعض الأفعال التي تنتهك حرمة الحياة الخاصة للأشخاص. ومن صور ذلك التقاط أو تسجيل أو نقل صورة شخص في مكان خاص دون إذنه أو رضاه، أو تسجيل أو نقل محادثات أو أقوال خاصة أو سرية بغير إذن صاحبها، متى توافرت الشروط التي حددها القانون.²

وتبرز خصوصية الاعتداء الإلكتروني على الحياة الخاصة في إمكانية استعمال الوسائل الرقمية في تسجيل أو تخزين أو نشر المعلومات والصور والمحادثات الخاصة، بحيث لا ينتهي الضرر بمجرد وقوع فعل التسجيل أو الحصول على البيانات، وإنما يمكن أن يتسع نطاقه نتيجة إعادة نشر المحتوى أو تداوله عبر الشبكات والمنصات الإلكترونية. ولذلك قد تشكل الوسيلة الإلكترونية عنصراً يزيد من انتشار الضرر وآثاره، دون أن يعني ذلك بالضرورة إنشاء وصف جنائي مستقل لكل فعل، إذ يتوقف التكييف على النص القانوني الذي تتوافر عناصره.³

كما يمكن أن يرتبط الاعتداء على الحياة الخاصة والمعطيات الشخصية بجرائم أخرى، خصوصاً عندما يتم الحصول على البيانات من خلال الدخول غير المشروع إلى نظام معلوماتي أو سرقة حساب إلكتروني أو استعمال وسائل احتيالية للوصول إلى المعلومات. ففي هذه الحالة قد تعدد الأوصاف القانونية بحسب الأفعال التي ارتكبها الجاني والنتائج التي ترتبت عنها، بما يسمح بتطبيق النصوص الخاصة بحماية الأنظمة المعلوماتية إلى جانب النصوص المتعلقة بحماية الخصوصية والمعطيات الشخصية، متى استوفت كل جريمة عناصرها القانونية.

¹ المواد 54 إلى 62، القانون رقم 07-18، سالف الذكر.

² المادة 303 مكرر، الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم.

³ المادة 303 مكرر، الأمر رقم 66-156، سالف الذكر؛ والمادة 2، القانون رقم 07-18، سالف الذكر.

وتكتسب المعطيات الشخصية أهمية إضافية عندما تكون متعلقة بمعلومات حساسة يمكن أن يؤدي كشفها أو استعمالها بطريقة غير مشروعة إلى إلحاق أضرار مادية أو معنوية بالشخص المعني. ولهذا لم يكتف المشرع بتنظيم جمع البيانات وتخزينها، وإنما وضع ضوابط لمعالجتها وتداولها، وربط مشروعية هذه العمليات باحترام الحقوق والحريات التي يحميها القانون¹.

وعليه، فإن الحماية الجنائية للحياة الخاصة والمعطيات الشخصية في التشريع الجزائري تقوم على تكامل النصوص الدستورية والجزائية والقانون الخاص بحماية المعطيات ذات الطابع الشخصي، بما يسمح بمواجهة صور متعددة من الاعتداءات التي يمكن أن تقع باستعمال الوسائل الإلكترونية. وتزداد أهمية هذه الحماية في البيئة الرقمية بالنظر إلى سرعة تداول البيانات وإمكانية نسخها ونشرها على نطاق واسع، وهو ما يجعل المساس بالخصوصية أكثر قابلية للانتشار واستمرار آثاره.

الفرع الثاني: جرائم التشهير والسب والقذف عبر الوسائط الإلكترونية

أدى انتشار شبكات التواصل الاجتماعي والمواقع الإلكترونية وتطبيقات الاتصال الفوري إلى توفير فضاء واسع للتعبير وتبادل المعلومات، غير أن هذه الوسائل أصبحت في الوقت نفسه مجالا لارتكاب أفعال تمس شرف الأشخاص واعتبارهم، من خلال نشر عبارات أو ادعاءات أو صور من شأنها الإساءة إليهم أمام الغير. وتتمثل أبرز هذه الصور في القذف والسب والتشهير المرتكب بواسطة الوسائط الإلكترونية، حيث تتميز هذه الأفعال بسرعة انتشار المحتوى وإمكانية وصوله إلى عدد كبير من الأشخاص، فضلا عن إمكانية الاحتفاظ به وإعادة نشره.

ويقوم القذف، وفقا للمادة 296 من قانون العقوبات الجزائري، على إسناد فعل علنا إلى شخص أو هيئة يكون من شأنه المساس بشرف أو اعتبار المجني عليه أو الهيئة التي أسند إليها الفعل. ويتطلب قيام هذه الجريمة وجود إسناد لفعل معين إلى شخص محدد، بحيث يمكن التحقق من ذلك الفعل أو مناقشته، وأن يكون من شأن هذا الإسناد المساس بالشرف أو الاعتبار². ولا تختلف طبيعة الفعل المسند باختلاف الوسيلة المستعملة، إذ يمكن أن يتم الإسناد بواسطة منشور إلكتروني أو رسالة

¹ المواد 4 إلى 12، القانون رقم 18-07، سالف الذكر.

² المادة 296، الأمر رقم 66-156، سالف الذكر.

أو تسجيل أو تعليق منشور على إحدى المنصات الرقمية، متى استوفت الواقعة العناصر التي يتطلبها النص.

أما السب، فقد عرفه المشرع الجزائري في المادة 297 من قانون العقوبات بأنه كل تعبير مشين أو عبارة تتضمن تحقيراً أو قدحاً لا ينطوي على إسناد واقعة معينة.¹ وبذلك يتمثل الفرق الأساسي بين القذف والسب في أن القذف يقوم على إسناد واقعة محددة إلى المجني عليه، بينما ينصرف السب إلى استعمال عبارات مهينة أو حاطة من الكرامة دون إسناد واقعة معينة. ويمكن أن ترتكب الصورتان عبر الوسائط الإلكترونية، سواء من خلال المنشورات أو التعليقات أو الرسائل أو غيرها من وسائل الاتصال الرقمي.²

وتتخذ جريمة التشهير الإلكتروني صوراً متعددة، من بينها نشر ادعاءات تمس سمعة شخص معين، أو تداول معلومات أو صور أو مقاطع إلكترونية بقصد الإساءة إليه، أو إعادة نشر محتوى يتضمن عبارات أو ادعاءات من شأنها النيل من شرفه واعتباره. غير أن وصف الفعل بأنه «تشهير» لا يكفي وحده لتحديد التكييف القانوني، إذ يتعين الرجوع إلى العناصر التي يحددها النص الجنائي لمعرفة ما إذا كان السلوك يشكل قذفاً أو سباً أو جريمة أخرى مستقلة بحسب طبيعة المحتوى والظروف التي تم فيها النشر.

وتظهر خصوصية هذه الجرائم عند ارتكابها علانية عبر الإنترنت، إذ يمكن للعبارة أو الصورة أو المنشور أن يصل إلى عدد كبير من الأشخاص خلال فترة قصيرة، كما يمكن إعادة نشره من طرف مستخدمين آخرين، مما يؤدي إلى توسيع دائرة انتشار الاعتداء. ولهذا تكتسب العلانية أهمية خاصة في الجرائم المرتكبة بواسطة الوسائط الإلكترونية، ويصبح تحديد طبيعة الوسيط وطريقة النشر ومدى إتاحتها للغير من المسائل التي ينبغي التحقق منها عند تحديد المسؤولية الجنائية.

كما أن البيئة الإلكترونية تثير إشكالات مرتبطة بتحديد هوية مرتكب الفعل، خصوصاً عند استخدام حسابات وهمية أو أسماء مستعارة، الأمر الذي يستدعي اللجوء إلى الوسائل التقنية والقانونية لتحديد مصدر المحتوى وربطه بالشخص المسؤول عنه. وقد نظم المشرع الجزائري في القانون

¹ المادة 297، الأمر رقم 66-156، سالف الذكر.

² المادتان 296 و 297، الأمر رقم 66-156، سالف الذكر.

رقم 04-09 بعض الإجراءات الخاصة بالتحري والتحقق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما يسمح للجهات المختصة باتخاذ إجراءات تتلاءم مع الطبيعة التقنية لهذه الجرائم.¹

ولا تقتصر آثار القذف والسب الإلكتروني على الضرر المعنوي المباشر، فقد يؤدي نشر المحتوى المسيء إلى الإضرار بالحياة المهنية أو الاجتماعية للمجني عليه، خاصة إذا كان المحتوى متاحاً للجمهور وقابلاً للتداول وإعادة النشر. كما أن بقاء المنشور أو التسجيل في البيئة الرقمية لفترة طويلة قد يؤدي إلى استمرار آثاره بعد وقوع الفعل الأصلي، وهو ما يمنح هذه الجرائم خصوصية من حيث نطاق الضرر مقارنة ببعض صور الاعتداء التقليدية.

وقد أحاط المشرع الجزائري هذه الأفعال بجرائم جنائية ضمن قانون العقوبات، مع اختلاف العقوبة بحسب طبيعة المجني عليه وصفته والظروف المرتبطة بالفعل. كما يمكن أن تخضع بعض الوقائع لنصوص قانونية أخرى عندما يتجاوز السلوك مجرد المساس بالشرف والاعتبار إلى انتهاك الحياة الخاصة أو التهديد أو الابتزاز أو نشر معطيات شخصية دون سند قانوني.²

ويستفاد من ذلك أن استعمال الوسائط الإلكترونية لا يزيل الطبيعة التقليدية لجرمي القذف والسب من حيث عناصرهما القانونية الأساسية، وإنما يوفر وسيلة تقنية جديدة لارتكابهما ويمنحهما قدرة أكبر على الانتشار. ومن ثم، فإن تحديد المسؤولية الجنائية يقتضي الجمع بين القواعد الموضوعية التي تحدد أركان القذف والسب، والقواعد الإجرائية التي تسمح بإثبات الفعل الإلكتروني وتحديد مرتكبه.

وعليه، فإن جرائم التشهير والسب والقذف عبر الوسائط الإلكترونية تمثل اعتداءً على شرف الأشخاص واعتبارهم باستعمال أدوات الاتصال الرقمية، وتتميز عن صورها التقليدية باتساع نطاق

¹ المواد 3 و5 و6، القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، 16 غشت سنة 2009.

² المادتان 296 و297، الأمر رقم 66-156، سالف الذكر؛ والمادة 303 مكرر، الأمر نفسه؛ والمواد 54 إلى 62، القانون رقم 07-18، سالف الذكر.

النشر وسرعة الانتشار وإمكانية إعادة تداول المحتوى، مما يفرض على القضاء والجهات المكلفة بالتحقيق مراعاة الخصائص التقنية للوسيط الإلكتروني عند إثبات الجريمة وتحديد المسؤولية عنها¹.

الفرع الثالث: التهديد والابتزاز الإلكتروني

أصبحت الوسائط الإلكترونية مجالاً لظهور صور متعددة من الاعتداء على الأشخاص، من بينها التهديد والابتزاز الإلكتروني، حيث يستغل الجاني وسائل الاتصال الرقمية للتأثير في إرادة الضحية وإجبارها على القيام بفعل أو الامتناع عنه، أو للحصول منها على منفعة مادية أو معنوية. وتزداد خطورة هذه الأفعال بالنظر إلى سهولة إخفاء هوية مرتكبها، وسرعة انتقال الرسائل والمحتويات الرقمية، وإمكانية استعمال الصور والمعلومات الخاصة كوسيلة للضغط على الضحية.

يقوم التهديد في مفهومه الجنائي على توجيه وعيد إلى شخص بإلحاق أذى به أو بغيره، وفق الصور والشروط التي حددها قانون العقوبات. وقد تناول المشرع الجزائري جرائم التهديد ضمن أحكام قانون العقوبات، وربط التجريم بطبيعة التهديد والوسيلة المستعملة والغاية التي يستهدفها، مع اختلاف العقوبة بحسب صورة الفعل وظروف ارتكابه.² ويمكن أن يتم التهديد بواسطة الوسائل الإلكترونية من خلال الرسائل النصية أو البريد الإلكتروني أو الحسابات الموجودة على شبكات التواصل الاجتماعي أو التسجيلات الصوتية والمرئية، متى توافرت العناصر القانونية للجريمة.

ويختلف الابتزاز الإلكتروني عن التهديد من حيث الغاية التي يستهدفها الجاني؛ إذ يقوم الابتزاز في الغالب على استعمال التهديد أو الضغط لحمل الضحية على تقديم مال أو منفعة أو القيام بفعل معين أو الامتناع عنه، وقد يستند الجاني إلى حيازة صور أو تسجيلات أو معلومات خاصة بالضحية واستخدامها وسيلة للضغط عليها. وبالتالي، قد يشكل التهديد إحدى الوسائل التي يعتمد عليها الجاني لتحقيق الابتزاز، في حين يكون الحصول على منفعة أو تحقيق غرض معين هو الهدف الذي يتجه إليه السلوك الابتزازي.³

¹ المواد 296 و 297 و 303 مكرر، الأمر رقم 156-66، سالف الذكر؛ والمواد 3 و 5 و 6، القانون رقم 09-04، سالف الذكر.

² المواد 284 إلى 287، الأمر رقم 156-66، سالف الذكر.

³ المواد 284 إلى 287، الأمر رقم 156-66، سالف الذكر؛ والمادة 371، الأمر نفسه، بحسب طبيعة الواقعة والغاية من التهديد.

وقد نظم المشرع الجزائري بعض صور الابتزاز ضمن النصوص العامة لقانون العقوبات، كما أقر حماية خاصة لبعض الأفعال التي تقع باستعمال تكنولوجيايات الإعلام والاتصال. ويخضع التكييف القانوني للوقائع إلى طبيعة السلوك المرتكب، فقد تتوافر في الواقعة عناصر جريمة التهديد، أو محاولة الحصول على المال عن طريق التهديد، أو جريمة أخرى متى كان المحتوى المستعمل في الابتزاز متعلقاً بالحياة الخاصة أو المعطيات الشخصية¹

وتأخذ الصور والتسجيلات والمعلومات الخاصة أهمية كبيرة في جرائم الابتزاز الإلكتروني، إذ قد يحصل الجاني عليها بطرق مختلفة، كسرقة الهاتف أو اختراق حساب إلكتروني أو الحصول عليها من الضحية مباشرة، ثم يهدد بنشرها أو إرسالها إلى أفراد عائلتها أو زملائها أو نشرها على منصات التواصل الاجتماعي. وفي هذه الحالة قد يتجاوز الاعتداء مجرد الضغط النفسي إلى المساس بالحقوق في الحياة الخاصة، مما يفتح المجال لتطبيق النصوص الجزائية التي تحمي الخصوصية، متى توافرت شروطها.

كما يمكن أن يقع الابتزاز بهدف الحصول على مبالغ مالية، بحيث يطالب الجاني الضحية بتحويل مبلغ معين مقابل الامتناع عن نشر الصور أو المعلومات أو التسجيلات التي بحوزته. وقد يتم تحويل الأموال عبر الحسابات البنكية أو وسائل الدفع الإلكترونية أو غيرها من الوسائل الرقمية، وهو ما قد يؤدي إلى تداخل الابتزاز مع جرائم أخرى تمس الأموال أو أنظمة الدفع أو المعالجة الآلية للمعطيات، بحسب الطريقة التي اتبعها الجاني².

وتتسم جرائم التهديد والابتزاز الإلكتروني بخصوصية واضحة من ناحية الإثبات الجنائي، لأن الدليل غالباً ما يكون ذا طبيعة رقمية، مثل الرسائل والمحادثات والتسجيلات والصور وبيانات الحسابات وسجلات الاتصال. ولذلك فإن إثبات الجريمة لا يقتصر على تقديم محتوى الرسالة أو المنشور، بل يتطلب، عند المنازعة في نسبته، التحقق من مصدره وسلامة الدليل وربطه بالشخص المشتبه فيه، مع احترام الإجراءات القانونية الخاصة بجمع الأدلة الإلكترونية وحفظها.

¹ المواد 284 إلى 287 و 371، الأمر رقم 66-156، سالف الذكر؛ والمادة 303 مكرر، الأمر نفسه، متى تعلق الفعل بانتهاك الحياة الخاصة.

² المواد 284 إلى 287 و 371، الأمر رقم 66-156، سالف الذكر؛ والمادتان 394 مكرر و 394 مكرر 1، الأمر نفسه، المعدل والمتمم بالقانون رقم 24-06 المؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 30، 30 أبريل سنة 2024.

وتزداد خطورة الابتزاز الإلكتروني عندما يستهدف أشخاصًا في وضعية تجعلهم أكثر عرضة للضغط، أو عندما يتعلق المحتوى المستعمل في التهديد بمعلومات شديدة الخصوصية. كما أن قابلية المحتوى الرقمي للنسخ وإعادة النشر تجعل مجرد تنفيذ التهديد بالنشر قادرًا على إحداث أضرار واسعة وسريعة، وهو ما يبرر أهمية التدخل القانوني لحماية الضحية وملاحقة مرتكب الفعل.

وقد عزز المشرع الجزائري الحماية الإجرائية في هذا المجال من خلال القانون رقم 04-09، الذي أقر قواعد خاصة للتحري والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما يسمح باتخاذ إجراءات تتناسب مع طبيعة الأدلة الرقمية ووسائل ارتكاب هذه الجرائم.¹ وتكتسب هذه الإجراءات أهمية خاصة في جرائم التهديد والابتزاز الإلكتروني، بالنظر إلى إمكانية حذف الرسائل أو تغيير الحسابات أو إخفاء آثار الاتصال.

ومن ثم، فإن التهديد والابتزاز الإلكتروني يمثلان صورتين من صور الاعتداء على الأشخاص باستعمال الوسائط الرقمية، ويتميزان بقدرة الجاني على ممارسة الضغط على الضحية عن بعد، مع إمكانية إخفاء هويته وتوسيع نطاق الضرر الناتج عن الفعل. ويظل تحديد المسؤولية الجنائية مرتبطًا بتوافر العناصر التي يتطلبها النص القانوني، وبإثبات الصلة بين الجاني والوسيلة الإلكترونية المستعملة في ارتكاب الفعل.²

¹ المواد 3 و5 و6، القانون رقم 04-09، سالف الذكر.

² المواد 284 إلى 287، الأمر رقم 66-156، سالف الذكر؛ والمواد 3 و5 و6، القانون رقم 04-09، سالف الذكر.

الفصل الثاني: تدابير وآليات مكافحة الجريمة الالكترونية في التشريع الجزائري

أفرز التطور المتسارع لتكنولوجيات الإعلام والاتصال تحديات قانونية متزايدة فرضت على المشرع الجزائري تطوير آليات الحماية لمواجهة الأفعال الإجرامية المرتكبة في البيئة الإلكترونية. ولم تقتصر هذه الحماية على التجريم والعقاب، وإنما امتدت إلى حماية المصالح والحقوق المرتبطة بالنظام المعلوماتي، بما فيها برامج الحاسوب والمصنفات الرقمية وقواعد البيانات، إلى جانب تجريم الاعتداءات الواقعة على الأنظمة والمعطيات المعلوماتية، ووضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن هذا المنطلق، يتناول المبحث الأول الحماية الموضوعية للنظام المعلوماتي من خلال أحكام الملكية الفكرية، وقانون العقوبات، والقانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ولا تكتمل مواجهة الجريمة الإلكترونية بمجرد تحديد الأفعال المجرّمة والعقوبات المقررة لها، وإنما تتطلب كذلك آليات جزائية وإجرائية تراعي خصوصية هذا النوع من الجرائم وطبيعة الأدلة الناتجة عنها. لذلك يتناول المبحث الثاني الجزاءات المقررة للجرائم الإلكترونية، سواء تعلق الأمر بالعقوبات الأصلية أو التكميلية والظروف المؤثرة فيها، ثم يبرز الخصوصية الإجرائية من خلال إجراءات البحث والتحري والتفتيش وضبط الأدلة الإلكترونية، وصولاً إلى دراسة حجية الدليل الإلكتروني وضوابط الحفاظ عليه، بما يسمح بتحقيق فعالية المكافحة مع احترام الضمانات القانونية المقررة للأشخاص.

المبحث الأول: الحماية الموضوعية للنظام المعلوماتي

تتطلب مكافحة الجريمة الإلكترونية إقرار حماية موضوعية تمتد إلى مختلف المصالح القانونية التي يمكن أن تستهدفها الأفعال المرتكبة في البيئة الرقمية، سواء تعلق الأمر بالأنظمة المعلوماتية أو البيانات أو البرامج والمصنفات الرقمية. وقد اعتمد المشرع الجزائري في هذا المجال على مجموعة من النصوص القانونية التي تتكامل فيما بينها، من خلال حماية برامج الحاسوب وقواعد البيانات في إطار الملكية الفكرية، وتجريم الاعتداءات الماسة بالأنظمة والمعطيات المعلوماتية ضمن قانون العقوبات، إلى جانب وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن ثم، سيتم تناول هذه الحماية من خلال ثلاثة مطالب، يخصص أولها لحماية النظام المعلوماتي في نصوص الملكية الفكرية، وثانيها لحماية النظام المعلوماتي في قانون العقوبات، وثالثها للحماية التي أقرها قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للنظام المعلوماتي

المطلب الأول: حماية النظام المعلوماتي في نصوص الملكية الفكرية

أصبحت الحماية القانونية للمصنفات الفكرية في البيئة الرقمية تقتضي مواجهة الاعتداءات التي يمكن أن تلحق ببرامج الحاسوب والمصنفات الرقمية وقواعد البيانات، خاصة مع سهولة نسخها واستغلالها وتداولها عبر الوسائط الإلكترونية. وقد وفر المشرع الجزائري حماية لهذه المصنفات من خلال أحكام الملكية الفكرية، بما يكفل حماية الحقوق الأدبية والمالية لأصحابها. وعليه، سيتم تناول حماية برامج الحاسوب في إطار حقوق المؤلف في الفرع الأول، ثم حماية المصنفات الرقمية وقواعد البيانات في الفرع الثاني، وأخيرًا بيان صور الاعتداء على حقوق الملكية الفكرية في البيئة الإلكترونية في الفرع الثالث.

الفرع الأول: حماية برامج الحاسوب في إطار حقوق المؤلف

أدى ظهور برامج الحاسوب وتطور استخدامها في مختلف المجالات إلى طرح مسألة تحديد النظام القانوني الملائم لحمايتها، باعتبارها نتاجًا فكريًا يجمع بين الطابع التقني والطابع الإبداعي. وقد

اتجه المشرع الجزائري إلى إخضاع برامج الحاسوب لنظام حقوق المؤلف¹، حيث أدرجها صراحة ضمن المصنفات الأدبية والفنية المحمية بموجب الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة. ويترتب على ذلك تمتع صاحب البرنامج بالحماية القانونية متى توافرت فيه شروط الحماية المقررة للمصنفات الفكرية.²

وقد نصت المادة 3 من الأمر رقم 03-05 على منح صاحب كل إبداع أصلي لمصنف أدبي أو فني الحقوق المنصوص عليها في الأمر³، كما أدرجت المادة 4 من القانون نفسه برامج الحاسوب ضمن المصنفات الأدبية والفنية المحمية. ويكشف هذا الاتجاه عن إرادة المشرع في توفير حماية قانونية للبرنامج المعلوماتي باعتباره إنتاجاً فكرياً، دون أن تكون طبيعة الوسيط الذي يثبت عليه البرنامج أو طريقة التعبير عنه مانعاً من تمتعه بالحماية.⁴

وتقوم حماية برنامج الحاسوب على توافر عنصر الأصالة، باعتبارها من الأسس التي تقوم عليها حماية المصنفات بموجب حقوق المؤلف. ولا تمتد الحماية إلى الأفكار والمبادئ والمناهج والتقنيات وإجراءات العمل في حد ذاتها، وإنما تنصرف إلى الشكل الذي تم فيه التعبير عن الإبداع وتنظيمه. وقد أكد المشرع الجزائري هذا المبدأ في المادة 7 من الأمر رقم 03-05، عندما استبعد من نطاق الحماية الأفكار والمفاهيم والمبادئ والمناهج والتقنيات وطرق العمل المرتبطة بالإبداع الفكري في ذاتها.⁵

وتشمل الحماية المقررة لبرامج الحاسوب الحقوق الأدبية والحقوق المالية للمؤلف. فالحق الأدبي يرتبط بشخصية المؤلف وبصلته بالمصنف، في حين تخول الحقوق المالية لصاحبها إمكانية استغلال البرنامج والاستفادة من العائد الناتج عنه. وقد منح المشرع للمؤلف، في إطار الحقوق المالية، سلطة

¹ الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 44، 23 يوليو سنة 2003، المادة 4، الفقرة (أ).

² المادة 3، الأمر رقم 03-05، سالف الذكر.

³ المادة 3، الأمر رقم 03-05، سالف الذكر.

⁴ المادة 4، الفقرة (أ)، الأمر رقم 03-05، سالف الذكر.

⁵ المادة 7، الأمر رقم 03-05، سالف الذكر.

استغلال مصنفه بأي شكل والحصول على العائد المالي الناتج عنه، كما خوله حق الترخيص للغير باستغلال المصنف وفقاً للشروط القانونية.¹

وتتجسد أهمية الحقوق المالية بالنسبة لبرامج الحاسوب في أن البرنامج يمكن نسخه وتوزيعه وتأجيريه واستغلاله تجارياً بسهولة، ولذلك منح المشرع صاحب الحق سلطة التحكم في عمليات الاستغلال التي تقع على البرنامج. وقد أقر الأمر رقم 03-05 للمؤلف الحق الاستثنائي في استنساخ مصنفه بأي وسيلة كانت، كما نص بصورة خاصة على التداول العمومي للمصنفات السمعية البصرية وبرامج الحاسوب عن طريق الإيجار التجاري.²

ولم يجعل المشرع حماية برنامج الحاسوب مطلقة، وإنما أقر بعض الاستثناءات المحددة قانوناً التي تراعي مصلحة مستعمل البرنامج. ومن أبرزها ما نصت عليه المادة 52، التي تسمح للحائز الشرعي لبرنامج الحاسوب باستنساخ نسخة واحدة منه أو اقتباسها عندما يكون ذلك ضرورياً لاستعمال البرنامج للغرض الذي اكتسب من أجله، أو لتعويض نسخة حائزة بصورة مشروعة لأغراض التوثيق في حالة ضياعها أو تلفها أو عدم صلاحيتها للاستعمال.³

كما قيد المشرع استعمال النسخة المستنسخة أو المقتبسة من البرنامج بالأغراض المحددة في المادة 52، وأوجب إتلافها عند انتهاء مشروعيتها حيازتها، وهو ما يؤكد أن الاستثناءات الواردة على حق المؤلف لا تمنح المستعمل حرية مطلقة في نسخ البرنامج أو استغلاله، وإنما تظل مرتبطة بالحدود التي رسمها القانون.⁴

وتؤكد خصوصية برامج الحاسوب كذلك من خلال استبعادها من بعض حالات الاستنساخ المسموح بها للمصنفات الأخرى. فقد نصت المادة 41 من الأمر رقم 03-05 ع⁵ إلى إمكانية استنساخ نسخة من المصنف للاستعمال الشخصي أو العائلي، لكنها استثنت من ذلك استنساخ

¹ المادتان 21 و22، الأمر رقم 03-05، سالف الذكر.

² المادة 27، الأمر رقم 03-05، سالف الذكر.

³ المادة 52، الأمر رقم 03-05، سالف الذكر.

⁴ المادة 53، الأمر رقم 03-05، سالف الذكر.

⁵ المادة 41، الأمر رقم 03-05، سالف الذكر.

برامج الحاسوب إلا في الحالات التي أجازتها المادة 52. ويعكس ذلك تشدد المشرع في حماية البرامج من النسخ غير المشروع بالنظر إلى سهولة استنساخها وإعادة توزيعها.¹

ولا تتوقف الحماية عند البرنامج في صورته المادية، وإنما تمتد إلى الحقوق المرتبطة باستغلاله ونشره وتداوله، بما يجعل أي استعمال خارج الحدود التي رسمها صاحب الحق أو القانون قابلاً لأن يشكل اعتداءً على حقوق المؤلف متى توافرت الشروط القانونية. وتبرز أهمية ذلك في البيئة الإلكترونية، حيث يمكن نسخ البرامج وتحميلها وإتاحتها للغير خلال فترة زمنية قصيرة، وهو ما يوسع نطاق الأضرار التي يمكن أن تلحق بصاحب الحق.

كما أقر المشرع الجزائري حماية جزائية للحقوق التي ينظمها الأمر رقم 03-05، من خلال تجريم بعض صور الاعتداء على حقوق المؤلف والحقوق المجاورة وفرض عقوبات على الأفعال التي تمس الحقوق المحمية. وبذلك لا تقتصر حماية برامج الحاسوب على الجانب المدني أو الحقوقي، وإنما تمتد إلى المجال الجزائي متى تحققت إحدى صور الاعتداء التي حددها القانون.²

ويظهر من ذلك أن المشرع الجزائري اختار نظام حقوق المؤلف كأساس لحماية برامج الحاسوب، فأخضعها للقواعد العامة المقررة للمصنفات المحمية، مع إقرار أحكام خاصة تراعي طبيعتها التقنية، لا سيما فيما يتعلق بالاستنساخ والاستعمال المشروع. ويحقق هذا النظام توازناً بين حماية المصالح الأدبية والمالية لصاحب البرنامج وبين تمكين الحائز الشرعي من استعمال البرنامج في الحدود التي يسمح بها القانون.

وعليه، فإن حماية برامج الحاسوب في التشريع الجزائري تقوم على الاعتراف بها صراحة كمصنفات محمية بحقوق المؤلف، مع إخضاعها لشروط الحماية العامة والاستثناءات الخاصة التي تراعي طبيعتها التقنية، إلى جانب إقرار حماية جزائية ضد الاعتداءات التي تستهدف الحقوق المقررة

¹ المادتان 41 و 52، الأمر رقم 03-05، سالف الذكر.

² المواد 151 إلى 159، الأمر رقم 03-05، سالف الذكر.

لصاحبها. وهو ما يمنح البرنامج المعلوماتي حماية متعددة الجوانب في مواجهة صور الاستغلال غير المشروع في البيئة الإلكترونية¹.

الفرع الثاني: حماية المصنفات الرقمية وقواعد البيانات

أدى التحول من الوسائط التقليدية إلى البيئة الرقمية إلى ظهور مصنفات فكرية يتم إنشاؤها أو تخزينها أو تداولها في صورة رقمية، الأمر الذي فرض امتداد الحماية القانونية لحقوق المؤلف إلى هذا النوع من المصنفات. ولم يجعل المشرع الجزائري الحماية مرتبطة بالوسيط المادي الذي يوجد عليه المصنف، وإنما ربطها بطبيعة الإبداع وأصالته، وهو ما يسمح بإدراج عدد من المصنفات الرقمية ضمن المصنفات المحمية متى توافرت فيها الشروط القانونية للحماية.

وقد أدرج المشرع الجزائري ضمن المصنفات المحمية المصنفات المكتوبة والأدبية والفنية والعلمية، بصرف النظر عن نوعها أو شكل التعبير عنها، وهو ما يسمح بحماية المصنفات التي يتم إنتاجها أو نشرها في شكل رقمي، كالمؤلفات الإلكترونية والمقالات والدراسات والصور والتسجيلات وغيرها، متى اتسمت بالأصالة وتوافرت فيها شروط الحماية المقررة قانوناً.² وتستند هذه الحماية إلى المادة 3 من الأمر رقم 03-05 التي تقرر الحماية لكل إبداع أصلي لمصنف أدبي أو فني، أيا كان نوعه أو نمطه أو طريقة التعبير عنه.³

وتتخذ المصنفات الرقمية صوراً متعددة، فقد يكون المصنف في أصله رقمياً، أي يتم إنشاؤه مباشرة باستعمال الوسائل الإلكترونية، وقد يكون مصنفاً تقليدياً تم تحويله إلى صيغة رقمية عن طريق المسح أو التصوير أو غيرهما من الوسائل التقنية. وفي كلتا الحالتين يمكن أن تنشأ حقوق للمؤلف متى كان المصنف مستوفياً لشروط الحماية، لأن الرقمنة في حد ذاتها لا تؤدي إلى إسقاط حقوق المؤلف المقررة على المصنف.

¹ المواد 3 و4 و21 و27 و151 إلى 159، الأمر رقم 03-05، سالف الذكر.

² المادة 4، الأمر رقم 03-05، سالف الذكر.

³ المادة 3، الأمر رقم 03-05، سالف الذكر.

أما قواعد البيانات، فتتمثل في مجموعات منظمة من البيانات أو المعلومات يتم ترتيبها بطريقة تسمح بتخزينها واسترجاعها والاستفادة منها باستخدام الوسائل الإلكترونية. وتكمن القيمة الفكرية في بعض قواعد البيانات في طريقة اختيار البيانات أو ترتيبها أو تنظيمها، وليس بالضرورة في البيانات المفردة التي تتكون منها. ولذلك تتجه الحماية إلى الجهد الإبداعي الذي يظهر في بناء قاعدة البيانات وتنظيم محتوياتها متى بلغ مستوى الأصالة المطلوب قانوناً¹.

ويستفاد من أحكام الأمر رقم 03-05 أن حماية حقوق المؤلف تقوم على أصالة المصنف، وهو ما يقتضي أن يكون العمل نتيجة إبداع فكري للمؤلف. ومن ثم، لا تتمتع كل قاعدة بيانات بالحماية لمجرد جمعها لعدد من المعلومات، وإنما ترتبط الحماية بالطابع الإبداعي في اختيار محتوياتها أو ترتيبها أو تنظيمها، وفقاً لما تسمح به قواعد حماية المصنفات الفكرية².

وتشمل الحماية كذلك العناصر الإبداعية التي يتضمنها المصنف الرقمي، فلا تمتد حقوق المؤلف إلى مجرد الأفكار والمعلومات والمبادئ في ذاتها، وإنما تنصرف إلى الطريقة التي تمت بها صياغة هذه العناصر والتعبير عنها. وقد أكد المشرع الجزائري ذلك صراحة عندما استبعد الأفكار والمفاهيم والمبادئ والمناهج وطرق العمل من الحماية المقررة بموجب حقوق المؤلف³.

ويترتب على حماية المصنفات الرقمية وقواعد البيانات تمتع أصحاب الحقوق بمجموعة من الحقوق الأدبية والمالية. فالحق الأدبي يحمي الصلة التي تربط المؤلف بمصنفه، بينما تسمح الحقوق المالية له بالتحكم في استغلال المصنف والحصول على المقابل المالي الناتج عنه. ويكتسب الجانب المالي أهمية خاصة في البيئة الرقمية، بالنظر إلى سهولة نسخ المصنفات وإتاحتها وتحميلها وتداولها دون إذن صاحب الحق.

كما أن البيئة الرقمية أوجدت وسائل جديدة لاستغلال المصنفات، من بينها الإتاحة عبر المواقع والمنصات الإلكترونية والتحميل والنشر الرقمي، وهو ما يفرض إخضاع هذه العمليات لموافقة صاحب الحق متى كانت داخلة ضمن حقوق الاستغلال التي يحتفظ بها. ولا يعني وجود المصنف على

¹ المادة 5، الأمر رقم 03-05، سالف الذكر.

² المادة 5، الأمر رقم 03-05، سالف الذكر.

³ المادة 7، الأمر رقم 03-05، سالف الذكر.

شبكة الإنترنت أنه أصبح مباحًا للجميع، بل تبقى الحقوق التي يقرها القانون لصاحب المصنف قائمة ما لم يوجد نص قانوني يسمح بالاستعمال أو ترخيص صادر عن صاحب الحق.

وفيما يتعلق بقواعد البيانات، فإن الاعتداء عليها قد يأخذ صورة نسخ قاعدة البيانات أو إعادة استخدامها أو إتاحتها للغير دون ترخيص، متى تعلق الأمر بعناصر أو تنظيم يتمتع بالحماية القانونية. كما قد يؤدي الاستيلاء على قاعدة بيانات إلى المساس بمصالح اقتصادية مهمة، خصوصًا عندما تتضمن بيانات تجارية أو معلومات ذات قيمة بالنسبة للمؤسسات، وهو ما يجعل الحماية القانونية لها تتقاطع أحيانًا مع حماية الأسرار التجارية والمعطيات الشخصية¹.

وقد أقر المشرع الجزائري حماية جزائية للحقوق المرتبطة بالمصنفات المحمية، بحيث يمكن أن تترتب المسؤولية الجزائية عند ارتكاب الأفعال التي تشكل اعتداءً على حقوق المؤلف والحقوق المجاورة وفقًا للأحكام الواردة في الأمر رقم 03-05². ويكتسب هذا الجانب أهمية خاصة في البيئة الرقمية، لأن سهولة نسخ المصنفات وإعادة نشرها تجعل الاعتداء عليها أكثر سرعة واتساعًا.

كما أن حماية المصنفات الرقمية لا تنفصل عن القواعد الدولية للملكية الفكرية، خاصة أن تداول المصنفات عبر الإنترنت لا يتوقف عند الحدود الإقليمية للدولة. وقد انضمت الجزائر إلى عدد من الاتفاقيات الدولية المتعلقة بحقوق المؤلف، الأمر الذي يعزز الإطار القانوني لحماية المصنفات في مواجهة الاستغلال غير المشروع، مع مراعاة الأحكام الوطنية المنظمة لهذه الحقوق³.

وعليه، فإن حماية المصنفات الرقمية وقواعد البيانات في التشريع الجزائري تقوم على إخضاعها لنظام حقوق المؤلف متى توافرت شروط الحماية، وبالأخص عنصر الأصالة، مع الاعتراف بالحقوق الأدبية والمالية لأصحابها وتحريم صور الاعتداء عليها. وتزداد أهمية هذه الحماية في البيئة الإلكترونية بالنظر إلى سهولة نسخ المحتوى الرقمي وتداوله وإتاحته للغير، مما يجعل احترام حقوق المؤلف ضرورة قانونية لضمان التوازن بين حرية تداول المعلومات وحماية الإبداع الفكري.

¹ المادتان 5 و 27، الأمر رقم 03-05، سالف الذكر؛ والمادة 2، القانون رقم 18-07، سالف الذكر.

² المواد 151 و 152 و 153، الأمر رقم 03-05، سالف الذكر.

³ المادة 162، الأمر رقم 03-05، سالف الذكر؛ واتفاقية برن لحماية المصنفات الأدبية والفنية، المؤرخة في 9 سبتمبر سنة 1886، المعدلة والمتممة، والتي انضمت إليها الجزائر بموجب المرسوم الرئاسي رقم 97-341 المؤرخ في 11 جمادى الأولى عام 1418 الموافق 13 سبتمبر سنة 1997.

الفرع الثالث: صور الاعتداء على حقوق الملكية الفكرية في البيئة الإلكترونية

أدى الانتشار الواسع للوسائط الإلكترونية إلى ظهور أساليب متعددة للاعتداء على حقوق الملكية الفكرية، مستفيدة من سهولة نسخ المحتوى الرقمي وتخزينه ونقله وإتاحته لعدد كبير من المستخدمين خلال فترة زمنية قصيرة. وتشمل هذه الاعتداءات مختلف الحقوق الأدبية والمالية التي يقرها القانون لصاحب المصنف، وقد نظم المشرع الجزائري صورًا متعددة منها ضمن الأمر رقم 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، مع ترتيب آثار قانونية وجزائية على الأفعال التي تقع بالمخالفة لأحكامه.¹

وتتمثل إحدى أبرز صور الاعتداء في الاستنساخ غير المشروع للمصنفات الرقمية، حيث يمكن نسخ كتاب إلكتروني أو مقال أو صورة أو تسجيل أو برنامج معلوماتي وإعادة إنتاجه دون الحصول على ترخيص من صاحب الحق. وقد منح المشرع للمؤلف حقًا استثنائيًا في استنساخ مصنفه بأي وسيلة كانت، مما يجعل إجراء النسخ خارج الحالات التي يسمح بها القانون اعتداءً على الحق المالي للمؤلف.² وتزداد خطورة هذا الفعل في البيئة الرقمية نتيجة إمكانية إنشاء عدد كبير من النسخ المتطابقة دون حدوث تدهور في جودة المصنف.

وتأخذ الاعتداءات كذلك صورة النشر أو الإتاحة غير المرخصة للمصنفات عبر الإنترنت، كرفع كتاب أو بحث أو صورة أو عمل فني على موقع إلكتروني أو منصة رقمية دون الحصول على إذن صاحب الحق، أو إتاحته للتحميل والتداول من طرف المستخدمين. وتدخل هذه الأفعال ضمن صور استغلال المصنف التي تخضع للحقوق الاستثنائية لصاحب الحق، متى لم تكن داخلة ضمن الاستثناءات التي أقرها القانون.³

ومن صور الاعتداء أيضًا الاقتباس أو التعديل غير المشروع للمصنف، عندما يتم تغيير محتوى المصنف أو إعادة صياغته أو إدخال تعديلات عليه دون مراعاة الحقوق المقررة للمؤلف. ويستند ذلك إلى الحق الأدبي للمؤلف في حماية مصنفه من أي تحريف أو تشويه أو تعديل من شأنه المساس

¹ المواد 151 إلى 159، الأمر رقم 03-05، سالف الذكر.

² المادة 27، الأمر رقم 03-05، سالف الذكر.

³ المادتان 27 و 99، الأمر رقم 03-05، سالف الذكر.

بسلامته أو بسمعته. وتزداد هذه الصورة انتشاراً في البيئة الرقمية بسبب سهولة معالجة الملفات الإلكترونية وتعديل محتوياتها وإعادة نشرها في صورة جديدة.¹

كما يظهر الاعتداء في نسبة المصنف إلى غير مؤلفه، وهي صورة تمس الحق الأدبي للمؤلف، حيث يقوم شخص بنشر مصنف الغير باسمه أو يحذف اسم صاحبه ويضع اسمه بدلاً منه، وهو ما يمكن أن يتحقق بالنسبة للكتب والدراسات والصور والتصاميم والمحتويات الرقمية المختلفة. وقد أقر المشرع للمؤلف حق نسبة المصنف إليه وحق تقرير نشره باسمه أو باسم مستعار، بما يحمي الرابطة المعنوية بين المؤلف وإنتاجه الفكري.²

وتبرز كذلك قرصنة المصنفات الرقمية باعتبارها من أكثر صور الاعتداء انتشاراً، وتشمل الحصول على المصنفات أو البرامج المحمية ونسخها أو توزيعها أو إتاحتها للغير دون ترخيص. ولا تقتصر القرصنة على البرامج المعلوماتية، وإنما قد تشمل الكتب الإلكترونية والموسيقى والأفلام والصور والتصاميم وقواعد البيانات وغيرها من المصنفات التي يمكن تداولها في البيئة الرقمية. وتسمح طبيعة الإنترنت بإعادة توزيع المصنف الواحد على نطاق واسع، مما يؤدي إلى توسيع دائرة الضرر الواقع على صاحب الحق.

وقد يتخذ الاعتداء صورة الاستغلال التجاري غير المرخص للمصنف، عندما يقوم شخص بتحقيق منفعة مالية من مصنف محمي دون الحصول على موافقة صاحب الحقوق، سواء من خلال بيعه أو تأجيريه أو توزيعه أو توفيره بمقابل عبر المنصات الإلكترونية. ويشكل هذا السلوك مساساً بالحقوق المالية للمؤلف، خاصة أن الاستغلال الاقتصادي للمصنف من الحقوق التي يحتفظ بها صاحب الحق وفقاً لأحكام القانون.³

كما يمكن أن يقع الاعتداء على الحقوق المرتبطة بقواعد البيانات، من خلال نسخ محتوياتها أو إعادة استغلالها أو إتاحتها للغير بصورة غير مشروعة، خاصة عندما تكون طريقة اختيار البيانات أو ترتيبها وتنظيمها ذات طابع إبداعي يستحق الحماية. ويقتضي تحديد الحماية في هذه الحالة التمييز

¹ المادة 25، الأمر رقم 03-05، سالف الذكر.

² المادتان 22 و 23، الأمر رقم 03-05، سالف الذكر.

³ المادتان 27 و 151، الأمر رقم 03-05، سالف الذكر.

بين البيانات والمعلومات في حد ذاتها، وبين الشكل الإبداعي الذي تم من خلاله جمعها أو ترتيبها وتنظيمها¹.

ومن صور الاعتداء الحديثة كذلك التحايل على الوسائل التقنية الموضوعية لحماية المصنفات الرقمية، كإزالة أو تعطيل وسائل الحماية التي يعتمد عليها صاحب الحق لمنع النسخ أو الدخول أو الاستعمال غير المرخص. وتكتسب هذه الأفعال أهمية خاصة في البيئة الإلكترونية، لأن أصحاب الحقوق يعتمدون على وسائل تقنية مختلفة للحد من الاستغلال غير المشروع لمصنفاتهم، الأمر الذي يجعل تجاوز هذه الوسائل وسيلة للتمهيد لارتكاب اعتداءات أخرى على الحقوق المحمية.

وقد أقر المشرع الجزائري حماية جزائية لحقوق المؤلف والحقوق المجاورة، حيث رتب عقوبات على مختلف الأفعال التي تشكل اعتداءً على الحقوق المحمية بموجب الأمر رقم 03-05. وتشمل الحماية الأفعال التي تمس الحقوق الأدبية والمالية، بما يسمح بمواجهة الاستغلال غير المشروع للمصنفات سواء وقع الاعتداء في البيئة التقليدية أو باستعمال الوسائل الإلكترونية².

وتتميز الاعتداءات الإلكترونية على الملكية الفكرية بكونها سريعة الانتشار ومتعددة النطاق وصعبة الحصر، إذ يمكن للمصنف المعتدى عليه أن ينتقل من موقع إلكتروني إلى آخر، وأن تتم إعادة نسخه وتداوله من طرف عدد كبير من المستخدمين. كما قد يصعب تحديد المصدر الأول للاعتداء عندما يتم استعمال حسابات وهمية أو خوادم موجودة خارج إقليم الدولة، الأمر الذي يطرح تحديات أمام تحديد المسؤولية وإثبات الفعل.

وعليه، فإن صور الاعتداء على حقوق الملكية الفكرية في البيئة الإلكترونية تتنوع بين النسخ والنشر والإتاحة غير المشروعة، والتحريف وانتحال المصنف، والقرصنة والاستغلال التجاري دون ترخيص، والاعتداء على قواعد البيانات والتحايل على وسائل الحماية التقنية. وقد سعى المشرع الجزائري إلى مواجهة هذه الأفعال من خلال توفير حماية قانونية وجزائية لحقوق أصحاب المصنفات، بما يتواءم مع طبيعة الاستغلال الرقمي للمصنفات وخصوصية البيئة الإلكترونية.

¹ المادة 5، الأمر رقم 03-05، سالف الذكر.

² المادة 11، معاهدة الويبو بشأن حق المؤلف، المعتمدة بجنيف في 20 ديسمبر سنة 1996، والتي انضمت إليها الجزائر بموجب المرسوم الرئاسي رقم 13-123 المؤرخ في 20 مارس سنة 2013.

المطلب الثاني: حماية النظام المعلوماتي في قانون العقوبات

أقر المشرع الجزائري حماية جنائية للأنظمة المعلوماتية والمعطيات المرتبطة بها من خلال تجريم الأفعال التي تستهدف سلامة هذه الأنظمة والبيانات التي تتضمنها، كما امتدت الحماية إلى الجرائم التي يمكن ارتكابها باستعمال الوسائل الإلكترونية متى توافرت عناصرها القانونية، بما يواكب تطور أساليب الإجرام في البيئة الرقمية. وعليه، سيتم التطرق في الفرع الأول إلى تجريم الاعتداء على الأنظمة المعلوماتية، وفي الفرع الثاني إلى تجريم الاعتداء على البيانات والمعطيات المعلوماتية، ثم دراسة الفرع الثالث المتعلق بتجريم الأفعال المرتكبة بواسطة الوسائل الإلكترونية.

الفرع الأول: تجريم الاعتداء على الأنظمة المعلوماتية

أصبحت الأنظمة المعلوماتية من أهم الوسائل التي تعتمد عليها الإدارات والمؤسسات والأشخاص في تخزين المعلومات ومعالجتها وتبادلها، وهو ما جعلها محلاً لأفعال إجرامية تستهدف الدخول إليها أو تعطيلها أو تغيير طريقة اشتغالها. وقد تدخل المشرع الجزائري بتجريم هذه الأفعال ضمن قانون العقوبات، من خلال إدراج أحكام خاصة بالمساس بأنظمة المعالجة الآلية للمعطيات، بما يوفر حماية جنائية للنظام المعلوماتي باعتباره مصلحة قانونية مستقلة.¹

وقد خصص المشرع الجزائري قسمًا ضمن قانون العقوبات للجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، وجرم في المادة 394 مكرر فعل الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات. وتتحقق الجريمة بمجرد تحقق الدخول أو البقاء غير المشروع وفق الشروط التي حددها النص، بما يعني أن الحماية الجنائية لا تتوقف على حدوث خسارة مالية أو إتلاف مادي للنظام.²

ويستفاد من ذلك أن المشرع يحمي حق صاحب النظام أو مستعمله المشروع في السيطرة على منظومته المعلوماتية، بحيث لا يجوز للغير الولوج إليها أو البقاء فيها دون سند قانوني. ويشمل ذلك

¹ الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم، لا سيما بالقانون رقم 24-06 المؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 30، 30 أبريل سنة 2024، المواد 394 مكرر إلى 394 مكرر 3.

² المادة 394 مكرر، الأمر رقم 66-156، سالف الذكر.

مختلف الأنظمة التي تستوفي مفهوم منظومة المعالجة الآلية للمعطيات، سواء كانت مملوكة لأشخاص طبيعيين أو معنويين، متى تحققت العناصر التي يتطلبها النص الجزائي¹.

ولا تقتصر الحماية على مجرد الدخول غير المشروع، وإنما تمتد إلى الأفعال التي تؤثر في سلامة النظام وطريقة اشتغاله. فقد شدد المشرع العقوبة عندما يؤدي الفعل إلى حذف أو تغيير المعطيات الموجودة في المنظومة، كما قرر عقوبة أشد عندما يترتب على السلوك تخريب نظام اشتغال المنظومة². ويكشف هذا التدرج عن اختلاف درجة الحماية بحسب النتيجة التي ترتبت عن الاعتداء، فالمساس بسلامة البيانات أو تعطيل النظام أكثر خطورة من مجرد الدخول غير المشروع إليه³.

ويأخذ الاعتداء على النظام المعلوماتي صوراً متعددة، فقد يتمثل في تعطيل النظام أو عرقلة سيره أو التأثير في وظائفه، سواء باستعمال برامج أو أوامر معلوماتية أو من خلال استغلال ثغرات تقنية تسمح بالتدخل في طريقة اشتغال المنظومة. ويقتضي التكيف القانوني للفعل تحديد السلوك الذي قام به الجاني والنتيجة التي ترتبت عنه ومدى انطباق النص الجزائي عليه.

كما جرم المشرع الجزائري الأفعال التي تستهدف إدخال معطيات بطريق الغش أو إزالة أو تعديل المعطيات الموجودة في منظومة المعالجة الآلية للمعطيات. ويظهر هنا الارتباط بين حماية النظام وحماية محتواه المعلوماتي، لأن العبث بالبيانات قد يؤدي بصورة مباشرة إلى التأثير في وظائف النظام أو النتائج التي ينتجها⁴.

وقد عزز المشرع الحماية من خلال تجريم تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات معدة أو برامج وأدوات مخصصة لارتكاب الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وفق الشروط التي حددها القانون. وتستهدف هذه الأحكام مواجهة بعض الأفعال التحضيرية التي توفر الوسائل التقنية اللازمة لارتكاب الاعتداءات على الأنظمة المعلوماتية⁵.

¹ المادة 394 مكرر، الأمر رقم 66-156، المعدل والمتمم، سالف الذكر.

² المادة 394 مكرر، الأمر رقم 66-156، المعدل والمتمم، سالف الذكر.

³ المادة 394 مكرر، الأمر رقم 66-156، المعدل والمتمم، سالف الذكر.

⁴ المادة 394 مكرر 1، الأمر رقم 66-156، المعدل والمتمم، سالف الذكر.

⁵ المادة 394 مكرر 2، الأمر رقم 66-156، المعدل والمتمم، سالف الذكر.

وتتضح أهمية هذه الحماية في مواجهة ما يعرف بالهجمات المعلوماتية التي تستهدف إتاحة النظام واستمرارية خدماته، خاصة عندما يكون النظام مرتبطاً بمرفق عمومي أو مؤسسة تقدم خدمات أساسية. وقد راعى المشرع درجة خطورة بعض الأفعال من خلال تشديد العقوبات عندما تتعلق الجريمة بأنظمة محددة أو تترتب عنها نتائج أكثر جسامة، وفقاً للحالات التي حددها قانون العقوبات.

ولا تنفصل الحماية الموضوعية للأنظمة المعلوماتية عن الحماية الإجرائية، إذ إن طبيعة هذه الجرائم تفرض وسائل خاصة للكشف عنها وإثباتها. وقد جاء القانون رقم 09-04 ليضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال تنظيم بعض إجراءات التحري والمراقبة وجمع الأدلة المرتبطة بالجرائم الإلكترونية.¹

ويطرح تجريم الاعتداء على الأنظمة المعلوماتية كذلك مسألة مبدأ الشرعية الجنائية، إذ لا يكفي وصف السلوك بأنه اعتداء إلكتروني لقيام المسؤولية الجنائية، بل يجب أن يكون الفعل مندرجاً ضمن سلوك مجرم بنص قانوني واضح، وأن تتوفر في الواقعة جميع العناصر المادية والمعنوية للجريمة. ويكتسب هذا الأمر أهمية خاصة في المجال المعلوماتي بسبب سرعة ظهور تقنيات وأساليب جديدة قد لا تتطابق دائماً بصورة مباشرة مع الأوصاف الجنائية القائمة.

وعليه، فإن المشرع الجزائري أقام حماية جنائية للأنظمة المعلوماتية من خلال تجريم الدخول أو البقاء غير المشروع فيها، وتجريم الأفعال التي تؤدي إلى حذف أو تغيير معطياتها أو تخريب نظام اشتغالها، فضلاً عن مواجهة بعض الوسائل والأفعال المرتبطة بارتكاب هذه الجرائم. وتكشف هذه الأحكام عن توجه نحو حماية سرية الأنظمة وسلامتها واستمرارية عملها، مع ربط المسؤولية الجنائية بتوافر الشروط التي يحددها النص الجزائي.²

¹ القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، 16 غشت سنة 2009، المواد 3 إلى 11.

² المواد 394 مكرر و394 مكرر 1 و394 مكرر 2، الأمر رقم 66-156، سالف الذكر.

الفرع الثاني: تجريم الاعتداء على البيانات والمعطيات المعلوماتية

تخضع البيانات والمعطيات المعلوماتية بحماية جنائية بالنظر إلى قيمتها في مختلف المجالات، إذ أصبحت تخزن داخل الأنظمة المعلوماتية وتستخدم في تسيير المؤسسات وإدارة المعاملات وتقديم الخدمات. وقد اتجه المشرع الجزائري إلى تجريم الأفعال التي تمس هذه المعطيات، سواء من خلال حذفها أو تغييرها أو إدخال بيانات إليها بطريقة غير مشروعة، بما يوفر حماية لسلامتها من العبث والتلاعب والاستعمال غير المشروع.¹

ويظهر هذا التجريم من خلال أحكام قانون العقوبات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث نص المشرع على معاقبة كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريقة الغش المعطيات التي يتضمنها.² ويتضح من هذا النص أن محل الاعتداء قد يكون المعطيات المخزنة داخل النظام، دون أن يكون من الضروري أن يستهدف الجاني النظام المعلوماتي ذاته بالتخريب أو التعطيل.

وتتخذ عملية الاعتداء على البيانات عدة صور، من أبرزها الحذف غير المشروع للمعطيات، ويقصد به إزالة بيانات موجودة داخل النظام دون ترخيص من صاحب الحق أو الشخص المخول قانوناً بذلك. وقد يؤدي هذا السلوك إلى فقدان معلومات مهمة أو تعطيل عمليات تعتمد عليها، خصوصاً عندما يتعلق الأمر بقواعد بيانات المؤسسات أو السجلات الإلكترونية أو المعلومات المرتبطة بالمعاملات.

كما تتمثل إحدى صور الاعتداء في تغيير المعطيات المعلوماتية، وذلك بإدخال تعديلات غير مشروعة عليها، كتحريف محتواها أو استبدال بعض المعلومات الواردة فيها أو تغيير قيمتها بما يؤدي إلى إنتاج معلومات غير صحيحة. وتظهر خطورة هذه الصورة عندما تكون البيانات محل التعديل

¹ المادة 394 مكرر 1، الأمر رقم 66-156، سالف الذكر.

² المادة 394 مكرر 1، الأمر رقم 66-156، سالف الذكر.

مرتبطة بالمعاملات المالية أو الإدارية أو المهنية، لأن تغييرها قد يؤدي إلى نتائج قانونية أو مالية تختلف عن النتائج التي كانت ستنتج عن البيانات الصحيحة¹.

وتأخذ الجريمة كذلك صورة إدخال معطيات بطريق الغش، وهي الحالة التي يقوم فيها الجاني بإدخال معلومات إلى النظام دون حق وبطريقة احتيالية، بما يؤدي إلى تغيير المحتوى المعلوماتي للنظام. ويشمل ذلك، بحسب ظروف الواقعة، إدخال بيانات وهمية أو غير صحيحة بقصد تحقيق نتيجة غير مشروعة، متى توافرت العناصر التي يتطلبها النص الجزائي².

ولا تقتصر الحماية الجزائية للبيانات على مواجهة الأفعال التي تقع داخل النظام، إذ يمكن أن تتصل المعطيات محل الاعتداء بأفعال أخرى مجرمة قانوناً، خصوصاً عندما تتعلق بالمعلومات الشخصية للأفراد. وقد خصص المشرع الجزائري حماية قانونية للمعطيات ذات الطابع الشخصي من خلال القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث وضع قواعد تتعلق بجمع هذه المعطيات ومعالجتها وحفظها واستعمالها³.

ويكتسب الاعتداء على المعطيات الشخصية خصوصية بالنظر إلى ارتباطه المباشر بحقوق الفرد وحرياته الأساسية، إذ قد يؤدي الحصول غير المشروع على المعلومات الشخصية أو استعمالها أو نشرها إلى المساس بالحياة الخاصة أو السمعة أو المصالح المالية للشخص المعني. ولذلك لا تقتصر الحماية على الجانب التقني للبيانات، وإنما تمتد إلى حماية الشخص الذي تتعلق به هذه البيانات.

كما يمكن أن يتم الاعتداء من خلال الحصول غير المشروع على البيانات أو إفشائها أو استعمالها خارج الغرض المحدد لها، وهو ما يختلف تكييفه القانوني بحسب طبيعة المعطيات والوسيلة المستعملة والصفة التي يتمتع بها مرتكب الفعل. فإذا تعلق الأمر بمعطيات شخصية، تطبق الأحكام

¹ المادة 394 مكرر 1، الأمر رقم 66-156، سالف الذكر.

² المادة 394 مكرر 1، الأمر رقم 66-156، سالف الذكر.

³ القانون رقم 07-18 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، 10 يونيو سنة 2018، المادتان 1 و2.

الخاصة بحمايتها، بينما قد تخضع الوقائع لنصوص أخرى عندما تكون البيانات مرتبطة بأسرار مهنية أو تجارية أو مالية¹.

وتبرز خطورة الاعتداء على البيانات كذلك في إمكانية نسخها ونقلها وإعادة استخدامها دون علم صاحبها أو دون الحصول على الترخيص اللازم، خصوصاً في ظل سهولة نقل الملفات وقواعد البيانات بين الأنظمة المختلفة. وقد يؤدي ذلك إلى فقدان صاحب البيانات السيطرة على المعلومات التي تخصه، أو إلى استعمالها في ارتكاب جرائم أخرى، كالاختيال الإلكتروني أو انتحال الهوية أو الابتزاز.

وقد أحاط المشرع الجزائري بعض صور الاعتداء على المعطيات بجزاءات جنائية، تختلف بحسب طبيعة الفعل والبيانات محل الاعتداء وصفة مرتكبه والنتائج المترتبة عنه. كما أقر القانون رقم 04-09 قواعد خاصة للتحري والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهو ما يساهم في تمكين السلطات المختصة من التعامل مع الأدلة والآثار الرقمية الناتجة عن الاعتداء على البيانات².

وتظهر أهمية الحماية الجنائية للبيانات في أن المعلومة الرقمية يمكن أن تكون في حد ذاتها محلاً للجريمة، وليس مجرد وسيلة لارتكابها. فقد يستهدف الجاني البيانات للحصول عليها أو تغييرها أو حذفها، وقد يستعملها بعد ذلك في تحقيق منفعة غير مشروعة أو إلحاق الضرر بالغير. ومن ثم، فإن حماية المعطيات المعلوماتية تقتضي تجريم الاعتداء عليها بصورة مستقلة عن الحماية المقررة للنظام الذي توجد داخله³.

وعليه، فإن تجريم الاعتداء على البيانات والمعطيات المعلوماتية في التشريع الجزائري يقوم على حماية سلامة المحتوى المعلوماتي من الإدخال أو الحذف أو التعديل غير المشروع، مع امتداد الحماية إلى المعطيات ذات الطابع الشخصي وفق الأحكام الخاصة بها. وتساهم هذه الحماية في ضمان

¹ المادتان 2 و3، القانون رقم 18-07، سالف الذكر.

² المواد 3 إلى 11، القانون رقم 09-04، سالف الذكر.

³ المادتان 394 مكرر و394 مكرر 1، الأمر رقم 66-156، سالف الذكر.

موثوقية المعلومات وسلامتها، وحماية المصالح المرتبطة بها، خاصة في ظل الاعتماد المتزايد على المعالجة الإلكترونية للبيانات في مختلف المجالات.

الفرع الثالث: تجريم الجرائم المرتكبة بواسطة الوسائل الالكترونية

لم يعد استعمال الوسائل الإلكترونية مقتصرًا على الاعتداء على الأنظمة المعلوماتية أو البيانات، وإنما أصبحت التكنولوجيا وسيلة لارتكاب أفعال إجرامية تمس مختلف المصالح التي يحميها القانون الجنائي. فقد تستخدم شبكة الإنترنت أو البريد الإلكتروني أو منصات التواصل الاجتماعي أو وسائل الاتصال الحديثة في ارتكاب جرائم تمس الأموال أو الأشخاص أو الشرف والاعتبار، دون أن يكون النظام المعلوماتي ذاته هو محل الاعتداء. ومن ثم، تقتضي الحماية الجنائية في البيئة الرقمية تطبيق النصوص التي تجرم السلوك الإجرامي بحسب طبيعته، مع مراعاة الوسيلة الإلكترونية التي استعملت في ارتكابه.¹

ويظهر ذلك من خلال جرائم الاحتيال المرتكبة باستعمال الوسائل الإلكترونية، حيث يمكن للجاني استخدام المواقع الإلكترونية أو الرسائل أو الحسابات الرقمية أو وسائل الدفع الإلكتروني لإيهام الضحية بوقائع غير صحيحة وحملها على تسليم مال أو منفعة. ولا يؤدي استعمال الوسيلة الإلكترونية في هذه الحالة إلى زوال الوصف الجنائي للفعل، وإنما تكون التكنولوجيا وسيلة لتنفيذ السلوك الاحتيالي، ويحدد التكييف القانوني وفق العناصر التي يتطلبها النص المجرم.²

كما يمكن استعمال الوسائل الإلكترونية في الاعتداء على الشرف والاعتبار، من خلال نشر عبارات أو ادعاءات تمس شخصًا معينًا عبر المواقع الإلكترونية أو شبكات التواصل الاجتماعي. وتطبق على هذه الأفعال الأحكام الجزائية المتعلقة بالقتل والسب متى توافرت عناصرها القانونية، مع مراعاة طبيعة الوسيلة التي تم بواسطتها النشر ومدى تحقق العلانية.³ ويكشف ذلك عن قابلية بعض الجرائم التقليدية للتكيف مع البيئة الإلكترونية دون الحاجة بالضرورة إلى إنشاء وصف جنائي مستقل لكل وسيلة تقنية جديدة.

¹ الأمر رقم 66-156، سالف الذكر، والمواد الخاصة بالجرائم التي يمكن ارتكابها باستعمال الوسائل الإلكترونية بحسب طبيعة الفعل المرتكب.

² المادة 372، الأمر رقم 66-156، سالف الذكر.

³ المادتان 296 و 297، الأمر رقم 66-156، سالف الذكر.

وتستعمل الوسائل الإلكترونية كذلك في التهديد والابتزاز، سواء من خلال الرسائل النصية أو البريد الإلكتروني أو الحسابات الإلكترونية، حيث قد يهدد الجاني الضحية بإلحاق ضرر بها أو نشر صور أو معلومات خاصة عنها بهدف حملها على القيام بفعل معين أو الامتناع عنه أو الحصول منها على منفعة. ويخضع الفعل للنصوص الجزائية التي تنظم التهديد أو غيره من الجرائم بحسب ظروف الواقعة ومضمون السلوك والغاية التي اتجه إليها الجاني.¹

وقد تمتد الجرائم المرتكبة بواسطة الوسائل الإلكترونية إلى المساس بالحياة الخاصة، خاصة عندما يتم تسجيل أو التقاط أو نقل أو نشر صور أو محادثات أو معلومات خاصة دون رضا الشخص المعني وفي الحالات التي يجرمها القانون. وقد خص المشرع الجزائري الحياة الخاصة بحماية جزائية ضمن قانون العقوبات، وهو ما يسمح بمواجهة بعض الاعتداءات التي تستعمل التكنولوجيا الحديثة وسيلة لتنفيذها.²

كما يمكن أن تشكل الوسائل الإلكترونية أداة لارتكاب جرائم تمس الأموال والمعاملات، كاستعمال بيانات أو وسائل إلكترونية للحصول على أموال الغير أو تحويلها أو إجراء معاملات بطرق احتيالية. وتختلف المسؤولية الجنائية بحسب طبيعة الفعل والوسيلة المستخدمة والنتيجة المترتبة عنه، فقد تتوافر في الواقعة عناصر جريمة من جرائم الأموال، وقد تتداخل معها جرائم المساس بأنظمة المعالجة الآلية للمعطيات إذا استلزم ارتكابها الدخول أو التدخل غير المشروع في نظام معلوماتي.

ويكتسب هذا النوع من الجرائم خصوصية من ناحية إثبات الفعل ونسبته إلى مرتكبه، إذ تترك الوسائل الإلكترونية آثاراً رقمية يمكن أن تتمثل في الرسائل الإلكترونية وسجلات الاتصال وبيانات الحسابات والمحتويات الرقمية وغيرها. وقد نظم المشرع الجزائري من خلال القانون رقم 09-04 قواعد خاصة للتحري والتحقق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما يسمح باستخدام إجراءات تتلاءم مع طبيعة الجرائم التي ترتكب باستعمال الوسائل الإلكترونية.³

¹ المواد 284 إلى 287، الأمر رقم 66-156، سالف الذكر.

² المادتان 303 مكرر و303 مكرر 1، الأمر رقم 66-156، سالف الذكر.

³ المواد 3 و5 و6 و9 إلى 11، القانون رقم 09-04، سالف الذكر.

كما أن استعمال الوسائل الإلكترونية في ارتكاب الجريمة قد يؤدي إلى تعدد الأوصاف القانونية للفعل الواحد، فاختراق حساب إلكتروني للحصول على صور خاصة، ثم استعمالها لتهديد صاحبها للحصول على المال، قد ينطوي بحسب الوقائع على أكثر من اعتداء يستوجب دراسة كل عنصر من عناصره بصورة مستقلة. ومن ثم، لا يكفي وصف الواقعة بأنها «جريمة إلكترونية»، بل ينبغي تحديد المصلحة القانونية المعتدى عليها والسلوك المادي والوسيلة المستعملة والنتيجة التي ترتبت عن الفعل¹.

ويقتضي مبدأ الشرعية الجنائية أن يكون تجريم الفعل قائماً على نص قانوني سابق، فلا يمكن اعتبار كل سلوك غير مألوف في البيئة الرقمية جريمة لمجرد استعمال التكنولوجيا في ارتكابه. ولذلك يعتمد التكييف الجنائي على النص الذي ينطبق على السلوك، سواء كان وارداً في قانون العقوبات أو في قانون خاص، مع مراعاة الأحكام المتعلقة بالوسائل الإلكترونية متى نص القانون عليها صراحة.²

وتبرز أهمية هذه القاعدة في مواجهة التطور المستمر للتكنولوجيا، لأن أساليب ارتكاب الجرائم تتغير بوتيرة أسرع من تطور النصوص القانونية. ومن ثم، فإن فعالية التجريم لا تقوم فقط على استحداث نصوص جديدة، وإنما كذلك على حسن تطبيق النصوص القائمة على الأفعال التي تستعمل الوسائل الإلكترونية كأداة لتنفيذها، دون التوسع في التجريم بما يتعارض مع مبدأ الشرعية.

وعليه، فإن الجرائم المرتكبة بواسطة الوسائل الإلكترونية لا تشكل بالضرورة فئة مستقلة من الجرائم من حيث محل الاعتداء، وإنما قد تمثل وسيلة تقنية لارتكاب جرائم ذات طبيعة مختلفة، كجرائم الاحتيال والتهديد والابتزاز والقذف والسب والمساس بالحياة الخاصة والاعتداء على الأموال. وتقوم مواجهتها في التشريع الجزائري على تطبيق النصوص الجزائية المناسبة لطبيعة كل فعل، إلى جانب القواعد الخاصة التي تراعي الخصائص التقنية لارتكاب الجريمة وإثباتها.

¹ المواد 394 مكرر إلى 394 مكرر 2، الأمر رقم 66-156، سالف الذكر.

² المادة 1، الأمر رقم 66-156، سالف الذكر.

المطلب الثالث: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

أدرك المشرع الجزائري أن مواجهة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال لا تتحقق من خلال التجريم والعقاب فقط، وإنما تستلزم وضع قواعد خاصة للوقاية والكشف والتحري، بالنظر إلى الطبيعة التقنية لهذه الجرائم وسرعة ارتكابها وانتشار آثارها. وفي هذا الإطار صدر القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث وضع أحكاماً تتعلق بنطاق تطبيقه، وأقر مجموعة من التدابير الوقائية وآليات الرقابة، كما رتب التزامات على مقدمي خدمات الاتصال بما يساهم في تسهيل الكشف عن الجرائم وضبط مرتكبيها. وعليه، سيتم تناول نطاق تطبيق القانون في الفرع الأول، ثم التدابير الوقائية وآليات الرقابة في الفرع الثاني، وأخيراً التزامات مقدمي خدمات الاتصال في مكافحة الجريمة الإلكترونية في الفرع الثالث.

الفرع الأول: نطاق تطبيق قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

أفرد المشرع الجزائري للجرائم المرتبطة بتكنولوجيات الإعلام والاتصال نظاماً قانونياً خاصاً بموجب القانون رقم 04-09، بهدف وضع قواعد تتلاءم مع الطبيعة التقنية لهذه الجرائم، سواء من حيث إجراءات البحث والتحري أو جمع الأدلة أو التعاون مع الجهات المختصة. ويحدد هذا القانون نطاقاً خاصاً لتطبيق أحكامه، فلا ينصرف إلى جميع الجرائم بصورة مطلقة، وإنما يرتبط بالجرائم التي تستعمل فيها تكنولوجيات الإعلام والاتصال في ارتكاب الفعل أو التي تكون ذات صلة مباشرة بالأنظمة المعلوماتية والاتصالات الإلكترونية.¹

وقد حددت المادة 2 من القانون رقم 04-09² المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث تشمل الجرائم التي يكون ارتكابها أو تسهيل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية، كما تشمل الجرائم التي يكون فيها النظام المعلوماتي أو

¹ أحمد مسعود مريم، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04-09، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، السنة الجامعية 2012-2013، ص 66.

² المادة 2، القانون رقم 04-09، سالف الذكر.

الاتصالات الإلكترونية محلاً للجريمة. ويكشف هذا التحديد عن اتساع نطاق القانون من حيث طبيعة العلاقة بين الجريمة والتكنولوجيا، إذ لا يشترط أن يكون النظام المعلوماتي هو محل الاعتداء في جميع الحالات، وإنما يكفي في بعض الصور أن تستخدم التكنولوجيا وسيلة لارتكاب الجريمة.¹

ويطبق القانون كذلك على الجرائم التي تستهدف الأنظمة المعلوماتية والمعطيات الإلكترونية، باعتبار أن هذه الأنظمة قد تكون محلاً مباشراً للاعتداء، كالدخول غير المشروع إليها أو المساس بسلامتها أو تغيير أو حذف المعطيات المخزنة فيها. كما يشمل الجرائم التي ترتبط باستخدام وسائل الاتصال الإلكترونية في تنفيذ النشاط الإجرامي، متى كانت الواقعة داخلة ضمن الحالات التي حددها القانون.²

ومن الناحية الإجرائية، لا يقتصر نطاق القانون على نوع معين من الجرائم، وإنما يحدد مجموعة من القواعد الخاصة بالبحث والتحري والتحقيق القضائي عندما تكون الجريمة مرتبطة بتكنولوجيات الإعلام والاتصال. وتشمل هذه القواعد مراقبة الاتصالات الإلكترونية، والتفتيش والحجز في المنظومات المعلوماتية، وجمع وتسجيل المعطيات المتعلقة بالاتصالات، وفق الشروط والضوابط القانونية المقررة.³

كما يرتبط نطاق تطبيق القانون بطبيعة البيانات الإلكترونية التي يمكن الحصول عليها أثناء إجراءات البحث والتحري، إذ تفرض البيئة الرقمية التعامل مع معلومات قد تكون قابلة للحذف أو التعديل أو النقل بسرعة. ولهذا أقر المشرع قواعد تسمح للجهات القضائية المختصة باتخاذ التدابير اللازمة للحفاظ على المعطيات المخزنة في منظومة معلوماتية، وضمان عدم فقدانها أو تغييرها خلال مرحلة التحقيق.⁴

¹ الحسن نائي، بغشام رقا، «ضوابط وإجراءات مراقبة الاتصالات الإلكترونية في التشريع الجزائري»، مجلة الدراسات القانونية المقارنة، المجلد 09، العدد 01، 2023، ص 16.

² جخدم محمد، «جرائم الفضاء الإلكتروني في ضوء القانون الجزائري رقم 09-04 بين قصور التجريم ورهانات التكيف التشريعي»، مجلة الدراسات القانونية والسياسية، المجلد 12، العدد 02، 2026، ص ص 56-66.

³ المادة 3، القانون رقم 09-04، سالف الذكر.

⁴ عماد يوسف، لهر ضربان، إجراءات التحري في الجرائم الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة الوادي، 2023، ص ص 40-35.

ويمتد نطاق تطبيق القانون كذلك إلى الحالات التي تكون فيها الجريمة عابرة للحدود، حيث قد تكون البيانات أو الأنظمة المعلوماتية موجودة في دولة أخرى، أو يكون مرتكب الجريمة في إقليم مختلف عن مكان تحقق النتيجة الإجرامية. وقد أقر المشرع في هذا الإطار قواعد للتعاون والمساعدة القضائية الدولية في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بما يسمح بتبادل المعلومات والمساعدة في جمع الأدلة وملاحقة مرتكبي الجرائم وفق الأطر القانونية المعمول بها.¹

وتظهر أهمية البعد الدولي في أن البيئة الإلكترونية لا تخضع في عملها للحدود الإقليمية التقليدية، فقد يقوم شخص موجود في دولة معينة باستعمال نظام أو خدمة إلكترونية موجودة في دولة ثانية، لإلحاق ضرر بشخص أو مؤسسة موجودة في دولة ثالثة. ويؤدي هذا التشابك إلى صعوبة تحديد مكان ارتكاب الجريمة ومكان تحقق نتيجتها، الأمر الذي يجعل التعاون القضائي الدولي عنصراً مهماً في مكافحة الجرائم الإلكترونية.²

وقد منح القانون أهمية كذلك للجهات المكلفة بالتحري والبحث عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إذ نظم بعض الإجراءات التي تمارسها السلطات القضائية والضبطية القضائية تحت إشراف الجهات المختصة، مع إخضاع استعمال الوسائل الخاصة بالتحري للضوابط القانونية.³ ويهدف ذلك إلى تحقيق التوازن بين فعالية البحث عن الجرائم الإلكترونية من جهة، واحترام الحقوق والحريات الفردية من جهة أخرى.

كما أن نطاق تطبيق القانون لا يعني منح سلطات التحقيق صلاحيات غير محدودة في الوصول إلى البيانات أو مراقبة الاتصالات، بل إن الإجراءات الخاصة تخضع لشروط وضمانات قانونية، خصوصاً عندما يتعلق الأمر بمراقبة الاتصالات الإلكترونية أو الدخول إلى منظومات معلوماتية أو اعتراض البيانات. وتكمن أهمية هذه الضوابط في حماية الحياة الخاصة والسرية، ومنع تحول وسائل مكافحة الجريمة الإلكترونية إلى وسيلة للمساس غير المبرر بالحقوق والحريات.

¹ المواد 15 إلى 18، القانون رقم 09-04، سالف الذكر.

² فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون عام، كلية الحقوق، جامعة الجزائر 1 بن يوسف بن خدة، 2018، ص 154.

³ حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، جامعة باتنة، 2015-2016، ص 177.

ويظهر من ذلك أن المشرع الجزائري تبني في القانون رقم 04-09 مفهوماً واسعاً للجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بحيث يشمل الجرائم التي تستهدف الأنظمة والبيانات المعلوماتية، وكذلك الجرائم التي تستخدم التكنولوجيا كوسيلة لارتكابها. كما وسع نطاق الحماية إجرائياً من خلال وضع قواعد خاصة للتحري وجمع الأدلة والتعاون الدولي، مع إخضاع هذه الإجراءات للضوابط القانونية اللازمة.

وعليه، فإن نطاق تطبيق قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يمتد إلى مختلف الجرائم التي ترتبط بالتكنولوجيا ارتباطاً مباشراً من حيث محل الجريمة أو وسيلة ارتكابها، كما يشمل مجموعة من الإجراءات الخاصة التي تسمح بالكشف عن الجريمة وجمع أدلتها وملاحقة مرتكبيها، مع مراعاة الضمانات القانونية المرتبطة بالحقوق والحريات الأساسية.

الفرع الثاني: التدابير الوقائية وآليات الرقابة

لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لم يقتصر تدخل المشرع الجزائري على التجريم والعقاب، وإنما أقر مجموعة من التدابير التي تسمح بالوقاية من بعض الأفعال الإجرامية والكشف عنها في الوقت المناسب، خاصة عندما تكون المعطيات الإلكترونية معرضة للحذف أو التغيير أو النقل. وقد نظم القانون رقم 04-09 إجراءات خاصة تسمح للجهات المختصة بمراقبة بعض الاتصالات الإلكترونية واعتراضها، إلى جانب حفظ المعطيات المتعلقة بالاتصالات وتحديد مصدرها ووجهتها، وذلك وفق الشروط والضوابط التي حددها القانون.¹

وتتمثل إحدى أهم آليات الرقابة في مراقبة الاتصالات الإلكترونية واعتراضها، حيث أجاز القانون، في حالات محددة، اللجوء إلى هذه الوسيلة عندما تقتضي ضرورات التحري أو التحقيق ذلك، وبناءً على إذن صادر عن السلطة القضائية المختصة. وتسمح هذه الآلية بالحصول على معلومات قد يكون من الصعب الوصول إليها بالوسائل التقليدية، خاصة في الجرائم التي تتم عن طريق الرسائل الإلكترونية أو وسائل الاتصال الحديثة.²

¹ المادتان 3 و4، القانون رقم 04-09، سالف الذكر.

² لحسن نائي، بغشام رقاوي، مرجع سابق، ص ص 16-20.

ولا تمنح هذه السلطة بصورة مطلقة، إذ أخضع المشرع عملية مراقبة الاتصالات لجملة من الشروط، من بينها أن تتم في إطار التحقيق أو التحري في الجرائم التي حددها القانون، وأن تكون تحت إشراف السلطة القضائية المختصة. ويهدف هذا التنظيم إلى تحقيق التوازن بين ضرورة استخدام وسائل فعالة لمكافحة الجريمة الإلكترونية وبين حماية الحق في سرية الاتصالات والحياة الخاصة.

كما أقر المشرع إجراء حفظ المعطيات المتعلقة بحركة الاتصالات، بالنظر إلى أهمية هذه البيانات في تحديد مصدر الاتصال ووجهته وتاريخ إجرائه ومدته وغيرها من المعلومات التقنية التي يمكن أن تساعد في الكشف عن مرتكب الجريمة. وتكتسب هذه البيانات أهمية خاصة في التحقيقات الإلكترونية، لأنها قد تسمح بربط نشاط رقمي معين بحساب أو جهاز أو اتصال محدد.¹

ومن التدابير ذات الأهمية كذلك إلزام بعض الأشخاص والجهات بحفظ المعطيات المعلوماتية التي تكون بحوزتهم، وفق الشروط والمدة التي يحددها القانون. ويهدف هذا الإجراء إلى منع ضياع الأدلة الرقمية، خصوصاً أن البيانات الإلكترونية يمكن حذفها أو تغييرها بسرعة، مما قد يؤدي إلى عرقلة عملية البحث والتحقيق إذا لم يتم اتخاذ التدابير اللازمة لحفظها.²

وقد سمح القانون أيضاً باتخاذ إجراءات تتعلق بالوصول إلى المعطيات المخزنة داخل منظومة معلوماتية عندما تتوفر الشروط القانونية، بما في ذلك الحالات التي تكون فيها المعطيات قابلة للوصول إليها من منظومة أخرى مرتبطة بها. ويكتسي هذا الإجراء أهمية خاصة في مواجهة الجرائم التي تستخدم أنظمة متعددة أو خدمات إلكترونية موزعة على أكثر من جهاز أو مكان.³

وتتصل التدابير الوقائية كذلك بعمل الهيئات والجهات المكلفة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث أقر المشرع إنشاء آليات مؤسسية تسمح بتنسيق الجهود وتبادل المعلومات المتعلقة بالتهديدات والأفعال الإجرامية المرتبطة بالبيئة الرقمية.

¹ أحمد مسعود مريم، مرجع سابق، ص ص 66-70.

² المادة 11، القانون رقم 09-04، سالف الذكر.

³ المادتان 5 و6، القانون رقم 09-04، سالف الذكر.

ويساهم هذا التنسيق في تحسين سرعة الاستجابة للجرائم الإلكترونية وتسهيل عملية جمع المعلومات التقنية اللازمة للتحقيق¹.

كما أن الرقابة في البيئة الإلكترونية لا تنحصر في مرحلة ما بعد وقوع الجريمة، وإنما يمكن أن يكون لها بعد وقائي واستباقي، من خلال رصد بعض المؤشرات والأنشطة التي قد تكشف عن وجود تهديد للأنظمة المعلوماتية أو الاتصالات الإلكترونية. غير أن استعمال هذه الوسائل يجب أن يظل مقيداً بالنصوص القانونية، لأن الاعتبارات الأمنية لا تبرر تجاوز الضمانات المقررة لحماية الحقوق والحريات.

ويكتسب الترخيص القضائي أهمية أساسية في هذا المجال، خاصة بالنسبة للإجراءات التي تمس سرية الاتصالات أو الحياة الخاصة. إخضاع بعض التدابير لإذن قضائي يسمح برقابة مشروعية الإجراء والتأكد من وجود مبررات جدية تستدعي اللجوء إليه، ويحول دون استعمال وسائل المراقبة بصورة تعسفية أو خارج الأغراض التي حددها القانون².

ومن جهة أخرى، ترتبط فعالية التدابير الوقائية بقدرة الجهات المكلفة بالتحري على التعامل مع الأدلة الرقمية بطريقة تضمن سلامتها وقابليتها للاستعمال أمام القضاء. فالحصول على البيانات لا يكفي وحده، وإنما ينبغي المحافظة عليها من التغيير أو الإتلاف وتوثيق كيفية الحصول عليها، بما يسمح بالتحقق من مصدرها وسلامة محتواها عند عرضها على الجهات القضائية³.

ويظهر من مجموع هذه الأحكام أن المشرع الجزائري اعتمد مجموعة من الآليات ذات الطبيعة التقنية والإجرائية للوقاية من الجرائم الإلكترونية ومراقبتها، تتراوح بين مراقبة الاتصالات وحفظ البيانات والوصول إلى المعطيات المخزنة، إلى جانب التنسيق بين الجهات المختصة. وقد حاول من خلال ذلك التوفيق بين فعالية مكافحة الجريمة الإلكترونية وبين ضرورة احترام الحقوق والحريات التي قد تتأثر باستعمال وسائل المراقبة والتحري.

¹ المادة 14، القانون رقم 09-04، سالف الذكر؛ وانظر كذلك: المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر سنة 2021، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

² المادة 4، القانون رقم 09-04، سالف الذكر.

³ جبراني نورة، لعماري سهام، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريش، 2025، ص 35-40.

وعليه، فإن التدابير الوقائية وآليات الرقابة التي أقرها المشرع الجزائري تشكل جانباً مهماً من منظومة مكافحة الجريمة الإلكترونية، لأنها تسمح بالتدخل للكشف عن النشاط الإجرامي وحفظ الأدلة الرقمية قبل ضياعها، غير أن فعاليتها تبقى مرتبطة باحترام الشروط والضمانات القانونية، وعلى رأسها الرقابة القضائية وحماية سرية الاتصالات والحياة الخاصة.

الفرع الثالث: التزامات مقدمي خدمات الاتصال في مكافحة الجريمة الإلكترونية

أحاط المشرع الجزائري مقدمي خدمات الاتصال بمجموعة من الالتزامات الخاصة في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالنظر إلى الدور الذي تؤديه هذه الجهات في توفير خدمات الاتصال ومعالجة وتخزين البيانات المتعلقة بها. وقد خصص القانون رقم 04-09 فصلاً كاملاً لهذه الالتزامات، ويميز بين واجب مساعدة السلطات المكلفة بالتحريات القضائية، وواجب حفظ المعطيات المتعلقة بحركة الاتصالات، فضلاً عن الالتزامات الخاصة بمقدمي خدمات الوصول إلى الإنترنت.¹

يقوم الالتزام الأول على مساعدة السلطات المكلفة بالتحريات القضائية، حيث ألزم المشرع مقدمي الخدمات بتقديم المساعدة اللازمة لجمع أو تسجيل البيانات المتعلقة بمحتوى الاتصالات في الوقت الحقيقي، ووضع المعطيات التي يلتزمون بحفظها تحت تصرف السلطات المختصة. ويهدف هذا الالتزام إلى تمكين الجهات المكلفة بالبحث والتحقيق من الوصول إلى المعلومات التقنية التي قد تكون ضرورية للكشف عن الجريمة وتحديد مرتكبها، خاصة عندما تكون البيانات محل البحث موجودة لدى مقدم الخدمة.²

ولم يجعل المشرع هذه المساعدة مفتوحة دون حدود، إذ ربطها بإطار تطبيق أحكام القانون وبطلبات السلطات المكلفة بالتحريات القضائية. كما ألزم مقدمي الخدمات بالمحافظة على سرية العمليات التي يقومون بها بناءً على طلب المحققين، وكذلك سرية المعلومات المرتبطة بها، ورتب على

¹ وداد بن سالم، عبد الله شيباني، «النظام القانوني لمقدمي خدمة الإنترنت في ظل القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها»، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 13، العدد 01، 2024، ص 59-74.

² المادة 10، القانون رقم 04-09، سالف الذكر.

الإخلال بهذا الالتزام إمكانية تطبيق العقوبات المتعلقة بإفشاء سر التحقيق والتحري.¹ ويحقق هذا الالتزام توازناً بين ضرورة التعاون مع السلطات القضائية وحماية سرية الإجراءات والمعلومات المتحصل عليها.

كما أوجب المشرع على مقدمي الخدمات حفظ المعطيات المتعلقة بحركة الاتصالات لمدة سنة واحدة ابتداءً من تاريخ تسجيلها. وتشمل هذه المعطيات، بحسب طبيعة ونوع الخدمة، البيانات التي تسمح بالتعرف على مستعملي الخدمة، والبيانات المتعلقة بالتجهيزات الطرفية المستعملة في الاتصال، والخصائص التقنية للاتصال وتاريخه ووقته ومدته، فضلاً عن البيانات المتعلقة بالخدمات الإضافية المطلوبة أو المستعملة ومقدميها، والبيانات التي تسمح بتحديد أطراف الاتصال وعناوين المواقع التي تمت زيارتها.²

وبالنسبة إلى نشاط الهاتف، ألزم المشرع المتعامل بحفظ البيانات التي تسمح بالتعرف على مستعمل الخدمة، إضافة إلى البيانات التي تسمح بتحديد موقع ومصدر الاتصال. وتكتسب هذه البيانات أهمية إجرائية، لأنها قد تساعد في تحديد مصدر الاتصال وربط نشاط معين بمستخدم أو جهاز أو مكان محدد، دون أن يعني ذلك أن مجرد وجود البيانات لدى مقدم الخدمة يكفي وحده لإثبات المسؤولية الجزائية، إذ تخضع قيمتها للتقدير القضائي ولمقتضيات الإثبات.³

وقد رتب المشرع على عدم احترام الالتزامات المتعلقة بحفظ المعطيات مسؤولية قانونية، إذ يمكن أن تترتب مسؤولية الأشخاص الطبيعيين والمعنويين عندما يؤدي الإخلال بهذه الالتزامات إلى عرقلة السير الحسن للتحريات القضائية. وبالنسبة للشخص الطبيعي، حدد القانون عقوبة الحبس من ستة أشهر إلى خمس سنوات وغرامة من 50.000 إلى 500.000 دينار، مع إخضاع الشخص المعنوي للغرامة وفق الأحكام المقررة في قانون العقوبات.⁴

¹ وداد بن سالم، عبد الله شيباني، مرجع سابق، ص 64-70.

² المادة 11، القانون رقم 09-04، سالف الذكر.

³ عماد يوسف، لزهو ضربان، مرجع سابق، ص 45-50.

⁴ المادة 11، القانون رقم 09-04، سالف الذكر.

وإلى جانب الالتزامات العامة المفروضة على مقدمي الخدمات، خص المشرع مقدمي خدمات الوصول إلى الإنترنت بالالتزامات إضافية، إذ ألزمهم بالتدخل دون تأخير لسحب المحتويات التي يسمحون بالوصول إليها عندما تكون محل مخالفة للقوانين، أو تخزينها أو جعلها غير قابلة للوصول إليها بمجرد علمهم بها، سواء كان العلم مباشراً أو غير مباشر. ويهدف هذا الالتزام إلى الحد من استمرار تداول المحتويات غير المشروعة داخل البيئة الإلكترونية.¹

كما ألزم مقدمي خدمات الوصول إلى الإنترنت بوضع أجهزة تقنية تسمح بالحد من إمكانية الوصول إلى الموزعين الذين يتضمنون معلومات مخالفة للنظام العام أو الآداب العامة، مع إعلام المشتركين بذلك. ويعكس هذا الالتزام توجهاً وقائياً لا يقتصر على التدخل بعد وقوع الجريمة، وإنما يهدف كذلك إلى الحد من إمكانية الوصول إلى بعض المحتويات غير المشروعة.²

وتظهر أهمية هذه الالتزامات من الناحية العملية في كون مقدم الخدمة يحتفظ ببيانات لا تتوافر عادة لدى الضحية أو السلطات بصورة مباشرة، الأمر الذي يجعله طرفاً أساسياً في عملية تتبع الأثر الرقمي. فبيانات التعريف بالمستخدم ومعلومات الاتصال والتجهيزات المستعملة وتاريخ ومدة الاتصال يمكن أن تساهم في تحديد مسار النشاط الإلكتروني محل التحقيق، خاصة عندما تكون الأدلة الأخرى قابلة للحذف أو التعديل.

غير أن إلزام مقدمي الخدمات بالتعاون مع السلطات لا يعني منح هذه الجهات صلاحية مطلقة في الكشف عن بيانات المستخدمين، وإنما يجب أن يتم ذلك وفق الإطار والإجراءات التي حددها القانون، وبما يراعي الضمانات المتعلقة بسرية الاتصالات والحياة الخاصة. وتزداد أهمية هذه الضمانات بالنظر إلى طبيعة البيانات التي يمكن الحصول عليها، والتي قد تسمح بالتعرف على عادات الاتصال والجهات التي تم التواصل معها وبعض المعلومات المرتبطة بالنشاط الإلكتروني للمستخدم.³

كما يرتبط التزام مقدمي الخدمات بحفظ البيانات بمبدأ سلامة الدليل الإلكتروني، إذ إن قيمة هذه البيانات في المجال الجزائي لا تتوقف على وجودها فقط، وإنما تتطلب الحفاظ عليها بطريقة

¹ وداد بن سالم، عبد الله شيباني، مرجع سابق، ص 64-70.

² المادة 12، القانون رقم 09-04، سالف الذكر.

³ أحمد مسعود مريم، مرجع سابق، ص 70-74.

تسمح بالتحقق من مصدرها ومضمونها وعدم تعرضها للتغيير. ولهذا فإن التعاون بين مقدمي الخدمات والسلطات القضائية يساهم في توفير عناصر إثبات يمكن الاستناد إليها في مراحل البحث والتحقيق والمحاكمة، مع بقاء تقدير حجيتها للجهة القضائية المختصة¹.

وعليه، يتضح أن المشرع الجزائري أسند إلى مقدمي خدمات الاتصال دورًا أساسيًا في منظومة مكافحة الجريمة الإلكترونية، من خلال مساعدة السلطات القضائية، وحفظ بيانات حركة الاتصالات لمدة سنة، والمحافظة على سرية العمليات، وسحب أو جعل بعض المحتويات غير المشروعة غير متاحة، ووضع آليات تقنية للحد من الوصول إلى المحتويات المخالفة. وتكشف هذه الالتزامات عن اعتماد المشرع على التعاون بين السلطات العامة والجهات التقنية الفاعلة في مجال الاتصالات لضمان فعالية مكافحة الجريمة الإلكترونية، مع ضرورة احترام الحدود القانونية والضمانات المرتبطة بالحقوق والحريات.

المبحث الثاني: الآليات الجزائية والإجرائية للجريمة الإلكترونية

تقتضي مكافحة الجريمة الإلكترونية توفير آليات جزائية وإجرائية تتلاءم مع طبيعة هذا النوع من الإجرام، إذ لا تكتمل الحماية القانونية بمجرد تجريم الأفعال وتحديد العقوبات المقررة لها، وإنما تستلزم كذلك وضع إجراءات خاصة تسمح بكشف الجرائم الإلكترونية والبحث عن مرتكبيها وضبط الأدلة الناتجة عنها. وقد أقر المشرع الجزائري، إلى جانب الأحكام العقابية الواردة في قانون العقوبات، قواعد خاصة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال، شملت مراقبة الاتصالات الإلكترونية والتفتيش والحجز في الأنظمة المعلوماتية وغيرها من الإجراءات الملائمة لطبيعة الدليل الرقمي. وعليه، سيتم تناول الإجراءات المقررة في الجريمة الإلكترونية من خلال دراسة العقوبات الأصلية والتكميلية والظروف المؤثرة فيها، ثم التطرق إلى الخصوصية الإجرائية في الجرائم الإلكترونية من خلال البحث والتحري والتفتيش وضبط الأدلة الإلكترونية وحجيتها وإجراءات الحفاظ عليها.

¹ جبراني نورة، لعماري سهام، مرجع سابق، ص 45-50.

المطلب الأول: الجزاءات المقررة في الجريمة الإلكترونية

تتطلب مواجهة الجريمة الإلكترونية إقرار جزاءات جنائية تتناسب مع خطورة الأفعال المرتكبة والنتائج المترتبة عنها، وقد أقر المشرع الجزائري ضمن قانون العقوبات عقوبات سالبة للحرية وعقوبات مالية بالنسبة لمختلف صور المساس بأنظمة المعالجة الآلية للمعطيات، كما قرر بعض العقوبات التكميلية والتدابير التي تهدف إلى الحد من آثار الجريمة ومنع استعمال الوسائل المستخدمة في ارتكابها، فضلاً عن تشديد العقوبة في حالات معينة بالنظر إلى طبيعة الجريمة أو محلها أو الظروف المحيطة بارتكابها. وعليه، سيتم تناول العقوبات الأصلية المقررة للجرائم الإلكترونية في الفرع الأول، ثم العقوبات التكميلية والتدابير المقررة في الفرع الثاني، وأخيراً تشديد العقوبة والظروف المؤثرة فيها في الفرع الثالث.

الفرع الأول: العقوبات الأصلية المقررة للجرائم الإلكترونية

أحاط المشرع الجزائري الجرائم المرتكبة ضد أنظمة المعالجة الآلية للمعطيات بجملة من العقوبات الأصلية، تتنوع بين العقوبات السالبة للحرية والغرامات المالية، مع اختلاف مقدارها بحسب طبيعة السلوك الإجرامي والنتيجة المترتبة عنه. وتظهر هذه السياسة العقابية من خلال المواد 394 مكرر وما يليها من قانون العقوبات، التي تدرجت في تحديد الجزاء بحسب درجة خطورة الاعتداء، سواء تعلق الأمر بالدخول أو البقاء غير المشروع في النظام، أو المساس بالمعطيات، أو تخريب نظام اشتغاله، أو استعمال الوسائل المعدة لارتكاب هذه الجرائم.¹

فبالنسبة إلى جريمة الدخول أو البقاء بطريق الغش في منظومة المعالجة الآلية للمعطيات أو محاولة ذلك، نصت المادة 394 مكرر، في صيغتها المعدلة بموجب القانون رقم 24-06، على عقوبة الحبس من ستة أشهر إلى سنتين، وغرامة من 60.000 إلى 200.000 دج. وقد ربط المشرع تشديد الجزاء بالنتيجة التي تترتب عن الفعل، إذ تضاعف العقوبة إذا أدى الدخول غير المشروع إلى حذف أو تغيير معطيات المنظومة، بينما تصل العقوبة إلى الحبس من سنة إلى ثلاث

¹ أمنية بصافة، «الأطر القانونية للجريمة السيبرانية في التشريع الجزائري بين الوقاية والمكافحة»، مجلة الدراسات الأكاديمية، المجلد 37، العدد 01، 2023، ص 110-106.

سنوات وغرامة من 100.000 إلى 300.000 دج إذا ترتب عن الأفعال تخريب نظام اشتغال المنظومة.¹

أما جريمة إدخال المعطيات بطريق الغش أو إزالتها أو تعديلها، فقد خصها المشرع بعقوبة أشد بالنظر إلى أن الفعل لا يقتصر على مجرد الولوج إلى النظام، وإنما يمتد إلى التأثير المباشر في محتواه المعلوماتي. وتنص المادة 394 مكرر 1 على الحبس من سنة إلى ثلاث سنوات، وغرامة من 500.000 إلى 2.000.000 دج لكل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.²

كما جرم المشرع بعض الأفعال المرتبطة بتوفير الوسائل والبيانات المعدة لارتكاب الجرائم المعلوماتية، حيث تعاقب المادة 394 مكرر 2 الأفعال المتعلقة بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات يمكن أن ترتكب بها الجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات. كما تشمل الحماية حيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم المذكورة، وهو ما يكشف عن توجه المشرع نحو عدم الاقتصار على معاقبة الاعتداء المكتمل، وإنما مواجهة بعض الأفعال المرتبطة به متى توافرت شروط التجريم.³

وتشمل العقوبات الأصلية كذلك الغرامات المقررة للأشخاص المعنوية، إذ لم يحصر المشرع المسؤولية في الشخص الطبيعي، وإنما قرر بالنسبة للشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم غرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. ويعكس ذلك إدراكًا لإمكانية ارتكاب الجرائم المعلوماتية في إطار المؤسسات والشركات والهيئات، وليس فقط من طرف أفراد مستقلين.⁴

¹ المادة 394 مكرر، الأمر رقم 66-156، سالف الذكر، المعدل والمتمم بالقانون رقم 24-06.

² المادة 394 مكرر 1، الأمر رقم 66-156، سالف الذكر.

³ المادة 394 مكرر 2، الأمر رقم 66-156، سالف الذكر؛ وانظر كذلك: عزالدين عثمان، «صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات»، مجلة الدراسات والبحوث القانونية، 2019.

⁴ المادة 394 مكرر 4، الأمر رقم 66-156، سالف الذكر؛ وانظر: بدر الدين خلاف، «التنظيم القانوني للجريمة المعلوماتية في الجزائر»، مجلة العلوم القانونية والاجتماعية، 2016.

وقد اعتمد المشرع في تحديد العقوبات على التدرج العقابي، بحيث تتفاوت شدة الجزاء بحسب خطورة السلوك والنتيجة التي أحدثها. فالدخول أو البقاء غير المشروع لا يعامل بالعقوبة نفسها المقررة لإدخال أو حذف أو تعديل المعطيات، كما تختلف العقوبة عندما يؤدي الاعتداء إلى تخريب نظام اشتغال المنظومة. ويمنح هذا التدرج القاضي إطاراً قانونياً يراعي اختلاف درجة الخطورة بين صور الاعتداء المختلفة¹.

كما شدد المشرع العقوبة في حالة تعلق الجريمة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، إذ تضاعف العقوبات المقررة للجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات، دون الإخلال بتطبيق العقوبات الأشد عند الاقتضاء.² ويستند هذا التشديد إلى طبيعة المصالح التي يمكن أن تتعرض للخطر عندما يستهدف الاعتداء أنظمة مرتبطة بالدولة أو بالمرافق والهيئات العامة.

ولا تقتصر السياسة العقابية على الجريمة التامة، إذ قرر المشرع الجزائري معاقبة الشروع في ارتكاب الجناح المنصوص عليها في هذا القسم بالعقوبات المقررة للجريمة ذاتها.³ ويكتسب ذلك أهمية خاصة في مجال الجرائم الإلكترونية، لأن النشاط الإجرامي قد يتوقف قبل تحقق النتيجة المقصودة بسبب تدخل تقني أو اكتشاف المحاولة أو فشل الوسيلة المستخدمة، دون أن يعني ذلك بالضرورة انتفاء الخطر الذي استهدف النظام المعلوماتي.⁴

ومن خلال هذه الأحكام يتضح أن العقوبات الأصلية المقررة للجرائم الإلكترونية في التشريع الجزائري تقوم على الجمع بين الحبس والغرامة، مع التدرج في مقدار الجزاء بحسب طبيعة الاعتداء ونتيجته، فضلاً عن امتداد المسؤولية إلى الشخص المعنوي ومعاقبة الشروع وتشديد العقوبات في الحالات التي تمس مصالح ذات أهمية خاصة. ويكشف ذلك عن اتجاه المشرع إلى توفير حماية جنائية تتلاءم مع خطورة الاعتداء على الأنظمة المعلوماتية والمعطيات التي تحتويها.

¹ أمنية بصفة، مرجع سابق، ص 106-110.

² المادة 394 مكرر 3، الأمر رقم 66-156، سالف الذكر، المعدلة بموجب القانون رقم 24-06.

³ المادة 394 مكرر 7، الأمر رقم 66-156، سالف الذكر.

⁴ فيصل نسيغة، عبير بعقلي، «الآليات القانونية الموضوعية لمكافحة الجريمة المعلوماتية»، مجلة الحقوق والعلوم الإنسانية، المجلد 04، العدد 02، 2011، ص 73-75.

وعليه، فإن الجزاء الأصلي في الجرائم الإلكترونية لا يأخذ صورة عقوبة واحدة موحدة، وإنما يتحدد وفقاً للتكييف القانوني للفعل والنتيجة المترتبة عنه والظروف التي ارتكب فيها، وهو ما يسمح بتحقيق قدر من التناسب بين خطورة الجريمة والجزاء المقرر لها، مع إبقاء العقوبات التكميلية والتدابير المقررة كوسائل إضافية للحد من آثار الجريمة، وهو ما سيتم بيانه في الفرع الموالي.

الفرع الثاني: العقوبات التكميلية والتدابير المقررة

لا تقتصر المواجهة الجزائية للجريمة الإلكترونية على العقوبات الأصلية المتمثلة في الحبس والغرامة، وإنما تمتد إلى مجموعة من العقوبات التكميلية والتدابير التي تهدف إلى الحد من الآثار المترتبة عن الجريمة ومنع استمرار النشاط الإجرامي أو إعادة ارتكابه. وتكتسب هذه الجزاءات أهمية خاصة في الجرائم الإلكترونية بالنظر إلى إمكانية ارتباط الجريمة بأجهزة وبرامج ووسائل تقنية استعملت في تنفيذها أو نتجت عنها، الأمر الذي يبرر إخضاع بعض هذه الوسائل لإجراءات المصادرة أو غيرها من الجزاءات التي يقرها القانون.¹

ويأتي المصادرة في مقدمة العقوبات التكميلية التي يمكن أن يكون لها تطبيق في المجال الإلكتروني، إذ تسمح بتجريد المحكوم عليه من الأشياء التي استعملت في ارتكاب الجريمة أو التي تحصلت منها، متى توافرت الشروط القانونية لذلك. وتكتسب المصادرة خصوصية في الجرائم الإلكترونية، لأن محلها قد يكون جهاز حاسوب أو معدات إلكترونية أو وسائط تخزين أو برامج أو غيرها من الأدوات التي ارتبط استعمالها بالفعل الإجرامي. وقد أدرج المشرع المصادرة ضمن العقوبات التكميلية المطبقة على الأشخاص المعنوية، كما جعلها من الوسائل التي يمكن أن تنصب على الشيء المستعمل في ارتكاب الجريمة أو الناتج عنها.²

وتظهر أهمية المصادرة بصورة أوضح بالنسبة إلى الأشخاص المعنوية، حيث نصت المادة 18 مكرر من قانون العقوبات على إمكانية الحكم عليها بالمصادرة، إلى جانب مجموعة من العقوبات التكميلية الأخرى، كحل الشخص المعنوي، وغلق المؤسسة أو أحد فروعها لمدة محددة، والإقصاء من الصفقات العمومية، والمنع من ممارسة نشاط مهني أو اجتماعي، فضلاً عن نشر أو تعليق حكم

¹ محمد حزيط، المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري، الجزائر، دار هومة للطباعة والنشر والتوزيع، 2014، ص 147-152.

² المادة 394 مكرر 6، الأمر رقم 66-156، سالف الذكر؛ وانظر كذلك: فيصل نسيغة، عبير بعقلي، مرجع سابق، ص 73-75.

الإدانة ووضع الشخص المعنوي تحت الرقابة القضائية.¹ وتسمح هذه الأحكام بمواجهة الحالات التي ترتكب فيها الجريمة الإلكترونية في إطار نشاط مؤسسة أو شركة وتتوفر شروط المسؤولية الجزائية للشخص المعنوي.

كما يمكن أن تمتد العقوبات التكميلية إلى غلق المؤسسة أو أحد فروعها، وهو جزاء قد تكون له أهمية عندما ترتبط الجريمة بالنشاط الذي تمارسه المؤسسة أو بالمكان الذي وقع فيه الفعل الإجرامي. وقد حدد المشرع مدة الغلق بالنسبة للشخص المعنوي بما لا يتجاوز خمس سنوات، الأمر الذي يجعل هذا الجزاء وسيلة للحد من استمرار النشاط الذي ساهم في ارتكاب الجريمة، مع مراعاة الشروط التي يفرضها القانون.²

ومن الجزاءات التي يمكن تطبيقها كذلك المنع من ممارسة نشاط مهني أو اجتماعي، سواء بصورة نهائية أو لمدة لا تتجاوز خمس سنوات بالنسبة للشخص المعنوي، متى كانت الجريمة مرتبطة بالنشاط محل المنع. وتكمن أهمية هذا الجزاء في إمكانية استخدام بعض الأنشطة المهنية أو التجارية كغطاء لارتكاب جرائم إلكترونية أو تسهيلها، وبالتالي فإن منع الشخص المعنوي من ممارسة النشاط الذي ارتبط بالجريمة قد يساهم في الحد من تكرارها.³

كما أتاح المشرع الإقصاء من الصفقات العمومية كعقوبة تكميلية للشخص المعنوي لمدة لا تتجاوز خمس سنوات. ويكون لهذا الجزاء أثر اقتصادي وقانوني مهم بالنسبة للمؤسسات التي تعتمد على التعامل مع الهيئات العمومية، إذ يحرم الشخص المعنوي المحكوم عليه من المشاركة في الصفقات العمومية خلال المدة المحددة في الحكم، وفقاً للشروط القانونية.⁴

ومن التدابير ذات الصلة كذلك الوضع تحت الرقابة القضائية بالنسبة للشخص المعنوي، لمدة لا تتجاوز خمس سنوات، عندما يكون النشاط الذي يمارسه مرتبباً بالجريمة التي أدت إلى إدانته.

¹ المادة 18 مكرر، الأمر رقم 66-156، سالف الذكر.

² المادة 18 مكرر، الأمر رقم 66-156، سالف الذكر.

³ المادة 18 مكرر، الأمر رقم 66-156، سالف الذكر.

⁴ المادة 18 مكرر، الأمر رقم 66-156، سالف الذكر.

وتسمح هذه الآلية بإخضاع النشاط محل الجريمة للمتابعة والرقابة بدل الاكتفاء بالجزاء المالي، بما يساهم في منع تكرار الأفعال التي أدت إلى المسؤولية الجزائية.¹

كما يمكن أن تشمل العقوبات التكميلية نشر وتعليق حكم الإدانة، وهو جزاء يمس الجانب المعنوي والمهني للشخص المحكوم عليه، ويهدف إلى إعلام الغير بالحكم الصادر ضده وفق الحدود والكيفية التي يحددها القضاء والقانون. وتبرز أهمية هذا الجزاء بالنسبة للأشخاص المعنوية التي تعتمد على الثقة والسمعة في ممارسة نشاطها، خاصة في المجالات التي ترتبط بإدارة البيانات أو تقديم الخدمات الرقمية.²

وفي المجال الإلكتروني تحديداً، تكتسب مصادرة البرامج والأدوات والوسائل المستعملة في ارتكاب الجريمة أهمية خاصة، لأن استمرار حيازة هذه الوسائل قد يسمح بإعادة استعمالها في ارتكاب أفعال مماثلة. وقد نصت الأحكام الخاصة بالمساحات بأنظمة المعالجة الآلية للمعطيات على مصادرة الأدوات والبرامج والوسائل المستعملة في ارتكاب الجرائم، مع مراعاة حقوق الغير حسن النية، كما قررت إغلاق المواقع محل الجرائم في الحالات والشروط التي حددها النص.³

ويكشف ذلك عن خصوصية الجزاء في الجريمة الإلكترونية، إذ لا يهدف فقط إلى معاقبة الجاني بعد ارتكاب الفعل، وإنما يسعى كذلك إلى إزالة الوسائل التي يمكن أن يستمر من خلالها النشاط الإجرامي. فمصادرة المعدات أو البرامج المستعملة في الجريمة، وإغلاق المواقع التي كانت محلاً لبعض الجرائم، يمكن أن يمنع استمرار الضرر أو إعادة استخدام الوسائل ذاتها في ارتكاب جرائم أخرى.

وتتصل هذه التدابير كذلك بفكرة الوقاية الخاصة، لأنها تستهدف تقليل احتمال عودة الجاني إلى استعمال الوسائل أو النشاط الذي ارتبط بالجريمة. غير أن تطبيقها يظل خاضعاً لمبدأ الشرعية

¹ المادة 18 مكرر، الأمر رقم 66-156، سالف الذكر.

² عبد القادر عدو، مبادئ قانون العقوبات الجزائري: القسم العام، الجزائر، دار هومة للطباعة والنشر والتوزيع.

³ المادة 394 مكرر 6، الأمر رقم 66-156، سالف الذكر.

وباقى الضمانات القانونية، ولا سيما حماية حقوق الغير حسن النية، وهو ما يظهر صراحة في النصوص التي قررت المصادرة في مجال الجرائم المعلوماتية.¹

كما ينبغي التمييز بين العقوبة التكميلية والتدبير الاحترازي، فالعقوبة التكميلية ترتبط بالحكم بالإدانة وتضاف إلى العقوبة الأصلية وفقاً لما يسمح به القانون، بينما يرتبط التدبير الاحترازي بفكرة مواجهة الخطورة الإجرامية أو منع استمرار آثار الجريمة. ويكتسب هذا التمييز أهمية في المجال الإلكتروني، لأن بعض الإجراءات المتعلقة بالأجهزة والبرامج والمواقع قد تهدف إلى منع استمرار الجريمة أكثر مما تهدف إلى تحقيق الردع العقابي وحده.²

وعليه، فإن العقوبات التكميلية والتدابير المقررة في مواجهة الجريمة الإلكترونية تسعى إلى استكمال العقوبات الأصلية من خلال مصادرة الوسائل والأدوات المستعملة في الجريمة، وغلق بعض المواقع أو المؤسسات، والمنع من بعض الأنشطة، والإقصاء من الصفقات العمومية، والرقابة القضائية، ونشر حكم الإدانة بحسب طبيعة المحكوم عليه وشروط كل جزء. وتساهم هذه الآليات في تحقيق حماية أكثر فعالية للنظام المعلوماتي، لأنها لا تقتصر على معاقبة مرتكب الجريمة وإنما تمتد إلى الوسائل والبيئة التي ساهمت في ارتكابها.

الفرع الثالث: تشديد العقوبة للجريمة الالكترونية

لم يكتف المشرع الجزائري بتحديد عقوبات موحدة لمختلف الجرائم الإلكترونية، وإنما أخذ بعين الاعتبار بعض الظروف التي من شأنها التأثير في جسامة الفعل الإجرامي، وبالتالي في مقدار العقوبة المقررة له. ويرتبط تشديد العقوبة في هذا المجال أساساً بطبيعة النظام المعلوماتي أو المعطيات محل الاعتداء، والنتائج المترتبة عن الفعل، والوسائل المستعملة في ارتكابه، إضافة إلى صفة الجاني أو الأشخاص والهيئات المستهدفة، بما يحقق قدرًا من التناسب بين خطورة السلوك والجزاء الجنائي المقرر له.³

¹ فيصل نسيقة، عبير بعقلي، مرجع سابق، ص ص 73-75.

² عبد القادر عدو، مرجع سابق.

³ طيب موفق شريف، «التوقيع الإلكتروني وحمايته جنائياً في القانون الجزائري»، المجلة الإفريقية للدراسات القانونية والسياسية، المجلد 01، العدد 01، 2017، ص ص 76-87.

ويظهر التشديد أولاً من خلال النتيجة المترتبة عن الدخول أو البقاء غير المشروع في النظام المعلوماتي، حيث لم يعامل المشرع الدخول غير المشروع معاملة واحدة، بل رتب عقوبة أشد عندما يؤدي هذا الفعل إلى حذف أو تغيير المعطيات الموجودة في النظام، كما رفع مقدار العقوبة عندما يصل الاعتداء إلى تخريب نظام اشتغال المنظومة. ويكشف هذا التدرج عن اعتماد المشرع على معيار النتيجة الإجرامية في تحديد درجة الخطورة.¹

وتتجلى صورة أخرى للتشديد عندما تكون الجريمة موجهة ضد أنظمة المعالجة الآلية للمعطيات التابعة للدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام، حيث قرر المشرع مضاعفة العقوبات المقررة للجرائم المنصوص عليها في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات. ويستند هذا التشديد إلى أهمية الأنظمة المستهدفة وما يمكن أن يترتب عن الاعتداء عليها من أضرار تتجاوز المصلحة الخاصة إلى المساس بالمصالح العامة للدولة.²

كما أخذ المشرع بعين الاعتبار صفة الجاني في بعض الجرائم المرتبطة بالبيئة المعلوماتية، إذ قد تزداد خطورة الفعل عندما يرتكبه شخص بحكم وظيفته أو مهنته يكون مؤتمناً على النظام أو المعطيات محل الاعتداء. فاستغلال الصلاحيات أو النفاذ المشروع إلى المعلومات من أجل تحقيق غرض إجرامي يختلف في درجة خطورته عن الاعتداء الصادر عن شخص لا تربطه علاقة بالنظام، لما ينطوي عليه من إخلال بالثقة واستغلال للسلطة أو الوظيفة.

ويؤثر كذلك تعدد الأشخاص المشتركين في ارتكاب الجريمة في تقدير المسؤولية والعقوبة، متى توافرت شروط المساهمة أو الاشتراك المنصوص عليها في قانون العقوبات. وتزداد أهمية ذلك في الجرائم الإلكترونية بسبب إمكانية توزيع الأدوار بين عدة أشخاص، فقد يتولى أحدهم اختراق النظام، بينما يقوم آخر باستخراج البيانات، ويتولى ثالث استعمالها لتحقيق منفعة غير مشروعة. ويخضع تحديد

¹ المادة 394 مكرر، الأمر رقم 66-156، سالف الذكر.

² المادة 394 مكرر 3، الأمر رقم 66-156، سالف الذكر.

مسؤولية كل مساهم للقواعد العامة للمساهمة الجنائية، مع مراعاة الدور الذي قام به كل شخص في تنفيذ الجريمة.¹

ومن الظروف المؤثرة كذلك الشروع في ارتكاب الجريمة، حيث قرر المشرع الجزائري بالنسبة للجنح المنصوص عليها في القسم المتعلق بالمساحات بأنظمة المعالجة الآلية للمعطيات معاقبة الشروع بالعقوبات المقررة للجريمة ذاتها. ويكتسب هذا الحكم أهمية خاصة في الجرائم الإلكترونية، لأن النشاط الإجرامي قد يتوقف قبل تحقيق النتيجة بسبب اكتشاف الاختراق أو فشل الوسيلة التقنية المستعملة، ومع ذلك يبقى السلوك محل تجريم متى تحققت شروط الشروع.²

كما قد تؤثر الطبيعة الخاصة للبيانات محل الاعتداء في التكييف القانوني للفعل والعقوبة المقررة له، خصوصاً عندما يتعلق الأمر بالمعطيات ذات الطابع الشخصي. فقد أقر المشرع الجزائري نظاماً خاصاً لحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وقرر جزاءات على بعض الأفعال التي تمس هذه المعطيات بالمخالفة للأحكام القانونية.³ ومن ثم، قد تخضع الواقعة إلى أحكام خاصة بالإضافة إلى النصوص العامة، بحسب طبيعة البيانات والسلوك المرتكب.

وتتصل شدة الجزاء كذلك بصفة الشخص المتضرر وطبيعة المصلحة المعتدى عليها، فالجريمة التي تستهدف نظاماً معلوماتياً تابعاً لهيئة عمومية أو مؤسسة ذات أهمية عامة قد تكون أكثر خطورة من الاعتداء على نظام ذي طبيعة خاصة، خصوصاً عندما يؤدي الفعل إلى تعطيل خدمة أو المساس بسير مرفق عمومي. ولهذا اتجه المشرع إلى إقرار حماية أكثر صرامة بالنسبة لبعض الأنظمة ذات الأهمية الخاصة.

ومن جهة أخرى، يمكن أن تؤثر الظروف المخففة والأعذار القانونية في العقوبة متى توافرت شروطها، إذ لا يعني تشديد العقوبة في بعض الجرائم الإلكترونية استبعاد تطبيق القواعد العامة التي

¹ المادة 41 وما بعدها، الأمر رقم 66-156، سالف الذكر؛ وانظر كذلك: سارة مهنوي، «الجريمة المعلوماتية في التشريع الجزائري»، مجلة الدراسات والبحوث القانونية، المجلد 08، العدد 02، 2019، ص 161.

² المادة 394 مكرر 7، الأمر رقم 66-156، سالف الذكر؛ وانظر: سارة مهنوي، مرجع سابق، ص 161.

³ القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، 10 يونيو سنة 2018.

تحكم تقدير الجزاء الجنائي. فالقاضي يلتزم بالنص القانوني من حيث الحد الأدنى والأقصى، مع مراعاة الظروف التي يسمح القانون بأخذها في الاعتبار عند تحديد العقوبة.¹

كما أن تعدد الجرائم أو ارتباط الجريمة الإلكترونية بجرائم أخرى يمكن أن يؤثر في تحديد العقوبة وفقاً لقواعد تعدد الجرائم المنصوص عليها في قانون العقوبات. فقد يرتكب الجاني، في واقعة واحدة أو في وقائع مترابطة، جريمة الدخول غير المشروع إلى نظام معلوماتي ثم يقوم بسرقة البيانات أو استعمالها في الاحتيال أو الابتزاز. وفي هذه الحالة ينبغي تحديد الوصف القانوني لكل فعل وتطبيق القواعد الخاصة بالتعدد وفقاً للوقائع والنصوص المنطبقة.²

ويأخذ التشديد صورة خاصة عندما يتعلق الأمر بالشخص المعنوي، إذ أقر المشرع مسؤولية الشخص المعنوي عن الجرائم وفق الشروط التي حددها القانون، وقرر له عقوبات تتلاءم مع طبيعته، من بينها الغرامة والعقوبات التكميلية. وتزداد أهمية ذلك في الجرائم الإلكترونية التي قد ترتكب داخل الشركات والمؤسسات من خلال استغلال البنية التحتية أو الموارد التقنية المتاحة فيها، متى ثبتت المسؤولية الجزائية للشخص المعنوي وفق القواعد القانونية.³

وعليه، يتضح أن تشديد العقوبة في الجرائم الإلكترونية يقوم على مجموعة من الاعتبارات التي ترتبط بخطورة النتيجة، وطبيعة النظام أو البيانات المستهدفة، وصفة الجاني، والظروف التي أحاطت بارتكاب الجريمة، وتعدد الجرائم أو المساهمين فيها. وقد سعى المشرع الجزائري من خلال ذلك إلى تحقيق التناسب بين الجزاء وخطورة الاعتداء، بحيث لا تكون العقوبة واحدة بالنسبة إلى جميع الصور، وإنما تتدرج بحسب جسامة الفعل والآثار التي يمكن أن تترتب عنه.⁴

¹ المواد 53 مكرر 4 وما يليها، الأمر رقم 66-156، سالف الذكر؛ وانظر: عبد القادر عدو، مرجع سابق.

² المواد 32 وما يليها، الأمر رقم 66-156، سالف الذكر؛ وانظر: محمد حزيط، مرجع سابق.

³ المادة 51 مكرر، الأمر رقم 66-156، سالف الذكر؛ والمادة 394 مكرر 4، الأمر نفسه.

⁴ خليفني فنيحة، مهداوي محمد صالح، «حجية الدليل الإلكتروني في إثبات الاعتداءات المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 2 من قانون العقوبات الجزائري»، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 61، العدد 04، 2024، ص ص 350-370.

المطلب الثاني: الخصوصية الإجرائية في الجرائم الإلكترونية

تفرض الطبيعة التقنية للجرائم الإلكترونية خصوصية على الإجراءات الجزائية المتعلقة بكشفها وإثباتها، إذ غالبًا ما تتطلب عملية البحث عن مرتكبيها الاستعانة بوسائل تقنية متخصصة للوصول إلى البيانات والمعلومات المرتبطة بالفعل الإجرامي. وقد أقر المشرع الجزائري أحكامًا إجرائية خاصة تسمح للجهات المختصة بإجراء التحريات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وإجراء التفتيش والبحث داخل الأنظمة المعلوماتية وضبط البيانات والوسائط الإلكترونية، إلى جانب وضع قواعد تتعلق بحفظ المعطيات وضمان سلامتها للاستناد إليها أمام القضاء. وعليه، سيتم تناول إجراءات البحث والتحري في الجرائم الإلكترونية في الفرع الأول، ثم التفتيش وضبط الأدلة الإلكترونية في الفرع الثاني، وأخيرًا حجية الدليل الإلكتروني وإجراءات الحفاظ عليه في الفرع الثالث.

الفرع الأول: إجراءات البحث والتحري في الجرائم الإلكترونية

تتميز إجراءات البحث والتحري في الجرائم الإلكترونية بخصوصية تفرضها طبيعة البيئة الرقمية التي ترتكب فيها هذه الجرائم، إذ قد لا تترك الجريمة آثارًا مادية تقليدية يمكن معابنتها بالوسائل المعتادة، وإنما تخلف بيانات رقمية موزعة بين أجهزة وأنظمة وشبكات مختلفة. لذلك اعتمد المشرع الجزائري، إلى جانب القواعد العامة للبحث والتحري، مجموعة من الوسائل التي تسمح للجهات المختصة بجمع المعلومات والكشف عن مرتكبي الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، مع إخضاع هذه الإجراءات للرقابة والضوابط القانونية¹

وتتولى الشرطة القضائية مهمة البحث والتحري عن الجرائم وجمع الأدلة والبحث عن مرتكبيها والمساهمين فيها، ما لم يبدأ فيها تحقيق قضائي. وقد أكد قانون الإجراءات الجزائية الجديد هذا الاختصاص، حيث وضع الشرطة القضائية تحت إشراف النيابة العامة ورقابة غرفة الاتهام، بما يضمن خضوع أعمال البحث والتحري للإطار القانوني المحدد لها.² وتكتسب هذه القواعد أهمية خاصة في

¹ نادية أيت عبد المالك، عبد القادر فلاح، «التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري»، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 2020، ص ص 1689-1708.

² المادة 47، القانون رقم 25-14 المؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 54، 13 غشت سنة 2025.

الجرائم الإلكترونية بالنظر إلى ضرورة التدخل السريع لحماية الأدلة الرقمية قبل حذفها أو تعديلها أو نقلها.

ولا تقتصر أعمال البحث والتحري في هذا المجال على المعايير التقليدية، وإنما يمكن أن تتطلب الاستعانة بالوسائل التقنية المتخصصة، سواء تعلق الأمر بفحص الأنظمة المعلوماتية أو تتبع البيانات الرقمية أو الاستعانة بالخبرة التقنية لتحديد مصدر النشاط الإجرامي. وقد أقر القانون رقم 04-09 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مجموعة من الإجراءات الخاصة التي تستجيب لهذه الطبيعة التقنية، ومن بينها مراقبة الاتصالات الإلكترونية، وجمع وتسجيل البيانات المتعلقة بالاتصالات، والحفظ العاجل للبيانات، إضافة إلى إجراءات البحث داخل المنظومات المعلوماتية.¹

ويأخذ البحث والتحري الإلكتروني كذلك صورة اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية والإلكترونية، متى توافرت الشروط القانونية اللازمة لذلك. وتسمح هذه الوسيلة بالحصول على معلومات قد تكون ذات أهمية في كشف النشاط الإجرامي، غير أن استعمالها لا يتم بصورة تلقائية، وإنما يرتبط بالجرائم والحالات التي أجاز فيها القانون اللجوء إليها وبالإذن والرقابة القضائية المقررين قانوناً.²

كما أتاح المشرع استخدام بعض أساليب البحث والتحري الخاصة التي تتلاءم مع الجرائم المستحدثة، ومنها التردد الإلكتروني والتسرب، متى توافرت شروطها القانونية. وتسمح هذه الوسائل للجهات المختصة بجمع المعلومات حول النشاط الإجرامي دون الاقتصار على الوسائل التقليدية التي قد تكون غير كافية في مواجهة مجرم يستخدم وسائل تقنية لإخفاء هويته أو نشاطه. وقد أكدت الدراسات القانونية الجزائرية أن قصور الوسائل التقليدية أمام الجرائم المعلوماتية دفع المشرع إلى إدخال أساليب بحث وتحري خاصة تخضع لضمانات قانونية محددة.³

¹ المواد 3 إلى 8، القانون رقم 04-09، سالف الذكر.

² المادتان 3 و4، القانون رقم 04-09، سالف الذكر.

³ نادية أيت عبد المالك، عبد القادر فلاح، مرجع سابق، ص ص 1689-1708.

ويكتسب التسرب الإلكتروني أهمية خاصة في بعض صور الجرائم الإلكترونية، حيث يمكن لضابط الشرطة القضائية، تحت رقابة السلطة القضائية المختصة، الولوج إلى منظومة معلوماتية أو نظام اتصالات إلكترونية قصد مراقبة الأشخاص المشتبه في ارتكابهم الجرائم المحددة قانوناً، وذلك من خلال إيهامهم بأنه فاعل معهم أو شريك لهم. وبظل هذا الأسلوب محكوماً بضوابط دقيقة، فلا يجوز أن يتحول تدخل الضابط إلى تحريض المشتبه فيه على ارتكاب الجريمة.¹

ومن الوسائل التي يمكن أن تستعملها الجهات المختصة كذلك جمع المعطيات المتعلقة بحركة الاتصالات في الوقت الفعلي، وهو إجراء يسمح بتحديد بعض البيانات التقنية المرتبطة بالاتصال، مثل مصدر الاتصال ووجهته وتاريخ إجرائه ومدته، بما يساعد على تكوين صورة عن النشاط الإلكتروني محل البحث. وتبرز أهمية هذا الإجراء في الحالات التي تكون فيها هوية مرتكب الجريمة غير معلومة أو عندما يتم استعمال وسائل تقنية لإخفاء مصدر الاتصال.²

كما نظم المشرع الحفظ العاجل للبيانات المعلوماتية، وهو إجراء تفرضه الطبيعة المتغيرة للدليل الرقمي؛ إذ يمكن للبيانات الإلكترونية أن تختفي أو تتغير بمجرد حذفها أو تعديلها من قبل المستخدم أو بفعل النظام التقني. ويسمح الحفظ العاجل بتثبيت البيانات الموجودة لدى الجهات الحائزة لها إلى حين اتخاذ الإجراءات القضائية اللازمة للحصول عليها واستعمالها في التحقيق.³

ولا تنفصل هذه الإجراءات عن دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، التي أنشأها القانون رقم 04-09، وأسند إليها مهام تتعلق بتنشيط وتنسيق عمليات الوقاية والمكافحة، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية، فضلاً عن تبادل المعلومات مع نظيراتها في الخارج.⁴ ويساهم هذا الدور في توفير الدعم التقني والمعلوماتي للجهات المكلفة بالبحث والتحري.

¹ المواد المتعلقة بأساليب البحث والتحري الخاصة، القانون رقم 25-14، سالف الذكر.

² المادة 10، القانون رقم 04-09، سالف الذكر.

³ المادة 11، القانون رقم 04-09، سالف الذكر.

⁴ المادتان 13 و14، القانون رقم 04-09، سالف الذكر.

كما أن الطابع العابر للحدود للجرائم الإلكترونية قد يفرض التعاون القضائي الدولي أثناء مرحلة البحث والتحري، خاصة عندما تكون البيانات أو الأنظمة المعلوماتية الموجودة محل التحقيق موجودة خارج الإقليم الوطني. وقد سمح القانون رقم 04-09 للسلطات المختصة بتبادل المساعدة القضائية الدولية من أجل جمع الأدلة ذات الشكل الإلكتروني وكشف مرتكبي الجرائم المشمولة بأحكامه.¹

ويظل استعمال وسائل البحث والتحري الخاصة مقيداً بمبدأ المشروعية الإجرائية، فلا يكفي أن تكون الوسيلة قادرة تقنياً على الوصول إلى البيانات، وإنما يجب أن يكون استخدامها مستنداً إلى نص قانوني وأن يتم وفق الشروط والإجراءات التي حددها المشرع. وتكتسب هذه الضمانة أهمية أكبر عندما يتعلق الإجراء بسرية الاتصالات أو الحياة الخاصة، لأن البحث عن الجريمة لا ينبغي أن يتحول إلى مساس غير مشروع بحقوق الأفراد وحرياتهم.²

ومن ثم، فإن إجراءات البحث والتحري في الجرائم الإلكترونية تجمع بين القواعد التقليدية للضبط القضائي والوسائل التقنية الخاصة التي فرضتها البيئة الرقمية، بما يسمح للجهات المختصة بتحديد مرتكبي الجرائم وجمع الأدلة الإلكترونية والمحافظة عليها. وقد اتجه المشرع الجزائري إلى توسيع وسائل التحري بما يتلاءم مع التطور التقني، مع إبقاء استعمالها خاضعاً للرقابة القضائية والضمانات المقررة قانوناً.³

الفرع الثاني: التفتيش وضبط الأدلة الإلكترونية

تقتضي خصوصية الجريمة الإلكترونية اعتماد إجراءات تفتيش تختلف في طبيعتها عن التفتيش التقليدي، بالنظر إلى أن محل البحث قد لا يكون شيئاً مادياً بالمعنى المعتاد، وإنما بيانات أو معلومات مخزنة داخل منظومة معلوماتية أو وسائط إلكترونية. وقد منح المشرع الجزائري للسلطات القضائية المختصة وضباط الشرطة القضائية صلاحية إجراء التفتيش داخل المنظومات المعلوماتية، بما فيها

¹ المادة 16، القانون رقم 04-09، سالف الذكر.

² المادتان 3 و9، القانون رقم 04-09، سالف الذكر.

³ بوسماحة أمينة، بوعرفة عبد القادر، « Evidentiary Mechanisms and Forensic Frameworks in the Investigation of Cybercrimes »، مجلة طلبة للدراسات العلمية الأكاديمية، المجلد 9، العدد 1، 2026، ص ص 1108-1121.

التفتيش عن بعد، بهدف الوصول إلى الأدلة الإلكترونية اللازمة لإثبات الجريمة، مع إخضاع هذا الإجراء لشروط وضمانات قانونية.¹

ويقصد بالتفتيش الإلكتروني البحث داخل منظومة معلوماتية أو نظام تخزين معلوماتي عن المعطيات والآثار الرقمية المرتبطة بالجريمة، بغرض ضبطها واستعمالها في الإثبات. ويختلف هذا الإجراء عن التفتيش التقليدي من حيث محله، إذ قد ينصب على بيانات غير مادية، كما قد يمتد إلى منظومة أخرى مرتبطة بالمنظومة محل التفتيش، وهو ما يفرض على القائم به الإلمام بالجوانب التقنية والقانونية في آن واحد.²

وقد نظم القانون رقم 04-09 هذا الإجراء بصورة صريحة، إذ أجاز للسلطات القضائية المختصة وضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المحددة قانوناً، الدخول بغرض التفتيش، ولو عن بعد، إلى منظومة معلوماتية أو جزء منها وإلى المعطيات المعلوماتية المخزنة فيها، وكذلك إلى منظومة تخزين معلوماتية. ويكشف ذلك عن تبني المشرع لمفهوم واسع لمحل التفتيش، بحيث لا يقتصر على الجهاز المادي، وإنما يشمل البيئة المعلوماتية والبيانات المخزنة فيها.³

كما أجاز المشرع تمديد التفتيش إلى منظومة معلوماتية أخرى عندما توجد أسباب تدعو إلى الاعتقاد بأن المعطيات المبحوث عنها مخزنة فيها، وكان من الممكن الدخول إليها انطلاقاً من المنظومة الأولى. ويشترط في هذه الحالة إعلام السلطة القضائية المختصة مسبقاً بذلك، وهو ما يحقق قدرًا من الرقابة على امتداد التفتيش ويحول دون التوسع غير المبرر في نطاقه.⁴

وتظهر خصوصية التفتيش الإلكتروني بصورة أوضح عندما تكون المعطيات محل البحث مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني؛ ففي هذه الحالة لا يسمح المشرع بالانتقال مباشرة إلى تلك المنظومة خارج الحدود، وإنما يجعل الحصول على البيانات عن طريق مساعدة السلطات الأجنبية المختصة، طبقاً للاتفاقيات الدولية ذات الصلة والقواعد المعمول بها في مجال التعاون القضائي

¹ علمي مخلوف، بومحراث ليندة، «ضوابط التفتيش في الجرائم الإلكترونية»، مجلة المعيار، المجلد 28، العدد 1، 2024، ص ص 389-402.

² دلال مولاي ملياني، «التفتيش في جرائم تكنولوجيايات الإعلام والاتصال»، مجلة القانون والعلوم السياسية، المجلد 2، العدد 1، 2016، ص ص 291-307.

³ المادة 5، القانون رقم 04-09، سالف الذكر.

⁴ المادة 5، القانون رقم 04-09، سالف الذكر.

الدولي.¹ ويعكس ذلك احترام مبدأ السيادة الإقليمية للدول، مع توفير وسيلة قانونية للوصول إلى الأدلة الإلكترونية العابرة للحدود.

ولتجاوز الصعوبات التقنية التي قد تواجه السلطات أثناء تنفيذ التفتيش، أجاز المشرع تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات التي تتضمنها، قصد مساعدتها وتزويدها بالمعلومات الضرورية لإنجاز مهمتها. ويكتسب هذا الحكم أهمية عملية بالنظر إلى إمكانية وجود أنظمة محمية بوسائل تقنية معقدة أو تحتاج إلى معرفة متخصصة للوصول إلى البيانات الموجودة فيها.²

أما بالنسبة إلى ضبط الأدلة الإلكترونية، فقد نظم المشرع الجزائري ذلك من خلال المادة 6 من القانون رقم 04-09، إذ أجاز للسلطة التي تبشر التفتيش، عند اكتشافها معطيات مخزنة يمكن أن تكون مفيدة في الكشف عن الجرائم، حجزها وفق الإجراءات المحددة قانوناً. ولا ينصرف الحجز بالضرورة إلى الجهاز المادي بأكمله، وإنما يمكن أن يتعلق بالمعطيات ذاتها أو بنسخ منها بحسب الحالة وطبيعة الوسيط الإلكتروني.³

وتكمن أهمية النسخ في إمكانية الحفاظ على البيانات الأصلية من التغيير أو الإتلاف، إذ قد يكون من غير العملي أو غير الضروري حجز النظام المعلوماتي بأكمله. ولذلك يمكن للجهة المكلفة بالتفتيش نسخ المعطيات التي تشكل دليلاً على الجريمة، مع اتخاذ التدابير التي تضمن عدم المساس بمحتواها أو سلامتها أثناء عملية النسخ والحفظ.⁴

كما أجاز المشرع اتخاذ تدابير لحماية المعطيات الموجودة في المنظومة عندما يتعذر حجزها مباشرة، وذلك من خلال وضع ترتيبات تقنية تمنع الوصول إليها أو استعمالها أو تغييرها خلال الفترة

¹ المادة 5، القانون رقم 04-09، سالف الذكر.

² المادة 5، القانون رقم 04-09، سالف الذكر.

³ المادة 6، القانون رقم 04-09، سالف الذكر.

⁴ المادة 6، القانون رقم 04-09، سالف الذكر.

اللازمة لإنجاز إجراءات التحقيق. وتكمن أهمية هذا الإجراء في أن الدليل الإلكتروني يتميز بسهولة محوه أو تعديله، مما يجعل المحافظة على حالته الأصلية عنصراً أساسياً في سلامة الإثبات.¹

ولا تنفصل عملية التفتيش والحجز الإلكتروني عن احترام الحق في الحياة الخاصة وسرية الاتصالات، لأن البحث داخل الأجهزة والأنظمة المعلوماتية قد يكشف، إلى جانب الأدلة المتعلقة بالجريمة، عن عدد كبير من البيانات الشخصية والمراسلات والملفات الخاصة. ولهذا أخضع المشرع الإجراءات الخاصة بالتفتيش الإلكتروني للضوابط القانونية، بما يحقق التوازن بين مقتضيات مكافحة الجريمة وحماية الحقوق والحريات الفردية.²

وقد أكدت الدراسات القانونية الجزائرية أن التفتيش الإلكتروني يثير إشكالات خاصة تتعلق بتحديد نطاقه ومحلّه وكيفية تنفيذ الحجز، خاصة عندما تكون الأدلة موزعة على أكثر من نظام أو مخزنة عن بعد. كما أن طبيعة البيئة الافتراضية تجعل من الضروري مراعاة الضوابط الموضوعية والشكلية للتفتيش، حتى لا يؤدي التوسع في البحث عن الأدلة إلى المساس غير المشروع بالخصوصية الإلكترونية للأفراد.³

ويظهر كذلك أن سلامة الدليل الإلكتروني ترتبط بصورة مباشرة بطريقة ضبطه، إذ إن أي تغيير أو حذف أو تدخل غير موثق في البيانات قد يثير الشك في مصدر الدليل ومضمونه. ومن ثم، ينبغي أن تتم عمليات الحجز والنسخ والحفظ بطريقة تسمح بإثبات مصدر البيانات والكيفية التي تم الحصول عليها بها، والمحافظة على سلامتها إلى غاية تقديمها أمام القضاء.⁴

كما أن التفتيش الإلكتروني قد يجري عن بعد، وهو ما يمثل إحدى أبرز الخصائص الإجرائية في مجال الجرائم الإلكترونية، إذ يمكن للسلطة المختصة الوصول إلى المنظومة أو البيانات محل البحث دون الحضور المادي إلى المكان الموجود فيه الجهاز. ويعكس هذا الإجراء طبيعة البيئة الرقمية التي

¹ المادتان 7 و8، القانون رقم 09-04، سالف الذكر.

² مفيدة مباركية، «الأدلة الجنائية الرقمية والحق في الخصوصية في ظل القانون 09-04»، مجلة العلوم الإنسانية، المجلد 25، العدد 6، 2021، ص 554-567.

³ علمي مخلوف، بومحرث ليندة، مرجع سابق، ص ص 389-402.

⁴ بوسماحة أمينة، بوعرفة عبد القادر، مرجع سابق، ص ص 1108-1121.

تسمح بالوصول إلى البيانات عبر الشبكات، لكنه في الوقت ذاته يفرض ضرورة احترام الحدود القانونية والإذن القضائي والضمانات المقررة لحماية الخصوصية.¹

وعليه، فإن التفتيش وضبط الأدلة الإلكترونية في التشريع الجزائري يقومان على آليات خاصة تتلاءم مع طبيعة الجريمة الرقمية، بدءًا من الدخول إلى المنظومة والتفتيش فيها، وإمكانية تمديد التفتيش إلى منظومة أخرى أو إجرائه عن بعد، وصولًا إلى حجز البيانات أو نسخها وحمايتها من التغير أو الإتلاف. وقد سعى المشرع من خلال هذه الإجراءات إلى تمكين السلطات من الوصول إلى الدليل الإلكتروني مع المحافظة، في الوقت ذاته، على الشرعية الإجرائية والحقوق الأساسية للأفراد.²

الفرع الثالث: حجية الدليل الإلكتروني وإجراءات الحفاظ عليه

أبرزت الطبيعة التقنية للجريمة الإلكترونية نوعًا خاصًا من الأدلة يتمثل في البيانات والمعلومات الرقمية التي يمكن أن توجد داخل أجهزة الحاسوب والهواتف والأنظمة المعلوماتية ووسائط التخزين وشبكات الاتصال. وقد أصبح هذا الدليل عنصرًا أساسيًا في إثبات الجرائم المرتكبة في البيئة الرقمية، غير أن الاستناد إليه أمام القضاء يثير مسألة مدى حجتيته وشروط قبوله، خاصة بالنظر إلى سهولة نسخه أو تعديله أو حذفه، وهو ما يجعل سلامة إجراءات جمعه وحفظه عنصرًا أساسيًا في تحديد قيمته الإثباتية.³

ويقصد بحجية الدليل الإلكتروني القوة الاستدلالية التي يتمتع بها في إثبات وقوع الجريمة ونسبتها إلى شخص معين، وتقوم هذه الحجية على مجموعة من الاعتبارات القانونية والفنية، في مقدمتها مشروعية الحصول على الدليل، وارتباطه بالواقعة محل المتابعة، وإمكانية التحقق من مصدره ومضمونه، وسلامته من التغير أو التلاعب. ولذلك فإن مجرد العثور على بيانات رقمية داخل جهاز أو منظومة معلوماتية لا يؤدي تلقائيًا إلى منحها قوة إثباتية مطلقة، وإنما تخضع قيمتها لتقدير القضاء في ضوء ظروف الحصول عليها وسلامتها.⁴

¹ المادة 5، القانون رقم 09-04، سالف الذكر.

² المواد 5 إلى 8، القانون رقم 09-04، سالف الذكر.

³ بوسماحة أمينة، بوعرفة عبد القادر، مرجع سابق، ص ص 1108-1121.

⁴ قصي علي عباس، «حجية الدليل الإلكتروني في الإثبات الجنائي»، مجلة كلية القانون والعلوم السياسية، 2024.

ويستند الإثبات الجزائي في التشريع الجزائري إلى مبدأ حرية الإثبات، حيث يمكن إثبات الجرائم بمختلف طرق الإثبات، ما لم ينص القانون على خلاف ذلك، ويترك تقدير قيمة الأدلة إلى اقتناع القاضي الجزائي. ومن ثم، لا يوجد ما يمنع من حيث المبدأ الاستناد إلى الدليل الإلكتروني في المجال الجزائي متى تم الحصول عليه بطريقة مشروعة وتوافرت فيه الشروط التي تسمح بالاعتماد عليه، شأنه في ذلك شأن باقي وسائل الإثبات.¹

وتتوقف حجية الدليل الإلكتروني بصورة أساسية على مشروعية الحصول عليه، إذ لا يكفي أن تكون البيانات صحيحة من الناحية التقنية، وإنما يجب أن يكون الوصول إليها وجمعها قد تم وفق الإجراءات التي يحددها القانون. فإذا تم الحصول على البيانات من خلال تفتيش أو اعتراض للاتصالات أو أي إجراء آخر دون احترام الشروط والضمانات القانونية المقررة، فإن ذلك قد يؤثر في القيمة القانونية للدليل ويثير مسألة مشروعية الإجراء الذي نتج عنه.²

كما ترتبط حجية الدليل الإلكتروني بضرورة سلامته وعدم تعرضه للتغيير منذ لحظة ضبطه إلى غاية تقديمه أمام القضاء. وتظهر هذه المسألة بصورة أكبر في البيئة الرقمية، لأن البيانات الإلكترونية قابلة للنسخ والتعديل والحذف دون أن يكون التغيير ظاهراً بالضرورة للعين المجردة. ولذلك ينبغي اتخاذ إجراءات تقنية وقانونية تسمح بإثبات أن البيانات المقدمة للقضاء هي ذاتها التي تم الحصول عليها أثناء البحث والتحري، ولم يطرأ عليها أي تغيير من شأنه التأثير في مضمونها.³

ويقتضي الحفاظ على الدليل الإلكتروني، في مرحلة أولى، تثبيت البيانات الموجودة في حالتها الأصلية فور ضبطها، ومنع الأشخاص غير المختصين من الوصول إليها أو تعديلها. ويشمل ذلك اتخاذ التدابير المناسبة لحماية الأجهزة ووسائل التخزين والأنظمة المعلوماتية التي تحتوي على البيانات محل التحقيق، مع توثيق الإجراءات التي اتخذت منذ اكتشاف الدليل إلى غاية تسليمه إلى الجهة المختصة بفحصه.⁴

¹ المادة 349، القانون رقم 14-25، سالف الذكر.

² المادتان 1 و 349، القانون رقم 14-25، سالف الذكر.

³ مفيدة مباركية، مرجع سابق، ص ص 554-567.

⁴ المادة 6، القانون رقم 04-09، سالف الذكر.

كما يمكن اللجوء إلى نسخ البيانات الإلكترونية بدل التعامل المباشر مع الأصل، خاصة عندما يكون الجهاز أو الوسيط المعلوماتي ضرورياً لاستمرار نشاط صاحبه أو عندما يكون نقل البيانات وحدها أكثر ملاءمة من حجز الجهاز بأكمله. غير أن النسخ ينبغي أن يتم بطريقة تقنية تضمن مطابقة النسخة للبيانات الأصلية، مع توثيق عملية النسخ والجهة التي قامت بها والوسيلة المستعملة، بما يسمح بالتحقق لاحقاً من سلامة الدليل¹.

وترتبط سلامة الدليل كذلك بما يعرف في المجال الجنائي بـ سلسلة حيازة الدليل، والمقصود بها توثيق مراحل انتقال الدليل منذ ضبطه إلى غاية عرضه أمام القضاء، مع تحديد الأشخاص الذين تعاملوا معه والإجراءات التي أجريت عليه. وتسمح هذه الآلية بإثبات عدم تعرض الدليل للتغيير أو الاستبدال خلال مراحل جمعه وفحصه وحفظه، وهو أمر بالغ الأهمية بالنسبة للأدلة الرقمية بسبب قابليتها العالية للنسخ والتعديل².

وتبرز أهمية الخبرة التقنية عندما تكون طبيعة الدليل الإلكتروني أو طريقة استخراجه تتطلب معرفة فنية متخصصة، إذ يمكن الاستعانة بخبير لفحص الأجهزة والبيانات واسترجاع الملفات المحذوفة وتحليل البيانات التقنية وتحديد الروابط بين مختلف المعطيات. ويساعد ذلك القضاء على فهم طبيعة الدليل ومصدره ومدى سلامته، دون أن يعني ذلك حلول الخبير محل القاضي في تقدير القيمة القانونية للدليل.

ومن جانب آخر، يتمتع القاضي الجزائري بسلطة في تقدير الدليل الإلكتروني ضمن إطار اقتناعه القضائي، بحيث لا تكون البيانات الرقمية ملزمة له بصورة آلية لمجرد استخراجها بطريقة تقنية. ويأخذ القاضي في تقديره مدى مشروعية الدليل، ودرجة يقينه، ومدى ارتباطه بالواقعة الإجرامية، ومدى إمكانية نسبته إلى المتهم، فضلاً عن سلامة الإجراءات التي اتبعت في جمعه وحفظه. وقد خلصت دراسات قانونية جزائرية إلى أن حجية الدليل الإلكتروني ترتبط أساساً بمشروعية الحصول عليه وسلامته ومدى اقتناع القاضي بقيمته في الإثبات³.

¹ المادة 6، القانون رقم 09-04، سالف الذكر.

² علمي مخلوف، بومحراث ليندة، مرجع سابق، ص ص 389-402.

³ المادة 349، القانون رقم 25-14، سالف الذكر.

ويظهر جانب آخر من الحجية في المحررات والبيانات الإلكترونية الموقعة إلكترونياً، حيث اعترف المشرع الجزائري بالإطار القانوني للتوقيع والتصديق الإلكترونيين بموجب القانون رقم 04-15، وأقر قواعد تضمن إمكانية الاعتماد على التوقيع الإلكتروني كوسيلة لإثبات هوية الموقع وسلامة البيانات المرتبطة به وفق الشروط التي حددها القانون.¹ وقد ساهم هذا التنظيم في تعزيز الثقة في البيئة الرقمية وتوفير أساس قانوني للاعتماد على بعض البيانات الإلكترونية في الإثبات .

كما أولى المشرع أهمية لحماية بيانات إنشاء التوقيع الإلكتروني، إذ ألزم صاحب شهادة التصديق الإلكتروني بالمحافظة على سريتها، وأوجب عليه اتخاذ الإجراءات اللازمة عند وجود شك في الحفاظ على هذه السرية أو عند وجود خلل في مطابقة البيانات للمعلومات الواردة في شهادة التصديق. ويهدف ذلك إلى منع استعمال بيانات التوقيع من طرف الغير وحماية سلامة الوثائق والبيانات الإلكترونية المرتبطة به.²

ولا تقتصر إجراءات الحفاظ على الدليل الإلكتروني على الجانب التقني، وإنما تشمل كذلك توثيق ظروف الحصول عليه، وتحديد زمان ومكان ضبطه، والجهة التي قامت بذلك، وطريقة استخراجها، والوسائل المستعملة في حفظه وفحصه. ويسمح هذا التوثيق بإقامة صلة واضحة بين الدليل الأصلي والدليل المقدم أمام القضاء، ويقلل من إمكانية الطعن فيه على أساس احتمال التغيير أو التلاعب.³

كما ينبغي المحافظة على سرية البيانات التي يتم ضبطها، خصوصاً عندما تحتوي الأجهزة أو الأنظمة المعلوماتية على معلومات شخصية أو مراسلات خاصة لا علاقة لها بالجريمة محل التحقيق. وبالتالي يجب أن تقتصر إجراءات الفحص على البيانات ذات الصلة بالواقعة، وأن يتم التعامل مع البيانات الأخرى وفق الحدود التي يسمح بها القانون، تحقيقاً للتوازن بين فعالية التحقيق وحماية الحياة الخاصة.

¹ القانون رقم 02-26 المؤرخ في 29 شعبان عام 1447 الموافق 17 فبراير سنة 2026، الذي يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 14، 18 فبراير سنة 2026.

² المواد المتعلقة بالتوقيع الإلكتروني وبيانات إنشاء التوقيع الإلكتروني، القانون رقم 02-26، سالف الذكر.

³ بوسماحة أمينة، بوعرفة عبد القادر، مرجع سابق، ص ص 1108-1121.

وتؤكد أهمية هذه الضمانات بالنظر إلى أن الدليل الإلكتروني قد يكون هشاً وسريع الزوال، فقد يؤدي إيقاف جهاز أو تغيير إعداداته أو فتح ملف أو تعديل أحد مكوناته إلى تغيير بعض البيانات أو فقدان معلومات مرتبطة بها. ولذلك ينبغي أن يتم التعامل مع الوسائط الإلكترونية وفق منهج تقني يهدف إلى المحافظة على حالتها الأصلية قدر الإمكان، مع تسجيل كل إجراء يتم اتخاذه أثناء عملية الاستخراج والتحليل.

وعليه، فإن حجية الدليل الإلكتروني في التشريع الجزائري لا تقوم على طبيعته الرقمية وحدها، وإنما ترتبط بمشروعية الحصول عليه، وسلامته، وإمكانية التحقق من مصدره، والمحافظة على سلسلة حيازته، ومدى صلته بالواقعة، واقتناع القاضي بقيمته الإثباتية. ومن ثم، فإن احترام إجراءات جمع الدليل وحفظه يمثل ضماناً أساسية لقبوله أمام القضاء، ويحول دون فقدان قيمته بسبب الشك في مصدره أو سلامة محتواه.

خاتمة

أفضت دراسة موضوع الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري إلى أن التطور المتسارع لتكنولوجيات الإعلام والاتصال أفرز أنماطاً إجرامية جديدة تختلف في طبيعتها ووسائل ارتكابها وآثارها عن الجرائم التقليدية، الأمر الذي فرض على المشرع الجزائري تطوير منظومته القانونية بما يسمح بمواجهة الاعتداءات التي تستهدف الأنظمة المعلوماتية والبيانات والأموال والأشخاص. وقد اتضح أن خصوصية الجريمة الإلكترونية لا ترتبط فقط بالوسيلة التقنية المستعملة في ارتكابها، وإنما تمتد إلى صعوبة اكتشافها وإثباتها، وسرعة زوال آثارها، وإمكانية ارتكابها من خارج إقليم الدولة، مما يجعل مواجهتها تقتضي تكامل الوسائل الموضوعية والإجرائية والتقنية.

وقد أظهر تحليل التشريع الجزائري أن المشرع اعتمد حماية متعددة المستويات، من خلال تجريم الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات في قانون العقوبات، إلى جانب القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الذي وضع آليات خاصة للوقاية والتحري وجمع الأدلة والتعاون القضائي. كما تتكامل هذه الحماية مع النصوص المتعلقة بحقوق المؤلف والحقوق المجاورة، وحماية المعطيات ذات الطابع الشخصي، والتوقيع والتصديق الإلكترونيين. ويؤكد هذا التعدد التشريعي أن مكافحة الجريمة الإلكترونية لم تعد مقتصرة على التجريم والعقاب، وإنما أصبحت مرتبطة كذلك بحماية البيئة الرقمية والوقاية من الاعتداءات التي قد تستهدفها.

كما تبين أن فعالية السياسة الجنائية في هذا المجال ترتبط بمدى قدرة القواعد الإجرائية على مواكبة خصوصية الدليل الإلكتروني، خاصة في مراحل البحث والتحري والتفتيش وضبط البيانات وحفظها. وقد عزز قانون الإجراءات الجزائية الجديد رقم 14-25 الإطار العام للإجراءات الجزائية في الجزائر، مع تأكيده لمبادئ الشرعية والمحكمة العادلة واحترام حقوق الإنسان، وهي ضمانات ينبغي أن تظل حاضرة عند استعمال الوسائل التقنية الخاصة في مكافحة الجرائم الإلكترونية.

توصلت الدراسة إلى جملة من النتائج، أهمها:

- تتميز الجريمة الإلكترونية بخصوصية تقنية وإجرائية تجعل مواجهتها أكثر تعقيداً من الجرائم التقليدية، خاصة بسبب سرعة تنفيذها وصعوبة تحديد مرتكبيها وإمكانية إخفاء آثارها.

- أظهر التشريع الجزائري اهتمامًا واضحًا بمكافحة الجريمة الإلكترونية من خلال الجمع بين النصوص العامة في قانون العقوبات والأحكام الخاصة الواردة في القانون رقم 09-04.
 - لم تقتصر الحماية القانونية على الأنظمة المعلوماتية، وإنما امتدت إلى البيانات والمعطيات الشخصية والبرامج والمصنفات الرقمية والمعاملات الإلكترونية.
 - أتاح المشرع الجزائري للجهات المختصة مجموعة من الوسائل الخاصة للبحث والتحري والتفتيش والوصول إلى البيانات الإلكترونية، بما يتلاءم مع الطبيعة التقنية للجريمة.
 - يمثل الدليل الإلكتروني عنصرًا أساسيًا في إثبات الجرائم الإلكترونية، إلا أن قيمته أمام القضاء ترتبط بسلامة إجراءات الحصول عليه وحفظه وإمكانية التحقق من مصدره وعدم تعرضه للتغيير أو التلاعب.
 - تظل الطبيعة العابرة للحدود لبعض الجرائم الإلكترونية من أبرز الإشكالات التي تواجه أجهزة العدالة، خصوصًا عندما تكون البيانات أو الأنظمة المعلوماتية محل البحث موجودة خارج الإقليم الوطني.
 - لا تكفي العقوبات وحدها لمواجهة الجريمة الإلكترونية، إذ تتطلب مكافحة الفعالة الجمع بين التجريم والعقاب والوقاية والتكوين والتعاون التقني والقضائي.
- استنادًا إلى النتائج المتوصل إليها، يمكن تقديم التوصيات الآتية:
- ضرورة مواصلة تحديث التشريع الجزائري بما يتلاءم مع التطور المستمر في تقنيات المعلومات والاتصال وظهور صور إجرامية إلكترونية جديدة.
 - العمل على تطوير إطار قانوني أكثر تكاملًا للجريمة الإلكترونية، بما يقلل من تشتت الأحكام المتعلقة بها بين مختلف النصوص القانونية.
 - دعم المصالح المختصة بمكافحة الجرائم الإلكترونية بالوسائل التقنية الحديثة والخبرات البشرية القادرة على اكتشاف الأدلة الرقمية وتحليلها وحفظها.
 - وضع بروتوكولات دقيقة وموحدة لجمع الأدلة الإلكترونية وحفظها وتوثيق سلسلة حيازتها، بما يعزز الثقة في الدليل الرقمي أمام الجهات القضائية.

- تعزيز التعاون القضائي والأمني الدولي في مجال الجرائم الإلكترونية، خصوصًا فيما يتعلق بتبادل المعلومات والحصول على الأدلة الإلكترونية الموجودة خارج الإقليم الوطني.
- تكثيف إجراءات الوقاية والتوعية بمخاطر الجريمة الإلكترونية، سواء بالنسبة للأفراد أو المؤسسات، مع نشر الثقافة القانونية والرقمية المتعلقة بحماية البيانات والحسابات والأنظمة المعلوماتية.
- تعزيز التعاون بين الدولة ومقدمي خدمات الاتصال والمؤسسات التقنية، مع ضمان احترام الحقوق والحريات الأساسية وحماية المعطيات ذات الطابع الشخصي.
- تحقيق توازن دقيق بين فعالية وسائل البحث والتحري الإلكترونية وبين حماية الحق في الخصوصية وسرية الاتصالات، بحيث لا تتحول مكافحة الجريمة إلى مساس غير مبرر بالحريات الفردية.

تفتح الدراسة الحالية المجال أمام عدد من الدراسات المستقبلية، خاصة في ظل التطور المستمر للبيئة الرقمية، ويمكن أن تتجه الأبحاث القادمة إلى دراسة الجوانب القانونية للذكاء الاصطناعي والجرائم المرتكبة بواسطته، ومدى قدرة قواعد المسؤولية الجنائية التقليدية على استيعاب الأفعال الإجرامية الناتجة عن الأنظمة الذكية.

كما يمكن توسيع البحث في مجال الدليل الإلكتروني والذكاء الاصطناعي في الإثبات الجنائي، خاصة فيما يتعلق بوسائل اكتشاف التلاعب بالبيانات الرقمية والتحقق من أصالتها، إضافة إلى دراسة الإشكالات المرتبطة بالأدلة المخزنة في الخدمات السحابية والمنصات الرقمية الأجنبية.

ومن الآفاق المهمة كذلك دراسة التعاون القضائي الدولي في مكافحة الجريمة الإلكترونية، بالنظر إلى أن الطبيعة العابرة للحدود لهذا النوع من الجرائم تفرض تطوير آليات أكثر سرعة وفعالية للوصول إلى الأدلة الرقمية وملاحقة مرتكبي الجرائم الذين يستغلون اختلاف الأنظمة القانونية بين الدول.

وبذلك، تبقى مكافحة الجريمة الإلكترونية مجالاً قانونياً متطوراً يحتاج إلى مراجعة مستمرة للتشريعات والآليات الإجرائية، حتى تظل الحماية الجنائية قادرة على مواكبة التحولات التقنية، مع المحافظة على مبادئ الشرعية واحترام الحقوق والحريات الأساسية.

قائمة المراجع والمصادر

قائمة المراجع والمصادر

أولاً: المصادر

1. الدستور

المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020، المتعلق بإصدار التعديل الدستوري، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 82، 30 ديسمبر سنة 2020.

2. القوانين

القانون رقم 25-14 المؤرخ في 9 صفر عام 1447 الموافق 3 غشت سنة 2025، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 54، 13 غشت سنة 2025.

القانون رقم 26-02 المؤرخ في 29 شعبان عام 1447 الموافق 17 فبراير سنة 2026، الذي يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الإلكترونية وبالتعريف الإلكتروني، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 14، 18 فبراير سنة 2026.

القانون رقم 06-01 المؤرخ في 21 محرم عام 1427 الموافق 20 فبراير سنة 2006، الجريدة الرسمية، المتعلق بالوقاية من الفساد ومكافحته، المعدل والمتمم بالقانون.

القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 34، 10 يونيو سنة 2018.

القانون رقم 23-09 المؤرخ في 3 ذي الحجة عام 1444 الموافق 21 يونيو سنة 2023، المتضمن القانون النقدي والمصرفي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 43، 27 يونيو سنة 2023.

القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، 16 غشت سنة 2009.

القانون رقم 24-06 المؤرخ في 19 شوال عام 1445 الموافق 28 أبريل سنة 2024، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 30، 30 أبريل سنة 2024.

3.الأوامر

الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو سنة 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 44، 23 يوليو سنة 2003.

4.المراسيم واللوائح والتنظيمات

المرسوم الرئاسي رقم 13-123 المؤرخ في 20 مارس سنة 2013، المتعلق بانضمام الجزائر إلى معاهدة الويبو بشأن حق المؤلف.

المرسوم الرئاسي رقم 97-341 المؤرخ في 11 جمادى الأولى عام 1418 الموافق 13 سبتمبر سنة 1997، المتعلق بانضمام الجزائر إلى اتفاقية برن لحماية المصنفات الأدبية والفنية.

المرسوم الرئاسي رقم 21-439 المؤرخ في 7 نوفمبر سنة 2021، الجريدة الرسمية، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثانيا: المراجع

أ- الكتب

أمين الشوابكة، جرائم الحاسوب والإنترنت: الجريمة المعلوماتية، الطبعة الأولى، عمان، الأردن، دار الثقافة للنشر والتوزيع، 2007.

عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، الطبعة الأولى، الإسكندرية، مصر، دار الفكر الجامعي، 2006.

عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي: دراسة متعمقة في التعريف بجرائم التقنية، الطبعة الأولى، الإسكندرية، مصر، منشأة المعارف، 2009.

عبد القادر عميمر، التحديات القانونية لإثبات الجريمة المعلوماتية، الجزائر، النشر الجامعي الجديد، 2021.

محمد حزيط، المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري، الجزائر، دار هومة للطباعة والنشر والتوزيع، 2014.

محمد عبد القادر عدو، مبادئ قانون العقوبات الجزائري: القسم العام، الجزائر، دار هومة للطباعة والنشر والتوزيع.

ب- الأطروحات ورسائل الماجستير ومذكرات الماستر

أولا: أطروحات الدكتوراه

حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه في الحقوق، تخصص قانون العقوبات والعلوم الجنائية، جامعة باتنة، 2015-2016.

فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم، تخصص قانون عام، كلية الحقوق، جامعة الجزائر 1 بن يوسف بن خدة، 2018-2019.

ثانيا: رسائل الماجستير

أحمد مسعود مريم، آليات مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04-09، مذكرة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، السنة الجامعية 2012-2013.

ثالثا: مذكرات الماستر

جبراني نورة، لعماري سهام، التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعرييج، 2025.

عماد يوسف، لزهر ضربان، إجراءات التحري في الجرائم الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة الوادي، 2023.

نعيمة بلكاوي، الدليل الإلكتروني في التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، جامعة عمار ثليجي بالأغواط، الجزائر، 2024.

ج- المقالات

أمنية بوسماحة، عبد القادر بوعرفة، «Evidentiary Mechanisms and Forensic Frameworks in the Investigation of Cybercrimes»، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 9، العدد 1، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر، 2026.

أمنية بصافة، «الأطر القانونية للجريمة السيبرانية في التشريع الجزائري بين الوقاية والمكافحة»، حوليات جامعة الجزائر 1، المجلد 37، العدد 01، جامعة الجزائر 1 بن يوسف بن خدة، الجزائر العاصمة، الجزائر، 2023.

بدر الدين خلاف، «التنظيم القانوني للجريمة المعلوماتية في الجزائر»، مجلة العلوم القانونية والاجتماعية، المجلد 6، العدد 2، جامعة زيان عاشور، الجلفة، الجزائر، 2021.

جخدم محمد، «جرائم الفضاء الإلكتروني في ضوء القانون الجزائري رقم 09-04 بين قصور التجريم ورهانات التكيف التشريعي»، مجلة الدراسات القانونية والسياسية، المجلد 12، العدد 02، الجزائر، 2026.

خليفة فتيحة، مهداوي محمد صالح، «حجية الدليل الإلكتروني في إثبات الاعتداءات المنصوص عليها في المواد 394 مكرر إلى 394 مكرر 2 من قانون العقوبات الجزائري»، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 61، العدد 04، جامعة الجزائر 1 بن يوسف بن خدة، الجزائر العاصمة، الجزائر، 2024.

دلال مولاي ملياني، «التفتيش في جرائم تكنولوجيات الإعلام والاتصال»، مجلة القانون والعلوم السياسية، المجلد 2، العدد 1، جامعة الدكتور مولاي الطاهر، سعيدة، الجزائر، 2016.

راضية عيمور، «الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري»، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 6، العدد 1، جامعة عمار ثليجي، الأغواط، الجزائر، 2022.

ربيع معزوز، آسيا زروقي، «الجريمة الإلكترونية وإجراءات مواجهتها في التشريع الجزائري»، مجلة القانون والعلوم السياسية، المجلد 7، العدد 2، المركز الجامعي علي كافي، تندوف، الجزائر، 2021.

سارة مهنوي، «الجريمة المعلوماتية في التشريع الجزائري»، مجلة الدراسات والبحوث القانونية، المجلد 08، العدد 02، الجزائر، 2019.

شول بن شهرة، مراد ماشوش، «السمات الخاصة للجريمة المعلوماتية»، مجلة المستقبل للدراسات القانونية والسياسية، المجلد 4، العدد 1، المركز الجامعي آفلو، الأغواط، الجزائر، 2020.

طيب موفق شريف، «التوقيع الإلكتروني وحمايته جنائيا في القانون الجزائري»، المجلة الإفريقية للدراسات القانونية والسياسية، المجلد 01، العدد 01، جامعة أحمد دراية، أدرار، الجزائر، 2017.

- عبيزة منيرة، بوبكر مصطفى، «الدليل الإلكتروني والسلطة التقديرية للقاضي»، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 3، جامعة لوئيسي علي البليدة 2، البليدة، الجزائر، 2018.
- عزالدين عثمان، «صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات»، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 3، جامعة الشهيد حمه لخضر، الوادي، الجزائر، 2018.
- علمي مخلوف، بومحراث ليندة، «ضوابط التفتيش في الجرائم الإلكترونية»، مجلة المعيار، المجلد 28، العدد 1، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، الجزائر، 2024.
- فيصل نسيبة، عبير بعقلي، «الآليات القانونية الموضوعية لمكافحة الجريمة المعلوماتية»، مجلة الحقوق والعلوم الإنسانية، المجلد 04، العدد 02، الجزائر، 2011.
- قصي علي عباس، «حجية الدليل الإلكتروني في الإثبات الجنائي»، مجلة كلية القانون والعلوم السياسية، العدد 26، بغداد، العراق، 2024.
- كليبي حسن، الطيب نجمة، «جريمة النصب الإلكتروني من منظور المشرع الجزائري»، مجلة المفكر، المجلد 20، العدد 1، جامعة محمد خيضر، بسكرة، الجزائر، 2025.
- لحسن نائي، بغشام رقا، «ضوابط وإجراءات مراقبة الاتصالات الإلكترونية في التشريع الجزائري»، مجلة الدراسات القانونية المقارنة، المجلد 09، العدد 01، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2023.
- محمود أحمد عبادة، «الجريمة الإلكترونية: مفهومها وصورها وسبل مكافحتها»، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 15، العدد 1، الجزائر، 2026.
- مفيدة مباركية، «الأدلة الجنائية الرقمية والحق في الخصوصية في ظل القانون 09-04»، مجلة المعيار، المجلد 25، العدد 6، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، الجزائر، 2021.
- ناجية شيخ، «حول مكافحة الجريمة الإلكترونية في التشريع الجزائري»، مجلة العلوم القانونية والسياسية، المجلد 9، العدد 2، جامعة الشهيد حمه لخضر، الوادي، الجزائر، 2018.

نادية أيت عبد المالك، عبد القادر فلاح، «التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري»، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، خميس مليانة، الجزائر، 2020.

وداد بن سالم، عبد الله شيباني، «النظام القانوني لمقدمي خدمة الإنترنت في ظل القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها»، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد 13، العدد 01، الجزائر، 2024.

فهرس المحتويات

فهرس المحتويات

اهداء	-
شكر وعرفان	-
قائمة المختصرات	-
مقدمة	1
الفصل الأول: ماهية الجريمة الإلكترونية وتنظيمها في التشريع الجزائري	7
المبحث الأول: ماهية الجريمة الالكترونية	9
المطلب الأول: تعريف الجريمة الالكترونية وتميزها عن الجريمة التقليدية	9
الفرع الأول: تعريف الجريمة الالكترونية	9
الفرع الثاني: تمييز الجريمة الالكترونية عن الجريمة التقليدية	13
المطلب الثاني: خصائص الجريمة الالكترونية	14
الفرع الأول: الطابع التقني للجريمة الالكترونية	14
الفرع الثاني: صعوبة اكتشاف وإثبات الجريمة الالكترونية	16
الفرع الثالث: الطابع العابر للحدود للجريمة الالكترونية	18
المطلب الثالث: معايير تصنيف الجريمة الالكترونية	19
الفرع الأول: تصنيف الجرائم الالكترونية بحسب محل الاعتداء	19
الفرع الثاني: تصنيف الجرائم الالكترونية بحسب وسيلة ارتكابها	22

المبحث الثاني: تنظيم الجرائم الالكترونية في التشريع الجزائري	24
المطلب الأول: جرائم التعدي على الأنظمة الآلية لمعالجة المعطيات	25
الفرع الأول: جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي	25
الفرع الثاني: جرائم المساس بسلامة النظام المعلوماتي ومعطياته	27
الفرع الثالث: جرائم الاعتداء على البيانات والبرامج المعلوماتية	29
المطلب الثاني: الجرائم الالكترونية الواقعة على الأموال	31
الفرع الأول: جريمة الاحتيال الالكتروني	31
الفرع الثاني: السرقة والاختلاس باستخدام الوسائل الالكترونية	34
الفرع الثالث: جرائم المساس بالمعاملات والأموال الالكترونية	36
المطلب الثالث: الجرائم الالكترونية الواقعة على الأشخاص	39
الفرع الأول: الاعتداء على الحياة الخاصة والمعطيات الشخصية الالكترونية	39
الفرع الثاني: جرائم التشهير والسب والقذف عبر الوسائط الالكترونية	42
الفرع الثالث: التهديد والابتزاز الالكتروني	45
الفصل الثاني: تدابير وآليات مكافحة الجريمة الالكترونية في التشريع الجزائري ..	48
المبحث الأول: الحماية الموضوعية للنظام المعلوماتي	50
المطلب الأول: حماية النظام المعلوماتي في نصوص الملكية الفكرية	50
الفرع الأول: حماية برامج الحاسوب في إطار حقوق المؤلف	50

الفرع الثاني: حماية المصنفات الرقمية وقواعد البيانات	54
الفرع الثالث: صور الاعتداء على حقوق الملكية الفكرية في البيئة الالكترونية .	57
المطلب الثاني: حماية النظام المعلوماتي في قانون العقوبات	60
الفرع الأول: تجريم الاعتداء على الأنظمة المعلوماتية	60
الفرع الثاني: تجريم الاعتداء على البيانات والمعطيات المعلوماتية	63
الفرع الثالث: تجريم الجرائم المرتكبة بواسطة الوسائل الالكترونية	66
المطلب الثالث: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال	69
الفرع الأول: نطاق تطبيق قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال	69
الفرع الثاني: التدابير الوقائية وآليات الرقابة	72
الفرع الثالث: التزامات مقدمي خدمات الاتصال في مكافحة الجريمة الالكترونية	75
المبحث الثاني: الآليات الجزائية والإجرائية للجريمة الالكترونية	78
المطلب الأول: الجزاءات المقررة في الجريمة الالكترونية	79
الفرع الأول: العقوبات الأصلية المقررة للجرائم الالكترونية	79
الفرع الثاني: العقوبات التكميلية والتدابير المقررة	82

الفرع الثالث: تشديد العقوبة للجريمة الالكترونية.....	85
المطلب الثاني: الخصوصية الإجرائية في الجرائم الالكترونية.....	89
الفرع الأول: إجراءات البحث والتحري في الجرائم الالكترونية.....	89
الفرع الثاني: التفتيش وضبط الأدلة الالكترونية.....	92
الفرع الثالث: حجية الدليل الالكتروني وإجراءات الحفاظ عليه.....	96
خاتمة.....	101
قائمة المراجع والمصادر.....	106
فهرس المحتويات.....	114
ملخص.....	119

ملخص: تتناول هذه الدراسة موضوع الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، من خلال بيان مفهومها وخصائصها وتمييزها عن الجريمة التقليدية، مع توضيح أهم معايير تصنيفها وصورها، لاسيما الجرائم الماسة بالأنظمة الآلية لمعالجة المعطيات، والجرائم الواقعة على الأموال، والجرائم الماسة بالأشخاص. كما تبحث الدراسة في الإطار القانوني الذي اعتمدته المشرع الجزائري لمواجهة هذه الجرائم، من خلال الحماية الموضوعية للنظام المعلوماتي في نصوص الملكية الفكرية وقانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إضافة إلى الآليات الجزائية والإجرائية المتمثلة في العقوبات الأصلية والتكميلية، وإجراءات البحث والتحري والتفتيش وضبط الأدلة الالكترونية، وحجية الدليل الالكتروني وإجراءات الحفاظ عليه. وتهدف الدراسة إلى إبراز مدى تكامل النصوص القانونية والآليات الإجرائية في التصدي للجريمة الالكترونية، في ظل ما تتميز به هذه الجرائم من طابع تقني وصعوبة في اكتشافها وإثباتها وطابعها العابر للحدود.

الكلمات المفتاحية: الجريمة الالكترونية؛ التشريع الجزائري؛ الدليل الالكتروني.

Abstract: This study addresses the issue of cybercrime and the mechanisms for combating it under Algerian legislation by examining its concept and characteristics and distinguishing it from traditional crime, while highlighting the main criteria for its classification and its various forms, particularly crimes against automated data processing systems, crimes involving property, and crimes against individuals. The study also examines the legal framework adopted by the Algerian legislator to combat these crimes through the substantive protection of information systems under intellectual property legislation, the Penal Code, and the Law on the Prevention of Offences Related to Information and Communication Technologies. In addition, it addresses the criminal and procedural mechanisms, including primary and supplementary penalties, investigation and inquiry procedures, the search for and seizure of electronic evidence, as well as the evidentiary value of electronic evidence and the procedures for preserving it. The study aims to highlight the extent to which legal provisions and procedural mechanisms complement each other in combating cybercrime, given the technical nature of these crimes, the difficulties involved in detecting and proving them, and their transnational character.

Keywords: Cybercrime; Algerian legislation; Electronic evidence.