



MÉMOIRE DE MASTER

Spécialité : Droit pénal et sciences criminelles - Réf : P4102/2026

TITRE

مكافحة الجريمة الالكترونية في القانون الجزائري

Présenté et soutenu par

Rania GUEDDOUCHE

Sadjida GUEDOUARI

Date de soutenance : 06/06/2026

JURY DE SOUTENANCE

Nom et Prénom	Grade	Qualité
Safia YOUSFI	MCA	Président
djeradi yacine	MCB	Encadrant
Kalache Khouloud	MCB	Examineur



Mohamed Khider University of Biskra
Faculty of Law and Political Science
Department of public Law

Master's Thesis

Field: **Law and Political Science**
Discipline: **Law**
Specialization: **Criminal Law and Criminal Sciences**

No.:

Prepared by:

Sadjida Guedouari
Rania Guedoush

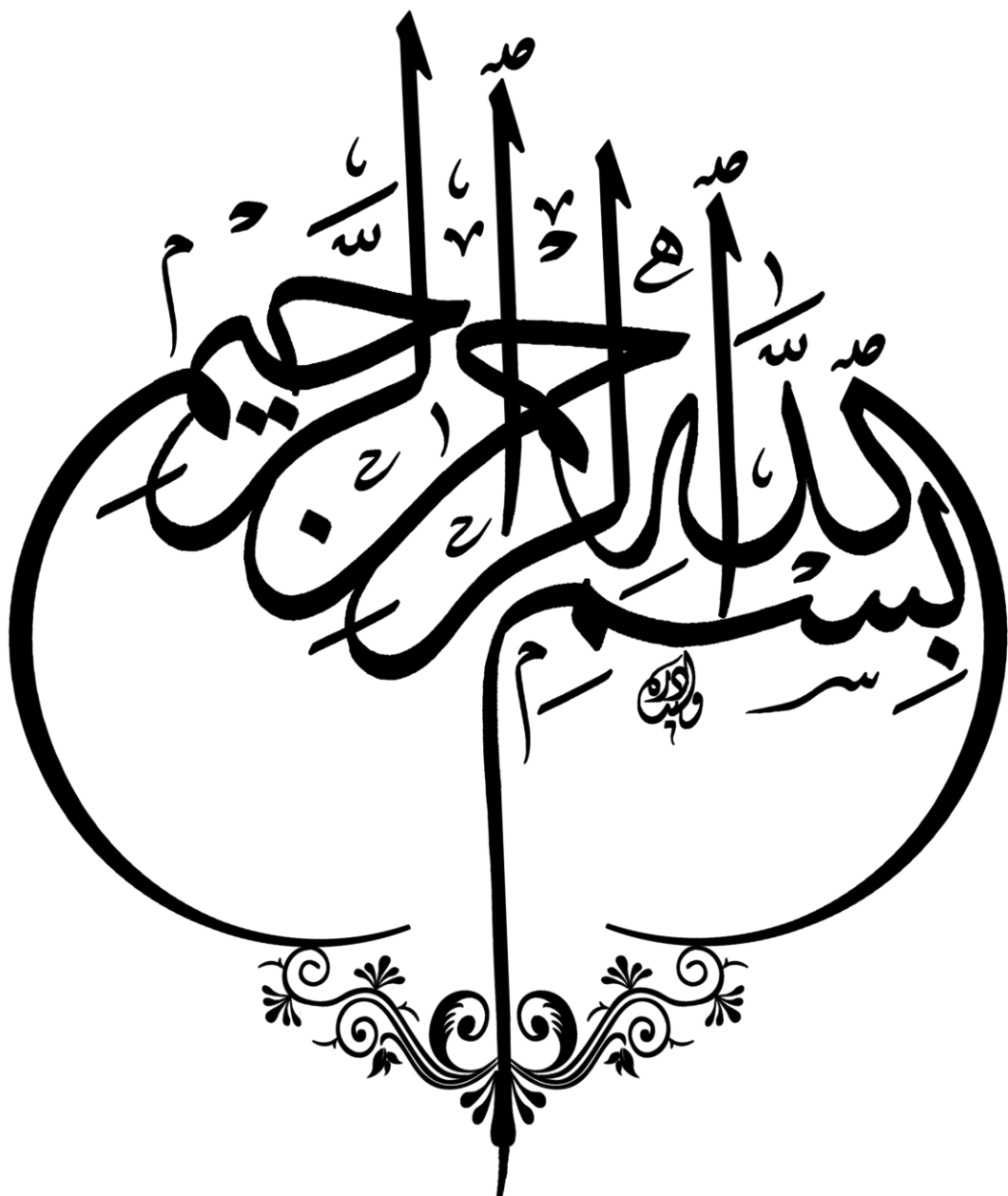
Date: /06/2026

Mechanisms for Combating Cybercrime in Algerian Legislation

Board of Examiners:

	Professor	University of Biskra	President
Dr. Djeradi Yacine	Lecturer Professor B	University of Biskra	Supervisor and Rapporteur
	Professor	University of Biskra	Examiner

Academic Year: 2025–2026



الإهداء

الحمد لله رب العالمين، والصلاة والسلام على أشرف المرسلين سيدنا محمد صلى الله عليه وسلم.

أهدي هذا العمل المتواضع:

إلى من كانت دعواتها ترافقني في كل خطوة، وإلى من غمرتني بحنانها وصبرها وعطائها دون مقابل...

"أمي"

إلى من كان سندي وقودتي في الحياة، وإلى من علمني أن الاجتهاد طريق النجاح، وأن الصبر مفتاح الوصول...

"أبي"

إلى إخوتي وأخواتي، الذين كانوا خير سند ومرقة.

إلى نروجة أخي، على ما وجدته منها من طيب المعاملة وصدق المودة.

إلى كل من كان له أثر طيب في حياتي، أهدي ثمرة هذا الجهد المتواضع.



ساجدة قدواري



الإهداء

بسم الله الرحمن الرحيم، والحمد لله على تمام فضله وكرمه، والصلاة والسلام على سيدنا محمد صلى الله عليه

وسلم.

أهدي ثمرة هذا العمل:

إلى أبي العزيز، الذي كان لي مثلاً في الصبر والسعي، والذي لم يخل عليّ يوماً بالدعم والنصيحة.

إلى أمي الغالية، مصدر الحنان والطمأنينة، وصاحبة الدعوات الصادقة التي كانت ترافقني في كل خطوة.

إلى أختي "صفية"، التي كانت قريبة مني دائماً بمحبتها واهتمامها ومساندتها.

إلى ابن عمي "أشرف"، على دعمه ووقوفه إلى جانبي طيلة هذه المرحلة.

إلى كل من شاركني لحظات التعب والأمل، وكان له أثر طيب في مسيرتي، أهدي هذا العمل المتواضع.



مرانية قدوش



شكر وعرفان

الحمد لله الذي بنعمته تتم الصالحات، نحمده سبحانه وتعالى على ما وفق وأعان، ونسأله أن ينفعنا بهذا العمل وأن يجعله علماً نافعا.

اللهم صل وسلم وبارك على سيدنا محمد وعلى آله وصحبه أجمعين.

تقدم بخالص الشكر والتقدير إلى أستاذنا المشرف الدكتور جرادى ياسين، الذي شرفنا بقبوله الإشراف على هذه الدراسة، وعلى ما قدمه لنا من توجيهات ونصائح علمية قيمة طيلة فترة إنجازه هذا العمل، فجزاه الله عنا خير الجزاء.

كما تتوجه بجزيل الشكر والتقدير إلى أعضاء لجنة المناقشة المحترمين، على تفضلهم بقبول مناقشة هذه المذكرة وقراءتها وتقييمها.

ولا يفوتنا أن نتقدم بالشكر لكل من مدّ لنا يد العون وسأهم في إنجازه هذا العمل، من أساتذتنا الكرام وزملائنا وأصدقائنا.

ونخص بالشكر الدكتور فاطمة الزهرة قداومري، على دعمها ومساندتها المتواصلة، كما نتقدم بالشكر إلى الأستاذة شرف الدين ومردة على المراجع القيمة التي قدمها، وإلى الأستاذ أحمد نوي على دعمه وتشجيعه. وفي الأخير، نشكر كل من ساعدنا من قريب أو بعيد في إنجازه هذا العمل المتواضع، سائلين الله التوفيق والسداد للجميع.

قائمة المختصرات

باللغة العربية:

ج. ر	الجريدة الرسمية
ع	العدد
مج	المجلد
ص	الصفحة
ق.ع. ج	قانون العقوبات الجزائري
ق.إ.ج.ج	قانون الإجراءات الجزائية الجزائري

باللغة الأجنبية:

P	Page
pp	Pages
Vol	Volume
No	Number
DOI	Digital Object Identifier
IJARCCE	International Journal of Advanced Research in Computer and Communication Engineering

مقدمة

شهد العالم خلال العقود الأخيرة تطورا تكنولوجيا متسارعا في مجال تكنولوجيا الإعلام والاتصال، خاصة مع التطورات الحديثة المرتبطة بالذكاء الاصطناعي والوسائط الرقمية، الأمر الذي رافقه توسع كبير في استعمال الأنظمة المعلوماتية في مختلف مجالات الحياة، سواء على مستوى الأفراد أو المؤسسات، مما أسهم في تسهيل المعاملات وتبادل المعلومات وتحقيق قدر كبير من السرعة والفعالية في أداء مختلف الأنشطة.

غير أنّ هذا التطور التقني، وعلى الرغم من مزاياه المتعددة، أفرز بالمقابل صورا مستحدثة من الإجرام ارتبطت بالبيئة الرقمية نتيجة سوء استغلال الوسائل التكنولوجية الحديثة، حيث ظهرت أنماط إجرامية جديدة تجاوزت في طبيعتها وأساليب ارتكابها الحدود التقليدية للجريمة، وفي مقدمتها الجريمة الإلكترونية التي أصبحت من أبرز التحديات القانونية والأمنية التي تواجه الدول الحديثة.

وفي ظل هذا التحول الرقمي، برزت الجريمة الإلكترونية كصورة إجرامية ذات طبيعة خاصة، تُرتكب عبر شبكات الحاسوب والأنظمة المعلوماتية، وتمتاز بجملة من الخصائص التي تميزها عن الجرائم التقليدية، لاسيما طابعها التقني وغير المادي، وسهولة ارتكابها، وسرعة انتشار آثارها، فضلا عن طابعها العابر للحدود، وهو ما يجعل اكتشافها وإثباتها أكثر تعقيدا مقارنة بالجرائم التقليدية. كما يعتمد المجرم المعلوماتي على وسائل تقنية متطورة لطمس آثار الجريمة وإخفاء الأدلة الرقمية، خاصة وأن محل الاعتداء في هذا النوع من الجرائم لا ينصب على أشياء مادية، وإنما على المعطيات والأنظمة والمعلومات الإلكترونية.

وأمام خصوصية هذا النوع من الإجرام، كشفت الجريمة الإلكترونية عن محدودية القواعد التقليدية للقانون الجنائي، سواء من حيث التجريم أو من حيث إجراءات البحث والتحري والإثبات، الأمر الذي فرض على التشريعات الحديثة ضرورة تبني آليات قانونية متخصصة تتلاءم مع خصوصية هذا النوع من الجرائم، بما يضمن تحقيق حماية فعالة للأنظمة المعلوماتية والمعطيات الرقمية، مع المحافظة في الوقت ذاته على الحقوق والحريات الأساسية للأفراد.

وتزداد خطورة الجريمة الإلكترونية بالنظر لما قد يترتب عنها من اعتداءات تمس بالحياة الخاصة وحرية الأفراد، من خلال اختراق الحسابات وسرقة البيانات الشخصية واستغلالها في الابتزاز أو النصب أو التداول غير المشروع، فضلا عن المساس بالمصالح الاقتصادية

للمؤسسات من خلال سرقة المعلومات والاعتداء على الأنظمة المعلوماتية والمعاملات الإلكترونية، وهو ما جعل مكافحتها تكتسي أهمية بالغة على المستويين الوطني والدولي. وفي هذا الإطار، سعى المشرع الجزائري إلى مواكبة التطورات المرتبطة بالإجرام الإلكتروني من خلال إرساء منظومة قانونية متكاملة تهدف إلى الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك بموجب القانون رقم 09-04، إلى جانب تدعيم أحكام قانون العقوبات بالنصوص المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فضلا عن استحداث آليات إجرائية خاصة ضمن قانون الإجراءات الجزائية تتلاءم مع خصوصية هذا النوع من الجرائم من حيث التحري والتحقيق والإثبات. كما عزز المشرع هذه المنظومة بجملة من القوانين الخاصة المرتبطة بحماية المعطيات الشخصية وتنظيم الاتصالات الإلكترونية والتوقيع والتصديق الإلكترونيين، إلى جانب إنشاء هيئات أمنية وقضائية وتقنية متخصصة تتولى الوقاية من الجريمة الإلكترونية ومكافحتها.

أهمية الدراسة:

تكتسي هذه الدراسة أهمية علمية بالنظر إلى تناولها لموضوع الجريمة الإلكترونية باعتباره من المواضيع القانونية الحديثة التي فرضت نفسها على الساحة الجنائية المعاصرة، خاصة في ظل التطور المتسارع لتكنولوجيات الإعلام والاتصال وتزايد الاعتماد على الأنظمة المعلوماتية والوسائط الرقمية في مختلف المجالات. كما تزداد أهمية هذا الموضوع بالنظر إلى ما تثيره الجريمة الإلكترونية من إشكالات قانونية متعلقة بخصوصية التجريم والإثبات والتحقيق، الأمر الذي دفع بالمشرع الجزائري إلى استحداث منظومة قانونية خاصة لمواجهتها. ومن هذا المنطلق، تتجلى الأهمية العلمية لهذه الدراسة في سعيها إلى تحليل الإطار القانوني الذي اعتمده المشرع الجزائري لمكافحة الجريمة الإلكترونية، من خلال دراسة مختلف الآليات الموضوعية والإجرائية والمؤسسية المقررة في التشريع الجزائري، مع الوقوف على أهم المستجدات القانونية التي مست هذا المجال، لاسيما التعديلات الأخيرة الواردة على قانون العقوبات وقانون الإجراءات الجزائية، بما يساهم في إثراء البحث العلمي في مجال القانون الجنائي والعلوم الجنائية، وإبراز خصوصية السياسة الجنائية الجزائرية في مواجهة هذا النوع من الجرائم.

أما الأهمية العملية لهذه الدراسة، فتبرز من خلال ارتباطها الوثيق بالواقع العملي والتطورات التكنولوجية الراهنة، لاسيما مع التوسع المتزايد في استعمال الوسائل التكنولوجية الحديثة وتطبيقات الذكاء الاصطناعي، وما صاحب ذلك من تطور أساليب ارتكاب الجرائم الإلكترونية وتزايد مخاطرها على الأفراد والمؤسسات. كما تسعى هذه الدراسة إلى تسليط الضوء على فعالية الآليات القانونية والإجرائية المعتمدة في الكشف عن الجرائم الإلكترونية وإثباتها، مع إبراز دور الهيئات الأمنية والقضائية والتقنية المختصة في مكافحتها، بما قد يساهم في دعم الجهود الرامية إلى تطوير المنظومة القانونية الجزائية وتعزيز فعاليتها في مواجهة هذا النوع من الجرائم.

إشكالية الدراسة:

وإزاء ما تثيره الجريمة الإلكترونية من تحديات قانونية وعملية، تطرح هذه الدراسة الإشكالية الرئيسية الآتية:

فيم تتمثل الآليات القانونية التي كرسها المشرع الجزائري لمجابهة الجريمة الإلكترونية؟

وتتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية، من أهمها:

- 1- ما هي صور التجريم التي أقرها المشرع الجزائري للأفعال المكونة للجريمة الإلكترونية؟
- 2- ما هي الجزاءات الجنائية المقررة للأفعال الإجرامية، سواء بالنسبة للشخص الطبيعي أو الشخص المعنوي؟
- 3- ما هو دور الآليات الإجرائية المعتمدة في التحقيق والإثبات في الجرائم الإلكترونية؟
- 4- ما هي حجية الدليل الإلكتروني في الإثبات الجنائي؟
- 5- ما هو الدور الذي تؤديه الهيئات القضائية والوقائية والتقنية المختصة في مكافحة الجريمة الإلكترونية في الجزائر؟

أهداف الدراسة:

تهدف هذه الدراسة إلى إبراز مختلف الآليات القانونية التي اعتمدها المشرع الجزائري لمجابهة الجريمة الإلكترونية، من خلال تحليل النصوص الموضوعية والإجرائية المنظمة لهذا النوع من الجرائم، وبيان مدى خصوصيتها مقارنة بالجرائم التقليدية، لاسيما فيما يتعلق بالتجريم والعقاب وإجراءات البحث والتحري والإثبات.

كما تسعى هذه الدراسة إلى الوقوف على أهم المستجدات التشريعية التي عرفها مجال مكافحة الجريمة الإلكترونية في الجزائر، خاصة التعديلات الأخيرة الواردة على قانون العقوبات وقانون الإجراءات الجزائية، مع تسليط الضوء على الأحكام القانونية المتعلقة بالدليل الإلكتروني والآليات المستحدثة المعتمدة في التحقيق في الجرائم الإلكترونية.

وتهدف الدراسة كذلك إلى إبراز دور الهيئات الأمنية والقضائية والتقنية المختصة في الوقاية من الجريمة الإلكترونية ومكافحتها، مع تقييم مدى فعالية المنظومة القانونية الجزائرية في مواجهة هذا النوع من الجرائم، وصولاً إلى تقديم بعض الاقتراحات والتوصيات التي من شأنها تعزيز فعالية آليات مكافحتها ومواكبة التطورات التكنولوجية الحديثة.

أسباب اختيار الموضوع:

في ضوء ما تقدّم، تم اختيار هذا الموضوع استناداً إلى أسباب ذاتية وأخرى موضوعية:

- **من الناحية الذاتية:** يعود اختيارنا لهذا الموضوع إلى اهتمامنا بتخصص القانون الجنائي، خاصة بعد إعادة فتح هذا التخصص بكلية الحقوق والعلوم السياسية بجامعة محمد خيضر بسكرة، وهو ما عزز رغبتنا في التعمق في دراسة القضايا الجنائية المستجدة. كما يرجع اختيار هذا الموضوع إلى اهتمامنا بالجريمة الإلكترونية باعتبارها من أبرز الظواهر الإجرامية المعاصرة المرتبطة بالتطور التكنولوجي، وما تثيره من إشكالات قانونية تستدعي البحث في الآليات القانونية المعتمدة لمجابهتها في التشريع الجزائري.

- **من الناحية الموضوعية:** تتمثل أسباب اختيار هذا الموضوع في الانتشار المتزايد للجرائم الإلكترونية وما تثيره من مخاطر تمس الأفراد والمؤسسات على المستويات الأمنية والاجتماعية والاقتصادية، خاصة في ظل التطور المستمر لتكنولوجيات الإعلام والاتصال وتطبيقات الذكاء الاصطناعي. كما يعود اختيار هذا الموضوع إلى أهمية دراسة الجوانب القانونية والإجرائية المرتبطة بمكافحة الجريمة الإلكترونية، بالنظر إلى خصوصية هذا النوع من الجرائم وما يطرحه من صعوبات تتعلق بالتحقيق والإثبات، إضافة إلى أهمية الوقوف على مدى فعالية المنظومة القانونية الجزائرية في مواجهة هذا النوع من الإجرام.

الصعوبات المعترضة للدراسة:

لم تكن هذه الدراسة بمنأى عن بعض الصعوبات التي اعترضت إنجازها، بالنظر إلى طبيعة موضوع الجريمة الإلكترونية وتشعب جوانبه القانونية والتقنية. ومن أبرز هذه الصعوبات

الطابع التقني لبعض المفاهيم المرتبطة بالجرائم الإلكترونية، خاصة ما تعلق بالأنظمة المعلوماتية والدليل الإلكتروني ووسائل التحقيق الحديثة، الأمر الذي استدعى الإلمام بالجوانب التقنية إلى جانب الجوانب القانونية.

كما واجهتنا صعوبة تتعلق بتعدد التشريعات المنظمة للجريمة الإلكترونية وتوالي التعديلات القانونية المرتبطة بها، فضلا عن تداخل الأحكام القانونية بين القواعد الموضوعية والإجرائية والقوانين الخاصة، وهو ما تطلب قدرا من الدقة والتركيز من أجل الإحاطة بمختلف الآليات القانونية المعتمدة لمجابهة هذا النوع من الجرائم في التشريع الجزائري.

الدراسات السابقة:

استندت هذه الدراسة إلى مجموعة من الدراسات العلمية التي تناولت موضوع الجريمة الإلكترونية وآليات مكافحتها، ومن أبرز هذه الدراسات:

– أطروحة دكتوراه للباحثة بعقيقي عير (2017-2018)، بعنوان: "مكافحة الجريمة الإلكترونية في التشريعين الجزائري والإماراتي - دراسة مقارنة"، تخصص النظام الجزائي والسياسة الجزائية المعاصرة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة. وقد تناولت هذه الدراسة الأحكام الموضوعية والإجرائية المتعلقة بمكافحة الجريمة الإلكترونية في كل من التشريع الجزائري والتشريع الإماراتي، مع إبراز أوجه المقارنة بينهما في مجال التجريم والعقاب وإجراءات المتابعة والتحقيق.

– مذكرة ماجستير للباحثة أمال قارة (2002)، الموسومة بـ: "الجريمة المعلوماتية"، والتي تعد من الدراسات المبكرة التي تناولت هذا الموضوع في مرحلة كان فيها التشريع الجزائري يفتقر إلى نصوص خاصة تنظم الجرائم المعلوماتية قبل صدور القانون رقم 09-04، حيث ركزت على تحديد مفهوم الجريمة المعلوماتية ومحاولة تكييفها ضمن القواعد العامة لقانون العقوبات، مع إبراز مظاهر الفراغ التشريعي آنذاك، وهو ما ساهم في تأصيل الدراسة الحالية وفهم الخلفية التشريعية التي سبقت تدخل المشرع الجزائري بنصوص خاصة.

– أطروحة دكتوراه للباحث عبد القادر مصطفى (2021-2022)، الموسومة بـ: "الآليات الجزائية الموضوعية لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، والتي تناولت بالدراسة والتحليل القواعد الموضوعية المتعلقة بتجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات والعقوبات المقررة لها في كل من قانون العقوبات والقانون رقم 09-04، مع

التركيز على مدى فعالية النصوص العقابية في الحد من الجرائم المعلوماتية، وهو ما وفر إطارا مرجعيا مهما للدراسة الحالية في جانبها المتعلق بالآليات الموضوعية لمكافحة الجريمة الإلكترونية.

ومن خلال استعراض هذه الدراسات، يتضح أنها ركزت أساسا على الجوانب الموضوعية أو المفاهيمية أو المقارنة للجريمة الإلكترونية، في حين تسعى الدراسة الحالية إلى معالجة موضوع آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري معالجة شاملة تجمع بين الجوانب الموضوعية والإجرائية والمؤسسية، مع التطرق إلى أهم المستجدات التشريعية الحديثة، لاسيما استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 11-21، إلى جانب التعديلات الأخيرة التي مست قانون العقوبات بموجب القانون رقم 06-24، وكذا قانون الإجراءات الجزائية بموجب القانون رقم 14-25، وهو ما يشكل إضافة علمية لهذه الدراسة مقارنة بالدراسات السابقة.

منهج الدراسة:

اعتمدت هذه الدراسة على كل من المنهج الوصفي والمنهج التحليلي. حيث تم الاعتماد على المنهج الوصفي من خلال وصف مختلف النصوص القانونية المنظمة للجريمة الإلكترونية في التشريع الجزائري، سواء تعلق الأمر بالقواعد الموضوعية المرتبطة بالتجريم والعقاب، أو القواعد الإجرائية المتعلقة بالتحري والتحقيق والإثبات، إلى جانب عرض مختلف الهيئات المختصة بمكافحة هذا النوع من الجرائم.

أما المنهج التحليلي، فتم الاعتماد عليه من خلال تحليل النصوص القانونية المتعلقة بالجريمة الإلكترونية، والوقوف على أهم المستجدات التشريعية التي عرفها هذا المجال، مع تقييم مدى فعالية الآليات القانونية المعتمدة لمجابهة الجريمة الإلكترونية في التشريع الجزائري.

تقسيم الدراسة:

من أجل الإحاطة بجوانب الموضوع محل الدراسة، ومعالجة الإشكالية المطروحة والتساؤلات المتفرعة عنها، وبلوغ الأهداف المرجوة، ارتأينا تقسيم هذه الدراسة إلى فصلين على النحو الآتي:

جاء الفصل الأول بعنوان: الآليات الموضوعية لمكافحة الجريمة الإلكترونية، موزعا على مبحثين؛ خصص المبحث الأول لدراسة تجريم الأفعال المكونة للجريمة الإلكترونية،

حيث تناول المطلب الأول الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفق قانون العقوبات، مقسما إلى الجرائم الماسة بالأنظمة المعلوماتية والجرائم الماسة بالمعطيات المعلوماتية داخل النظام، في حين ركّز المطلب الثاني على الجرائم الإلكترونية في القوانين الخاصة المكملة، من خلال دراسة تجريم الاعتداء على المعطيات ذات الطابع الشخصي في القانون رقم 07-18، وتجريم الاعتداءات المرتبطة بقطاع البريد والاتصالات الإلكترونية في القانون رقم 04-18.

بينما خصّص المبحث الثاني لتناول الجزاءات المقررة للأفعال المكونة للجريمة الإلكترونية، مع إبراز أحكام الشروع والمساهمة والعقوبات على الأشخاص الطبيعيين والمعنويين.

أما الفصل الثاني فقد جاء بعنوان: الآليات الإجرائية والمؤسسية لمكافحة الجريمة الإلكترونية، ويتضمن بدوره مبحثين؛ جاء المبحث الأول موسوما ب: الآليات الإجرائية لمكافحة الجريمة الإلكترونية، حيث تطرق المطلب الأول إلى آليات التحقيق الجنائي، كما تناول الدليل الإلكتروني كآلية مستحدثة في إثبات الجريمة الإلكترونية.

بينما خصّص المبحث الثاني لدراسة الآليات المؤسسية لمكافحة الجريمة الإلكترونية، من خلال استعراض الهيئات الوقائية والقضائية والتقنية والأمنية المختصة في كشف الجرائم الإلكترونية ضمن مطلبين منفصلين.

ونختم الدراسة بعرض أبرز النتائج التي توصلنا إليها، مع تقديم مجموعة من الاقتراحات العملية لتعزيز فعالية آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري.

الفصل الأول:

الآليات الموضوعية لمكافحة الجريمة الإلكترونية

Substantive Mechanisms for Combating
Cybercrime

الفصل الأول: الآليات الموضوعية في مكافحة الجريمة الإلكترونية

مع التطور المتسارع لتكنولوجيات الإعلام والاتصال واعتماد الأفراد والمؤسسات عليها في مختلف المجالات، برزت الجريمة الإلكترونية كظاهرة جنائية حديثة تتسم بالتعقيد والسرعة والامتداد العابر للحدود، الأمر الذي كشف محدودية النصوص التقليدية للقانون الجنائي وعدم كفايتها لمواجهة خصوصيات الإجرام في الفضاء الرقمي، لهذا تدخل المشرع الجزائري بإرساء إطار قانوني متخصص، وذلك بموجب القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹، معتمدا مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" بدلا من "الجريمة الإلكترونية"².

ويستكمل هذا الإطار بإحالة هذه الجرائم، إلى أحكام قانون العقوبات³ لتحديد أركانها والجزاءات المقررة لها، فضلا عن تدعيمه بجملة من النصوص الخاصة، لاسيما القوانين المتعلقة بحماية المعطيات ذات الطابع الشخصي⁴، والبريد والاتصالات الإلكترونية⁵، والتوقيع والتصديق الإلكترونيين⁶، بما يعكس توجهها نحو إرساء منظومة قانونية متكاملة ومرنة لمكافحة الجريمة الإلكترونية.

¹ القانون رقم 09-04، المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، ع 47، صادرة في 16 أوت 2009.

² تنص المادة 2 من نفس القانون على أن هذا النوع من الجرائم يشمل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وكذا كل جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

³ الأمر رقم 66-156، المؤرخ في 8 جوان 1966، يتضمن قانون العقوبات، ج ر، ع 49، صادرة في 11 جوان 1966، المعدل والمتمم.

⁴ القانون رقم 18-07، المؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، ع 34، صادرة في 10 جوان 2018.

⁵ القانون رقم 18-04، المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر، ع 27، صادرة في 13 ماي 2018، المعدل والمتمم بالقانون رقم 25-11، المؤرخ في 24 جويلية 2025، ج ر، ع 48، الصادرة في 24 جويلية 2025.

⁶ القانون رقم 15-04، المؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر، ع 06، صادرة في 10 فيفري 2015.

الفصل الأول: الآليات الموضوعية في مكافحة الجريمة الإلكترونية

وفي ضوء هذا الإطار، يهدف هذا الفصل إلى استعراض الآليات الموضوعية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، من خلال دراسة تجريم الأفعال المكونة لها في قانون العقوبات والتشريعات الخاصة (المبحث الأول)، ثم بيان الجزاءات المقررة لها في إطار السياسة العقابية المعتمدة (المبحث الثاني).

المبحث الأول

تجريم الأفعال المكونة للجريمة الإلكترونية

Criminalization of Acts Constituting Cybercrime

يشكل التجريم الجنائي الأساس الذي يركز عليه المشرع الجزائري في مكافحة الجريمة الإلكترونية، من خلال تحديد الأفعال المجرّمة وضبط نطاقها القانوني في مواجهة السلوكيات المستحدثة التي أفرزها تطور تكنولوجيات الإعلام والاتصال، وقد سعى المشرع إلى إرساء منظومة قانونية متكاملة لحماية أنظمة المعالجة الآلية للمعطيات المعلوماتية من مختلف صور الاعتداء التي قد تطالها، عبر إدراج نصوص ضمن قانون العقوبات إلى جانب قواعد خاصة تستجيب لخصوصيات البيئة الرقمية.

وعلى هذا الأساس، يتناول هذا المبحث تجريم الأفعال المكونة للجريمة الإلكترونية، من خلال دراسة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات المعدل والمتمم¹ (المطلب الأول)، ثم الجرائم المنصوص عليها في التشريعات الخاصة (المطلب الثاني)، قصد إبراز ملامح الإطار القانوني المعتمد في مجال مكافحة الجريمة الإلكترونية.

¹ القانون رقم 24-06، المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156، يتضمن قانون العقوبات، ج ر، ع 30، الصادرة في 30 أبريل 2024.

المطلب الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفق قانون العقوبات

يعتبر تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات من أبرز مظاهر تطور السياسة الجنائية المعاصرة، في ظل ما يشكله الاعتداء على الأنظمة المعلوماتية والمعطيات الرقمية من تهديد لأمن المعلومات وسلامة المعاملات الإلكترونية.

وفي هذا الإطار، أدرج المشرع الجزائري، بموجب تعديل قانون العقوبات، مجموعة من النصوص الجزائية ضمن المواد 394 مكرر إلى 394 مكرر 8، بهدف توفير حماية قانونية للأنظمة المعلوماتية والمعطيات المعالجة داخلها من مختلف صور الاعتداء.

ويقصد بأنظمة المعالجة الآلية للمعطيات تلك المنظومات التقنية التي تتيح معالجة المعلومات بصفة آلية، باعتبارها محل الحماية الجنائية في هذا النوع من الجرائم.¹ وعلى هذا الأساس، جرم المشرع الجزائري مجموعة من الأفعال التي تستهدف هذه الأنظمة أو المعطيات المعالجة داخلها، سواء تعلّق الأمر بالمساس بالأنظمة المعلوماتية ذاتها (الفرع الأول) أو بالمعطيات المخزنة والمعالجة فيها (الفرع الثاني).

الفرع الأول: الجرائم الماسة بالأنظمة المعلوماتية

تمتد الجريمة الإلكترونية لتشمل الأنظمة المعلوماتية ذاتها باعتبارها منظومة متكاملة، بما في ذلك ما قد يطلها من أفعال تمس سلامة عملها أو تعطل وظائفها أو تستهدف مكوناتها المادية والبرمجية.

وقد عرفت المادة الثانية من القانون رقم 04-09 في فقرتها "ب"، المنظومة المعلوماتية بأنها: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منه أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

¹ لم يضع المشرع الجزائري تعريفا دقيقا لأنظمة المعالجة الآلية للمعطيات ضمن قانون العقوبات، غير أنه يمكن استخلاص مفهومها من القانون رقم 04-09، كما عرّفها الفقه بأنها مجموعة من الوسائل التقنية المترابطة (مادية وبرمجية) التي تمكّن من إدخال البيانات ومعالجتها وتخزينها واسترجاعها بصفة آلية. راجع في ذلك: آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار دار هوم للطباعة والنشر والتوزيع، الجزائر، 2007، ص 102.

تأسيسا على ما تقدّم، يتناول هذا الفرع الجرائم المرتبطة بالولوج غير المشروع، بما يشمل الدخول والبقاء غير المشروع داخل النظام (أولا)، وكذا الجرائم التي تمس بسير النظام ووظائفه، من خلال الإخلال بسلامته أو تعطيل عمله أو الاستعمال غير المشروع له (ثانيا).

أولا: جرائم الولوج غير المشروع إلى الأنظمة المعلوماتية

تعتبر جرائم الولوج غير المشروع من أبرز صور الاعتداء على الأنظمة المعلوماتية، إذ تنصب على اختراقها والدخول إليها دون ترخيص، بما يشكل انتهاكا لحرمتها وسلامة وظائفها، ويندرج هذا السلوك ضمن ما يعرف بالقرصنة المعلوماتية.¹

ومن الناحية القانونية، تقوم هذه الجرائم على صورتين أساسيتين: الدخول غير المشروع إلى النظام، والبقاء غير المشروع داخله، باعتبارهما الأساس الذي تتبني عليه باقي صور الاعتداء على الأنظمة والمعطيات.

1- جريمة الدخول غير المشروع إلى النظام المعلوماتي:

يقوم تجريم الدخول غير المشروع إلى النظام المعلوماتي على اعتبار أن الولوج إليه يمثل المدخل الأساسي لأي تعامل معه، مما يجعل تنظيم حق الدخول وضبطه أساسا للحماية القانونية. ولهذا اتجهت التشريعات الحديثة إلى تجريم كل دخول غير مرخص به، باعتباره مرحلة تمهيدية لاعتداءات أخطر قد تمس بالمعطيات أو تعرقل سير الأنظمة.²

وفي هذا الإطار، نصت المادة 394 مكرر من قانون العقوبات، المعدلة بالقانون رقم 06-24، على معاقبة كل من يدخل أو يبقى عن طريق الغش في منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

ويستفاد من هذا النص أن المشرع تبنى مفهوما واسعا يشمل كل ولوج يتم بوسائل احتيالية لتجاوز أنظمة الحماية.

¹ عبد القادر مصطفىاوي، الآليات الجزائية الموضوعية لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أطروحة دكتوراه في القانون العام، تخصص قانون جنائي وعلم الإجرام، كلية الحقوق، جامعة الجزائر 1، 2021/2022، ص 96.

² نفس المرجع، ص 97.

وتقوم هذه الجريمة على ركنين: ركن مادي يتمثل في فعل الولوج غير المشروع¹، وركن معنوي يقوم على توافر القصد الجنائي بعنصره العلم والإرادة.²

أ- الركن المادي:

يتحقق الركن المادي لهذه الجريمة من خلال قيام الجاني بنشاط إجرامي إيجابي يتمثل في الدخول إلى نظام المعالجة الآلية للمعطيات أو أحد مكوناته، بما يقتضي تدخلا فعلياً يهدف إلى تجاوز الوسائل التقنية أو المنطقية لحماية النظام³، ولا يتحقق الركن المادي عن طريق الامتناع أو النشاط السلبي، إذ يشترط تدخل مباشر من الجاني.⁴

ولا تقتصر الجريمة على فئة معينة من الأشخاص؛ فهي يمكن أن تصدر عن أي شخص مهما كانت صفته أو خبرته أو مهنته، سواء كان متخصصاً في المجال المعلوماتي أو لا، وسواء كان قادراً على الاستفادة من الدخول أم لا، مما يعكس الطابع العام للتجريم الذي يهدف إلى حماية النظام في حد ذاته.⁵

يشمل مفهوم الدخول كل الأفعال التي تتيح الولوج إلى النظام أو التحكم في البيانات التي يحتويها، سواء بصورة مباشرة أو غير مباشرة، على أن يكون الدخول غير مشروع، أي تم دون سند قانوني أو إذن من الجهة المخولة بذلك⁶، ولم يقيد المشرع وسيلة الدخول، فتتحقق الجريمة باستخدام أي وسيلة تقنية أو منطقية، بما في ذلك:

- استخدام كلمة سر تخص شخصاً آخر أو برنامجاً خاصاً.
- استخدام الشفرات أو الرموز المسموح بها جزئياً من قبل آخرين.

¹ أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الديوان الوطني للأشغال التربوية، الجزائر، 2002، ص 47.

² محمد حماد مرهج الهيتي، جرائم الحاسوب: ماهيتها - موضوعها - أهم صورها والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع، عمان، الأردن، 2006، ص 182.

³ عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، مصر، 2002، ص 28، 29.

⁴ عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونياً، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، 2000، ص 600.

⁵ نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، ص 343.

⁶ محمد حماد مرهج الهيتي، المرجع السابق، ص 183.

- الدخول عبر حساب شخص مخول قانونيا.

وتكتمل الجريمة بمجرد دخول الجاني إلى النظام كله أو جزء منه، بما في ذلك تجاوز الحدود المسموح بها في برامج معينة، حتى لو كان النظام نفسه متاحا للجمهور¹، فعلى سبيل المثال، إذا دخل شخص إلى موقع عام للبيع الإلكتروني، لكنه تجاوز الصفحات العامة إلى إعدادات حساسة أو بيانات محمية، فإن هذا يعد دخولا غير مشروع، بينما يظل مجرد الاطلاع على الشاشة دون الدخول الفعلي إلى النظام غير كاف لتكوين الركن المادي للجريمة.²

ومن الناحية الفقهية، يعد مصطلح "الاتصال بالنظام المعلوماتي" أدق في التعبير عن هذا السلوك، إذ يكفي لقيام الجريمة تحقق اتصال فعلي بين الجاني والنظام، ويظل المعيار الحاسم هو مدى توافر الحق في هذا الاتصال، سواء تعلق الأمر بكامل النظام أو جزء منه.³ أما طبيعة هذه الجريمة، فهي من الجرائم الشكلية التي لا تتطلب تحقق نتيجة مادية معينة، إذ يكفي مجرد فعل الدخول غير المشروع، كما أنها جريمة مستمرة طالما استمر الاتصال غير المشروع بالنظام، ما يجعل الاعتداء قائما طوال فترة التواجد فيه دون وجه حق.

ب- الركن المعنوي:

يشترط لقيام جريمة الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات توافر القصد الجنائي، الذي يمثل الرابطة النفسية بين السلوك الإجرامي وإرادة الجاني، وعلى هذا الأساس، لا تتحقق المسؤولية الجزائية إلا إذا اتجهت إرادة الفاعل إلى ارتكاب الفعل المجرم مع علمه بعدم مشروعيته.

وتعد هذه الجريمة من الجرائم العمدية التي يتخذ فيها الركن المعنوي صورة القصد الجنائي العام القائم على عنصري العلم والإرادة، إذ يتعين أن يكون الجاني مدركا لكون دخوله غير مشروع، وأن تتجه إرادته رغم ذلك إلى تحقيق هذا الدخول.⁴

¹ مسعود خثير، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010، ص 115، 116.

² عبد الفتاح بيومي حجازي، المرجع السابق، ص 30.

³ عبد الله سليمان، شرح قانون العقوبات الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2002، ص 321.

⁴ آمال قارة، الجريمة المعلوماتية، مذكرة ماجستير، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2002، ص 60.

وبالمقابل، ينتفي قصد الجنائي إذا كان الدخول مشروعاً أو تم نتيجة غلط في الواقع، كأن يعتقد الجاني بحسن نية أن له الحق في الدخول، أو يجهل القيود المفروضة عليه، وهو ما يؤدي إلى انتفاء المسؤولية لغياب العلم بعدم المشروعية.

كما لا يؤثر الباعث على ارتكاب الفعل في قيام القصد الجنائي، إذ يظل هذا الأخير قائماً متى توافر عنصره، بغض النظر عن الدافع، سواء كان الفضول أو الرغبة في التحدي أو اختبار القدرات التقنية.¹

غير أنه، وبالرجوع إلى نص المادة 394 مكرر، يتبين أن المشرع لم يكتف بتوافر القصد الجنائي العام، بل اشترط قيام قصد خاص يتمثل في استعمال الغش كوسيلة لتحقيق الدخول، وهو ما يقتضي ثبوت نية التحايل لتجاوز وسائل الحماية المفروضة على النظام.² وأخيراً، ووفقاً للقواعد العامة، يجب أن يكون القصد الجنائي معاصراً للسلوك الإجرامي، بحيث يتوافر منذ لحظة مباشرة الفعل، فإذا وقع الدخول ابتداءً عن طريق الخطأ دون توافر القصد، انتفت الجريمة في هذه المرحلة، غير أنه إذا استمر الشخص في التواجد داخل النظام رغم علمه بعدم مشروعية ذلك، فإن سلوكه يندرج ضمن جريمة مستقلة تتمثل في البقاء غير المصرح به داخل النظام المعلوماتي.

2- جريمة البقاء غير المشروع داخل النظام المعلوماتي:

عالج المشرع الجزائري جريمة البقاء غير المصرح به ضمن أحكام المادة 394 مكرر من قانون العقوبات، ويستفاد من هذا النص أن نطاق التجريم لا يقتصر على فعل الدخول غير المشروع فحسب، بل يمتد ليشمل كذلك كل استمرار غير مبرر في التواجد داخل النظام المعلوماتي.³

¹ محمد حماد مرهج الهيتي، المرجع السابق، ص 87.

² نسيم دردور، جرائم المعلوماتية في ضوء القانون الجزائري والمقارن، مذكرة ماجستير، شعبة القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة، 2013، ص 34.

³ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر، 2004، ص 235.

وتأسيسا على ذلك، يمكن تعريف البقاء غير المشروع بأنه كل استمرار في التواجد داخل نظام المعالجة الآلية للمعطيات بالمخالفة لإرادة الجهة المخولة قانونا بإدارته أو الترخيص بالولوج إليه، سواء كان هذا التواجد ناشئا عن دخول مشروع أو غير مشروع.¹ كما يشمل هذا المفهوم مختلف صور الاستعمال غير المرخص للنظام، كالإطلاع على المعطيات أو معالجتها أو الاستفادة منها دون سند قانوني.

أ- الركن المادي:

يتحقق الركن المادي من خلال استمرار الاتصال غير المشروع بالنظام المعلوماتي، ويكتمل بمجرد بقاء الجاني داخله رغم علمه بعدم أحقيته في ذلك، ويقاس هذا البقاء بالمدة التي يستمر خلالها في استعمال النظام أو الاستفادة منه دون ترخيص، بحيث تُكتمل الجريمة بمجرد استمرار هذا الوضع، على عكس جريمة الدخول التي تتحقق بمجرد الولوج الفعلي. ويفهم من الفقه أن البقاء غير المشروع يكتسب صفة الجريمة حتى إذا كان الدخول أصلا مشروعاً أو حدث عن طريق الخطأ، إذ يتحول إلى فعل إجرامي بمجرد استمرار الجاني في التواجد داخل النظام بعد علمه بعدم أحقيته.

وفي هذا السياق، يعرف فعل البقاء على أنه: "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام".²

كما يمكن أن يجتمع الركن المادي لجريمة الدخول مع الركن المادي للبقاء، في حالة دخول النظام دون تصريح واستمرار الجاني في التواجد فيه، ليصبح الفعل الواحد مشتملا على جريمتين مترابطتين.³

يشير الفقه إلى ضرورة الفصل الزمني بين الجريمتين لتحديد نطاق كل منهما بدقة، فتتحقق جريمة الدخول غير المشروع منذ اللحظة التي يقوم فيها الجاني بالولوج الفعلي إلى النظام أو أحد مكوناته، سواء كان الدخول مشروعاً أو غير مشروع، أو حتى وقع عن طريق

¹ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر، 1999، ص 601.

² علي عبد القادر القهوجي، المرجع السابق، ص 133.

³ نائلة عادل محمد فريد قروة، المرجع السابق، ص 346.

الخطأ، أما جريمة البقاء غير المشروع، فتبدأ منذ اللحظة التي يدرك فيها الجاني عدم أحقيته في الاستمرار داخل النظام أو عندما يواصل التجوال داخله بعد انتهاء المدة المسموح بها له.¹

ب- الركن المعنوي:

تعد جريمة البقاء غير المشروع من الجرائم العمدية التي يشترط لقيامها توافر القصد الجنائي العام، المتمثل في عنصريه المتلازمين: العلم والإرادة، إذ يقتضي عنصر العلم أن يكون الجاني مدركا تماما لعدم مشروعية تواجده داخل نظام المعالجة الآلية للمعطيات، بينما يتمثل عنصر الإرادة في اختياره البقاء داخل النظام واستمراره في الاتصال به رغم علمه بعدم أحقية ذلك.²

وتتميز جريمة البقاء بأنها شكلية ومستمرة: لا يشترط لقيامها تحقق نتيجة إجرامية محددة، وتستمر حالة الاعتداء طوال مدة بقاء الجاني داخل النظام المعلوماتي دون وجه حق.³

ثانيا: الجرائم الماسة بسير الأنظمة المعلوماتية

لم تعد حماية الأنظمة المعلوماتية تقتصر على منع الولوج غير المشروع إليها، بل امتدت لتشمل ضمان سلامة سيرها ووظائفها الأساسية، إذ يشكل كل مساس بأدائها الطبيعي خطرا حقيقيا على المعطيات والمصالح المرتبطة بها، وهو ما دفع المشرع الجزائري إلى تجريم الأفعال التي تمس بسير هذه الأنظمة، سواء من خلال تشديد العقاب على بعض الصور الإجرامية أو بإقرار تجريم مستقل للاعتداء على وظيفتها.

1- جرائم المساس بسلامة النظام المعلوماتي:

تندرج هذه الصورة ضمن الأشكال المشددة لجريمة الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات، متى ترتب عن ذلك نتائج تمس بسلامة المعطيات أو بنظام اشتغال المنظومة.

¹ علي عبد القادر القهوجي، المرجع السابق، ص 135.

² أمنة أمحمدي بوزينة، خصوصية قواعد التجريم عن الاعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، مجلة بيلوفيليا لدراسات المكتبات والمعلومات، العدد 05، مارس 2020، جامعة العربي التبسي - تبسة، الجزائر، ص 78، 77.

³ نهلة عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص 61.

وقد نصت المادة 394 مكرر، في فقرتيها الثانية والثالثة من قانون العقوبات المعدل بالقانون 06-24، على مضاعفة العقوبة إذا نتج عن الفعل حذف أو تغيير للمعطيات، وتشديدها إذا أدى إلى تخريب نظام اشتغال المنظومة.

ويستفاد من ذلك أن المشرع الجزائري اعتمد معيار النتيجة الضارة كأساس لتشديد العقوبة، باعتبارها أثرا لاقتران الجريمة البسيطة بضرر فعلي، مما يعكس توجهها نحو تعزيز الحماية الجنائية للبيئة المعلوماتية، غير أن حصر هذه النتائج في صور محددة قد يثير إشكالات عملية في استيعاب بعض الأضرار التقنية المستحدثة، رغم أن هذا الظرف المشدد يظل مرتبطا بالأفعال الأصلية المنصوص عليها في الفقرة الأولى من المادة ذاتها.¹

أ- الركن المادي:

يتكون الركن المادي لهذه الجريمة من ثلاثة عناصر مترابطة:

- **السلوك الإجرامي:** ويتمثل في الدخول أو البقاء غير المصرح بهما في نظام المعالجة الآلية للمعطيات.

- **النتيجة الإجرامية:** وتتمثل في إحدى الصور التي حددها المشرع على سبيل الحصر، وهي:

❖ **حذف المعطيات:** ويقصد به إزالة المعلومات من النظام، وهو أخطر صور الاعتداء لما ينطوي عليه من إعدام كلي للبيانات.

❖ **تغيير المعطيات:** ويتمثل في إدخال تعديلات على المعلومات بما يفقدها قيمتها أو دلالتها، مع بقائها من الناحية الشكلية داخل النظام.

❖ **تخريب نظام اشتغال المنظومة:** أي المساس بالوظائف التقنية للنظام بما يجعله غير صالح للاستعمال أو عاجزا عن أداء مهامه.

- **العلاقة السببية:** بحيث يجب أن تكون النتيجة الإجرامية مترتبة مباشرة عن السلوك الإجرامي، وإلا انتفى الظرف المشدد.

وعليه، إذا انتفت العلاقة السببية، كأن تكون النتيجة راجعة إلى سبب أجنبي كالقوة القاهرة أو الحادث الفجائي، فإن الجريمة تقوم في صورتها البسيطة دون المشددة.

¹ البركة الطيبي، المرجع السابق، ص 176.

كما تجدر الإشارة إلى أن نتيجة حذف أو تغيير المعطيات تتقاطع مع جريمة التلاعب بالمعطيات، غير أن الاختلاف الجوهرى بينهما يكمن في الركن المعنوي؛ إذ تكون النتيجة في جريمة التلاعب مقصودة لذاتها، بينما في هذه الصورة المشددة تعد نتيجة غير مقصودة.¹

ب- الركن المعنوي:

تتميز هذه الصورة بخصوصية في الركن المعنوي، إذ أن النتيجة المشددة (حذف، تغيير، أو تخريب) لا يشترط أن تكون مقصودة من الجاني، بل يكفي أن تكون نتيجة غير عمدية مترتبة عن سلوك عمدي يتمثل في الدخول أو البقاء غير المشروع، وقد أكدت ذلك الفقرة الثالثة من المادة 394 مكرر.

يلاحظ أن المشرع يشدد العقاب حتى على النتائج غير المقصودة متى ترتبت عن فعل عمدي، نظرا لخطورتها، وهو ما يثير نقاشا حول مدى مسؤولية الجاني عن نتائج لم يكن يتوقعها.

2- جرائم المساس بوظيفة النظام المعلوماتي:

تمثل هذه الجريمة صورة مستقلة من صور الاعتداء على الأنظمة المعلوماتية، حيث تستهدف الوظيفة الأساسية للنظام والمتمثلة في ضمان السير العادي للمعالجة الآلية للمعطيات.

أ- الركن المادي:

يتجسد الركن المادي في كل فعل من شأنه المساس بالأداء الوظيفي للنظام، ومن ذلك:

- **التعطيل أو التوقيف:** ويقصد به إعاقة السير العادي للنظام، سواء بشكل كلي أو جزئي، بما يؤدي إلى ببطء أو توقف في أداء وظائفه، وقد يتحقق ذلك بالمساس بالمكونات المادية (كإتلاف وسائط التخزين أو قطع الشبكات) أو بالبرمجيات، مما يؤدي إلى فقدان البيانات أو انقطاع الاتصال بين الأجهزة.²

¹ البركة الطيبي، المرجع السابق، ص 178، 179، راجع أيضا: إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة آفاق للبحوث والدراسات، العدد 04، جوان 2019، المركز الجامعي إيليزي، الجزائر، ص 189.

² مسعود خثير، المرجع السابق، ص 121.

- **الإفساد:** ويتمثل في إحداث خلل في النظام يجعله غير قادر على أداء وظائفه بشكل صحيح، وذلك من خلال التلاعب بالبرامج أو البيانات، بما يؤدي إلى نتائج غير دقيقة أو غير متوقعة عند تشغيله.¹

ويترتب عن هذه الأفعال اختلال التوازن الوظيفي للنظام، وفقدانه لقدرته على تقديم الخدمات بصورة سليمة، وهو ما يعكس خطورة هذه الجرائم على الثقة في البيئة الرقمية.

ب- الركن المعنوي:

تعتبر هذه الجريمة من الجرائم العمدية التي تتطلب توافر القصد الجنائي العام بعنصره:

- **العلم:** بإدراك الجاني لطبيعة فعله وآثاره على النظام المعلوماتي.

- **الإرادة:** باتجاه إرادته إلى إحداث التعطيل أو الإفساد.

حيث يعتمد الفاعل الإضرار بالنظام بغرض تحقيق مصلحة غير مشروعة أو الإضرار بالغير، مع علمه بأن سلوكه من شأنه أن يؤدي إلى تعطيل العمليات أو إحداث خسائر مادية أو تقنية.²

الفرع الثاني: الجرائم الماسة بالمعطيات المعلوماتية داخل النظام

لم يقتصر تدخل المشرع الجزائري في مجال مكافحة الجريمة الإلكترونية على تجريم الأفعال الماسة بالأنظمة المعلوماتية في حد ذاتها، بل امتد ليشمل الأفعال التي تستهدف المعطيات داخل هذه الأنظمة، باعتبارها محل الحماية الجنائية وجوهر الاعتداء.

وقد عرفت المادة 02 فقرة (ج) من القانون رقم 04-09 المعطيات المعلوماتية على أنها أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

¹ نبيل ونوغي، الجريمة المعلوماتية في التشريع الجزائري، مجلة العلوم القانونية والاجتماعية، المجلد 04، العدد 03، 2019، جامعة زيان عاشور - الجلفة، الجزائر، ص 136.

² مسعود خثير، المرجع السابق، ص 122.

ومن ثمّ، فإنّ المساس بها يشكل خطراً يفوق، في كثير من الأحيان، مجرد الولوج غير المشروع إلى النظام المعلوماتي، لما قد يترتب عنه من الإضرار بسلامة المعطيات وتكاملها وموثوقيتها.

وعلى هذا الأساس، أقرّ المشرع مجموعة من النصوص الجزائية التي ترمي إلى حماية المعطيات من مختلف صور الاعتداء، سواء تعلّق الأمر بالتلاعب بها بشكل مباشر (أولاً)، أو بالتعامل غير المشروع فيها (ثانياً).

أولاً: جريمة التلاعب غير المشروع بالمعطيات المعلوماتية

تقوم هذه الجريمة على ركنين أساسيين: مادي ومعنوي، وذلك على النحو الآتي:

1- الركن المادي:

نصت المادة 394 مكرر 1 من قانون العقوبات، المعدلة بالقانون 06-24، على معاقبة كل من يدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو يزيل أو يعدّل المعطيات التي يتضمنها.

ويتبيّن من ذلك أن المشرع حصر صور السلوك الإجرامي في ثلاث حالات: إدخال معطيات غير صحيحة، أو حذفها، أو تعديلها، وهي أفعال تنصب جميعها على سلامة المعطيات باعتبارها محل الحماية الجنائية.¹

ويستفاد كذلك أن نطاق التجريم يقتصر على الأفعال التي تمس سلامة أو تكامل المعطيات، دون أن يمتد إلى مجرد نسخها أو نقلها، ما لم يقترن ذلك بأحد الأفعال المجرّمة، وهو ما يعكس تبني المشرع لمفهوم محدد للتلاعب المعلوماتي.

كما تتميز هذه الجريمة باستقلالها عن جرائم الدخول أو البقاء غير المشروع، إذ يمكن أن تتحقق دون ولوج مباشر إلى النظام، كحالات استخدام البرمجيات الخبيثة التي تحدث تغييراً في المعطيات عن بعد.²

¹ زكرياء ذيب، تجريم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 07، العدد 02، 2023، كلية الحقوق والعلوم السياسية، جامعة عمار ثلجي - الأغواط، الجزائر، ص 1307.

² آمال قارة، المرجع السابق، ص 122.

2- الركن المعنوي:

تعد جريمة التلاعب غير المشروع بالمعطيات المعلوماتية من الجرائم العمدية، التي تتطلب توافر القصد الجنائي العام، المتمثل في علم الجاني بعدم مشروعية سلوكه واتجاه إرادته إلى تغيير المعطيات، دون اشتراط تحقق نتيجة ضارة¹، مما يدل على أن المشرع يعاقب على مجرد السلوك الخطر حماية لسلامة الأنظمة المعلوماتية.

ولا تقتصر صفة الفاعل على الغير، بل قد تمتد إلى الأشخاص المصرح لهم بالولوج إلى النظام، متى تجاوزوا حدود الترخيص، وهو ما يوسع من نطاق الحماية ليشمل الأخطار الداخلية.

ويعكس ذلك توجهها تشريعيا حديثا يقوم على حماية سلامة المعطيات كقيمة قانونية مستقلة، غير أن حصر الأفعال المجرّمة قد يثير صعوبات في مواجهة الأساليب التقنية المستحدثة، مما قد يستدعي تطوير النصوص مستقبلا.²

ثانيا: جريمة التعامل غير المشروع في المعطيات ذات المصدر غير المشروع

نصت المادة 394 مكرر 2 من قانون العقوبات الجزائي المعدل والمتمم على تجريم كل تعامل عمدي وغير مشروع بالمعطيات المرتبطة بالجرائم المعلوماتية، سواء كانت وسيلة لارتكابها أو ناتجة عنها، بما يشمل التصميم، التجميع، النشر، الإتجار، الحيازة أو الإفشاء لأي غرض كان.

وتتخذ هذه الجريمة صورتين أساسيتين:

- **المعطيات التي تعد وسيلة لارتكاب الجرائم المعلوماتية**، حيث يتم تجريم كل أشكال التعامل فيها، من تصميم وتجميع وتوفير ونشر واتجار، بما يعكس توجهها وقائيا يهدف إلى تجفيف منابع الجريمة قبل وقوعها.

¹ مسعود، خثير، المرجع السابق، ص 125.

² مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيايات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة ماجستير، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح-ورقلة، الجزائر، 2013، ص 38.

- **المعطيات المتحصّل عليها من جريمة معلوماتية**، حيث يجرمّ المشرع حيازتها أو إفشاءها أو نشرها أو استعمالها، بغض النظر عن الغرض، وهو ما يهدف إلى منع استغلال العائد الإجرامي للمعلوماتية.

ويعكس هذا التوجه توجهها تشريعيا متقدما يقوم على التجريم التبعي، وتوسيع عبارة "لأي غرض كان" يمنح النص شمولية في التجريم، إلا أنه قد يثير إشكالات تتعلق بالتناسب بين الفعل والعقوبة في الحالات محدودة الخطورة.¹

المطلب الثاني: الجرائم الإلكترونية في التشريعات الخاصة

لم يعد الفضاء الرقمي مجرد مجال تقني، بل أضى إطارا قانونيا تتداخل فيه مصالح حماية المعطيات وسلامة الاتصالات وضمان الثقة في المعاملات الإلكترونية، وقد أفرز هذا التحول أنماطا جديدة من الجرائم، استدعت تدخل المشرع الجزائري ليس فقط من خلال قانون العقوبات، بل أيضا عبر تشريعات خاصة تتلاءم مع خصوصية البيئة الرقمية.

وعلى هذا الأساس، يهدف هذا المطلب إلى إبراز أحكام التجريم الإلكتروني في عدة تشريعات خاصة، غير أننا سنقتصر على دراسة بعضها، وذلك عبر ثلاثة فروع رئيسية تشمل الجرائم الماسة بالمعطيات الشخصية (الفرع الأول)، والجرائم المرتبطة بتنظيم الاتصالات الإلكترونية (الفرع الثاني)، وأخيرا الجرائم المتعلقة بالتوقيع والتصديق الإلكترونيين (الفرع الثالث).

الفرع الأول: الجرائم الماسة بالمعطيات الشخصية في القانون رقم 07-18

مع تزايد مخاطر الاعتداء على المعطيات ذات الطابع الشخصي نتيجة التطور الرقمي، تدخل المشرع الجزائري بموجب القانون رقم 07-18 المعدل والمتمم لإرساء إطار قانوني لحماية الأشخاص الطبيعيين عند معالجة هذه المعطيات، مع تحديد الأفعال المجرّمة والعقوبات في المواد 54 إلى 74.

وتتقسم الجرائم الماسة بالمعطيات الشخصية إلى: الجرائم المتعلقة بالقواعد الشكلية للمعالجة (أولا)، الجرائم المتعلقة بالقواعد الموضوعية للمعالجة (ثانيا).

¹ محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، مج 01، ع 01، 2009، جامعة زيان عاشور بالجلفة، الجزائر، ص 384، 385.

أولاً: الجرائم المتعلقة بالقواعد الشكلية للمعالجة

أخضع المشرع الجزائري المسؤول عن المعالجة لجملة من الإجراءات الشكلية المسبقة التي يتعين احترامها قبل الشروع في معالجة المعطيات ذات الطابع الشخصي، ورتّب على مخالفتها قيام مسؤولية جزائية وفقاً لأحكام القانون رقم 07-18 المعدل والمتمم، ويمكن حصر هذه الجرائم فيما يلي:

1- الجرائم المتعلقة بعدم استيفاء الشروط المسبقة للمعالجة:

يترتب عن مخالفة الأحكام المتعلقة بالشروط المسبقة للمعالجة قيام جرائم تتمثل في معالجة المعطيات دون موافقة الشخص المعني أو رغم اعتراضه¹، وكذا إنجاز معالجة دون الحصول على تصريح أو ترخيص².

أ- جريمة معالجة المعطيات الشخصية دون موافقة أو رغم اعتراض الشخص المعني:

تتحقق هذه الجريمة بمخالفة أحكام المادتين 7 و 36 من القانون رقم 07-18³، حيث أوجبت المادة 7 ضرورة الحصول على الموافقة الصريحة للشخص المعني كشرط أساسي لمشروعية المعالجة، في حين خوّلت المادة 36 لهذا الأخير حق الاعتراض على معالجة معطياته الشخصية متى توفرت أسباب مشروعة، كما تتشدد الحماية بالنسبة للمعطيات الحساسة، إذ تنص المادة 1/18 على مبدأ حظر معالجتها⁴، مع إقرار استثناء يتمثل في حالة موافقة الشخص المعني.

وعليه، فإن معالجة هذه المعطيات في غياب هذه الموافقة تشكل جريمة منصوصاً عليها في المادة 57، والمتعلقة بمعالجة معطيات حساسة دون موافقة الشخص المعني⁵.

¹ المادة 55 من القانون رقم 07-18، السالف ذكره.

² المادة 56 من نفس القانون.

³ انظر: المادتين 7 و 36 من نفس القانون.

⁴ انظر: المادة 18 من القانون رقم 07-18، السالف ذكره.

⁵ المادة 57 من نفس القانون.

ب- جريمة إنجاز معالجة للمعطيات الشخصية دون الحصول على تصريح أو ترخيص:

تقوم هذه الجريمة استنادا إلى المادة 56/ف1 من القانون رقم 18-07، نتيجة مخالفة أحكام المادة 12 منه، التي أخضعت معالجة المعطيات ذات الطابع الشخصي لضرورة الحصول المسبق على تصريح أو ترخيص من السلطة الوطنية لحماية المعطيات الشخصية بصفتها الجهة المختصة.

كما وسّع المشرع نطاق التجريم بموجب المادة 56/2، ليشمل تقديم تصريحات كاذبة، أو مواصلة نشاط المعالجة رغم سحب وصل التصريح أو الترخيص الممنوح.¹

2- الجرائم المتعلقة بإجراءات الحماية والتعاون مع السلطة الوطنية:

إلى جانب إخضاع المعالجة للشروط المسبقة، أقرّ المشرع الجزائري التزامات لاحقة تتعلق بضمان أمن المعطيات الشخصية وتعزيز الرقابة عليها، من خلال فرض قواعد خاصة بحمايتها ووجوب التعاون مع السلطة الوطنية لحماية المعطيات الشخصية، ويترتب عن الإخلال بهذه الالتزامات قيام جرائم جزائية، وهو ما يقتضي بيانها على النحو الآتي:

أ- جريمة عدم الالتزام بسلامة وسرية معالجة المعطيات الشخصية:

تقوم هذه الجريمة، وفقا للمادة 65 من القانون رقم 18-07، في حالة إخلال المسؤول عن المعالجة² بالالتزامات المفروضة عليه بموجب المادتين 38 و39 من ذات القانون، والمتعلقتين بضمان سلامة وسرية المعالجة.³

فقد أوجبت المادة 38 اتخاذ التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع، أو الضياع، أو التلف، أو النشر، أو

¹ الزهرة جقريف، الحماية الجزائية للمعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون 18-07، مجلة العلوم القانونية والاجتماعية، مج 06، ع 04، ديسمبر 2021، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور- الجلفة، الجزائر، ص 491.

² انظر: نص المادة 12/03 من القانون رقم 18-07 التي عرفت المسؤول عن المعالجة.

³ انظر: المادة 65 من نفس القانون.

الفصل الأول: الآليات الموضوعية في مكافحة الجريمة الإلكترونية

الولوج غير المرخص، خاصة في حالة نقل المعطيات عبر الشبكات¹، وتشمل هذه التدابير وسائل تقنية كالتشفير، وأنظمة الحماية بكلمات المرور، والبرمجيات الأمنية الكفيلة بمنع الاختراق أو التلاعب بالمعطيات، بما يتناسب مع طبيعة المخاطر المحتملة.²

وعليه، يلتزم المسؤول عن المعالجة ببذل عناية كافية في هذا المجال، إذ إن أي تقصير في اتخاذ هذه التدابير من شأنه أن يلحق ضررا بالأشخاص المعنيين.

من جهة أخرى، ألزمت المادة 39 المسؤول عن المعالجة، في حالة اللجوء إلى معالج من الباطن³، باختيار هذا الأخير على أساس تقديمه لضمانات كافية تتعلق بأمن وسرية المعالجة، مع ضرورة تأطير هذه العلاقة بموجب عقد رسمي يحتج به عند الإخلال بالالتزامات التعاقدية.⁴

ب- جريمة الامتناع عن التعاون مع السلطة الوطنية لحماية المعطيات الشخصية:

حرصا على فعالية الرقابة، جرم المشرع الجزائري، بموجب المادة 61 من القانون رقم 07-18، كل سلوك من شأنه عرقلة عمل السلطة الوطنية لحماية المعطيات الشخصية، ويتخذ هذا السلوك عدة صور، منها الاعتراض على إجراء عمليات التحقق في عين المكان، سواء بوسائل مادية كمنع الدخول أو غلق المحلات أو تعطيل الأجهزة، أو بوسائل تقنية كرفض تمكين الأعوان من كلمات المرور أو وسائل الولوج إلى الأنظمة المعلوماتية.

كما يشمل هذا السلوك رفض تزويد أعوان السلطة الوطنية بالمعلومات والوثائق الضرورية، أو إخفاءها أو إتلافها، أو تقديم معلومات غير مطابقة للحقيقة أو بشكل غير واضح عند الطلب.

¹ انظر: المادة 38 من القانون رقم 07-18، السالف ذكره.

² عز الدين طباش، "الحماية الجزائرية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل قانون 07/18 المعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، المجلة الأكاديمية للبحث القانوني، ع 02، 2018، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر، ص 47.

³ انظر: المادة 13/3 من القانون رقم 07-18 التي عرفت المعالج من الباطن.

⁴ المادة 39 من نفس القانون.

وإلى جانب ذلك، جرم المشرع، بموجب المادة 66 من ذات القانون، عدم قيام مقدم الخدمات بإعلام السلطة الوطنية أو الشخص المعني بكل انتهاك يمس المعطيات الشخصية، وتشمل هذه الانتهاكات، وفقا للمادة 43، حالات إتلاف المعطيات أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، وهو ما يعكس توجه المشرع نحو تكريس مبدأ الشفافية والإخطار كآلية أساسية لحماية المعطيات الشخصية.¹

ثانيا: الجرائم المتعلقة بالقواعد الموضوعية للمعالجة

تتعلق هذه الجرائم بالإخلال بالمبادئ الجوهرية التي تحكم مشروعية معالجة المعطيات ذات الطابع الشخصي، سواء من حيث كيفية جمعها أو كيفية استغلالها، بما يمس بحقوق الأشخاص المعنيين وحياتهم الأساسية.

1- جرائم الجمع غير المشروع للمعطيات الشخصية:

تتعدد صور هذه الجرائم بحسب طبيعة المخالفة، فقد تتصل بأساليب الجمع المستعملة، أو بطبيعة المعطيات محل الجمع، لاسيما تلك المرتبطة بالوضعية الجزائية للشخص المعني.

أ- جريمة استعمال الأساليب غير المشروعة في جمع المعطيات الشخصية:

تعتبر هذه الجريمة من الجرائم التي تقع في المرحلة الأولية للمعالجة، وقد نصت عليها المادة 59 من القانون 07-18 على معاقبة كل من يجمع المعطيات ذات الطابع الشخصي بطريقة تدليسة وغير نزيهة وغير مشروعة.

- الركن المادي:

يتجسد في فعل جمع المعطيات، أي الحصول على معلومات تخص شخصا طبيعيا واحدا أو عدة أشخاص، سواء تم ذلك يدويا أو بوسائل آلية²، وفقا للمادة 04، ويشترط أن تكون

¹ الزهرة جقريف، مرجع سابق، ص 492.

² عز الدين طباش، مرجع سابق، ص 30.

المعطيات ذات طابع شخصي، وأن يتم الجمع باستعمال وسائل تدليسية أو غير نزيهة أو غير مشروعة، كوسائل الخداع أو استغلال النفوذ أو مخالفة القواعد المهنية.¹

- الركن المعنوي:

تعتبر هذه الجريمة عمدية، تقوم على توافر القصد الجنائي، المتمثل في علم الجاني بالطابع الشخصي للمعطيات وبعدم مشروعية الوسائل المستعملة، واتجاه إرادته إلى ارتكاب فعل الجمع بالمخالفة للقانون.²

ب- جريمة جمع المعطيات المتعلقة بالوضعية الجزائية للشخص المعني:

نصت عليها المادة 68 من القانون 07-18 على معاقبة كل من يوضع أو يحفظ في الذاكرة الآلية، المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن.

وتتميز هذه الجريمة بارتباطها بنوع خاص من المعطيات، وبقصرها على المعالجة الآلية. ويتحقق ركنها المادي من خلال سلوك الوضع أو الحفظ في الذاكرة الآلية، أي إدراج هذه المعطيات في نظام معلوماتي أو الإبقاء عليها فيه، وتعد من الجرائم المستمرة في حالة الحفظ. ولا تقوم الجريمة إلا إذا تم هذا السلوك خارج الحالات التي يجيزها القانون.³

2- جرائم الاستغلال غير المشروع للمعطيات الشخصية:

تتصرف هذه الجرائم إلى كل استعمال للمعطيات الشخصية على نحو يخالف الأغراض المحددة لها أو القواعد المنظمة لاستغلالها، بما يشكل انحرافا عن مبدأ تخصيص الغرض وضوابط الحماية القانونية.

وتشمل هذه الجرائم ما يلي:

¹ عز الدين طباش، مرجع سابق، ص 32.

² عبد الوهاب ملياني، الجرائم الماسة بالمعطيات الشخصية على ضوء القانون رقم 07-18، مجلة البحوث القانونية والاقتصادية، مج 06، ع 01، 2023، المركز الجامعي آفلو، الجزائر، ص 276.

³ عز الدين طباش، مرجع سابق، ص 33.

أ- جريمة استعمال المعالجة لأغراض غير تلك المصرح بها أو المرخص بها:

نصت عليها المادة 58 من نفس القانون على معاقبة كل من ينجز أو يستعمل معالجة معطيات لأغراض أخرى غير تلك المصرح أو المرخص بها.

- الركن المادي:

يتحقق عند قيام المسؤول عن المعالجة بتغيير أو توسيع الأغراض التي صرح بها أو رخصت له، بما يخالف ما ورد في التصريح أو الترخيص، خرقاً لأحكام المادة 14 المتعلقة بتحديد الغرض من المعالجة.¹

- الركن المعنوي:

تعتبر هذه الجريمة عمدية، تقوم على علم الجاني بمخالفة الأغراض المصرح بها واتجاه إرادته إلى استغلال المعطيات لتحقيق أهداف مغايرة.

ب- جريمة الاحتفاظ بالمعطيات خارج المدة المحددة:

نصت عليها المادة 65 فقرة 2 من نفس القانون على معاقبة كل من يحتفظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص.

وتقوم هذه الجريمة عند الإبقاء على المعطيات بعد انقضاء مدة حفظها المحددة، خرقاً للبند السادس من المادة 14، مع مراعاة ما نصت عليه المادة 29 بشأن ضرورة عدم تجاوز مدة الحفظ للغرض من المعالجة، مع إمكانية الترخيص بالتمديد لأغراض علمية أو تاريخية أو إحصائية.²

¹ نفس المرجع، ص 53، 54.

² انظر: المادة 29 من القانون 18-03، السالف ذكره.

ج- جريمة السماح لغير المؤهلين بالولوج إلى المعطيات الشخصية:

نصت عليها المادة 60 من نفس القانون على معاقبة كل من سمح لأشخاص غير مؤهلين بالولوج المعطيات ذات طابع شخصي.

- الركن المادي:

يتحقق بكل سلوك إجرامي يفيد تمكين الغير من الاطلاع على المعطيات، كمنح كلمات المرور أو ترك الأنظمة مفتوحة أو عدم منع الولوج رغم العلم به، شريطة أن يكون الشخص غير مؤهل وفقا لما يحدده التصريح أو الترخيص، لاسيما البند 4 من المادة 14.

- الركن المعنوي:

تعد الجريمة عمدية، قوامها علم الجاني بعدم صفة الشخص المخول له الولوج، واتجاه إرادته إلى تمكينه من ذلك، مع إمكانية مساءلة الغير كشريك إذا كان عالما بعدم أحقيته، فضلا عن إمكانية تطبيق نصوص أخرى، كالمادة 394 مكرر من قانون العقوبات في حالة الدخول غير المشروع إلى نظام المعالجة الآلية.¹

الفرع الثاني: الجرائم الماسة بتنظيم الاتصالات الإلكترونية في القانون رقم 04-18

يعتبر القانون رقم 04-18 المتعلق بالبريد والاتصالات الإلكترونية الإطار التشريعي المنظم لقطاع الاتصالات في الجزائر، حيث لم يقتصر على ضبط النشاط وتنظيمه، بل أقر كذلك حماية جزائية لسرية وسلامة الاتصالات الإلكترونية، من خلال تجريم مجموعة من الأفعال التي تمس بالمراسلات أو تعرقل سيرها.

وانطلاقا من ذلك، يمكن تصنيف الجرائم الماسة بتنظيم الاتصالات الإلكترونية إلى جرائم تمس بسرية الاتصالات (أولا)، وأخرى تمس بسلامتها (ثانيا)، على النحو الآتي:

¹ عز الدين طباش، مرجع سابق، ص 55، 56.

أولاً: الجرائم الماسة بسرية الاتصالات الإلكترونية

تهدف هذه الجرائم إلى حماية مضمون المراسلات الإلكترونية من أي تدخل غير مشروع، تكريساً لمبدأ سرية الاتصالات، وهو ما نص عليه القانون رقم 04-18، وخصوصاً المادة 164 منه، التي تنص معاقبة كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها.

1- جريمة اعتراض المراسلات الإلكترونية:

تتمثل في كل فعل يرمي إلى اعتراض أو التقاط المراسلات الإلكترونية أثناء انتقالها دون وجه حق، وهو ما يشكل انتهاكاً لسرية الاتصالات التي كرسها القانون رقم 04-18، لاسيما من خلال حظر أي اعتراض خارج الحالات المرخص بها قانوناً.

2- جريمة الاطلاع غير المشروع على المراسلات الإلكترونية:

تتحقق هذه الجريمة بمجرد اطلاع الجاني على مضمون المراسلات الإلكترونية دون صفة أو ترخيص قانوني، سواء أثناء نقلها أو بعد تخزينها، ويعد ذلك مساساً بحرمة الحياة الخاصة وسرية الاتصالات.

3- جريمة إفشاء المراسلات:

تتحقق هذه الجريمة عند إفشاء أو نشر مضمون المراسلات دون وجه حق، خاصة إذا كان الشخص ملزماً قانوناً بالحفاظ على سريتها، كالمعاملين في قطاع الاتصالات، مما يشكل إخلالاً بالالتزامات المهنية والقانونية.¹

ثانياً: الجرائم الماسة بسلامة الاتصالات الإلكترونية

تهدف هذه الجرائم إلى حماية السير العادي للاتصالات الإلكترونية وضمان سلامتها من أي تدخل يؤدي إلى تعطيلها أو تحريفها.

¹ انظر: المادة 164 من القانون رقم 04-18، السالف ذكره.

1- جريمة تحويل المراسلات الصادرة عن طريق البريد الإلكتروني:

يتحقق هذا الفعل عند تغيير وجهة الرسائل أو إعادة توجيهها إلى غير المرسل إليه، ويجرم القانون هذه الأفعال بالمادة 165، مع تطبيق العقوبات نفسها على متعاملي البريد والاتصالات الإلكترونية.¹

2- جريمة عرقلة أو تشويش الاتصالات الإلكترونية:

تتحقق هذه الجريمة بكل فعل من شأنه تعطيل أو عرقلة أو تشويش الاتصالات الإلكترونية، وقد نص المشرع صراحة على تجريم الأفعال التي تمس سلامة تجهيزات الاتصالات، لاسيما تلك التي تؤدي إلى قطعها أو إتلافها، وذلك وفقا للمواد 179 و180 و181 من القانون رقم 18-04.

وتجسد هذه النصوص حماية جزائية متدرجة لسلامة الاتصالات الإلكترونية، إذ تعاقب المادة 179 على الأفعال المرتكبة عمدا والمتمثلة في قطع أو تلف الكابلات البحرية أو تجهيزات الاتصالات، بما يعرقل سير الخدمة، وهو ما يعكس جسامة الفعل وأهمية توافر القصد الجنائي.²

¹ المادة 165 من نفس القانون على: "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج أو بإحدى هاتين العقوبتين، كل متعامل للبريد يفتح أو يحول أو يخرب البريد أو يساعد في ارتكاب هذه الأفعال. تسري نفس العقوبات على كل متعامل للاتصالات الإلكترونية يحول، بأي طريق كانت، المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية، أو أمر أو ساعد في ارتكاب هذه الأفعال..."

² المادة 179 من القانون رقم 18-04 على معاقبة كل من يتسبب في قطع أو إتلاف منشآت الاتصالات بما يؤدي إلى تعطيل الخدمة، بقولها: "يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات، وبغرامة من 5.000.000 دج إلى 10.000.000 دج، كل من يقطع عمدا كابلا بحريا أو يسبب له تلفا قد يوقف أو يعطل الاتصالات الإلكترونية كليا أو جزئيا..."

في حين وسّعت المادة 180 نطاق التجريم ليشمل الأفعال الناتجة عن الإهمال أو الخطأ، تأكيداً لمسؤولية مرتكبها عن الإخلال بواجب الحيطة والحذر، مع تقرير عقوبة أخف تتناسب ودرجة الخطورة.¹

أما المادة 181، فقد كرّست التزاماً قانونياً بالإبلاغ عن الأضرار التي تمس تجهيزات الاتصالات، حيث يعد الامتناع عن ذلك سلوكاً مجزماً لما ينطوي عليه من تقاوم محتمل للأضرار وتهديد لاستمرارية الخدمة.²

وبذلك، يتضح أن المشرع الجزائري قد اعتمد معياراً قائماً على التدرج في المسؤولية الجزائية بحسب درجة الخطورة وطبيعة السلوك، موازناً بين متطلبات الردع وضرورة حماية البنية التحتية للاتصالات الإلكترونية.

الفرع الثالث: الجرائم الماسة بالتوقيع والتصديق الإلكترونيين في القانون رقم 04-15

يشكّل كل من التوقيع الإلكتروني والتصديق الإلكتروني ركيزتين أساسيتين لضمان أمن المعاملات الإلكترونية ومصداقيتها، إذ يحلان محل التوقيع التقليدي ويكفلان إضفاء الثقة على المبادلات التي تتم عبر البيئة الرقمية، ونظراً لما يكتسبانه من أهمية متزايدة، فقد أصبحت عرضة لمختلف صور الاعتداء الإجرامي، الأمر الذي استوجب تدخل المشرع الجزائري من خلال القانون رقم 04-15، قصد تجريم الأفعال التي تمسّ بسلامتهما ووظيفتهما.

¹ المادة 180 من نفس القانون، تنص على: "يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2)، وبغرامة من 500.000 دج إلى 1.000.000 دج، كل شخص يقطع، تهاونا أو خطأ، كابلاً بحرياً أو يسبب له تلفاً قد يوقف أو يعطل الاتصالات الإلكترونية كلياً أو جزئياً".

² المادة 181 من نفس القانون، على: "يعاقب بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات، وبغرامة من 5.000.000 دج إلى 10.000.000 دج، أو بإحدى هاتين العقوبتين، كل من لا يبلغ السلطات المختصة عن تسببه في قطع كابل بحري أو تلفه".

أولاً: جريمة إفشاء البيانات الشخصية أو إساءة استعمالها

تنص المادة 68 من القانون رقم 04-15 على معاقبة كل من يحوز أو يفشي أو يستعمل، دون وجه حق، بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير. ويستفاد من ذلك أنّ المشرع قد أحاط بيانات إنشاء التوقيع الإلكتروني بحماية جزائية مشددة، بالنظر إلى خطورتها البالغة في إثبات الهوية الإلكترونية، وما قد ينجم عن إساءة استعمالها من مساس جسيم بأمن المعاملات الإلكترونية.

ثانياً: جريمة الإخلال بسرية البيانات

ألزمت المادة 42 من القانون ذاته مؤدي خدمات التصديق الإلكتروني بواجب المحافظة على سرية البيانات والمعلومات المرتبطة بشهادات التصديق الإلكتروني التي يصدرها¹، ويترتب على الإخلال بهذا الالتزام قيام المسؤولية الجزائية وفقاً للمادة 70 من نفس القانون.² مما يدل على أنّ المشرع يسعى إلى توفير حماية فعالة للبيانات الشخصية، بالنظر إلى خصوصيتها، إذ أن جمع هذه البيانات أو تخزينها لا يفقدها سريتها، كما أنّ موافقة المعني على جمعها لا تعني السماح بتداولها أو الكشف عنها للغير خارج الحدود التي يقرّها القانون.

ثالثاً: جريمة جمع البيانات الشخصية للمعني دون موافقته

تنص المادة 43 من القانون رقم 04-15 على أنه لا يجوز لمؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني إلا بناء على موافقته الصريحة، وفي حالة مخالفة هذا الالتزام، تطبق عليه عقوبات جزائية.³

¹ انظر: المادة 42 من القانون رقم 04-15.

² تنص المادة 70 من القانون رقم 04-15 على أنه: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون".

³ تنص المادة 71 من القانون رقم 04-15 على أنه: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون".

يفهم من هذا الحكم أنّ المشرع اشترط الحصول على موافقة صريحة من الشخص المعني كشرط أساسي لجمع بياناته الشخصية، وهو ما يهدف إلى تعزيز حماية حياته الخاصة ومنع أي استعمال غير مشروع لهذه البيانات في إطار خدمات التصديق الإلكتروني.

المطلب الثالث: أحكام الشروع والاتفاق الجنائي في مجال الجريمة الإلكترونية

رغم الطابع التقني للجريمة الإلكترونية، فإنها تخضع في جانب كبير منها للقواعد العامة في قانون العقوبات، خاصة فيما يتعلق بالشروع والاتفاق الجنائي، مع مراعاة خصوصية الوسط الرقمي من حيث السلوك الإجرامي وطرق إثباته.

وقد وسّع المشرع الجزائري نطاق الحماية ليشمل الأفعال السابقة على اكتمال الجريمة، سواء تعلّق الأمر بالشروع (الفرع الأول) أو بالاتفاق الجنائي (الفرع الثاني)، بهدف الحد من الجرائم الإلكترونية والتدخل قبل تحقق نتائجها.

الفرع الأول: الشروع في الجريمة الإلكترونية

يقوم التجريم على عدم مساءلة الشخص عن مجرد النوايا ما لم تتجسد في سلوك مادي، غير أن المشرع يعاقب على الشروع متى بلغ الفعل درجة من الخطورة، ويقصد بالشروع قيام الجاني في تنفيذ الجريمة دون تحقق نتائجها لأسباب خارجة عن إرادته، فتكون الجريمة غير مكتملة.¹

وقد عزّف المشرع الجزائري الشروع في المادة 30 من قانون العقوبات تحت تسمية "المحاولة"²، وبينّ أنه يقوم على البدء في التنفيذ وعدم تمام الجريمة بسبب ظروف مستقلة عن إرادة الفاعل.

¹ صليحة بن عودة، الشروع في الجرائم المعلوماتية بين الوقاية والردع، مجلة دقاتر الحقوق والعلوم السياسية، مج 01، ع

02، 2021، معهد الحقوق والعلوم السياسية، بالمركز الجامعي مغنية، الجزائر، ص 73.

² انظر: المادة 30 من ق. ع. ج.

ويقتصر الشروع - كأصل عام - على الجنايات، ويمتد إلى الجنح متى نص القانون على ذلك صراحة، في حين لا يتصور في المخالفات، ولا يتصور في المخالفات، وقد أكد المشرع الجزائري هذا الاتجاه من خلال المادة 31 من قانون العقوبات.¹

وبالنظر لخطورة الجرائم المعلوماتية، نصت المادة 394 مكرر 7 على معاقبة الشروع في الجنح المعلوماتية بنفس عقوبة الجريمة التامة²، وهو ما يعكس تشديد الحماية الجزائية في هذا المجال.

أولاً: الركن المادي للشروع في الجريمة الإلكترونية

يتحقق الركن المادي للشروع بالبدا في تنفيذ الفعل الإجرامي، أي الانتقال من مرحلة التفكير والتحضير إلى مرحلة التنفيذ³، أي أنه لا يعاقب على التفكير أو الأعمال التحضيرية، ما لم تشكل جرائم مستقلة⁴، ويميّز الفقه بين:

- **المعيار الموضوعي:** وذلك بربط البدء في التنفيذ بتحقيق جزء من الركن المادي، كإدخال فيروس إلى نظام معلوماتي بقصد إتلافه أو محاولة اختلاس بيانات.

- **المعيار الشخصي:** وذلك بالاعتداد بإرادة الجاني وخطورته الإجرامية.⁵

¹ انظر: المادة 31 من ق. ع. ج.

² انظر: المادة 394 مكرر 7 من ق. ع. ج.

³ معمر فراق، الشروع في الجريمة بين التشريع العقابي المعاصر والفقه الجنائي الإسلامي، مجلة الحقيقة، مج 17، ع 04، ديسمبر 2018، جامعة أحمد دراية - أدرار، الجزائر، ص 09.

⁴ سامح، القليوبي، جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2010، ص

⁵ عمر أبو الفتوح عبد العظيم الحامي، الحماية الجنائية للمعلومات المسجلة إلكترونياً (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2010، ص 112، 114.

ويظل الشروع جريمة ناقصة، يعتري النقص فيها الركن المادي، بينما يكتمل فيها القصد الجنائي لدى الجاني، إلا أنّ النتيجة الإجرامية لا تتحقق لأسباب خارجة عن إرادته¹، كما لا يعاقب على العدول الاختياري إذا تم قبل إتمام تنفيذ الجريمة.²

ثانياً: الركن المعنوي للشروع في الجريمة الإلكترونية

يقوم الركن المعنوي على القصد الجنائي، أي اتجاه إرادة الجاني إلى ارتكاب جريمة تامة، ويجب أن يكون هذا القصد معاصراً للبدء في التنفيذ، ولا يتصور الشروع في الجرائم غير العمدية لغياب القصد، كحالة الإلتلاف غير العمدي للبيانات نتيجة خطأ مهني، لانقضاء القصد الجنائي.³

ووفقاً للقواعد العامة لا يطبق الشروع في الجرائم الشكلية التي تتم بمجرد الفعل، مثل جريمة الدخول أو البقاء غير المشروع في نظام معلوماتي، إذ تتحقق هذه الجريمة بمجرد الفعل ذاته، غير أن المشرع الجزائري، وبالنظر لخطورة الجرائم المعلوماتية، ساوى بين عقوبة الشروع والجريمة التامة، بهدف تشديد الحماية الجنائية للأنظمة المعلوماتية والمعاملات الإلكترونية، بالنظر لما قد ينجم عن الاعتداء عليها من أضرار جسيمة، لاسيما ذات الطابع الاقتصادي.⁴

¹ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 118.

² صليحة بن عودة، مرجع سابق، ص 81.

³ عمر أبو الفتوح عبد العظيم الحمامي، مرجع سابق، ص 117.

⁴ صليحة بن عودة، مرجع سابق، ص 82.

الفرع الثاني: الاتفاق الجنائي في الجريمة الإلكترونية

يقصد بالاتفاق الجنائي تلاقي إرادتين أو أكثر على ارتكاب جريمة معينة ولو لم تنفذ¹، ويخضع الاتفاق الجنائي في التشريع الجزائري، كأصل عام، للقواعد العامة في قانون العقوبات، لاسيما أحكام المساهمة الجنائية وجريمة تكوين جمعية أشرار، مع وجود بعض الأحكام الخاصة في مجال الجرائم الإلكترونية.

وفيما يلي بيان أركان الاتفاق الجنائي في الجريمة الإلكترونية:

أولاً: الركن الشرعي

خلافًا للقواعد العامة في قانون العقوبات، لاسيما ما تعلق بجريمة تكوين جمعية أشرار المنصوص عليها في المادة 177 منه²، أقر المشرع الجزائري تنظيمًا خاصًا للاتفاق الجنائي في الجرائم الإلكترونية بموجب المادة 394 مكرر 5 من القسم السابع المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.³

وبالرجوع لنص المادة الأخيرة، نجد أن المشرع قد جَرَّم مجرد المشاركة في اتفاق أو مجموعة من شأنها ارتكاب إحدى الجرائم الإلكترونية، شريطة أن يكون هذا الاتفاق مجسداً بأفعال مادية.

ويعكس هذا التوجه موقفاً وسطاً، إذ لم يجرم النية المجردة احتراماً لمبدأ الشرعية، وفي المقابل لم ينتظر اكتمال الجريمة، بل تدخل في مرحلة سابقة عليها تحقيقاً للاعتبارات الوقائية والردعية.

وبذلك وسَّع المشرع نطاق الحماية ليشمل الأفعال التحضيرية ذات المظهر المادي، خاصة تلك المرتبطة بالأنشطة التقنية وشبكات القرصنة.⁴

¹ أسامة صلاح محمد، التكيف القانوني للاتفاق الجنائي في الجريمة، دراسة مقارنة بين التشريع الجنائي العراقي والسوداني، المجلة الأكاديمية للبحوث القانونية والسياسية، مج 05، ع 01، 2021، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي - الأغواط، الجزائر، ص 63.

² انظر: المادة 177 من ق.ع.ج.

³ تنص المادة 394 مكرر 5 من ق.ع.ج على أنه: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسداً بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

⁴ علي عبد القادر القهوجي، مرجع سابق، ص 126.

ثانيا: الركن المادي

يقوم الركن المادي في الاتفاق الجنائي أساسا على السلوك الإجرامي، دون اشتراط النتيجة، ويتمثل في وجود اتفاق بين عدة أشخاص على غرض إجرامي، مقرون بأفعال مادية تجسده، وهو ما يسهم في تجاوز صعوبة الإثبات في الجرائم الإلكترونية.

1- الاتفاق:

يقصد به اتحاد إرادتين أو أكثر على ارتكاب جريمة معينة بشكل نهائي، ولا يعتد به إذا شابه تردد أو عدم توافق بين أطرافه، بحيث لا تنصهر إراداتهم في اتجاه إجرامي واحد.¹ وقد أقر المشرع هذا المفهوم في المادة 176 من قانون العقوبات²، بينما اشترطت المادة 394 مكرر 5 اقترانه بمظهر مادي خارجي، يتجسد في أعمال تحضيرية، كافتناء برامج اختراق أو التنسيق التقني.

2- موضوع الاتفاق:

يشترط أن ينصب الاتفاق على ارتكاب أو إعداد جناية أو جنحة وفقا للمادة 179، دون أن يعتد به في المخالفات.

أما في مجال الجرائم الإلكترونية، فقد حددت المادة 394 مكرر 5 موضوعه في إحدى الجرائم الواردة في القسم السابع، بشرط تجسيده بأفعال مادية. ويجب التمييز بين هذه الأفعال التحضيرية وبين البدء في التنفيذ الذي يشكل شروعا، ومن أمثلتها الحصول على كلمات المرور، أو تبادل تقنيات الاختراق، أو شرح كيفية استعمال الفيروسات بقصد الإتلاف أو التعديل.

3- تعدد أطراف الاتفاق:

يتطلب الاتفاق الجنائي توافر إرادتين على الأقل دون حد أقصى، وفقا للمواد 176 و 177 و 394 مكرر 5 من قانون العقوبات، كما يشترط تمتع الأطراف بالأهلية الجزائية، وأن تنتفي موانع المسؤولية، كصغر السن أو الإكراه، دون اعتبار لطبيعة العلاقة بينهم.³

¹ راجع محمد فاضل، الجرائم الواقعة على أمن الدولة، مطبعة جامعة دمشق، 1963، ص 85.

² انظر: المادة 176 من ق.ع.ج.

³ عبد القادر بونيف، موقف القانون الجزائري من الاتفاق الجنائي في الجرائم السيبرانية، مجلة البحوث القانونية والاقتصادية، مج 08، ع 01، 2025، ص 866.

ثالثا: الركن المعنوي

يقوم الركن المعنوي على توافر القصد الجنائي العام، المتمثل في العلم والإرادة.

1- العلم:

يتحقق بإدراك الجاني أن موضوع الاتفاق ينصرف إلى ارتكاب جريمة أو الإعداد لها، وينتفي إذا جهل الطبيعة غير المشروعة للغرض المتفق عليه، كمن يعتقد أن النشاط محل الاتفاق مشروع، بينما هو في حقيقته موجه لارتكاب جرائم معلوماتية، مثل تداول برامج خبيثة على أنها برامج عادية، غير أن الجهل بالقانون لا يعد عذرا، كما يسأل الجاني إذا علم لاحقا بالغرض الإجرامي واستمر في الاتفاق.

2- الإرادة:

يجب أن تتجه إرادة الجاني إلى الانخراط الجدي في الاتفاق وتنفيذه، ولا يكفي مجرد العلم، وتنفي في حالة المشاركة الصورية أو لأغراض التبليغ، كما يجب توافرها لدى جميع الأطراف، وإلا انتفى قيام الاتفاق الجنائي.¹

¹ عبد القادر بونيف، مرجع سابق، ص 867.

المبحث الثاني

الجزاءات المقررة للأفعال المكونة للجريمة الإلكترونية

Sanctions Prescribed for Acts Constituting Cybercrime

كرّس التشريع الجزائري نظاما عقابيا متكاملا لمواجهة الجريمة الإلكترونية، من خلال قانون العقوبات والقوانين الخاصة، بما يعكس توجهها تشريعا صارما لتعزيز حماية الأنظمة المعلوماتية والمعطيات والاتصالات الإلكترونية، ويتميز هذا النظام بعدة خصائص، أبرزها التدرج في العقوبات بحسب جسامة الفعل ونتيجته، والتوسع في نطاق تطبيق العقاب على الشروع والاتفاق الجنائي، إضافة إلى العقوبات التكميلية وفرض المسؤولية الجزائية على الشخص المعنوي.

يهدف هذا المبحث إلى تقديم تحليل دقيق للجزاءات المقررة للأفعال المكونة للجريمة الإلكترونية في التشريع الجزائري، مع التركيز على العقوبات الأصلية والتكميلية، وبيان كيفية تطبيقها على الأشخاص الطبيعيين والمعنويين، بالإضافة إلى التدابير الجزائية المقررة للأفعال السابقة على التنفيذ.

وسيتناول المبحث على النحو التالي:

المطلب الأول: العقوبات الأصلية المقررة للجريمة الإلكترونية.

المطلب الثاني: العقوبات التكميلية المقررة للجريمة الإلكترونية.

المطلب الثالث: عقوبة الشروع والاتفاق الجنائي في الجريمة الإلكترونية.

المطلب الأول: العقوبات الأصلية المقررة للجريمة الإلكترونية

يقتضي تحديد الجزاءات الجنائية المقررة للجريمة الإلكترونية الوقوف على العقوبات الأصلية التي تشكل الأساس في السياسة العقابية، باعتبارها الأداة الرئيسية للردع والزجر، وتتنوع هذه العقوبات بحسب طبيعة الفاعل، بين شخص طبيعي وشخص معنوي، بما يعكس خصوصية المسؤولية الجزائية في المجال الرقمي.

وعليه، سيتم تناول هذا المطلب من خلال فرعين، يخص الأول للعقوبات المطبقة على الشخص الطبيعي (الفرع الأول)، بينما يعنى الثاني بالعقوبات المقررة للشخص المعنوي (الفرع الثاني).

الفرع الأول: العقوبة الأصلية المطبقة على الشخص الطبيعي في الجريمة الإلكترونية

سنتطرق في هذا الفرع إلى العقوبات الأصلية المقررة للشخص الطبيعي، حيث تتدرج تبعا لخطورة الأفعال المرتكبة وطبيعة الاعتداء الواقع على الأنظمة المعلوماتية أو المعطيات، وانسجاما مع ذلك، سيتم التمييز بين العقوبات المذكورة في قانون العقوبات (أولا)، والعقوبات المنصوص عليها في التشريعات الخاصة (ثانيا).

أولا: عقوبة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفق قانون العقوبات

استنادا إلى النصوص القانونية المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية، سنعرض فيما يلي العقوبات المقررة لهذه الجرائم بحسب طبيعة كل مخالفة.

1- عقوبة الجرائم الماسة بالأنظمة المعلوماتية:

أ- عقوبة جرائم الولوج غير المشروع إلى الأنظمة المعلوماتية:

تعاقب المادة 394 مكرر في فقرتها الأولى من قانون العقوبات، بعد تعديلها بموجب القانون 06-24، كل دخول أو بقاء غير مشروع داخل نظام معلوماتي عن طريق الغش، بعقوبة تجمع بين الحبس الذي يمتد من ستة أشهر إلى سنتين، وغرامة مالية تتراوح بين 60.000 و 200.000 دج، كما يشمل التجريم كذلك محاولة ارتكاب هذا الفعل.¹

يتضح من ذلك، أن المشرع يجرم مجرد المساس بسلامة النظام المعلوماتي ولو دون تحقق نتيجة مادية، وهو ما يعكس تبني سياسة وقائية تقوم على حماية النظام في حد ذاته، كما

¹ انظر: المادة 394 مكرر من ق.ع.ج.

أن الجمع بين الحبس والغرامة يعكس رغبة في تحقيق ردع مزدوج، شخصي ومالي، يتناسب مع الطبيعة التقنية لهذه الجرائم.

ب- عقوبة الجرائم الماسة بسير الأنظمة المعلوماتية:

شدّدت المادة 394 مكرر في فقرتيها الثانية والثالثة من نفس القانون العقوبة إذا ترتب عن الدخول أو البقاء غير المشروع حذف أو تعديل للمعطيات، حيث تضاعف العقوبة في هذه الحالة، أما إذا بلغ الفعل حدّ الإضرار بسير المنظومة وتعطيلها، فقد رفع المشرع العقوبة إلى الحبس من سنة إلى ثلاث سنوات، مع غرامة تتراوح بين 100.000 و 300.000 دج.¹ ويعكس هذا التدرج اعتماد المشرع معيار النتيجة في تقدير جسامة الفعل، إذ لم يكتف بتجريم السلوك في حد ذاته، بل ربط تشديد العقوبة بمدى الضرر الناتج عنه، ويجسد ذلك انتقالاً من حماية شكلية للنظام إلى حماية موضوعية تمتد إلى سلامة المعطيات ووظائف النظام، بما يعزز فعالية الردع الجنائي.

2- عقوبة الجرائم الماسة بالمعطيات المعلوماتية داخل النظام

أ- عقوبة جريمة التلاعب غير المشروع بالمعطيات المعلوماتية:

نصت المادة 394 مكرر 1 من نفس القانون، بعد تعديلها، على معاقبة كل تدخل احتيالي على المعطيات، سواء بإدخال بيانات غير صحيحة أو حذفها أو تعديلها، بعقوبة الحبس من سنة إلى ثلاث سنوات، وغرامة مالية من 500.000 إلى 2.000.000 دج.² يظهر من تشديد العقوبة مقارنة بجريمة الدخول غير المشروع أن المشرع يعتبر المعطيات جوهر الحماية الجنائية، باعتبارها تمثل القيمة الحقيقية للنظام المعلوماتي، ومن ثم فإن المساس بها يعد أكثر خطورة من مجرد الولوج غير المشروع.

ب- عقوبة جريمة التعامل غير المشروع في المعطيات ذات المصدر غير المشروع:

أقرت المادة 394 مكرر 2 من نفس القانون عقوبات مشددة لكل تعامل غير مشروع في المعطيات ذات المصدر غير القانوني، بما يشمل مختلف صور الاستغلال كالتجميع والنشر

¹ انظر: الفقرة 02 و 03 من المادة 394 مكرر من ق.ع.ج.

² انظر: المادة 394 مكرر 1 من ق.ع.ج.

والإتجار والحياسة والاستعمال، حيث حددت العقوبة بالحبس من سنة إلى خمس سنوات، وغرامة تتراوح بين 1.000.000 و 5.000.000 دج.¹

يتضح أن المشرع لم يقتصر على تجريم الفعل الأصلي، بل امتد إلى تجريم الأفعال اللاحقة المرتبطة به، وهو ما يعكس تبني مقاربة شمولية تهدف إلى تجفيف منابع الجريمة الإلكترونية ومنع تداول المعطيات غير المشروعة داخل الفضاء الرقمي.

ج- الظروف المشددة الخاصة:

أقرت المادة 394 مكرر 3 من نفس القانون مضاعفة العقوبات إذا استهدفت الجرائم الأنظمة المرتبطة بالدفاع الوطني أو المؤسسات العمومية.²

ويدل هذا التشديد على إدراك المشرع لخطورة الاعتداء على البنى التحتية الحيوية للدولة، حيث يرتقي الفعل في هذه الحالة من مجرد جريمة معلوماتية إلى تهديد للأمن الوطني.

ثانيا: العقوبات المقررة للجرائم الإلكترونية في التشريعات الخاصة

حدد المشرع الجزائري بمقتضى قوانين خاصة الجزاءات المطبقة على مختلف الانتهاكات المرتبطة بالمعطيات الشخصية، وتنظيم الاتصالات الإلكترونية، والتوقيع والتصديق الإلكترونيين، وسنستعرض هذه العقوبات وفق تقسيم يراعي طبيعة كل مجموعة من الجرائم.

1- العقوبات المقررة للجرائم الماسة بالمعطيات الشخصية في القانون 07-18

أ- عقوبة الإخلال بالشروط المسبقة للمعالجة:

تعاقب المادة 55 من القانون رقم 07-18 كل من يخالف قواعد مشروعية معالجة المعطيات الشخصية، لاسيما في حالة عدم الحصول على موافقة الشخص المعني أو تجاهل حقه في الاعتراض، بعقوبة الحبس من سنة إلى ثلاث سنوات، وغرامة من 100.000 إلى 300.000 دج³، وذلك استنادا إلى أحكام المادتين 7 و 36 اللتين تكرسان مبدأ الموافقة المسبقة وحق الاعتراض كضمانتين أساسيتين لحماية المعطيات الشخصية.

¹ انظر: المادة 394 مكرر 2 من ق.ع.ج.

² انظر: المادة 394 مكرر 3 من ق.ع.ج.

³ انظر: المادة 55 من القانون رقم 07-18.

كما تعاقب المادة 56 من نفس القانون كل من يقوم بمعالجة المعطيات الشخصية دون استيفاء إجراءات التصريح أو الحصول على الترخيص المسبق، بعقوبة الحبس من سنتين إلى خمس سنوات، وغرامة من 200.000 إلى 500.000 دج، في مخالفة لأحكام المادة 1.12¹. تشير هذه الأحكام إلى حرص المشرع على احترام الشروط القانونية المسبقة لعملية المعالجة، سواء ما تعلق بموافقة الشخص المعني أو إجراءات الترخيص، بما يعكس مبدأ الشفافية وحماية الحقوق الفردية.

ب- عقوبة الإخلال بإجراءات الحماية والتعاون مع السلطة الوطنية:

تعاقب المادة 65 من القانون رقم 18-07 المسؤول عن المعالجة في حالة إخلاله بواجب ضمان سلامة وسرية المعطيات الشخصية، وذلك بمخالفة الالتزامات المنصوص عليها في المادتين 38 و39، بغرامة تتراوح بين 200.000 و500.000 دج.²

كما تعاقب المادة 61 من نفس القانون كل سلوك من شأنه عرقلة عمل السلطة الوطنية لحماية المعطيات الشخصية، بعقوبة الحبس من ستة أشهر إلى سنتين، وغرامة من 60.000 إلى 200.000 دج.³

وفي نفس السياق، تقرر المادة 66 عقوبة الحبس من سنة إلى ثلاث سنوات، وغرامة من 100.000 إلى 300.000 دج، في حق مقدم الخدمات الذي يمتنع عن إعلام السلطة الوطنية أو الشخص المعني بأي انتهاك للمعطيات، بما يشمل الإلتاف أو الضياع أو الإفشاء أو الولوج غير المرخص إليه، كما هو محدد في المادة 4.43⁴.

يتضح من خلال هذه الأحكام أن المشرع الجزائري لم يقتصر على تنظيم شروط معالجة المعطيات الشخصية، بل وسّع نطاق الحماية ليشمل ضمان أمنها وفرض التعاون مع السلطة الوطنية المختصة.

¹ انظر: المادة 56 من القانون رقم 18-07.

² انظر: المادة 65 من القانون رقم 18-07.

³ انظر: المادة 61 من القانون رقم 18-07.

⁴ انظر: المادة 66 من القانون رقم 18-07.

ج- عقوبة الجمع غير المشروع للمعطيات الشخصية:

تعاقب المادة 59 من القانون رقم 07-18 كل من يقوم بجمع معطيات ذات طابع شخصي بوسائل تدليسية أو غير نزيهة أو بطرق غير مشروعة، بعقوبة الحبس من سنة إلى ثلاث سنوات وغرامة من 100.000 إلى 300.000 دج.¹

كما تعاقب المادة 68 من نفس القانون كل من يقوم، خارج الحالات المسموح بها قانوناً، بجمع أو تسجيل أو حفظ معطيات شخصية تتعلق بالوضعية الجزائية للأشخاص، كالمعلومات المرتبطة بالجرائم أو الإدانات أو التدابير الأمنية، وذلك بعقوبة الحبس من ستة أشهر إلى ثلاث سنوات، وغرامة من 60.000 إلى 300.000 دج.²

يتضح أن المشرع شدد حماية مرحلة جمع المعطيات، خاصة المعطيات الحساسة، مع تدرج العقوبة حسب خطورة الفعل.

د- عقوبة الاستغلال غير المشروع للمعطيات الشخصية:

تعاقب المادة 58 من القانون رقم 07-18 كل من ينجز أو يستعمل معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص لها، بالحبس من ستة أشهر إلى سنة وغرامة من 60.000 إلى 100.000 دج.³

كما تعاقب المادة 65 فقرة 2 كل من يحتفظ بهذه المعطيات خارج المدة القانونية أو المحددة في التصريح أو الترخيص، بغرامة تتراوح بين 200.000 و500.000 دج.⁴ في حين شددت المادة 60 العقوبة على السماح لغير المؤهلين بالولوج إلى المعطيات الشخصية، حيث قررت الحبس من سنتين إلى خمس سنوات وغرامة من 200.000 إلى 500.000 دج.⁵

¹ انظر: المادة 59 من القانون رقم 07-18.

² انظر: المادة 68 من القانون رقم 07-18.

³ انظر: المادة 58 من القانون رقم 07-18.

⁴ انظر: المادة 65 فقرة 2 من القانون رقم 07-18.

⁵ انظر: المادة 60 من القانون رقم 07-18.

يتضح من هذه الأحكام أن المشرع الجزائري وسّع الحماية لتشمل مرحلة استغلال المعطيات، من خلال ضبط غايات استعمالها، وتحديد مدة الاحتفاظ بها، وتقييد الولوج إليها، بما يعكس توجهها نحو ضمان الاستعمال المشروع والأمن للمعطيات الشخصية.

2- العقوبات المقررة للجرائم الماسة بتنظيم الاتصالات الإلكترونية في القانون 04-18

أ- العقوبات المقررة للجرائم الماسة بسرية الاتصالات الإلكترونية:

تعاقب المادة 164 من القانون رقم 04-18 كل من ينتهك سرية المراسلات الإلكترونية، سواء تعلق الأمر بالاطلاع غير المشروع على مضمونها أو إفشائه أو نشره أو استعماله دون ترخيص، وذلك بعقوبة الحبس من سنة إلى خمس سنوات وغرامة من 500.000 إلى 1.000.000 دج.¹

ويتضح من هذا الحكم أن المشرع أولى أهمية بالغة لحماية سرية الاتصالات، باعتبارها من مظاهر الحياة الخاصة، حيث جرم مختلف صور الاعتداء عليها، بما يعكس توجهها نحو تكريس الثقة في البيئة الرقمية.

ب- العقوبات المقررة للجرائم الماسة بسلامة الاتصالات الإلكترونية:

تعاقب المادة 165 من القانون رقم 04-18 الأفعال التي تمس سلامة المراسلات الإلكترونية، لاسيما تحويلها أو اعتراضها أو إتلافها من قبل متعاملي البريد أو الاتصالات الإلكترونية، بعقوبة الحبس من سنة إلى ثلاث سنوات وغرامة قد تصل إلى 5.000.000 دج، أو بإحدى هاتين العقوبتين.²

كما شددت المادة 179 من نفس القانون العقوبة في حالة المساس العمدي بالبنية التحتية للاتصالات، كقطع أو إتلاف الكابلات أو التجهيزات، حيث تصل العقوبة إلى الحبس من خمس إلى عشر سنوات وغرامة مرتفعة³، نظرا لخطورة الأثر المترتب عن تعطيل الخدمة.

¹ انظر: المادة 164 من القانون رقم 04-18.

² انظر: المادة 165 من القانون رقم 04-18.

³ انظر: المادة 179 من القانون رقم 04-18.

في المقابل، خففت المادة 180 العقوبة عندما يكون الفعل ناتجا عن الإهمال أو الخطأ، حيث قررت الحبس من ستة أشهر إلى سنتين، وغرامة من 500.000 دج إلى 1.000.000 دج¹، مما يعكس تمييز المشرع بين القصد العمدي والخطأ غير العمدي في تقدير المسؤولية. أما المادة 181 من القانون السالف ذكره، فقد جرّمت الامتناع عن الإبلاغ عن الأضرار التي تمس منشآت الاتصالات، مقررّة عقوبة الحبس من ثلاث (3) سنوات إلى خمس (5) سنوات، وغرامة من 5.000.000 دج إلى 10.000.000 دج، أو بإحدى هاتين العقوبتين²، بما يكرّس التزاما قانونيا يهدف إلى الحد من تفاقم الأضرار وضمان استمرارية الخدمة. ويتضح من خلال هذه الأحكام أن المشرع الجزائري اعتمد تدرجا في العقوبات بحسب جسامّة الفعل ونتيجته، مع التمييز بين السلوك العمدي وغير العمدي، بما يحقق التوازن بين حماية البنية التحتية للاتصالات وضمان استمرارية المرفق العام.

3- العقوبات المقررة للجرائم الماسة بالتوقيع والتصديق الإلكترونيين في القانون 04-15

أ- عقوبة إفشاء بيانات إنشاء التوقيع الإلكتروني أو إساءة استعمالها:

تعاقب المادة 68 من القانون رقم 04-15 كل من يحوز أو يفشي أو يستعمل، دون وجه حق، بيانات إنشاء توقيع إلكتروني موصوف خاص بالغير، بعقوبة الحبس من ثلاثة أشهر إلى ثلاث سنوات وغرامة من 1.000.000 إلى 5.000.000 دج، أو بإحدى هاتين العقوبتين³.

ويستفاد من هذا الحكم أن المشرع أحاط هذه البيانات بحماية جزائية مشددة، بالنظر إلى دورها الحاسم في إثبات الهوية الإلكترونية، وما قد يترتب عن إساءة استعمالها من تهديد لأمن المعاملات الرقمية.

ب- عقوبة الإخلال بسرية بيانات التصديق الإلكتروني:

تعاقب المادة 70 من نفس القانون مؤدي خدمات التصديق الإلكتروني في حالة إخلاله بواجب سرية البيانات، بعقوبة الحبس من ثلاثة أشهر إلى سنتين وغرامة من 200.000 إلى

¹ انظر: المادة 180 من القانون رقم 04-18.

² انظر: المادة 181 من القانون رقم 04-18.

³ انظر: المادة 68 من القانون رقم 04-15.

1.000.000 دج، أو بإحدى هاتين العقوبتين، وذلك في مخالفة الالتزامات القانونية المفروضة عليه.¹

ج- عقوبة جمع البيانات الشخصية دون موافقة المعني:

تعاقب المادة 71 من نفس القانون مؤدي خدمات التصديق الإلكتروني الذي يقوم بجمع البيانات الشخصية دون موافقة صاحبها، بعقوبة الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 200.000 إلى 1.000.000 دج، أو بإحدى هاتين العقوبتين²، مما يؤكد ضرورة احترام إرادة الشخص المعني كشرط لمشروعية المعالجة.

يتضح من خلال هذه الأحكام أن المشرع الجزائري اعتمد حماية جزائية متكاملة لبيانات التوقيع والتصديق الإلكترونيين، من خلال تجريم مختلف صور الاعتداء عليها، بما يعزز الثقة في المعاملات الإلكترونية.

الفرع الثاني: العقوبات الأصلية المطبقة على الشخص المعنوي في الجريمة الإلكترونية

أقرّ التشريع الجزائري، متأثراً بالتوجهات الحديثة في السياسة الجنائية الدولية، مبدأ مساءلة الشخص المعنوي عن الجرائم الإلكترونية، ويستند هذا المبدأ إلى أحكام المادة 12 من الاتفاقية الدولية لمكافحة الجريمة الإلكترونية³، التي تقضي بإمكانية مساءلة الشخص المعنوي جزائياً متى ارتكبت الجريمة باسمه أو لحسابه من قبل أحد أجهزته أو ممثليه، سواء بصفته فاعلاً أصلياً أو شريكاً أو متدخلاً، بصرف النظر عن كون الجريمة تامة أو في مرحلة الشروع. اعتمد المشرع الجزائري هذا التوجه صراحة من خلال المادة 18 مكرر من قانون العقوبات⁴، التي أرست نظاماً متكاملاً للعقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح، بما يشمل الجرائم الإلكترونية، حيث شددت المادة 394 مكرر 4 من هذا القانون وكذا المادة 75 من القانون 04-15 على أن الغرامة المطبقة على الشخص المعنوي

¹ انظر: المادة 70 من القانون رقم 04-15.

² انظر: المادة 71 من نفس القانون.

³ اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المعتمدة في 23 نوفمبر 2001، الأمم المتحدة، متاحة على موقع مكتب الأمم المتحدة المعني بالمخدرات والجريمة <https://www.unodc.org>، تمت زيارة الموقع بتاريخ 28 مارس 2026، بتوقيات: 15.38.

⁴ انظر: المادة 18 مكرر من ق.ع.ج.

الفصل الأول: الآليات الموضوعية في مكافحة الجريمة الإلكترونية

تضاعف خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي¹، بما يعكس رغبة المشرع في تحقيق الردع المالي، بالنظر لخطورة هذه الجرائم.

يلاحظ من خلال هذا النظام العقابي أن المشرع الجزائري اعتمد مزيجا من العقوبات المالية والتنظيمية لضمان الردع والوقاية معا، مع إدراك خطورة استغلال الكيانات القانونية في ارتكاب الجرائم الإلكترونية.

المطلب الثاني: العقوبات التكميلية المقررة للجريمة الإلكترونية

إلى جانب العقوبات الأصلية، نص التشريع الجزائري على مجموعة من العقوبات التكميلية التي يمكن توقيعها على الشخص الطبيعي والشخص المعنوي على حد سواء، وفق أحكام قانون العقوبات الجزائري والقوانين الخاصة بالجرائم الإلكترونية.

تهدف هذه العقوبات إلى منع استمرار الفعل الإجرامي، وضمان عدم استفادة الجاني من الوسائل المستخدمة في ارتكاب الجريمة، وحماية البيئة الرقمية والمجتمع من المخاطر المرتبطة بالجرائم الإلكترونية.

ولتوضيح هذه العقوبات وتنظيمها، يمكن تقسيمها إلى فرعين:

الفرع الأول: العقوبات التكميلية المشتركة

تتضمن العقوبات التكميلية التي يمكن توقيعها على الشخص الطبيعي والمعنوي ما يلي:

أولا: المصادرة

المصادرة هي إجراء قضائي يتم بمقتضاه نقل ملكية أشياء متصلة بالجريمة إلى الدولة، حيث تنزع من الجاني، سواء كان شخصا طبيعيا أو معنويا، كل الأشياء التي استعملت أو أعدت لاستعمالها في ارتكاب الجريمة أو التي نتجت عنها.²

¹ فارس خطابي، الحماية الجزائية للتوقيع الإلكتروني، أطروحة دكتوراه، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2021/2020، ص 179، 179.

² محمد عبد العزيز إبراهيم مدحت، قانون العقوبات القسم العام النظرية العامة للعقوبة والتدابير الاحترازية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2007، ص 142.

الفصل الأول: الآليات الموضوعية في مكافحة الجريمة الإلكترونية

وتتدرج المصادرة ضمن العقوبات التكميلية وفقا للمادة 09 من قانون العقوبات، فلا يحكم بها مستقلة عن العقوبة الأصلية، كما تستلزم صدور حكم بالإدانة، وألا تمس بحقوق الغير حسن النية.¹

وفي مجال الجرائم الإلكترونية، تمتد المصادرة لتشمل مختلف التجهيزات والوسائل التقنية المستعملة في ارتكاب الجريمة، كالأجهزة الحاسوبية، والبرمجيات، والخوادم، بهدف منع استمرار الفعل الإجرامي، وتعزيز الردع.

ويستند ذلك إلى أحكام المادة 394 مكرر 6 من قانون العقوبات، التي تجيز مصادرة الوسائل والأدوات المستخدمة في الجرائم الماسة بالأنظمة المعلوماتية.²

كما نصّت بعض القوانين الخاصة على إمكانية المصادرة كعقوبة تكميلية، من بينها المادتان 71 و72 من القانون 07-18 المتعلق بحماية المعطيات ذات الطابع الشخصي، والمادتان 165 و178 من القانون 05-18 المتعلق بالبريد والاتصالات الإلكترونية، فضلا عن المادة 72 من القانون 04-15 المتعلق بالتوقيع والتصديق الإلكتروني.

ثانيا: إغلاق المواقع الإلكترونية أو المحلات

يهدف تعليق أو إغلاق المواقع الإلكترونية أو المحلات المستخدمة في ارتكاب الجريمة، سواء بشكل دائم أو مؤقت³، إلى قطع مصدر استغلال الوسائل المرتبطة بالفعل الإجرامي، ومنع تكرار الأفعال الإجرامية.

ويقصد بالمواقع تلك التي تقدم خدمات تسمح بالدخول غير المشروع إلى الأنظمة أو التلاعب بالمعطيات، أو تعليم تصميم معطيات غير مشروعة ونشرها أو الاتجار بها، أما المحل أو مكان الاستغلال فيضم الأجهزة المستعملة في ارتكاب الجريمة.⁴

ومثال على ذلك، إغلاق مقهى إلكتروني أو موقع على الإنترنت استخدم في تنفيذ جرائم المعلوماتية، وفق نص المادة 394 مكرر 6 من قانون العقوبات.

¹ شهرزاد بوعزيز، مستجدات عقوبة المصادرة في قانون العقوبات الجزائري، مجلة الدراسات والبحوث القانونية، مج 10، ع 02، جوان 2025، جامعة المسيلة، الجزائر، ص 339.

² انظر: المادة 394 مكرر 6 من ق.ع.ج.

³ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة التاسعة، دار هومه لطباعة والنشر والتوزيع، الجزائر، 2008، ص 448.

⁴ غنية باطلي، الجريمة الإلكترونية دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، 2015، ص 217.

ثالثا: المنع من ممارسة نشاط مهني أو اجتماعي

ويقصد بذلك حظر الشخص الطبيعي أو المعنوي من ممارسة نشاط مهني أو اجتماعي معين، إما مؤقتا أو دائما، حسب جسامة الجريمة.¹

رابعا: نشر أو تعليق حكم الإدانة

يقصد به إعلان الحكم الصادر بالإدانة في مكان عام أو عبر وسيلة إعلامية إلكترونية، لتحقيق رادع إعلامي، وتعزيز الشفافية والثقة في النظام القضائي، وإظهار خطورة السلوك الإجرامي، ويجوز تطبيقه على الشخص الطبيعي أو المعنوي، ويعكس إرادة المشرع في الجمع بين العقوبة الجزائية والأثر الاجتماعي المعنوي.²

الفرع الثاني: العقوبات التكميلية الخاصة بالشخص المعنوي

بالإضافة إلى العقوبات التكميلية المشتركة، يجوز للقاضي توقيع تدابير خاصة بالشخص المعنوي، من أبرزها:

أولا: حل المؤسسة أو غلقها

يشمل إنهاء وجود الشخص المعنوي القانوني أو إغلاقه مؤقتا أو دائما، حسب جسامة الجريمة، وتعتبر هذه العقوبة أشد العقوبات التكميلية للشخص المعنوي، إذ تمس وجوده القانوني وتمنع إمكانية تكرار الأفعال الإجرامية³، مثل حل شركة استخدمت نشاطها في ارتكاب جرائم معلوماتية أو في تصريف بيانات شخصية بشكل غير مشروع.

ثانيا: الوضع تحت الحراسة القضائية

يتمثل في إخضاع نشاط الشخص المعنوي لمراقبة قضائية محددة المدة⁴، تقتصر على النشاط الذي ارتكبت الجريمة بمناسبته، بهدف منع استغلاله مستقبلا في ارتكاب أفعال مماثلة.

¹ عبد الحكم سيد سالمان، الجرائم المعلوماتية وآثارها في ضوء قانون مكافحة جرائم تقنية المعلومات، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2023، ص 243.

² وردية فتحي، عن خصوصية الجزاء في الجرائم المالية، المجلة النقدية للقانون والعلوم السياسية، مج 10، ع 01، 2015، كلية الحقوق والعلوم السياسية، جامعة مولود معمري - تيزي وزو، الجزائر، ص 27.

³ غنية باطلي، مرجع سابق، ص 221.

⁴ فتحي محددة، إدريس قرفي، إجراءات المتابعة القضائية للشخص المعنوي المسؤول جزائيا بين التشريعين الفرنسي والجزائري، مجلة العلوم القانونية والسياسية، ع 04، جانفي 2012، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، ص 152.

ويظهر من هذه التدابير التكميلية توجه المشرع الجزائري نحو التوازن بين الردع والوقاية، إذ تتجاوز العقوبة الجانب المالي أو الأساسي لتشمل تدابير تنظيمية ووقائية تمنع استمرار الجريمة أو إعادة ارتكابها، سواء من قبل الشخص الطبيعي أو المعنوي.

المطلب الثالث: عقوبة الشروع والاتفاق الجنائي في الجريمة الإلكترونية

يتناول هذا المطلب العقوبات المقررة لكل من الشروع في الجرائم الإلكترونية (الفرع الأول)، والاتفاق الجنائي المتعلق بها (الفرع الثاني).

الفرع الأول: عقوبة الشروع في الجريمة الإلكترونية

أقر المشرع الجزائري تجريم الشروع في الجرائم الإلكترونية صراحة بموجب المادة 394 مكرر 7 من قانون العقوبات، حيث طبق على الشروع نفس عقوبة الجريمة التامة.¹ هذا التجريم الاستثنائي يعكس وعي المشرع بخطورة الجرائم المعلوماتية وأضرارها المحتملة حتى في مراحلها الأولى، كما يبرز الطابع الصارم للسياسة الجنائية الجزائرية التي توسع نطاق العقاب وتعزز الردع، لا سيما في ظل سرعة تنفيذ هذه الجرائم وصعوبة تدارك آثارها.

الفرع الثاني: عقوبة الاتفاق الجنائي في الجريمة الإلكترونية

جرّم المشرع الجزائري على تجريم الاتفاق الجنائي في مجال الجرائم الإلكترونية بموجب المادة 394 مكرر 25²، تماشيا مع المعايير الدولية مثل المادة 11 من اتفاقية مكافحة الجريمة الإلكترونية، ويعاقب القانون على الاتفاق بنفس عقوبة الجريمة المرتبطة به، نظرا لما يمثله من خطر كونه يمهّد لارتكاب جرائم قد تضرر بالأنظمة المعلوماتية.

وفي حالة تعدد الجرائم محل الاتفاق، تطبق عقوبة الجريمة الأشد، لضمان التناسب بين جسامة الفعل وخطورته الإجرامية.³

¹ خاليدة بن بعلاش، علي عثمان، الأحكام الموضوعية والإجرائية لمكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة أبحاث قانونية وسياسية، مج 06، ع 02، ديسمبر 2021، جامعة محمد الصديق بن يحيى، جبل، الجزائر، ص 704.

² انظر: المادة 394 مكرر 5 من ق.ع.ج.

³ أمال حابت، الجريمة المعلوماتية في التشريع الجزائري بين قانوني 04-15 و 09-04، مجلة هيروودوت للعلوم الإنسانية والاجتماعية، مج 07، ع 25، 2023، مؤسسة هيروودوت للبحث العلمي والتكوين، الجزائر، ص 59.

الفصل الثاني:

الآليات الإجرائية والمؤسسية لمكافحة الجريمة الإلكترونية

Procedural and Institutional Mechanisms for Combating Cybercrime

تشكل الجريمة الإلكترونية تحدياً حقيقياً أمام مختلف التشريعات الوطنية، بما فيها التشريع الجزائي، ويرجع ذلك إلى الطبيعة الخاصة لهذا النوع من الجرائم، المرتبطة بالبيئة الرقمية التي تتميز بسرعة التنفيذ، وسهولة ارتكاب الفعل الإجرامي، وصعوبة اكتشافه وإثباته، لاسيما وأن الجريمة الإلكترونية غالباً ما تتخذ طابعاً خفياً ومستترا يميزها عن الجرائم التقليدية.

كما تتفاقم صعوبة مواجهتها بالنظر إلى الخبرة التقنية التي يمتلكها الجاني، والتي تمكنه من محو الآثار الرقمية وطمس الأدلة الإلكترونية في وقت وجيز¹، حتى وصفت بعض الأدلة الإلكترونية بأنها مجرد "نبضات إلكترونية" قد تختفي في أقل من ثانية، لارتباطها ببيئة افتراضية لا تترك أثاراً مادية ملموسة بالمعنى التقليدي.²

وأمام هذه الخصوصية، لم يعد التصدي للجريمة الإلكترونية يقتصر على وضع نصوص تجزيمية فحسب، بل استلزم اعتماد آليات إجرائية خاصة تتلاءم مع طبيعتها التقنية، تشمل إجراءات التحقيق التقليدية والمستحدثة (المبحث الأول)، إلى جانب إسناد مهمة مكافحتها إلى هيئات ومؤسسات متخصصة تتولى الوقاية منها ومتابعتها والتحقيق فيها (المبحث الثاني).

¹ عبد الحكم سيد سالم، الجرائم المعلوماتية وآثارها في ضوء قانون مكافحة جرائم تقنية المعلومات، مركز الدراسات العربية، مصر، الطبعة الأولى، 2023، ص45.

² سيد علي السيد محمد، الجرائم الإلكترونية، دار التعليم الجامعي، الاسكندرية، مصر، 2024، ص99.

المبحث الأول

الآليات الإجرائية لمكافحة الجريمة الإلكترونية

Procedural Mechanisms for Combating Cybercrime

فرضت الجريمة الإلكترونية على التشريعات الحديثة اعتماد آليات إجرائية خاصة لمكافحتها، وذلك لمواكبة المستجدات والتحديات التي أفرزها التطور التكنولوجي، لاسيما ما تتميز به هذه الجرائم من سرعة في التنفيذ، وتعقيد في الأساليب، وطابع عابر للحدود، الأمر الذي يصعب من عملية اكتشافها وإثباتها.

وأمام هذه التحولات، لم يعد الاعتماد على القواعد الإجرائية التقليدية كافيا لمواجهة هذا النوع من الجرائم، بل أصبح من الضروري تبني آليات إجرائية مستحدثة تتلاءم مع طبيعتها التقنية وخصوصية أدلتها الرقمية.

غير أن دراسة هذه الآليات تقتضي بداية التطرق إلى الإجراءات التقليدية المعتمدة في مجال التحقيق الجنائي، قبل الانتقال إلى الآليات المستحدثة التي أفرزتها البيئة الرقمية. وعليه، سيتم التطرق في هذا المبحث إلى إجراءات التحقيق المعتمدة في مكافحة الجريمة الإلكترونية (المطلب الأول)، ثم دراسة الدليل الرقمي بوصفه من أبرز وسائل الإثبات المستحدثة في المجال الجنائي (المطلب الثاني).

المطلب الأول: آليات التحقيق الجنائي في مكافحة الجريمة الإلكترونية

يعتبر التحقيق الجنائي مرحلة محورية في منظومة العدالة الجزائية، إذ يهدف إلى كشف الحقيقة بشأن الجريمة المرتكبة من خلال جمع الأدلة والقرائن وتحليلها في إطار من الشرعية القانونية واحترام حقوق الأفراد وحرياتهم.

ويباشر هذا التحقيق من قبل جهات مختصة، على رأسها الضبطية القضائية وتحت إشراف السلطة القضائية، وفق إجراءات دقيقة تضمن التوازن بين فعالية البحث عن الحقيقة وصون الضمانات الأساسية للمتهم.

وسنتناول في هذا المطلب آليات التحقيق الجنائي التقليدية في مكافحة الجريمة الإلكترونية (الفرع الأول)، ثم آليات التحقيق المستحدثة لمواجهتها (الفرع الثاني).

الفرع الأول: آليات التحقيق الجنائي التقليدية في مكافحة الجريمة الإلكترونية

تشكل آليات التحقيق الجنائي التقليدية الأساس الذي تقوم عليه إجراءات البحث والتحري في المادة الجزائية، إذ اعتمدت عليها أجهزة العدالة منذ نشأتها في كشف الجرائم وتحديد مرتكبيها، وتتمثل هذه الآليات في مجموعة من الوسائل القانونية الكلاسيكية، كالمعاينة والتفتيش، التي تهدف إلى جمع الأدلة المادية والمعنوية في إطار احترام مبدأ الشرعية وضمان حقوق الأفراد.

وعليه، سيتم التطرق في هذا الفرع إلى المعاينة (أولاً)، ثم التفتيش (ثانياً)، باعتبارهما من أبرز آليات التحقيق التقليدية المعتمدة في المجال الجزائي.

أولاً: المعاينة في الجريمة الإلكترونية

تعتبر المعاينة من أهم إجراءات التحقيق الجنائي التقليدية، إذ تهدف إلى الوقوف على حالة الأشخاص أو الأماكن أو الأشياء المرتبطة بالجريمة، بغرض إثبات حالتها وضبط كل ما من شأنه المساهمة في كشف الحقيقة.

وقد عرّفها الفقه بأنها: "رؤية مكان أو شخص أو شيء بالعين لإثبات حالته وضبط ما يلزم لإظهار الحقيقة"¹، كما تعرف أيضاً بأنها إثبات حالة الأماكن أو الأشياء أو الأشخاص وكل ما يفيد في الكشف عن ملابسات الجريمة.²

ورغم الأهمية البالغة التي تكتسبها المعاينة في الجرائم التقليدية، بالنظر إلى ما تخلفه هذه الأخيرة من آثار مادية وأدلة جنائية ملموسة تسهل على الضبطية القضائية وجهات التحقيق عملية جمع الأدلة وضبطها، فإن أهميتها تتضاءل نسبياً في مجال الجريمة الإلكترونية، بسبب الطبيعة الخاصة لهذا النوع من الجرائم.³

وتبرز صعوبة المعاينة في الجرائم الإلكترونية لعدة اعتبارات، يتمثل أولها في أن هذه الجرائم غالباً لا تخلف آثاراً مادية ظاهرة يمكن الاستناد إليها في الإثبات، باعتبارها تقع داخل

¹ محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الاسكندرية، الطبعة الأولى، 2014، ص716.

² نهلا عبد القادر المومني، مرجع سابق، ص59.

³ عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، بهجات للطباعة والتجليد القاهرة، مصر، الطبعة الأولى، 2009، ص60.

بيئة رقمية افتراضية، أما الاعتبار الثاني فيتعلق بإمكانية وصول عدة أشخاص إلى مسرح الجريمة الإلكترونية خلال الفترة الفاصلة بين ارتكاب الجريمة واكتشافها أو مباشرة التحقيق بشأنها، وهي مدة قد تطول في كثير من الأحيان، مما يتيح إمكانية التلاعب بالأدلة الرقمية أو محوها أو تعديلها، الأمر الذي يثير الشك حول سلامة الأدلة المستخلصة ومصادقيتها.¹ كما تزداد صعوبة المعاينة عند محاولة الوصول إلى الملفات المحذوفة أو المخفية أو المؤمنة بكلمات مرور، خاصة إذا كانت ضمن أنظمة معلوماتية معقدة ومتشابكة عبر الشبكات، وهو ما يستلزم الاستعانة بخبرات تقنية متخصصة لضمان الحفاظ على الدليل الرقمي وسلامته.²

أ- الضوابط والشروط الواجب مراعاتها عند معاينة مسرح الجريمة الإلكترونية

قبل صدور القانون رقم 14-25 المتضمن قانون الإجراءات الجزائية الجديد³، كان إجراء المعاينة، خاصة تلك المتعلقة بالوسائط المعلوماتية أو المرتبطة بتفتيش المساكن، يقوم أساسا على رضا الشخص المعني بالإجراء كشرط قانوني لمباشرتها في غير حالات التلبس أو وجود إذن قضائي مسبق، حيث نصت المادة 64 من قانون الإجراءات الجزائية الملغى على عدم جواز تفتيش المساكن ومعاينتها وضبط الأشياء المتعلقة بالجريمة إلا برضا صريح مكتوب من الشخص الذي ستتخذ لديه هذه الإجراءات، ويثبت ذلك في المحضر تحت طائلة البطلان⁴، كما كان هذا الرضا يشكل الأساس القانوني الذي يسمح لضابط الشرطة القضائية بإجراء المعاينة في الحالات التي لا يشملها نظام التفتيش الاستثنائي المرتبط ببعض الجرائم الخطيرة، وهو ما جعل مشروعية المعاينة، بما فيها المعاينة المعلوماتية، تقوم في جانب معتبر منها على إرادة الشخص محل الإجراء، خاصة عند غياب الإذن القضائي.

غير أنّ المشرع الجزائري، بموجب القانون رقم 14-25، أعاد تنظيم الإطار القانوني لإجراءات المعاينة تنظيمًا جديدًا، حيث أصبح الإذن القضائي المسبق هو الأساس القانوني

¹ خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، مصر، 2012، ص 60، 61.

² عبد الحكم سيد سالمان، مرجع سابق، ص 194.

³ القانون رقم 14-25، مؤرخ في 3 أوت 2025، يتضمن قانون الإجراءات الجزائية، ج ر، ع 54، صادرة في 13 أوت 2025.

⁴ انظر: المادة 64 من قانون الإجراءات الجزائية الملغى بموجب القانون رقم 14-25.

لإجراء المعاينة، إذ نصت المادة 75 على عدم جواز انتقال ضباط الشرطة القضائية إلى مساكن الأشخاص لإجراء المعاينة إلا بإذن مكتوب سابق صادر عن وكيل الجمهورية أو قاضي التحقيق، مع وجوب استظهار هذا الإذن قبل الدخول إلى المسكن والشروع في المعاينة تحت طائلة البطلان، كما أوجب المشرع أن يتضمن الإذن القضائي بيان وصف الجريمة محل البحث وعنوان الأماكن المراد تفتيشها وإجراء الحجز فيها، وأن تتم هذه العمليات تحت الإشراف المباشر للقاضي المختص، وهو ما يعكس انتقال المشرع من نظام قائم على رضا الشخص إلى نظام قائم على الرقابة القضائية المسبقة كضمانة أساسية لمشروعية إجراءات المعاينة.¹

إضافة إلى ذلك، أجاز القانون الجديد إجراء عمليات التفتيش والمعاينة والحجز في أي ساعة من ساعات الليل أو النهار في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال وغيرها من الجرائم الخطيرة، متى تم ذلك بناء على إذن مكتوب مسبق من وكيل الجمهورية المختص أو قاضي التحقيق.²

كما خول المشرع لوكيل الجمهورية أو قاضي التحقيق سلطة الإذن باتخاذ ترتيبات تقنية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بل والدخول إلى الأماكن الخاصة دون علم أو رضا الأشخاص المعنيين عند الضرورة، متى تعلق الأمر بجرائم تكنولوجيات الإعلام والاتصال، وهو ما يؤكد تكريس الإذن القضائي كبديل تشريعي عن شرط الرضا الذي كان مقررا في القانون الملغى في المادة 114.

وعليه، يتضح أن القانون رقم 14-25 أحدث تحولا جوهريا في الشروط القانونية لإجراء المعاينة المعلوماتية، إذ لم يعد رضا الشخص المعني يشكل أساسا قانونيا لإجرائها كما كان عليه الحال في ظل القانون الملغى، وإنما أصبحت هذه الإجراءات تقوم أساسا على الإذن القضائي المسبق باعتباره ضمانة قانونية لتحقيق التوازن بين حماية الحياة الخاصة ومتطلبات مكافحة الجريمة المعلوماتية.

وبمقتضى أحكام المادة 155 من قانون الإجراءات الجزائية، خول المشرع لقاضي التحقيق سلطة استكمال إجراء المعاينة التي سبق أن باشرتها الضبطية القضائية أو تأكيد نتائجها، حيث

¹ انظر: المادة 75 من القانون رقم 14-25.

² انظر: المادة 78 من نفس القانون.

الفصل الثاني: الآليات الإجرائية والمؤسسية لمكافحة الجريمة الإلكترونية

ينتقل إلى مكان وقوع الجريمة مرفوقاً بأمين الضبط، للقيام بجميع المعاينات التي يراها ضرورية لكشف الحقيقة، وذلك بعد إخطار وكيل الجمهورية، الذي يحق له مرافقة قاضي التحقيق أثناء هذا الإجراء¹، وتخضع هذه المعاينة لجملة من الإجراءات نذكر من بينها:

- تصوير الحاسب والأجهزة الطرفية المتصلة به ويحدد مكان التقاط الصورة² وتسجيل وقت التقاط الصورة.³
- ملاحظة وإثبات حالة التوصيلات والكابلات المرتبطة بمختلف مكونات النظام المعلوماتي.
- التأكد من خلو المحيط الخارجي من أي مؤثرات مغناطيسية، وذلك قبل نقل أو التعامل مع أي وسيط معلوماتي من مسرح الجريمة.
- التدقيق في كيفية إعداد النظام، وتحديد نقطة الاتصال، ومعرفة نوع الجهاز الذي تم من خلاله الولوج إلى النظام.
- إنجاز نسخ احتياطية من الأقراص الصلبة ومختلف الوسائط الإلكترونية، بما يضمن الحفاظ على المعطيات.
- تجميد العمل بالحاسوب أو بأي مكوّن من مكوناته، ويعد هذا الإجراء وسيلة لحماية الدليل من الإتلاف أو الحذف أو التشويه.⁴
- التحفظ عما قد يوجد بسلة المهملات، من الأوراق الملقاة أو الممزقة أو أوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة وفحصها ورفع البصمات منها.⁵

¹ محمد حزيط، الوجيز في قانون الإجراءات الجزائية الجزائري، دار بلقيس، 2026، الجزائر، ص323.

² وسيم حسام الدين الأحمد، مكافحة الجريمة الإلكترونية في التشريعات والاتفاقيات الدولية، دار غيداء للنشر والتوزيع، عمان، الأردن، ط1، 2020، ص116.

³ لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة الإلكترونية، دار الحامد للنشر والتوزيع، عمان، الأردن، ط 1، 2015، ص204.

⁴ وسيم حسام الدين الأحمد، مرجع سابق، ص116.

⁵ علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، الأردن، 2012، ص34.

وعلى الأجهزة القائمة بالتحقيق أن تقوم باتخاذ كافة التدابير الاحترازية سواء كانت شخصية ترد على المتهم أو عينية إذا انصبت على الأشياء التي استخدمها الجاني لارتكاب الجريمة.¹

ثانيا: التفتيش والضبط في مجال الجريمة الإلكترونية

يعتبر إجراء التفتيش من أهم الإجراءات التي تكون في التحقيق، وبواسطته يتغير مسار الحقيقة من المجهول إلى العلم بحقيقة الجاني، وثبوت الأدلة ضده، يضمن العدالة الحققة.

غير أن بعض رجال القانون يصفون التفتيش على أنه إجراء خطير، لأنه قد يمس بحقوق المواطنين التي كفلها الدستور، ويمس بخصوصيتهم مهما كانوا، أي سواء كان الجاني أم مجني عليه، أم لا علاقة له أساسا بالقضية.

وعليه، سنتناول مفهوم التفتيش في مجال الجريمة الإلكترونية، وشروطه وإجراءاته، ثم نتطرق إلى ضبط الأشياء والبيانات الناتجة عنه.

1- التفتيش:

لم يضع المشرع الجزائري تعريفا محددا للتفتيش، شأنه في ذلك شأن أغلب التشريعات المقارنة، تاركا مهمة تعريفه للفقهاء والقضاء، مكتفيا بتنظيم أحكامه وشروط ممارسته ضمن قانون الإجراءات الجزائية.

ويعتبر التفتيش من أهم إجراءات التحقيق الجنائي، لما له من دور في البحث عن الأدلة المرتبطة بالجريمة وضبطها بما يسهم في كشف الحقيقة وتحديد مرتكب الفعل الإجرامي.

وقد عرّفه الفقه بأنه: "إجراء يهدف إلى ضبط الأدلة وكل ما يتعلق بالجريمة من أجل نسبتها إلى فاعلها وتمكين صاحب الحق من حقوقه"²، كما عرّف أيضا بأنه: "إجراء للبحث عن شيء يتصل بجريمة وقعت ويفيد في الكشف عن الحقيقة وعن مرتكبها، باعتباره وسيلة من

¹ محمد معروف عبد الله، علم العقاب، المكتبة القانونية، بغداد، العراق، ط2، 2010، ص59.

² عبير بعقيقي، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والاماراتي، دراسة مقارنة، أطروحة دكتوراه في الحقوق، تخصص النظام الجزائي والسياسة الجزائية المعاصرة، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، 2018-2019، ص 224.

الفصل الثاني: الآليات الإجرائية والمؤسسية لمكافحة الجريمة الإلكترونية

وسائل الإثبات المادي تهدف إلى اكتشاف الأشياء المخفية أو الأشخاص الفارين من وجه العدالة".¹

ويتضح من خلال هذه التعريفات أن التفتيش يعد وسيلة قانونية للبحث عن الأدلة المادية المرتبطة بالجريمة، غير أن خطورته تكمن في إمكانية مساسه بحرمة الحياة الخاصة، الأمر الذي يقتضي ممارسته وفق الضوابط والشروط التي يحددها القانون.

وقد نظم المشرع الجزائري إجراء التفتيش في المواد من 155 إلى 160 من قانون الإجراءات الجزائية، حيث خول لقاضي التحقيق سلطة الانتقال إلى أماكن وقوع الجريمة أو إلى أي موقع يحتمل العثور فيه على أدلة تفيد في الكشف عن الحقيقة، سواء كانت هذه الأماكن داخلة ضمن نطاق اختصاصه الإقليمي أو خارجه، مع إمكانية الاستعانة بالإقامة القضائية عند الاقتضاء.

كما أجازت المادة 234 من القانون ذاته لقاضي التحقيق تفويض هذه المهمة إلى قاض آخر أو إلى أحد ضباط الشرطة القضائية المختصين إقليمياً.²

ونظراً لأهمية إجراء التفتيش وخطورته، حرص المشرع على تقييده بجملة من الشروط الشكلية والموضوعية، بهدف تحقيق التوازن بين مقتضيات البحث والتحري من جهة، وضمان حماية حرمة الحياة الخاصة وحرمة المساكن من جهة أخرى.

ولا يقتصر مفهوم السكن في هذا المجال على محل الإقامة الرئيسي فحسب، بل يمتد ليشمل ملحقاته كالساحات والأسطح، إضافة إلى أماكن الإقامة الثانوية ولو كانت غير مأهولة بصفة دائمة، كغرف الفنادق والمكاتب، فضلاً عن مقرات الشركات والمحلات ذات الطابع المهني أو الصناعي.³

¹ محمود إبراهيم غازي، مرجع سابق، ص 730.

² انظر: المادة 234 من قانون الإجراءات الجزائية السالف ذكره.

³ محمد حزيط، مرجع سابق، ص 326.

أ- شروط اجراء عملية التفتيش في الجريمة الإلكترونية:

تنقسم شروط التفتيش إلى شروط موضوعية وأخرى شكلية، وذلك على النحو الآتي:

1-1- الشروط الموضوعية:

تتمثل الشروط الموضوعية في ضرورة ثبوت وقوع الجريمة فعليا، مع توافر دلائل جديّة ترجّح نسبتها إلى شخص معيّن، كما يشترط وجود قرائن قوية تفيد احتمال العثور على أدلة أو أشياء ذات صلة بالجريمة، سواء في مسكن المشتبه فيه أو في أي مكان آخر يحتمل أن يحتوي على عناصر إثبات مفيدة تساهم في كشف الحقيقة.¹

ففي الجرائم المتعلقة بالإنترنت، يكون محل التفتيش غالبا الحاسوب بمكوّناته المادية والبرمجية، إضافة إلى شبكات الاتصال المرتبطة به، والتي قد تشمل الخوادم والمزوّدات الآلية وسائر الملحقات التقنية، وقد تكون هذه الوسائل في حيازة شخص معيّن أو موجودة في مكان له صلة بالمسكن.²

ولا يعدّ التفتيش مشروعاً إلا إذا كان إجراء ضرورياً ومتناسبا، بحيث لا تتوافر وسيلة أخرى أقلّ مساساً بالحقوق والحريات يمكن من خلالها الوصول إلى الأدلة المطلوبة، مع ضرورة مراعاة التناسب بين جسامة الجريمة وخطورة هذا الإجراء.

1-2- الشروط الشكلية:

لضمان مشروعية التفتيش، يتعيّن احترام جملة من الضوابط الشكلية التي نصّ عليها قانون الإجراءات الجزائية، ويتمثّل الأصل في أن يجري التفتيش بناء على أمر قضائي صادر عن قاضي التحقيق، يحدّد بدقة المكان المراد تفتيشه والغرض منه، دون جواز تجاوز حدوده. ومع ذلك، أجاز المشرع على سبيل الاستثناء إجراء التفتيش دون إذن مسبق في حالات محدّدة، كحالة التلبّس أو عند وجود خطر وشيك يتمثّل في ضياع الأدلة، وفي مثل هذه الحالات، يمكن لقاضي التحقيق أن يفوّض وكيل الجمهورية أو أحد ضباط الشرطة القضائية المختصين للقيام بهذا الإجراء، وفي جميع الأحوال، يلتزم القائم بالتفتيش بإخطار وكيل

¹ محمد حزيط، مرجع سابق، ص 327.

² حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009، ص 490.

الجمهورية فوراً، مع بيان الأسباب التي استدعت اللجوء إلى هذا الإجراء الاستثنائي، وإلا عدّ التفتيش باطلاً لعدم احترامه الضوابط القانونية.¹

ب - إجراءات التفتيش:

نصّ المشرع الجزائري، من خلال القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، على إجراءات التفتيش والحجز داخل المنظومة المعلوماتية²، كما أجاز في بعض القوانين الخاصة اللجوء إلى التفتيش الإلكتروني، مثل القانون رقم 02-24 المتعلق بالوقاية من التزوير واستعمال المزور ومكافحته.³

ونظراً لخصوصية الجريمة الإلكترونية، التي يكون محلها غالباً نظاماً معلوماتياً، فقد أصبح التفتيش ينصب على الحاسوب وما يرتبط به من مكونات مادية ومعنوية؛ حيث يشمل المكونات المادية (Hardware)، والمتمثلة في الأجهزة الملموسة، والمكونات غير المادية (Software) التي تتضمن أنظمة التشغيل والبرمجيات، إضافة إلى شبكات الاتصال بالإنترنت سواء كانت سلكية أو لاسلكية، محلية أو دولية.⁴

ويباشر قاضي التحقيق إجراء التفتيش بنفسه، بعد إخطار وكيل الجمهورية، كما يمكنه الانتقال إلى مكان الواقعة رفقة أمين الضبط، وفقاً للإجراءات القانونية المعمول بها.⁵

- تفتيش المكونات المادية:

يتمّ التفتيش في هذه الحالة في مكان تواجد الأجهزة، ويخضع لمجمل القواعد والإجراءات العامة للتفتيش، وذلك تقادياً لأي مساس بحرمة وخصوصية المساكن، وقد تكون الأجهزة محل الجريمة الإلكترونية مرتبطة بمكونات مادية خارجية، كما هو الحال في الشركات والبنوك، حيث تعتمد الجهة المختصة على التفتيش المادي للمكاتب والسجلات، إضافة إلى الاستعانة بكاميرات المراقبة.

¹ محمد حزيط، مرجع سابق، ص 327.

² نفس المرجع، ص 243.

³ القانون رقم 02-24، مؤرخ في 26 فيفري 2024، يتعلق بمكافحة التزوير واستعمال المزور، ج ر، ع 15، صادرة في 29 فيفري 2024.

⁴ عبير بعقيقي، مرجع سابق، ص 226.

⁵ محمد حزيط، مرجع سابق، ص 327.

ومن مظاهر هذا النوع من التفتيش أيضا ما يقوم به التقنيون من فحص لأجهزة الطابعات، من خلال تتبع البيانات وإصدار أوامر بالطباعة، بما يسمح بالحصول على الملفات التي تمت طباعتها سابقا، كما يشمل التفتيش فحص الهواتف النقالة والألواح الإلكترونية، للتحقق من إمكانية ربطها بالحواسيب واستخدامها في ارتكاب الجريمة أو الاحتفاظ بأدلة رقمية ذات صلة.¹

- تفتيش المكونات المعنوية (البرمجية):

يعتبر هذا النوع من التفتيش من أكثر الإجراءات تعقيدا، إذ يواجه المحققون صعوبات تقنية كبيرة، رغم التطور التكنولوجي الحاصل، ذلك أن هذا التطور لا يخدم أجهزة العدالة فحسب، بل يستفيد منه أيضا مرتكبو الجرائم المعلوماتية، وقد تناول المشرع الجزائري هذا النوع ضمن أحكام القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

ويشمل تفتيش المكونات المعنوية البحث داخل البرمجيات (Software)، من خلال فحص ملفات نظام التشغيل والبرامج والتطبيقات المخزنة، قصد استخراج الأدلة الرقمية ذات الصلة بالجريمة. كما قد يمتد التفتيش إلى الشبكات المعلوماتية، وهو ما يطرح صعوبات إضافية من حيث الوقت والجهد والتعقيد التقني، ولهذا يلجأ المحققون في كثير من الأحيان إلى التعاون مع الجهات المزودة بخدمات الإنترنت، بهدف تضيق نطاق البحث، من خلال تحديد المنطقة التي وقع فيها الاعتداء، وتتبع الأنشطة الرقمية للأشخاص المتواجدين فيها أو المرتبطين بالمجني عليه، بما يساعد في الوصول إلى الفاعل وجمع الأدلة اللازمة لإثبات الجريمة.²

وهناك ما يعرف بالتفتيش عن بعد، فيعدّ من أبرز المستجدات في مجال مكافحة الجريمة الإلكترونية، وقد نظمته المشرع الجزائري بموجب القانون رقم 04-09، لاسيما في نص المادة 05 منه.

¹ عبير بعقيقي، مرجع سابق، ص 226.

² عبير بعقيقي، مرجع سابق، ص 226، 227.

ويقصد به تمكين ضباط الشرطة القضائية والجهات المختصة بالتحقيق من الولوج إلى منظومة معلوماتية أو جزء منها، وكذا إلى البيانات المخزنة فيها أو في أنظمة تخزين مرتبطة بها، كما أجاز المشرع إمكانية توسيع نطاق التفتيش ليشمل منظومات معلوماتية أخرى مرتبطة بالمنظومة الأصلية، متى توفرت أسباب جدية تدعو للاعتقاد بوجود أدلة بها، وهو ما يعزز فعالية البحث والتحري في الجرائم الإلكترونية التي تتسم غالبا بالتشعب والترابط الشبكي، غير أن هذا الامتداد ليس مطلقا، بل قيده المشرع بضرورة الإعلام المسبق للسلطة القضائية المختصة، كضمانة أساسية لحماية الحقوق والحريات، كما نظم حالة امتداد التفتيش خارج الإقليم الوطني، حيث اشترط اللجوء إلى آليات التعاون الدولي، وفقا للاتفاقيات الثنائية أو متعددة الأطراف، وفي إطار مبدأ المعاملة بالمثل.¹

2- الضبط أو الحجز في الجريمة الإلكترونية:

من الطبيعي أنه عقب انتهاء جهة التحقيق أو الضبطية القضائية من عملية التفتيش، تأتي مرحلة ضبط وحجز الأشياء المتحصّل عليها.²

وفي مجال الجريمة الإلكترونية، لا يكون الحجز منصبا بالضرورة على كامل النظام المعلوماتي، بل ينصبّ أساسا على المعطيات المعلوماتية ذات الصلة بالجريمة، وقد نصّت المادة 06 من القانون رقم 04-09 على أنه إذا أسفرت عملية التفتيش داخل المنظومة المعلوماتية عن اكتشاف معطيات مخزنة تقيد في كشف الجريمة وتحديد مرتكبها، ولم يكن من الضروري حجز كامل المنظومة، تقوم السلطة المختصة بنسخ المعطيات محل البحث، إلى جانب المعطيات المرتبطة بها واللازمة لفهمها، على دعامة تخزين إلكترونية قابلة للحجز، مع وضعها في أحرار وفقا للإجراءات المنصوص عليها في قانون الإجراءات الجزائية.

وتلتزم الجهة القائمة بالتفتيش والحجز، في جميع الأحوال، بالحفاظ على سلامة المعطيات الموجودة داخل المنظومة محل العملية، ومع ذلك، يجوز لها استخدام الوسائل التقنية الضرورية لاستخراج هذه المعطيات أو إعادة تشكيلها، بما يجعلها قابلة للاستغلال في إطار التحقيق، شريطة ألا يؤدي ذلك إلى المساس بمحتواها أو مضمونها.³

¹ انظر: المادة 05 من القانون رقم 04-09 السالف ذكره.

² رشيدة بوكري، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2012، ص418.

³ انظر: المادة 06 من القانون رقم 04-09 السالف ذكره.

كما نصّت المواد 07 و08 و09 من القانون ذاته على جملة من التدابير التقنية المكّلة، حيث أجازت اللجوء إلى الوسائل المناسبة لمنع الوصول إلى المعطيات محل البحث أو إلى النسخ المتاحة للأشخاص المصرّح لهم باستخدامها.¹

وأجازت المادة 08 للسلطة المختصة أن تأمر باتخاذ التدابير الضرورية للحيلولة دون الاطلاع على المعطيات التي يشكّل محتواها جريمة، وذلك من خلال تكليف شخص مؤهل باستعمال الوسائل التقنية الملائمة لتحقيق هذا الغرض.²

أما المادة 09، فقد قيّدت استعمال المعلومات المتحصّل عليها من خلال إجراءات المراقبة، بحيث لا يجوز استخدامها إلا في الحدود التي تقتضيها ضرورات التحقيقات القضائية، ضماناً لعدم التعسّف وحماية للحقوق والحريات.³

- الاستعانة بالخبرة من أجل ضبط الأدلة الإلكترونية:

أجازت المادة 05 من القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الاستعانة بذوي الخبرة التقنية أثناء إجراءات البحث والتحري، وذلك بالنظر إلى الطابع التقني المعقد للأنظمة المعلوماتية وما تتسم به الأدلة الإلكترونية من خصوصية وصعوبة في الاكتشاف والتحليل، الأمر الذي يجعل اللجوء إلى الخبرة إجراء ضرورياً لضمان فعالية التفتيش الإلكتروني ودقته.⁴

وتعرّف الخبرة بأنها إجراء فني يلجأ إليه في المسائل التي تستوجب معارف أو تقنيات متخصصة، بهدف استخلاص عناصر أو أدلة يمكن الاستناد إليها في الإثبات، وتعدّ الخبرة كذلك وسيلة استشارية فنية يستعين بها المحقق أو القاضي لمساعدته على فهم المسائل ذات الطابع التقني التي تخرج عن نطاق معارفه القانونية العامة، لاسيما في الجرائم الإلكترونية التي تتطلب الإلمام بالجوانب التقنية للمنظومات المعلوماتية ووسائل تخزين البيانات ومعالجتها.

¹ انظر: المادة 07 من القانون رقم 04-09 السالف ذكره.

² انظر: المادة 09 من نفس القانون.

³ انظر: المادة 09 من نفس القانون.

⁴ انظر: المادة 09 من نفس القانون.

ومن ثم، يصبح اللجوء إلى الخبرة أمراً حتمياً كلما تعلّق الأمر بمسائل تقنية دقيقة لا تتوافر بشأنها الكفاءة اللازمة لدى أعضاء السلطة القضائية بحكم تكوينهم القانوني، بما يضمن سلامة إجراءات البحث والتحري وحسن تقدير الأدلة الرقمية وصولاً إلى كشف الحقيقة.¹

غير أنّ الخبرة، رغم أهميتها، لا تقتيد قاضي الموضوع، إذ تبقى خاضعة لسلطته التقديرية باعتبارها من وسائل الإثبات الجنائي التي يجوز له الأخذ بها أو استبعادها وفقاً لقناعته.

الفرع الثاني: آليات التحقيق الجنائي المستحدثة في مكافحة الجريمة الإلكترونية

نصّ المشرع الجزائري على أساليب التحري الخاصة بموجب المواد من 114 إلى 127 من القانون رقم 14-25 المتعلق بقانون الإجراءات الجزائية، حيث أجاز لقاضي التحقيق اللجوء إلى هذه الوسائل في بعض الجرائم الخطيرة، من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

وتتمثّل هذه الأساليب أساساً في اعتراض المراسلات، وتسجيل الأصوات، وعملية التسرّب، وهي وسائل استثنائية تبرّرها خطورة الجرائم محل المتابعة وصعوبة اكتشافها بالطرق التقليدية، لاسيما في الجرائم الإلكترونية التي تتسم بالتعقيد والتخفي.

وسنتناول في هذا الإطار آليات التحقيق الجنائي المستحدثة في مجال مكافحة الجريمة الإلكترونية، وذلك من خلال التطرّق إلى التسرّب الإلكتروني (أولاً)، ثم اعتراض المراسلات والمراقبة الإلكترونية (ثانياً)، وأخيراً الكشف عن الجريمة الإلكترونية بالاعتماد على المعطيات (ثالثاً)، لما لهذه الآليات من دور فعّال في مواجهة هذا النوع المتطور من الجرائم.

¹ عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، مداخلة علمية، ضمن فعاليات المؤتمر العربي الأول: (العلوم الأدلة الجنائية والطب الشرعي)، المنعقد أيام 12-14 نوفمبر 2007، المنظم بجامعة نايف العربية للعلوم الأمنية، الرياض، ص 24.

أولاً: التسرب الإلكتروني

قبل التطرق إلى مفهوم التسرب الإلكتروني، يقتضي الأمر بداية الوقوف على مفهوم التسرب في صورته التقليدية، باعتباره أحد أساليب التحري الخاصة التي أقرّها المشرع الجزائري لمواجهة الجرائم الخطيرة، فقد نظم المشرع إجراء التسرب ضمن المواد من 120 إلى 127 من قانون الإجراءات الجزائية، محددًا شروط اللجوء إليه وكيفيات تنفيذه.

أ- تعريف التسرب:

عرّفت المادة 121 فقرة 1 التسرب بأنه قيام ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة، من خلال الاندماج معهم أو مصاحبتهم أو التظاهر بمشاركتهم في نشاطاتهم الإجرامية، وذلك بهدف جمع الأدلة وكشف الحقيقة، كما أجاز المشرع، بموجب الفقرة 2 من نفس المادة، استعمال هوية مستعارة لضرورة إنجاح العملية، مع إعفاء القائم بالتسرب من المسؤولية الجزائية عن الأفعال التي قد يرتكبها في هذا الإطار، شريطة ألا تشكّل هذه الأفعال تحريضاً على ارتكاب الجرائم.¹

ومن جهة، حدّدت المادة 123 نطاق الأفعال التي يمكن مباشرتها أثناء عملية التسرب، كاختفاء أو حيازة أو نقل أو تسليم المواد أو الأموال أو المنتجات أو الوثائق المتحصّل عليها من الجرائم أو المستعملة في ارتكابها، إضافة إلى وضع الوسائل ذات الطابع القانوني أو المالي تحت تصرف مرتكبي هذه الجرائم، وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.²

كما أجاز المشرع، بموجب المادة 127، سماع ضابط الشرطة القضائية الذي قام بعملية التسرب كشاهد، دون الكشف عن هويته الحقيقية، ضماناً لسلامته وحماية لحسن سير التحقيق.³

¹ انظر: المادة 121 فقرة 1 وفقرة 2 من ق.إ.ج.ج.

² انظر: المادة 123 من نفس القانون.

³ انظر: المادة 127 من نفس القانون.

أما في مجال الجرائم الإلكترونية، يقصد بالتسرب قيام ضابط أو عون من الشرطة القضائية بالدخول إلى العالم الافتراضي بهدف كشف الجرائم، وذلك من خلال الولوج إلى مواقع أو منصات إلكترونية، وقد يشمل ذلك المشاركة في محادثات أو الانخراط في مجموعات اتصال يشتبه في تورط أفرادها في نشاط إجرامي، ويكون ذلك تحت غطاء افتراضي، حيث يظهر المتسرب بمظهر شخص عادي أو بصفات وأسماء مستعارة، بغرض كسب ثقة المشتبه فيهم وجمع المعلومات والأدلة، غير أنّ هذا الإجراء لا يعني القيام بأعمال اختراق غير مشروعة أو إحداث ثغرات تقنية، بل يتم في إطار قانوني منظم وتحت رقابة السلطة القضائية، مع احترام الضوابط التي تضمن عدم تجاوز حدود المشروعية، ويهدف التسرب أساسا إلى تتبع الأساليب الإجرامية، وفهم طرق ارتكاب الجرائم الإلكترونية، وجمع أدلة تساهم في تحديد هوية الفاعلين وتقديمهم للعدالة.¹

ب- شروط التسرب وإجراءاته:

لإجراء عملية التسرب، يشترط أن تكون الجريمة من بين الجرائم الخطيرة المنصوص عليها في قانون الإجراءات الجزائية، كما هو الحال بالنسبة للجرائم الإلكترونية أو تلك المتصلة بتكنولوجيا الإعلام والاتصال، ويتعين الحصول على إذن مسبق من قاضي التحقيق لمباشرة هذه العملية، التي تتم تحت رقابته، وذلك بعد إخطار وكيل الجمهورية، كما يجب أن يكون هذا الإذن مكتوبا ومسببا، تحت طائلة البطلان، وفقا لأحكام المادة 124 من قانون الإجراءات الجزائية، على أن يتضمن تحديد الجريمة محلّ التحري، وبيان هوية ضابط الشرطة القضائية المكلف بالتسرب، وكذا مدة العملية التي لا تتجاوز أربعة (4) أشهر قابلة للتجديد، وخلال تنفيذ العملية، يمنع على ضابط الشرطة القضائية الكشف عن هويته الحقيقية، وإلا تعرض للعقوبات المنصوص عليها قانونا، والتي قد تصل إلى الحبس من سنتين إلى خمس (5) سنوات، وغرامة مالية تتراوح بين 200.000 و500.000 دينار جزائري، وذلك وفقا للمادة 125 فقرة 2.

كما يجوز لقاضي التحقيق، الذي أذن بإجراء التسرب، أن يأمر بوقفه قبل انقضاء المدة المحددة له، وذلك طبقا للمادة 124 فقرة 5، إذا اقتضت مصلحة التحقيق ذلك، وتودع الرخصة

¹ الطاهر ياكّر، الجرائم الإلكترونية الأحكام الموضوعية والإجرائية، دراسة مقارنة، دار بلقيس، الجزائر، 2024، ص 102، 103.

في ملف الاجراءات بعد الانتهاء من عملية التسرب¹، وفي حالة ما إذا أدى كشف هوية ضابط الشرطة القضائية المتسرب إلى تعرض أحد الأشخاص المعنيين، أو أزواجهم أو أبنائهم أو أصولهم المباشرين لأعمال عنف أو ضرب وجرح، فإن العقوبة المقررة تتمثل في الحبس من خمس (5) إلى عشر (10) سنوات، وغرامة مالية تتراوح بين 500.000 دج و1.000.000 دج.

أما إذا ترتب عن هذا الكشف وفاة أحد هؤلاء الأشخاص، فإن العقوبة تشدد لتصل إلى الحبس من عشر (10) سنوات إلى عشرين (20) سنة، وغرامة من 1.000.000 دج إلى 2.000.000 دج، وذلك دون الإخلال، عند الاقتضاء، بتطبيق الأحكام الواردة في الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات.²

ثانيا: اعتراض المراسلات والمراقبة الإلكترونية

نصّ المشرع الجزائري على هذا الأسلوب الخاص ضمن المواد من 114 إلى 119 من قانون الإجراءات الجزائية، حيث أجاز لقاضي التحقيق اللجوء إلى اعتراض المراسلات، وتسجيل الأصوات، والتقاط الصور، وذلك في إطار التحقيق في الجرائم الخطيرة، على غرار عملية التسرب سالفه الذكر، وسنتناول مفهوم عملية اعتراض المراسلات والتقاط الصور وشروطها واجراءاتها.

1- مفهوم عملية اعتراض المراسلات والتقاط الصور:

يعرّف بعض الفقه اعتراض المراسلات بأنه: عملية مراقبة سرية للمراسلات السلوكية واللاسلكية في إطار أعمال البحث والتحري عن الجرائم، بقصد جمع الأدلة أو الحصول على معلومات تتعلق بالأشخاص المشتبه في ارتكابهم للجريمة أو المساهمة فيها.

وتتم هذه المراقبة عبر اعتراض المراسلات أو تسجيلها أو نسخها، باعتبارها بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض، أما تسجيل الأصوات فيتم من خلال إخضاع الهواتف للمراقبة وتسجيل المكالمات التي تجرى عبرها، كما قد يتم باستخدام أجهزة

¹ انظر: المادة 124 من ق.إ.ج.ج.

² انظر: المادة 125 من نفس القانون.

دقيقة كالميكروفونات الحساسة القادرة على التقاط الأصوات وتسجيلها، أو عبر النقاط الإشارات اللاسلكية أو الإذاعية¹، أما بما يتعلق بالنقاط الصور، فتعدّ عملية التقاط الصور الفوتوغرافية من بين التقنيات الحديثة التي استحدثها المشرع الجزائري في مجال البحث والتحري عن جرائم الفساد، وذلك من خلال اعتماد أساليب التصوير بمختلف أشكالها وأنواعها²، فيقصد بالالتقاط تصوير شخص أو عدة أشخاص داخل أماكن خاصة أو عامة، باستخدام وسائل تقنية مختلفة، سواء في المساكن أو المحلات أو الفضاءات العامة، ويميز الفقه بين اعتراض المكالمات الهاتفية ووضع الخط الهاتفي تحت المراقبة؛ إذ يتم الاعتراض عادة دون رضا الشخص المعني، في حين يتم وضع الخط تحت المراقبة بناء على طلبه أو بموافقته، وذلك تحت إشراف وتقدير الجهة القضائية المختصة، وبمساهمة مصالح البريد والمواصلات.³

2- شروط وإجراءات اعتراض المراسلات والتقاط الصور:

حدد المشرع الجزائري في المواد من 114 إلى 119 من قانون الإجراءات الجزائية، شروط وإجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، والتي يمكن تلخيصها فيما يلي:

يباشر إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من طرف ضابط الشرطة القضائية بناء على إذن مكتوب ومسبب، وتحت رقابة السلطة القضائية، ويجوز، في هذا الإطار، اعتراض المراسلات التي تتم عبر وسائل الاتصال السلكية واللاسلكية دون علم الأشخاص المعنيين، مع اتخاذ الترتيبات التقنية اللازمة لتسجيل الأصوات والتقاط الصور في إطار سري يضمن فعالية التحري.⁴

وقد حددت المادة 116 من قانون الإجراءات الجزائية شروط صحة هذا الإذن، إذ يجب أن يتضمن جميع البيانات التي تسمح بتحديد طبيعة الاتصالات محل المراقبة، وهوية

¹ زوليغة زوزو، مشروعية أساليب التحري الحديثة، مجلة الحقوق والعلوم السياسية، ع 8، جوان 2017، جامعة خنشلة، ص763.

² عبد الحميد سفيان، أساليب التحري الخاصة في قانون الإجراءات الجزائية الجزائري، مجلة صوت القانون، مج 09، ع 02 ماي 2023، كلية الحقوق والعلوم السياسية، جامعة لونيبي علي البليدة 2، ص212.

³ زوليغة زوزو، مرجع سابق، ص763.

⁴ محمد حزيط، مرجع سابق، ص351.

الأشخاص المعنيين إن أمكن، وتحديد الأماكن المقصودة، إضافة إلى بيان الجريمة التي تبرر اللجوء إلى هذا الإجراء.¹

كما قيد المشرع مدة هذا الإجراء بأربعة (4) أشهر قابلة للتجديد وفق مقتضيات التحقيق، مع ضرورة احترام نفس الشروط الشكلية والموضوعية عند كل تجديد، بما يضمن تحقيق التوازن بين متطلبات التحقيق وحماية حريات الأفراد وحقوقهم.

ويؤكد ذلك على أن هذه الإجراءات، بحكم طبيعتها، تمثل مساسا مباشرا بالحياة الخاصة، مما يفرض إخضاعها لضوابط قانونية صارمة، من بينها الإذن المسبق المسبب وتحديد المدة، وعليه، فإن احترام مبادئ الشرعية والتناسب في استعمال هذه الوسائل يساهم في الكشف عن الحقيقة، دون المساس غير المشروع بحقوق وحريات الأفراد.²

ثالثا: الكشف عن الجريمة الإلكترونية عن طريق المعطيات

تلعب المعطيات دورا محوريا في الكشف عن الجريمة المعلوماتية، إذ يعتمد عليها كوسيلة أساسية للوصول إلى الدليل الرقمي، ويتم الاستفادة منها إما من خلال إجراءات الحفظ والإفشاء العاجلين، وذلك لضمان عدم ضياعها أو تغييرها، أو عن طريق تجميعها في وقتها الفعلي، بما يسمح بتتبع النشاط الإجرامي أثناء وقوعه.

1- الحفظ والإفشاء العاجلان للمعطيات الإلكترونية:

يعدّ كل من الحفظ والإفشاء العاجلين للمعطيات الإلكترونية من بين الإجراءات المستحدثة التي أقرّها المشرع لمواكبة خصوصية الجريمة المعلوماتية، وذلك بهدف تأمين الدليل الرقمي وضمان عدم ضياعه أو العبث به.

وقد نصّ على هذين الإجرائين بموجب المادة 10 من القانون رقم 04-09³، ويسند تنفيذ هذا الإجراء أساسا إلى مقدّمي خدمات الإنترنت، حيث يلتزمون بحفظ المعطيات محل

¹ انظر: المادة 116 من ق.إ.ج.ج.

² محمد حزيط، مرجع سابق، ص 351.

³ انظر: المادة 10 من القانون 04-09 السالف ذكره.

الطلب عن طريق تخزينها أو أرشفتها، بما يضمن الحفاظ على حالتها الأصلية ومنع إتلافها أو تغيير محتواها.

ويتم ذلك وفق آليات تقنية ملائمة تحدّدتها الجهة المختص، مع مراعاة طبيعة المعطيات ومكان تنفيذ إجراء الحفظ، كما يشمل هذا الإجراء أنواعا متعددة من المعطيات الإلكترونية القابلة للحفظ¹، شريطة التقيد بجملة من الضوابط القانونية والتقنية التي تحكم هذا المجال، والتي سيتم التطرق إليها تباعا.

1-1- المعطيات محل التحفظ:

نصّت المادة 11 من القانون رقم 04-09 على تحديد فئة معطيات المرور التي يلتزم مقدمو خدمات الاتصالات بالاحتفاظ بها، بناء على طلب الجهات القضائية المختصة، وتشمل هذه المعطيات على وجه الخصوص:

- البيانات التي تسمح بتحديد هوية مستعملي الخدمات؛
 - البيانات المرتبطة بالتجهيزات المستعملة في عملية الاتصال، بما في ذلك الرقم التسلسلي للجهاز، نوعه، وكيفية تشغيله؛
 - البيانات التي تمكّن من تحديد هوية كل من المرسل والمستقبل، كأرقام الهواتف أو عناوينهم؛
 - المعطيات ذات الطابع التقني، إضافة إلى تاريخ ووقت الاتصال ومدته؛
 - المعلومات المتعلقة بالخدمات الإضافية المطلوبة أو المستعملة، وكذا الجهات المقدمة لها.²
- ويهدف هذا الالتزام إلى تمكين السلطات القضائية من تتبع الاتصالات والكشف عن الجرائم، مع ضرورة احترام الضوابط القانونية المتعلقة بحماية الحياة الخاصة والمعطيات الشخصية والمتمثلة في

¹ نوال مجدوب، الآليات الإجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، مج 06، ع 03، 2023، المركز الجامعي آفلو، الجزائر، ص204.

² انظر: المادة 11 من القانون رقم 04-09 السالف ذكره.

1-2- الضوابط القانونية لحفظ المعطيات:

حددت مدة حفظ المعطيات المذكورة في المادة 11 من القانون رقم 09-04 بسنة واحدة ابتداء من تاريخ تسجيلها، ودون الإخلال بالعقوبات الإدارية المقررة عند عدم احترام الالتزامات المنصوص عليها، تقوم المسؤولية الجزائية للأشخاص الطبيعيين أو المعنويين متى ترتب عن ذلك عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من ستة (6) أشهر إلى خمس (5) سنوات وبغرامة من 50.000 دج إلى 500.000 دج، في حين يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المنصوص عليها في قانون العقوبات، وتحدد كميّات تطبيق هذه الأحكام عند الاقتضاء عن طريق التنظيم.¹

2- تجميع معطيات المرور بوقتها الفعلي:

بالإضافة إلى الالتزامات المنصوص عليها في المادة 11 المتعلقة بالاحتفاظ بمعطيات المرور، أقرّ المشرع الجزائري في المادة 12 التزامات إضافية تقع على عاتق مقدمي خدمات الإنترنت، ترمي إلى تعزيز الرقابة على المحتوى الرقمي وضمان احترام النظام العام والآداب العامة.

وفي هذا الإطار، يتعين على مقدمي الخدمات، التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد علمهم، بشكل مباشر أو غير مباشر، بمخالفتها للقوانين، وذلك من خلال حذفها أو تخزينها أو منع الولوج إليها، كما يلتزمون، بوضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تتضمن معلومات مخالفة للنظام العام أو الآداب العامة، مع ضرورة إعلام المشتركين بوجود هذه المحتويات.²

وبذلك، يتضح أن المشرع قد وسّع من نطاق التزامات مقدمي خدمات الإنترنت، من مجرد حفظ المعطيات إلى التدخل في المحتوى، بما يحقق توازنا بين

¹ انظر: المادة 11 من القانون رقم 09-04 السالف ذكره.

² انظر: المادة 12 من نفس القانون.

متطلبات الأمن المعلوماتي وحماية النظام العام من جهة، وضمان استخدام منضبط لشبكة الإنترنت من جهة أخرى.

المطلب الثاني: الدليل الإلكتروني كآلية مستحدثة في إثبات الجريمة الإلكترونية

يعتبر الدليل الرقمي أو الإلكتروني من أحدث الوسائل الإجرائية المعتمدة في مجال التحقيق الجنائي، نظرا لما يواكب التطور التكنولوجي المتسارع.

وعليه، سيتم التطرق في هذا المطلب إلى مفهوم الدليل الإلكتروني (الفرع الأول)، ثم بيان حجّيته في الإثبات الجنائي للجريمة الإلكترونية (الفرع الثاني).

الفرع الأول: مفهوم الدليل الإلكتروني

سنتناول في هذا الفرع تعريف الدليل الرقمي (أولا)، وبيان أهم خصائصه، والجراءات المستحدثة لجمع الدليل الرقمي في التشريعات المقارنة، وأيضا أهم التقسيمات التي تناولها الفقه والتشريع لتقسيم الدليل الإلكتروني

أولا: تعريف الدليل الرقمي

لم يضع المشرع الجزائري تعريفا محددا لهذا النوع من الأدلة، تاركا هذه المهمة للفقه، إلا أن الدليل الإلكتروني أو الرقمي هو أحد وسائل الإثبات حسب نص المادة 349 من قانون الإجراءات الجزائية¹، وبصفة عامة، يقصد بالدليل كل ما من شأنه إثبات صحة أو عدم صحة واقعة محل التحقيق، إذ لا يعتد أي نظام قضائي بواقعة ما لم تكن ثابتة وصحيحة.²

وقد ذهب جانب من الفقه إلى تعريف الدليل الرقمي بأنه ذلك المكوّن المستخلص من أجهزة الحاسب الآلي، والذي يكون في شكل إشارات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها بواسطة برامج وتطبيقات وتقنيات خاصة، ثم تقديمها في صورة دليل قابل للاعتماد أمام القضاء.

¹ انظر: المادة 349 من ق.إ.ج.ج.

² أشرف علي قوقزة، محمد حداد، الأدلة الرقمية في إثبات الجرائم الإلكترونية في التشريع الأردني (دراسة مقارنة)، دار المناهج، الأردن، الطبعة الأولى، 2021، ص47.

في حين يرى اتجاه آخر أنه يتمثل في عملية تجميع البيانات المخزنة على الحاسب الآلي وترجمتها وفق إجراءات قانونية وتقنية، وذلك في أي مرحلة من مراحل التحقيق¹، ومن خلال هذه التعريفات، يتضح أن الدليل الرقمي يقتضي بالضرورة تدخل مختصين وتقنيين لاستخراجه وتحليله، نظرا لكونه يوجد في صورة غير مادية داخل أنظمة الحاسوب، الأمر الذي يستلزم تحويله إلى شكل قابل للفهم والاستعمال القضائي، بما يؤدي في النهاية إلى تكوين قناعة قاضي الموضوع وقيل أيضا أنه جسم الجريمة المعلوماتية.²

وعرّفت المنظمة الدولية لأدلة الحاسوب الدليل الرقمي بأنه المعلومات المخزنة أو المستقلة في شكل ثنائي، والتي يمكن الاعتماد عليها أمام القضاء.

وبناء على ذلك، يمكن تعريف الدليل الرقمي بأنه كل معلومة يتم تخزينها في أجهزة الحاسوب وملحقاتها، مثل الأقراص الصلبة والأقراص المرنة وغيرها من وسائل وتقنيات المعلومات كأجهزة الطباعة والفاكس، أو تلك المتداولة عبر شبكات الاتصال. ويتم جمع هذه المعلومات وتحليلها باستخدام برامج وتطبيقات وتقنيات خاصة، بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبها.³

ب- خصائص الدليل الرقمي:

يتميز الدليل الرقمي بمجموعة من الصفات التي تميزه عن غيره من الأدلة التقليدية أو الحديثة والمتمثلة في:

توصف الأدلة الجنائية التقليدية بإمكانية التخلص منها بسهولة نسبية، بخلاف الدليل الإلكتروني أو الرقمي الذي يصعب محوه نهائيا، إذ يظل غالبا مخزنا داخل النظام وقابلا للاسترجاع حتى بعد محاولة إتلافه أو إخفائه.

¹ أشرف علي قوقزة، محمد حداد، مرجع سابق، ص 47.

² لميز أمينة، الدليل الرقمي كآلية لإثبات الجرائم المعلوماتية، مجلة بحوث في القانون والتنمية، ع 3، جوان 2023، جامعة بومرداس، ص 12.

³ محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، مكتبة الوفاء القانونية، الاسكندرية، مصر، الطبعة الأولى، 2014، ص 675، 676.

فبفضل التطور التكنولوجي، أضحت هناك برامج وتقنيات متقدمة تمكّن من استعادة البيانات المحذوفة، كاسترجاع الصور أو الملفات من الحاسوب بعد حذفها، ومع ذلك، فإن هذا التطور ذاته أفرز إشكالية قانونية مهمة، تتمثل في سعي الجناة في الجرائم المعلوماتية إلى استعمال برامج وأدوات متخصصة لطمس الآثار الرقمية والتخلص من الأدلة، كبرامج المسح الآمن أو التشفير، وهو ما يطرح تحديات حقيقية أمام جهات التحقيق، ويستدعي تطوير وسائل تقنية وقانونية فعّالة لضمان الحفاظ على الدليل الرقمي وكشفه.¹

وعليه فإن لجوء الجاني في الجرائم المعلوماتية إلى استعمال برامج تمكّنه من التخلص من الدليل الرقمي، حتى عن بعد، يعد قرينة قوية يمكن للخبراء الاستناد إليها لإثبات محاولات طمس الأدلة، بما يدعم إدانة المتهم متى ثبت ذلك تقنيا، الأمر الذي يبرز ضرورة تدخل المشرع الجزائري لتعزيز النصوص القانونية وتشديد العقوبات المتعلقة بإتلاف أو إخفاء الأدلة الرقمية بواسطة الوسائل التقنية، نظرا لخطورة هذا السلوك على سير العدالة.²

كما يتميز الدليل الرقمي بطبيعته غير المادية، إذ يتخذ شكلا إلكترونيا غير ملموس، لا يدرك بالحواس العادية، وإنما يتطلب الاستعانة بأجهزة وتقنيات خاصة لاستخراجه وتحليله، ورغم ذلك، فإنه لا يقل أهمية عن الدليل المادي، بل قد يفوقه من حيث الدقة والقدرة على تتبع الأنشطة، نظرا لإمكانية رصد مختلف تحركات المستخدم وأنشطته عبر الأنظمة المعلوماتية.³

ويتخذ الدليل الرقمي عدة أشكال رئيسية، من بينها الصور الرقمية، والتسجيلات الصوتية أو المرئية، والنصوص المكتوبة، وغيرها من البيانات الإلكترونية التي يمكن توظيفها في الإثبات الجنائي.⁴

¹ محمود إبراهيم غازي، مرجع سابق، ص 676.

² حسين بن السعيد الغافري، مرجع سابق، ص 536.

³ عبد الناصر محمود فرغلي، محمد عبيد سيف سعيد المسماري، مرجع سابق، ص 14.

⁴ الطاهر ياكور، مرجع سابق، ص 133.

ج- الإجراءات المستحدثة لجمع الدليل الرقمي في التشريعات المقارنة:

تعد إجراءات التفتيش من أهم الوسائل المستحدثة لجمع الدليل الرقمي في التشريعات المقارنة، لما لها من دور فعال في تتبع الجناة والكشف عن هويتهم، إذ يتم من خلالها تعقب المشتبه فيه عبر النظام أو الموقع الإلكتروني الذي استخدم في ارتكاب الجريمة، إضافة إلى فحص وتحليل البيانات التي تم نقلها منه أو إليه أو المخزنة داخله، كما تسمح هذه الإجراءات باستخراج الأدلة الرقمية بطريقة قانونية وتقنية تضمن حجيتها أمام الجهات القضائية.

ومن أهم هذه الإجراءات المستحدثة في مجال جمع الدليل الرقمي ما يلي:

1- استخدام بروتوكول TCP/IP:

يعتبر بروتوكول الإنترنت (IP) من أهم البروتوكولات المعتمدة في بيئة الشبكات، حيث يساهم بشكل أساسي في جمع الأدلة الرقمية وتتبع مصدر الاتصالات، ويعرف عنوان بروتوكول الإنترنت بأنه عنوان رقمي فريد يمنح لكل جهاز متصل بشبكة معلوماتية تعتمد هذا البروتوكول، بما يسمح بتمييزه عن غيره من الأجهزة وتحديد موقعه داخل الشبكة، كما يتيح هذا العنوان للأجهزة الأخرى إمكانية التعرف عليه وإرسال حزم البيانات إليه عبر الشبكة.

وينقسم عنوان بروتوكول الإنترنت إلى نوعين رئيسيين: عنوان بروتوكول الإنترنت العام (Public IP)، الذي يستخدم للتواصل عبر شبكة الإنترنت، وعنوان بروتوكول الإنترنت الخاص (Private IP)، الذي يُستعمل داخل الشبكات المحلية.¹

يتولى عنوان بروتوكول الإنترنت العام (Public IP) مهمة تمكين الاتصال بشبكة الإنترنت، حيث يمنح من قبل مزود خدمة الإنترنت (ISP) للمستخدمين، سواء كانوا أشخاصا طبيعيين أو معنويين، وذلك ضمن نطاق عناوين تشرف على تنظيمها هيئات دولية مختصة، ويؤدي هذا العنوان دورا محوريا في البنية الرقمية، إذ يسمح بالتعرف على هوية الجهاز المتصل بالشبكة وتحديد موقعه التقريبي ضمنها، ومن الناحية التقنية، يمكن عنوان بروتوكول الإنترنت من تمييز الشبكة التي ينتمي إليها الجهاز، وكذلك تحديد موقعه داخل تلك الشبكة،

¹ واضح الحاج، التنظيم القانوني لعنوان بروتوكول الإنترنت، مجلة الدراسات القانونية المقارنة، مج 07، ع 01، 2021، جامعة حسيبة بن بوعلي، الشلف، الجزائر، ص 2188.

مما يجعله أداة فعالة في تتبع الاتصالات الإلكترونية وتحديد مصدرها، ويمكن توضيح ذلك بالقول إن الاسم يحدد موضوع البحث، بينما يبين العنوان مكان وجوده، ويوضح المسار الكيفية التي يتم بها الوصول إليه.

ينقسم عنوان بروتوكول الإنترنت إلى نوعين أساسيين: عناوين عامة (Public IP) وعناوين خاصة (Private IP)، كما تصنف العناوين العامة من حيث طبيعة تخصيصها إلى عناوين ثابتة (Static IP) وعناوين ديناميكية (Dynamic IP).

فالعنوان الثابت يخصص بصفة دائمة لجهاز معين، بما يضمن استقرار الاتصال وإمكانية الوصول إليه في أي وقت، وهو ما يجعله شائع الاستخدام لدى مزودي خدمات الاستضافة والبريد الإلكتروني، أما العنوان الديناميكي فيتميز بطابعه المتغير، إذ يمنح للمستخدم لفترة زمنية محددة ويتغير عند كل اتصال جديد بالشبكة، ويعد الأكثر استخداماً لدى الأفراد نظراً لمرونته وكفاءته في استغلال العناوين.¹

وفيما يتعلق بعناوين بروتوكول الإنترنت الخاصة أو المحلية (Private IP)، فهي العناوين التي يقوم الموجه (Router) بتخصيصها لتمكين الحواسيب وباقي الأجهزة من الاتصال فيما بينها داخل نطاق الشبكة المحلية، وتكون الأجهزة التي تستخدم هذا النوع من العناوين معروفة فقط داخل هذه الشبكة، دون أن يكون لها ظهور مباشر على شبكة الإنترنت، وغالباً ما يتم توزيع هذه العناوين عن طريق بروتوكول التهيئة الآلية للمضيفين (DHCP)، الذي يتولى إسناد عناوين IP بشكل تلقائي للأجهزة، بما يساهم في تنظيم عملية الاتصال وتسهيل تبادل البيانات داخل نفس الوسط الشبكي.

ويتميز هذا النوع من العناوين بكونه ذا نطاق داخلي محدود، إذ لا يمكن استخدامه لإرسال أو استقبال المعطيات عبر شبكة الإنترنت بشكل مباشر، وإنما يقتصر دوره على تأمين الاتصال داخل الشبكات المحلية، مما يمنحه طابعاً تقنياً ووظيفياً مهماً في إدارة الشبكات.²

¹ واضح الحاج، مرجع سابق، ص 2188.

² نفس المرجع، ص 2189.

2- استخدام معلومات البروكسي (proxy):

يقصد بالبروكسي (Proxy) نظام أو خادم وسيط يتولى الربط بين جهاز المستخدم (العميل) والخادم الهدف، حيث يقوم بإعادة توجيه الطلبات الصادرة من المستخدم إلى المواقع أو الخدمات على شبكة الإنترنت، ثم يعيد الاستجابات إليه، وتستعمل هذه التقنية لعدة أغراض، من بينها تحسين الأداء عبر التخزين المؤقت (Caching)، وتعزيز أمن الشبكات من خلال مراقبة حركة المرور، كما يمكن أن تستخدم لإخفاء الهوية الحقيقية للمستخدم أو موقعه الجغرافي، ولا يعد البروكسي في حد ذاته جدارا ناريا، غير أنه قد يوظف ضمن منظومة الحماية كوسيلة لتصفية الاتصالات والتحكم فيها.¹

ومن الناحية العملية، يحتفظ خادم البروكسي بسجلات (Logs) تتضمن معلومات عن الطلبات المارة عبره، مثل عناوين IP، وتوقيت الاتصال، والموارد المطلوبة، وهو ما يمنح هذه المعطيات قيمة كبيرة في مجال الإثبات الجنائي الرقمي.

وعليه، يتعين على الخبراء التقنيين، في إطار التحقيقات، فحص هذه السجلات المحفوظة بعناية، لما قد تتضمنه من بيانات تساعد في تتبع نشاط المستخدمين وتحديد مصدر الاتصالات، شريطة احترام الضوابط القانونية المتعلقة بجمع الأدلة الرقمية وحمايتها.²

3- استخدام معلومات الكوكيز (ملفات الارتباط)

تسهم ملفات تعريف الارتباط (Cookies)، وهي ملفات نصية صغيرة تخزن على جهاز المستخدم، في جمع معلومات محددة عن نشاطه على المواقع الإلكترونية، فعند زيارة أي موقع، يقوم المتصفح بحفظ ملف يحتوي على بيانات تمكّن الموقع من التعرف على المستخدم وتحسين تجربة التصفح، ومن بين هذه البيانات سجل الزيارات، وتفضيلات المستخدم، وبعض المعلومات المرتبطة بسلوكه داخل الموقع.

¹ Mrs. Vijaya Sayaji Chavan, Mr. Mohan Mali, "Proxy Server – A Catching Technique" International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 10, No. 1, 2021, pp. 59–61, DOI: 10.17148/IJARCCE.2021.10111.

² الطاهر ياكور، مرجع سابق، ص 136، 137.

كما تتيح هذه الملفات إمكانية تتبّع سلوك المستخدم عبر مواقع مختلفة، مما يساعد في تحليل أنماط الاستخدام وتحسين الخدمات المقدمة.

ومن ناحية أخرى، تكتسي هذه المعطيات أهمية في مجال التحقيقات الرقمية، إذ يمكن الاعتماد عليها للكشف عن آثار النشاط الإلكتروني للمستخدم، شريطة احترام الضوابط القانونية المتعلقة بحماية الخصوصية وضمان سلامة الدليل الرقمي.¹

4- استخدام نظام جرة العسل :

يعرّف نظام (Honeypot) بأنه نظام حاسوبي يصمّم خصيصاً ليكون هدفاً ظاهرياً للهجمات الإلكترونية، دون أن يحتوي على بيانات ذات قيمة حقيقية، ويعتمد هذا النظام على مبدأ الخداع، من خلال إيهام المهاجم بسهولة اختراقه، بما يجذبه إلى استهدافه بدلاً من الأنظمة الفعلية داخل الشبكة، ويهدف ذلك إلى تحويل مسار الهجوم وحماية باقي الأجهزة، وفي الوقت ذاته تمكين الجهات المختصة من مراقبة سلوك المهاجم وجمع أكبر قدر ممكن من المعلومات حول الأساليب والتقنيات التي يستخدمها في تنفيذ اعتداءاته.²

ثانياً: أقسام الدليل الإلكتروني

تتعدد تقسيمات الدليل الإلكتروني تبعاً لطبيعته التقنية والقانونية، حيث اعتمدت التشريعات والقضاء بعض التصنيفات، في حين وضع الفقه تقسيمات أخرى، وذلك على النحو الآتي:

أ- تقسيمات التشريع والقضاء :

تشمل الأدلة الإلكترونية مختلف الوسائط والأجهزة القادرة على تخزين البيانات أو نقلها، ومن أبرزها الأقراص المغناطيسية كالأقراص الصلبة والمرنة ووسائط التخزين القابلة للإزالة، إضافة إلى الأشرطة المغناطيسية المستخدمة في حفظ النسخ الاحتياطية واسترجاع البيانات، كما تمتد لتشمل الأجهزة الإلكترونية المختلفة كالحواسيب والهواتف الذكية وأجهزة الإرسال

¹ الطاهر ياكّر، مرجع سابق، ص 137.

² حسين بن سعيد الغافري، مرجع سابق، ص 514.

والاستقبال، لما تحتويه من بيانات ومعلومات ذات قيمة إثباتية، فضلا عن أجهزة المودم التي قد تتضمن سجلات للاتصالات والبيانات المتبادلة عبر شبكة الإنترنت، كذلك تعد التسجيلات الصوتية الإلكترونية، كتسجيلات المكالمات الهاتفية الناتجة عن المراقبة الإلكترونية، من صور الدليل الإلكتروني متى تم الحصول عليها وفقا للإجراءات القانونية المقررة.¹

ب- تقسيمات الفقه:

قسم الفقه الأدلة الرقمية إلى ثلاثة أنواع رئيسية تتمثل في الأدلة الفنية، والقولية، والمادية؛ فالأدلة الفنية هي التي يتم التوصل إليها بواسطة الخبراء والفنيين المختصين، اعتمادا على التحليل التقني والمعالجة العلمية للمعطيات الرقمية لاستخلاص نتائج ذات قيمة إثباتية.

أما الأدلة القولية، فتستمد من أقوال الأشخاص، سواء تعلق الأمر بشهادة الشهود أو الاستجواب أو المواجهة أو الاعتراف.

في حين تتمثل الأدلة المادية في كل ما يتم الحصول عليه عن طريق المعاينة أو التفتيش من عناصر محسوسة قابلة للضبط والفحص، وتكتسي أهمية خاصة في تكوين قناعة القاضي الجزائي لما توفره من عناصر موضوعية تدعم عملية الإثبات.²

الفرع الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي للجريمة الإلكترونية

تقاس القوة الاستدلالية للدليل الرقمي بمدى قدرته على إثبات صحة نسبة الفعل إلى شخص معين أو نفيها، وهي تعبر عن القيمة الإثباتية لما يتم الحصول عليه من مخرجات الحاسوب بمختلف صورها، سواء كانت ورقية أو إلكترونية أو محفوظة على وسائط مصغرة، في كشف الحقيقة، غير أنه لا يكفي مجرد الحصول على الدليل الرقمي وتقديمه أمام الجهات القضائية لاعتماده كوسيلة إثبات في المجال الجزائي، إذ يبقى تقدير حجيته وقيمته الإثباتية

¹ أشرف علي قوقزة، محمد الحداد، مرجع سابق، ص 94، 95.

² نفس المرجع، ص 96.

خاضعا للسلطة التقديرية للقاضي الجزائي، الذي يتمتع بحرية تقييم الأدلة المعروضة عليه وفقا لقناعته الوجدانية، بهدف الوصول إلى الحقيقة.¹

وانطلاقا من ذلك، تبرز أهمية تحديد الشروط الواجب توافرها لقبول الدليل الرقمي أمام القضاء الجزائي، بما يضمن سلامته وموثوقيته وحجيته في الإثبات.

❖ شروط قبول الدليل الرقمي

يخضع الدليل الرقمي شأنه شأن باقي الأدلة إلى التمهيص، وبيان مدى خضوعه لشروط الدليل الإلكتروني:

1- مشروعية الدليل الرقمي:

يقصد بمشروعية الدليل الرقمي ضرورة الحصول عليه وفق الإجراءات التي يحددها القانون، وبما يضمن احترام حقوق الأفراد وحرياتهم الأساسية، تحقيقا للتوازن بين متطلبات حماية المجتمع من الجريمة، وضمان عدم التعسف في استعمال السلطة أثناء إجراءات البحث والتحري، وعليه، يتعين جمع الدليل الرقمي بطرق مشروعة قانونا، إذ يترتب على مخالفة ذلك بطلان الإجراءات وعدم جواز الاحتجاج به كوسيلة إثبات.

وترتبط مشروعية الحصول على الدليل الرقمي ارتباطا وثيقا بإجراءات التفتيش التي تهدف إلى البحث عنه وضبطه، خاصة في البيئة الرقمية.²

2- مناقشة الدليل الرقمي:

يشترط لصحة الحكم الجزائي أن تناقش الأدلة المعروضة أمام القاضي أثناء الجلسة، بحيث تطرح عليه بصورة مباشرة، ويمنح الخصوم فرصة الاطلاع عليها ومناقشتها، ويترتب على ذلك ضرورة وجود أصل ثابت للدليل ضمن ملف الدعوى، وهو ما نصّت عليه المادة

¹ فتوح الشاذلي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2003، ص 195.

² الطاهر ياكور، مرجع سابق، ص 142.

349 فقرة 2 من قانون الإجراءات الجزائية¹، وينطبق هذا الحكم كذلك على الدليل الرقمي مهما كانت صورته، ويقصد بمناقشة الدليل أن جميع الأدلة المستمدة من جرائم الحاسوب والإنترنت، سواء كانت في شكل مطبوعات، أو معروضة على أجهزة الحاسوب، أو مخزنة على حوامل البيانات، أو محفوظة على أشرطة أو أقراص مغناطيسية، تخضع كلها للمناقشة عند تقديمها كوسائل إثبات أمام المحكمة الجزائية، بما يضمن احترام مبدأ المواجهة وحقوق الدفاع.²

¹ انظر: المادة 394 فقرة 02 من ق.إ.ج.ج.

² الطاهر ياكور، مرجع سابق، ص145.

المبحث الثاني

الآليات المؤسسية لمكافحة الجريمة الإلكترونية

Institutional Mechanisms for Combating Cybercrime

في ظل التنامي المتسارع لظاهرة الجريمة الإلكترونية وتعقد أساليبها، لم يعد التصدي لها مقتصرًا على النصوص القانونية فحسب، بل أضحت يستوجب إرساء منظومة مؤسسية متكاملة تجمع بين الطابع الوقائي، القضائي، والتقني، لهذا عمل المشرع الجزائري على إحداث وتفعيل جملة من الهيئات المتخصصة التي تتكامل أدوارها في مجال الوقاية والكشف والمتابعة.

وانطلاقًا من ذلك، سنتناول في هذا المبحث الهيئات ذات الطابع الوقائي والقضائي (المطلب الأول)، والهيئات التقنية والأمنية المختصة في كشف الجرائم الإلكترونية (المطلب الثاني).

المطلب الأول: الهيئات الوقائية والقضائية في مكافحة الجرائم الإلكترونية

تضطلع الهيئات الوقائية والقضائية بدور محوري في مواجهة الجريمة الإلكترونية، سواء من خلال آليات الوقاية والتنسيق، أو عبر المتابعة القضائية المتخصصة، وقد حرص المشرع على استحداث هياكل تتلاءم مع خصوصية هذا النوع من الجرائم، بما يحقق التوازن بين البعد الوقائي والردع القانوني.

وعلى هذا الأساس، سنتطرق في هذا المطلب الهيئة الوطنية للوقاية ومكافحة الجرائم الإلكترونية (الفرع الأول)، والقطب الجزائي لمكافحة الجرائم الإلكترونية (الفرع الثاني).

الفرع الأول: الهيئة الوطنية للوقاية ومكافحة الجرائم الإلكترونية

أنشأ المشرع الجزائري سنة 2009 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها¹، في إطار تعزيز الآليات المؤسسية لمواجهة الجرائم الإلكترونية، وقد أضفى عليها بموجب المرسوم الرئاسي رقم 15-261² صفة السلطة الإدارية المستقلة، بما يمنحها قدرا من الاستقلالية في أداء مهامها، غير أنّ هذا التوجه لم يدم طويلا، إذ تمّ العدول عنه بموجب المرسوم الرئاسي رقم 19-172³، الذي أعاد تكييفها كمؤسسة عمومية ذات طابع إداري خاضعة لسلطة وزارة الدفاع الوطني⁴.

وبالرجوع إلى اختصاصات هذه الهيئة، نجد أنّ المادة 4 من المرسوم الرئاسي رقم 15-261 كانت قد حدّتها بصورة شاملة، حيث أسندت إليها وظائف متعددة تجمع بين الطابع الاستشاري والتحري، فضلا عن دورها كمرصد وطني يتولى جمع وتسجيل وحفظ المعطيات الرقمية، إلى جانب مساهمتها في مساعدة الجهات القضائية، وكذا تكوين المحققين في مجال الجرائم المعلوماتية، غير أنّ إلغاء هذا المرسوم وتعويضه بالمرسوم الرئاسي رقم 19-172 لم يبقِ على نفس المنهجية في تحديد المهام، إذ لم يورد هذا الأخير اختصاصات الهيئة بشكل إجمالي ومباشر، وإنما عمد إلى توزيعها ضمن هياكلها التنظيمية، لاسيما مجلس التوجيه والمديرية العامة، بما يعكس توجهها جديدا في تنظيم وتسيير نشاطها⁵.

¹ انظر: المادة 13 من القانون رقم 09-04 السالف الذكر.

² المرسوم الرئاسي رقم 15-261، مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، ع 53، المؤرخة في 08 أكتوبر 2015.

³ المرسوم الرئاسي رقم 19-172، مؤرخ في 06 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر، ع 37، مؤرخة في 09 جوان 2019.

⁴ انظر: المادة 02 من هذا المرسوم.

⁵ أمال حابت، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، مج 05، ع 03، ديسمبر 2021، جامعة الوادي، الجزائر، ص 466، 467.

أولاً: تشكيلة الهيئة الوطنية للوقاية ومكافحة الجرائم الإلكترونية

تتخذ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تنظيماً هيكلياً يقوم على توزيع وظيفي دقيق لمهامها، وفي هذا الإطار، نصّ المرسوم الرئاسي رقم 19-172 على أنّ الهيئة تتشكل أساساً من جهازين رئيسيين يتمثلان في مجلس التوجيه والمديرية العامة¹، وهو ما يستفاد من أحكام المواد المنظمة لتشكيلها وتسييرها، من المادة 05 إلى 15 من هذا المرسوم.

1- مجلس التوجيه:

يتخذ مجلس التوجيه صفة الجهاز التداولي الذي يعهد إليه بضبط التوجهات العامة لنشاطها، وطبقاً لأحكام المرسوم الرئاسي رقم 19-172، يتكوّن هذا المجلس من مجموعة من الأعضاء يمثلون قطاعات سيادية وإدارية وتقنية ذات صلة بمجال مكافحة الجرائم المعلوماتية، بما يضمن تنوع الخبرات وتكاملها داخل الهيئة، إذ يرأسه وزير الدفاع الوطني أو ممثله².

وتتمثل وظيفته أساساً في رسم الاستراتيجية العامة للهيئة، وتحديد سياستها في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلى جانب دراسة المسائل الكبرى المرتبطة بنشاطها، واتخاذ القرارات والتوصيات اللازمة لضمان حسن سيرها وتنسيق تدخلاتها، كما يسهم في توجيه عمل المصالح التابعة للهيئة وضبط أولوياتها، بما يحقق الفعالية والانسجام في أدائها³.

2- المديرية العامة:

تمثل المديرية العامة الجهاز التنفيذي للهيئة، وتتولى تنفيذ التوجهات والقرارات الصادرة عن مجلس التوجيه، حيث يشرف عليها مدير عام يعيّن وفقاً للإجراءات القانونية المعمول بها، ويتحمّل مسؤولية تسيير الهيئة وضمان السير الحسن لنشاطها⁴.

¹ انظر: المادة 04 من المرسوم رقم 19-172 السالف ذكره.

² انظر: المادة 05 من نفس المرسوم.

³ انظر: المادة 06 من نفس المرسوم.

⁴ انظر: المادة 09 من نفس المرسوم.

تضم المديرية العامة حسب ما نصت عليه المادة 10 من المرسوم السالف ذكره: مديرية تقنية، مديرية للإدارة والوسائل، مصالح.

وتكمن وظيفتها في مباشرة الأعمال التقنية والعملياتية، لاسيما في مجال المراقبة الإلكترونية، والتحري في الجرائم المعلوماتية¹، وجمع وتحليل المعطيات الرقمية، فضلا عن تقديم الدعم التقني للسلطات القضائية المختصة²، كما تتولى مهمة التسيير الإداري والمالي اليومي لمختلف الموارد البشرية للهيئة، كما تتولى تسيير إنفاق ميزانية الهيئة³، بما يترجم فعليا الدور الوقائي والقمعي المنوط بها.

ثانيا: مهام الهيئة الوطنية للوقاية ومكافحة الجرائم الإلكترونية

تتولى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جملة من المهام ذات الطابع الوقائي والقمعي في آن واحد من خلال توزيع مهامها ضمن هياكلها التنظيمية، حيث تضطلع بدور استباقي يتمثل في مراقبة الاتصالات الإلكترونية وجمع وتحليل المعطيات الرقمية بهدف الكشف المبكر عن التهديدات المعلوماتية، لاسيما تلك المرتبطة بالإرهاب وأمن الدولة، بما يسمح بالحد من وقوعها قبل تجسدها فعليا.⁴

كما تمارس دورا قمعيا من خلال البحث والتحري عن الجرائم المعلوماتية بعد وقوعها، عبر مباشرة إجراءات المراقبة الإلكترونية والتفتيش والحجز للأنظمة والبيانات الرقمية، وذلك في إطار قانوني وتحت إشراف الجهات القضائية المختصة.

والى جانب ذلك، تؤدي الهيئة وظيفة مساعدة للقضاء من خلال تقديم الخبرة التقنية، وجمع الأدلة الرقمية وتحليلها، وتنفيذ الإنابات القضائية، فضلا عن مساهمتها في تعزيز التعاون والتنسيق، سواء على الصعيد الوطني مع مختلف الأجهزة الأمنية والقضائية، أو على

¹ انظر: المادة 11 من المرسوم رقم 19-172 السالف ذكره.

² انظر: المادة 12 من نفس المرسوم.

³ انظر: المادة 15 من نفس المرسوم.

⁴ سهيلة بوزيرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، مج 17، ع 02، 2022، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، ص 568.

المستوى الدولي عبر تبادل المعلومات، بما يعزز فعالية مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.¹

الفرع الثاني: القطب الجزائي لمكافحة الجرائم الإلكترونية

واكب المشرع الجزائري التطورات المتسارعة التي يشهدها العالم في مجال الجريمة الإلكترونية، فاستحدث جملة من الآليات الإجرائية، كما سبق بيانه في المبحث الأول، بهدف تعزيز مكافحتها والحد من آثارها، غير أن فعالية هذه الآليات تظل مرتبطة بوجود أجهزة قضائية متخصصة تتولى تطبيقها، الأمر الذي أدى إلى إنشاء أقطاب جزائية متخصصة بالنظر إلى خطورة الجرائم الإلكترونية وما تنطوي عليه من مساس بحقوق الأفراد وأمن المجتمع.

ورغم أن المشرع الجزائري لم يضع تعريفا صريحا للأقطاب الجزائية، مكتفيا بتحديد اختصاصاتها، كما لم يتوسع الفقه بدوره في تعريفها، إلا أنه يمكن القول بأنها جهات قضائية جزائية متخصصة في معالجة والفصل في الجرائم الإلكترونية والجرائم المرتبطة بها²، ومنحت اختصاصا قضائيا موسعا للنظر في بعض الجرائم المعقدة والمنظمة، مع خضوعها للقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية.

وعليه، سيتم التطرق في هذا الفرع إلى الهيكل التنظيمي للقطب الجزائي (أولا)، ثم اختصاصات الأقطاب الجزائية (ثانيا).

أولا: الهيكل التنظيمي للقطب الجزائي لمكافحة الجرائم الإلكترونية

يتحدد التنظيم الهيكلي للقطب الجزائي الوطني ضمن دائرة اختصاص مجلس قضاء الجزائر، حيث أنشئ كهيئة قضائية وطنية متخصصة في المتابعة والتحقيق في الجرائم الإلكترونية³، ويفهم من هذا التموقع المؤسسي أن المشرع لم يتجه إلى إنشاء جهة قضائية

¹ إلهام خوشي، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة الأبحاث القانونية والسياسية، مج 04، ع 01، 2022، جامعة محمد الصديق بن يحيى، جيجل، الجزائر، ص 69.

² إبراهيم بباح، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كآلية لمكافحة الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، مج 18، ع 03، 2025، جامعة زيان عاشور، الجلفة، ص 423.

³ انظر: المادة 335 من قانون الإجراءات الجزائية.

مستقلة خارج الهرم القضائي التقليدي، بل اختار إدماج هذا القطب ضمن البنية القضائية القائمة، وهو ما يسمح بالاستفادة من الضمانات الإجرائية المعروفة، مع إدخال عنصر التخصص، كما يعكس اختيار مجلس قضاء الجزائر كمقر لهذا القطب توجهها نحو مركزية الاختصاص، بالنظر إلى ما تتمتع به هذه الجهة من إمكانيات بشرية وتقنية، إضافة إلى قربها من الهيئات الوطنية ذات الصلة، وهو ما يساهم في تعزيز فعالية التنسيق المؤسسي.

ويضم القطب جهازا قضائيا متكاملا يتكون من:

1- وكيل الجمهورية لدى القطب:

يتولى تحريك الدعوى العمومية ومباشرة إجراءات المتابعة على المستوى الوطني¹، ويعد هذا الامتداد في الاختصاص خروجاً عن القواعد التقليدية التي تقيد وكيل الجمهورية بالنطاق الإقليمي للمحكمة، الأمر الذي يعكس رغبة المشرع في توحيد السياسة الجزائية في مجال الجرائم الإلكترونية، كما يسمح هذا التوحيد بتفادي تشتت المتابعات وتضاربها، خاصة في الجرائم التي تمتد آثارها عبر عدة ولايات أو حتى خارج الحدود الوطنية.

2- قاضي التحقيق:

يختص بالتحقيق في الجرائم المعقدة، خاصة تلك التي تتطلب وسائل تقنية أو تعاوناً قضائياً دولياً²، ويستفاد من ذلك أن وظيفة التحقيق داخل هذا القطب تتجاوز الدور التقليدي، لتصبح وظيفة ذات طابع تقني متخصص، تستدعي الإلمام بوسائل الإثبات الرقمية، وأساليب تتبع البيانات، وآليات التعاون القضائي الدولي. كما أن إحالة الجرائم المعقدة إلى هذا القطب يعكس إدراك المشرع لخصوصية الإثبات في المجال الرقمي، والذي يختلف جذرياً عن الإثبات في الجرائم التقليدية.

¹ انظر: المادة 336 من ق.إ.ج.ج.

² انظر: المادتان 336 و338 من نفس القانون.

3- رئيس القطب (جهة الحكم):

يتولى الفصل في القضايا المعروضة، خاصة الجناح المرتبطة بتكنولوجيات الإعلام والاتصال.¹

ويظهر هذا التنظيم أن القطب يجمع بين وظائف المتابعة والتحقيق والحكم، وهو ما يكرّس فكرة التخصص المتكامل، حيث تتولى جهة قضائية واحدة مختلف مراحل الدعوى العمومية، كما أن تخصيص قضاة للفصل في هذا النوع من القضايا يسمح بتراكم الخبرة القضائية، وتحقيق نوع من الاستقرار في الاجتهاد القضائي، ويمارس هؤلاء جميعا اختصاصهم على كامل الإقليم الوطني، وهو ما يعكس الطابع الوطني لهذا القطب.²

ويعد هذا الامتداد الإقليمي من أبرز خصائص القطب، إذ يتلاءم مع الطبيعة اللامادية للجريمة الإلكترونية التي لا تعترف بالحدود الجغرافية، كما يساهم في تجاوز الإشكالات المرتبطة بتنازع الاختصاص المكاني، والتي غالبا ما تطرح في الجرائم المرتبطة بالشبكات المعلوماتية، ومن جهة أخرى، فإن هذا التنظيم يوحي بوجود نوع من المركزية الوظيفية، حيث تجمع مختلف القضايا ذات الطابع الإلكتروني في جهة واحدة، وهو ما يسمح بتطوير خبرة متخصصة، غير أنه قد يطرح في المقابل تحديات عملية تتعلق بكثافة القضايا وتراكم الملفات، كما يفهم من طبيعة الجرائم التي يعالجها القطب أنه يعتمد ضمنا على دعم تقني وخبرة متخصصة، بالنظر إلى اشتراط المشرع في بعض الحالات اللجوء إلى وسائل تحري خاصة وخبرة فنية³، ويعكس هذا التوجه إدراك المشرع بأن الجرائم الإلكترونية لا يمكن معالجتها بالوسائل التقليدية فقط، بل تتطلب توظيف أدوات تقنية متطورة، مثل تحليل الأنظمة المعلوماتية، وتتبع المعطيات الرقمية، واسترجاع البيانات المحذوفة.

كما يستلزم ذلك التعاون مع خبراء ومختصين في مجال الإعلام الآلي، وهو ما يكرّس الطابع متعدد التخصصات لهذا القطب، وبالإضافة إلى ذلك، يمكن استنتاج أن فعالية هذا الهيكل التنظيمي ترتبط بمدى التنسيق بين مختلف الفاعلين داخله، سواء على مستوى النيابة أو

¹ انظر: المادة 335 من ق.إ.ج.ج.

² انظر: المادة: 336 من نفس القانون.

³ انظر: المادة 338 من نفس القانون.

التحقيق أو الحكم، فضلا عن التنسيق مع الجهات التقنية والأمنية، فنجاح هذا القطب لا يتوقف فقط على النصوص القانونية، بل يمتد إلى كفاءة الموارد البشرية وقدرتها على استيعاب التطورات التكنولوجية المتسارعة.

وعليه، يظهر أن المشرع الجزائري قد تبنى نموذجا تنظيميا يقوم على ثلاثة مرتكزات أساسية: التخصص، والمركزية، والتكامل الوظيفي، وهي عناصر تهدف في مجملها إلى تعزيز فعالية العدالة الجزائية في مواجهة الجرائم الإلكترونية ذات الطبيعة المعقدة.

ثانيا: اختصاصات القطب الجزائي لمكافحة الجرائم الإلكترونية

يتمتع القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال باختصاصات واسعة ومتنوعة، تعكس إرادة المشرع في إرساء نظام قضائي متخصص قادر على مواجهة الجريمة الإلكترونية بمختلف صورها، سواء من حيث طبيعتها التقنية أو من حيث آثارها الخطيرة على النظام العام.

1- الاختصاص النوعي العام:

يختص القطب بالمتابعة والتحقيق في الجرائم المرتكبة باستعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة ذات صلة بتكنولوجيات الإعلام والاتصال، سواء كانت هذه الوسائل أداة مباشرة لارتكاب الجريمة أو مجرد وسيلة مساعدة على ارتكابها.

ويستفاد من ذلك أن معيار الاختصاص لا يقوم فقط على طبيعة الفعل، وإنما أيضا على الوسيلة المستعملة، وهو ما يسمح بإدراج طيف واسع من الأفعال الإجرامية ضمن اختصاص هذا القطب، حتى وإن كانت في أصلها جرائم تقليدية، كما يختص القطب بالحكم في هذه الجرائم إذا كانت تشكل جنحا¹، ويعكس هذا التحديد توزيعا وظيفيا دقيقا للاختصاص، حيث يحتفظ القطب بدور الفصل في الجرح، بينما تخضع الجنايات لنظام إجرائي خاص، بما يضمن احترام التدرج في خطورة الجرائم.

¹ انظر: المادة 335 من ق.إ.ج.ج.

ومن جهة أخرى، فإن هذا الاختصاص العام يشكل الإطار الأساسي الذي تنبثق عنه باقي صور الاختصاص، سواء الحصري أو المشترك، مما يجعله بمثابة القاعدة العامة في تحديد مجال تدخل القطب.

2- الاختصاص الحصري:

يمارس القطب اختصاصا حصريا في مجموعة من الجرائم التي اعتبرها المشرع ذات خطورة خاصة، بالنظر إلى طبيعتها أو آثارها أو ارتباطها بالأمن العام ونص عليها المشرع في المادة 337 من قانون الاجراءات الجزائية، ومن بينها:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.
- جرائم نشر وترويج الأخبار الكاذبة التي من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.
- الجرائم المنظمة أو العابرة للحدود المتعلقة بنشر معلومات مغرضة تمس بالنظام والأمن العموميين.
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات الخاصة بالإدارات والمؤسسات العمومية.
- جرائم الاتجار بالبشر أو بالأعضاء البشرية أو تهريب المهاجرين باستعمال الوسائل التكنولوجية
- جرائم التمييز وخطاب الكراهية عبر الوسائط الإلكترونية.¹

ويلاحظ أن المشرع لم يعتمد معيارا واحدا لتحديد هذا الاختصاص، بل جمع بين عدة معايير، أبرزها خطورة المصلحة المحمية، والطابع المنظم أو العابر للحدود، إضافة إلى الوسيلة المستعملة، ويعكس هذا التعدد في المعايير رغبة في إحاطة شاملة بمختلف صور الجريمة الإلكترونية التي قد تهدد استقرار الدولة والمجتمع.

¹ انظر: المادة 337 من ق.إ.ج.ج.

كما يمتد هذا الاختصاص الحصري ليشمل الجرائم الإلكترونية الأكثر تعقيدا، والتي تعرّف بأنها الجرائم التي تتسم بتعدد الفاعلين أو الشركاء، أو تعدد الضحايا، أو اتساع الرقعة الجغرافية، أو جسامة الأضرار، أو الطابع المنظم أو العابر للحدود، أو تلك التي تستلزم وسائل تحرّ خاصة أو خبرة فنية أو تعاوناً قضائياً دولياً.¹

ويستفاد من هذا التعريف أن المشرع اعتمد معيار التعقيد كضابط مستقل، وهو ما يسمح بإخضاع جرائم جديدة لا تدخل ضمن القائمة المحددة لنفس النظام الحصري متى توافرت فيها عناصر التعقيد.

كما أن هذا التوجه يعكس وعياً تشريعياً بطبيعة الجريمة الإلكترونية التي تتسم بالتطور المستمر، مما يستدعي نصوصاً مرنة قادرة على استيعاب صور جديدة من الإجرام، وتخضع الجرائم الداخلة ضمن الاختصاص الحصري لإجراءات خاصة منصوص عليها في القانون.²

ويؤكد ذلك أن المشرع لم يكتف بتخصيص جهة قضائية، بل أرفق هذا التخصيص بنظام إجرائي متميز يتلاءم مع خصوصية هذه الجرائم، سواء من حيث طرق التحري أو وسائل الإثبات أو آجال الإجراءات.

3- الاختصاص المشترك:

إلى جانب الاختصاص الحصري، يمارس القطب اختصاصاً مشتركاً مع الجهات القضائية الأخرى في بعض الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.³

ويفهم من ذلك أن المشرع لم يتجه إلى احتكار كامل للاختصاص، بل أبقى على قدر من المرونة يسمح بتوزيع القضايا وفقاً لمعيار الملاءمة وطبيعة الجريمة.

ويعد هذا الاختصاص المشترك تجسيدا للتوازن بين مبدأ التخصص ومبدأ القاضي الطبيعي، حيث لا تنزع جميع القضايا من الجهات القضائية العادية، وإنما فقط تلك التي

¹ انظر: المادة 338 من ق.إ.ج.ج.

² انظر: المادة 339 من نفس القانون.

³ انظر: المادة 340 من نفس القانون.

تستدعي تدخلا متخصصا، وفي هذه الحالة، تطبق إجراءات خاصة أمام القطب¹، ويظهر ذلك أن تدخل القطب، حتى في إطار الاختصاص المشترك، يظل محكوما بقواعد إجرائية متميزة، بما يحافظ على خصوصية المعالجة القضائية للجرائم الإلكترونية.

4- قواعد تنازع الاختصاص:

نظرا لتعدد الأقطاب الجزائية الوطنية وتداخل اختصاصاتها، وضع المشرع قواعد واضحة لحل تنازع الاختصاص، حيث:

- يؤول الاختصاص إلى القطب الجزائي الوطني الاقتصادي والمالي عند تزامن الاختصاص بينه وبين القطب محل الدراسة.²
- يؤول الاختصاص إلى القطب الجزائي الوطني لمكافحة الإرهاب والجريمة المنظمة عبر الوطنية عند التداخل معه.³

ويستفاد من هذه الأحكام أن المشرع اعتمد نوعا من التدرج في الاختصاص بين الأقطاب، يقوم على تغليب الجهة الأكثر تخصصا أو الأكثر ارتباطا بطبيعة الجريمة، كما تهدف هذه القواعد إلى تقادي ازدواجية المتابعة وتضارب القرارات القضائية، وهو ما يعزز الأمن القانوني ويضمن حسن سير العدالة، ومن جهة أخرى، تعكس هذه الأحكام إدماج القطب الجزائي لمكافحة الجرائم الإلكترونية ضمن منظومة أوسع من الأقطاب المتخصصة، مما يكرس توجهها عاما نحو التخصص القضائي كآلية لمواجهة الجرائم المعاصرة.

يتبين أن المشرع الجزائري قد أرسى من خلال هذه الأحكام نظاما متكاملا للاختصاص القضائي في مجال الجرائم الإلكترونية، يقوم على توسيع مفهوم الجريمة، وإقرار اختصاص حصري في الجرائم الخطيرة والمعقدة، مع الإبقاء على قدر من المرونة من خلال الاختصاص المشترك، إلى جانب وضع قواعد دقيقة لحل تنازع الاختصاص، وهو ما يعكس توجهها حديثا نحو تعزيز فعالية العدالة الجزائية في البيئة الرقمية.

¹ انظر: المادة 340 من ق.إ.ج.ج.

² انظر: المادة 341 من نفس القانون.

³ انظر: المادة 342 من نفس القانون.

المطلب الثاني: الهيئات التقنية والأمنية المختصة في كشف الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بكونها تخلف آثارا رقمية معقدة يصعب كشفها بالوسائل التقليدية، مما يفرض تدخل هيئات متخصصة تعتمد على الخبرة التقنية وأساليب التحليل الجنائي الرقمي.

وفي هذا الإطار، تضطلع الأجهزة التقنية والأمنية بدور حاسم في تعقب الأنشطة الإجرامية، وجمع الأدلة الرقمية، وتحليلها بما يضمن دعم فعالية التحقيقات القضائية.

وعليه، سيخصص هذا المطلب لدراسة كل من المعهد الوطني للأدلة الجنائية وعلم الإجرام (الفرع الأول)، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني (الفرع الثاني)، المصلحة المركزية لمكافحة الجرائم السيبرانية (الفرع الثالث).

الفرع الأول: المعهد الوطني للأدلة الجنائية وعلم الإجرام

تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب المرسوم الرئاسي رقم 04-183¹، ويعد مؤسسة عمومية ذات طابع إداري، توضع تحت وصاية وزير الدفاع الوطني، مع ممارسة هذه الوصاية من طرف قائد الدرك الوطني بتفويض منه.

يتكون هذا المعهد من إحدى عشر دائرة متخصصة في مجالات مختلفة جميعها تتضمن انجاز الخبرة، التكوين، والتعليم، وتقديم المساعدات التقنية، ومن بين هذه الدوائر توجد دائرة الاعلام الآلي والالكتروني التي تتولى معالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما يقدم المساعدة التقنية للمحققين.²

سنتناول في هذا الصدد الهيكل التنظيمي للمعهد الوطني للأدلة الجنائية وعلم الإجرام (أولا) ثم مهامه (ثانيا).

¹ المرسوم الرئاسي رقم 04-183، مؤرخ في 26 جوان 2004، يتضمن احداث المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر، ع 41، صادرة في 27 جوان 2004.

² حنان مهداوي، التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، مج 06، ع 02، 2022، جامعة عمار ثلجي، الأغواط، الجزائر، ص 1073.

أولاً: الهيكل التنظيمي للمعهد الوطني في تحليل الأدلة الرقمية

نصّ المرسوم الرئاسي المتعلق بإنشاء المعهد على أنه يدار من طرف مدير عام، ويسير بواسطة مجلس توجيه، كما يدعم بمجلس علمي يضطلع بدور استشاري في المجال العلمي والتقني ويتكوّن المعهد من مجموعة من الهياكل التنظيمية الأساسية التي تضطلع بمهام إدارية وعلمية وتقنية متكاملة، تتمثل في مديرية الأدلة الجنائية، ومديرية الدراسات والبحوث الإجرامية، إضافة إلى مصلحة التنظيم والمناهج، ومصلحة الإدارة والوسائل¹، وتتولى هذه الهياكل ضمان السير المنتظم لنشاط المعهد، من خلال التكفل بمختلف الجوانب المرتبطة بالخبرة الجنائية، والبحث العلمي الإجرامي، والتنظيم الإداري، فضلاً عن توفير الوسائل البشرية والمادي الضرورية لأداء المهام التقنية والعلمية المنوطة به، وقد أحال النص التنظيمي تحديد مهام هذه المديریات والمصالح، وكذا كفاءات تنظيمها الداخلي، إلى قرار يصدر عن وزير الدفاع الوطني، بما يتيح مرونة في تكييف الهيكلة التنظيمية للمعهد وفق متطلبات العمل والتطورات العلمية والتقنية في مجالي الأدلة الجنائية وعلم الإجرام².

سنتناول هنا المدير العام للمعهد ومجلس التوجيه والمجلس العلمي:

1- المدير العام للمعهد:

تنصّ المادة 8 على أن مهام المدير العام للمعهد يتولاها ضابط سام من الدرك الوطني، ويتم تعيينه بموجب مرسوم رئاسي بناء على اقتراح من وزير الدفاع الوطني، كما تنتهي مهامه وفق الأشكال والإجراءات نفسها³.

أما المادة 9، فقد حدّدت صلاحيات المدير العام، حيث يعدّ المسؤول الأول عن السير العام للمعهد وتسييره، وتمنح له السلطة السلمية والتأديبية على جميع المستخدمين، وبصفته هذه، يتولى المدير العام جملة من المهام، من أبرزها السهر على تطبيق القوانين والتنظيمات المعمول بها، وضمان النظام والأمن داخل المعهد، وتمثيل المعهد أمام الجهات القضائية وفي

¹ انظر: المادة 06 من المرسوم الرئاسي رقم 04-183 السالف ذكره.

² انظر: المادة 07 من نفس المرسوم.

³ انظر: المادة 08 من نفس المرسوم.

مختلف التصرفات المدنية، كما يختص بإبرام الصفقات والاتفاقيات والعقود في إطار التشريع والتنظيم الساريين، والسهر على تلبية احتياجات المعهد من حيث الموارد البشرية والمادية في حدود الإمكانيات المتاحة¹، إضافة إلى إعداد تقديرات الميزانية والعمل على تحيينها عند الاقتضاء، والالتزام بالنفقات والأمر بصرفها في حدود الاعتمادات المالية المخصصة.

ويكلف كذلك بإعداد مشروع النظام الداخلي للمعهد وعرضه على مجلس التوجيه للمداولة، مع السهر على تطبيقه بعد اعتماده، وتحضير اجتماعات مجلس التوجيه، وعرض التقرير السنوي لنشاطات المعهد عليه، فضلا عن ضمان تنفيذ مقرراته وتوصياته ومن جهة أخرى، يسهر المدير العام على توفير الوسائل الضرورية للخبرة والاستعلام الطبي الشرعي، ويضمن حسن تسيير الموارد البشرية والمادية بما يكفل السير الأمثل للتحقيقات القضائية على المستويين الوطني والدولي كما يحضر المدير العام اجتماعات مجلس التوجيه بصفة استشارية، ويتولى المعهد أمانة هذا المجلس، ويجوز له الاستعانة بأي شخص ذي كفاءة مهنية لتقديم الاستشارة بشأن المسائل المدرجة في جدول الأعمال².

2- مجلس التوجيه:

اعتمد المشرع مجلس التوجيه كهيئة تداولية واستراتيجية تتولى تحديد برامج عمل المعهد وضبط شروط سيره العام، فضلا عن تقييم النتائج المحققة بصورة دورية، كما يختص المجلس بدراسة مشاريع تنظيم المعهد، وبرامج نشاطه، وآفاق تطويره، واتفاقيات التعاون التي يبرمها، إضافة إلى مشاريع الميزانية والحصائل المالية والنظام الداخلي والتقرير السنوي لنشاط المعهد³، ويتأخرس مجلس التوجيه ممثل عن وزير الدفاع الوطني، ويضم في عضويته ممثلين عن عدة قطاعات وزارية ذات صلة بمجال نشاط المعهد، من بينها الداخلية، والعدل، والمالية، والصحة، والتعليم العالي، والطاقة، والفلاحة، والنقل، والبريد وتكنولوجيا الإعلام والاتصال، والصناعة، وهو ما يعكس الطابع متعدد الاختصاصات الذي يميز مجال الأدلة الجنائية وعلم الإجرام.

¹ انظر: المادة 09 من المرسوم رقم 04-183 السالف الذكر.

² انظر: المادة 09 من نفس المرسوم.

³ انظر: المادة 10 من نفس المرسوم.

كما يحضر المدير العام اجتماعات المجلس بصوت استشاري، ويتولى المعهد أمانة المجلس، مع إمكانية الاستعانة بأشخاص ذوي كفاءة مهنية عند الحاجة¹، ويتم تعيين أعضاء مجلس التوجيه لمدة ثلاث سنوات قابلة للتجديد، بناء على اقتراح السلطات التي يتبعون لها، مع استخلاف الأعضاء المنقطعة عهدتهم وفقا للإجراءات نفسها²، ويجتمع مجلس التوجيه في دورتين عاديتين سنويا بناء على استدعاء من رئيسه، كما يمكن عقد دورات غير عادية كلما اقتضت الضرورة ذلك، سواء بطلب من رئيس المجلس أو بطلب من ثلثي أعضائه أو بطلب من المدير العام للمعهد³، ولا تصح مداولات مجلس التوجيه إلا بحضور ثلثي أعضائه على الأقل، وتتخذ القرارات بالأغلبية البسيطة للأعضاء الحاضرين، وفي حالة تعادل الأصوات يكون صوت الرئيس مرجحا، كما تدون المداولات في محاضر رسمية ترسل إلى وزير الدفاع الوطني للموافقة عليها، ولا تصبح بعض المداولات نافذة، لاسيما المتعلقة بالميزانية والحسابات والاقتتات والهبات، إلا بعد الموافقة الصريحة لوزير الدفاع الوطني⁴.

3- المجلس العلمي:

يعتبر المجلس العلمي هيئة استشارية علمية وتقنية تساعد إدارة المعهد في تحديد النشاطات العلمية وأعمال التكوين وتقييمها، فضلا عن اقتراح مناهج جديدة في مجال التحريات الجنائية، كما يبدي رأيه بشأن برامج البحث العلمي، ومشاريع اقتناء التجهيزات والوثائق، واتفاقيات التعاون العلمي، وبرامج توظيف المستخدمين العلميين وترقيتهم، إضافة إلى تقييم مناهج التحليل ودراسة المرجعيات القضائية والإدارية والمالية المتعلقة بالفحوص والخبرات⁵، ويتألف المجلس العلمي خبير ذو كفاءة معترف بها يعين من طرف وزير الدفاع الوطني بناء على اقتراح المدير العام للمعهد، ويضم في عضويته مدير الدراسات والبحوث الإجرامية، ورؤساء المصالح، وطبيبا شرعيا، إلى جانب ممثلين عن المستخدمين التقنيين والإداريين، كما يمكن للمجلس الاستعانة بأشخاص ذوي اختصاص وخبرة للمساهمة في دراسة المسائل العلمية

¹ انظر: المادة 11 من المرسوم رقم 04-183 السالف الذكر.

² انظر: المادة 12 من نفس المرسوم.

³ انظر: المادة 13 من نفس المرسوم.

⁴ انظر: المواد 14-15-16 من نفس المرسوم.

⁵ انظر: المادة 17 من نفس المرسوم.

والتقنية المطروحة¹، ويجتمع المجلس العلمي مرة واحدة على الأقل كل ثلاثة أشهر بناء على استدعاء من رئيسه، وتدون مداولاته في محاضر رسمية تسجل في سجل خاص، مع تبليغ مستخرج منها إلى وزير الدفاع الوطني.²

ثانيا: مهام المعهد الوطني في التحقيقات الجنائية المعلوماتية

تتمثل مهام المعهد، وفقا لما نصت عليه المادة 04، فيما يلي:

- إنجاز الخبرات والفحوص العلمية التي تدخل ضمن اختصاص القضاة والمحققين أو الجهات المخولة، بناء على طلبهم، في إطار التحريات الأولية والتحقيقات القضائية، بهدف إثبات الأدلة التي تمكّن من تحديد مرتكبي الجرائم، تقديم المساعدة العلمية خلال إجراء التحريات المعقدة، من خلال توظيف أساليب الشرطة العلمية والتقنية الهادفة إلى جمع وتحليل الأشياء والآثار والوثائق المستخرجة من مسرح الجريمة.
- الإسهام في إعداد الدراسات والتحليل الهادفة إلى الوقاية من مختلف أشكال الإجرام والحدّ منها.
- تصميم وإنشاء بنوك للمعطيات وفقا لأحكام القانون، بما في ذلك قواعد البيانات الخاصة بالبصمات الجينية، على أن توضع تحت تصرف القضاة والمحققين لتمكينهم من إجراء المقارنات واستنتاج الروابط المحتملة بين الجناة وأساليب نشاطهم الإجرامي.
- المبادرة بإجراء البحوث في مجال الإجرام، مع الاعتماد على التقنيات الحديثة والمتطورة.
- العمل على تطوير البحث التطبيقي وأساليب التحري التي أثبتت نجاعتها في مجالي علم الإجرام والأدلة الجنائية، سواء على المستوى الوطني أو الدولي.
- المشاركة في الملتقيات والمحاضرات والندوات الوطنية والدولية التي تسهم في تطوير كفاءات مستخدمي المعهد.

¹ انظر: المادة 18 من المرسوم رقم 04-183 السالف الذكر.

² انظر: المادة 19 من نفس المرسوم.

- إعداد برامج البحوث المسندة إلى جهات خارجية، مع ضمان متابعتها وتقييم نتائجها.¹

الفرع الثاني: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني

تأسس مركز الوقاية من جرائم الإعلام الآلي ومكافحتها التابع للدرك الوطني عام 2008 كخطوة استراتيجية لتعزيز الأمن العمومي وحماية الأنظمة المعلوماتية، خاصة في القطاعات الحساسة كالبنوك والمؤسسات الرسمية، ويتخذ المركز من "بئر مراد رابيس" مقرا له، حيث يعمل كقطب تقني متخصص في تحليل المعطيات الرقمية وتحديد هويات الجناة، سواء كانوا أفراداً أو شبكات إجرامية.

كما يضطلع بدور حيوي في دعم المحققين وتوجيه التحريات التكنولوجية ومعاينة الأدلة الرقمية، مع التركيز بشكل خاص على مكافحة القرصنة والإرهاب الإلكتروني²، وذلك بالتوازي مع جهود مستمرة لتطوير كفاءات الكوادر البشرية من مهندسين وقانونيين عبر التكوين المتخصص والتعاون الدولي.

على صعيد المهام الميدانية، يتولى المركز المراقبة الدائمة لشبكة الإنترنت والاتصالات الإلكترونية تحت إشراف قضائي، مساهما في عمليات التحري والتسلل الرقمي لردع الجريمة بالتعاون مع مختلف الهيئات الأمنية والوحدات الإقليمية.

وتعكس الإحصائيات الرسمية لعام 2020 تحولا خطيرا في المشهد الإجرامي نحو الفضاء الافتراضي؛ حيث سجلت مصالح الأمن والدرك قرابة 8000 جريمة إلكترونية، وقفزت القضايا لدى الأمن الوطني من 500 قضية في 2015 إلى 5200 قضية في 2020، بينما عالج الدرك الوطني 1362 جريمة تورط فيها 1028 شخصا، وتصدرت جرائم القذف والسب قائمة هذه التجاوزات بنسبة فاقت 55%، تليها الجرائم الموجهة ضد الأمن العمومي، والابتزاز،

¹ Noui, Ahmed, & Guedouari, Fatma Zohra, A Legal Vision of Electronic Crime and the Controls to Confront It in Algerian Law, The International Conference on "Cybercrime and the Evidentiary Value of Digital Evidence in Proof", Maghreb-Mashreq Strategic Studies Center (United Kingdom), January 1, 2024, p. 286, <https://doi.org/10.5281/zenodo.19329875>

² سميحة بلقاسم، حميد بوشوشه، الجريمة الإلكترونية بعد جديد للجرائم في الجزائر واقعها وآليات مجابقتها، مجلة العلوم الإنسانية، مج 10، ع 01، جوان 2023، جامعة العربي بن المهيدي أم البواقي، ص 551.

والنصب، والاعتداء على الخصوصية، مما يبرز التحديات المتزايدة التي يواجهها المركز في حماية الفضاء الرقمي.¹

الفرع الثالث: المصلحة المركزية لمكافحة الجرائم السيبرانية

تعتبر المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني إحدى أهم الآليات الأمنية المستحدثة لمواجهة الإجرام السيبراني في الجزائر، حيث جاء إنشاؤها في إطار تكييف هيكل مديرية الشرطة القضائية مع متطلبات الأمن المعلوماتي والتطور المتسارع للجرائم الإلكترونية، وقد بدأت هذه المصلحة في شكل فصيلة متخصصة شكّلت النواة الأولى لجهاز أمني موجه خصيصا لمكافحة هذا النوع من الجرائم سنة 2011، قبل أن يتم تعزيزها بإنشاء المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وإدراجها ضمن الهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015.²

تضطلع هذه المصلحة بعدة مهام أساسية، من أبرزها تقديم الدعم التقني لمصالح الشرطة القضائية في مجال التحريات، والمساهمة في حماية الأنظمة المعلوماتية والفضاء السيبراني الوطني، إلى جانب التعاون والمشاركة في التحقيقات ذات البعد الوطني والدولي المتعلقة بالجرائم الإلكترونية.

كما تتولى مهمة اليقظة المعلوماتية من خلال رصد الشبكات المفتوحة والبحث عن المحتويات غير المشروعة التي تشكل جرائم أو تمس بالنظام العام، فضلا عن مساهمتها في تكوين وتأهيل عناصر الشرطة المختصين في هذا المجال على مستوى أمن الولايات، ولا يقتصر دور هذه المصلحة على الجانب الردعي والتقني فحسب، بل يمتد أيضًا إلى الجانب الوقائي من خلال توعية وتحسيس المواطنين بمخاطر استعمال شبكة الإنترنت، لاسيما فئة الأطفال باعتبارهم الأكثر عرضة لهذه التهديدات.

¹ سميحة بلقاسم، حميد بوشوشه، مرجع سابق، ص 551.

² نفس المرجع، ص 552.

وفي إطار تعزيز فعالية هذه الجهود، خاصة بالنظر إلى الطابع العابر للحدود الذي تتسم به الجرائم الإلكترونية، تحرص المديرية العامة للأمن الوطني على تفعيل تعاونها الدولي، حيث تعد عضوا فعالا في المنظمة الدولية للشرطة الجنائية (الإنتربول)، التي تتيح آليات متقدمة لتبادل المعلومات على المستوى الدولي، وتسهّل إجراءات تسليم المجرمين، وتنفيذ الإنابات القضائية الدولية، إلى جانب نشر أوامر القبض بحق المبحوث عنهم دوليا.¹

¹ سميحة بلقاسم، حميد بوشوشه، مرجع سابق، ص 548-549 .

الخاتمة

في ختام هذه الدراسة المتعلقة بآليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، يتبين أن التطور المتسارع لتكنولوجيات الإعلام والاتصال وما صاحبه من توسع في استعمال الوسائط الرقمية وتطبيقات الذكاء الاصطناعي، قد أدى إلى بروز أنماط إجرامية حديثة اتسمت بالتعقيد والطابع العابر للحدود، الأمر الذي جعل الجريمة الإلكترونية من أبرز التحديات التي تواجه المنظومة الجنائية المعاصرة، سواء من حيث التجريم أو من حيث آليات التحري والتحقيق والإثبات.

وقد سعى المشرع الجزائري إلى مواكبة هذه التحولات من خلال إرساء منظومة قانونية تهدف إلى مجابهة الجريمة الإلكترونية، وذلك عبر تدعيم القواعد الموضوعية المتعلقة بالتجريم والعقاب، واستحداث آليات إجرائية خاصة تتلاءم مع خصوصية هذا النوع من الجرائم، إلى جانب إنشاء هيئات قضائية وأمنية وتقنية مختصة تتولى مهام الوقاية والكشف والتحري والمتابعة.

كما أظهرت هذه الدراسة أن فعالية مكافحة الجريمة الإلكترونية لم تعد مرتبطة فقط بوجود نصوص قانونية تجرم الأفعال الماسة بالأنظمة المعلوماتية، وإنما أصبحت تقتضي أيضا توفير آليات تقنية وبشرية متخصصة قادرة على مواكبة التطور المستمر لوسائل الإجرام الإلكتروني، خاصة في ظل التطور المتسارع للتكنولوجيا الحديثة وما نتج عنها من ظهور أساليب إجرامية أكثر تعقيدا.

النتائج المستخلصة من الدراسة:

أسفرت هذه الدراسة عن جملة من النتائج الأساسية، يمكن إجمال أهمها فيما يلي:

1. تتميز الجريمة الإلكترونية بخصوصية قانونية وتقنية تجعلها تختلف عن الجرائم التقليدية من حيث طبيعتها ووسائل ارتكابها وطرق إثباتها.
2. تبني المشرع الجزائري سياسة جنائية خاصة لمواجهة الجريمة الإلكترونية، من خلال إدراج نصوص تجرimeية ضمن قانون العقوبات إلى جانب سن قوانين خاصة مكمله.
3. جرم المشرع الجزائري مختلف الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، سواء تعلق الأمر بالدخول غير المشروع إلى الأنظمة المعلوماتية أو الاعتداء على المعطيات الإلكترونية.

4. توسع نطاق الحماية الجنائية ليشمل المعطيات ذات الطابع الشخصي بموجب القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.
5. شمل التجريم أيضا الاعتداءات المرتبطة بقطاع البريد والاتصالات الإلكترونية بموجب القانون رقم 04-18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.
6. أقر المشرع الجزائي أحكام الشروع والمساهمة الجنائية في الجرائم الإلكترونية، بما يسمح بتوسيع نطاق المتابعة الجزائية.
7. اعترف المشرع الجزائي بالمسؤولية الجزائية للشخص المعنوي في الجرائم الإلكترونية إلى جانب الشخص الطبيعي.
8. تتسم الجرائم الإلكترونية بصعوبة اكتشافها وإثباتها بسبب اعتماد مرتكبيها على وسائل تقنية حديثة لطمس الأدلة الرقمية وإخفاء آثار الجريمة.
9. استحدث المشرع الجزائي مجموعة من الآليات الإجرائية الخاصة بمكافحة الجريمة الإلكترونية، لاسيما ما تعلق بتفتيش الأنظمة المعلوماتية واعتراض المراسلات الإلكترونية وتمديد الاختصاص المحلي لوكيل الجمهورية وضباط الشرطة القضائية.
10. تدارك المشرع الجزائي من خلال قانون الإجراءات الجزائية رقم 14-25 الإشكال الذي كان يثار في ظل الأحكام السابقة المتعلقة باشتراط رضا الشخص المعني بإجراء المعاينة، حيث أصبح هذا الإجراء يتم بناء على إذن قضائي دون اشتراط موافقة الشخص محل المعاينة، بما يعزز فعالية إجراءات البحث والتحقيق في الجرائم الإلكترونية.
11. يشكل الدليل الإلكتروني وسيلة أساسية في إثبات الجرائم الإلكترونية، بالنظر إلى ارتباط هذا النوع من الجرائم بالبيئة الرقمية.
12. ترتبط حجية الدليل الإلكتروني بمدى احترام الضوابط القانونية والتقنية المتعلقة بجمعه وحفظه واستخراجه.
13. أظهر قانون الإجراءات الجزائية المعدل بموجب القانون رقم 14-25 توجهها تشريعيا نحو تدعيم آليات مكافحة الجرائم الإلكترونية ومواكبة التطورات التقنية الحديثة.

14. ساهم استحداث القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 11-21 في تعزيز التخصص القضائي في مجال مكافحة الجريمة الإلكترونية.
 15. تضطلع الهيئات الأمنية المختصة، لاسيما المصالح المكلفة بمكافحة الجرائم السيبرانية، بدور أساسي في كشف الجرائم الإلكترونية وجمع الأدلة الرقمية.
 16. تؤدي الهيئات التقنية دورا مهما في دعم التحقيقات المرتبطة بالجريمة الإلكترونية، من خلال تقديم الخبرة التقنية اللازمة للكشف عن الجرائم المعلوماتية وتتبع مرتكبيها.
 17. تساهم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في تعزيز آليات الوقاية والتنسيق بين مختلف الجهات المتدخلة في هذا المجال.
 18. ما تزال المنظومة القانونية الجزائرية تواجه تحديات مرتبطة بسرعة تطور وسائل الإجرام الإلكتروني مقارنة بالتطور التشريعي.
 19. تتطلب فعالية مكافحة الجريمة الإلكترونية تكوين موارد بشرية متخصصة تجمع بين الكفاءة القانونية والخبرة التقنية.
 20. تبرز أهمية التعاون والتنسيق بين مختلف الهيئات القضائية والأمنية والتقنية من أجل ضمان فعالية مكافحة الجرائم الإلكترونية.
 21. تفرض الطبيعة العابرة للحدود للجريمة الإلكترونية ضرورة تعزيز التعاون الدولي في مجال تبادل المعلومات والمساعدة القضائية والتقنية.
- الاقتراحات المقدمة:**

- بناء على ما سبق، يمكن تقديم جملة من الاقتراحات من أجل تعزيز فعالية مكافحة الجريمة الإلكترونية في التشريع الجزائري، من أهمها:
- ✓ مواصلة تحيين النصوص القانونية المتعلقة بالجريمة الإلكترونية بما يواكب التطورات المتسارعة لتكنولوجيات الإعلام والاتصال وتطبيقات الذكاء الاصطناعي.
 - ✓ تعزيز التكوين المتخصص للقضاة وأعضاء النيابة العامة وضباط الشرطة القضائية في مجال الجرائم الإلكترونية والأدلة الرقمية.

الخاتمة

- ✓ دعم المصالح الأمنية والتقنية المختصة بالإمكانات البشرية والتقنية اللازمة لمواجهة الجرائم الإلكترونية.
- ✓ تعزيز آليات حماية المعطيات ذات الطابع الشخصي وضمان أمن الأنظمة المعلوماتية.
- ✓ تدعيم التعاون والتنسيق بين مختلف الهيئات القضائية والأمنية والتقنية المختصة بمكافحة الجريمة الإلكترونية.
- ✓ تكثيف برامج التوعية والتحسيس بمخاطر الجرائم الإلكترونية وسبل الوقاية منها، خاصة لفئة القصر ومستخدمي الوسائط الرقمية.
- ✓ تشجيع البحث العلمي المتخصص في مجال الجرائم الإلكترونية والأمن السيبراني.
- ✓ تعزيز التعاون الدولي في مجال مكافحة الجريمة الإلكترونية، خاصة في مجال تبادل الخبرات والمعلومات والمساعدة القضائية.

قائمة المصادر والمراجع

أولاً: المصادر

1- النصوص التشريعية والتنظيمية:

❖ باللغة العربية:

أ- القوانين:

1. القانون رقم 04-09، المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، ع 47، صادرة في 16 أوت 2009.
2. القانون رقم 04-15، المؤرخ في 01 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر، ع 06، صادرة في 10 فيفري 2015.
3. القانون رقم 07-18، المؤرخ في 10 جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، ع 34، صادرة في 10 جوان 2018.
4. القانون رقم 02-24، مؤرخ في 26 فيفري 2024، يتعلق بمكافحة التزوير واستعمال المزور، ج ر، ع 15، صادرة في 29 فيفري 2024.
5. القانون رقم 06-24، المؤرخ في 28 أبريل 2024، المعدل والمتمم للأمر رقم 66-156، يتضمن قانون العقوبات، ج ر، ع 30، الصادرة في 30 أبريل 2024.
6. القانون رقم 04-18، المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، ج ر، ع 27، صادرة في 13 ماي 2018، المعدل والمتمم بالقانون رقم 11-25، المؤرخ في 24 جويلية 2025، ج ر، ع 48، الصادرة في 24 جويلية 2025.
7. القانون رقم 14-25، مؤرخ في 3 أوت 2025، يتضمن قانون الإجراءات الجزائية، ج ر، ع 54، صادرة في 13 أوت 2025.

ب-الأوامر:

1. الأمر رقم 66-156، المؤرخ في 8 جوان 1966، يتضمن قانون العقوبات، ج ر، ع 49، صادرة في 11 جوان 1966، المعدل والمتمم.

ج-المراسيم:

1. المرسوم الرئاسي رقم 04-183، مؤرخ في 26 جوان 2004، يتضمن احداث المعهد الوطني للأدلة الجنائية وعلم الاجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر، ع 41، صادرة في 27 جوان 2004.

2. المرسوم الرئاسي رقم 15-261، مؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج ر، ع 53، المؤرخة في 08 أكتوبر 2015.
3. المرسوم الرئاسي رقم 19-172، مؤرخ في 06 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج ر، ع 37، مؤرخة في 09 جوان 2019.

ثانيا: المراجع

❖ المراجع باللغة العربية:

أ-الكتب:

1. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، الطبعة التاسعة، دار هومه لطباعة والنشر والتوزيع، الجزائر، 2008.
2. أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الديوان الوطني للأشغال التربوية، الجزائر، 2002.
3. أشرف علي قوقزة، محمد حداد، الأدلة الرقمية في اثبات الجرائم الالكترونية في التشريع الأردني (دراسة مقارنة)، دار المناهج، الأردن، الطبعة الأولى، 2021.
4. آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار دار هومه للطباعة والنشر والتوزيع، الجزائر، 2007.
5. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر، 2009.
6. خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، مصر، 2012.
7. رشيدة بوكري، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، الطبعة الأولى، 2012.
8. سيد علي السيد محمد، الجرائم الالكترونية، دار التعليم الجامعي، الاسكندرية، مصر، 2024.
9. الطاهر ياكور، الجرائم الالكترونية الأحكام الموضوعية والاجرائية، دراسة مقارنة، دار بلقيس، الجزائر، 2024.
10. عبد الحكم سيد سالم، الجرائم المعلوماتية وآثارها في ضوء قانون مكافحة جرائم تقنية المعلومات، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر، 2023.

11. عبد الحكم سيد سالمان، الجرائم المعلوماتية وآثارها في ضوء قانون مكافحة جرائم تقنية المعلومات، مركز الدراسات العربية، مصر، الطبعة الأولى، 2023.
12. عبد الفتاح بيومي حجازي، الجوانب الاجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، بهجات للطباعة والتجليد القاهرة، مصر، الطبعة الأولى، 2009.
13. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، القاهرة، مصر، 2004.
14. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الثاني، دار الفكر الجامعي، الإسكندرية، مصر، 2002.
15. عبد الله سليمان، شرح قانون العقوبات الجزائري، ديوان المطبوعات الجامعية، الجزائر، 2002.
16. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، مصر، 1999.
17. علي عدنان الفيل، اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، الأردن، 2012.
18. عمر أبو الفتوح عبد العظيم الحامي، الحماية الجنائية للمعلومات المسجلة إلكترونياً (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2010.
19. غنية باطلي، الجريمة الإلكترونية دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، 2015.
20. فارس خطابي، الحماية الجزائرية للتوقيع الإلكتروني، أطروحة دكتوراه، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2020/2021.
21. فتوح الشاذلي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2003.
22. لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة الإلكترونية، دار الحامد للنشر والتوزيع، عمان، الأردن، ط 1، 2015.
23. محمد حزيط، الوجيز في قانون الاجراءات الجزائية الجزائري، دار بلقيس، 2026، الجزائر.
24. محمد حماد مرهج الهيتي، جرائم الحاسوب: ماهيتها - موضوعها - أهم صورها والصعوبات التي تواجهها، دار المناهج للنشر والتوزيع، عمان، الأردن، 2006.
25. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.
26. محمد عبد العزيز إبراهيم مدحت، قانون العقوبات القسم العام النظرية العامة للعقوبة والتدابير الاحترازية، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2007.

27. محمد فاضل، الجرائم الواقعة على أمن الدولة، مطبعة جامعة دمشق، 1963.
28. محمد معروف عبد الله، علم العقاب، المكتبة القانونية، بغداد، العراق، ط2، 2010.
29. محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الاسكندرية، الطبعة الأولى، 2014.
30. محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الالكترونية، مكتبة الوفاء القانونية، الاسكندرية، مصر، الطبعة الأولى، 2014.
31. مسعود خثير، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010.
32. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005.
33. نهلة عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.
34. وسيم حسام الدين الأحمد، مكافحة الجريمة الالكترونية في التشريعات والاتفاقيات الدولية، دار غيداء للنشر والتوزيع، عمان، الأردن، ط1، 2020.

ب- الرسائل العلمية:

❖ أطروحات الدكتوراه:

1. عبد القادر مصطفى، الآليات الجزائية الموضوعية لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أطروحة دكتوراه في القانون العام، تخصص قانون جنائي وعلم الإجرام، كلية الحقوق، جامعة الجزائر 1، 2022/2021.
2. عبير بعقيقي، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والاماراتي، دراسة مقارنة، أطروحة دكتوراه في الحقوق، تخصص النظام الجزائي والسياسة الجزائية المعاصرة، جامعة محمد خيضر بسكرة، كلية الحقوق والعلوم السياسية، 2018-2019.

❖ رسائل الماجستير:

1. آمال قارة، الجريمة المعلوماتية، مذكرة ماجستير، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2002.
2. مريم أحمد مسعود، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 09-04، مذكرة ماجستير، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح-ورقلة، الجزائر، 2013.

3. نسيم دردور، جرائم المعلوماتية في ضوء القانون الجزائري والمقارن، مذكرة ماجستير، شعبة القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة، 2013.

ج-المقالات القانونية:

1. ابراهيم بباح، القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال كآلية لمكافحة الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، مج 18، ع 03، 2025، جامعة زيان عاشور، الجلفة.
2. أسامة صلاح محمد، التكييف القانوني للاتفاق الجنائي في الجريمة، دراسة مقارنة بين التشريع الجنائي العراقي والسوداني، المجلة الأكاديمية للبحوث القانونية والسياسية، مج 05، ع 01، 2021، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي - الأغواط، الجزائر.
3. إلهام خرشي، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مجلة الأبحاث القانونية والسياسية، مج 04، ع 01، 2022، جامعة محمد الصديق بن يحيى، جيجل، الجزائر.
4. أمال حابت، الجريمة المعلوماتية في التشريع الجزائري بين قانوني 04-15 و 04-09، مجلة هيروودوت للعلوم الإنسانية والاجتماعية، مج 07، ع 25، 2023، مؤسسة هيروودوت للبحث العلمي والتكوين، الجزائر.
5. أمال حابت، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، لوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، مج 05، ع 03، ديسمبر 2021، جامعة الوادي، الجزائر.
6. حنان مهداوي، التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، مج 06، ع 02، 2022، جامعة عمار ثليجي، الأغواط، الجزائر.
7. خاليدة بن بعلاش، علي عثمان، الأحكام الموضوعية والإجرائية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة أبحاث قانونية وسياسية، مج 06، ع 02، ديسمبر 2021، جامعة محمد الصديق بن يحيى، جيجل، الجزائر.
8. زكرياء ذيب، تجريم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 07، العدد 02، 2023، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي - الأغواط، الجزائر.

9. الزهرة جقريف، الحماية الجزائية للمعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون 07-18، مجلة العلوم القانونية والاجتماعية، مج 06، ع 04، ديسمبر 2021، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور - الحلفة، الجزائر.
10. زوليخة زوزو، مشروعية أساليب التحري الحديثة، مجلة الحقوق والعلوم السياسية، ع 8، جوان 2017، جامعة خنشلة.
11. سامح، القليوبي، جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، مصر، 2010.
12. سميحة بلقاسم، حميد بوشوشه، الجريمة الالكترونية بعد جديد للجرائم في الجزائر واقعها وآليات مجابقتها، مجلة العلوم الانسانية، مج 10، ع 01، جوان 2023، جامعة العربي بن المهيدي أم البواقي.
13. سهيلة بوزبرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، مج 17، ع 02، 2022، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر.
14. شهرزاد بوعزيز، مستجدات عقوبة المصادرة في قانون العقوبات الجزائري، مجلة الدراسات والبحوث القانونية، مج 10، ع 02، جوان 2025، جامعة المسيلة، الجزائر، ص 339.
15. صليحة بن عودة، الشروع في الجرائم المعلوماتية بين الوقاية والردع، مجلة دفاتر الحقوق والعلوم السياسية، مج 01، ع 02، 2021، معهد الحقوق والعلوم السياسية، بالمركز الجامعي مغنية، الجزائر.
16. عبد الحميد سفيان، أساليب التحري الخاصة في قانون الاجراءات الجزائية الجزائري، مجلة صوت القانون، مج 09، ع 02 ماي 2023، كلية الحقوق والعلوم السياسية، جامعة لونيبي علي البليدة 2.
17. عبد القادر بونيف، موقف القانون الجزائري من الاتفاق الجنائي في الجرائم السيبرانية، مجلة البحوث القانونية والاقتصادية، مج 08، ع 01، 2025.
18. عبد الوهاب ملياني، الجرائم الماسة بالمعطيات الشخصية على ضوء القانون رقم 07-18، مجلة البحوث القانونية والاقتصادية، مج 06، ع 01، 2023، المركز الجامعي آفلو، الجزائر.
19. عز الدين طباش، "الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل قانون 07/18 المعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"، المجلة الأكاديمية للبحث القانوني، ع 02، 2018، كلية الحقوق والعلوم السياسية، جامعة بجاية، الجزائر.

20. فتحي محدة، إدريس قرفي، إجراءات المتابعة القضائية للشخص المعنوي المسؤول جزائيا بين التشريعين الفرنسي والجزائري، مجلة العلوم القانونية والسياسية، ع 04، جانفي 2012، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر.
21. لميز أمينة، الدليل الرقمي كآلية لإثبات الجرائم المعلوماتية، مجلة بحوث في القانون والتنمية، ع 3، جوان 2023، جامعة بومرداس.
22. محمد خليفة، خصوصية الجريمة الإلكترونية وجهود المشرع الجزائري في مواجهتها، مجلة دراسات وأبحاث، مج 01، ع 01، 2009، جامعة زيان عاشور بالجلفة، الجزائر.
23. معمر فراق، الشروع في الجريمة بين التشريع العقابي المعاصر والفقه الجنائي الإسلامي، مجلة الحقيقة، مج 17، ع 04، ديسمبر 2018، جامعة أحمد دراية - أدرار، الجزائر.
24. نوال مجدوب، الآليات الاجرائية للكشف عن الجريمة المعلوماتية، مجلة البحوث القانونية والاقتصادية، مج 06، ع 03 2023، المركز الجامعي آفلو، الجزائر.
25. واضح الحاج، التنظيم القانوني لعنوان بروتوكول الانترنت، مجلة الدراسات القانونية المقارنة، مج 07، ع 01، 2021، جامعة حسيبة بن بوعلي، الشلف، الجزائر.
26. وردية فتحي، عن خصوصية الجزاء في الجرائم المالية، المجلة النقدية للقانون والعلوم السياسية، مج 10، ع 01، 2015، كلية الحقوق والعلوم السياسية، جامعة مولود معمري - تيزي وزو، الجزائر.

د-الملتقيات العلمية:

1. عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثاني، 2000.
2. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة، مداخلة علمية، ضمن فعاليات المؤتمر العربي الأول: (العلوم الأدلة الجنائية والطب الشرعي)، المنعقد أيام 12-14 نوفمبر 2007، المنظم بجامعة نايف العربية للعلوم الأمنية، الرياض.

هـ-المواقع الالكترونية:

اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، المعتمدة في 23 نوفمبر 2001، الأمم المتحدة، متاحة على موقع مكتب الأمم المتحدة المعني بالمخدرات والجريمة

<https://www.unodc.org>، تمت زيارة الموقع بتاريخ 28 مارس 2026، بتوقيت: 15.38.

❖ المراجع باللغة الأجنبية:

1. Mrs. Vijaya Sayaji Chavan, Mr. Mohan Mali, “**Proxy Server – A Catching Technique**” International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 10, No. 1, 2021, pp. 59–61, DOI: [10.17148/IJARCCE.2021.10111](https://doi.org/10.17148/IJARCCE.2021.10111).
2. Noui, Ahmed, & Guedouari, Fatma Zohra, **A Legal Vision of Electronic Crime and the Controls to Confront It in Algerian Law**, The International Conference on “Cybercrime and the Evidentiary Value of Digital Evidence in Proof”, Maghreb–Mashreq Strategic Studies Center (United Kingdom), January 1, 2024, p. 286, <https://doi.org/10.5281/zenodo.19329875>.

..

فهرس المحتويات

الصفحة	فهرس المحتويات
أ-ز	مقدمة
6	الفصل الأول: الآليات الموضوعية في مكافحة الجريمة الإلكترونية
9	المبحث الأول: تجريم الأفعال المكونة للجريمة الإلكترونية
10	المطلب الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفق قانون العقوبات
10	الفرع الأول: الجرائم الماسة بالأنظمة المعلوماتية
11	أولاً: جرائم الولوج غير المشروع إلى الأنظمة المعلوماتية
16	ثانياً: الجرائم الماسة بسير الأنظمة المعلوماتية
19	الفرع الثاني: الجرائم الماسة بالمعطيات المعلوماتية داخل النظام
20	أولاً: جريمة التلاعب غير المشروع بالمعطيات المعلوماتية
21	ثانياً: جريمة التعامل غير المشروع في المعطيات ذات المصدر غير المشروع
22	المطلب الثاني: الجرائم الإلكترونية في التشريعات الخاصة
22	الفرع الأول: الجرائم الماسة بالمعطيات الشخصية في القانون رقم 07-18
23	أولاً: الجرائم المتعلقة بالقواعد الشكلية للمعالجة
26	ثانياً: الجرائم المتعلقة بالقواعد الموضوعية للمعالجة
29	الفرع الثاني: الجرائم الماسة بتنظيم الاتصالات الإلكترونية في القانون رقم 04-18
30	أولاً: الجرائم الماسة بسرية الاتصالات الإلكترونية
30	ثانياً: الجرائم الماسة بسلامة الاتصالات الإلكترونية
32	الفرع الثالث: الجرائم الماسة بالتوقيع والتصديق الإلكترونيين في القانون رقم 15-
33	أولاً: جريمة إفشاء البيانات الشخصية أو إساءة استعمالها
33	ثانياً: جريمة الإخلال بسرية البيانات
33	ثالثاً: جريمة جمع البيانات الشخصية للمعني دون موافقته
34	المطلب الثالث: أحكام الشروع والاتفاق الجنائي في مجال الجريمة الإلكترونية
34	الفرع الأول: الشروع في الجريمة الإلكترونية
35	أولاً: الركن المادي للشروع في الجريمة الإلكترونية
36	ثانياً: الركن المعنوي للشروع في الجريمة الإلكترونية
37	الفرع الثاني: الاتفاق الجنائي في الجريمة الإلكترونية

37	أولاً: الركن الشرعي
38	ثانياً: الركن المادي
39	ثالثاً: الركن المعنوي
40	المبحث الثاني: الجزاءات المقررة للأفعال المكونة للجريمة الإلكترونية
41	المطلب الأول: العقوبات الأصلية المقررة للجريمة الإلكترونية
41	الفرع الأول: العقوبة الأصلية المطبقة على الشخص الطبيعي في الجريمة الإلكترونية
41	أولاً: عقوبة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفق قانون العقوبات
43	ثانياً: العقوبات المقررة للجرائم الإلكترونية في التشريعات الخاصة
48	الفرع الثاني: العقوبات الأصلية المطبقة على الشخص المعنوي في الجريمة الإلكترونية
49	المطلب الثاني: العقوبات التكميلية المقررة للجريمة الإلكترونية
49	الفرع الأول: العقوبات التكميلية المشتركة
49	أولاً: المصادرة
50	ثانياً: إغلاق المواقع الإلكترونية أو المحلات
51	ثالثاً: المنع من ممارسة نشاط مهني أو اجتماعي
51	رابعاً: نشر أو تعليق حكم الإدانة
51	الفرع الثاني: العقوبات التكميلية الخاصة بالشخص المعنوي
51	أولاً: حل المؤسسة أو غلقها
51	ثانياً: الوضع تحت الحراسة القضائية
52	المطلب الثالث: عقوبة الشروع والاتفاق الجنائي في الجريمة الإلكترونية
52	الفرع الأول: عقوبة الشروع في الجريمة الإلكترونية
52	الفرع الثاني: عقوبة الاتفاق الجنائي في الجريمة الإلكترونية
53	الفصل الثاني: الآليات الإجرائية والمؤسسية لمكافحة الجريمة الإلكترونية
54	المبحث الأول: الآليات الإجرائية لمكافحة الجريمة الإلكترونية
54	المطلب الأول: آليات التحقيق الجنائي في مكافحة الجريمة الإلكترونية
55	الفرع الأول: آليات التحقيق الجنائي التقليدية في مكافحة الجريمة الإلكترونية
55	أولاً: المعاينة في الجريمة الإلكترونية
59	ثانياً: التفتيش والضبط في مجال الجريمة الإلكترونية

66	الفرع الثاني: آليات التحقيق الجنائي المستحدثة في مكافحة الجريمة الإلكترونية
67	أولاً: التسرب الإلكتروني
69	ثانياً: اعتراض المراسلات والمراقبة الإلكترونية
71	ثالثاً: الكشف عن الجريمة الإلكترونية عن طريق المعطيات
74	المطلب الثاني: الدليل الإلكتروني كآلية مستحدثة في إثبات الجريمة الإلكترونية
74	الفرع الأول: مفهوم الدليل الإلكتروني
74	أولاً: تعريف الدليل الرقمي
80	ثانياً: أقسام الدليل الإلكتروني
81	الفرع الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي للجريمة الإلكترونية
84	المبحث الثاني: الآليات المؤسسية لمكافحة الجريمة الإلكترونية
84	المطلب الأول: الهيئات الوقائية والقضائية في مكافحة الجرائم الإلكترونية
85	الفرع الأول: الهيئة الوطنية للوقاية ومكافحة الجرائم الإلكترونية
86	أولاً: تشكيلة الهيئة الوطنية للوقاية ومكافحة الجرائم الإلكترونية
87	ثانياً: مهام الهيئة الوطنية للوقاية ومكافحة الجرائم الإلكترونية
88	الفرع الثاني: القطب الجزائي لمكافحة الجرائم الإلكترونية
88	أولاً: الهيكل التنظيمي للقطب الجزائي لمكافحة الجرائم الإلكترونية
91	ثانياً: اختصاصات القطب الجزائي لمكافحة الجرائم الإلكترونية
95	المطلب الثاني: الهيئات التقنية والأمنية المختصة في كشف الجريمة الإلكترونية
95	الفرع الأول: المعهد الوطني للأدلة الجنائية وعلم الإجرام
96	أولاً: الهيكل التنظيمي للمعهد الوطني في تحليل الأدلة الرقمية
99	ثانياً: مهام المعهد الوطني في التحقيقات الجنائية المعلوماتية
100	الفرع الثاني: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني
101	الفرع الثالث: المصلحة المركزية لمكافحة الجرائم السيبرانية
103	الخاتمة
108	قائمة المصادر والمراجع
117	فهرس المحتويات

ملخص المذكرة

ملخص المذكرة باللغة العربية:

أدى التطور المتسارع لتكنولوجيات الإعلام والاتصال وما صاحبه من انتشار واسع لاستعمال الوسائط الرقمية وتطبيقات الذكاء الاصطناعي إلى بروز أنماط إجرامية حديثة عُرفت بالجريمة الإلكترونية، والتي أصبحت تشكل تهديدا حقيقيا للأفراد والمؤسسات، بالنظر إلى ما تتميز به من طابع تقني وصعوبة في الاكتشاف والإثبات. وأمام تنامي هذا النوع من الجرائم، سعى المشرع الجزائري إلى وضع منظومة قانونية خاصة تهدف إلى مجابقتها، من خلال سن قواعد موضوعية تتعلق بتجريم الأفعال الماسة بالأنظمة المعلوماتية والمعطيات الإلكترونية، إلى جانب استحداث آليات إجرائية ومؤسسية تتلاءم مع خصوصية هذا النوع من الإجرام.

وقد تناولت هذه الدراسة مختلف الآليات القانونية التي اعتمدها المشرع الجزائري لمكافحة الجريمة الإلكترونية، سواء من خلال دراسة الأحكام الموضوعية المتعلقة بالتجريم والعقاب، أو من خلال التطرق إلى الآليات الإجرائية المرتبطة بالتحري والتحقق والإثبات، إضافة إلى إبراز دور الهيئات الأمنية والقضائية والتقنية المختصة في مكافحة هذا النوع من الجرائم. وقد خلصت الدراسة إلى أن المشرع الجزائري بذل جهودا معتبرة في سبيل تدعيم المنظومة القانونية الخاصة بمكافحة الجريمة الإلكترونية، غير أن التطور المستمر لوسائل الإجرام الإلكتروني يفرض ضرورة مواصلة تحديث التشريعات الوطنية وتعزيز التكوين والتنسيق والتعاون بين مختلف الجهات المختصة لضمان فعالية أكبر في مواجهة الجرائم الإلكترونية.

الكلمات المفتاحية: الجريمة الإلكترونية، الدليل الإلكتروني، الأنظمة المعلوماتية، التحقيق الإلكتروني، مكافحة الجريمة الإلكترونية.

Abstract of the thesis:

The rapid development of information and communication technologies, along with the widespread use of digital media and artificial intelligence applications, has led to the emergence of new forms of crime known as cybercrime. This type of crime poses a real threat to individuals and institutions due to its technical nature and the difficulties in detecting and proving it. In response to the growing spread of cybercrime, the Algerian legislator has sought to establish a specific legal framework to combat it by adopting substantive legal rules criminalizing acts targeting information systems and electronic data, as well as procedural and institutional mechanisms tailored to the particular nature of such crimes.

This study examines the legal mechanisms adopted by the Algerian legislator to combat cybercrime, analyzing substantive provisions on criminalization and punishment, as well as procedural mechanisms for investigation, inquiry, and evidence. The study also highlights the role of the competent security, judicial, and technical authorities in combating cybercrime. It concludes that the Algerian legislator has made considerable efforts to strengthen the legal framework governing cybercrime; however, the continuous evolution of cybercriminal methods requires ongoing modernization of national legislation, as well as enhanced training, coordination, and cooperation among the competent authorities to ensure greater effectiveness in combating cybercrime.

Keywords: Cybercrime, Electronic Evidence, Information Systems, Electronic Investigation, Combating Cybercrime.

وفي ختام هذا العمل، نقر بأن الكمال غاية لا تدرك، وأن كل جهد بشري يظل عرضة للنقص، كما قيل: "لا يكتب إنسان في يومه إلا قال في غده لو غير هذا لكان أحسن، ولو نريد هذا لكان يستحسن، ولو قدم هذا لكان أفضل، ولو ترك هذا لكان أجمل، وهذا من أعظم العبر، ودليل على استيلاء النقص على البشر".

والحمد لله رب العالمين
