

إجراءات البحث والتحري في الجريمة المعلوماتية في القانون الجزائري.

مذكرة مكملّة لنيل شهادة الماستر في شعبة: حقوق.
تخصص: قانون جنائي وعلوم جنائية.

إشراف الأستاذة:
عبدلي حبيبة.

إعداد الطالب:
بوهلال فاتح.

أعضاء لجنة المناقشة

الاسم واللقب	الرتبة	الصفة
د. بوخيرة حسين	أستاذة محاضر (أ)	رئيساً.
د. عبدلي حبيبة	أستاذ تعليم عالي	مشرفاً ومقراً.
د. العالية نوال	أستاذ محاضر (أ)	مناقشاً وممتحناً.

إهداء

إلى من لا يكن للكلمات أن توفي
حقها، الوالدين الكريمين إلى من لا
أستطيع الاستغناء عنهم، وإلى كل
الأهل، والأقارب وجميع الأصدقاء
والزملاء.

شكر وعرفان

اشكر اولا وأخيرا الله تعالى الذي أسبغ علينا نعمه ، ضاهرة وباطنة ، وأمدني بالصبر لتذلل الصعوبات امامي وأعانني كل العون على انجاز هذه المذكرة ، ثم اشكر استاذتي الكريمة عبدلي حبيبة التي قبلت الإشراف على مذكرتي وساعدتني في كل خطوة لبلوغ نهاية البحث.

أشكر أيضا كل من ساهم وبذل جهدا ولو بضئيل في انجاز ومراجعة هذه المذكرة ، كما اشكر الأساتذة الكرام أعضاء لجنة المناقشة لتفضلهم بقبول المناقشة .

المقدمة

شهد العالم تحولاً جذرياً في العقود الأخيرة، مدفوعاً بثورة تكنولوجية أعادت تشكيل كل جانب من جوانب الحياة البشرية. ففيما يمكن وصفه بـ "قرية صغيرة" من المجتمعات المترابطة، يتواصل الأفراد ويتعلمون ويعملون ويتفاعلون اجتماعياً عبر شبكة من الشبكات الرقمية تتجاوز الحدود الجغرافية. وقد أصبح التقدم في أجهزة الحاسوب وملحقاتها والبرمجيات أساسياً ليس فقط للعمليات الحكومية ومؤسسات الأعمال، بل أيضاً للأنشطة الشخصية اليومية. وقد عزز هذا التكامل التكنولوجي راحة وكفاءة غير مسبوقتين، ولكنه أثار أيضاً مخاوف عميقة بشأن الدور المستقبلي للجهد البشري في عالم تحكمه الآلات. تقيس العديد من الدول تقدمها وقدرتها التنافسية بناءً على إتقانها للأدوات والابتكارات التكنولوجية الحديثة. من استكشاف الفضاء إلى الرعاية الصحية، ومن التعليم إلى الزراعة، أصبحت البراعة التكنولوجية مؤشراً رئيسياً للتنمية الوطنية. ومع ذلك، فإن هذه النعمة التكنولوجية سلاح ذو حدين. فبينما تُمكن المجتمعات، فإنها تفتح أيضاً أبواباً لإساءة الاستخدام والاستغلال. وقد برزت الجرائم الإلكترونية، على وجه الخصوص، كتهديد خطير، قادر على عبور الحدود بسهولة، مما يجعل المفاهيم التقليدية للاختصاص القضائي بالية. يستغل المجرمون شبكات المعلومات المتطورة، وأدوات القرصنة، والمنصات الرقمية لتنفيذ أنشطة غير مشروعة تتراوح من السرقة المالية إلى التجسس. مع ذلك، يمكن لهذه الجرائم غير المباشرة، التي غالباً ما تكون غير عنيفة بطبيعتها، أن تقوض الاستقرار الاجتماعي وتضعف ثقة الجمهور بالمؤسسات. تُهدد الهجمات الإلكترونية على الأنظمة المصرفية، وسرقة الهوية، ونشر المعلومات الكاذبة، واختراقات البيانات غير القانونية، نسيج المجتمعات الحديثة. وإدراكاً لهذه المخاطر، بدأت دول العالم بتطبيق تدابير تشريعية تهدف إلى مكافحة الجرائم الإلكترونية. فعلى سبيل المثال، سنتت الجزائر قوانين شاملة تُحدد عقوبات واضحة لمختلف الجرائم الإلكترونية، وتُرسي أطراً قانونية لمقاضاة الجناة بفعالية. وقد عمل الخبراء القانونيون وصانعو السياسات في الجزائر بجد لتفسير

القوانين القائمة وتكييفها مع العصر الرقمي، بما يضمن تحقيق العدالة في الفضاء الإلكتروني. وقد أكدوا على أهمية التعاون الدولي، نظرًا لطبيعة التهديدات الإلكترونية العابرة للحدود. وتهدف هذه الجهود إلى حماية المواطنين، وتأمين البنية الأساسية الرقمية، وتعزيز الاستخدام المسؤول للتكنولوجيا، وتحقيق التوازن بين فوائد الابتكار والحاجة إلى الأمن والنظام في عالم مترابط بشكل متزايد.

أهمية الدراسة:

إن أهمية الدراسة تظهر من خلال:

أولاً: الأهمية العلمية:

موضوع البحث يعالج موضوعاً حساساً يتعلق بالمسؤولية الجنائية لمرتكب الجرائم المعلوماتية، والذي أدى تقشيها لأحداث خطيرة، مما يهدد مستعملي الأنترنت.

ثانياً: الأهمية العملية:

تسليط الضوء على مدى نجاعة القوانين الوطنية في مجال الجريمة المعلوماتية لحماية مستخدمي الإنترنت وإبراز واقع تفعيل القانون المستحدث لمحاربة الجريمة المعلوماتية.

أهداف الدراسة:

تهدف الدراسة إلى:

- التعرف على الجريمة المعلوماتية.
- دراسة أركان الجريمة المعلوماتية في التشريع الجزائري ومدى اختلافها مع أركان الجريمة التقليدية.
- التعرف على الهيئات المختصة لمكافحة الجريمة المعلوماتية وإجراءات التحقيق للكشف عن الجريمة المعلوماتية.

أسباب اختيار الموضوع:

أولاً: دوافع شخصية

- اهتمامي الخاص بكل ما يتعلق بالتكنولوجيا والفضاء الرقمي، ما جعلني أستشعر خطورة الجرائم المعلوماتية وتأثيرها المباشر على الأفراد والمجتمعات.
- التحدي العلمي الذي يطرحه الموضوع، من خلال الحاجة إلى الربط بين الإطار النظري والتحليل الواقعي، وهو ما أراه فرصة لتطوير قدراتي البحثية.

ثانياً: دوافع موضوعية

- الانتشار الواسع لما يُعرف بالجرائم المعلوماتية، واعتبارها خطراً عالمياً يمس مختلف المجالات، خصوصاً الاقتصادية والأمنية.
- غياب الأجهزة المتخصصة أو قصور بعض الدول في مكافحة هذا النوع من الجرائم بشكل فعال، ما يستوجب دراسة معمّقة لآليات التحقيق والملاحقة.

- قلة الدراسات الأكاديمية المتخصصة التي تناولت الجريمة المعلوماتية بشكل دقيق، حيث تُعامل غالبًا بطريقة سطحية وتُدرج ضمن الجرائم التقليدية.
- الحاجة الملحة إلى تأصيل نظري واضح للجريمة المعلوماتية، وتقديم شرح مفصل لكل من الدارسين والممارسين في الميدان القانوني.
- التطور السريع للأنظمة الرقمية مقابل بطء التحديث التشريعي، ما يزيد من أهمية معالجة الموضوع من منظور قانوني حديث ومتجدد.

الإشكالية

مع التقدم السريع للتكنولوجيا وتزايد عدد المستخدمين حول العالم، ظهرت أشكال جديدة من الجرائم الإلكترونية، مُشكلةً تهديدات جسيمة للأفراد والمؤسسات على حد سواء. تتراوح هذه الأنشطة الخبيثة بين اختراق البيانات وسرقة الهوية، وصولاً إلى عمليات الاحتيال المالي وهجمات برامج الفدية، مُسببةً أضراراً وخسائر مالية واسعة النطاق. ونتيجةً لذلك، استجابت الحكومات والهيئات التنظيمية بتحديث القوانين وتطبيق لوائح أكثر صرامة لفهم هذه التهديدات المُتطورة ومنعها ومكافحتها بشكل أفضل. وتُعدّ الجهود المُستمرة ضرورية لحماية البيئات الرقمية، وضمان سلامة المستخدمين، والحفاظ على الثقة في عالمنا المُتصل بشكل متزايد. وبناءً على كل ذلك نطرح إشكالية الدراسة المحورية:

ماهي الإجراءات اللازمة لمكافحة الجريمة وكشف اللبس فيها؟

منهج الدراسة:

إن البحث في الموضوع محل الدراسة يتطلب الاعتماد على المنهج الوصفي التحليلي و الذي يسمح ببيان مختلف الأحكام والنصوص القانونية وإجراء مقارنة بين المفاهيم من خلال القيام بتحليل قانوني للمواد والأحكام المتعلقة بهذا الموضوع.

خطة الدراسة

للإجابة على الإشكالية الرئيسية للموضوع، مع ما ينبثق عنها من إشكالات فرعية، قمنا بتقسيم الدراسة إلى: مقدمة، وفصلين، وخاتمة.

خصصنا **الفصل الأول** لدراسة كل ما يتعلق بالجريمة المعلوماتية من خلال مبحثين، بينا تناولنا في المبحث الأول ماهية الجريمة المعلوماتية، تعريف، أنواع، الطبيعة القانونية، كما درسنا في المبحث الثاني الحماية الجنائية من خلال النصوص القانونية. أما **الفصل الثاني** تطرقنا فيه آليات وإجراءات التحري في مجال الجريمة المعلوماتية وذلك في مبحثين، المبحث الأول الوحدات المختصة في مكافحة الجريمة المعلوماتية، والمبحث الثاني إجراءات التحري للكشف عن الجريمة المعلوماتية.

الفصل الأول

الفصل الأول: الإطار المفاهيمي للجريمة المعلوماتية

تُعد الجريمة المعلوماتية من أبرز وأخطر التحديات التي أفرزها التطور التكنولوجي الهائل في العصر الحديث. فقد أصبحت هذه الجريمة تشكل تهديدًا حقيقيًا للأفراد، والمؤسسات، والدول على حد سواء، نظرًا لقدرتها الفائقة على تجاوز الحدود الجغرافية، والانتشار بسرعة مذهلة في فضاء الإنترنت الواسع. ولم تعد هذه الجرائم مقتصرة على مجرد أفعال فردية محدودة، بل تحوّلت إلى شبكات معقدة وعابرة للحدود، توظف تقنيات متطورة لأغراض غير مشروعة تمس الأمن القومي والاقتصادي والاجتماعي.

ومن هنا، فإن معالجة هذا النوع من الجرائم يتطلب أولاً فهمًا دقيقًا لطبيعتها، ومعرفة شاملة بخلفياتها التقنية والقانونية، قبل الخوض في إشكاليات المسؤولية الجنائية المترتبة عنها. إذ لا يمكن الإحاطة بأبعاد هذه الجريمة دون التطرق إلى مفهومها العام، والتمييز بينها وبين باقي الجرائم التقليدية، فضلاً عن تحديد أنواعها، والأهداف التي يسعى مرتكبوها إلى تحقيقها من خلال استغلال التكنولوجيا.

إنّ التحول الرقمي الذي يشهده العالم لم يصحبه تطور تشريعي كافٍ يواكب هذه المستجدات المتسارعة، ومن هذا المنطلق، يستوجب علينا في المرحلة الأولى من البحث تسليط الضوء على الإطار النظري للجريمة المعلوماتية، من خلال تعريفها، وتحليل أنواعها ودوافعها وأهدافها (المبحث الأول).

ثم ننتقل إلى القوانين المتعلقة بالمسؤولية الجنائية في هذا السياق، وبذلك، يحاول هذا العمل الجمع بين التأسيس النظري والمعالجة القانونية العملية لموضوع يعدّ من أهم القضايا الراهنة في مجال القانون الجنائي المعاصر (المطلب الثاني).

المبحث الأول: ماهية الجريمة المعلوماتية

تكتسي الجريمة المعلوماتية أهمية متزايدة في العصر الرقمي نتيجة الاعتماد الكبير على وسائل التكنولوجيا الحديثة في مختلف مجالات الحياة، سواء على الصعيد الفردي أو المؤسسي أو الحكومي. من هذا المنطلق، يُعدُّ فهم هذا النوع من الجرائم ضرورة ملحة تفرضها التطورات المتسارعة في مجال تكنولوجيا المعلومات والاتصال. وتبعاً لذلك سيتطرق إلى السياق المعرفي للجريمة المعلوماتية "لتحليل شامل لمفهوم الجريمة المعلوماتية (المطلب الأول) ثم إلى أركان الجريمة المعلوماتية (المطلب الثاني)، ثم إلى أنواع الجريمة المعلوماتية (الفرع الثالث).

المطلب الأول: السياق المعرفي للجريمة المعلوماتية

لقد تنوعت التعريفات المتعلقة بالجريمة المعلوماتية، وتفاوتت من حيث الشمول والدقة، حيث اتسم بعضها بالضيق في المفهوم بينما اتجه البعض الآخر نحو توسيع النطاق بشكل كبير. هذا التباين أدى إلى غياب تعريف موحد أو فهم مشترك يضبط هذه الظاهرة المعقدة. فبين من يركز على الجانب التقني، ومن يراها جريمة تقليدية بأسلوب حديث، ظل الإطار المفاهيمي غير مستقر. ويترتب على هذا الغموض صعوبات عدة في ضبط الجريمة تشريعياً وعملياً. كما يعرقل ذلك صياغة حلول فعّالة لمواجهتها. إذ لا يمكن مقاومة ما لا يُفهم بشكل واضح. من هنا، تظهر ضرورة التوافق على تعريف جامع مانع لتسهيل مكافحتها. سنتطرق إلى تعريف الجريمة المعلوماتية (الفرع الأول)، وإلى خصائص الجريمة المعلوماتية (الفرع الثاني).

الفرع الأول: تعريف الجريمة المعلوماتية

أولاً: التعريف الفقهي

يقدم الفقهاء والعلماء تعريفات متنوعة للجرائم الإلكترونية، يعكس كل منها وجهات نظر وسياقات مختلفة. يصف البروفيسور روزنبالت الجريمة الإلكترونية بأنها أنشطة غير قانونية تتضمن نسخ المعلومات المخزنة داخل أنظمة الحاسوب، أو تعديلها، أو حذفها، أو الوصول غير المصرح به إليها. ويسلط تعريفه الضوء على الجوانب التقنية والتلاعب بالبيانات الرقمية.

من ناحية أخرى، يُعرّف سولا روز الجريمة الإلكترونية تعريفاً أوسع بأنها أي جريمة منصوص عليها في قانون العقوبات تتعلق بتكنولوجيا المعلومات، مع التركيز على التصنيف القانوني لهذه الجرائم. يؤكد هذا المنظور على أهمية التكنولوجيا في الأنشطة الإجرامية الحديثة. وبشكل عام، وعلى الرغم من اختلاف الصياغة، تُقر هذه التعريفات بالجرائم الإلكترونية باعتبارها أفعالاً غير قانونية تتعلق بالمعلومات الرقمية، وغالباً ما يُسهلها استخدام أجهزة الحاسوب والتكنولوجيا ذات الصلة، مما يعكس الطبيعة المتطورة للجريمة في العصر الرقمي.

تركز بعض التعريفات على الأساليب المستخدمة، وخاصة استخدام أجهزة الحاسوب والأجهزة الرقمية كأدوات أو وسائل لارتكاب الجرائم، منها:

تعريف الأستاذ جون فور ستر " فعل إجرامي يستخدم الحاسوب في ارتكابه كأداة رئيسية ويعرفها تادمان بأنها كل أشكال السلوك غير المشروع الذي يرتكب بواسطة الحاسب¹.

ونشير أيضا إلى أن جانبا من الفقه والمؤسسات ذات العلاقة بهذا الموضوع وضعت عددا من التعريفات التي تقوم على أساس سمات شخصية لدى مرتكب الفعل تعرف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 حيث عرفت الجريمة المعلوماتية أي جريمة لفاعلها معرفة فنية بالحاسبات تمكن من ارتكابها. كما عرفها الأستاذ دافيد تومسن أي جريمة يكون متطلبا لاقتوافها أن تتوافر لدى فاعلها المعرفة بتقنية الحاسب الآلي².

ثانيا: التعريف القانوني

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02-الفقرة - أ من القانون رقم المؤرخ في 04-09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها³ بالقول بأن "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية، فإنه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب المتعلقة بالجريمة هذه فنعرفها بأنها " كل السلوكيات المجرمة التي يشكل الحاسوب وشبكات

¹ هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992. ص 120.

² هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة، 2000، ص 20.

³ المادة 02-الفقرة - أ من القانون رقم المؤرخ في 04-09 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

الاتصال الخاصة به وسيلة لارتكابها أو محلاً لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الإلكترونية".

الفرع الثاني: خصائص الجريمة المعلوماتية

تختلف الجريمة المعلوماتية عن الجريمة التقليدية في جوانب متعددة، تجعل منها ظاهرة إجرامية ذات طابع خاص. ويبرز هذا الاختلاف في السمات العامة التي تميزها، مثل الطابع غير المادي وارتباطها الوثيق بالتكنولوجيا. كما يختلف الدافع وراء ارتكابها، إذ غالباً ما يكون مرتبطاً بالتحايل على الأنظمة أو السعي لتحقيق مكاسب رقمية أو معلوماتية. إضافة إلى ذلك، فإن طريقة تنفيذ الجريمة المعلوماتية تتم بوسائل إلكترونية معقدة يصعب تتبعها، مما يجعل اكتشافها والتحقيق فيها أكثر تعقيداً مقارنة بالجرائم التقليدية. ومن أهم خصائصها:

أولاً: صعوبة اكتشاف الجريمة المعلوماتية

غالباً ما تظل الجرائم المتعلقة بالإنترنت خفية وتمر دون أن يُلاحظها مرتكبوها، إذ يستخدمون أساليب متطورة لتنفيذ أنشطتهم غير المشروعة. يلجأ هؤلاء المجرمون إلى القرصنة لاختراق أنظمة الأمن، وسرقة الأموال أو البيانات الحساسة، والتجسس لجمع معلومات سرية، ونشر فيروسات خبيثة لتعطيل الأنظمة أو إتلافها. هذه التقنيات المتطورة تُصعب الكشف عنها، مما يسمح لهذه الجرائم بالاستمرار دون أن يُلاحظها أحد لفترات طويلة¹.

غالباً ما يكون تنفيذ مثل هذه الإجراءات معقداً للغاية ويتطلب تحديات تقنية، وغالباً ما يُخفى عن الأنظار خوفاً من فقدان عملائهم أو مواجهة الانتقام. هذا التعقيد، بالإضافة إلى القدرة على محو

1 محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، ص32.

الأدلة أو إتلافها بسرعة، يجعل الكشف عنها والإبلاغ عنها أمرًا بالغ الصعوبة. ونتيجةً لذلك، تظل هذه الممارسات سرية، مما يُعقّد جهود كشف الحقيقة ومحاسبة الجناة في القطاعات المتضررة¹.

ثانياً: صعوبة إثبات الجريمة المعلوماتية

تعمل الجرائم الإلكترونية في عالم رقمي يتجاوز حدود الفضاء المادي، مما يزيد من صعوبة كشفها وملاحقة مرتكبيها. يعتمد هذا النوع من النشاط الإجرامي بشكل كبير على التكنولوجيا المتقدمة، مما يتطلب من المحققين استخدام تقنيات وأدوات متخصصة غالباً ما تكون خارج نطاق تدابير الأمن القياسية. حالياً، تقتصر العديد من وكالات إنفاذ القانون والأنظمة القضائية إلى الخبرة التكنولوجية اللازمة للتصدي بفعالية لهذه التهديدات المعقدة. بالإضافة إلى ذلك، فإن الأطر القانونية التقليدية غير مجهزة لمواكبة التطور السريع للتهديدات الإلكترونية، مما يترك فجوات في التنفيذ والملاحقة القضائية. لذلك، هناك حاجة ملحة لتطوير المعرفة المتخصصة، وقوانين محدثة، واستراتيجيات تكيفية لمكافحة المشهد المتغير باستمرار للجرائم الإلكترونية بفعالية وضمان تحقيق العدالة في العصر الرقمي².

ثالثاً: أسلوب ارتكاب الجريمة المعلوماتية

الجرائم المعلوماتية تبرز بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها، فإذا كانت الجريمة التقليدية تتطلب نوعاً من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر كما هو الحال في جريمة السرقة³، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت مع وجود مجرم يوظف

1 نهال عبد القادر المومني، الجرائم المعلوماتية، ط2 ، دار الثقافة للنشر والتوزيع، ص56.

2 - محمد عبيد الكعبي، مرجع سابق، ص40.

3 نهال عبد القادر المومني، مرجع سابق، ص57-58.

خبرته التوجه النظري والإطار المنهجي للدراسة أو اختراق خصوصيات الغير للتغريب وقدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس بالقاصرين كل ذلك دون الحاجة لسفك الدماء).

رابعاً: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص

عادةً ما تتضمن الجرائم الإلكترونية جهوداً تعاونية بين عدة أفراد. غالباً ما يتولى متخصص تقني الجوانب التقنية، مثل الاختراق أو تثبيت البرامج الضارة، بينما يساعد آخرون من بيئة الضحية في إخفاء آثار الاختراق. ويعملون معاً على إخفاء عمليات التلاعب، وتنفيذ النشاط الإجرامي، وضمان نقل البيانات أو الأموال المسروقة بأمان. هذا العمل الجماعي المنسق يجعل عمليات المجرمين الإلكترونيين أكثر تعقيداً ويصعب اكتشافها¹.

خامساً: خصوصية مجرمي المعلوماتية

غالباً ما يكون مجرمو الإنترنت ماهرين في التكنولوجيا أو يمتلكون على الأقل معرفة أساسية بالحاسوب والإنترنت، مما يميزهم عن المجرمين التقليديين. تُمكنهم خبرتهم التقنية من تنفيذ جرائم مثل القرصنة وسرقة الهوية واختراق البيانات بفعالية أكبر. يميل هؤلاء المجرمون إلى العمل في المجال الرقمي، مستغلين ثغرات أنظمة الحاسوب والشبكات. وتتميز جرائمهم بشكل رئيسي باعتمادهم على الأدوات والمهارات الرقمية، مما يجعلهم أكثر مرونة وصعوبة في الكشف عنهم مقارنةً بالمجرمين التقليديين. ويستمر مجرمو الإنترنت في التطور، مما يُشكل تحديات كبيرة لأجهزة إنفاذ القانون حول العالم².

1 محمد عبيد الكعبي، المرجع السابق، ص42.

2 نهال عبد القادر المومني، مرجع سابق، ص57-58.

سادسا: الجريمة المعلوماتية جريمة عابرة للحدود

بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدرة التي تتمتع بها الحواسيب وشبكتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

الفرع الثالث: أنواع الجريمة المعلوماتية

تُعد الجرائم المعلوماتية من الجرائم الحديثة والمتعددة الأشكال، حيث تختلف حسب طبيعة الهدف الذي تستهدفه والأسلوب المستخدم في ارتكابها. هذا التنوع ناتج عن البيئة الرقمية المرنة التي تتيح للمجرمين استهداف الأفراد، الأنظمة، أو الممتلكات بطرق يصعب كشفها. من هنا، أصبح من الضروري تصنيف هذه الجرائم لتسهيل دراستها وفهمها قانونيًا وعمليًا. فبعضها يمس الحقوق الفردية كالحياة الخاصة والشرف، بينما يركّز البعض الآخر على الإخلال بالأمن العام أو استغلال الأنظمة. يساعد هذا التصنيف في تطوير وسائل الوقاية والمواجهة. وفي هذا الفرع، سيتم عرض أبرز أنواع الجرائم المعلوماتية وتحليل خصائصها وتحدياتها. ومنه تنقسم أنواع الجريمة المعلوماتية الى:

أولاً: الجرائم التي تقع على الأشخاص: تُعرّض هذه الجرائم الحقوق الشخصية الأساسية، وهي حقوق جوهريّة لكل فرد، للخطر، بما في ذلك الحق في الحياة، والسلامة الجسدية والحرية والشرف. هذه الحقوق جوهريّة لكرامة الإنسان، ولا يمكن اختزالها في مجرد مصالح أو ممتلكات اقتصادية. إن حماية هذه

الحقوق الأساسية تضمن احترام الأفراد وسلامتهم، وتحافظ على النسيج الأخلاقي والاجتماعي لمجتمعنا، وتعلي من شأن قيمة الإنسان.

1. الجريمة انتحال الشخصية: يستخدم المجرمون اليوم منصات الإنترنت لسرقة المعلومات

الشخصية، مثل العناوين وأرقام الضمان الاجتماعي والبيانات المصرفية. وغالبًا ما يستغلون الإعلانات المزيفة أو رسائل البريد الإلكتروني المزيفة لخداع الأفراد ودفعهم للكشف عن بيانات حساسة. وبمجرد حصولهم على هذه المعلومات، ينتحلون شخصية ضحاياهم لتنفيذ أشكال مختلفة من الاحتيال، بما في ذلك عمليات شراء غير مصرح بها ببطاقات الائتمان، وعمليات احتيال مالي، وحتى سرقة الهوية. ومع تطور التكنولوجيا، تتطور أساليب انتحال الشخصية، مما يجعل من الضروري على الناس توخي الحذر وحماية بياناتهم الشخصية على الإنترنت¹.

2. جريمة المضايقة والملاحقة: هي جريمة حديثة شائعة بشكل متزايد، وتتميز بالتهديد والترهيب

والمضايقة عبر منصات التواصل الاجتماعي. يمكن أن يُسبب هذا النوع من الإساءة ضررًا نفسيًا بالغًا، حتى دون أي اتصال جسدي، مما يُسبب للضحايا القلق والخوف والضييق النفسي. غالبًا ما يُقارن القضاة المطاردة الإلكترونية بالتهديدات التقليدية في الواقع، مُشددين على خطورتها. ومع استمرار انتشارها، يزداد الوعي بآثارها الضارة على الصحة النفسية أهمية. تتطلب معالجة هذه المشكلة اتخاذ تدابير قانونية أقوى وأنظمة دعم أقوى لحماية الضحايا ومنع المزيد من الأذى².

¹ منير محمد الجنبهي ممدوح محمد الجنبهي، جرائم الأنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص 42-43

² محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004، ص 45.

3. **جرائم التغيرير والاستدراج:** هي من أشهر جرائم الانترنت ومن أكثرها انتشارا خاصة بين أواسط صغار السن ومن مستخدمي الشبكة، وهي تقوم على عنصر الإمام حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين علاقة صداقة أو زواج على الانترنت والجريمة المعلوماتية التي قد تتطور إلى لقاء مادي بين الطرفين، وهذه الجرائم لا تعرف الحدود ولا يمكن حصرها، وهي دون حدود سياسية أو اجتماعية اذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها أي مستخدم حسن النية¹.

4. **جرائم التشهير وتشويه السمعة:** مع انتشار الشائعات والأخبار الكاذبة التي تطول وتمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية أو حتى دينية، وقد ظهرت على شبكة الانترنت بعض المواقع والتي جندت نفسها لهدف واحد هو خدمة تلك الشائعات والأخبار الكاذبة وذلك بهدف تشهير وتشويه سمعة تلك الرموز، وكذلك لتسميم أفكار الناس أو محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم. وأبرز وسائل ارتكاب هذه الجريمة إنشاء مواقع على الشبكة تحتوي المعلومات المطلوب إدراجها ونشرها أو إرسالها عبر المواقع الالكترونية، ومن أمثلتها إرسال الصور غير اللائقة أو معلومات غير صحيحة².

5. **الجرائم المخلة بالأخلاق والآداب العامة:** الإنترنت عالم واسع، حيث يمكن للجميع مشاهدة ما يريدون. لكن بعض الأمور المقبولة في بلد ما قد تكون مخالفة للقواعد في بلد آخر. على سبيل المثال، يُعدّ تحريض الأطفال على القيام بأشياء سيئة، أو غير قانونية، أو مشاركة صور أو

¹ عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة د. الطاهر مولاي، سعيدة، سنة 2016/2015، ص19.

² منير محمد الحنيهي، ممدوح محمد الجنيهي، المرجع السابق، ص34.

مقاطع فيديو غير مسموح بها، أو التحدث معهم بطريقة مسيئة على الإنترنت أمرًا غير قانوني. مشاهدة أو مشاركة صور ومقاطع فيديو للبالغين، تُعرف باسم المواد الإباحية، أمر شائع جدًا على الإنترنت، وخاصة في بعض أنحاء العالم. قد تكون هذه الأشياء السيئة في صور أو مقاطع فيديو أو محادثات أو رسائل، ولأن الإنترنت متاح للجميع، فقد يكون من الصعب منع انتشارها¹.

ثانياً: الجرائم التي تقع على الأموال: هي جرائم الاعتداء على الأموال والتي تهدد الحقوق ذات القيمة المالية ويدخل في نطاق هاته الحقوق الحق ذو قيمة اقتصادية.

فإذا كان موضوع الاعتداء على الأموال في نطاق ما ينصب على الحاسب الآلي ذاته وما يرتبط به أسلاك وما يتصل به من ملحقات فإنه هنا لا يثير أي صعوبة في تطبيق النصوص الجزائية التقليدية كون الأمر يتعلق بمال عادي منقول، أما إذا وقع الاعتداء على ما يتعلق بفن الحاسب الآلي من برمجيات ونظم فإن النصوص التشريعية التقليدية قاصرة عن حمايتها لما لهذا المجال من طابع خاص غير تقليدي².

1. جرائم صناعة ونشر الفيروسات: يشبه الفيروس الموجود على جهاز الكمبيوتر برنامجًا صغيرًا مُسببًا للمشاكل. يمكنه التسلل إلى جهاز الكمبيوتر والتسبب في مشاكل. في بعض الأحيان، ينسخ نفسه ويحاول السيطرة على برامج أخرى، أو قد يحذفها فيوقف جهاز الكمبيوتر عن العمل بشكل صحيح. تعتمد طريقة عمله على نوع مُسبب المشاكل. يمكن أن يبدأ العمل بمجرد فتح رسالة تحتوي عليه، أو بمجرد تشغيل برنامج يحتوي على الفيروس.

1 انظر محمد امين احمد الشوابكة، المرجع أعلاه، ص 114.

2 انظر محمد امين احمد الشوابكة، المرجع السابق، ص 136.

يُعد هذا النوع من أعطال الكمبيوتر مشكلة كبيرة في جميع أنحاء العالم. الفيروسات موجودة منذ زمن طويل، حتى قبل الإنترنت، عندما تحدث عنها رجل ذكي يُدعى فون نيومان. أحد الفيروسات الشهيرة كان يُطلق عليه "فيروس رسالة الحب" أو "الدودة الحمراء"، وفي عام 2001، تسبب في توقف العديد من أجهزة الكمبيوتر - أكثر من 250,000 - عن العمل في غضون ساعات قليلة¹.

2. جرائم الاختراقات: القرصنة هي دخول شخص ما إلى جهاز كمبيوتر شخص آخر أو شبكته الإلكترونية دون إذن. يستخدم هؤلاء برامج ومهارات حاسوبية خاصة لتجاوز نظام الأمان المُصمم للحفاظ على أمان كل شيء. قد يخترق الناس أجهزة الكمبيوتر لأسباب مختلفة. يفعل البعض ذلك لمجرد الاطلاع على ما يمكنهم اكتشافه، مثل الاستكشاف. بينما يخترق آخرون لسرقة معلومات شخصية أو أشياء تخص شخصاً آخر، غالباً لبيعها أو استخدامها لاحقاً.

وقد يكون السبب تبديل أو تحريف أو تعطيل المعلومات في أجهزة الغير، وهو أخطر أنواع الاختراق، ومن أبرز ضحايا الاختراق فهي مواقع الانترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها وهذه العملية تسمى تغيير وجه الموقع².

3. جريمة تعطيل الأجهزة والشبكات: يطال تعطيل أجهزة الحاسب الآلي عبر برابحها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الإلكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة ونتم

1 منير محمد الحنبيهي ممدوح محمد الحنبيهي، المرجع السابق، ص 36.

2 منير محمد الحنبيهي ممدوح محمد الحنبيهي، المرجع أعلاه، ص 37.

عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها وهو الأمر الذي يعيقها عن تأدية عملها¹.

4. **جريمة النصب والاحتيال**²: أصبح التعاقد عبر الانترنت حاجة وضرورة نظرا لسرعة وسهولة التعامل عبرها، لكن هذه الميزة ما لبثت أن شابتها سلبيات عديدة هي عبارة عن أفعال إجرامية تعرف بالنصب والاحتيال ومن بينها:

- خرق التعاملات عبر طرق احتيال جديدة تم ابتكارها، وكذلك زادت من وقوع جرائم النصب التي لا يزال يقع فيها عدد كبير من مستخدمي الانترنت.
- إما المظهر الأبرز للاحتيال فهو سرقة معلومات البطاقات الائتمانية واستخدام هذه المعلومات لسرقة المبالغ الموجودة داخل حسابات الضحايا، ومرتكبو الجرائم عبر تلك الوسائل يسهل هروبهم وتواريهم لذلك من الصعب جدا ملاحقتهم والقبض عليهم.

المطلب الثاني: أركان للجريمة المعلوماتية

تتخذ الجريمة المرتكبة عبر الانترنت من الفضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع، والمجرم يقوم بهذا الفعل، من خلال هذا التشابه سوف نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة. قبل التطرق إلى أركان الجريمة المعلوماتية يجب معرفة خصائص هذه الجريمة المعلوماتية وهذا ما سنطرق إليه في الفرع الأول المعنون "الركن الشرعي" و في الفرع الثاني المعنون "الركن المادي" و في الفرع الثالث المعنون "الركن المعنوي".

1 منير محمد الجنيهي ممدوح محمد الجنيهي، المرجع أعلاه، ص38.

2 عبد الكريم شيباني ، مرجع سابق، ص 23.

الفرع الأول: الركن الشرعي

يُعد الركن الشرعي أحد الأسس الجوهرية في بناء الجريمة من الناحية القانونية، إذ لا جريمة ولا عقوبة دون نص قانوني يجرم الفعل بشكل صريح. وتكمن أهمية هذا الركن في ضمان احترام سيادة القانون، وتحقيق الأمن القانوني للأفراد، من خلال منع التجريم والعقاب بأثر رجعي أو وفقًا لتفسيرات موسّعة وغير دقيقة. ويتفرع عن هذا الركن العديد من القضايا التي تتصل بمشروعية الفعل المرتكب، ومدى التزام القاضي بالنصوص القانونية دون تجاوزها. وفي هذا السياق، يمكن تناول الركن الشرعي من زاويتين رئيسيتين: الأولى تتعلق بدوره في تحديد الجريمة وتحقيق العدالة، والثانية تتصل بآثار تجاهل هذا الركن على مشروعية العقوبات والنظام القانوني ككل.

أولاً: أهمية الركن الشرعي للجريمة

في مجال القانون الجنائي، يلعب الركن القانوني للجريمة دوراً أساسياً في تحديد ماهية السلوك غير القانوني. ويتطلب هذا الركن وجود قانون تجريم واضح ومحدد يُعرّف الفعل المحظور وينص على العقوبة المقابلة له لحظة وقوعه. ومن المبادئ الأساسية عدم جواز معاقبة الأفراد على أفعال ارتكبت قبل سن القانون أو بعد إلغائه، مما يؤكد على أهمية اليقين القانوني والإنصاف. لذا، يتحمل القضاة مسؤولية التفسير الدقيق للقوانين الجزائية، والامتناع عن توسيع نطاقها أو إجراء مقارنات بين الأفعال المجرمة وغير المجرمة. يضمن هذا التفسير الدقيق الحفاظ على سيادة القانون، ومنع العقوبات التعسفية

أو الظالمة، وحماية حقوق الأفراد من خلال الالتزام الدقيق بلغة القانون ومقصده كما هو قائم وقت ارتكاب الجريمة¹.

ثانياً: أثر تجاهل الركن الشرعي.

إن تجاهل مشروعية الجرائم والعقوبات يحول دون تطبيق القواعد الجنائية بأثر رجعي، مما يضمن محاسبة الأفراد فقط بموجب القوانين السارية وقت ارتكاب أفعالهم. هذا المبدأ أساسي للعدالة، إذ يحمي المواطنين من القوانين ذات الأثر الرجعي. توجد استثناءات عندما ينص القانون صراحةً على ذلك أو عند تطبيق القانون الأنسب للمتهم، مؤكداً على وجوب إثبات المسؤولية الجنائية دائماً وفقاً للمعايير القانونية السابقة المعمول بها، وذلك حفاظاً على العدالة ومنعاً للعقوبات التعسفية².

إن الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسيين:

• مطابقة الفعل لنص التجريم.

• ألا يخضع الفعل المرتكب لسبب من أسباب الإباحة.

في الإطار القانوني المعياري، يعني توافق الفعل مع القانون الجنائي توافقه مع النصوص التشريعية والأنظمة المرعية. ولا اعتبار العقوبة مبررة، من الضروري أن ينص القانون المنطبق صراحةً على العقوبة

1 أسامة احمد المناعة، جلال محمد الزغبى، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014، ص45.

2 حنان ربحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت 2014، ص57.

نفسها للفعل المرتكب. وهذا يضمن الوضوح والاتساق والإنصاف في تطبيق العدالة الجنائية، ويحافظ على سيادة القانون¹.

الفرع الثاني: الركن المادي

يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور والقانون وقد ذهب الدكتور رضا فرح إلى تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر:

- السلوك الإجرامي.
- النتيجة الإجرامية.
- العلاقة السببية بين الفعل والنتيجة.

أولاً: السلوك الإجرامي: يمكن تصنيف السلوك في الأفعال البشرية إلى فئتين: أفعال إيجابية، حيث يُنتج الأفراد عمداً نتيجة معينة، وأفعال سلبية، تتضمن تجنباً واعياً للإجراءات الضرورية. في عالم الجرائم الإلكترونية، يُلاحظ كلا النوعين بشكل بارز. غالباً ما ينخرط الجناة في أفعال إيجابية مثل اختراق الأنظمة، ونشر البرامج الضارة، أو سرقة المعلومات الحساسة. على العكس من ذلك، تتجلى الأفعال السلبية عندما يختار الأفراد أو الجماعات الامتناع عن الإجراءات، مثل عدم تطبيق تدابير أمنية أو إهمال التحديثات المناسبة، مما يخلق ثغرات أمنية. مع التقدم التكنولوجي السريع، تطورت طبيعة ونطاق الجرائم الإلكترونية بشكل كبير. تُمكن هذه الابتكارات المجرمين من ابتكار أساليب هجوم أكثر تعقيداً

¹ بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007، ص94-95.

وتطورًا ومراوغة، مما يُمثل تحديات جديدة لجهود الأمن السيبراني. غالبًا ما تكون الدفاعات التقليدية غير كافية ضد هذه التهديدات المتطورة، مما يتطلب التكيف المستمر وتحسين الاستراتيجيات لمكافحة الجرائم الإلكترونية بفعالية¹.

ثانيا: النتيجة الإجرامية: النتيجة الإجرامية هي النتيجة الملموسة لأفعال الفرد، من وجهة نظر المشرع. وهي تُبرز الأثر الملموس الذي يحدث كنتيجة مباشرة للسلوك غير القانوني، بغض النظر عن أي عوامل أو ظروف أخرى محتملة قد تؤثر على الوضع².

ثالثا: العلاقة السببية بين الفعل والنتيجة: في السياق القانوني أو التحليلي القياسي، تُشكل العلاقة السببية رابطًا أساسيًا بين الفعل ونتيجته. فهي تُثبت أن أفعال الفرد تسببت مباشرة في النتيجة، مما يجعلها أساسية لفهم المساءلة. تُعد هذه الصلة حيوية لأنها تُحدد ما إذا كان ينبغي تحميل الشخص مسؤولية النتيجة. عادةً، تمتد المسؤولية إلى حد الشروع، مما يعني أنه يُمكن تحميل الشخص المسؤولية إذا حاول ارتكاب جريمة، حتى لو لم تتحقق النتيجة المرجوة. ومع ذلك، في حالات الجرائم غير المتعمدة، مثل الحوادث، فإن إنكار العلاقة السببية يمكن أن يؤثر بشكل كبير على المسؤولية. إذا ادعى المرء أن أفعاله لم تُسبب النتيجة، فإن ذلك يُقوّض أساس تحديد اللوم أو المسؤولية، مما يؤدي غالبًا إلى التبرئة أو تقليل المسؤولية. وبالتالي، فإن إثبات علاقة سببية واضحة أمر أساسي للعدالة والإجراءات القانونية³.

1 أسامة احمد المناعة، جلال محمد الزغبى، المرجع السابق، ص51-52.

2 بلعلبات إبراهيم، المرجع السابق، ص18.

3 أسامة احمد المناعة، جلال محمد الزغبى، المرجع السابق، ص58-59.

الفرع الثالث: الركن المعنوي

في إطار الجرائم التي تستهدف الأشخاص من خلال الوسائل الإلكترونية، يُعدّ الركن المعنوي أحد الأركان الأساسية لقيام الجريمة، حيث يُعنى بإثبات نية الجاني ووعيه عند ارتكاب السلوك الإجرامي. وتزداد أهمية هذا الركن في الجرائم الإلكترونية نظرًا لطبيعتها المعقدة وتعدد وسائل ارتكابها. وفيما يلي تحليل لهذا الركن من خلال تقسيمه إلى محورين:

أولاً: أهمية الركن المعنوي في الجرائم الإلكترونية

في سياق جرائم الإنترنت، يعتمد الركن المعنوي أساسًا على نية الجاني ارتكاب أفعال غير قانونية، مثل انتحال الشخصية أو سرقة بطاقات الائتمان. لا يكفي مجرد قيام الفرد بهذه الأفعال؛ بل يجب أيضًا أن يكون لديه وعي واعٍ بالخطأ المرتكب. يجب أن تكون النتيجة الإجرامية قائمة، أي أن يدرك الفرد أن أفعاله ستسبب ضررًا أو ضررًا للآخرين. يؤكد هذا الركن المعنوي على أهمية النية والوعي في إثبات المسؤولية الأخلاقية والقانونية لمرتكبي هذه الجرائم الإلكترونية.¹

ثانيًا: صور تحقق الركن المعنوي ومظاهره

يختلف الركن المعنوي في الجرائم الإلكترونية اختلافًا كبيرًا باختلاف الظروف. على سبيل المثال، يتطلب الوصول غير المصرح به إلى أنظمة الحاسوب عادةً نيةً واضحة؛ إذ يجب أن ينخرط الجاني عن علم في نشاط غير قانوني. أما إذا تمكن شخص ما من الوصول عن طريق الخطأ أو الإهمال، ثم توقف فورًا بعد إدراكه أن أفعاله غير قانونية، فإن الوضع يختلف أخلاقيًا وقانونيًا. في مثل هذه

1 خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان 2011، ص 73-74.

الحالات، تُعتبر النية الإجرامية غائبة عمومًا، لأن الفرد لم يتعمد ارتكاب جريمة. يهدف المشرعون إلى التمييز بين سوء النية والانتهاكات العرضية، مع التركيز على وعي المتهم وأفعاله المتعمدة. يساعد هذا النهج الدقيق على ضمان محاكمة الأفراد المذنبين حقًا فقط¹.

الاحتتيال الإلكتروني فعل إجرامي متعمد ينطوي على نية عامة وأخرى خاصة. يخرق مرتكبه الحدود القانونية عمدًا، مدرّجًا تمامًا عدم قانونية أفعاله. دوافعه الأساسية هي تحقيق مكاسب مالية غير مشروعة أو حرمان الآخرين من ممتلكاتهم بوسائل خادعة. غالبًا ما تتضمن هذه الجرائم مخططات متطورة مصممة لاستغلال الأنظمة الرقمية، مما يُبرز الحاجة إلى إنفاذ صارم وتدابير أمنية صارمة لحماية الأفراد والمؤسسات من هذه الأنشطة الخبيثة².

المبحث الثاني: الحماية الجنائية من خلال النصوص القانونية

نظرًا للتطور السريع في مجال التكنولوجيا وتزايد استخدام الأنظمة المعلوماتية في مختلف مجالات حياة الفرد الجزائري، ظهرت أنواع جديدة من الجرائم أفرزها هذا التحول الرقمي، وهو ما دفع المشرّع الجزائري إلى ضرورة التدخل لمواكبة هذا التغير وحماية المصالح العامة والخاصة من الاعتداءات الإلكترونية. وتبعًا لذلك سيتطرق موقف المشرع الجزائري من الجريمة المعلوماتية (المطلب الأول)، ثم إلى جرائم الاعتداء الماسة بالأنظمة المعلوماتية (المطلب الثاني).

1 حنان ريجان مبارك المضحاكي، المرجع السابق، ص107.

2 أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية 2006، ص112-113.

المطلب الأول: موقف المشرع الجزائري من الجريمة المعلوماتية

لم يجد المشرع الجزائري بدا من تعديل قانون العقوبات لما كان فراغ قانوني في هذا المجال، وكان ذلك بموجب القانون رقم 15/04 المؤرخ في 10/11/2004 المتمم والمعادل للأمر 66/156 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام.

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة.

لذلك فقد أثار المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها، وحصرها فقط في صور الأفعال التي تشكل اعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها (الفرع الأول). ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها (الفرع الثاني).

الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

تبني المشرع الجزائري للدلالة على الجريمة المعلوماتية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته أي المحتوى وما يحتويه من مكونات غير مادية محلا للجريمة المعلوماتية، ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي

يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام، فإن ثبت تخلف هذا الشرط الأولي، فلا يكون هناك محال لهذا البحث إذ أن هذا الشرط يعتبر عنصراً لازماً لكل منها.

ولما كانت مكونات النظام المعلوماتي غير المادية لا تظهر على حالة واحدة إذ قد تكون مخزنة به أو منقولة منه أو عليه، فإن الأمر يتوجب التطرق لدراسة المقصود بنظام المعالجة الآلية للمعطيات.

أولاً: المقصود بنظام المعالجة الآلية للمعطيات.

على الصعيد الدولي، اعتمدت معاهدات واتفاقيات مختلفة تعريفات واسعة مماثلة لتسهيل التعاون والإنفاذ عبر الحدود. على سبيل المثال، تُعرّف الاتفاقية الدولية بشأن الجرائم الإلكترونية (ICPC) نظام معالجة البيانات الآلي بأنه أي جهاز أو أجهزة مترابطة قادرة على إجراء معالجة آلية للبيانات من خلال برنامج مُحدد. تُغطي هذه اللغة الشاملة النطاق المتنوع للأنظمة المستخدمة عالمياً، من أجهزة الكمبيوتر الفردية إلى مراكز البيانات الواسعة وبيئات السحابة الافتراضية. وبالمثل، تُعرّف الاتفاقية الأوروبية بشأن الجرائم الإلكترونية هذه الأنظمة بأنها أي جهاز أو أجهزة مترابطة قادرة على تنفيذ معالجة آلية، مُشددةً على الطبيعة المترابطة للأنظمة الحديثة.¹

يتوافق مشروع القانون العربي النموذجي مع هذه المعايير الدولية، إذ يصف نظام معالجة البيانات الآلي بأنه مجموعة من وحدات المعالجة - تشمل الذاكرة والبرامج وأجهزة الإدخال/الإخراج ووحدات الاتصال - تعمل معاً لتحقيق نتائج محددة. ويؤكد هذا التعريف على التشغيل الجماعي لمختلف مكونات

1 سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، سنة دراسية 2012/2013، ص 42-43.

الأجهزة والبرمجيات، مؤكداً أن جوهر هذه الأنظمة يكمن في ترابطها وتنسيق عملها، لا في أي بنية تقنية محددة.

ومن هذه التعريفات، يتضح أن "نظام معالجة البيانات الآلي" يشمل أي مجموعة مترابطة من الأجهزة والبرمجيات المصممة لمعالجة المعلومات تلقائياً. ويشمل ذلك جمع البيانات وتخزينها ومعالجتها ونقلها وتبادلها، ويتم ذلك جميعاً من خلال برنامج محدد. ويتمثل الجانب الحاسم في ربط المكونات وتشغيلها الجماعي - أي كيفية عملها معاً بسلاسة لأداء وظائفها المقصودة. ويضمن هذا الفهم الواسع والشامل قدرة القانون على تنظيم مجموعة واسعة من الأنظمة الحالية والمستقبلية بفعالية، مما يحمي الأنشطة الرقمية ويعزز الثقة في البيئة الرقمية.

ثانياً: مدى اشتراط الحماية التقنية للنظام المعلوماتي.

يؤدي الفقه القانوني دوراً حاسماً في تشكيل الإطار القانوني المحيط بالجرائم التي تتطوي على أنظمة معالجة البيانات الآلية، لا سيما في تحديد ما إذا كانت الحماية التقنية ضرورية لإثبات المسؤولية الجنائية. في القانون الفرنسي، يرى الرأي السائد أن الحماية التقنية ليست شرطاً أساسياً لاعتبار الجريمة الإلكترونية جريمة، بل تُعتبر هذه الحماية في المقام الأول دليلاً على سوء نية الجاني ونيته الإجرامية. ويؤكد هذا المنظور أن وجود نية خبيثة أو وصول غير قانوني كافٍ لإثبات السلوك الإجرامي، بغض النظر عما إذا كانت التدابير الأمنية التقنية مطبقة وقت ارتكاب الجريمة أم لا.¹

في مقابل ذلك، يؤيد منظور ثانٍ أهمية التدابير الأمنية كعنصر أساسي في اعتبار الهجوم جريمة. ويجادل المؤيدون بأن الوصول غير المصرح به يفترض خرقاً لبروتوكولات الأمن، وبالتالي،

1 سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، المرجع السابق، ص45.

فإن الحماية التقنية جزء لا يتجزأ من عملية التجريم. ويؤكدون أن وجود هذه الضمانات أو غيابها يمكن أن يساعد في التمييز بين الأنشطة المشروعة والمصرح بها والاختراقات غير القانونية. يُحذّر منتقدو اشتراط الحماية التقنية من أن فرض مثل هذا الشرط قد يُقيّد نطاق التجريم ظلماً ليقصر على الأنظمة المزوّدة بضمانات مُحدّدة. ويكتسب هذا الرأي أهمية خاصة بالنظر إلى الانتشار الواسع لأنظمة المعلومات عالية الأمان في البيئة الرقمية الحالية، مما يجعل هذا الشرط غير عملي وغير عادل.

في حين تُسهم الحماية التقنية بلا شك في حماية البيانات وكشف الاختراقات، إلا أنها لا تستطيع، بمعزل عن غيرها، منع أو تجريم جميع أشكال الجرائم الإلكترونية. لذلك، يجب أن يتجاوز القانون الجنائي الفرنسي مجرد التدابير التقنية ليشمل الحماية القانونية التي تُعالج السياق الأوسع للجرائم الإلكترونية. وخلال المناقشات البرلمانية، أعرب عن معارضة لفكرة فرض الحماية التقنية كشرط ضروري للمسؤولية الجنائية، مُشدّدين على أهمية اتباع نهج قانوني شامل يعكس واقع تحديات الأمن السيبراني الحديثة.

الفرع الثاني: المقصود بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال

شهدت العقود الأخيرة تطوراً مذهلاً في مجال تكنولوجيا الإعلام والاتصال، الأمر الذي أدى إلى بروز جرائم من نوع جديد تستغل هذا الفضاء الرقمي بطرق متزايدة التعقيد. وقد دفعت هذه الظاهرة الدول، ومن بينها الجزائر، إلى إعادة النظر في ترسانتها القانونية للتعامل مع هذا النوع المستحدث من الجرائم. في هذا السياق، تبرز أهمية القانون رقم 04/09 كمحطة مفصلية في تنظيم الجرائم المرتكبة عبر الوسائط التكنولوجية. وفيما يلي عرض لهذا التحول التشريعي من خلال نقطتين أساسيتين:

أولاً: الإطار القانوني قبل صدور القانون رقم 04/09

قبل صدور القانون رقم 04/09 في 9 أوت 2009، كان الإطار القانوني الجنائي الجزائري المتعلق بالجرائم الإلكترونية ضيق النطاق نسبياً. كان التشريع الحالي يتناول في المقام الأول الأفعال التي تؤثر بشكل مباشر على أنظمة معالجة البيانات الآلية، مثل أجهزة الكمبيوتر والبنية التحتية الرقمية ذات الصلة. وبموجب هذه الأحكام السابقة، كانت الأفعال الإجرامية التي تنطوي على التلاعب أو الإلتلاف أو الوصول غير المصرح به إلى المعلومات أو الأنظمة أو الشبكات تُعتبر جزءاً من سلوك إجرامي أوسع نطاقاً، وليست فئة مستقلة تتطلب معالجة قانونية متخصصة. وقد عكس هذا النهج المحدود الفهم السائد آنذاك بأن الجرائم الإلكترونية هي في المقام الأول شذوذات تقنية وليست مكونات أساسية للنشاط الإجرامي.¹

ثانياً: التحول الذي أحدثه القانون رقم 04/09

كشف التطور السريع لتكنولوجيا المعلومات والاتصالات واندماجها الشامل في الحياة اليومية عن قيود هذا النهج القانوني التقليدي. وبدأت الأنشطة الإجرامية تستغل المنصات الرقمية بطرق أكثر تطوراً، مما أدى إلى تغيير طبيعة الجرائم القائمة بشكل فعال، وأدى إلى ظهور فئات جديدة تماماً من الجرائم. إدراكاً لهذه التحديات، أصدر المشرع الجزائري القانون رقم 04/09 عام 2009، الذي مثّل نقطة تحوّل جوهرية في الموقف القانوني للبلاد تجاه الجرائم الإلكترونية. وسّع هذا القانون نطاق الأحكام

1 سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، المرجع السابق، ص 42-43.

الجنائية ليشمل صراحةً الجرائم المرتكبة عبر أنظمة المعلومات وشبكات الاتصالات الإلكترونية أو التي تُسهّلها¹.

من أبرز سمات القانون رقم 04/09 تعريفه الواسع والشامل للجرائم الإلكترونية. فبدلاً من حصره في أفعال محددة كالقرصنة أو سرقة البيانات، يشمل القانون أي جريمة تُرتكب عبر نظام معلومات أو شبكة إلكترونية، سواءً كانت هذه الأفعال مُدرجة صراحةً في قانون العقوبات الساري أم لا. يُقرّ هذا النهج بإمكانية استخدام المنصات الرقمية كأدوات لمجموعة واسعة من الأنشطة غير المشروعة، بما في ذلك الإرهاب والتزوير والفحش والجرائم الأخلاقية. على سبيل المثال، يُقرّ القانون بإمكانية استخدام الجماعات الإرهابية لخدمات الرسائل المشفرة لتنسيق الهجمات، أو بإمكانية استخدام التزوير الإلكتروني لتزوير الوثائق الرسمية إلكترونياً. وبذلك، يتكيف الإطار القانوني مع المشهد المتطور للسلوك الإجرامي، مما يضمن امتلاك السلطات للأدوات اللازمة لمكافحة جميع أشكال الجرائم الإلكترونية.

أثار التوسع الذي أحدثه القانون رقم 04/09 جدلاً واسعاً بين علماء القانون والممارسين القضائيين وصانعي السياسات. وتتعلق إحدى القضايا المحورية بما إذا كانت القوانين الجنائية القائمة، حتى بعد تعديلها، كافية لمعالجة تعقيدات الجرائم الإلكترونية بفعالية. ويجادل البعض بأن المبادئ القانونية التقليدية، مثل مبدأ الشرعية، تفرض قيوداً مهمة على التجريم. وينص هذا المبدأ على أنه لا يمكن اعتبار أي فعل إجرامياً إلا إذا نص عليه القانون صراحةً، مما يمنع التجريم التعسفي أو بأثر رجعي. وبالتالي، فإن توسيع نطاق المسؤولية الجنائية ليشمل أشكالاً جديدة من السلوك الإلكتروني يتطلب أحكاماً قانونية واضحة ومحددة. وقد خضع استخدام القانون لعبارات فضفاضة، مثل "أي جريمة

1 القانون رقم 04/09 المؤرخ في 5 أغسطس 2009، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، ص 5.

أخرى"، للتدقيق لأنه يُخاطر بانتهاك مبدأ الشرعية، مما قد يسمح بتطبيقات غامضة أو فضفاضة للقانون الجنائي.¹

علاوة على ذلك، يُعزز حظر القياس في القانون الجنائي الموضوعي ضرورة وجود تعريفات قانونية دقيقة. يمنع هذا المبدأ المحاكم من توسيع نطاق المسؤولية الجنائية بناءً على أوجه التشابه المُتصوّرة بين الجرائم التقليدية والجرائم الإلكترونية فقط. تُشدد المادة 2 من القانون رقم 04/09 على وجوب استناد التجريم إلى نصوص قانونية واضحة².

وفي الختام، يُمثّل القانون رقم 04/09 الصادر في 9 أغسطس/آب 2009 تطوراً محورياً في القانون الجنائي الجزائري، إذ يعكس إدراكاً للأثر التحويلي لتكنولوجيا المعلومات والاتصالات على السلوك الإجرامي. وبينما يُوسّع القانون بشكل كبير نطاق ما يُشكّل جريمة إلكترونية، فإنه يُثير أيضاً تساؤلات مهمة حول التوازن بين الإنفاذ القانوني الفعال والالتزام بالمبادئ القانونية الأساسية. ومع استمرار تطور التكنولوجيات الرقمية، فإن التطوير المستمر للتشريعات والتفسير القضائي سيكون ضروريا لضمان بقاء الإطار القانوني شاملاً وسليماً من الناحية الدستورية. لذلك ندعو المشرع الجزائري لتعديل النصوص القائمة لتستوعب الصور المتطورة للجرائم التقليدية والتي يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية.

1 عبد العزيز جغام، "الجرائم الإلكترونية في ظل قانون 04/09"، المجلة الجزائرية للقانون والعلوم السياسية، العدد 14، 2017، ص. 86.

2 المادة 2 من القانون 04/09 تنص على أنه "لا تُعدّ الأفعال جرائم إلا بنص صريح وواضح يحدد أركانها والعقوبة المقررة لها".

المطلب الثاني: جرائم الاعتداء الماسة بالأنظمة المعلوماتية.

استحدثت المشرع بموجب القانون رقم 04-15¹ مجموعة من النصوص، التي جرم من خلالها كل الأفعال والسلوكيات المرتبطة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها جزاء.

ويمكن الإشارة قبلها، إلى تعريف الجريمة المعلوماتية أو الجريمة السيبرانية أو جريمة الفضاء الإلكتروني مثلما يسميها البعض، وهي جريمة يستخدم الحاسوب في ارتكابها، وهي عبارة عن مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي وسواء كان ذلك بطريقة مباشرة أو غير مباشرة، والمهم في ذلك هو استخدام وسائل الاتصال الحديثة بشأنها من حاسوب، أو أية آلة ذكية أخرى، وتتميز الجريمة المعلوماتية عن الجريمة التقليدية من حيث تعريفها، وخصائصها، وأركانها، وكذا القانون وجب تطبيقه عليها.

وتجدر الإشارة إلى أن جريمة الاعتداء على نظام المعالجة الآلية للمعطيات تتحقق في صورتين: تبرز الأولى في جرمي الدخول والبقاء غير المرخص بهما في النظام، وبينما تظهر الصورة الثانية في تلك النتائج غير المشروعة ضد معطيات النظام المترتبة عن فعل الدخول أو البقاء، وعليه سوف نتناول الصور البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات (الفرع الأول)، ثم الصور المشددة الاعتداء على نظام المعالجة الآلية للمعطيات (الفرع الثاني).

1 - قانون رقم 04-15 مؤرخ في 10 نوفمبر، 2004 يتضمن قانون العقوبات، جريدة رسمية عدد 71 لسنة 2004، معدل ومتمم. وذلك من خلال المواد من 394 مكرر إلى 394 مكرر 07، المضافة بموجب القانون نفسه.

الفرع الأول: الصور البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات

نظرًا للمكانة المحورية التي تحتلها نظم المعالجة الآلية للمعطيات في البنى التحتية الرقمية، فإن أي اعتداء عليها يُعدّ مساسًا خطيرًا بأمن المعلومات وسلامة الأنظمة. وقد اهتم المشرّع بتجريم هذا النوع من السلوك، لاسيما في صورته الأولية التي تُشكّل في ذاتها تمهيدًا لأفعال أكثر خطورة. وتتمثل الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات في شكلين رئيسيين: تتمثل الصورة البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات في شكل الدخول (أولا) أو البقاء (ثانيا) غير المرخص بهما.

أولا: الدخول غير المرخص به

فيما يتعلق بالأنظمة غير المحمية، تُرسي المادة 394 من القانون 04-15 من قانون العقوبات الجزائري المعدل والمتمم مكرّر من قانون العقوبات الجزائري¹ إطارًا قانونيًا واسعًا وقويًا يهدف إلى حماية البنية التحتية للمعلومات الرقمية. ويؤكد هذا النهج الشامل إدراك الدولة لأهمية تأمين جميع أنظمة معالجة البيانات ضد الوصول غير المصرح به، بغض النظر عن مستوى الأمان أو الحساسية المتصورة لها. ويُجرّم القانون صراحةً أي فعل ينطوي على دخول احتيالي إلى نظام معالجة بيانات آلي، سواء نجح الجاني في الوصول إليه أو حاول ذلك. ويؤكد هذا الموقف على جدية التعامل مع الاختراقات الرقمية، مؤكّدًا أن الفعل الإجرامي يُعتبر مكتملاً لحظة محاولة الوصول غير المصرح به أو لحظة حدوثه.

¹ قانون رقم 04-15 مؤرخ في 10 نوفمبر، 2004 يتضمن قانون العقوبات، جريدة رسمية عدد 71 لسنة 2004، معدل ومتمم. وذلك من خلال المواد من 394 مكرر إلى 394 مكرر، 07 المضافة بموجب القانون نفسه.

وتعكس العقوبات المنصوص عليها في هذه المادة خطورة هذه الجرائم. وينص القانون على السجن لمدة تتراوح بين ثلاثة أشهر وسنة واحدة، كإجراء عقابي وراذع للمجرمين المحتملين. بالإضافة إلى السجن، يواجه المخالفون عقوبات مالية - غرامة تتراوح بين 500,000 و 100,000 دينار جزائري. تُعزز هذه الغرامات العواقب القانونية المرتبطة بسوء السلوك الإلكتروني، وتُبرز أهمية حماية أنظمة المعلومات ضمن الإطار القانوني الوطني.

ومن الجوانب الجديرة بالملاحظة في هذه اللائحة تركيزها على المسؤولية الجنائية. إذ يُوضح القانون أن إثبات الفعل المادي - أي دخول النظام أو محاولة دخوله دون تصريح - كافٍ لاستدعاء المسؤولية الجنائية. ولا يشترط إثبات أي ضرر أو تلف لاحق ناتج عن هذا الفعل. ويتمشى هذا الموقف مع تصنيف هذه الجرائم كجرائم شكلية. ففي المصطلحات القانونية، تُوصف الجريمة الشكلية بإتمام الفعل نفسه، بغض النظر عما إذا كان يُسبب ضرراً ملموساً. ولذلك، يُصنف القانون محاولة الاختراق كجريمة في حد ذاتها، مما يؤكد على الطبيعة الوقائية لهذا التشريع لا التفاعلية.

علاوة على ذلك، يُشدد القانون على أنه لكي تنشأ المسؤولية، يجب أن يكون الدخول احتيالياً. وهذا يعني أن أي دخول غير مُصرح به يجب أن يكون غير مشروع - أي يفترق إلى تصريح أو موافقة قانونية - مما يُميزه عن الدخول العرضي أو الحميد. يُبرز التركيز على الاحتيال سوء النية أو الخداع المتضمن في مثل هذه الأفعال، ويساعد على التمييز بين السلوك الإجرامي والاتصال البريء أو العرضي بأنظمة معالجة البيانات.

ومن المهم أن المادة 394 مكرر تُطبق على جميع أنظمة المعلومات، بغض النظر عن تدابيرها الأمنية أو حالتها المحمية. لا يُحدد القانون أنواعاً معينة من الأنظمة أو يُحدد الحماية المطلوبة، مثل ضمانات القرصنة المتقدمة. يمنع هذا التطبيق الواسع الجناة من استغلال الثغرات التقنية بالادعاء بأن

هدفهم يفتقر إلى حماية محددة أو أنه غير محمي بطبيعته. من خلال إرساء قاعدة عامة، يسعى القانون الجزائري إلى إنشاء درع شامل ضد جميع أشكال الوصول الرقمي غير المصرح به، مما يُعزز التزام البلاد بالأمن السيبراني وسلامة البنية التحتية الرقمية.

ثانياً: البقاء غير المرخص به

يقصد بالبقاء غير المرخص به هنا، الدخول إلى النظام والاستمرار في التواجد داخله وذلك دون إذن صاحبه، رغم علمه بأن بقاءه فيه غير مرخص¹.

ولقد سوى المشرع الجزائري بموجب المادة 394 مكرر من قانون العقوبات السابق بين كل من جريمة الدخول غير المرخص به والبقاء غير المرخص به، وهو ما يؤكد تطبيق الجزاء نفسه على السلوكين وهي عقوبة الحبس من ثلاثة (03) أشهر إلى سنة، وغرامة مالية من 50000 دج إلى 100000 دج ويعتبر فعل البقاء مثله مل فعل الدخول، بمثابة الركن المادي للجريمة، ونضيف هنا ونؤكد أن البقاء قد يحتمل صورتين مختلفتين هما:

1. تتمثل الصورة الأولى، في حالة تحقق فعل البقاء غير المرخص به داخل نظام المعالجة الآلية للمعطيات منفصلاً عن فعل الدخول ويكون الدخول إلى نظام المعالجة مشروعاً، حتى وإن كان خطأً أو صدفة، غير أنه وبتفطن الفاعل للوضع وبدلاً من الانسحاب أو مغادرة النظام فوراً، فإنه يستمر في استغلال النظام، فهنا يعاقب على جريمة البقاء غير المرخص به.

1 آمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر 2007، ص102.

2. بينما تكمن الصورة الثانية، في حالة تحقق فعل البقاء غير المرخص به متصلا ومجتعا مع فعل الدخول وهي حالة أكثر تشديدا من سابقتها كون فعل الدخول وفعل البقاء مجتمعين وينشأن بصفة غير مشروعة، كأن يتم الدخول دون ترخيص أو إذن سابق، ثم يستمر في البقاء داخله. والإشكال الذي يمكن أن يثيره هذا الاجتماع والتداخل للسلوكين من دخول إلى النظام والبقاء فيه، هو تحديد النطاق الزمني لكل واحدة منها، بمعنى متى تنتهي جريمة الدخول؟ ومتى تبدأ جريمة البقاء؟ ومن أجل الإجابة عن الإشكال، فلقد تضاربت آراء فقهية عن المسألة، إذ هناك من يرى بأن الجريمة المتعلقة بالبقاء داخل النظام تبدأ من اللحظة التي يتم فيها الدخول الفعلي للمجرم إلى النظام، وذلك بتجوله وتنقله داخل هذا الأخير، وهنا تكون جريمة الدخول مكتملة، وهناك من يرى بأن جريمة البقاء تكون في الوقت الذي يعلم فيه المتدخل بأن بقاءه في النظام غير مشروع، ولم ينسحب من النظام¹.

ومهما يكن من أمر، فإن المشرع الجزائري ومن خلال المادة 394 مكرر قد تطرق إلى الدخول ثم إلى البقاء، وكأن المشرع يصنف الأولى بجريمة وقتية كون فترة استمرارها قصيرا جدا والأخرى بجريمة مستمرة، مقارنة بالأولى.

1 أمير فرج يوسف، الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004، ص28.

الفرع الثاني: الصور المشددة الاعتداء على نظام المعالجة الآلية للمعطيات

نظرًا لأهمية نظم المعالجة الآلية للمعطيات في العصر الرقمي، فقد أصبحت محلًا لعدد من التهديدات الإجرامية التي تستهدف سلامتها ووظائفها. ومن بين أبسط صور هذه الاعتداءات، ما يتمثل في محاولات الوصول غير المشروع إليها، سواء من خلال الدخول أو حتى البقاء غير المرخص بهما. وقد اعتبر المشرع هذين الشكلين من الأفعال خرقًا خطيرًا لخصوصية وأمن الأنظمة المعلوماتية، وأفرد لهما أحكامًا خاصة.

أولاً: الدخول غير المرخص به إلى نظام المعالجة الآلية

يُقصد به قيام شخص ما باختراق نظام معلوماتي أو التسلل إليه دون إذن صاحب الحق أو دون توفر صفة قانونية تخوله ذلك. ويُعد هذا الفعل جريمة قائمة بذاتها حتى وإن لم يصاحبها أي فعل آخر كالإتلاف أو التغيير أو النسخ. ويُبرر تجريم هذا الشكل من السلوك كونه يمثل تهديدًا لبنية النظام المعلوماتي، كما قد يُمهد لجرائم لاحقة أكثر ضررًا مثل سرقة البيانات أو إتلافها.

وقد نصّ القانون رقم 04/09 في مادته السادسة على: * "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من 50.000 دج إلى 200.000 دج كل من يدخل أو يحاول الدخول بطريقة احتيالية إلى كل أو جزء من نظام المعالجة الآلية للمعطيات".¹

1 القانون رقم 04/09 المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، سنة 2009.

ثانياً: البقاء غير المرخص به في نظام المعالجة الآلية

لا يقتصر التجريم على لحظة الدخول غير المشروع فحسب، بل يمتد أيضاً إلى حالة البقاء في النظام بعد الدخول دون إذن، سواء تم ذلك بعد الدخول بطريقة شرعية (مثلاً بانتحال صفة مستخدم مرخص) أو غير شرعية. فالمشرع يرى أن الاستمرار غير المبرر في الولوج إلى النظام يشكل خطراً مماثلاً، بل قد يكون أكثر تعقيداً كونه قد يُستغل للقيام بأفعال تخريبية أو تجسسية.

ويعاقب القانون على هذا السلوك بنفس العقوبة المقررة للدخول غير المشروع، وهو ما يعكس حرص المشرع على حماية النظام المعلوماتي من جميع صور التعدي غير المصرح بها.¹

1 القانون رقم 04/09 المؤرخ في 5 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، سنة 2009.

خلاصة الفصل

خصص هذا الفصل الموسوم بـ"الإطار المفاهيمي للجريمة المعلوماتية" الذي استنتجنا منه أن الجريمة المعلوماتية جريمة مستحدثة تستهدف للاعتداء على المعطيات بدلالاتها التقنية الواسعة أو الاستعانة بها لارتكاب جرائم تحاكي الجرائم التقليدية في العالم الافتراضي، وفي هذا الفصل تم تناول تعريف الجريمة المعلوماتية وذلك حسب الاتجاهات القانونية، ثم بعد ذلك تم تحديد الطبيعة القانونية لها ثم تبيان خصائصها، بالإضافة إلى الهدف من ارتكابها، ثم تم التعرّيج بعد ذلك إلى استيضاح موقف التشريع الجزائري من الجريمة المعلوماتية من خلال النصوص القانونية الموضوعة لمواجهة هذه الجريمة، والصور التي جاعت هذه النصوص القانونية ، وفي الأخير إبراز أهم صور هذه الجريمة.

الفصل الثاني

الفصل الثاني: آليات وإجراءات التحري في مجال الجريمة المعلوماتية

تُعد الجريمة المعلوماتية من أبرز التحديات التي فرضها العصر الرقمي، وهي تختلف في طبيعتها عن الجرائم التقليدية، إذ إن الجاني في هذا النوع من الجرائم لا يلجأ إلى القوة أو الوسائل المادية، بل يعتمد على ذكائه التقني وقدرته على استغلال الثغرات الموجودة في الأنظمة المعلوماتية.

ويتميز مرتكب الجريمة المعلوماتية بامتلاكه معرفة دقيقة بكيفية تشغيل الحواسيب، والتعامل مع قواعد البيانات، وتصميم البرامج واختراقها دون أن يترك وراءه أثرًا ماديًا يسهل تتبعه أو يكشف عن هويته. وهذا ما يجعل من عملية تعقب الجناة وتحديد هويتهم أمرًا في غاية الصعوبة، ويُعَدُّ من مهمة أجهزة إنفاذ القانون والمحققين في هذا المجال.

ففي ظل غياب الأدلة التقليدية يستدعي ذلك إنشاء وحدات متخصصة تمتلك المعرفة التقنية والوسائل التكنولوجية المناسبة لملاحقة هذه الجرائم وكشف ملابساتها. وقد أدرك المشرع الجزائري خطورة هذه الظاهرة، فعمل على وضع إطار قانوني وتنظيمي يُمكن السلطات من مجابقتها بفعالية.

ولأجل فهم أعمق لطرق مكافحة هذه الظاهرة، كان من الضروري تسليط الضوء على الآليات المعتمدة على المستوى الوطني في التصدي للجريمة المعلوماتية. ويتضمن هذا محورين أساسيين، هما: الوحدات المتخصصة المكلفة بإجراء عمليات البحث والتحقيق في الجرائم المعلوماتية على المستوى الوطني، من حيث هيكلتها، مهامها، ووسائل عملها (المبحث الأول)، ثم الإجراءات القانونية للتحري والكشف عن الجريمة المعلوماتية، من خلال استعراض النصوص القانونية المعتمدة، والضوابط الإجرائية التي تحكم عملية جمع الأدلة الرقمية وتقديمها أمام الجهات القضائية المختصة (المبحث الثاني).

المبحث الأول: الوحدات المختصة التي تتولى إجراءات البحث والتحقيق في الجريمة المعلوماتية

يقدم هذا المبحث لمحة عامة عن أبرز الهيئات المعنية بمكافحة الجرائم الإلكترونية، مع التركيز على دورها في الوقاية والتحقيق. تتألف هذه الوحدات المتخصصة من محققين يعملون كضباط شرطة قضائية، يتمتعون بخبرة واسعة في أنظمة المعلومات والتقنيات الرقمية وأساليب الجرائم الإلكترونية. تتيح لهم معرفتهم المتخصصة إجراء بحوث شاملة، وجمع الأدلة الرقمية، وإجراء التحقيقات بدقة وكفاءة. غالبًا ما تتعاون هذه الوحدات بشكل وثيق مع المدعين العامين وقضاة التحقيق، لضمان اتباع الإجراءات القانونية والملاحقة القضائية السليمة للقضايا. ولتحقيق ذلك، تستخدم تقنيات تحقيق متقدمة وأدوات متطورة مصممة خصيصًا للكشف عن الجرائم الإلكترونية وتحليلها. من أبرز هذه الهيئات الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات. والذي سندرس فيه الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (المطلب الأول)، ثم ندرس الأجهزة الأمنية المسؤولة عن إجراء البحث والتحقيق (المطلب الثاني).

المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

طُرح مفهوم إنشاء هيئة وطنية مُخصصة للوقاية من الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات لأول مرة في عام 2009 من خلال القانون 09-04. وقد نصت المادة 13 من هذا التشريع صراحةً على إنشاء مثل هذه الهيئة، على أن تُحدد اللوائح اللاحقة التفاصيل المُحددة المتعلقة بهيكلها ووظائفها. ومع ذلك، وعلى الرغم من المتطلب القانوني الواضح، فقد شهد التقدم في إنشاء الهيئة تأخيرًا كبيرًا، امتد لأكثر من ست سنوات. ولم يصدر المرسوم الرئاسي رقم 15-268 أخيرًا إلا في 8 أكتوبر 2015، مما يمثل خطوة محورية في هذه المبادرة. وقد حدد هذا المرسوم تكوين الهيئة الوطنية وإطارها التنظيمي، مقدمًا مخططًا واضحًا لتشكيلها ونطاق عملها. وقد اعتُبر إنشاء هذه الهيئة خطوة حاسمة لتعزيز الأمن السيبراني الوطني، ومكافحة المد المتصاعد للجرائم الإلكترونية، وضمان

اتباع نهج منسق لمواجهة تحديات الأمن المتعلقة بتكنولوجيا المعلومات والاتصالات في جميع أنحاء البلاد.¹ والذي سنتناول فيه التعريف بالهيئة واختصاصاتها (الفرع الأول)، ثم تشكيلة الهيئة وطبيعة عملها (الفرع الثاني).

الفرع الأول: التعريف بالهيئة واختصاصاتها

نظرًا لتزايد الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال، استحدثت الجزائر هيئة وطنية متخصصة لمكافحتها والوقاية منها. تتميز هذه الهيئة باستقلالية قانونية ومالية، وتعمل تحت إشراف وزير العدل، مما يمنحها فعالية أكبر في أداء مهامها. وتُعد هذه الهيئة أداة مؤسساتية مركزية في التصدي للجرائم المعلوماتية. يتناول هذا الفرع محورين أساسيين: أولاً، التعريف بالهيئة من حيث طبيعتها ومكانتها، وثانياً، بيان اختصاصاتها القانونية والعملية وفقاً للمرسوم الرئاسي 15-261. تهدف هذه المعالجة إلى تسليط الضوء على مدى جاهزية الدولة لمواجهة التحديات الرقمية المتزايدة.

أولاً: التعريف بالهيئة

هي هيئة إدارية مستقلة تعمل تحت إشراف وزير العدل، يقع مقرها الرئيسي في مدينة الجزائر العاصمة. تتمتع باستقلالية قانونية ومالية، مما يسمح لها بالعمل بفعالية دون أي تدخل خارجي. يُحدد القانون 04-09 مسؤولياتها، الذي يُحدد مهامها وصلاحياتها الأساسية. يتمثل دور الهيئة الرئيسي في

1 حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص -قانون العقوبات والعلوم الجنائية، جامعة باتنة 1، السنة الجامعية 2015/2016

ضمان الامتثال للمعايير المعمول بها في نطاق اختصاصها، وتعمل في إطار يضمن الشفافية والمساءلة والالتزام بسيادة القانون في جميع أنشطتها¹.

ثانياً: اختصاصات الهيئة

بينت الفقرة الثانية 02 من المادة 04 من المرسوم الرئاسي 15—261 المهام الأساسية التي تكلف بها الهيئة وهي وعلى سبيل الحصر مهام الهدف منها هو الوقاية من الجرائم المعلوماتية ومكافحتها من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون المصالح الشرطة القضائية وأبرز مهام هذه الهيئة هي:

1. اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال.
2. تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.
3. مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدّها بالمعلومات والخبرات القضائية.
4. ضمان المراقبة الوقائية للاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالاعمال الارهابية والتخريبية والماسة بأمن الدولة وذلك تحت قاضي مختص وذلك كاختصاص حصري.
5. تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مسارها من أجل استعمالها في الاجراءات القضائية.

1 تنص المادة 14 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على انه "تتولى الهيئة المذكورة في المادة 13.

6. المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات المعلومات.

7. تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المعلوماتية.

8. تنفيذ الطلبات الصادرة عن الدول الأجنبية وتطوير سبل التبادل معها.

9. المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

الفرع الثاني: تشكيلة الهيئة وطبيعة عملها

لضمان أداء هذه الهيئة لمهامها بكفاءة، تم تنظيمها وفق هيكل إداري وتقني محكم يعكس طابع التكامل بين الجانب القانوني والتقني. يتناول هذا الفرع تفصيلاً تشكيلة الهيئة من جهتين أساسيتين: أولاً، الجانب الإداري الذي يشرف عليه وزير العدل ويضم ممثلين عن عدة قطاعات حساسة؛ وثانياً، الجانب التقني الذي تضطلع به مديريات متخصصة، تُعنى باليقظة الإلكترونية، التحريات التقنية، وتحليل الجرائم المعلوماتية. يهدف هذا العرض إلى إبراز التنظيم الداخلي للهيئة بما يسمح لها بالاستجابة الفعالة للتهديدات الرقمية المتزايدة في الجزائر.

أولاً: تشكيلة الهيئة الإدارية

تعمل الهيئة بموجب نظام إدارة منظم وهرمي، مصمم لضمان الرقابة والتنسيق الفعالين بين مختلف القطاعات. وعلى رأسها لجنة يقودها وزير العدل، الذي يقدم التوجيه الاستراتيجي والإرشاد السياسي. وتتألف هذه اللجنة من مسؤولين رئيسيين من وزارات الداخلية وتكنولوجيا المعلومات والاتصالات والدرك الوطني والأمن الوطني والرئاسة ووزارة الدفاع. ولدمج الرقابة القضائية وضمان النزاهة القانونية، فإن قاضيين من المحكمة العليا أعضاء في هذه اللجنة أيضاً. وتدعم قرارات اللجنة المديرية العامة، التي يرأسها شخص معين من قبل الرئيس ومسؤول عن العمليات اليومية. وتشمل واجبات المديرية إدارة برامج العمل، وإعداد مسودات الميزانية، وتجميع تقارير الأنشطة لرصد التقدم وضمان المساءلة. ومع ذلك، لا تعمل اللجنة ولا المديرية العامة بمعزل عن بعضها البعض؛ بل تعملان

بالتعاون مع الوكالات والجهات المعنية الأخرى لدعم مهمة الهيئة والتكيف مع التحديات الأمنية المتطورة¹.

ثانيا: تشكيلة الهيئة التقنية

إضافة إلى اللجان الإدارية تضم الهيئة مديريات تتقسم من حيث مهامها وتشكيلتها بالطابع التقني، باعتبارها المختصة بإنجاز المهام التقنية المتعلقة بالوقاية وبمكافحة الجرائم المعلوماتية وهذه المديريات هي:

1. مديرية المراقبة الوقائية واليقظة الإلكترونية: لم يشر الأمر الرئاسي 15-261 إلى تشكيلة هذه المديرية، غير أنه ومن خلال تحليل نص المادة 18 منه² يمكن لنا تحديد تشكيلتها في مجموعة من ضباط وأعوان الشرطة القضائية المختصين في مجال مكافحة الجرائم المعلوماتية، من سلك الأمن الوطني وكذلك الدرك الوطني والمصالح العسكرية للاستعلام والأمن، يعينون بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل والدفاع والداخلية، يساعدهم مستخدمي الدعم التقني والإداري من نفس الأسلاك.
- تعمل هذه المديرية على إنجاز المهام التالية:

1 المواد 06 الى 10 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

2 الأمر الرئاسي رقم 15-261 المؤرخ في 23 أوت 2015، المتعلق بإنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 48، سنة 2015.

أ. تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية والقيام بإجراءات التفتيش والحجز داخل الأنظمة المعلوماتية إذا ما تعلق الأمر جرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة بناء على رخصة مكتوبة من السلطة القضائية وتحت رقابة القاضي المختص.

ب. إرسال المعلومات المحصل عليها إلى السلطات القضائية ومصالح الشرطة القضائية.

ج. تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة وجمع المعطيات التي تسمح بتحديد مكان تواجد مرتكبي الجرائم المعلوماتية والتعرف عليهم.

د. جمع كل المعلومات واستغلالها من أجل الكشف عن الجرائم المعلوماتية.

هـ. المشاركة في حملات التوعية حول مخاطر تكنولوجيا الإعلام والاتصال

و. تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائياً أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المعلوماتية.

إذن وبالنظر إلى تشكيلة والمهام الملحقه بهذه المديرية فإنه يمكن وصفها بأنها المركز العملياتي للهيئة بما أنها تتولى الجانب التقني الخاص بإنجاز الأعمال المتعلقة بالبحث والتحقيق في الجرائم المعلوماتية، ولعل أن ما يزيد من دورها الفعال هو تنصيبها على رأس مركز العمليات التقنية وكذلك الملحقات مما يبرز دورها الفعال في تسيير وتأطير الأعمال المتعلقة بالوقاية أو بمكافحة الجرائم المعلوماتية¹.

2. **مديرية التنسيق التقني:** لم ينص المرسوم الرئاسي 15-261 على تشكيلة مديرية التنسيق التقني مما يترك المجال للقول بأنها تشكيلتها تكون بناء على قرارات مشتركة بين وزراء العدل

1 - المواد 11-13-14-18-21 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- والدفاع والداخلية على شاکلة مديرية المراقبة الوقائية واليقظة الإلكترونية، غير أنها تختلف عنها من حيث المهام الموكلة إليها، فتتمثل مهامها أكثر في الدور الوقائي والإعلامي من خلال توليها:
- أ. إنجاز الخبرات القضائية في مجال اختصاص الهيئة.
 - ب. تكوين قاعدة معطيات تحليلية للإجرام المعلوماتي.
 - ج. إعداد الإحصائيات الوطنية للإجرام المعلوماتي.
 - د. تسيير المنظومة المعلوماتية وإدارتها¹.

إذن فمن خلال استعراض الهيكل العام للهيئة ومجمل اختصاصاتها، يتضح لنا جليا مدى اقتناع الهيئة التشريعية بضرورة تفعيل دور الهيئة في مجال الوقاية ومكافحة الجرائم المعلوماتية ولو بشكل متأخر، نظرا لتوسع تطبيقات تقنية المعلوماتية في المجتمع الجزائري على الصعيدين الحكومي والاجتماعي، وهو ما ينبئ بتنامي الإجرام المعلوماتي وازدياد حجم التهديدات التي يشكلها على سلامة الأنظمة المعلوماتية وأمن المعطيات المخزنة والمتداولة عبرها.

1 المادة 12 من المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

المطلب الثاني: الأجهزة الأمنية

في إطار التصدي للجرائم المعلوماتية وضمان الأمن السيبراني، تلعب الأجهزة الأمنية دورًا محوريًا في تنفيذ عمليات التحري والتحقيق، والتدخل السريع عند وقوع الاعتداءات التي تستهدف الأنظمة المعلوماتية. وتُعَد كل من جهاز الأمن الوطني وجهاز الدرك الوطني من بين أبرز الفاعلين في هذا المجال، نظرًا لما يتمتعان به من صلاحيات وإمكانات تقنية وبشرية متخصصة. ولتوضيح مساهمة كل منهما، سيتم التطرق إلى الوحدات التابعة لسلك الأمن الوطني (الفرع الأول) ، ثم إلى الوحدات التابعة للدرك الوطني (الفرع الثاني).

الفرع الأول: الوحدات التابعة لسلك الأمن الوطني

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم وبالأخص تلك المستحدثة منها كالجرائم المعلوماتية، وألتي تعتبر نتاج التطور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات.

أولاً: على المستوى المركزي

تخضع المديرية العامة للأمن الوطني (DGSN) حاليًا لعملية إعادة هيكلة شاملة تهدف إلى تعزيز كفاءتها وفعاليتها التشغيلية. وفي إطار هذه المبادرة، تُنشئ المديرية العامة للأمن الوطني وحدات متخصصة مُخصصة لمعالجة فئات مُحددة من الجرائم. صُممت هذه الخطوة الاستراتيجية لتمكين أجهزة إنفاذ القانون من الاستجابة بسرعة ودقة أكبر للمشهد الإجرامي المُتطور. ومن أبرز التطورات إنشاء إدارة مُخصصة للجرائم الإلكترونية ضمن الشرطة القضائية، تُعرف باسم الشرطة العلمية والتقنية. تُكَلَّف

هذه الوحدة المتخصصة بالتحقيق في الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات، مما يعكس الأهمية المتزايدة للأمن السيبراني في العالم الحديث. ويلعب المختبر المركزي للشرطة العلمية، الكائن في الجزائر العاصمة، دورًا محوريًا في التحليل الجنائي في مختلف التحقيقات الجنائية. وهو مُجهز بتقنيات متقدمة ويعمل به خبراء مُدربون تدريبًا عاليًا يُجرون فحوصات مفصلة للأدلة. ويضم المختبر قسمًا فنيًا مسؤولًا عن تحليل الأدلة المتعلقة بالأسلحة والتزوير والجرائم الإلكترونية، من بين أمور أخرى. ويُدير كل نوع من أنواع الجرائم فريق مُتخصص داخل هذه الوحدات، مما يضمن خبرة مُركزة وتحقيقات مُعمّقة. وتمثل هذه الهيكلية الجديدة جهدًا استراتيجيًا تبذله المديرية العامة للأمن الوطني لتحديث قدراتها والتعامل بشكل أفضل مع تعقيدات الجريمة المعاصرة.¹

ثانياً: على المستوى الجهوي

قامت بإنشاء مخابر جهوية للشرطة العلمية في كل من ولايتي قسنطينة وهران، بالإضافة إلى ثلاث 03 مخابر أخرى قيد الإنجاز على مستوى - ورقلة - بشار - تمنراست ينتظر تسليمها قريباً لأجل تعميم هذا النوع من النشاط على كافة ربوع الوطن.

على مستوى كل مخبر مصلحة تسمى دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية ، تتولي هذه المصلحة أعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية، وذلك تحت تسمية دائرة الأدلة الرقمية والآثار التكنولوجية" والتي لم تكن عند استحداثها سنة 2004 سوى

1 مساهمة المخبر الجهوي للشرطة العلمية في كل من قسنطينة وهران في إدارة الدليل ضمن التقنيات الخاصة للتحقيق - وثيقة خاصة صادرة عن نيابة مديرية الشرطة العلمية والتقنية - مديرية الشرطة القضائية- المديرية العامة للأمن الوطني - ص02-03.

قسم، غير أن الارتفاع الملحوظ لعدد القضايا الناتجة عن الجرائم المعلوماتية، بسبب الانتشار المتزايد لتقنية المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية هي:

أ. قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.

ب. قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

ج. قسم تحليل الأصوات.

تضم الدائرة في صفوفها ثمانية 08 أعضاء محققين أربع 04 منهم عناصر شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية، والبقية هم أعوان شبیهون، يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي، إضافة إلى إمامهم بالجانب القانوني، ومما يزيد من فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث والتحقيق في الجرائم المعلوماتية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الاطلاع على كل المستجدات القانونية منها والتقنية في مجال الإجرام المعلوماتية.¹

ومن مهام هذه المخابر ضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية في مجال التحريات الالكترونية، وذلك من خلال القيام بعمليات البحث عن المعطيات المشبوهة والمعلومات الرقمية على مختلف أشكالها: ملفات، رسائل الكترونية، برامج، صور،... هذا البحث يتم عن طريق استعمال برامج ووسائل خاصة تمكن من استرجاع كل المعطيات المحذوفة، والإطلاع على محتوى كل الوسائط الرقمية.²

1 حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص180.

2 مساهمة الشرطة العلمية والتقنية في مجال التحقيقات الجنائية - وثيقة خاصة صادرة عن مديرية الشرطة القضائية - المديرية العامة للأمن الوطني - ص46.

تلعب الدائرة دوراً مهماً للغاية في الكشف عن أسرار الجرائم المعلوماتية، من خلال مختلف الإجراءات التي تباشرها إما أثناء مرحلة البحث والاستدلال، أو أثناء مرحلة التحقيق القضائي.

فأما أثناء مرحلة البحث والتحري فإن أعضاء الدائرة عادة ما يستجيبون للطلبات التي يقدمها لهم عناصر الشرطة التابعون لفرق مكافحة الجرائم المعلوماتية الموزعة على كل مديريات الأمن الوطني، أو الطلبات وكيل الجمهورية أو قاضي التحقيق التي تردهم في شكل إنابة قضائية، من أجل دعمهم ومساعدتهم أثناء مرحلة المعاينة لمسرح الجريمة وكذلك لحجز الأدلة المتواجدة عليها.

أما أثناء مرحلة التحقيق القضائي فإن دور الدائرة لا يتعدى لأن يكون دور خبير، وذلك من خلا إعداد تقارير خبرة بناء على طلبات وكيل الجمهورية وبالخصوص قاضي التحقيق، كنتيجة لقيام المحققين بأعمال تحليل الأدلة المحجوزة والعمل على استخراج الأدلة الإلكترونية منها، كتحليل محتوى الأقراص الصلبة للحواسيب المستعملة في الجريمة، أو حواسيب الضحايا، وكذلك كل دعائم التخزين الإلكترونية بمختلف أنواعها وأشكالها، وكذلك المواقع التي تم اختراقها واستهدافها وصولاً إلى تحديد المواقع الجغرافي وعناوين المجرمين، وذلك بالاستعانة بوسائل مادية خاصة متطورة ذات جودة عالية¹.

وفي الأخير فإن ما يمكن قوله بهذا الخصوص أن المديرية العامة للأمن الوطني تولي أهمية بالغة في مجال مكافحة الإجرام المعلوماتي.

ثالثاً: على المستوى المحلي

في سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية، خلقت المديرية العامة للأمن الوطني سنة 2016 ما يقارب 48 فرقة لمكافحة الجرائم المعلوماتية على مستوى مصالحها

1 - حسين سعيداني، اليات التحقيق في الجرائم المعلوماتية، مرجع سابق، ص 181.

بأمن والولايات، يتمثل دورها في تلقي الشكاوى والبحث والحقيق في الجرائم المعلوماتية وتقريب الإدارة من المواطن.

الفرع الثاني: الوحدات التابعة للدرك الوطني

تضع قيادة الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية.

تعمل مؤسسة الدرك الوطني جادة إلى التطلع بمختلف الجرائم المرتكبة على شبكة الإنترنت وهذا لتسهيل مهمة البحث والمعاينة والتفتيش في أنظمة الحواسيب والعمل على مراقبة مختلف الشبكات وبالتالي فقد تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، وذلك حسب الاختصاص والصلاحيات وطبيعة الجريمة إلى ثلاث 03 مستويات مركزية، جهوية، محلية، وهو ما سنتناوله تبعا.

أولاً: على المستوى المركزي: تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم المعلوماتية ودعم أعمال البحث والتحقيق بشأنها من خلال الهيئات التالية:

أ. **مديرية الأمن العمومي والاستغلال:** وهي الهيئة التي تعمل على التنسيق بين مخلف الوحدات الإقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

ب. **المصلحة المركزية للتحريات الجنائية:** وهي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والاتصال¹.

1 معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني - البيض - الجزائر 3

ج. المعهد الوطني للأدلة الجنائية وعلم الإجرام: يعد المعهد الوطني للأدلة الجنائية وعلم الإجرام مؤسسة عمومية ذات طابع إداري، تم إنشاؤه بمرسوم رئاسي رقم 183—04 بتاريخ: 26 جوان 2004، في إطار عصرنه قطاع الدرك الوطني، وهو يشكل كذلك أداة مستلهمة من الخبرات التطبيقية والتحليل الحديثة والمدعومة بالتكنولوجيات المناسبة، يعد المعهد بمثابة هيئة مختصة في إجراء الخبرات والمعائنه وذلك بمختلف دوائره، بما فيها دائرة الإعلام الآلي ولإلكترونيك، التي أوكلت لها مهام تحليل الأدلة الخاصة بالجرائم المعلوماتية، و ن الخدمة الأساسية التي يقدمها هذا المعهد في هذا الشأن:

- القيام بالخبرات العملية أو الخبرات اللازمة في توجيه التحقيقات القضائية بطلب من القضاة بما فيها تلك المتعلقة بالجرائم المعلوماتية.
- مساعدة المحققين للسير الحسن للمعائنهات، عن طريق دعمهم الأفراد المؤهلين أثناء الحاجة.
- تنفيذ مناهج الشرطة العلمية والتقنية لجمع وتحليل الأدلة المأخوذة من مسرح الجريمة.
- ضمان المساعدة العلمية في التحريات المعقدة كحال التحريات الخاصة بالجرائم المعلوماتية.
- المشاركة في الأبحاث والتحليل المتعلقة بالوقاية للتقليل من جميع أشكال الإجرام بما فيها المعلوماتية.

تعتبر مشاركة ومساهمة المعهد الوطني للأدلة الجنائية وعلم الإجرام بصفته الهيئة المكلفة بالتحاليل والخبرات في ميدان علم الإجرام في وضع سياسة مكافحة الإجرام¹.

1 الموقع الرسمي لقيادة الدرك الوطني - تاريخ التصفح 31 مارس 2019 - الرابط الإلكتروني:

http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

د. مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية: أنشأ هذا المركز حديثاً ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية⁽¹⁾، إذ يوفر المساعدة التقنية للمحققين ويساهم في توجيه التحقيقات المرتبطة بتكنولوجيا الإعلام والاتصال، فهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والاستغلال لقيادة الدرك الوطني ويحقق المهام التالية:

1. ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت.
2. القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.
3. مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة في شبكة الأنترنت.
4. المشاركة في عمليات التحري والتسرب عبر شبكة الأنترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.
5. المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

إذن تعتبر هذه الهيئات التابعة للدرك الوطني مسؤولة عن تنفيذ إجراءات البحث والتحقيق بشأن الجرائم المعلوماتية، وذلك على نطاق وطني بحيث تعتبر هيئات دعم وإسناد ونقاط وصل بين مختلف الوحدات الأخرى المتخصصة والتي توجد كذلك على مستويات أدنى منها الجهوية والمحلية.

ثانيا: على المستوى الجهوي

تُعدّ أجهزة الشرطة القضائية الإقليمية التابعة للدرك الوطني ركيزةً أساسيةً في حفظ الأمن والنظام في جميع أنحاء البلاد. فهي تُنسّق بين مختلف الوحدات، مما يضمن تعاونًا سلسًا أثناء التحقيقات. وبفضل مواردها المتخصصة، تُعالج هذه الأجهزة قضايا مُعقّدة مثل الجرائم الإلكترونية والجريمة المنظّمة والإرهاب. ويتمتع كوادرها الواسعة بتدريب مُتقدّم وخبرة قانونية واسعة، مما يُمكنهم من إجراء تحقيقات دقيقة وجمع أدلة حيوية. وتلعب هذه الأجهزة دورًا حيويًا على الصعيد الوطني، حيث تدعم الإجراءات القضائية وتضمن تحقيق العدالة. وتجعلها خبراتها وقدراتها العملية لا غنى عنها في حماية السلامة العامة وتعزيز سيادة القانون.

ثالثا: على المستوى المحلي

تؤدي وحدات البحث التابعة للدرك الوطني، والمكونة من خبراء ذوي خبرة عالية، دورًا محوريًا في مكافحة الجريمة المنظمة، مع التركيز بشكل خاص على الجرائم الإلكترونية. تتولى هذه الفرق المتخصصة تحقيقات معقدة، وغالبًا ما تعمل بتعاون وثيق مع الوحدات الإقليمية لضمان استجابة منسقة. وقد عززت جهودها بشكل كبير قدرات الدرك في تحديد وتقنيك الشبكات الإجرامية العاملة في المجال الرقمي. وإدراكًا للطبيعة المتطورة للتهديدات الإلكترونية، أنشأ الدرك وحدات متخصصة في مكافحة جرائم تكنولوجيا المعلومات والاتصالات ضمن كل مجموعة إقليمية. هذه الوحدات المتخصصة مجهزة بأدوات وخبرات متقدمة، مما يسمح لها بوضع وتنفيذ سياسات فعالة لمكافحة التهديدات

الإلكترونية. ويُعد نهجها الاستباقي أمراً بالغ الأهمية لحماية الأمن الوطني وحماية المواطنين من الجرائم الرقمية.¹

المبحث الثاني: الإجراءات القانونية للتحري والكشف عن الجريمة المعلوماتية

لمواجهة التحديات المتزايدة التي تفرضها الجرائم المعلوماتية، أصبح من الضروري اعتماد آليات قانونية فعّالة تُمكن من الكشف عنها وتتبع مرتكبيها. وتختلف هذه الآليات بين ما هو تقليدي اعتمدته الجهات القضائية منذ سنوات، وما هو حديث فرضته طبيعة الجريمة الرقمية وتطور تكنولوجيا المعلومات. وفي هذا السياق، سيتم التطرق إلى الإجراءات الكلاسيكية المعتمدة في الكشف عن الجرائم المعلوماتية (المطلب الأول)، ثم إلى الإجراءات الحديثة التي تم تطويرها لمواكبة هذا النوع الجديد من الإجرام (المطلب الثاني).

المطلب الأول: إجراءات التحري الكلاسيكية للكشف عن الجريمة المعلوماتية

تشمل إجراءات التحري الكلاسيكية المعتمدة في الكشف عن الجرائم المعلوماتية تلك الوسائل القانونية المألوفة في الجرائم التقليدية. وتُعتبر المعاينة والتفتيش من أبرز هذه الإجراءات، حيث يلجأ إليها المحققون لجمع الأدلة وتحديد طبيعة الجريمة ومكان وقوعها. رغم أن طبيعة الجريمة المعلوماتية تختلف من حيث الوسيلة والبيئة، إلا أن هذه الإجراءات تظل ضرورية كأساس أولي للتحري. وتُستخدم المعاينة لتحديد المعطيات التقنية المرتبطة بالجريمة، في حين يُعد التفتيش وسيلة للوصول إلى الأدلة الرقمية المخزنة على الأجهزة الإلكترونية. ورغم محدودية فعاليتها في بعض الحالات التقنية المعقدة، فإنها تظل جزءاً لا يمكن الاستغناء عنه في المسار القانوني للتحقيق. وعليه سوف نبرز هذه إجراءات

1 معلومات مقدمة من قبل الفرقة الإقليمية للدرك الوطني - البيض - الجزائر.

في فرعين، يتمثل في معاينة مسرح جرائم الماسة بأنظمة المعلوماتية (الفرع الأول)، والى تفتيش أنظمة المعالجة الآلية للمعطيات وضبطها (الفرع الثاني). كما يلي:

الفرع الأول: معاينة مسرح جرائم الماسة بأنظمة المعلوماتية

يُعدّ فحص مسرح الجريمة خطوة جوهرية في التحقيق في الجرائم الإلكترونية، ويشمل معاينة دقيقة للموقع أو الأشخاص أو الأدوات ذات الصلة بالجريمة بهدف جمع الأدلة وتحليلها. يقوم بهذا الفحص ضابط شرطة قضائية مختص، ويساعد في الكشف عن معلومات حاسمة لدعم المحاكمة. رغم أن هذا الإجراء يطبق على جميع الجرائم، إلا أن المادة 61 من قانون الإجراءات الجزائية الجزائري¹ تجعله إلزامياً فقط في الجنايات الكبرى، بينما يبقى اختياريًا في حالات الجنح. يُمكن إجراء الفحص في الأماكن العامة دون إذن، أما في الأماكن الخاصة، فيشترط وجود إذن قانوني أو موافقة صاحب المكان، مما يضمن حماية الخصوصية وشرعية الإجراءات. ويضمن الالتزام بهذه البروتوكولات القانونية الحفاظ على سلامة الأدلة، وإجراء التحقيقات بشكل قانوني وأخلاقي. ولمعاينة مسرح الجرائم المعلوماتية، يجب التفرقة بين حالتين:

1 المادة 61 من قانون الإجراءات الجزائية الجزائري تنص على أن ضابط الشرطة القضائية يجب أن يُجري معاينة لمكان الجريمة في حالات الجنايات والجنح المتلبس بها، مع احترام شروط الدخول للمساكن الخاصة وفق القانون.

أولاً: معارضة الجرائم الواقعة على المكونات المادية للحاسوب (Hardware)

كشاشة العرض ومفاتيح التشغيل والأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسوس، فهي لا تثير أية مشكلة بحيث يمكن لضابط الشرطة القضائية معاينتها والتحقق على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.¹

ثانياً: معارضة الجرائم الواقعة على المكونات غير المادية أو بواسطتها (Software)

كذلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدته، وهذه الصعوبات، تتلخص فيما يلي:

- أ. قلة الآثار المادية المترتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب.
- ب. الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالباً ما تكون طويلة، وذلك بين اقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لإحداث تغييرات أو العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل المستقى من المعاينة.

ولنجاح المعاينة في الجرائم المعلوماتية يوصي الخبراء بوجوب إتباع ومراعاة قواعد وإرشادات فنية أبرزها ما يلي:

1 طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 2011، 1-2012، ص131.

- أ. القيام بتصوير الحاسوب وما قد يتصل به من أجهزة ظرفية ومحتوياته، وأوضاع المكان الذي يوجد به بصفة عامة مع التركيز على تصوير أجزائه الخلفية وملحقاته، ومراعاة تسجيل الزمان والتاريخ والمكان الذي التقطت فيه كل صورة.
- ب. يجب ملاحظة وإثبات الحالة التي تكون عليها توصيلات الكابلات (الخيوط الكهربائية للحاسوب)، والتي تكون متصلة بمكونات النظام، حتى يسهل القيام بعملية مقارنة وتحليل لها عند عرض الموضوع على المحكمة.
- ج. عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة، وذلك قبل إجراء الاختبارات اللازمة للتأكد من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة ومحو للبيانات المسجلة.¹
- د. وضع مخطط تفصيلي للمنشأة الواقعة بها الجريمة مع كشف تفصيلي بالمسؤولين بها ودور كل واحد منهم.
- هـ. ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.
- و. التحفظ على ما تحتويه سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة، والأشرطة والأقراص الممغنطة غير السليمة أو المحطمة وفحصها، ورفع البصمات التي قد تكون لها صلة بمرتكبي الجريمة.

1 طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 2011، 1-2012، ص131.

ز. القيام بحفظ المستندات الخاصة بالإدخال، وكذا مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة، وذلك من أجل رفع البصمات التي قد تكون موجودة عليها¹.

الفرع الثاني: تفتيش أنظمة المعالجة الآلية للمعطيات وضبطها

يُجرى البحث لجمع أدلة حاسمة مرتبطة بالجريمة، وتُعدّ أي مواد مُصدرة دليلاً مباشراً على الجريمة. يُعدّ ضبط المواد الرقمية والمادية واحتجازها وحفظها إجراءات تحقيقية أساسية في الجرائم الإلكترونية، إذ تُساعد سلطات إنفاذ القانون على تأمين الأدلة المحتملة قبل تعديلها أو إتلافها. تُعد هذه الخطوات حيوية لضمان نزاهة التحقيق، وتسهيل التحليل الدقيق، ودعم تحقيق العدالة في نهاية المطاف، وهو ما سنبرزه فيما يلي:

أولاً: تفتيش نظم المعلوماتية

في إجراء تحقيقي قياسي، يُجرى فحص مادي شامل للحاويات لتحديد العناصر المتعلقة بالجرائم الإلكترونية. تلتزم هذه العملية التزاماً صارماً بالبروتوكولات القانونية المعمول بها، مما يضمن الحصول على التصاريح اللازمة. تُولى اعتبارات خاصة لعمليات تفتيش المكونات، مما يسمح بإجراء فحص دقيق عند الضرورة، مع الالتزام بالقوانين واللوائح المعمول بها.² وهي:

1 - طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 2011، 1-2012، ص131.

2 يمل الحاسوب الآلي المحل الرئيسي للتفتيش في نظم المعلوماتية، وينصب التفتيش على المكونات المالية: وهي مجموعة من الوحدات لكل منها وظيفة محددة وتصل مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل، وتسمى بمعدات الحاسوب وهي: وحدات الإخال، وحدة الذاكرة الرئيسية، وحدة ذاكرة القراءة، وحدة الحاسوب والمنطق، الشاشة، وحدة التحكم، وحدة الذاكرة المساعدة، وحدة الإخراج، الطابعة، أنظر: طارق إبراهيم الدسوقي عطية، الامن المعلوماتي ، دار الشر الجديدة اسكندرية، سنة 2009، ص 441.

الحالة الأولى: تخضع المكونات الموجودة في أماكن خاصة، مثل المساكن، لقوانين تفتيش المساكن الخاصة وضمانات قانونية مُنشأة بموجب تشريعات مختلفة. تضمن هذه الحماية الحفاظ على حقوق خصوصية الأفراد، وتمنع عمليات التفتيش غير القانونية أو الاقتحامات من قبل السلطات أو جهات خارجية.

الحالة الثانية: في الوضع الاعتيادي، يُشكّل عزل مكونات الحاسوب أو ربطها بأجهزة بعيدة تحديات كبيرة في كشف البيانات وتحليلها. وقد تُعيق هذه التكوينات القدرة على فحص النظام والتحقق من سلامته بدقة، مما قد يجعل التقييمات الشاملة مستحيلة. لذا، من الضروري وضع قيود وضمانات قانونية تُنظّم عملية التفتيش. تضمن هذه الإجراءات إجراء جميع الإجراءات بشكل أخلاقي وآمن، مع حماية خصوصية المستخدم والحفاظ على سلامة النظام. وتساعد الإرشادات السليمة على منع الوصول غير المصرح به، وضمان الامتثال للوائح، وتعزيز الثقة في عملية التفتيش عند التعامل مع الأجهزة البعيدة أو المترابطة.¹

وقد حذا المشرع الجزائري حذو معظم التشريعات المعاصرة، بأن قرر المادة 65 مكرر 5 وما يليها من قانون الإجراءات الجزائية التي تسمح إذا اقتضت ضرورات التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات باعتراض المراسلات وتسجيل الأصوات والنقاط الصور.

الحالة الثالثة: وفقاً للمبادئ القانونية المتعارف عليها، لا يجوز تفتيش مكونات الحاسوب الموجودة في الأماكن العامة، كالمطاعم أو سيارات الأجرة، إلا بإذن صريح، بما يتماشى مع نفس الحماية والقيود

1 طرشي نورة، المرجع السابق، ص115.

المطبقة عند تفتيش الأفراد. ويجب أن تلتزم هذه الإجراءات بالضمانات المقررة، بما يضمن احترام حقوق الخصوصية وإجراء عمليات التفتيش بشكل قانوني وبتصريح مناسب¹.

ثانيا: تفتيش نظم الحاسوب المنطقية أو المعنوية

يعرف الكيان المنطقي للحاسوب بأنه: "مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"².

وفقاً للمادة 47، الفقرة الرابعة، من قانون الإجراءات الجزائية الجزائري، يتمتع قضاة التحقيق بسلطة تفتيش ومصادرة البيانات والأنظمة الحاسوبية في جميع أنحاء البلاد في أي وقت. يخول هذا الحكم القضاة إصدار أوامر تُمكن مسؤولي إنفاذ القانون من الوصول إلى المعلومات الرقمية الضرورية للتحقيقات الجارية. تضمن هذه الإجراءات قدرة السلطات على مكافحة الجرائم الإلكترونية بفعالية وجمع الأدلة اللازمة، مما يعزز الإطار القانوني للتحقيقات الرقمية على الصعيد الوطني.

ثالثا: القواعد الشكلية لتفتيش نظم المعلوماتية

تتلخص هذه القواعد كما يلي:

أ/ إجراء التفتيش بحضور أشخاص معينين بالقانون: بموجب الإطار القانوني الجزائري، والمنصوص عليه تحديداً في المادة 45 من قانون الإجراءات الجزائية، تخضع عمليات التفتيش التي تجريها السلطات لضمانات إجرائية صارمة. تتطلب هذه الإجراءات مشاركة المتهم أو ممثله القانوني، بما يضمن حماية

1 طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي ، دار النشر الجديدة الإسكندرية، سنة 2009، ص385.

2 غففي كامل غففي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007.

حقوقهما طوال العملية. بالإضافة إلى ذلك، يجب على ضابط الشرطة القضائية الإشراف على التفتيش للحفاظ على الشرعية وحسن السلوك. وعند الضرورة، يجوز حضور شاهدين لضمان الشفافية والمساءلة. تعمل هذه القواعد على دعم مبادئ الشرعية والإنصاف واحترام الحقوق الفردية أثناء إجراءات التحقيق. ومع ذلك، من المهم ملاحظة أن هذه الحماية الإجرائية لا تشمل الجرائم الإلكترونية أو القضايا التي تنطوي على بيانات رقمية. في مثل هذه الحالات، غالبًا ما تُطبق بروتوكولات مختلفة، مما يعكس الطبيعة الفريدة للأدلة الرقمية والتحديات التي تشكلها لإجراءات التحقيق التقليدية.

ب/ إعداد محضر خاص بالتفتيش: ويكون بتكليف القائم بالتفتيش باصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط، تسجل فيه جميع وقائع التحقيق بالتفصيل، وذكر البيانات والأشياء والوثائق التي يتم ضبطها بكل أمانة ودقة وحرص.

ت/ إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده: تتطلب عمليات فحص الأنظمة الفعالة نهجًا احترافيًا ومنهجيًا يُركّز على الدقة والشمول. تبدأ هذه العملية بتحديد دقيق للنظام، مما يضمن فهمًا واضحًا لبنيته ومكوناته. يُعدّ الإلمام التام بمبادئ علوم الحاسوب أمرًا أساسيًا لتفسير التكوينات المعقدة وتحديد نقاط الضعف المحتملة. ويلعب التعاون مع خبراء الأنظمة ذوي الخبرة دورًا حاسمًا، إذ يوفر وصولًا قيمًا ورؤى ثاقبة للبنى المعقدة التي قد يتعذر الوصول إليها لولا ذلك. يساعد إجراء تحليل شامل لمكونات الأجهزة والبرمجيات على كشف الثغرات الأمنية التي قد تُعرض الأمان للخطر. وتُعد معالجة هذه المشكلات بشكل استباقي أمرًا بالغ الأهمية للحفاظ على سلامة النظام بأكمله وأمنه. وفي نهاية

المطاف، يضمن النهج المنضبط والمستتير حمايةً قويةً من التهديدات الناشئة، ويعزز أداءً موثوقاً للنظام¹.

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش يجب على القائم بالتفتيش اتخاذ الخطوات التالية عند تنفيذ إذن التفتيش والتي تتلخص في ما يلي:

1. تأمين حماية مسرح الجريمة، بضمان فصل القوة الكهربائية عن موقع المعاينة وأجهزة خادمة شبكة الانترنت، لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير على آثار الجريمة.
2. إبعاد المتهم عن مكان النظام إن كان قريباً منه.
3. أخذ الحيطة لمنع تمكن المتهم من الدخول عن بعد للنظام المعلوماتي.
4. الدخول إلى الموقع ببطء، لكي لا يتم تشويه أو إتلاف الدليل.
5. عدم لمس لوحة المفاتيح، لأن ذلك قد يستلزم استخدام برامج أخرى احتيالية أ صعبة.
6. يجب العناية بالملاحظات وكلمات السر ورموز الشفرة إلى غيرها من العمليات والإجراءات الفنية التي تساعد على الكشف عن الجريمة المراد إثباتها².

في سياق القانون الجزائري، لا يُحدد المُشرع إطاراً زمنياً مُحددًا لإجراء عمليات تفتيش أنظمة الحاسوب. بل إن النهج القانوني السائد يمنح المُحققين سلطة تقديرية مُعينة لتحديد التوقيت المُناسب لهذه العمليات. وتتبع هذه المرونة من إدراك أن الجرائم الإلكترونية غالباً ما تقع ليلاً، حيث تكون قنوات الاتصال أقل ازدحاماً، ويكون الوصول إلى الأنظمة الرقمية أسهل في كثير من الأحيان، ويكون نشاط المُستخدمين

1 طرشي نورة، المرجع السابق، ص125.

2 عفيفي كامل عفيفي، المرجع السابق، ص65.

في أدنى مستوياته. ويهدف القانون، من خلال منح هذه السلطة التقديرية، إلى تسهيل إجراءات التحقيق الفعّالة مع مراعاة الواقع العملي لعمليات الجرائم الإلكترونية. ويتماشى هذا النهج مع الأحكام الواردة في المادة 47 من قانون الإجراءات الجزائية الجزائري، التي تُشدد على أهمية اتخاذ إجراءات تحقيقية مُرنة لتحقيق العدالة في المجال الرقمي.¹

المطلب الثاني: إجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية

تطور الجريمة المعلوماتية وتعقيد أساليب ارتكابها فرض على المنظومة القانونية الوطنية تحديث آليات التحري والتتبع، بما يواكب التطورات التكنولوجية المتسارعة. وقد جاء التعديل الذي أدخله القانون 06/22 المؤرخ في 20 ديسمبر 2006 على قانون الإجراءات الجزائية، استجابة لهذا التحدي، حيث نص على جملة من الإجراءات المستحدثة المخصصة للكشف عن الجرائم المرتبطة بأنظمة المعالجة الآلية للمعطيات. وسيتطرق في هذا المطلب إلى فرعين، الفرع الأول يتمثل في الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، والفرع الثاني يتمثل أسلوب التسرب أو الاختراق.

الفرع الأول: الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

يمنح القانون الجزائري للشرطة القضائية صلاحية اعتراض الاتصالات وتسجيل الأصوات والتقاط الصور في إطار التحقيقات بالجرائم الإلكترونية، مع مراعاة احترام الحياة الخاصة. تُعد هذه الوسائل فعالة لكنها قد تمس بحرمة المراسلات والحرية الشخصية، وهو ما يثير جدلاً قانونياً وأخلاقياً. المادة 03 من القانون 04/09 تشترط أن تتم هذه الإجراءات وفقاً لضوابط محددة، أبرزها إذن من وكيل الجمهورية. يميز الفقه بين اعتراض المكالمات دون علم الشخص، والمراقبة بطلب منه. نصت المادة

1 طرشي نورة، المرجع السابق، ص126.

65 مكرر 5 على حصر الجرائم التي تُجيز استخدام هذه الوسائل. رغم فائدتها في التحقيق، فرض المشرع ضوابط صارمة لضمان الشرعية، منها السر المهني وعدم التعسف، وهو ما سنشير إليه على النحو التالي:

أولاً: مباشرة التحري بإذن من وكيل الجمهورية

لم يسمح المشرع بإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بقصد التحري والتحقيق عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إلا بإذن من وكيل الجمهورية المختص، وتباشر هذه العمليات تحت مراقبته، وهذا ما قرره المادة 04 من القانون 04/09 التي جاء فيها أنه: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة." ويجب أن يتضمن الإذن كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء أكانت سكنية أو غير سكنية، كما يجب أن يتضمن نوع الجريمة التي تبرر اللجوء إلى هذه التدابير ومدة هذه التدابير¹، لذلك فإن الإذن المسلم من قبل وكيل الجمهورية للتحقيق في جريمة ما لا يصلح للتحقيق في جريمة أخرى، إلا بإذن جديد، كذلك يجب أن يتضمن الإذن كل الأماكن التي توضع فيها الترتيبات التقنية من أجل التقاط وتسجيل وتثبيت الكلام المتقوه به بصفة خاصة من شخص أو عدة أشخاص².

وعند مباشرة التحريات والتحقيقات، يحزر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص، محضر عن كل عملية اعتراض للمراسلات وتسجيل الأصوات والتقاط للصور،

1 المادة (65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

2 المادة (65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

وحتى عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتسجيل الصوتي أو السمعي البصري، كما يذكر في المحضر تاريخ وساعة بداية هذه العمليات والانتهاؤها منها¹، نحث يشتمل المحضر على كل البيانات المذكورة سابقا وتكون محددة تحديدا نافيا للجهالة، ويجب أن يشتمل المحضر على توقيع محرره في نهايته²، بعد أن يصنف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب، المراسلات أو الصور أو المحادثات المسجلة أو المفيدة في إظهار الحقيقة في محضر يودع بملف المتهم، وننسخ وتترجم المكالمات التي تتم باللغات الأجنبية عند الاقتضاء، بمساعدة مترجم يسخر لهذا الغرض³

ثانيا: التزام السر المهني

تكون إجراءات التحري والتحقيق سرية، ومن ثم فإن بحثها ضمن الضمانات الممنوحة للمتهم⁴، والسرية تعني القيام قدر الإمكان ممن هو قائم بالتحري أو كلف بإجراء من إجراءاته أو ساهم فيه بالمحافظة على السر المهني، وبالتالي صارت السرية ليس هدفها كما كان عليه من قبل هو تسهيل قمع المتهم، بل صارت وسيلة لضمان الحريات الشخصية⁵.

فقد نص المشرع صراحة على أن هذه العمليات تتم بمراعاة السر المهني ودون المساس به⁶، فالضابط المأذون له باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، ملزم قانونا بكتمان السر

1 المادة (65 مكرر 9) الأمر رقم 155/66 المعدل والمتمم بموجب المدة (14) من القانون رقم 22/06.

2 كمال كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، مصر، 2000، ص 271.

3 المادة (65 مكرر 10) الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

4 المادة (11) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

5 سهيلة بوزيرة، مواجهة الصفقات العمومية المشبوهة، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة جيجل، 2008،

ص 127

6 المادة (65 مكرر 7) الأمر رقم 155/66 المعدل والمتمم بموجب المدة (14) من القانون رقم 22/06.

المهني ويجب أن يتخذ مقدا التدابير اللازمة لضمان احترام ذلك السر¹، وقد نص قانون الإجراءات الجزائية على أن تكون إجراءات التحري والتحقيق سرية²، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع، وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه، لذلك فعملية التحري عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات تتم بسرية مطلقة، فيمنع منعاً باتاً أن يخبر المشتبه فيه بهذه التحريات أو أي شخص آخر، كذلك يمنع على ضابط الشرطة المأذون له أو المناب أن يفصح عن مضمون محضر التحريات لأي شخص كان، وإلا وقع تحت طائلة الجزاء الجنائي بتهمة إفشاء السر المهني، فيجب على ضباط الشرطة القضائية ومروؤسيهم عدم إفشاء الأسرار التي جمعوها أثناء التحريات، لأن سمعة المواطنين لا يجوز أن تظل مهددة ببيانات غير مؤكدة.

الفرع الثاني: أسلوب التسرب أو الاختراق

في ظل تطور أشكال الجريمة، لاسيما الجرائم المعلوماتية، أصبح من الضروري إرساء آليات تحرّ فعالة ومواكبة لهذا التطور، وهو ما دفع المشرّع الجزائري إلى تبني تقنية "التسرب" ضمن تعديل قانون الإجراءات الجزائية سنة 2006، وذلك كوسيلة استثنائية هدفها تعقب الجريمة من الداخل، دون المساس بالضمانات القانونية المكفولة للأفراد. ويمكن تحليل هذا الإجراء من خلال نقطتين أساسيتين:

1 المادة (45/ 3) من الأمر رقم 155/66 المعدل والمتمم بموجب المادة (14) من القانون رقم 22/06.

2 المادة (11) الأمر رقم 155/66 معدل ومتمم.

أولاً: شروط وضوابط تنفيذ التسرب

يُعتبر التسرب تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، عندما تقتضي ضرورات التحري والتحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر 5)¹. كما يجوز لوكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن شروط محددة.

ويُشترط حصول الضابط المكلف بالتسرب على الإذن من وكيل الجمهورية المختص، ويجب أن تتم العملية تحت إشرافه ومراقبته. فإن قرر ضابط الشرطة القضائية مباشرة هذا الإجراء، وجب عليه أولاً إخطار وكيل الجمهورية بذلك، ثم يقوم بمنحه إذنًا مكتوبًا لضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، على أن يتم ذكر هويته فيه، وهذا تحت طائلة البطلان المطلق. ويجب أن يكون الإذن مكتوبًا ويتضمن كل ما يتعلق بعملية التسرب وكذلك هوية ضباط وأعوان الشرطة المأذون لهم بالتسرب.

والتسرب هو قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه فيهم، بإيهامهم أنه فاعل معهم أو شريك لهم. فالتسرب إذاً هو قيام المأذون له بالتحقيق في الجريمة بمراقبة الأشخاص المشتبه في ارتكابهم جريمة، أو التوغل داخل جماعة إجرامية بإيهامهم أنه شريك لهم.

1 قانون الإجراءات الجزائية المعدل والمتمم. الأمر رقم 66-155 المؤرخ في 8 جوان 1966، المعدل بالأمر رقم 06-22 المؤرخ في 20 ديسمبر 2006، المادة 65 مكرر 5.

ويسمح لضباط وأعوان الشرطة القضائية بأن يستعملوا لهذا الغرض هوية مستعارة، وأن يرتكبوا عند الضرورة بعض الجرائم، دون أن يكونوا مسؤولين جزائياً، وذلك بهدف مراقبة أشخاص مشتبّه فيهم وكشف أنشطتهم الإجرامية، بإخفاء الهوية الحقيقية.

ثانياً: الضمانات القانونية وحدود صلاحيات المتسرب

يجوز لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب، والأشخاص الذين يُسَخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائياً، القيام بما يلي:

أ. اقتناء، أو حيازة، أو نقل، أو تسليم، أو إعطاء مواد، أو أموال، أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

ب. استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي، وكذا وسائل النقل، أو التخريب، أو الإيواء، أو الحفظ أو الاتصال.

ج. ويُحظر على المتسرب إظهار الهوية الحقيقية في أي مرحلة من مراحل الإجراءات مهما كانت الأسباب، إلا لرؤسائهم السلميين، لأن هذا سيؤدي إلى إفشال الخطة المتبعة في القبض على المشتبه فيهم وتعريض العضو المكشوف عن هويته للخطر.

وقد أكد المشرع ذلك بموجب المادة (65 مكرر 16)¹، حيث نص صراحة على أنه:

"لا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات."

1 قانون الإجراءات الجزائية المعدل والمتمم. الأمر رقم 66-155 المؤرخ في 8 جوان 1966، المعدل بالأمر رقم 06-22 المؤرخ في 20 ديسمبر 2006، المادة 65 مكرر 16.

كما عاقب المشرع كل من يكشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات، وبغرامة من 50.000 دج إلى 2.000.000 دج.

وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، فتكون العقوبة الحبس من خمس (5) سنوات إلى عشر (10) سنوات والغرامة من 200.000 دج إلى 500.000 دج.

أما إذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص، فتكون العقوبة الحبس من 10 إلى 20 سنة والغرامة من 500.000 إلى 1.000.000 دج.

ورغم أن المشرع أجاز مثل هذه الأفعال، التي تُعد في أصلها جرائم، من أجل خلق الثقة وتعزيزها في ضباط الشرطة القضائية وأعوانهم المرخص لهم بإجراء عملية التسرب من قبل المشتبه فيهم، والنجاح في إيهامهم بأنهم شركاء أو فاعلون، إلا أنه منع هؤلاء الضباط أو الأعوان من أن يُحرّضوا المشتبه فيهم على ارتكاب الجريمة. بمعنى أن المشرع يمنع على الضباط والأعوان المتسربين أن يخلقوا الفكرة الإجرامية للشخص الموضوع تحت المراقبة ويدفعوه لارتكاب الجريمة، لأن ذلك يُعد سبباً لبطلان الإجراء.

خلاصة الفصل

خصص هذا الفصل لدراسة آليات وإجراءات التحري في مجال الجريمة المعلوماتية، وتطرقنا فيه الى الأجهزة المختصة المكافحة للجريمة المعلوماتية والمتمثلة في الهيئة الوطنية للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام والاتصال، الأجهزة الأمنية سواء الامن الوطني أو الدرك الوطني سواء على المستوى الوطني أو الجهوي أو المحلي، ثم بعد ذلك تم التطرق الى الإجراءات القانونية للتحري من أجل الكشف ومكافحة الجريمة المعلوماتية، التي تكمن المحقق من التعرف على الجاني وتوقيفه وتقديمه أمام النيابة العامة لأخذ جزاءه.

الخاتمة

سعيًا من المشرع لتدارك الفراغ التشريعي الذي وقع فيه بخصوص مجال مكافحة الجرائم المعلوماتية، قد قام بإدراج تعديلات خاصة على قانون العقوبات الجزائري، وإستحدث قانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، محاولة منه للتقليص من هذه الجرائم المستحدثة والعابرة للحدود.

ويمكن اجمال نتائج الدراسة في النقاط التالية:

1. الجرائم المعلوماتية من بين الجرائم المستحدثة والعابرة للحدود.
2. هي من الجرائم المختلفة من حيث خصائصها عن الجريمة التقليدية، كما أنها صعبة الإثبات والاكتشاف كما يقل الإبلاغ فيها.
3. الجرائم المعلوماتية من بين الجرائم التي لا يتطلب فيها العنف على الإطلاق ويتصف المجرم المعلوماتي فيها بالذكاء والسرعة كذلك يكون متميزا بالدقة والتخصص في مسائل تكنولوجيا المعلومات.
4. هي من بين الجرائم التي تتوافق مع غيرها من الجرائم في مدى توفر القصد الجنائي العام.
5. إسرار الدولة إلى إيجاد حلول قانونية ردعية للحد من انتشار هذه الجريمة، كذلك تسخير الكفاءات البشرية للوقاية من تأثير هذه الجرائم على الأمن العام وكذا حماية المواطنين من خطورتها.

ونجمل الاقتراحات فيما يلي:

1. استحداث تعريف قانوني خاص لهذا النوع المستجد من الجرائم، نظرا لازديادهم وخطورته، الأمر الذي يستوجب إضفاء تعريف يبين نوعية الجريمة لعدم الوقوع في الخطأ خاصة من ناحية التكييف.

2. على المشرع أن يقوم بتطوير بنيته التشريعية تماشياً مع التطور السريع والملحوظ لهذه الجريمة.
3. إنشاء أقسام متخصصة بالجرائم المعلوماتية.
4. ضرورة تخصيص شرطة جنائية خاصة وخبراء من ذوي الكفاءة العالية في مجال الأنترنت.
5. توفير الوسائل والأجهزة المسخرة والمتنوعة لقمع الجريمة وتطوير قاعدة البيانات لتتماشا مع الجريمة وتطورها.
6. ضرورة إبرام معاهدات واتفاقيات دولية لردع الجريمة المعلوماتية.
7. على السلطات المختصة الإكثار من الحملات التوعوية للمواطنين من أجل وضعهم في الصورة لتوخي الحيلة والحذر من هذه الجرائم التي تتزايد أكثر فأكثر.

قائمة المصادر والمراجع

أولاً: الدساتير

1. دستور الجمهورية الجزائرية الديمقراطية الشعبية الصادر بتاريخ 1996/11/28 الجريدة الرسمية العدد 76 الصادرة في 1996/12/08 معدل ومتمم بقانون 01/16 المؤرخ في 2016/03/06 جريدة رسمية رقم 14 الصادرة في 2016/03/07 والمعدل في 2020/12/30 جريدة رسمية العدد 82.

ثانياً: القوانين والأوامر

1. القانون رقم 15-04 مؤرخ في 10 نوفمبر 2004، يتضمن تعديل قانون العقوبات.
2. القانون رقم 06/23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية.
3. القانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثالثاً: المراسيم التنفيذية

1. المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الكتب بالعربية:

الكتب الخاصة:

1. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية 2006.
2. أسامة احمد المناعة، جلال محمد الزغبى، جرائم تقنية نظم المعلومات الالكترونية، الطبعة الثالثة، دار النشر والتوزيع، عمان 2014.
3. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة، الجزائر، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، الجزائر 2007.
4. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.
5. حنان ربحان مبارك المضحاكي، الجرائم المعلوماتية، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت 2014.
6. خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنات، الطبعة الاولى، دار الثقافة للنشر والتوزيع، عمان 2011.
7. خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، عين مليلة، الجزائر، 2010.
8. طارق إبراهيم الدسوقي عطية، الامن المعلوماتي ، دار الشر الجديدة الاسكندرية، سنة 2009.
9. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007.
10. محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004.

11. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، سنة 2008.
12. منير محمد الجنبهي ممدوح محمد الجنبهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.
13. نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2 ، دار الثقافة للنشر والتوزيع.
14. هدى قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.
15. هشام محمد فريد رستم، العقوبات ومخاطر جرائم المعلوماتية، دار النهضة العربية، القاهرة، 2000.

الكتب العامة:

1. بلعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، الطبعة الأولى، دار الخلدونية، الجزائر، 2007.
2. حسن صادق المرصفاوي، المرصفاوي في التحقيق الجنائي، الطبعة الثانية، منشأة المعارف، الإسكندرية، مصر، 1990.
3. خلفي عبد الرحمن، محاضرات في قانون الإجراءات الجزائية، دار الهدى عين مليلة، الجزائر، 2010.
4. كمال كمال الرخاوي، إذن التفتيش فقها وقضاء، الطبعة الأولى، دار الفكر والقانون، المنصورة، 2000.

5. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثانية، الجزائر، 2009.

6. محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة الثامنة، دار الجامعة الجديدة، 2008.

مذكرات جامعية

1. بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة 16 و 17 نوفمبر 2015، كلية الحقوق جامعة بسكرة.

2. حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص - قانون العقوبات العلوم الجنائية، جامعة باتنة 1، السنة الجامعية 2015/2016.

3. سعيداني نعيم، اليات البحث والتحري عن الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، جامعة الحاج لخضر باتنة، سنة دراسية 2012/2013.

4. سهيلة بوزيرة، مواجهة الصفقات العمومية المشبوهة، مذكرة ماجستير في القانون الخاص، كلية الحقوق جامعة جيجل، 2008.

5. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، السنة 2011/2012.

6. عبد الكريم شيباني، الحماية الإجرائية والموضوعية للجريمة المعلوماتية، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة د. الطاهر مولاي، سعيدة، سنة 2015/2016.

الموقع الرسمي لقيادة الدرك الوطني - تاريخ التصفح 31 مارس 2019 - الرابط الإلكتروني:

http://www.mdn.dz/site_cgn/index.php?L=ar&P=undefined

الفهرس

II.....	إهداء
III.....	شكر وعرفان
1	المقدمة
7	الفصل الأول: الإطار المفاهيمي للجريمة المعلوماتية
8	المبحث الأول: ماهية الجريمة المعلوماتية
8	المطلب الأول: السياق المعرفي للجريمة المعلوماتية
9	الفرع الأول: تعريف الجريمة المعلوماتية
11.....	الفرع الثاني: خصائص الجريمة المعلوماتية
14.....	الفرع الثالث: أنواع الجريمة المعلوماتية
19.....	المطلب الثاني: أركان الجريمة المعلوماتية
20.....	الفرع الأول: الركن الشرعي
22.....	الفرع الثاني: الركن المادي
24.....	الفرع الثالث: الركن المعنوي
25.....	المبحث الثاني: الحماية الجنائية من خلال النصوص القانونية
26.....	المطلب الأول: موقف المشرع الجزائري من الجريمة المعلوماتية
26.....	الفرع الأول: مفهوم نظام المعالجة الآلية للمعطيات

29.....	الفرع الثاني: المقصود بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال
33.....	المطلب الثاني: جرائم الاعتداء الماسة بالأنظمة المعلوماتية.
34.....	الفرع الأول: الصور البسيطة للاعتداء على نظام المعالجة الآلية للمعطيات
38.....	الفرع الثاني: الصور المشددة للاعتداء على نظام المعالجة الآلية للمعطيات
42.....	الفصل الثاني: آليات وإجراءات التحري في مجال الجريمة المعلوماتية
43.....	المبحث الأول: الوحدات المختصة التي تتولى إجراءات البحث والتحقيق في الجريمة المعلوماتية
43.....	المطلب الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
44.....	الفرع الأول: التعريف بالهيئة واختصاصاتها
47.....	الفرع الثاني: تشكيلة الهيئة وطبيعة عملها
51.....	المطلب الثاني: الأجهزة الأمنية
51.....	الفرع الأول: الوحدات التابعة لسلك الأمن الوطني
55.....	الفرع الثاني: الوحدات التابعة للدرك الوطني
59.....	المبحث الثاني: الإجراءات القانونية للتحري والكشف عن الجريمة المعلوماتية
59.....	المطلب الأول: إجراءات التحري الكلاسيكية للكشف عن الجريمة المعلوماتية
60.....	الفرع الأول: معاينة مسرح جرائم الماسة بأنظمة المعلوماتية
63.....	الفرع الثاني: تفتيش أنظمة المعالجة الآلية للمعطيات وضبطها
68.....	المطلب الثاني: إجراءات التحري المستحدثة للكشف عن الجرائم المعلوماتية
68.....	الفرع الأول: الكشف بواسطة أسلوب اعتراض المراسلات وتسجيل الأصوات والتقاط الصور
71.....	الفرع الثاني: أسلوب التسرب أو الاختراق
76.....	الخاتمة
78.....	قائمة المصادر والمراجع
79.....	الفهرس
84.....	الملخص

الملخص

تُشكّل الجرائم الإلكترونية تحدياتٍ كبيرةً لإجراءات التحقيق التقليدية، مما يُعقّد جهود جمع الأدلة وحفظها بفعالية. ومع التطور السريع للتهديدات الرقمية، يجب على جهات إنفاذ القانون التكيف مع أساليب جديدة تُمكنها من مواكبة الجرائم الإلكترونية المُعقّدة. وقد اتخذت الجزائر خطواتٍ استباقية لمعالجة هذه القضايا من خلال تطبيق إصلاحاتٍ تشريعية. ففي عام 2006، صدر القانون رقم 06-22، الذي عدّل قانون العقوبات ليُعالج تحديدًا الجرائم التي تتطوي على أنظمة بيانات آلية، مُدرّكًا الطبيعة الفريدة للأدلة الرقمية. وفي وقتٍ لاحق، في عام 2009، صدر القانون رقم 04-09 لوضع قواعد مُخصصة للجرائم المُتعلقة بتكنولوجيا المعلومات والاتصالات، مُوفّرًا إطارًا قانونيًا أوضح للتحقيقات الرقمية. وقد أدخلت هذه القوانين آليات تحقيق مُتطورة، مثل الأدلة الجنائية الرقمية والدوريات الإلكترونية، بهدف تحسين فعالية إنفاذ القانون في الفضاء الإلكتروني. ومع ذلك، وعلى الرغم من فوائدها، فقد أثّرت مخاوف بشأن شرعية بعض التدابير وآثارها على الخصوصية، مما يُسلّط الضوء على النقاش الدائر حول الموازنة بين الأمن وحقوق الأفراد في العصر الرقمي.

Abstract:

Cybercrimes pose significant challenges to traditional investigative procedures, complicating efforts to effectively collect and preserve evidence. With the rapid evolution of digital threats, law enforcement must adapt to new methods to keep pace with complex cybercrimes. Algeria has taken proactive steps to address these issues through legislative reforms. In 2006, Law No. 22-06 was enacted, which amended the Penal Code to specifically address crimes involving automated data systems, recognizing the unique nature of digital evidence. Later, in 2009, Law No. 09-04 was enacted to establish specialized rules for crimes related to information and communication technologies, providing a clearer legal framework for digital investigations. These laws introduced advanced investigative mechanisms, such as digital forensics and electronic patrols, with the aim of improving the effectiveness of law enforcement in cyberspace. However, despite their benefits, concerns have been raised about the legality of some measures and their impact on privacy, highlighting the ongoing debate about balancing security and individual rights in the digital age.