جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون خاص

إجراءات البحث والتحري الخاصة في ظل تفشي الجريمة الإلكترونية في التشريع الجزائري

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: قانون جنائي والعلوم الجنائية

من إعداد الطالبتين:

كروم عونية مولات شيماء

جلايلي خديجة

تحت إشراف الأستاذ:

د. مرزوق محمد

أعضاء لجنة المناقشة

د. نابي عبد القادر	جامعة سعيدة	رئيساً
د. مرزوق محمد	جامعة سعيدة	مشرفاً ومقرراً
د. نقادي حفيظ	جامعة سعيدة	عضواً

السنة الجامعية: 2024-2025.

جامعة سعيدة، الدكتور مولاي الطاهر

كلية الحقوق والعلوم السياسية

قسم القانون خاص

إجراءات البحث والتحري الخاصة في ظل تفشي الجريمة الإلكترونية في التشريع الجزائري

مذكرة لاستكمال متطلبات الحصول على درجة ماستر في الحقوق

تخصص: قانون جنائي والعلوم الجنائية

من إعداد الطالبتين:

كروم عونية مولات شيماء

جلايلي خديجة

تحت إشراف الأستاذ:

د. مرزوق محمد

أعضاء لجنة المناقشة

د. نابي عبد القادر	جامعة سعيدة	رئيساً
د. مرزوق محمد	جامعة سعيدة	مشرفاً ومقرراً
د. نقادي حفيظ	جامعة سعيدة	عضواً

السنة الجامعية: 2024-2025.

إهـــداء

إلى والدي الحبيبين اللذين كانوا سبب في نجاحي أطال الله في عمرهما
إلى من كانت دعواتها سندًا في لحظات ضعفي، وابتسامتها أملًا لي (أمي) ،هذا الإنجاز لكِ، قبل أن يكون لي.دمتِ فخر قلبي وسبب كل نجاح أعيشه اليوم

أهدي نجاحي إلى من أحمل إسمه بكل فخر إلى مصدر إلهام و النجاح و قدوتي في هذه الحياة أبي الغالي

إلى أخي (عبد الكريم) الذي كان سندا و صديقا

إلى جدتي الغالية،
رمز الحنان والدعاء الصادق،
شكراً على دعواتك التي كانت ترافقني في كل خطوة،
وعلى وجودك معي أطال الله في عمرك

إلى عمي الغالي (كروم عثمان]الذي فقدناه حديثا و غادرنا جسداً، وبقي حياً في الذاكرة والدعاء،
أتذكرك بكل خير، وأهدي لك هذا العمل عرفاناً لما قدمته لي من دعم ومحبة في حياتك،
رحمك الله رحمة واسعة، وجعل مثواك الجنة
أتقدم بشكر إلى كافة أفراد عائلتي و كل من ساندني في مسيرتي

شيماء

إهـــداء

أهدي هذا العمل إلى أعز ما يملك الإنسان في هذه الدنيا إلى ثمرة نجاحي إلى من أوصى بهما الله سبحانه وتعالى (وبالوالدين إحسانا)

إلى الشمعة التي تحترق من أجل أن تضييئ أيامي إلى من ذاقت مرارة الحياة و حلوها إلى قرة عيني وسبب نجاحي و توفيقي في دراستي (أمي)

إلى الذي أحسن تربيتي و تعليمي و كان مصدر عوني و نوري و جلاء حزني و رمز عطائي و وجهني نحو الصلاح و الفلاح(أبي)

إلى اخوتي و جميع أفراد عائلتي و أصدقائي و صديقاتي شكرا لكم

خديجة

شكر وتقدير

الشكر و التقدير

الحمدلله على توفيقه و إحسانه و الحمد لله على فضله و إنعامه و الحمد لله على جوده و إكرامه نشكر الله عزوجل الذي أمدنا بعونه و وهبنا من فضله و مكننا من إنجاز هذا العمل و لا يسعنا إلا أن نتقدم بشكر الجزيل إلى كل من ساهم في تكويننا و الأخص بالذكر أستاذنا الفاضل **(مرزوق محمد)** الذي تكرم بإشرافه على هذه المذكرة و لم يبخل علينا بنصائحه الموجهة فكان لنا نعم الموجه و المرشد

قائمة المختصرات

ق: قانون

ج. ر. ج. ج: الجريدة الرسمية الجمهورية الجزائرية

ج.ر: جريدة رسمية

ع: عدد

ط: طبعة

ص: صفحة

مقدمة

مقدمة:

تُعد الجريمة المعلوماتية من أبرز الظواهر الإجرامية المعاصرة التي فرضت نفسها بقوة على الساحة القانونية والتقنية والاجتماعية، نظراً لما تطرحه من إشكاليات متعددة وتحديات غير مسبوقة. فقد أدّى التطور الهائل في تقنيات المعلومات والاتصال، والانتشار الواسع لاستخدام شبكة الإنترنت والوسائط الرقمية، إلى تغيّر طبيعة الجريمة وأساليب ارتكابها، حيث انتقلت من المجال الواقعي إلى المجال الافتراضي، وأصبح بالإمكان تنفيذ أفعال مجرّمة عن بُعد، باستخدام أجهزة الحاسوب أو الهواتف الذكية، دون الحاجة إلى الحضور المادي أو المباشر في موقع الجريمة.

وتنطوي الجرائم المعلوماتية على مجموعة من الأفعال التي تُرتكب باستخدام تقنيات رقمية، وتستهدف أنظمة الحواسيب، أو البيانات المخزنة، أو الاتصالات الإلكترونية، وتتنوع هذه الأفعال بين القرصنة(Hacking) ، سرقة البيانات، التزوير الإلكتروني، اختراق الحسابات البنكية، الاحتيال الإلكتروني، نشر الفيروسات، والتجسس السيبراني. وتكمن خطورة هذه الجرائم في كونها لا تقتصر على إلحاق الأذى بالأفراد فقط، بل تمتد لتطال المؤسسات الاقتصادية، والبنوك، والهيئات الحكومية، وحتى أمن الدولة ذاته، مما يجعلها جرائم عابرة للحدود، ذات تأثير دولي، قد يصعب أحيانًا تحديد الجاني أو الدولة المسؤولة عن التحقيق والملاحقة القضائية.

في ظل هذه التحولات الرقمية الكبرى، برزت الحاجة الماسّة إلى بناء منظومة قانونية متكاملة تعالج هذا النوع المستجد من الجرائم، وتوفر الحماية القانونية الكافية للمعلومات والبيانات، بما يضمن سرية الاتصالات وسلامة الشبكات الإلكترونية. وقد أولت التشريعات الحديثة، بما في ذلك التشريع الجزائري، اهتمامًا متزايدًا بمكافحة الجرائم المعلوماتية، من خلال إصدار قوانين خاصة، وتعديل القوانين الجنائية التقليدية، وإدماج الجرائم الرقمية ضمن منظومة التجريم والعقاب.

ويهدف هذا البحث إلى تسليط الضوء على الإطار العام للجريمة المعلوماتية، من خلال معالجة الجوانب المفاهيمية والقانونية المرتبطة بها، وتحليل أنواعها، ودوافعها، وطرق ارتكابها، إضافة إلى استعراض

أبرز التدابير الوقائية والتقنية والقانونية لمكافحتها. وسينقسم البحث إلى فصلين أساسيين: يتناول الفصل الأول الإطار المفاهيمي للجريمة المعلوماتية، ويُعنى بتحديد المفاهيم الأساسية ذات الصلة، وتوضيح طبيعتها القانونية وخصائصها المميزة عن الجرائم التقليدية، فيما يُركز الفصل الثاني على الحماية القانونية للجريمة المعلوماتية، سواء من حيث النصوص القانونية الوطنية والدولية، أو من حيث الوسائل والإجراءات العملية للكشف عنها والحد من انتشارها.

وتكمن أهمية هذا الموضوع في كونه يمس أحد أخطر التحديات التي تواجه المجتمعات الحديثة، في ظل الاعتماد المتزايد على الوسائط الرقمية في مختلف مناحي الحياة، من تعليم، وتجارة، وصحة، وإدارة، وتواصل اجتماعي. ومع ازدياد حالات الجرائم السيبرانية على الصعيد العالمي، بما في ذلك الجزائر، بات من الضروري دراسة هذا النوع من الجرائم دراسة معمقة، تستند إلى مقاربة شاملة تجمع بين الجوانب التقنية، القانونية، والاجتماعية، بهدف صياغة رؤية متكاملة لمكافحتها والحد من آثارها المدمّرة على الأفراد والمجتمع والدولة.

إن التغير السريع في طبيعة التكنولوجيا، وما يصاحبه من تطور في أساليب الجريمة الإلكترونية، يفرض تحديًا مستمرًا على المشرّع والجهات الأمنية والعدلية، ويجعل من الضروري تحديث المنظومة القانونية والتقنية لمواكبة هذا التطور، ووضع آليات تعاون دولي فعالة لمكافحة هذه الظاهرة العابرة للحدود. ومن هذا المنطلق، تكتسب دراسة الجريمة المعلوماتية راهنية وضرورة بالغة، سواء على المستوى الأكاديمي أو العملي، بما يُسهم في رفع مستوى الوعي القانوني، وتطوير السياسات العامة، وتعزيز الأمن السيبراني في الجزائر وفي العالم.

وتتمثل الإشكالية الرئيسية في هذا البحث في كيفية مواجهة التحديات القانونية التي تطرأ بسبب الجرائم المعلوماتية، ومدى قدرة التشريع الجزائري على توفير حماية فعالة ضد هذه الجرائم، خاصة في ظل تزايد استخدام الإنترنت ووسائل التواصل الحديثة. لذا، يطرح السؤال التالي :

هل استطاع المشرع الجزائري أو يواكب تطورات الجريمة المعلوماتية ويقدم حماية قانونية لها؟

تستهدف هذه الدراسة تحليل الجريمة المعلوماتية في التشريع الجزائري، ودراسة النصوص القانونية الخاصة بحماية البيانات والأمن السيبراني، بالإضافة إلى الكشف عن الجرائم المعلوماتية. سيتم التركيز على القوانين الجزائرية المتعلقة بالجريمة المعلوماتية، مثل قانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.

سيعتمد البحث على المنهج الوصفي التحليلي، حيث سيتم تحليل النصوص القانونية المتعلقة بالجريمة المعلوماتية وتقييم فعاليتها في التصدي لهذه الجرائم. كما سيتم استخدام المنهج المقارن لمقارنة التشريعات الجزائرية مع التشريعات الدولية مثل قوانين الاتحاد الأوروبي والأمم المتحدة في مجال مكافحة الجرائم الإلكترونية.

من أبرز الصعوبات التي قد تواجه البحث هي محدودية المصادر القانونية المتخصصة في الجريمة المعلوماتية في الجزائر، وصعوبة الحصول على بيانات دقيقة حول حجم الجرائم المعلوماتية في البلاد. كما أن تطور الجرائم المعلوماتية بشكل سريع يتطلب متابعة مستمرة للمتغيرات القانونية والتكنولوجية المرتبطة بالموضوع.

تناولنا في الفصل الأول الإطار المفاهيمي للجريمة المعلوماتية وما يتصل به من تعريفات وخصائص وأنواع، ثم يأتي الفصل الثاني ليعالج الجوانب القانونية والعملية المتعلقة بهذه الظاهرة، من خلال دراسة سُبل الحماية القانونية المقرّرة، وآليات الكشف عنها والتصدي لها، وذلك بهدف بيان مدى نجاعة المنظومة التشريعية في مواجهة هذا النوع المستحدث من الجرائم في ظل التطور التكنولوجي المتسارع.

الفصل الأول

الإطار المفاهيمي للجريمة المعلوماتية

شهد العالم في العقود الأخيرة تطورًا هائلًا في تكنولوجيات الإعلام والاتصال، ما أدى إلى ظهور نمط جديد من الجرائم يُعرف بـ"الجريمة المعلوماتية"، وهي جرائم ترتكب باستخدام الحواسيب والشبكات والأنظمة المعلوماتية. واستجابة لهذا الواقع المستجد، تدخل المشرع الجزائري بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009[1]، الذي وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومن أبرز ما جاء به هذا القانون إقرار أساليب حديثة للتحري والتقصي، تتماشى مع خصوصيات هذا النوع من الجرائم. إلا أن هذه الأساليب، رغم نجاعتها، طرحت إشكاليات قانونية تتعلق بمدى مشروعيتها ومدى احترامها للحقوق والحريات الأساسية. ومن هذا المنطلق، تبرز أهمية تحديد الإطار المفاهيمي للجريمة المعلوماتية كما ورد في هذا النص القانوني، لفهم أبعادها القانونية والإجرائية. ولهذا قمنا بتقسمه إلى مبحثين:

المبحث الأول ماهية الجريمة المعلوماتية

المبحث الثاني: الطبيعة القانونية للجريمة المعلوماتية

[1] قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 أوت سنة 2009، العدد 47. يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المبحث الأول: ماهية الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية فعل إجرامي يُرتكب باستخدام الأجهزة الإلكترونية أو يستهدف الأنظمة المعلوماتية، مثل الحواسيب أو الشبكات أو البيانات الرقمية. تشمل هذه الجرائم الاحتيال الإلكتروني، الاختراق، سرقة الهوية، نشر الفيروسات، والتجسس السيبراني. مع تطور التكنولوجيا وزيادة الاعتماد على الإنترنت، أصبحت هذه الجرائم تشكل تهديدًا كبيرًا للأفراد والمؤسسات والدول، مما يستدعي تطوير تشريعات وإجراءات أمنية للحد منها ومكافحتها.

المطلب الأول: التطور التاريخي للجريمة المعلوماتية

ظهرت الجريمة المعلوماتية مع تطور تكنولوجيا المعلومات والاتصالات، حيث بدأت بشكل بسيط ثم تطورت لتصبح من أكثر الجرائم تعقيدًا وخطورة. يمكن تقسيم تطورها التاريخي إلى عدة مراحل:

الفرع الأول: تطور الجريمة المعلوماتية مع تقدم التكنولوجيا

تشكل الجرائم الالكترونية واحدة من أخطر صور الإجرام في العصر الحالي، نظرا لارتباطها الكبير بالتطور التكنولوجي الحاصل على مختلف الأصعدة. وتعد الجرائم الإلكترونية جريمة ضد أجهزة الكمبيوتر ونظام المعلومات بهدف الحصول على وصول غير مصرح به والتحكم في الجهاز أو حرمان المستخدم أو المالك الشرعي من الوصول إلى النظام. كما قد يتم ارتكابها ضد الأشخاص من خلال الاستعانة بهذه الأجهزة والأنظمة لتشكل جرائم خبيثة شكلت معضلة للدول التي تسعى جاهدة لمكافحتها[1].

ويعد كلا من جريمتي الاحتيال الالكتروني والذم الالكتروني من الأمثلة البارزة على هذا النوع من الإجرام المستحدث، حيث تعد صور جديدة لجرائم كلاسيكية كانت معروفة مسبقا. وتتطلب هذه الجريمة كغيرها من أنواع الجرائم، توفر الركنين المادي والمعنوي، مع السعي الدائم للدول من أجل الحفاظ على مبدأ الشرعية من خلال تكريس الركن الشرعي لها عبر تجريم مختلف الأفعال المؤدية لها.

كان لحصول التطور التكنولوجي المعاصر وسيطرته على المجتمعات في كافة نواحي الأحياء، آثار إيجابية كثيرة، تمثلت على سبيل المثال وليس الحصر بانتشار في التقنية العالية، من برامج متقدمة،

[1] زهير خريبط خلف، الجريمة الالكترونية كوجه مستحدث من وجوه الجريمة، مجلة القرار للبحوث العلمية، العدد السادس، المجلد الثاني، السنة الأولى، حزيران يونيو 2024، متاح على الموقع: https://www.elqarar.com/، تم الإطلاع عليه يوم: 2025/02/22 على الساعة 14:30.

وحسابات آلية، أو الحاسب الآلي، وشبكات اتصال، ساهم في تقريب المسافات بين ملايين من البشر، وخلق فرصا جديدة سهلت من عملية الوصول إلى المعلومات، وتبادلها، حتى أصبح يسمى هذا العصر، بعصر المعلومات. فالكمبيوتر على سبيل المثال الذي زادت أهميته نتيجة التطور التكنولوجي الضخم، في شتى مجالات الحياة المعاصرة، فلم يعد يوجد فرع من أي نشاط إلا ويستخدم في معاملاته الكمبيوتر ومن أكثر الأنشطة التي تستخدم الكمبيوتر البنوك والشركات والهيئات والمطارات وغيرها، بل هناك من يرى بان المجتمعات المعاصرة ستصوت قريبا من خلال جهاز الكمبيوتر مباشرة. ومن ناحية ثانية، وللأسف، فقد أنتج هذا التطور أنواع جديدة من الجريمة تسمى الجريمة الإلكترونيةcyber crimes ، فقد أثر هذا التطور بخلق فرص جديدة للمجرمين، حيث مكنت مجرمي الفضاء الإلكتروني من تصفح الأنترنت وارتكاب جرائم مثل القرصنة، والاحتيال، والتخريب للكمبيوتر، والإتجار بالمخدرات، والتعامل في معلومات العدالة، والمواد الإباحية، دون القبض عليهم أو الكشف عن جرائمهم، فشكلت بالتالي أنماط جديدة ومتعددة من الإجرام المستحدث، كان أبطالها لصوص الحاسب الذين يدخلون إلى أنظمة الحاسب وقواعد المعلومات ويسرقونها، أو يعبثون بها، والجرائم التي تخترق الحماية الأمنية في النظم القانونية حيث يتم تجنب العقاب فيها.

أولاً: الجرائم الإلكترونية في تسعينات القرن العشرين

شهدت هذه المرحلة أنواعا فريدة من جرائم الكمبيوتر التي ظهرت بظهور الإنترنت منها الدخول غير المصرح به إلى نظام الكمبيوتر والعبث بمحتوياته وتدميرها والهجوم على مواقع معلوماتية وتدميرها، وشملت جرائم الكمبيوتر التجسس الصناعي والأمني والاستيلاء على بطاقات الائتمان البنكية واستخدامها بطريقة غير مشروعة وكذلك الإساءة إلى سمعة الأفراد وتحقيرهم عبر الرسائل الإلكترونية[1].

أما في الألفية الجديدة فإنها شهدت تزايدا في حجم الجرائم الإلكترونية ومن خلال ما سبق فإنه يتبين أن الجرائم الإلكترونية لها جذور تاريخية ترجع في ذلك إلى الأربعينيات والخمسينيات من القرن الماضي ولكنها لم تكن معروفة كما هي عليه الآن، حيث بدأت الآن الدول تتسابق في وضع التشريعيات

[1] عفاف بعون نسيمة أولاد سالم، الجريمة الإلكترونية – قراءة سوسيوتاريخية في النشأة والآثار، مجلة القبس للدراسات النفسية والاجتماعية، المجلد (05) العدد (20)، 2023، ص73-74.

التي تعمل على الوقاية والمكافحة من هذه الجرائم الالكترونية. وبنتيجة هذا التطور في عالم المعلوماتية نشأت ونمت أنواع جديدة من الجرائد التي ما كانت لتبصر النور لولا ظهور الكمبيوتر حيث شهدت التسعينيات والقرن الحالي أنواعا فريدة من جرائم الكمبيوتر وترافق ذلك مع ظهور الإنترنت وبدأت أنشطة الهاكرز باختراق مواقع المعلومات ونظمه عبر الإنترنت "، والدخول دون تصريح أو تخويل إلى النظم والعبث بالبيانات والمعلومات المخزنة فيها أو تدميرها التي يتيحها الإنترنت بشكل كبير، وكذلك تعطيل الأنظمة والبرمجيات الخبيثة أو التدمير المادي لها أو استغلالها دون تصريح أو الهجوم عبر الإنترنت على مواقع المعلوماتية لتعطيل عملها، وشملت جرائم الكمبيوتر أنشطة التجسس الصناعي والأمن والاستيلاء على البيانات ذات القيمة الاقتصادية أو الاستيلاء على أرقام بطاقات الائتمان واستخدامها بشكل غير مشروع للاستيلاء على الأموال، وكذلك الإساءة إلى سمعه الأفراد وتحقيرهم عبر الرسائل الالكترونية أو استغلال مواقع انترنت لترويج محتوى غير قانوني[1].

ثانياً: الجرائم المعلوماتية في العصر الحديث (الثورة الرقمية)

تشهد الجزائر تصاعدًا مقلقًا في معدلات الجريمة الإلكترونية، حيث احتلت مراتب متقدمة عربيًا وإفريقيًا، بنسبة 85% وفق التقارير الأخيرة. وقد سجلت الأجهزة الأمنية ارتفاعًا بنسبة تفوق 50% في عدد الجرائم المعلوماتية مقارنة بالسنة الماضية، إذ تم التحقيق في أكثر من 400 قضية خلال سنة ونصف، ما يعكس المخاطر المتزايدة التي تطرحها التكنولوجيات الحديثة. وتتنوع هذه الجرائم بين الإرهاب السيبراني، المساس بالخصوصية، الابتزاز، الاحتيال الإلكتروني، وقرصنة الحسابات على مواقع التواصل الاجتماعي، مستهدفةً بوجه خاص فئة الشباب والمراهقين، ولا سيما الفتيات، مما يعزز خطورة هذه الظاهرة على الأمن الاجتماعي.

وقد بادرت السلطات الجزائرية إلى إنشاء فرق متخصصة في مكافحة الجرائم الإلكترونية على مستوى جميع الولايات، مدعمة بخبراء تلقوا تكوينًا عالي المستوى، بغرض التصدي لهذه التحديات

[1] يونس عرب، موسوعة القانون وتقنية المعلومات (دليل أمن المعلومات والخصوصية)، الجزء الأول، منشورات اتحاد المصارف العربية، 2002، ص306.

الأمنية. إلا أن التوسع المستمر في استخدام شبكات التواصل الاجتماعي، وخاصة "فيسبوك"، لا يزال عاملًا رئيسيًا في تزايد جرائم التشهير، انتحال الهوية، والقذف الإلكتروني[1].

كما أن العصابات الإلكترونية باتت تستهدف المؤسسات الاقتصادية والمصرفية، من خلال القرصنة البنكية والتلاعب بالتحويلات المالية والوثائق الرسمية، مما يهدد الاستقرار الاقتصادي. وأمام هذه التحديات، تدخل رئيس الجمهورية باستحداث جهاز وطني لمكافحة الإجرام الإلكتروني، لكن يظل تطبيق العقوبات في هذه الجرائم معقدًا، بسبب قلة الخبرة التقنية ونقص الكوادر المتخصصة. لذا، بات من الضروري تبني استراتيجيات عقابية وتقنية متطورة لحماية الضحايا، لاسيما الأطفال ورجال الأعمال، وتعزيز التشريعات لمواكبة التطورات المتسارعة في هذا المجال.

الفرع الثاني: الثقافة الفرعية لمجرمي المعلوماتية

سوف نلقي الضوء في هذا العنصر على الثقافة الفرعية لمرتكبي الجرائم المعلوماتية أو ما يطلق عليهم لفظ "الهاكرز" (Hackers)، وذلك من خلال التركيز على مستويين الأول يتضمن تحديد عناصر أو مكونات تلك الثقافة، أما المستوى الثاني للتحليل فسوف نركز فيه على الإطار الأخلاقى المجرمى المعلوماتية باعتباره ثقافة فرعية. ونتوقف بادئ ذي بدئ عند مفهوم "الهاكرز" لنوضح بأنه قد استخدم لوصف الأشخاص الذين يقتحمون بطريقة غير شرعية أنظمة

الحاسب الآلي المملوكة للآخرين، وأيضا استخدام الحاسب الآلي والإنترنت في الأنشطة غير القانونية والتدميرية. ومنه تتلخص الثقافة الفرعية للهاكرز في كونها لغة مشتركة فيما بين مجرمي المعلوماتية والنظر إليهم على أنهم بمثابة أعضاء في جماعة يتبادلون الخبرات والمعارف ويشتركون في عدد من السمات وتتضمن الثقافة الفرعية مجرمي المعلوماتية "الهاكرز " مجموعة من القيم والمعايير والاتجاهات التي قد تشكل إطارا أخلاقيا خاصا يعمل من خلاله مجرمي المعلوماتية. إن لتلك الثقافة عناصر ومكونات رئيسية أسهمت بصورة أساسية في تكوينها، ومن أبرز تلك العناصر سيطرة الشباب الذكور على هذا النشاط الإجرامي والمعرفة الجيدة بالتكنولوجيا والمهارة اللازمة لتنفيذ هذا العمل ودور العلاقات الاجتماعية في

[1] طيبي رتيبة، العولمة وأثرها في بروز الجرائم المعلوماتية المستحدثة، مجلة سوسيولوجيا الجريمة، جامعة على لونيسي البليدة2، 2021، ص63.

اكتساب المعرفة والسرية والغفلية ودورهما في إتمام هذا النشاط. ويمكن القول بأن الاستعداد للسيطرة على الآلة واستخدامها في الاتصال مع الآخرين يكون من خلال الشباب وبالأخص الذكور، حيث كشفت الدراسات عن أن متوسط أعمار مرتكبي الجرائم المعلوماتية من سن 16-40 وهم في سن التعليم في الكليات والمعاهد.

ومن هذا المنطلق يرتبط الإجرام المعلوماتي بثقافة الشباب أكثر من ارتباطه بثقافة الآباء، فالفجوة بين ما يفهمه الهاكرز حول تكنولوجيا الحاسب الآلي وآبائهم الذين لا يفهمون تلك التكنولوجيا إنما يجعل الاختراق أداة ربما تكون مثالية للتعبير عن ثقافة الشباب وبالتالي إظهار الهوة أو الفجوة بين الأجيال، فالاختراق أصبح مجالا حيويا بالنسبة للشباب والمراهقين لكي يقوموا بالسيطرة والاستقلال وتحدي السلطة الأبوية وبالتالي السلطة المجتمعية. ويتضح لنا مما سبق أن الثقافة الفرعية تكونت من خلال الشباب الذكور الذين يميلون إلى استخدام الحاسب الآلي وينظرون إلى أفعال الاختراق وكل أنشطة الإجرام المعلوماتي على أنها بمثابة تحد وقهر للنظام القائم في المجتمع بالإضافة إلى القدرة على إثبات الذات، ومن ناحية أخرى يزعمون بأن ثقافتهم تختلف عن ثقافة أبائهم الذين ليسوا على دراية كافية بتكنولوجيا الحاسب الآلي[1].

كما تلعب العلاقات الاجتماعية دورا رئيسيا في تكوين الثقافة الفرعية واكتساب المعرفة لدى مجرمي المعلوماتية، فالهاكرز يدخلون في علاقات مع جماعات اجتماعية تمدهم بالخبرة والدعم الفني وتبادل الخبرات والمعلومات، ويتم ذلك ذلك من خلال مشاركتهم في المنتديات العامة وحضورهم للاجتماعات واللقاءات الدورية وتبادل الخبرات والمعارف. هذا ويرى الكثيرون من الهاكرز أن هناك مواثيق أخلاقية ترشد سلوكهم وتعطي المبرر لهذا السلوك، فأخلاق الهاكرز في جزء منها تؤكد بأن المعلومات يجب أن تكون متاحة بالمجان ودون قيود وأن تتاح للجميع بسهولة ويسر دون حواجز أو قيود، وأن حق استخدام هذه المعلومات والاطلاع عليها يعد حقا مكتسبا لجميع أفراد المجتمع.

[1] طيبي رتيبة، المرجع السابق، ص62.

وبهذا فإن الجرائم المعلوماتية ترتكب في حالات كثيرة لإثبات الذات أو إظهار نوع من التحدي دون أن يكون هناك دافع مادي من وراء ارتكاب تلك الأنشطة الإجرامية، فالكثير من مجرمي المعلوماتية كانوا شبابا يفكرون في الحاسب الآلي على أنه نوع من الألعاب الترفيهية مثل ألعاب الفيديو (Video Games). وقد تبدأ الجريمة في الأصل بإحدى اللعب أو المباريات التي يشترك فيها الشباب مع جهازه الخاص به وشيئا فشيئا يحدث ما لا يحمد عقباه ويودي بنفسه إلى دائرة الفعل الإجرامي.

المطلب الثاني: المحددات المفاهيمية للجريمة المعلوماتية

في العصر الرقمي الذي نعيشه اليوم، أصبحت التكنولوجيا جزءًا لا يتجزأ من حياتنا اليومية، حيث نعتمد على الإنترنت في مختلف المجالات، من التواصل الاجتماعي إلى العمليات المصرفية والتجارة الإلكترونية. ومع هذا التطور الهائل، ظهرت تحديات جديدة، من أبرزها الجريمة المعلوماتية، التي تُعرَّف على أنها أي نشاط إجرامي يُرتكب باستخدام الحواسيب أو الشبكات الإلكترونية بهدف الإضرار بالأفراد أو المؤسسات أو حتى الدول.

الفرع الأول: تعريف الجريمة المعلوماتية

تعتبر الجريمة المعلوماتية أي فعل غير قانوني يُرتكب باستخدام الأجهزة الإلكترونية أو أنظمة الحاسوب، ويستهدف البيانات أو الشبكات بهدف السرقة أو التخريب أو الاحتيال. تشمل هذه الجرائم الاختراق، الاحتيال الإلكتروني، وانتهاك الخصوصية.

1. التعريف الفقهي للجريمة المعلوماتية

- **التعريف اللغوي:** "المعلوماتية يقصد بها المعالجة الآلية للمعلومات، وهي ترجمة للمصطلح الفرنسي informatique وتعني تكنولوجيا تجميع ومعالجة وإرسال المعلومات بواسطة الكمبيوتر"[1].
- **التعريف الفقهي:** "ليس هناك اتفاق للفقهاء حول هذه المسألة، لهذا نجد البعض اعتمد على التعريف الواسع حيث عرفوها بأنها كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشياء المعنوية".

[1] خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، 2008، ص43.

2. التعريف المشرع الجزائري للجريمة المعلوماتية

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة -02- الفقرة - أ - من القانون رقم 09-04 المؤرخ في 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]. 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 السلوكات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها أو محلا لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الإلكترونية**"[2].

الفرع الثاني: أهداف الجريمة المعلوماتية

أولاً: تحقيق مكاسب غير مشروعة: يمكن للمجرمين استخدام البيانات المصرفية المسروقة في تنفيذ عمليات احتيال مالي مثل سرقة أموال من الحسابات أو إجراء معاملات غير مشروعة. كما يمكن بيع المعلومات السرية التي تخص الأفراد أو المؤسسات إلى جهات منافسة لتحقيق مكاسب مالية ضخمة. ومن الناحية السياسية، قد تُستخدم هذه المعلومات في حملات تضليل أو تشويه سمعة شخصيات بارزة لتحقيق أهداف غير قانونية[3].

ثانياً: إلحاق الضرر بالأنظمة والمعلومات: لا تقتصر الجريمة المعلوماتية على الوصول غير المشروع إلى البيانات لتحقيق مكاسب مالية أو سياسية، بل تمتد أيضًا إلى إلحاق الضرر بالأنظمة والمعلومات من خلال تدميرها أو تعطيلها أو التلاعب بها بطرق تؤثر سلبًا على المؤسسات والأفراد. فمن خلال الهجمات الإلكترونية مثل الفيروسات والبرمجيات الخبيثة، يمكن للمجرمين تدمير قواعد البيانات، مما يؤدي إلى فقدان المعلومات الحيوية للمؤسسات المالية والحكومية. بالإضافة إلى ذلك، قد يلجأ المهاجمون

[1] المادة -02- الفقرة -أ- من القانون رقم 09-04 المؤرخ في 05 أوت 2009، المشار إليه سابقاً.

[2] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال متطلبات شهادة الماستر علوم التسيير، تخصص: إدارة التحقيقات الاقتصادية والمالية، جامعة قاصدي مرباح – ورقلة-، 2018-2019، ص04.

[3] عمار حشمان، مرجع نفسه، ص09.

إلى تعطيل الأنظمة الحاسوبية عبر هجمات حجب الخدمة(DDoS) ، مما يؤدي إلى توقف المواقع الإلكترونية والخدمات الرقمية، مما يتسبب في خسائر فادحة للشركات والبنوك وحتى البنية التحتية الوطنية. كما يمكن استغلال الثغرات الأمنية لاختراق الأنظمة والتلاعب بالبيانات، سواء من خلال تعديل المعلومات أو حذفها نهائيًا، مما يهدد سلامة المعاملات المصرفية وسرية الاتصالات الحكومية. وبذلك، لا تحقق الجرائم المعلوماتية مكاسب غير مشروعة فحسب، بل تؤدي أيضًا إلى زعزعة استقرار الأنظمة المعلوماتية وإلحاق أضرار جسيمة بالأفراد والمؤسسات والدول.

ثالثاً: تهديد الأمن السيبراني: تمثل الجرائم المعلوماتية تهديدًا جوهريًا للأمن السيبراني، إذ تتجاوز تحقيق المكاسب غير المشروعة إلى استهداف الأنظمة وتعطيلها أو التلاعب بها، مما يلحق أضرارًا جسيمة بالمؤسسات والأفراد والدول. فمن خلال الهجمات الإلكترونية، مثل البرمجيات الخبيثة وهجمات الفدية (Ransomware)، يتمكن المهاجمون من احتجاز البيانات الحساسة وابتزاز الضحايا ماليًا، مما يهدد الاستقرار الاقتصادي والمؤسسي. كما تستهدف الهجمات السيبرانية البنية التحتية الحيوية، كأنظمة الطاقة والنقل والاتصالات، مما قد يؤدي إلى اضطرابات واسعة تهدد الأمن القومي. إضافةً إلى ذلك، تُستخدم هجمات حجب الخدمة (DDoS) لتعطيل المواقع والخدمات، مما يعرقل العمليات الرقمية ويقوض ثقة المستخدمين[1].

أما على المستوى الاستراتيجي، فتمثل الاختراقات وسيلة للتجسس وسرقة المعلومات العسكرية والاقتصادية، حيث تستغل الجماعات الإجرامية والجهات المعادية الثغرات الأمنية للوصول إلى بيانات حساسة، مما يزعزع الاستقرار السياسي والاقتصادي. وبذلك، تشكل الجرائم المعلوماتية خطرًا متناميًا يستدعي تعزيز وسائل الحماية الرقمية واتخاذ تدابير أمنية صارمة للحد من تداعياتها.

[1] عمار حشمان، مرجع سابق، ص09.

الفرع الثالث: أنواع الجريمة المعلوماتية

في ظل التطور التكنولوجي المتسارع، تعد الجرائم المعلوماتية من أكثر الجرائم تنوعًا وتعقيدًا، إذ تختلف باختلاف الهدف والمساس بالمصالح المحمية قانونًا. ومن أبرز هذه الأنواع، الجرائم المرتبطة بسرية البيانات، والتي تستهدف انتهاك خصوصية المعلومات وسرية البيانات الشخصية أو المؤسسية. كما تبرز الجرائم المرتبطة بتخريب الأنظمة، التي تهدف إلى إتلاف أو تعطيل أنظمة المعلومات والشبكات التقنية، مما ينعكس سلبًا على الأفراد والمؤسسات على حد سواء.

أولاً: الجرائم المرتبطة بسرية البيانات

الجرائم التي تستهدف بالاعتداء أو التهديد الحقوق ذات الطابع الشخصي، وهي الحقوق المرتبطة بالفرد والتي تعد من مقومات شخصيته ولا تخضع للمعاملات الاقتصادية. ومن أبرز هذه الحقوق: الحق في الحياة، الحق في سلامة الجسد، الحق في الحرية، والحق في حماية الشرف.

1- الجريمة انتحال الشخصية: هي جريمة قديمة جدا تتمثل صورها في الكثير من الجرائم التي ترتكب بالطرق التقليدية، إلا أنه ومع انتشار شبكة الانترنت فقد أخذ هذا النوع شكلا جديدا وهي انتحال شخصية الفرد على الشبكة الالكترونية واستغلالها أسوء استغلال وذلك بأخذ البيانات الشخصية كالعنوان وتاريخ الميلاد ورقم الضمان الاجتماعي وما شابهها من أجل الحصول على بطاقات ائتمانية وغيره، ومن خلال هذه المعلومات يستطيع المحرم إخفاء شخصيته الحقيقية والتصرف بحرية تحت اسم مستعار، وغالبا ما يتحصل المنتحل على تلك المعلومات عن طريق الكم الهائل من الإعلانات التي تزدحم بها شبكة الانترنت[1].

2-**جريمة المضايقة والملاحقة:** وهو نوع حديث من الجرائم المتزايدة باستمرار مع كل إضفاء وتحديث يطال برامج الحوارات المتبادلة والدردشة، وهي عبارة عن مساحات معروفة في الفضاء الالكتروني تتيح لمستخدميها الاشتراك في محادثات بين بعضهم البعض.

[1] منير محمد الجنبيهي ممدوح محمد الجنبيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005، ص42-43.

وجرائم الملاحقة تشمل رسائل تهديد وتخويف ومضايقة وقد شبه القضاة هذه الجريمة خارج الشبكات بجرائم التهديد العلني، ولا تتطلب الجريمة المرتكبة عبر الإنترنت أي اتصال مادي بين المجرم والضحية مما يدل أن لها تأثيرات سلبية نفسية فهي لا تؤدي إلى أي تصرفات عنف مادية[1].

3 - **جرائم التغرير 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 إذ يستطيع كل مراسل عبر الشبكة ارتكابها بكل سهولة وكذلك يقع ضحيتها أي مستخدم حسن النية[2].

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 الغير اللائقة أو معلومات غير صحيحة[3].

5-**الجرائم المخلة بالأخلاق والآداب العامة:** إذا كانت شبكة الانترنت تتسم بالعالمية ولا تقتصر على مستخدم دون الآخر، فإن ما يتم عرضه من مواد تعد مخلة بالآداب والأخلاق العامة في بلد معين قد تشكل جريمة يعاقب عليها القانون في حين أنها لا تكون كذلك في أي بلد آخر، وتشمل هذه الجرائم تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم عبر الوسائل الالكترونية أو محاولة إغوائهم

[1] محمد أمين احمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، الطبعة الأولى، عمان، 2004، ص45.

[2] 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.

[3] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق، ص34.

لإرتكاب هذه الأنشطة، أو نشر معلومات عنهم عبر الحاسب الآلي ودعوتهم إلى القيام بالأعمال الفاحشة، وتصوير قاصرين ضمن أنشطة للجنس.

والأعمال الإباحية هي من أشهر الأعمال الحالية وأكثرها رواجا خاصة في الدول العربية وأوروبا والدول الآسيوية، وتشمل الجرائم المخلة بالأخلاق والآداب العامة على الانترنت كافة الإشكال سواء كانت صور أو فيديو أو حوارات أو أرقام هاتفية مما خول هذه الشبكة أن تكون في متناول أيدي الجميع ودون أي حواجز[1].

ثانياً: الجرائم المرتبطة بتخريب الأنظمة

تُعدّ جرائم الاعتداء على الأموال من الجرائم التي تمسّ الحقوق ذات الطبيعة المالية، والتي تشمل الحقوق ذات القيمة الاقتصادية. وفي هذا السياق، إذا انصبّ الاعتداء على الأموال على الأجهزة المادية للحاسب الآلي، بما في ذلك مكوناته المادية كالأسلاك والملحقات، فإن ذلك لا يثير أي إشكالية من حيث تطبيق القواعد الجزائية التقليدية، نظراً لكونها أموالاً منقولة تخضع للحماية القانونية المعتادة. أما في الحالات التي يكون فيها الاعتداء موجهاً إلى العناصر غير المادية المرتبطة بالحاسب الآلي، كبرمجياته ونظمه التشغيلية، فإن النصوص التشريعية التقليدية قد تعجز عن توفير الحماية القانونية الكافية، نظراً للطبيعة غير التقليدية لهذه الأصول الرقمية، مما يستدعي تطوير أطر قانونية خاصة تتلاءم مع طبيعة هذه الاعتداءات وتضمن الحماية الفعالة لها[2].

- **جرائم صناعة ونشر الفيروسات**: الفيروس هو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي، ولكنها مصممة بحيث يمكنها التأثير على كافة البرامج الأخرى الموجودة على الجهاز بأن تجعل تلك البرامج نسخة منها أو أن تعمل على مسح كافة البرامج الأخرى وبالتالي تعطلها عن العمل.

يتحدد مبدأ عمل الفيروسات الإلكترونية وفقًا لأسلوب تصميمها وآلية تشغيلها، حيث قد تبدأ نشاطها بمجرد فتح الرسالة التي تحتوي عليها، أو فور تشغيل البرنامج المصاب بها. وتُعدّ برمجة الفيروسات من أخطر الجرائم الإلكترونية وأكثرها انتشارًا، لما تُلحقه من أضرار جسيمة بأنظمة الحواسيب والمعلوماتية. وترجع الجذور النظرية لفكرة الفيروسات الإلكترونية إلى أربعينيات القرن الماضي، عندما

[1] محمد أمين أحمد الشوابكة، المرجع أعلاه، ص114.

[2] محمد امين احمد الشوابكة، المرجع السابق، ص136.

تناولها العالم الرياضي "فون نيومان" في سياق دراسته لأنظمة الحوسبة، وذلك قبل ظهور شبكة الإنترنت. ومن بين أبرز الفيروسات التي أحدثت أضرارًا واسعة النطاق فيروس "رسائل الحب" (Love Letter Virus) وفيروس "الدودة الحمراء" (Code Red Worm)، حيث تسبب الأخير في تعطيل أكثر من 250,000 جهاز حاسوب خلال أقل من تسع ساعات عام 2001، مما يُبرز مدى خطورة هذه البرمجيات التخريبية وتأثيرها الواسع على الأمن السيبراني[1].

2 - **جرائم الاختراقات:** الاختراق هو عبارة عن عملية دخول غير مصرح به إلى أجهزة الغير والشبكات الالكترونية، ويتم هذا الاختراق بواسطة برامج متطورة يستخدمها كل من يملك الخبرة وله القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحاسبات أو الشبكات. وتختلف أسباب الاختراق باختلاف أهداف المخترق، فمنهم من يخترق أجهزة البعض أو مواقعهم لمجرد الفضول والبعض الأخر لسرقتها، وهذا هو السبب الأبرز الذي يدفع المخترقين إلى الدخول إلى مواقع الحواسيب الأخرى لسرقة معلوماتهم التي قد يكونون قد عرضوها مقابل مبلغ مالي للاطلاع عليها.

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 الموقع.

3- **جريمة تعطيل الأجهزة والشبكات:** يطال التعطيل أجهزة الحاسب الآلي عبر برابجها، كما قد يؤدي تعطيل البرامج إلى أعطال فنية تقع على القطع الالكترونية للجهاز والهدف من التعطيل منع الحواسيب والشبكات من تأدية عملها دون أن تتم عملية اختراق فعلية لتلك الأجهزة وتتم عملية تعطيل الأجهزة عن طريق إرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطلها وهو الأمر الذي يعيقها عن تأدية عملها[2].

[1] منير محمد الحنبيهى ممدوح محمد الحنبيهي، مرجع سابق، ص36.

[2] منير محمد الجنبيهي ممدوح محمد الجنبيهي، مرجع نفسه، ص37-38.

4- الجرائم المرتبطة بالتحايل والاحتيال المعلوماتي:

صبح 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 النصب والاحتيال ومن بينها[1]:

- 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.

الفرع الرابع: الخصائص الأساسية للجريمة المعلوماتية

تتفرد الجريمة المعلوماتية عن الجريمة التقليدية في عدة جوانب، سواء من حيث سماتها العامة، أو الدوافع التي تقف وراء ارتكابها، أو الأساليب المستخدمة في تنفيذها. ومن أبرز خصائصها:

أولاً: صعوبة اكتشاف الجريمة المعلوماتية

تتميز الجرائم الإلكترونية بطابعها الخفي، حيث غالبًا ما تمر دون أن يدرك الضحية وقوعها، حتى في أثناء اتصاله بالإنترنت. ويعود ذلك إلى امتلاك الجاني مهارات تقنية متقدمة تمكنه من تنفيذ جرائمه بدقة، مثل نشر الفيروسات، واختراق الأنظمة لسرقة الأموال أو البيانات الشخصية، أو إتلافها، إضافةً إلى عمليات التجسس والتنصت على الاتصالات وغيرها من الأنشطة الإجرامية الرقمية[2].

تتسم أساليب تنفيذ هذه الجرائم بالطابع التقني المعقد، مما يزيد من صعوبة كشفها والتعامل معها. كما أن الإبلاغ عنها يظل محدودًا في كثير من الحالات، نظرًا لمخاوف الضحايا من فقدان ثقة عملائهم أو تعرض سمعتهم للخطر. ويضاف إلى ذلك أن الأدلة الرقمية التي يمكن أن تسهم في إثبات

[1] عبد الكريم شيباني، مرجع سابق، ص23.

[2] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، مصر، 2009، ص32.

هذه الجرائم قد تتعرض للتدمير في غضون أجزاء من الثانية، مما يعوق عملية التتبع والملاحقة القانونية للمجرمين[1].

ثانياً: صعوبة إثبات الجريمة المعلوماتية

تحدث الجرائم المعلوماتية في فضاء افتراضي خارج نطاق العالم المادي التقليدي، حيث تعتمد في وقوعها على بيئة الحاسوب وشبكة الإنترنت، مما يزيد من تعقيد مهمة الأجهزة الأمنية وجهات التحقيق في كشفها وملاحقتها. ونظرًا للطبيعة التقنية لهذه الجرائم، فإن التصدي لها يتطلب مستوى متقدمًا من المعرفة التكنولوجية، سواء في اكتشافها أو تتبعها. غير أن الجهات الأمنية والقضائية لا تزال تواجه تحديات في هذا المجال نتيجة لنقص الخبرات المتخصصة، مما يستلزم تأهيل كوادر ذات كفاءة تقنية عالية لتعزيز قدرتها على التعامل مع هذه الظاهرة. وفي ظل التطورات المتسارعة في مجال التكنولوجيا، لم تعد القوانين التقليدية كافية لمواكبة أساليب ارتكاب الجرائم المعلوماتية، الأمر الذي يستدعي تحديث الأطر التشريعية وتبني نهج أكثر تكيفًا مع المستجدات الرقمية[2].

ثالثاً: الأسلوب المعتمد في ارتكاب الجريمة المعلوماتية

إن الجرائم المعلوماتية تتميز بآليات ارتكابها المختلفة، حيث تعتمد بشكل أساسي على الوسائل التقنية بدلاً من القوة الفيزيائية. ففي حين تتطلب الجرائم التقليدية استخدام القوة البدنية، مثل الكسر أو الخلع في حالات السرقة، فإن الجرائم المعلوماتية تُرتكب عبر التلاعب بالبيانات، واختراق الأنظمة، واستغلال الثغرات الأمنية بطرق معقدة ودقيقة، مما يجعل اكتشافها ومكافحتها أكثر تعقيدًا[3]، كما تعتمد هذه الجرائم على شبكة المعلومات الدولية (الإنترنت) ووجود مجرم يمتلك معرفة تقنية متقدمة، يوظف خبراته في استغلال الثغرات الأمنية أو اختراق خصوصيات الآخرين لتحقيق أهدافه الإجرامية. وقد تتجسد هذه الجرائم في أشكال متعددة، مثل التجسس، أو استغلال القاصرين، أو الاحتيال الإلكتروني،

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع، ص.56

[2] محمد عبيد الكعبي، مرجع سابق، ص 40.

[3] نهلا عبد القادر المومني، مرجع سابق، ص57-58.

وكل ذلك يتم دون الحاجة إلى استخدام العنف الجسدي أو إراقة الدماء، مما يجعل كشفها والحد منها أكثر تعقيدًا مقارنة بالجرائم التقليدية.

رابعاً: الجريمة المعلوماتية باعتبارها جريمة جماعية

ما مَيَّز الجريمة المعلوماتية غالبًا بطابعها الجماعي، حيث يتعاون أكثر من شخص في ارتكابها بهدف الإضرار بالجهة المستهدفة. وعادةً ما تتطلب هذه الجرائم تضافر جهود شخص يمتلك خبرة تقنية متقدمة في مجال الحاسوب والإنترنت، ليتولى الجوانب الفنية للعملية الإجرامية، إلى جانب شخص آخر قد يكون من داخل المؤسسة المستهدفة أو من خارجها، يتولى تسهيل عملية الاختراق، إخفاء الأدلة، أو تحويل المكاسب الناتجة عن الجريمة، مما يزيد من تعقيد تتبعها وكشف مرتكبيها[1].

خامساً: خصائص مجرمي الجريمة المعلوماتية

يطلق على مرتكب الجريمة المعلوماتية مصطلح "المجرم الإلكتروني" أو "المعلوماتي"، وهو يتمتع بخصائص تميزه عن المجرم التقليدي. ففي حين أن الجرائم التقليدية لا تتطلب بالضرورة مستوى علميًا أو معرفيًا معينًا من الجاني، فإن الجرائم المعلوماتية تختلف في طبيعتها، إذ تُعتبر ذات طابع فني وتقني في الغالب. ولذلك، فإن مرتكبها يكون عادةً شخصًا متخصصًا في مجال تقنية المعلومات، أو على الأقل يمتلك حدًا أدنى من المعرفة والمهارات التي تمكنه من استخدام الحاسوب والتعامل مع شبكة الإنترنت لتنفيذ أنشطته الإجرامية بطرق يصعب اكتشافها أو تعقبها بسهولة[2].

سادساً: الطابع العابر للحدود للجريمة المعلوماتية

مع ظهور شبكات المعلومات، تلاشت الحدود الجغرافية التقليدية أمام تدفق البيانات ونقل المعلومات بين الدول المختلفة. فقد أصبحت الحواسيب وشبكاتها قادرة على تبادل كميات هائلة من المعلومات بسرعة فائقة، حتى بين أنظمة تفصل بينها آلاف الأميال. ونتيجة لذلك، لم تعد الجرائم المعلوماتية مقتصرة على نطاق جغرافي محدد، بل بات من الممكن أن تمتد آثار الجريمة الواحدة لتؤثر على جهات متعددة في دول مختلفة في الوقت ذاته، مما يزيد من تعقيد مكافحتها ويستدعي تعاونًا دوليًا فعالًا لمواجهتها.

[1] محمد عبيد الكعبي، المرجع السابق، ص42.

[2] نهلا عبد القادر المومني، مرجع سابق، ص 58-57.

المبحث الثاني: الطبيعة القانونية للجريمة المعلوماتية

قبل التطرق إلى أركان الجريمة المعلوماتية، من المهم الوقوف أولًا على دوافع ارتكاب هذا النوع من الجرائم، لما لها من دور أساسي في فهم السلوك الإجرامي المرتبط باستخدام التكنولوجيا. فالجريمة المعلوماتية غالبًا ما تنشأ عن دوافع متعددة، قد تكون مادية بحتة كالسعي وراء الربح غير المشروع، أو معنوية كالرغبة في الانتقام أو إثبات الذات. كما قد تلعب العوامل النفسية والاجتماعية والتقنية دورًا في تعزيز هذا النوع من الجرائم. بناءً عليه، سنعالج هذه الدوافع في المطلب الأول، لننتقل بعدها إلى تحليل الأركان القانونية التي تقوم عليها الجريمة المعلوماتية في المطلب الثاني.

المطلب الأول: دوافع الجريمة الإلكترونية

إن الجريمة التقليدية والمجرم التقليدي يختلفان تماما عن الجريمة الإلكترونية والمجرم الإلكتروني، لذا من الطبيعي أن نجد نفس الاختلاف في الأسباب والعوامل التي تدفع إلى ارتكاب الفعل غير المشروع، فالدافع (الباحث)، الغرض، الغاية، مفاهيم لكل منها دلالته القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباحث ليس عنصرا من عناصر القصد الجرمي أن الباحث لا أثر له في وجود القصد الجنائي، وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة لا تتمايز، فالدافع هو العامل المحرك للإرادة، والذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام، وهو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى، أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، ويتمثل بتحقيق النتيجة التي أصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات، وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام، أو سلب مال المجني عليه في جريمة القتل[1].

[1] مسعود شهيرة، نفس المرجع السابق، ص13.

وبالنسبة للجريمة الإلكترونية فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنطوية تحت هذا المفهوم، وأهم هذه الدوافع سيتم بيانها من خلال الفرعين الآتيين:

الفرع الأول: الدوافع الشخصية لارتكاب الجريمة الإلكترونية

تصنف هذه الدوافع إلى دوافع مادية، وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة الإلكترونية، أو تأثير العنصر الذهني المعنوي على المجرم الإلكتروني ودفعه لارتكاب جريمته، وهذا ما سنتطرق إليه[1]:

أ. **الدوافع المادية:**

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع المجرم الإلكتروني تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية ويستغل الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك وراءه، فيعتمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الألية للبنوك والمؤسسات المالية إن كان أحد موظفيها أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه، أو لحساب شركائه، أو لحساب من يعمل لحسابهم إن كان خارج المؤسسة ، كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو على المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب، وقد أشارت في هذا الإطار مجلة " SECURITE INFORMATIQUE " وهي مجلة متخصصة في الأمن أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، والمعلوماتي 23%من أجل سرقة معلومات، و19% أفعال أخلاق 15% الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية وفي حقيقة الأمر أن في حال نجاح المجرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية،

[1] مسعود شهيرة، الجريمة الإلكترونية في التشريع الجزائري، المرجع السابق، ص15.

وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية، حيث تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة لأنظمة المعلوماتية، وأن 64 % لحقت بهم خسائر مادية جراء هذه الاعتداءات[1].

ب. **الدوافع الذهنية لارتكاب الجريمة**

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي، واثبات الذات، وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في التحدي و قهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام المجرم الإلكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل هذا المجرم إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي وإثبات المقدرة.

الفرع الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية

قد يتأثر المجرم الإلكتروني ببعض المواقف قد تكون دافعه على اقتراف الإجرام الإلكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال. ويمكن إبراز أهم الدوافع كالآتي:

- **دافع الانتقام وإلحاق الضرر برب العمل:**

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية ، فهذه الأمور تجعله يقدم على ارتكاب جريمته[2]، كما يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، وذلك أنه غالبا ما يصدر عن الشخص الذي يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور

[1] سعيدان نعيم، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجيستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر باتنة، 2012 – 2013، ص60-61، نقلا عن نهلا عبد القادر المومني، الجرائم المعلوماتية، ط (2)، 2010، ص90، ونقلا عن ضاح محمود الحمود ونشأت مفقي المجالي، جرائم الأنترنيت، دار المنار للنشر والتوزيع، 2005، ص31.

[2] صغير يوسف، الجريمة المرتكبة عبر الأنترنيت، مذكرة لنيل شهادة الماجستير القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو، 2013/03/06، ص 09، نقلا عن كحلوش علي، جرائم الحاسوب وأساليب مواجهتها مجلة صادرة عن مديرية الأمن الوطني، العدد 84، 2007. ص42.

بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة ، فيتولد لدى المجرم الإلكتروني الرغبة في الانتقام من رب العمل ومثال ذلك أن الانتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

دافع التعاون والتواطؤ

هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منظمة حول أنشطتهم.

وإذا كانت هذه أبرز الدوافع لارتكاب الجريمة الإلكترونية مع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب الجريمة الإلكترونية قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة، إلى تدميرها أو على الأقل حيازتها للقيام بعملية الابتزاز والحصول على الأموال، لذلك فإن هذه الدوافع قد لا تتوقف عند هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدة، بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة[1].

المطلب الثاني: التشريعات الوطنية والدولية لمكافحة الجريمة الإلكترونية

تُعد الجريمة الإلكترونية من أبرز التحديات التي تواجه الدول في العصر الرقمي، لما لها من آثار خطيرة على الأمن الوطني والمجتمعي. وقد دفعت هذه التهديدات المتزايدة العديد من الدول إلى سنّ تشريعات وطنية متخصصة، تتكامل مع الاتفاقيات والمعاهدات الدولية، لمكافحة هذا النوع من الجرائم. وتهدف هذه المنظومة القانونية إلى الوقاية من الجرائم الرقمية، وتجريم مرتكبيها، وتعزيز التعاون الدولي في تتبع وملاحقة المجرمين.

[1] سعيداني نعيم، المرجع السابق، ص62.

الفرع الأول: التشريعات الوطنية لمكافحة الجريمة الإلكترونية

تُولي الجزائر أهمية متزايدة لمكافحة الجريمة الإلكترونية، وذلك من خلال تطوير إطارها التشريعي بما يتماشى مع التحديات الأمنية التي يفرضها العصر الرقمي. وقد شكل القانون رقم 09-04 المؤرخ في 5 أوت 2004[1] النواة الأساسية في هذا المجال، إذ نصّ صراحة على تجريم مختلف الأفعال المرتبطة باستخدام تكنولوجيا المعلومات والاتصال بشكل غير مشروع، مثل الدخول غير المصرح به إلى الأنظمة المعلوماتية، وتدمير المعطيات الرقمية، وانتهاك الخصوصية الإلكترونية. كما تضمّن هذا القانون عقوبات صارمة تصل إلى السجن لمدة عشر سنوات، إلى جانب غرامات مالية معتبرة، تعكس مدى خطورة هذه الجرائم على الأمن السيبراني الوطني. وقد تم بموجب هذا الإطار القانوني تأسيس هيئة وطنية مختصة بالوقاية من الجرائم الإلكترونية ومكافحتها، تعمل على تنسيق الجهود بين مختلف الهيئات الأمنية، مع تعزيز التعاون مع المنظمات الدولية المعنية.

وعلى الصعيد الدستوري، جاء التعديل الدستوري لسنة 2020 ليكرّس التوجه نحو تعزيز التعاون القضائي والأمني الدولي، حيث نصّت المادة 50 على ضرورة الالتزام بالاتفاقيات الدولية ذات الصلة[2]، خاصة ما يتعلق بتسليم المجرمين في القضايا المرتبطة بالجرائم الإلكترونية، في إطار احترام السيادة الوطنية. ويُعدّ هذا المبدأ منسجماً مع مصادقة الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات سنة 2010، التي تدعو الدول الأعضاء إلى تبادل المعلومات وتنسيق الجهود بشأن الجرائم العابرة للحدود، كما تمثل خطوة في الاتجاه الصحيح نحو الانخراط في الجهد الدولي لمكافحة الجريمة الإلكترونية.

وفي الإطار المؤسساتي، أنشأت الجزائر مكتباً وطنياً للإنتربول (NCB) مقره الجزائر العاصمة، وهو يشكل همزة وصل بين الأجهزة الأمنية الجزائرية وشبكة الإنتربول العالمية، مما مكّن الجزائر من تحقيق نتائج ملموسة في توقيف مشتبه فيهم متورطين في قضايا مثل الاحتيال الإلكتروني، وسرقة الهوية الرقمية، وقرصنة قواعد البيانات.

[1] القانون رقم 09-04، المشار إليه.

[2] المادة 50، في سياق العهد الدولي الخاص بالحقوق المدنية والسياسية، تؤكد على أهمية الالتزام بالاتفاقيات الدولية ذات الصلة. وهذا يعني أن الدول الأطراف ملزمة بتطبيق أحكام العهد دون أي استثناءات أو قيود، وهذا يشمل الوحدات الاتحادية.

ورغم هذه الجهود التشريعية والمؤسساتية، تواجه الجزائر عدة تحديات تعرقل الفعالية الكاملة لمكافحة هذا النوع من الجرائم. من أبرزها عدم توافق بعض التشريعات الوطنية مع المعايير الدولية، لا سيما فيما يتعلق بالأدلة الإلكترونية وآليات تبادل المعلومات الجنائية مع الدول الأخرى. كما تُبرز الحاجة إلى تكوين الكوادر القضائية والأمنية في التعامل مع الأدلة الرقمية المعقدة، التي تتطلب خبرات تقنية عالية ومعرفة بالمعايير العالمية لجمعها وتحليلها. ومن التحديات الأخرى كذلك، ضرورة تعزيز التعاون الإقليمي، خاصة مع منظمات مثل "الأفريبول"، لمواجهة الجرائم المنظمة التي تتخطى الحدود الوطنية.

وعليه، فإن الإطار القانوني الجزائري لمكافحة الجريمة الإلكترونية يُظهر توجهاً جدياً نحو حماية الفضاء السيبراني الوطني، إلا أنّ فعاليته تظل مرهونة بمدى قدرته على التكيف المستمر مع التطورات التكنولوجية المتسارعة، ومدى انفتاحه على التعاون الدولي والإقليمي، وتحديث آليات التنفيذ والتكوين، لضمان استجابة أكثر نجاعة واحترافية لهذه التحديات المستجدة.

الفرع الثاني: التشريعات الدولية لمكافحة الجريمة الإلكترونية

تعد اتفاقية بودابست لعام 2001 (الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية) واحدة من أبرز التشريعات الدولية لمكافحة الجرائم الإلكترونية. أقرها مجلس أوروبا بهدف توحيد الجهود بين الدول لمواجهة جرائم مثل الاختراق غير المشروع، التلاعب بالبيانات، والاحتيال الإلكتروني. تنص الاتفاقية على ضرورة سن قوانين وطنية تجرّم هذه الأفعال، وتعزز التعاون الدولي في جمع الأدلة وملاحقة المجرمين عبر الحدود. كما شددت على أهمية حماية الخصوصية مع ضمان فعالية الإجراءات الأمنية، وانضمت إليها دول خارج أوروبا مثل الولايات المتحدة واليابان، مما وسّع نطاق تأثيرها.[1]

من جهتها، بذلت منظمة الأمم المتحدة جهودًا تشريعية عبر مؤتمرات دولية مثل مؤتمر نابولي (1994) ومؤتمر الدوحة (2015)، حيث دعت إلى تحديث القوانين الوطنية لتشمل جرائم الإنترنت، ودعمت التعاون في تسليم المجرمين وتبادل المعلومات. كما أصدرت الجمعية العامة قرارات مثل القرار

[1] محمود محمد صفاء الدين على شرشر، الجهود الدولية والتشريعية لمكافحة جرائم الانترنت، مجلة البحوث القانونية والعلوم الاقتصادية، المنوفية متاح على الموقع: https://jslem.journals.ekb.eg/article_202042_ed932acc3346987c283aee46f8d66c2a.pdf، تم الإطلاع عليه يوم: 2025/03/15 على الساعة 23:30.

63/55 (2000) الذي يحث الدول على تطوير تشريعات لمكافحة الاستغلال الجنسي للأطفال عبر الإنترنت. بالإضافة إلى ذلك، تبنت الأمم المتحدة اتفاقية مكافحة الجريمة المنظمة عبر الوطنية (2000)[1]، التي تضمنت بنودًا لتجريم الأفعال الإلكترونية العابرة للحدود، مثل غسل الأموال وقرصنة البرمجيات، مما يعكس تكيف التشريعات الدولية مع التحديات التقنية الحديثة.

المطلب الثالث: أركان الجريمة المعلوماتية توسع فيه

تتألف الجريمة المعلوماتية من الأركان الثلاثة الأساسية للجريمة التقليدية، إلا أنها تتميز بسمات خاصة تميزها عن الجرائم الأخرى. وفي هذا المطلب، سنقوم بتفصيل هذه الأركان الثلاثة، بدءًا بالركن الشرعي للجريمة المعلوماتية (الفرع الأول)، ثم الركن المادي لها (الفرع الثاني)، وأخيرًا الركن المعنوي الذي يكتمل به قوامها (الفرع الثالث).

الفرع الأول: الركن الشرعي

استنادًا إلى مبدأ الشرعية المنصوص عليه في المادة الأولى من قانون العقوبات الجزائري، والتي تقضي بعدم وجود جريمة أو عقوبة دون نص قانوني، قام المشرّع الجزائري من خلال القانون رقم 04-15[2] بتجريم بعض صور الجريمة المعلوماتية، محددًا العقوبات المترتبة على مرتكبيها. وقد تم تضمين هذه الأحكام في القسم السابع مكرر من الفصل الثالث، المعني بـ "الجنايات والجنح ضد الأموال"، ضمن الباب الثاني المخصص لـ "الجنايات والجنح ضد الأفراد"، وذلك في المواد 394 مكرر إلى 394 مكرر 08 من قانون العقوبات المعدل والمتمم.

أما القانون رقم 09-04[3]،فقد جاء ليضع إطارًا خاصًا للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث ركّز على التدابير الوقائية الهادفة إلى الحد من الجرائم المعلوماتية،

[1] – القرارات 63/55 في 4 كانون الأول/ديسمبر 2000، و121/56 في 19 كانون الأول/ديسمبر 2001 بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

[2] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم لقانون العقوبات الجريدة الرسمية العدد 71، الصادرة بتاريخ نوفمبر 2004.

[3] المادة 03 من القانون رقم 09-04، المشار إليه سابقاً.

وذلك من خلال اعتماد آليات تقنية لمراقبة الاتصالات الإلكترونية، وتسجيل محتواها بشكل فوري، إضافة إلى منح الجهات المختصة صلاحية إجراء عمليات التفتيش داخل النظم المعلوماتية.

ويؤكد هذا التوجه التشريعي على ضرورة الامتثال الصارم لمبدأ الشرعية الجنائية، بوصفه أحد الركائز الأساسية التي تقوم عليها العدالة الجنائية الحديثة، وهو المبدأ الذي يُعبَّر عنه قانونًا بعبارة "لا جريمة ولا عقوبة إلا بنص". ويترتب على هذا المبدأ نتائج جوهرية، أهمها أن عملية التجريم والعقاب تُعد من اختصاص المشرّع دون غيره، بما يضمن حماية الحريات الفردية من التعسف أو التقديرات الشخصية للقاضي. ولذلك، فإن تقنين الجرائم بشكل دقيق ومحدد يمنع القاضي من التوسع في تفسير النصوص الجنائية أو اللجوء إلى القياس لملء فراغ تشريعي محتمل، وهو ما يشكل قيدًا ضروريًا على السلطة التقديرية للقضاء في هذا المجال.

وبناءً على هذا الأساس، لا يجوز اعتبار أي فعل غير منصوص على تجريمه في القانون بمثابة جريمة، حتى وإن كان مشابهًا من حيث الطبيعة أو الأثر لفعل مجرَّم. فمجرد التشابه أو القياس لا يكفي لإضفاء الصفة الإجرامية، بل يجب أن يتوفر نص قانوني صريح وواضح يحدد الفعل ويبين أركانه والعقوبة المقررة له. وهذا ما يعزز الأمن القانوني، ويُكسب القواعد الجنائية طابعها الإلزامي واليقيني، ويُجنّب الأفراد المفاجأة أو الغموض فيما يتعلق بما هو محظور أو معاقب عليه[1].

كما أن هذا التقييد يكرّس مبدأ الفصل بين السلطات، ويحول دون تغوّل السلطة القضائية على السلطة التشريعية، إذ أن وظيفة القاضي في المجال الجنائي تنحصر في تطبيق النصوص القانونية وتفسيرها تفسيرًا ضيقًا يتوافق مع طبيعتها الخاصة، لا في ابتداع جرائم أو عقوبات جديدة. وبذلك يُسهم احترام مبدأ الشرعية في ضمان العدالة والمساواة بين المواطنين، ويُحصّن النظام القانوني من الانحراف أو الاستنسابية، ويُرسّخ دولة القانون والمؤسسات.

[1] المادة 03 من القانون رقم 09-04، المشار إليه سابقاً.

الفرع الثاني: الركن المادي

يُعد الركن المادي للجريمة الجانب الملموس والظاهر لها، حيث يتجسد في الأفعال التي تمثل اعتداءً ملموسًا وفقًا لنصوص التجريم المعتمدة. فالمبدأ العام يقرّ بأنه "لا جريمة دون ركن مادي" أو "لا جريمة دون فعل". إلا أن الطبيعة المادية للجريمة المعلوماتية تختلف إلى حد ما عن الجرائم التقليدية، نظرًا لكونها تقوم على أنماط خاصة من الأفعال الإجرامية، والتي تتجلى في صور متعددة، أبرزها:

1*الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات

نصّت المادة 394 مكرر من قانون العقوبات الجزائري[1] على أن الدخول أو الدخول غير المشروع مع البقاء في نظام المعالجة الآلية للمعطيات، أو حتى مجرد الشروع في ذلك، يُعد فعلًا إجراميًا. ويأخذ هذا الفعل صورتين رئيسيتين[2]:

- **الصورة البسيطة:** يتحقق السلوك الإجرامي هنا من خلال:
  - **فعل الدخول غير المشروع** :وهو مجرد الوصول إلى المعلومات المخزنة داخل النظام دون علم ورضا مالكه، سواء كان النظام مغلقًا إلا أمام فئات محددة أو مفتوحًا بمقابل مالي.
  - **البقاء غير المشروع** :ويعني استمرار التواجد داخل النظام الإلكتروني دون إذن صاحبه، أو تجاوز المدة المصرّح بها، أو الامتناع عن الانسحاب الفوري بعد انتهاء التصريح، أو إساءة استخدام الصلاحيات الممنوحة، مثل طباعة معلومات مسموح فقط برؤيتها.
- **الصورة المشددة:** وفقًا لما ورد في الفقرتين الثانية والثالثة من المادة 394 مكرر، يتم تشديد العقوبة إذا نتج عن الدخول أو البقاء غير المشروع أي من الأفعال التالية:
  - محو أو تحويل المعطيات الموجودة داخل النظام.
  - إحداث خلل في وظائف النظام يؤدي إلى تعطيله أو التأثير على تشغيله، مثل تخريب برمجياته أو أنظمة تشغيله.

[1] المادة 394 مكرر من قانون العقوبات الجزائري تنص على معاقبة كل من يدخل أو يظل في نظام معالجة أوتوماتيكية للمعطيات أو يحاول ذلك باستخدام الغش، أو يسبب تلفًا في هذا النظام.

[2] حمز خضري وعشاش حمزة، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية المجلد 06 العدد 02 جوان 2020، ص 173-175.

2*إدخال المعطيات بطريق الغش

يعني هذا الفعل، وفقًا للمادة 394 مكرر 01 من قانون العقوبات، إضافة بيانات جديدة إلى نظام المعالجة الآلية أو التلاعب في البيانات المخزنة داخله، سواء بتعديلها أو تغيير محتواها. ومن أبرز الأمثلة على ذلك[1]:

- الاستخدام غير المشروع لبطاقات السحب والائتمان، سواء من قبل أصحابها الشرعيين بطرق احتيالية أو من قبل الغير عن طريق السرقة أو التزوير.

يؤكد هذا التنظيم القانوني على ضرورة حماية الأنظمة المعلوماتية من أي اعتداء غير مشروع، سواء كان ذلك بالوصول غير المصرّح به أو بالتلاعب في البيانات، مما يعكس تطور التشريعات لمواجهة التحديات التي يفرضها الفضاء الرقمي.

الفرع الثالث: الركن المعنوي

يتجسد الركن المعنوي في معظم الجرائم، بشكل عام، في صورة القصد الجنائي، والذي يقوم على عنصرين أساسيين :إرادة الجاني في ارتكاب الفعل غير المشروع، وعلمه بأن هذا الفعل مجرَّم قانونًا.وبذلك، لا يُساءل الجاني جنائيًا إلا إذا ثبت توافر الإدراك والوعي لدى الفاعل بكون سلوكه مخالفًا للقانون، إلى جانب اتجاه إرادته نحو تحقيق النتيجة الإجرامية[2]، وينطبق هذا المبدأ أيضًا على الجريمة المعلوماتية، حيث يقوم ركنها المعنوي على توافر الإرادة الجرمية لدى الفاعل .ويتجلى ذلك من خلال الصياغة التي اعتمدها المشرّع الجزائري في قانون العقوبات، إذ استخدم مصطلحات مثل "الغش"، "العمد"، و"إعداد الجريمة"، الواردة في المواد 394مكرر، 394 مكرر 1، 394 مكرر 2، وأخيرًا 394 مكرر 5. تعكس هذه العبارات اشتراط القصد الجنائي في ارتكاب الجرائم المعلوماتية، مما يعني ضرورة ثبوت علم الجاني بعدم مشروعية فعله واتجاه إرادته إلى تحقيقه.

[1] حمز خضري وعشاش حمزة، خصوصية اركان الجريمة المعلوماتية في التشريع الجزائري، مرجع سابق، ص 173-175.

[2] أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الطبعة الرابعة عشر، دار هومة للطباعة والنشر والتوزيع الجزائر، 2014، ص145.

تعكس العقوبات المقررة لهذه الجرائم أن الجريمة المعلوماتية تُعد جريمة عمدية بامتياز، حيث لا يُفترض فيها القصد الجنائي، بل يتعين توافره بشكل واضح. ومع ذلك، يختلف الركن المعنوي من جريمة معلوماتية إلى أخرى، وفقًا لطبيعة الفعل المرتكب.

فعلى سبيل المثال، تتطلب جريمة الدخول غير المصرح به إلى نظام الحاسوب توافر القصد الجنائي العام، والذي يتحقق بعلم الجاني بعناصر الركن المادي للجريمة، أي إدراكه بأن الولوج إلى النظام دون إذن يُعد فعلاً غير مشروع. ويعود هذا التجريم إلى حرص المشرّع على حماية الحاسوب وما يحتويه من برامج ومعلومات باعتباره محلًا للحق القانوني، مما يستوجب معاقبة أي اعتداء عليه يتم بوعي وإرادة جنائية واضحة[1].

تُعد جريمة الاحتيال الإلكتروني من الجرائم العمدية التي لا تقوم إلا بتوافر القصد الجنائي لدى الجاني، وهذا القصد يُعد من الأركان الأساسية لقيام المسؤولية الجنائية. وفي هذا السياق، يُشترط لتوافر القصد الجنائي في جريمة الاحتيال الإلكتروني أن يجتمع فيه نوعان من القصد :القصد الجنائي العام والقصد الجنائي الخاص.

أما القصد الجنائي العام، فيتجلى في علم الجاني بأنه يرتكب فعلاً غير مشروع، أي أنه يقوم بسلوك محظور قانوناً، سواء تمثل ذلك في استخدام وسائل تكنولوجية، أو برمجيات خبيثة، أو تقنيات الخداع الإلكتروني، مع إدراكه التام بأن هذا السلوك مخالف للقانون ومضر بحقوق الآخرين. فالمحتال يعلم بأنه يقدم بيانات كاذبة أو مضللة، أو ينتحل صفة أو صفة وهمية، أو يستخدم وسائل غير مشروعة عبر الشبكة المعلوماتية.

أما القصد الجنائي الخاص، فيتمثل في نية الجاني تحقيق غرض معين، وهو غالباً تحقيق ربح غير مشروع لنفسه أو لغيره، أو إلحاق ضرر مادي بالغير، كأن يهدف إلى الاستيلاء على أموال أو بيانات شخصية أو معلومات مصرفية أو ملكيات رقمية دون وجه حق. ويتميز هذا النوع من القصد بتوافر نية الإضرار والرغبة الواعية في الحصول على منافع مادية أو معنوية بطرق غير قانونية.

[1] يوسف جفال، التحقيق في الجريمة الإلكترونية، 2016-2017، ص17.

ويُعد القصد الخاص في جريمة الاحتيال الإلكتروني بمثابة العامل الفاصل الذي يميزها عن غيرها من الجرائم المعلوماتية، إذ أن الجاني لا يكتفي بمجرد الدخول إلى النظام المعلوماتي أو اختراق الحسابات، وإنما تكون نيته متجهة منذ البداية إلى خداع الضحية وسلبه ماله أو ممتلكاته الإلكترونية أو المادية، من خلال الإيهام والتضليل باستخدام وسائل التكنولوجيا الحديثة.

وبالتالي، فإن تحقق هذين القصدين معًا، العام والخاص، هو ما يؤسس المسؤولية الجنائية الكاملة في جريمة الاحتيال الإلكتروني، ويُظهر الطابع العمدي الواضح لهذه الجريمة، التي تستند إلى سلوك خادع وإرادة مجرمة واعية، تجعل من الجاني فاعلاً مسؤولًا عن فعله سواء من حيث النية أو النتيجة[1].

[1] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي للنشر والتوزيع، مصر، 2006، ص121.

الفصل الثاني

الحماية القانونية والكشف عن الجرائم المعلوماتية

أدى التطور التكنولوجي المتسارع إلى ظهور نوع جديد من الجرائم، تُعرف بالجرائم المعلوماتية، التي تُرتكب عبر الوسائط الإلكترونية، مما فرض تحديات كبيرة على المنظومة القانونية التقليدية. ومع تزايد الاعتماد على التكنولوجيا في مختلف مجالات الحياة، برزت الحاجة إلى توفير حماية قانونية فعّالة للأفراد والمؤسسات ضد المخاطر المرتبطة بالعالم الرقمي. إدراكًا لهذه التحديات، بادر المشرع الجزائري إلى إصدار نصوص قانونية مستحدثة، لاسيما بموجب القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية[1]، وذلك بهدف سد الفراغ التشريعي وتأمين بيئة رقمية آمنة. تبرز أهمية هذا الموضوع في الوقوف على الجهود التشريعية الجزائرية في حماية المجتمع من الجرائم المعلوماتية، وكشف الجناة، وتوفير الضمانات اللازمة لاحترام الحقوق والحريات الأساسية أثناء مكافحة هذه الجرائم.

وأصبحت الجرائم المعلوماتية تمثل تهديدًا حقيقيًا يتطلب تفعيل آليات متخصصة للتحقيق والكشف عنها. لذلك، سنخصص المبحث الأول لبيان الجهات المختصة بالتحقيق في الجرائم المعلوماتية، ثم نتناول في المبحث الثاني إجراءات التحقيق المعتمدة للكشف عن مرتكبي هذه الجرائم.

[1] القانون 18-04 المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر، عدد 27، الصادرة بتاريخ 13 مايو 2018.

المبحث الأول: الجهات المختصة في التحقيق في الجرائم المعلوماتية

أدى الانتشار الواسع للتكنولوجيا إلى بروز الجرائم المعلوماتية، مما تطلب إنشاء جهات مختصة للتحقيق فيها وضمان مكافحتها بكفاءة. وفي هذا الإطار، سنتناول في المطلب الأول الهيئة الوطنية لمكافحة الجرائم المعلوماتية، ثم نعرج في المطلب الثاني على الأجهزة الأمنية المختصة ودورها الحيوي في هذا المجال.

المطلب الأول: الهيئة الوطنية لمكافحة الجرائم المعلوماتية

نظراً لخطورة الجرائم المعلوماتية وتعقيدها، أنشئت الهيئة الوطنية لمكافحة الجرائم المعلوماتية لتتولى مهمة التصدي لهذا النوع من الجرائم. وسنتناول في هذا المطلب تعريف هذه الهيئة واختصاصاتها في الفرع الأول، ثم نوضح في الفرع الثاني كيفية تكوينها وطبيعة عملها.

الفرع الأول: تعريف الهيئة واختصاصاتها

تُعد الهيئة الوطنية لمكافحة الجرائم المعلوماتية إحدى الآليات المستحدثة في التشريع الجزائري لمواجهة التحديات المتزايدة التي تفرضها الجريمة الإلكترونية. وتُعتبر هذه الهيئة ذات طابع وطني، إداري، وتتمتع بالشخصية المعنوية والاستقلال المالي، وتخضع لوصاية الوزير الأول.

وفقًا للمادة 13 من القانون رقم 09-04[1]، تُنشأ هيئة وطنية تُعنى بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .تُحدد تشكيلتها وتنظيمها وكيفيات سيرها بموجب مرسوم رئاسي.

تتمثل مهام الهيئة، كما ورد في المادة 14 من نفس القانون في[2]:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

[1] المادة 13 من القانون رقم 09-04: المؤرخ في 5 أغسطس 2009، المشار إليه سابقاً.

[2] المادة 14 من نفس القانون.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات المتعلقة بهذه الجرائم، بما في ذلك جمع المعلومات وإنجاز الخبرات القضائية.
- تبادل المعلومات مع نظيراتها في الخارج لتحديد مكان وهوية مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

في إطار تعزيز منظومة الأمن السيبراني في الجزائر، تقوم الهيئة الوطنية المختصة بمكافحة الجرائم المعلوماتية بدور محوري يتطلب التنسيق المستمر بين مختلف الهيئات الوطنية ذات الصلة. وتتمثل أبرز اختصاصاتها في متابعة تنفيذ السياسات العامة المتعلقة بمكافحة الجرائم المعلوماتية على الصعيدين الوقائي والتعقبي، بالإضافة إلى تقديم المقترحات والتوصيات بشأن التدابير القانونية والإدارية اللازمة لتحصين البيئة الرقمية ضد التهديدات المتزايدة. كما تسهم الهيئة في تطوير التشريعات المتعلقة بالأمن السيبراني، بهدف تعزيز القدرة على التصدي للمخاطر الرقمية وحماية الحقوق القانونية للمواطنين في الفضاء الإلكتروني[1].

تتمثل إحدى المهام الأساسية للهيئة في استقبال ومعالجة الشكاوى والبلاغات المتعلقة بالجرائم المعلوماتية، وهو ما يتطلب منها التنسيق الفعال مع الهيئات القضائية والجهات الأمنية لضمان تسريع الإجراءات القانونية وتحقيق العدالة في قضايا الجرائم الرقمية. كما تعمل الهيئة على التعاون المستمر مع الهيئات الدولية المتخصصة في مجال مكافحة الجرائم المعلوماتية، ما يعزز من تبادل الخبرات والمعرفة في مواجهة التحديات العابرة للحدود.

يهدف هذا الإطار المؤسسي إلى تعزيز الحماية القانونية للمجتمع الرقمي في الجزائر، عبر ضمان استجابة فعالة للأخطار السيبرانية المتزايدة في ظل التطورات التكنولوجية السريعة التي يشهدها العالم. كما يعكس هذا التوجه جزءًا من الجهود الوطنية الهادفة إلى تحديث التشريعات الجزائرية بما يتماشى مع المعايير الدولية لمكافحة الجرائم الإلكترونية، حيث تُعتبر هذه المبادرة جزءًا من مسار تحديث المنظومة القانونية في

[1] بلعيد، رشيد، الجرائم الإلكترونية في القانون الجزائري، دار الهناء للطباعة و النشر والتوزيع، الجزائر، 2020، ص45-67.

الجزائر. وفقًا للدكتور رشيد بلعيد، الأكاديمي الجزائري المتخصص في القانون الجنائي، فقد تناول في مؤلفاته القوانين المتعلقة بالجرائم الإلكترونية وأهمية وضع إطار قانوني فعال لمكافحة هذه الجرائم في ظل التغيرات التكنولوجية المتسارعة.

الفرع الثاني: تكوين الهيئة وطبيعة عملها

إن تكوين الهيئة الوطنية المختصة بمكافحة الجرائم المعلوماتية في القانون الجزائري يعد من المواضيع المهمة في إطار تعزيز الحماية القانونية للأمن المعلوماتي. وفيما يلي توضيح لكل عنصر من هذا الموضوع، مع توجيهك للمرجع القانوني المناسب مع الصفحات والسنة:

أولاً: تكوين الهيئة الوطنية لمكافحة الجرائم المعلوماتية

تُعتبر الهيئة الوطنية لمكافحة الجرائم المعلوماتية إحدى الآليات المؤسساتية الحديثة التي أنشأتها الدولة الجزائرية لمواجهة التحديات المتزايدة المرتبطة بالجريمة السيبرانية، التي باتت تشكل تهديدًا حقيقيًا للأمن القومي والاقتصادي والاجتماعي. وقد تم تكوين هذه الهيئة استنادًا إلى جملة من النصوص القانونية والتنظيمية التي تهدف إلى تعزيز قدرات الدولة في ميدان التحقيق والتصدي للجرائم المعلوماتية، لا سيما تلك المرتكبة عبر الشبكات والأنظمة المعلوماتية.

من بين النصوص القانونية المؤسسة لدور الهيئة، نجد القانون رقم 09-04 المؤرخ في 5 أغسطس 2009[1]، والذي شكّل الإطار القانوني المرجعي الأول في هذا المجال. وقد نصّ هذا القانون على مجموعة من الأحكام الخاصة بإجراءات التحري والمتابعة القضائية في الجرائم الإلكترونية، كما أقرّ أدوات قانونية تسمح بإنشاء أجهزة متخصصة على غرار الهيئة الوطنية.

[1] القانون رقم 09-04، المشار إليه سابقاً.

وفي سياق التطورات التشريعية الحديثة، المرسوم الرئاسي رقم 22-187 المؤرخ في 17 شوال عام 1443 الموافق 18 ماي سنة 2022، يتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. (الجريدة الرسمية عدد 35 لسنة 2022) [1].

ونشر محتوى يحرض على الكراهية أو الإرهاب عبر الإنترنت، واختراق الأنظمة المعلوماتية، حيث تم تشديد العقوبات على مرتكبي هذه الأفعال. وبناءً على ذلك، أُنيط بالهيئة الوطنية مهمة التنسيق مع الضبطيات القضائية والسلطات الأمنية لضمان التحقيق التقني المتخصص في هذه الجرائم.

وتقديم الدعم التقني والقانوني للسلطات القضائية والإدارية .ويُعد هذا الإطار القانوني خطوة استراتيجية نحو إرساء منظومة فعالة للوقاية من الجرائم السيبرانية والتصدي لها بوسائل تقنية ومؤسساتية متخصصة.

وإجمالًا، تُعد الهيئة الوطنية لمكافحة الجرائم المعلوماتية ثمرة لتكامل المنظومة القانونية الجزائرية، التي تسعى لمواكبة التطورات الرقمية والحد من مخاطر الفضاء السيبراني، وذلك من خلال أدوات تشريعية وتنظيمية تسمح بالتحري الفعّال، والتعاون بين مختلف المصالح الأمنية والقضائية، في سبيل تحقيق الأمن الرقمي الوطني.

ثانياً: طبيعة عمل الهيئة

تُعدّ الهيئة الوطنية لمكافحة الجرائم المعلوماتية الجهة المحورية في الجزائر المكلفة بالتصدي للجرائم الإلكترونية المتزايدة في ظل التحول الرقمي الذي تشهده الدولة. وتتولى الهيئة مهامًا متعددة تشمل الرصد والمراقبة المستمرة للفضاء السيبراني، بهدف كشف الأنشطة غير المشروعة التي تمس بأمن المعلومات والأنظمة الرقمية، سواء تعلّق الأمر باختراق البيانات، أو التزوير الإلكتروني، أو نشر المحتوى المضر عبر

[1] المرسوم الرئاسي رقم 22-187 المؤرخ في 17 شوال عام 1443 الموافق 18 ماي سنة 2022، يتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. (الجريدة الرسمية عدد 35 لسنة 2022).

الوسائط الإلكترونية. كما تضطلع الهيئة بمهمة التحقيق والتحرّي في الجرائم الإلكترونية بالتعاون مع المصالح الأمنية والقضائية المختصة، مما يسهم في تتبّع الجناة وتقديمهم للعدالة.

وتعمل الهيئة أيضًا على تقديم الاستشارات والدعم الفني للمؤسسات العمومية والخاصة في مجال الأمن السيبراني، من خلال إصدار توصيات وقائية تهدف إلى تعزيز حماية البنية التحتية الرقمية في البلاد، فضلاً عن تنظيم حملات توعوية لفائدة المواطنين حول مخاطر الجرائم المعلوماتية وسبل الوقاية منها.

إنّ الدور المتعاظم للهيئة الوطنية لمكافحة الجرائم المعلوماتية يعكس التزام الدولة الجزائرية بحماية فضائها الرقمي، وتعزيز ثقة المواطنين في الخدمات الإلكترونية، لا سيما في ظل الرقمنة المتسارعة للإدارة والقطاعات الحيوية.

ثالثاً: قوانين خاصة بمكافحة الجرائم المعلوماتية

صدر القانون رقم 09-04 كإطار تشريعي خاص بمكافحة الجرائم المعلوماتية في الجزائر[1]، وذلك استجابة للتطور السريع في مجال تكنولوجيا المعلومات والاتصالات، وازدياد التهديدات الإلكترونية التي تطال الأفراد والمؤسسات على حد سواء. وقد جاء هذا القانون ليغطي الفراغ التشريعي الذي كانت تعاني منه المنظومة القانونية الجزائرية في مواجهة الجرائم المستحدثة المرتبطة باستخدام الحواسيب والشبكات الإلكترونية، والتي يصعب إخضاعها للأحكام التقليدية لقانون العقوبات. ومن أبرز ما تضمنه هذا القانون هو إقراره لجملة من التدابير الزجرية والوقائية تهدف إلى تعزيز الحماية الجنائية للمعلومات والمعطيات الإلكترونية، سواء تعلقت بالحياة الخاصة للأفراد أو بأسرار المؤسسات والهيئات العمومية والخاصة. كما جرم العديد من الأفعال مثل الدخول غير المشروع إلى نظم المعلومات، واعتراض أو تعديل البيانات الإلكترونية دون إذن، واستعمال المعطيات الشخصية دون وجه حق، بالإضافة إلى محاربة نشر البرمجيات الخبيثة والاحتيال المعلوماتي. واعتمد القانون مقاربة شاملة لا تقتصر فقط على التجريم والعقاب، بل شملت كذلك آليات التعاون الدولي، وتطوير القدرات التقنية لمصالح الأمن

[1] القانون رقم 09-04، الشمار إليه سابقاً.

والقضاء، لمواكبة طبيعة هذه الجرائم العابرة للحدود، مما يعكس رغبة المشرّع في إرساء توازن بين حماية الحريات الرقمية وضمان الأمن المعلوماتي في البيئة الافتراضية.

رابعاً: إجراءات التحقيق والملاحقة القانونية

تُولي الهيئة الوطنية لمكافحة الجرائم الإلكترونية أهمية بالغة لاستخدام التقنيات الحديثة في رصد وتتبع الأنشطة الإجرامية على الفضاء الرقمي، حيث تعتمد على منظومات إلكترونية متطورة وتقنيات الذكاء الاصطناعي لتحليل البيانات الرقمية وكشف محاولات الاختراق والقرصنة، بالإضافة إلى تقنيات تتبع العناوين الرقمية (IP tracking) وتحليل الأدلة الرقمية .(Digital Forensics) وتُعزّز هذه الجهود عبر شراكات استراتيجية مع الوكالات الأمنية المحلية، مثل الدرك الوطني والأمن الوطني، فضلاً عن التعاون مع أجهزة دولية متخصصة، كالإنتربول ويوروبول، بهدف تبادل المعلومات والخبرات وتنسيق التحقيقات العابرة للحدود، نظرًا للطابع العالمي للجرائم الإلكترونية.

وفي السياق ذاته، تلتزم الهيئة باتباع الإجراءات القانونية المنصوص عليها في التشريع الجزائري، خصوصًا بعد التعديل الذي طرأ على قانون الإجراءات الجزائية بموجب القانون رقم 15-03 المؤرخ في 1 فبراير 2015[1]، الذي أدرج أحكامًا جديدة تتعلق بالجرائم المعلوماتية وأساليب التحقيق الخاصة بها. فقد سمح هذا التعديل للجهات القضائية باستخدام وسائل التحقيق التقنية مثل التفتيش الإلكتروني، المصادرة الرقمية، المراقبة عن بُعد، والتنصت على المراسلات الإلكترونية، بما يضمن فعالية التحريات دون الإخلال بضمانات المحاكمة العادلة. كما نصت المادة 65 مكرر من القانون المعدل على إمكانية إجراء تفتيش لأي نظام معلوماتي بإذن قضائي، وهي خطوة تُعدّ تطورًا تشريعيًا لمواكبة التحديات التقنية للجرائم الحديثة. ومن ثمّ، فإن الهيئة تستند في ملاحقتها للجناة إلى هذه الأدوات القانونية والتقنية، مما

[1] القانون رقم 15-03 المؤرخ في 1 فبراير 2015 هو قانون يتعلق بعصرنة العدالة في الجزائر. يُعرف أيضًا باسم "قانون عصرنة العدالة". نص القانون على استخدام تقنيات التوقيع والتصديق الإلكترونيين في المجال القضائي، بالإضافة إلى استخدام المحادثة المرئية عن بعد في الإجراءات القضائية.

يعكس حرص الدولة على دمج التكنولوجيا ضمن منظومة العدالة الجنائية لضمان الفعالية والحماية القانونية في آنٍ واحد[1].

خامساً: تعاون الهيئة مع الهيئات الدولية

تُعَدُّ الهيئة الوطنية لمكافحة الجرائم المعلوماتية أحد الركائز الأساسية في التصدي للتهديدات السيبرانية، لا سيما في ظل تزايد الجرائم الإلكترونية ذات الطابع العابر للحدود، والتي تتطلب تضافرًا دوليًا لمواجهتها بفعالية. ومن هذا المنطلق، تعمل الهيئة على تعزيز تعاونها مع الهيئات والمنظمات الدولية المعنية بمكافحة الجريمة الإلكترونية، وعلى رأسها منظمة الشرطة الجنائية الدولية (الإنتربول)، من خلال تبادل المعلومات والخبرات، والمشاركة في العمليات المشتركة، وتنسيق الجهود الرامية إلى تتبع مرتكبي هذه الجرائم وتقديمهم للعدالة. كما تولي الهيئة اهتمامًا خاصًا بإبرام اتفاقيات تعاون ثنائية ومتعددة الأطراف مع عدد من الدول، تهدف إلى تسهيل تبادل البيانات التقنية والأدلة الرقمية، وتوفير الدعم المتبادل في مجالات التحري والتحقيق والتكوين.

وقد جاء القانون رقم 18-07[2]، ليؤطر الجوانب القانونية المرتبطة بحماية البيانات الشخصية، التي تشكل محورًا حساسًا في قضايا الجرائم الإلكترونية. كما تضمن قانون العقوبات الجزائري، لاسيما في التعديلات الأخيرة بالقانون رقم 20-05 الصادر سنة 2020[3]، مواد صريحة تجرّم الأفعال المتعلقة بالولوج غير المشروع إلى الأنظمة المعلوماتية، أو إتلاف البيانات، أو التشويش على أنظمة التشغيل، وذلك ضمن فصل خاص بالجرائم الإلكترونية. بالإضافة إلى ذلك، تعمل الدولة على مواكبة التطورات التشريعية الدولية من خلال الانضمام إلى اتفاقيات دولية كاتفاقية بودابست بشأن الجرائم السيبرانية، وهو

[1] المادة 65 من القانون رقم 15-03 المؤرخ في 1 فبراير 2015.

[2] قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018. يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. 21 أفريل 2020.

[3] القانون رقم 20-05 المؤرخ في 28 أفريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والذي يتضمن إنشاء المرصد الوطني للوقاية من التمييز وخطاب...

ما يُترجم في السياسات العمومية الداعمة لإنشاء بيئة تشريعية متكاملة ومتوافقة مع المعايير الدولية في هذا المجال[1].

سادساً: التوعية والتدريب

لا تقتصر مهام الهيئة المختصة بمكافحة الجرائم المعلوماتية في الجزائر على الملاحقة القضائية للجرائم المرتكبة عبر الفضاء السيبراني، بل تتعدى ذلك إلى دور وقائي وتوعوي بالغ الأهمية. إذ تسعى الهيئة إلى تعزيز وعي المواطنين بمخاطر الجرائم السيبرانية من خلال إطلاق حملات إعلامية وتثقيفية موجهة لمختلف فئات المجتمع، وخصوصًا فئة الشباب التي تُعدّ الأكثر عرضة للاستعمال اليومي لتكنولوجيا المعلومات. كما تنظم الهيئة، بالتعاون مع قطاعات التعليم والتكوين المهني، دورات تدريبية ومحاضرات تهدف إلى تعريف الأفراد بحقوقهم وسبل الحماية القانونية في البيئة الرقمية.

وفي ذات السياق، تعمل الهيئة على تقديم برامج تدريب متقدمة موجهة للكوادر العاملة في مجال الأمن السيبراني، وذلك بهدف تطوير مهاراتهم التقنية والقانونية وتمكينهم من التصدي للتقنيات الحديثة التي يستخدمها المجرمون الإلكترونيون، والذي نصّ على إنشاء هيئة وطنية لحماية الفضاء السيبراني، وعلى ضرورة إعداد إستراتيجية وطنية للوقاية من هذه الجرائم، تشمل جانب التوعية والتكوين، إلى جانب المتابعة القانونية.

كما نصّ قانون العقوبات المعدل بالأمر رقم 21-09 المؤرخ في 8 يونيو 2021 على جرائم جديدة تتعلق بالمساس بأنظمة المعلومات والمعطيات الشخصية[2]، وشدد العقوبات على من يثبت تورطهم في اختراق الشبكات أو الاحتيال الإلكتروني أو نشر المحتوى الضار عبر الإنترنت. وأكد القانون

[1] المرسوم الرئاسي رقم 06-03 المؤرخ في 19 يناير 2006، العدد 46، الذي يحدد القواعد الخاصة بالتعاون مع الهيئات الدولية في مجال مكافحة الجرائم الإلكترونية.

[2] الأمر رقم 21-09، المؤرخ في 08/06/2021، المتضمن حماية المعلومات والوثائق الإدارية ج. ر. ج. ج، عدد 45 الصادرة بتاريخ 09 يونيو 2021.

ذاته على تعزيز التعاون بين الجهات القضائية والأمنية، وعلى التنسيق مع الهيئات الدولية المختصة، ما يدل على البعد الشامل والمتعدد الأبعاد الذي تنتهجه الجزائر في مكافحة هذه الجرائم.

المطلب الثاني: الأجهزة الأمنية المختصة

إلى جانب الهيئة الوطنية، تضطلع الأجهزة الأمنية المختصة بدور أساسي في مكافحة الجرائم المعلوماتية، مستفيدة من إمكانياتها التقنية والبشرية. وسنتناول في هذا المطلب الوحدات التابعة للأمن الوطني في الفرع الأول، ثم ننتقل إلى دراسة الوحدات التابعة للدرك الوطني في الفرع الثاني.

الفرع الأول: الوحدات التابعة للأمن الوطني

يتجلى دور الأمن الوطني في مكافحة الجرائم المعلوماتية من خلال مديرية الشرطة القضائية، وبوجه خاص الفرقة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتُعنى هذه الفرقة بالتحقيق في الجرائم السيبرانية على المستوى الوطني، كما تستفيد من تجهيزات رقمية متطورة وخبرات بشرية متخصصة في مجالات تحليل الأدلة الرقمية وتتبع الأنشطة المشبوهة على شبكة الإنترنت.

كما تضم مختلف ولايات الوطن فرقًا محلية متخصصة في مكافحة الجرائم المعلوماتية، تعمل تحت إشراف رؤساء الأمن الولائي، وتقوم بالتنسيق مع النيابة العامة من أجل التحري، الضبط، والتحقيق، خصوصًا في الجرائم التي تمس بالأمن العام أو تنطوي على مساس بحرمة الحياة الخاصة عبر الوسائل الإلكترونية[1].

الفرع الثاني: الوحدات التابعة للدرك الوطني

يضطلع الدرك الوطني، باعتباره جهازًا ذا طابع عسكري ومكلفًا بمراقبة المناطق الريفية وشبه الحضرية، بدور بارز في مكافحة الجريمة المعلوماتية من خلال فصيلة التحقيق في الجرائم السيبرانية التابعة

[1] الجمهورية الجزائرية الديمقراطية الشعبية، وزارة الداخلية والجماعات المحلية، المديرية العامة للأمن الوطني، دليل الشرطة الجزائرية في مكافحة الجرائم الإلكترونية، ط.1، الجزائر، 2020، ص. 45-60.

للمصلحة المركزية للتحريات الجنائية .وتعمل هذه الفصيلة وفق آليات تنسيق دقيقة مع النيابة المختصة، كما تعتمد على تقنيات متقدمة في مجال التحليل الرقمي وتتبع العناوين الإلكترونية المجهولة.

كما أنشأ الدرك الوطني المنصة الوطنية للإبلاغ عن الجرائم المعلوماتية المعروفة باسم "PREVSEC"، والتي تسمح للمواطنين بالتبليغ عن أي فعل مشبوه عبر الإنترنت، وتشكل مصدرًا مهمًا لانطلاق التحقيقات السيبرانية. كما يخضع أعوان الدرك لتكوين دوري ومتخصص في مجال الأمن السيبراني، بالتعاون مع هيئات دولية مختصة[1].

المطلب الثالث: القطب الجزائي المتخصص في مكافحة جرائم الإعلام والاتصال

رغم الأهمية التي خص بها المشرع الجزائري الأقطاب الجزائية المتخصصة، إلا أنه لم يضع لها تعريفا محددا، وكانت بداية ظهور هذه الأقطاب مع صدور القانون: 04-14 المعدل والمتمم للأمر: 66-155 المتضمن قانون الإجراءات الجزائية، الذي تطرق في المواد ،37 ، 40 ، 329 إلى إمكانية تمديد الاختصاص الإقليمي لوكيل الجمهورية، قاضي التحقيق وقاضي الحكم، عندما يتعلق الأمر بالبحث والتحري عن جرائم محددة (جرائم المخدرات الجريمة المنظمة عبر الحدود الوطنية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات جرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف)[2].

ثم صدر المرسوم التنفيذي رقم 06-348 المؤرخ في: 05-10-2006 المعدل والمتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في: 17-10-2016[3]، الذي تضمن توسيع الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، وأعطى بذلك للجهات القضائية المتخصصة اختصاصا أوسع. ويمكن تعريف الأقطاب الجزائية المتخصصة من خلال استقراء النصوص القانونية المتعلقة بسيرها

[1] قيادة الدرك الوطني، التقرير السنوي حول الجرائم الإلكترونية في الجزائر، الجزائر، 2022، ص. 22-40. وكذلك: الموقع الرسمي لقيادة الدرك الوطني www.mdn.dz قسم الأمن السيبراني، تم الاطلاع عليه بتاريخ: 02 أبريل2025.

[2]تنص الفقرة 02 من المادة: 37 من ق إ ج :" يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

[3] المرسوم التنفيذي رقم 06-348 ، المؤرخ في: 05-10-2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج ر ، عدد 63 ، بتاريخ: 08-10-2006.

بأنها: "جهات قضائية متخصصة للنظر في بعض الجرائم التي حددها القانون، وليست جهات قضائية خاصة تنشط بإجراءات قانونية خاصة تخرج عن النظام القضائي ساري المفعول"[1].

الفرع الأول: الإطار القانوني والتنظيمي للقطب الجزائي المتخصص في مكافحة جرائم الإعلام والاتصال

يشكّل القطب الجزائي المتخصص في مكافحة جرائم الإعلام والاتصال آلية مؤسساتية أنشئت في سياق سعي الدولة الجزائرية إلى تطوير منظومتها القضائية لمواجهة التحديات المستجدة في الفضاء الرقمي، وهو ما تجسد في مجموعة من النصوص القانونية التي أرست الأساس التنظيمي والقانوني لهذا القطب.

وقد استند المشرّع في هذا الإطار إلى القانون رقم 09-04 المؤرخ في 5 أغسطس 2004 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، حيث نصّ هذا القانون على تجريم مجموعة من الأفعال التي ترتكب بواسطة الأنظمة المعلوماتية، مثل اختراق النظم، الاحتيال المعلوماتي، التعدي على الحياة الخاصة من خلال وسائل الاتصال، ونشر المحتويات غير القانونية عبر الشبكة العنكبوتية.

كما تعززت مكانة هذا القطب بموجب التعديل الدستوري لسنة 2020، والذي كرس صراحة في ديباجته وفي بعض مواده مسؤولية الدولة في حماية الفضاء السيبراني الوطني، وضمان أمن المعطيات الرقمية، وهو ما يبرر استحداث أجهزة قضائية متخصصة قادرة على التعامل مع هذا النوع المعقد من الجرائم ذات الطابع التقني والعابر للحدود.

[1] عميور خديجة، قواعد اختصاص الأقطاب الجزائية للنظر في جرائم الفساد، مجلة دراسات في الوظيفة العامة، العدد 02 جامعة جيجل، 2014، ص134.

[2] القانون رقم 09-04، المشار إليه سابقاً.

ويُعد القطب الجزائي المتخصص بمثابة محكمة نوعية داخل المنظومة القضائية الوطنية، يتمتع باختصاص نوعي في نظر الجرائم المرتبطة بالإعلام والاتصال، ويضم في تشكيلته قضاة ذوي تكوين متخصص في الميدان الرقمي، ما يضمن فعالية الإجراءات واستيعاب خصوصيات الجريمة السيبراني[1]ة.

الفرع الثاني: المهام القضائية والأبعاد الاستراتيجية للقطب في حماية الفضاء السيبراني

يضطلع القطب الجزائي المتخصص بجملة من المهام القضائية والفنية التي تهدف إلى ضمان حماية شاملة ومتكاملة للفضاء الرقمي الوطني، وذلك من خلال اعتماد مقاربة متعددة الأبعاد تجمع بين التحري، التحليل، الردع، والوقاية. فعلى المستوى القضائي، يختص القطب بالتحقيق في الجرائم السيبرانية المعقدة، مثل: اختراق قواعد البيانات، الهجمات السيبرانية، سرقة الهوية الرقمية، والاحتيال المالي الإلكتروني. كما يتولى مهمة جمع الأدلة الرقمية وتحليلها بالاعتماد على تقنيات الطب الشرعي الرقمي، بالتعاون مع خبراء في الأمن السيبراني، ما يسمح بتقديم قرائن فنية ذات حجية أمام القضاء.

أما على المستوى التنسيقي، فإن القطب يعمل بتكامل مع الهيئة الوطنية للوقاية من جرائم الإعلام والاتصال، مما يُعزز منظومة تبادل المعلومات ورصد التهديدات بشكل وقائي واستباقي. كما يشارك في عمليات التعاون القضائي والأمني الدولي، لاسيما مع أجهزة مثل الإنتربول والأفريبول، بغية تتبع الشبكات الإجرامية العابرة للحدود.

وفي سياق مواكبة التطورات الرقمية، يلعب القطب دورًا استراتيجيًا في اقتراح تعديلات تشريعية لتكييف القوانين الوطنية مع التحديات الجديدة كجرائم الذكاء الاصطناعي، العملات الرقمية، والجرائم الواقعة عبر تطبيقات مشفّرة.

غير أن فاعلية القطب تواجه جملة من التحديات، من بينها نقص الكفاءات التقنية لدى بعض الجهات القضائية، وتسارع تطور الوسائل التقنية للجريمة مقارنة بقدرة التشريعات على التكيّف. لذلك، توصي الدراسات القانونية بضرورة تعزيز التكوين المتخصص للقضاة، وتحديث النصوص القانونية بصفة دورية، وتعزيز التعاون الإقليمي والدولي في مجال مكافحة الجريمة الإلكترونية.

[1] القانون رقم 09-04، المشار إليه سابقاً.

المبحث الثاني: إجراءات التحقيق للكشف عن الجرائم المعلوماتية

تُعدّ إجراءات التحقيق في الجرائم المعلوماتية من الخطوات الجوهرية لكشف هذا النوع المعقد من الجرائم. فهي تعتمد على تقنيات رقمية متطورة لجمع الأدلة وتتطلب خبرات فنية متخصصة. وتكمن أهميتها في تتبع الآثار الإلكترونية وتحديد هوية الجناة لضمان محاسبتهم قانونيًا.

معظم التشريعات الجنائية لم تضع تعريفاً للتحقيق، فذلك ليس قصوراً منها لأن وضع التعريفات ليست من أعمال المشرع وانما من اختصاص الفقهاء كما ذكرنا سابقاً فإذا كان المشرع يعني احيانا بوضع بعض التعريفات ببعض تشريعاته فإنه لا يستهدف منها أغراضاً علمية محضة، بل يقصد من ورائها ترتيب آثار قانونية، لذا تعددت التعريفات الفقهية للتحقيق الجنائي[1].

المطلب الأول: الأساليب التقليدية في التحقيق في الجرائم المعلوماتية

إنَّ الأساليب التقليدية في التحقيق الجنائي محدودة الفعالية عند التعامل مع الجرائم المعلوماتية نظرًا لطبيعتها الرقمية والمعقدة. إذ تعتمد هذه الأساليب على جمع الأدلة المادية والاستجواب المباشر، وهو ما لا يتناسب مع طبيعة الجرائم التي تُرتكب عبر الشبكات والأنظمة الإلكترونية. لذلك بات من الضروري تطوير منهجيات متخصصة تواكب تطور الجريمة المعلوماتية.

الفرع الأول: معاينة مسرح الجريمة

تعتبر معاينة مسرح الجريمة من أولى الخطوات الحاسمة في التحقيق الجنائي، حيث تُوفر للمحققين الأدلة الأولية التي تسهم في كشف ملابسات الجريمة. تتطلب هذه العملية دقة وتنظيماً عاليين لضمان توثيق كل التفاصيل المادية والبيئية. ومن خلال المعاينة، يمكن إعادة تشكيل الأحداث وتحديد الأدوات أو الأشخاص المحتمل تورطهم في الجريمة.

[1] محمد سعيد نمور، أصول الإجراءات الجزائية، شرح لقانون أصول المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، الطبعة الثانية، عمان، 2011، ص327.

أولاً: معاينة الجرائم على المكونات المادية للحاسوب

تُعد المكونات المادية للحاسوب (كالأجهزة، الخوادم، الهواتف الذكية، أو الوسائط التخزينية) محورًا رئيسيًا في التحقيقات الجنائية المعلوماتية. وفقًا للتشريع الجزائري، تُنظم عملية المعاينة بموجب المادة 03 من القانون 09-04 [1]، والمتعلق بقواعد الوقاية من الجرائم المتصلة بتكنولوجيا المعلومات ومكافحتها، والتي تُلزم السلطات المختصة بضبط الأدلة المادية وحفظها وفق إجراءات تقنية وقانونية دقيقة.

في إطار مكافحة الجرائم المعلوماتية في الجزائر، تُنظَّم إجراءات مصادرة الأجهزة الإلكترونية وتحليل الأدلة الرقمية ضمن إطار قانوني صارم يضمن احترام الحقوق الأساسية ويُعزز مصداقية الأدلة. أولًا، الحصول على إذن قضائي مسبق يُعد شرطًا جوهريًّا بموجب مبدأ الشرعية المنصوص عليه في المادة 47 من الدستور الجزائري، والتي تؤكد أن التدابير الإكراهية لا تُتخذ إلا بأمر قضائي. يُلزم هذا الإجراء السلطات الأمنية بتقديم طلب مُفصَّل يوضح الأسباب الجرمية المبررة للمصادرة، مما يحول دون التعسف ويحمي خصوصية الأفراد. ثانيًا، يخضع توثيق مسرح الجريمة الرقمية لمعايير دقيقة تشمل تسجيل الحالة الأولية للأجهزة وبياناتها عبر تقنيات التصوير الفوتوغرافي، وتسجيلات الفيديو، وإعداد تقارير فنية تُوثق أوصاف المكونات المادية والبرمجية وربطها بالوقائع الجنائية، مثل نسخ الهاش (Hash) للبيانات لتأكيد سلامتها. ثالثًا، يُفرض استخدام أدوات فنية متخصصة كأجهزة عزل البيانات) مثل «الكتابة العازلة» أو (Write Blockersالتي تمنع تعديل المحتوى الرقمي أثناء الحجز أو التحليل، وفقًا للمرسوم التنفيذي رقم 11-276[2]، الذي يُلزم بضمان سلامة الأدلة من العبث أو التلف. تُجرى هذه الإجراءات تحت إشراف خبراء مُعتمدين لتعزيز الحجية القضائية للأدلة، مع إرفاق شهادات ضبط الجودة في التقارير النهائية، مما يعكس التكامل بين الإطار القانوني والتقني في مواجهة التحديات الإلكترونية الحديثة.

[1] المادة 03 من القانون 09-04، المشار إليه سابقاً.

[2] المرسوم التنفيذي رقم 11-276 المؤرخ في 24 أغسطس 2011، العدد 53، هو مرسوم يتعلق بشروط وأساليب مكافحة الجرائم المعلوماتية في الجزائر. يهدف هذا المرسوم إلى تحديد الإجراءات والضمانات اللازمة لمكافحة الجرائم التي ترتكب باستخدام تكنولوجيا المعلومات والاتصالات، مثل القرصنة الإلكترونية، الاحتيال الإلكتروني، التجسس، التحرش الإلكتروني، وتوزيع المعلومات الكاذبة.

ثانياً: معاينة الجرائم على المكونات غير المادية

شهد التشريع الجزائري تطورًا لافتًا في مجال مكافحة الجرائم الموجهة ضد المكونات غير المادية، لا سيما تلك المرتبطة بالبيانات الرقمية والملكية الفكرية، وذلك من خلال إصدار مجموعة من القوانين الحديثة التي تواكب التغيرات التكنولوجية المتسارعة.

كما جاء القانون 09-04 ليعزز الوقاية من جرائم تقنية المعلومات، حيث جرم اختراق البنى التحتية ونشر البرمجيات الضارة، مع ربط بعض الجرائم الإلكترونية بأفعال إرهابية. وفي سياق حماية المعاملات الرقمية، نص قانون 18-05 على تجريم التزوير الإلكتروني وانتحال الهوية، بينما اهتم قانون 03-14 بحماية الملكية الفكرية من خلال تجريم قرصنة البرمجيات وتوزيع المحتوى المنسوخ[1]. غير أن هذا التطور التشريعي يواجه تحديات عدة، أبرزها محدودية المرونة في مواكبة الجرائم المستحدثة وضعف التنسيق الدولي، خاصة مع عدم انضمام الجزائر لاتفاقية بودابست، فضلاً عن نقص التوعية المجتمعية. لذلك، فإن فعالية هذه المنظومة القانونية تبقى مرهونة بتعزيز الآليات التنفيذية وتكثيف الجهود التعاونية على المستويين الوطني والدولي.

الفرع الثاني: تفتيش الأنظمة المعلوماتية

يُعدّ تفتيش الأنظمة المعلوماتية إجراءً قانونيًا يُلجأ إليه للكشف عن الجرائم المعلوماتية وجمع الأدلة الرقمية المخزنة داخل الحواسيب أو الخوادم أو أي وسيلة إلكترونية. يهدف هذا التفتيش إلى ضمان سلامة المعلومات وعدم التلاعب بها قبل تحليلها قضائيًا. ويُمارس وفقًا لضوابط قانونية صارمة لحماية الخصوصية وضمان احترام الحقوق الأساسية للأفراد.

[1] القانون رقم 18-05، المشار إليه سابقاً.

أولاً: تفتيش نظم الحاسوب

غير أن المشرع الجزائري ومن خلال نفس النص القانوني أكد على أنه لا يجوز إجراء عمليات المراقبة في الحالات السابقة المذكورة إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة. القواعد الإجرائية تضمنت المواد من 5 إلى 9 من القانون 09-04 مجموعة من القواعد الإجرائية التي تهدف إلى الوقاية من الجرائم الالكترونية ومكافحتها، وتتمثل هذه الإجراءات في:

-تفتيش المنظومات المعلوماتية[1]، حيث يجوز للسلطات القضائية في إطار قانون الإجراءات الجزائية وفي الحالات التي تسمح باللجوء إلى المراقبة الالكترونية التي سبق وأشرنا إليها الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، وإلى منظومة تخزين معلوماتية.

وإذا تبين أن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل، كما يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

- **حجز المعطيات المعلوماتية:** عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم ومرتكبيها يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، وإذا استحال إجراء الحجز لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي

[1] المواد من 05 إلى 09 من القانون 09-04، المشار إليه سابقاً.

تحتويها المنظومة المعلوماتية والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة[1].

وفي إطار ممارسة سلطة التفتيش يمكن للسلطة التي تباشر هذه الإجراءات أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، وتستعين في ذلك بالأشخاص المؤهلين لاستعمال الوسائل التقنية المناسبة لذلك[2].

-إلزام مقدمي الخدمات بضرورة المساهمة في الوقاية من الجرام الالكترونية: فرض القانون 09/04 على مقدمي الخدمات مجموعة من الالتزامات تساهم بدورها في الوقاية من الجرائم الالكترونية ومكافحتها، وتتمثل أهم هذه الالتزامات:

-تقديم المساعدة للسلطات، حيث يجب على مقدمي الخدمات تقديم المساعدة اللازمة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات، وبوضع المعطيات التي يتعين حفظها تحت تصرف السلطات المكلفة بالتحريات القضائية، كما يتعين على مقدمي الخدمات في إطار هذه المساعدة كتمان سرية العمليات التي ينجزونها بطلب من المحققين، وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق[3].

- **حفظ المعطيات المتعلقة بحركة السير**: يلتزم مقدمو الخدمات بحفظ ما يلي[4]:
  - المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
  - المعطيات المتعلقة بالتجهيزات المستعملة للاتصال.
  - المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

[1] المواد 06 و07 و08 القانون 09-04، المشار إليه سابقاً

[2] المادة 08 القانون 09-04، من نفس المرجع.

[3] المادة 10 القانون 09-04، مرجع نفسه.

[4] المادة 11 القانون 09-04، مرجع نفسه.

- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم بالاتصال وكذا عناوين المواقع المطلع عليها.

إضافة إلى ما سبق خص المشرع الجزائري مقدمي خدمة الانترنيت بالتزامات معينة تهدف كذلك إلى الوقاية من الجرائم الالكترونية ومكافحتها، وتتمثل هذه الالتزامات في[1]:

- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.
- وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة واخبار المشتركين لديهم بوجودها.
- إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته نفصل مهام الهيئة ودورها في الوقاية من الجرائم الالكترونية ومكافحتها في جزئية لاحقة من دراستنا والمتعلقة بمكافحة الجريمة الالكترونية بموجب الهياكل الخاصة.

➢ **التعاون والمساعدة القضائية الدولية:** أقر المشرع الجزائري من خلال القانون 04/09 أن المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني[2]. وفي إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم الالكترونية وكشف مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الالكتروني[3]، غير أنه يرفض تنفيذ طلبات المساعدة القضائية الدولية إذا كان من شأنها المساس بالسيادة الوطنية أو النظام العام

[1] المادة 12 القانون 09-04، المشار إليه سابقاً.
[2] المادة 15 القانون 09-04، المرجع نفسه.
[3] المادة 16 القانون 09-04، المرجع نفسه.

كما يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب[1]

المطلب الثاني: أساليب البحث والتحري الخاصة

حاول المشرع الجزائري من خلال تقنين أساليب التحري الخاصة أن يوازن بين ضرورة الوصول إلى الحقيقة في الجرائم الخطيرة وحماية الحقوق والحريات الأساسية للأفراد، وقد تمثلت أبرز هذه الأساليب في اعتراض المراسلات بمختلف أشكالها، والتقاط الصور وتسجيل الأصوات دون علم المعني بالأمر، بالإضافة إلى تقنية "التسرب" التي تُمكن الجهات الأمنية من التسلل إلى الجماعات الإجرامية بهدف جمع الأدلة. وتُطبق هذه الوسائل ضمن شروط قانونية صارمة وتحت رقابة قضائية لضمان مشروعيتها وعدم المساس بحقوق المتهمين.

الفرع الأول: أساليب اعتراض المراسلات وتسجيل المحادثات

تُعد أساليب اعتراض المراسلات وتسجيل المحادثات من أبرز الوسائل التي قد تُستخدم في إطار التحري أو التحقيق الجنائي، لكنها تمسّ بشكل مباشر الحق في الخصوصية. ونظرًا لخطورتها، فقد أحاطها المشرّع بضوابط قانونية صارمة توازن بين متطلبات العدالة واحترام الحقوق والحريات الأساسية. ويستوجب اللجوء إليها ترخيصًا قضائيًا مسبقًا، وتطبيقًا محدودًا في حالات الضرورة القصوى التي تهدد الأمن أو النظام العام.

أولاً: اعتراض المراسلات

يقصد باعتراض المراسلات التتبع السري والمتواصل للمشتبه به قبل وبعد ارتكابه للجريمة ثم القبض عليه متلبس بها، كم يعرف على أنه إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة[2].

[1] المادة 18 القانون 09-04، المشار إليه سابقاً.

[2] ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، الطبعة الأولى، دار المطبوعات الجامعية، 2009، جامعة القاهرة، ص15.

ولقد نص المشرع الجزائري بموجب المادة 65 مكرر 5 من قانون الإجراءات الجزائية أنه يجوز لوكيل الجمهورية أو لقاضي التحقيق في حالة فتح تحقيق قضائي أن يأذن لضابط الشرطة القضائية بترخيص كتابي، وتحت إشرافه مباشرة للقيام باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع الترتيبات التقنية دون موافقة الشخص المعني من أجل القيام بالتقاط وتثبيت وبث وتسجيل الكلام في سرية من طرف أي شخص وفي أي مكان عام أو خاص والتقاط الصور ولكل شخص ونظرا لخطورة هذا الإجراء وتعارضه أحيانا مع حماية الحياة الخاصة مصلحة المجتمع في محاربة الجرائم المنصوص عليها على سبيل الحصر في المادة 65 مكرر 5 من القانون 22/06 المعدل والمتمم لقانون الإجراءات الجزائية، قيده المشرع بشروط معينة منها: عدم حجز المراسلات البريدية والالكترونية إلا بإذن من السلطة القضائية المختصة، وأن تكون الجريمة جناية أو جنحة، وأن يكون الحجز والإحتفاظ بالرسائل والمراسلات في حدود ما هو مفيد لإظهار الحقيقية، ويعاد الباقي إلى صاحبه أو يسلم إلى المرسل إليه أو يترك خارج الملف[1].

ثانياً: تسجيل الأصوات:

إن التنصت كمفردة يعبر عنها البعض بكلمة التصنت للتعبير عن فعل الإصغاء والاستماع إلى محادثات بشتى الوسائل، وبالرجوع إلى المعاجم العربية والفرنسية نجد مفردة واحدة هي التنصت لكن مفهوم التشريع للتنصت يختلف عن المفهوم اللغوي لكونه مخصص للجريمة، وحتى وإن اختلفت التسميات فهي تؤدي إلى نفس المعنى، ويعد التشريع الوطني من بين التشريعات التي انتهجت أسلوب التنصت في التحريات القضائية[2].

ولم ينص المشرع الجزائري على تعريف التسجيل الصوتي، كما لم ينص على إجراء اعتراض المراسلات، وإنما أشار لها في المادة 65 مكرر 05 فقرة 02 من قانون الإجراءات الجزائية فيما يلي:

[1] أنظر المادتين 65 و65 مكرر 05 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

[2] عبد الحميد سفيان، أساليب التحري الخاصة في قانون الإجراءات الجزائية الجزائري، مجلة صوت القانون المجلد التاسع، العدد 02 (2023)، ص209-213

وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، ويفهم من الفقرة الثالثة من المادة 65 كرر 05 من القانون 22-06 المعدل والمتمم لقانون الإجراءات الجزائية التي أوردها المشرع[1]، أن الحديث الفردي الذي ينطق به الشخص حتى مع نفسه يمكن أن يكون صالحا للتجريم، كأن يسجل حديثه لنفسه" طالما أن المشرع استخدم عبارة تسجيل الكلام الذي يتفوه به المشتبه فيه"، ولم يستثني الحديث الذي يتلفظ به الشخص مع نفسه من النص القانوني. وسواء كان الكلام مباشرا أو كان مسجلا[2].

والتسجيل الصوتي المتخذ كوسيلة للتحري عن الجرائم يشمل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية[3].

وأجاز المشرع الجزائري لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له باستعمال الوسائل الخاصة في البحث والتحري ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينوبه أن يسخر ويكلف كل عون مؤهل وصاحب خبرة في مجال المواصلات يعمل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية، لاستخدامه بالتكفل بالجوانب التقنية لعمليات اعتراض المراسلات وتسجيل الأصوات وهذا حسب ما جاء في نص المادة 65 مكرر 08 من قانون الإجراءات الجزائية[4].

[1] المادة 65 مكرر 5 من القانون 22-06 التي تعدل وتتمم قانون الإجراءات الجزائية، تتعلق بإجراءات التحري الخاصة، مثل اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، في جرائم معينة، بحسب ASJP. هذه الإجراءات تستخدم للبحث عن أدلة في قضايا مثل الفساد، ولكنها تخضع لإجراءات قضائية صارمة وضوابط قانونية.

[2] مجراب الدوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة الدكتوراه علوم في القانون العام، كلية الحقوق، السنة الجامعية 2016/2015، ص239-240.

[3] مقني بن عمار بوراس عبد القادر، التنصت على المكالمات الهاتفية واعتراض المراسلات كآلية للوقاية من جرائم الفساد، الملتقى الوطني حول الآليات القانونية لمكافحة الفساد جامعة ورقلة، 2 و3 ديسمبر 2008، ص14.

[4] أنظر المادة 65 مكرر 08 من قانون الإجراءات الجزائية.

ثالثاً: التقاط الصور

لقد كان البحث والتحري في الجريمة إلى عهد غير قريب يستخدم أسلوب مكمل لتسجيل الواقعة الإجرامية بالكتابة وهي الصورة الفوتوغرافية التي تحل محل الأشياء التي لا يمكن للشخص التعبير عنها بالكتابة، وكانت الصورة في حد ذاتها ولازالت إلى يومنا هذا تحقق جملة من الفوائد من بينها إتاحتها للمحقق الإطلاع على محل الحادث كلما أراد ذلك، اضافة الى الاحتفاظ بمسرح الجريمة على الحالة التي كانت عليها وقت ارتكابها، لفترة طويلة من الزمن، وكذا إظهار آثار الجريمة مما يتيح للمحقق مراجعتها والتدقيق فيها[1].

وتعتبر عملية التقاط الصور الفوتوغرافية من التقنيات المستحدثة التي جاء بها المشرع الجزائري فيما يخص البحث والتحري عن جرائم الفساد بأسلوب التصوير بمختلف أنواعه، وقد عبر عن عملية التصوير أو التقاط الصور في قانون الإجراءات الجزائية في نص المادة 65 مكرر 09 بعبارة الالتقاط وإنَّ هذا الإجراء يقوم أساسا على استخدام الكاميرات أو أجهزة خاصة تلتقط الصور والصوت لوضعية شخص أو عدة أشخاص مشتبه في أمرهم، على الحالة التي كانوا عليها وقت التصوير لغرض استخدام محتوى الفيلم كمادة إثبات ودليل مادي، ويمكن ضابط الشرطة القضائية من سماع ورؤية ما يدور في حياة المشتبه فيه طوال مدة التحري والبحث، ومن خلالها يلزم ضابط الشرطة القضائية بتحرير محضر عن العملية التي قام بها وتسجيل تاريخ وساعة بدايتها ونهايتها كما يتعين عليه أن يصف المراسلات والصور والمحادثات المسجلة في محضر يودع بالملف وفقا لما نصت عليه المادتين 65 مكرر 09 و65 مكرر 10 قانون الإجراءات الجزائية[2].

[1] محمد حماد مرهج الهيتي، أصول البحث والتحقيق الجنائي موضوعة، أشخاصه، القواعد التي تحكمه، الطبعة 2014، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، الإمارات، ص334-335.

[2] أنظر المادتين 65 مكرر 09 و65 مكرر 10 من المادة 65 مكرر من قانون الإجراءات الجزائية الجزائري تتعلق بحماية المتهمين من الكشف عن هوياتهم. تُحظر الإفصاح عن هوية المتهم دون موافقته، ويُعاقَب من يَتَسَرَب أو يُكشف عن هويته بالعقوبات المنصوص عليها في المادة.

وفي حالة القيام بهذا الإجراء دون إذن مكتوب ومسبب ومحدد المدة من طرف الجهة القضائية المختصة، يكون مرتكبا لجنحة المساس بحرمة الحياة الخاصة ويعاقب القانون على هذا الفعل بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات، وبغرامة مالية من 50.000 دج إلى 300.000 دج وفقا لنص المادة 303 مكرر من قانون العقوبات[1].

رابعاً: التسرب

التسرب لغة مشتق من الفعل تسرب تسربا أي دخل وانتقل خفية وهي الولوج والدخول بطريقة أو بأخرى إلى مكان أو جماعة[2]. ويقصد بالتسرب اصطلاحا: " الولوج بطريقة سرية إلى مكان ما أو جماعة وجعلهم يعتقدون بأن المتسرب ليس غريبا عنهم وعن حوارهم، وطمأنتهم بأنه واحد منهم وهو ما يسهل له معرفة انشغالاتهم وتوجهاتهم وأهدافهم المستقبلية[3].

كما يعرف التسرب على أنه: "تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط الشرطة القضائية أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه فاعل أو شريك"[4]، فيكون المتسرب في اتصال مع الأشخاص المشتبه فيهم ويربط معهم علاقات ضيقة للمحافظة على السر المهني، حتى الوصول إلى الأهداف المرجوة من هاته العملية وفي الوقت المحدد لها[5].

ويعد التسرب أو الاختراق تقنية جديدة أدرجها المشرع في تعديل قانون الإجراءات الجزائية سنة 2006، وأورد المشرع تعريفا له في المادة: 65 مكرر 12 من قانون الإجراءات الجزائية في الفقرة الأولى

[1] أنظر المادة 303 مكرر من قانون العقوبات.

[2] ابن منظور، لسان العرب، طبعة مراجعة ومصححة، ج 1، دار الحديث، القاهرة، مصر، 711هـ، ص1200.

[3] هوام علوة، التسرب كآلية للكشف عن الجرائم في ق.إ.ج.ج، مجلة الفقه والقانون، باتنة، الجزائر، 2012، ص02.

[4] عبد الرحمان خلفي محاضرات في قانون الإجراءات الجزائية، دار الهدى، بجاية، ص 75 15 فوزي عمارة: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب إجراءات تحقيق قضائي في مواد الجزائية، مجلة العلوم الإنسانية، العدد 33، جامعة منتوري، قسنطينة، جوان 2010، ص245.

[5] أنظر المادة 65 مكرر 14 من قانون الإجراءات الجزائية المعدل والمتمم.

منها كالآتي: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة إيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

والتسرب أو الاختراق يسمح لضابط أو عون الشرطة القضائية المرخص له بإجراء عملية التسرب والأشخاص الذين يسخرون لهذا الغرض، دون أن يكونوا مسؤولين جزائيا[1].

الفرع الثاني: الأساليب المبتكرة مثل التسرب أو الاختراق

بما أن التسرب هي عبارة عن تقنية جديدة من تقنيات البحث والتحري الخاصة، التي أدرجها المشرع الجزائري في تعديل قانون الإجراءات الجزائية لسنة 2006 عندما تقتضي ضرورات البحث والتحري أو التحقيق في إحدى الجرائم الواردة على سبيل الحصر، وكما أنه تقنية من تقنيات التحري التي تسمح للشخص التوغل داخل جماعة إجرامية، فإن المشرع الجزائري نجده قد احاط هذه العملية بمجموعة من الشروط كما أعطى بعض الصفات التي ينبغي أن يتسرب بها العون، المتمثلة في السرية والخديعة واستعمال الهوية المستعارة.

كما جعل المتسرب يظهر كفاعل أصلي في العملية أو شريك فيها أو خاف، إلى جانب أنه قد حدد الجهات التي خول لها مراقبة العملية وكذا تلك الجهات المختصة في تنفيذها.

لقد عرفه المشرع الجزائري في نص المادة 65 مكر 12 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية على أنه يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف، وهو التعريف المتطابق للتعريف الذي قدمه المشرع الفرنسي للتسرب في نص المادة 706-81-03 من قانون الإجراءات الجزائية الفرنسي[2]، على عكس

[1] أنظر المادة 65 مكرر 14 من قانون الإجراءات الجزائية.

[2] coordonne l'opération, qui comprend les éléments strictement nécessaires a la constatation des infractions et ne mettant pas en danger la sécurité de l'agent infiltré et des personnes requises au sens de l'article 706-82 >>

ما جاء بمسودة مشروع قانون يقضي بتغيير وتتميم قانون المسطرة الجنائية المغربية، التي نصت على إمكانية اللجوء إلى التسرب أو "الإختراق دون أن يعطى من خلالها تعريفا دقيقا له[1].

ومن خلال التعاريف السابقة للتسرب أو الإختراق، فإنه يمكننا نحن بدورنا أن نعرفه على أنه" وسيلة أو إجراء قانوني مخول لضباط الشرطة القضائية خلال القيام بمهمة البحث والتحري الخاصة عن بعض الجرائم الخطيرة والحديثة، وهذا بإذن من النيابة العامة وتحت إشراف ومراقبة السلطة القضائية، حيث من خلاله تستخدم بعض التقنيات والتسرب او التوغل داخل الجماعة الإجرامية والتظاهر بالإشتراك في الجريمة، قصد جمع الأدلة عنها والكشف عن مرتكبيها".

إن التسرب الذي يقوم به ضابط أو عون الشرطة القضائية قد يظهر فيه دوره كفاعل أصلي في الجريمة أو يظهر فيه كشريك لها، كما قد يمكن له إخفاء الأشياء المتحصل عليها من الجريمة لإيهام الأشخاص المشتبه فيهم بأنهم جزءا منهم، إلى جانب أن العملية أعطيت صلاحية منحها لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية المختص إقليميا.

لقد نصت المادة 65 مكرر 12 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية على أنه: " يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة أو بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف.

من خلال نص المادة 65 مكرر 12 السالفة الذكر نستخلص أن المشرع الجزائري قد حدد ثلاثة صور يتم بها التسرب وهي إعتبار الضابط أو العون المتسرب كفاعل أصلي أو شريك، أو يتم التسرب

- art 706-81-3 "l'infiltration fait l'objet d'un rapport rédigé par l'officier de police judiciaire ayant

[1] أنظر مسودة مشروع قانون يقضي بتغيير وتتميم قانون المسطرة الجنائية المتاح على الموقع الإلكتروني لوزارة العدل المغربية:
www.justice .gov.ma والذي تم الإطلاع عليها بتاريخ 27/06/2017 على الساعة 22:00 ، كما تجدر الإشارة إلى أن مسودة المشروع منبثقة عن توصيات الحوار الوطني الشامل والعميق لإصلاح منظومة العدالة الذي أصدرته مؤخرا وزارة العدل والحريات المغربية الذي جاء ليعدل ويتمم القانون الحالي رقم 01-22 المتعلق بالمسطرة الجنائية الصادر بتنفيذه الظهير الشريف رقم 1.02.255 الصادر في 25 ديجنبر 1432 الموافق 03 أكتوبر 2002 الجريدة الرسمية عدد 5078 بتاريخ 27 ذي القعدة الموافق 30 يناير 2003، هي مسودة شبه نهائية تم إقرارها سنة 2014 وغير مصادق عليها بعد في إنتظار المصادقة عليها لتعد بمثابة قانون معدل ومتمم للقانون رقم 01-22 المتعلق بالمسطرة الجنائية.

خفية، وهي نفس الصور التي جاء بها المشرع الفرنسي في نص المادة 706-81 من قانون الإجراءات الجزائية الفرنسي التي نصت على أنه يمكن لضابط الشرطة القضائية أو عون الشرطة القضائية المتسرب التظاهر أمام الأشخاص المجرمين كأشخاص فاعلين أو شركاء أو متلقين[1]، والتي حددتها كذلك مسودة مشروع قانون يقضي بتغيير وتتميم قانون المسطرة الجنائية المغربية في نص المادة 82-11 منها، التي نصت على أنه:" يتيح الإختراق الضابط أو عون الشرطة القضائية المختص تحت إشراف ومراقبة النيابة العامة تتبع ومراقبة الأشخاص المشتبه فيهم من خلال التظاهر أما هؤلاء الأشخاص بأنه فاعل، أو شريك أو مساهم أو مستفيد من الأفعال الإجرامية موضوع البحث، ويمكنه لهذه الغاية إستعمال هوية مستعارة، كما يمكنه عند الضرورة إرتكاب إحدى الأفعال المبينة في المادة 82-12 بعده.

ويعتبر فاعلا وفق نص المادة 41 من الأمر 15666 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم، كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة إستعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي[2]، إذ أنه ولكي يتوصل ضابط أو عون الشرطة القضائية المأذون له بعملية التسرب إلى الهدف المنشود، لابد أن يتصرفوا مع المشتبه فيهم كأنهم عناصر منهم وفاعلين مساهمين في الجريمة، لكسب ثقتهم وللحصول على دليل مادي الإيقاع المشتبه فيهم وليس لتحريضهم على ارتكاب الجريمة[3].

كما عرف المشرع الجزائري الشريك في الجريمة في المادة 42 من الأمر 66-156 المتضمن قانون العقوبات الجزائري المعدل والمتمم على أنه كل شخص لم يشترك إشتراكا مباشرا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على إرتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه

[1] 13art 706-81 «...l'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilite dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire charger de coordonner l'opération a surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes comme un de leurs coauteurs, complices ou receleurs... >>>

[2] أنظر المادة 41 من الأمر 66-156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم، ج.ر.ع 49 الصادرة بتاريخ: 1966/07/11.

[3] مجراب الذوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم في القانون العام. جامعة الجزائر 01 بن يوسف بن خدة كلية الحقوق السنة الجامعية 2015 2016، ص364.

بذلك[1]، كما حدد الأشخاص الذين يدخلون في حكم الشريك بموجب المادة 43 من ذات الأمر وهو كل شخص إعتاد أن يقدم مسكنا أو مكانا للاجتماع الواحد أو أكثر من الأشرار الذين يمارسون اللصوصية أو العنف ضد أمن الدولة والأمن العام والأشخاص والأموال مع علمه بسلوكهم الإجرامي[2].

وعملا بمحتوى هذه النصوص القانونية الخاصة بالشريك، فإنه يعتبر عون أو ضابط الشرطة القضائية المأذون له بعملية التسرب وكذا العون المسخر شركاء في الجريمة، بالنظر إلى المساعدة المادية والمعنوية التي يقدمونها للمشتبه فيهم لإنجاز مخططاتهم الإجرامية، لكن دون أن يكونوا مسؤوليين جزائيا عن ذلك لأنها تدخل ضمن الأفعال المبررة.

كما جعل المشرع الجزائري وعلى غرار المشرعين الفرنسي وما جاء بمسودة مشروع قانون يقضي بتغيير وتتميم قانون المسطرة الجنائية المغربية من بين الصور التي تتم بها عملية التسرب الإخفاء، والذي تطرقت إليه نص المادة 387 من الأمر 66-156 المتضمن قانون العقوبات الجزائري المعدل والمتمم[3]، والتي على حسبها يجوز لعون أو ضابط الشرطة القضائية المأذون له والمسخر للعملية، بأن يلجأ إلى إخفاء الأشياء المتحصل عليها من الجريمة لإيهام الأشخاص المشتبه فيهم بأنهم جزءا منهم، وهذا دون أن يرتب عليهم أية مسؤولية جزائية[4].

ويعتبر فاعلا وفق نص المادة 41 من الأمر 66-156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم، كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على إرتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة إستعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي[5]، إذ أنه ولكي يتوصل ضابط أو عون الشرطة القضائية المأذون له بعملية التسرب إلى الهدف

[1] أنظر المادة 42 من الأمر 66-150، المرجع السابق.

[2] أنظر المادة 43، المرجع نفسه.

[3] أنظر المادة 387، المرجع نفسه.

[4] مجراب الدوادي، المرجع السابق، ص365.

[5] أنظر: المادة 41 من الأمر 66-156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم، ج.ر.ع 49 الصادرة بتاريخ: 1966/07/11.

المنشود، لابد أن يتصرفوا مع المشتبه فيهم كأنهم عناصر منهم وفاعلين مساهمين في الجريمة، لكسب ثقتهم وللحصول على دليل مادي الإيقاع المشتبه فيهم وليس لتحريضهم على إرتكاب الجريمة[1].

كما عرف المشرع الجزائري الشريك في الجريمة في المادة 42 من الأمر 66-156 المتضمن قانون العقوبات الجزائري المعدل والمتمم على أنه كل شخص لم يشترك إشتراكا مباشرا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على إرتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك[2]، كما حدد الأشخاص الذين يدخلون في حكم الشريك بموجب المادة 43 من ذات الأمر وهو كل شخص إعتاد أن يقدم مسكنا أو مكانا للإجتماع لواحد أو أكثر من الأشرار الذين يمارسون اللصوصية أو العنف ضد أمن الدولة والأمن العام والأشخاص والأموال مع علمه بسلوكهم الإجرامي[3].

وعملا بمحتوى هذه النصوص القانونية الخاصة بالشريك، فإنه يعتبر عون أو ضابط الشرطة القضائية المأذون له بعملية التسرب وكذا العون المسخر شركاء في الجريمة، بالنظر إلى المساعدة المادية والمعنوية التي يقدمونها للمشتبه فيهم لإنجاز مخططاتهم الإجرامية، لكن دون أن يكونوا مسؤولين جزائيا عن ذلك لأنها تدخل ضمن الأفعال المبررة.

[1] مجراب الدوادي، المرجع السابق، ص 364.

[2] أنظر المادة 42 من الأمر 66-156، المرجع السابق.

[3] أنظر المادة 43، المرجع نفسه.

خـــــاتمة

خاتمة

في ختام هذا البحث حول الجريمة المعلوماتية في التشريع الجزائري، نلاحظ أن هذه الجريمة أصبحت من التحديات الكبرى التي تواجه الأنظمة القانونية في العصر الحديث. فقد أسهم التطور السريع للتكنولوجيا في ظهور أنواع جديدة من الجرائم التي تهدد أمن الأفراد والمجتمعات، مما يفرض ضرورة تحديث التشريعات القانونية لمواكبة هذه المتغيرات وتحمي المجتمع من أخطارها.

تناولنا في هذا البحث الإطار المفاهيمي للجريمة المعلوماتية، مع التطرق إلى صورها المختلفة مثل القرصنة الإلكترونية، التزوير الإلكتروني، الاحتيال عبر الإنترنت، وجرائم الاعتداء على البيانات الشخصية. كما تم تحليل أركان هذه الجرائم، من حيث الفاعل، الموضوع، والنتيجة، مع التأكيد على ضرورة وجود أدلة رقمية تفي بالمعايير القانونية لضمان صحة التحقيقات والمحاكمات.

فيما يتعلق بالحماية القانونية المقررة في التشريع الجزائري لمكافحة الجريمة المعلوماتية، فقد قامت الجزائر بسن عدة قوانين تستهدف مكافحة هذه الجرائم وحماية حقوق الأفراد والمجتمع، ومن أبرز هذه القوانين:

1. القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بمكافحة الجريمة الإلكترونية، والذي يُعد من أولى التشريعات التي تناولت هذا النوع من الجرائم في الجزائر. يحدد هذا القانون الجرائم الإلكترونية مثل القرصنة، التزوير الإلكتروني، والاحتيال عبر الإنترنت، ويحدد العقوبات المتعلقة بها.
2. القانون رقم 18-07 المؤرخ في 10 مايو 2018، المتعلق بحماية الأشخاص الطبيعيين في ما يخص معالجة البيانات ذات الطابع الشخصي .يهدف هذا القانون إلى تنظيم كيفية معالجة البيانات الشخصية وحمايتها من الاستغلال غير المشروع، وهو خطوة هامة في حماية حقوق الأفراد في العصر الرقمي.

رغم هذه الخطوات التشريعية المهمة، فإن التحديات التي تطرحها الجريمة المعلوماتية تقتضي من المشرع الجزائري الاستمرار في تحديث القوانين وتطوير آليات جديدة لمواكبة الابتكارات التكنولوجية. من الضروري أن تستمر الجزائر في تعزيز دور الأجهزة القضائية والأمنية لمكافحة الجرائم الإلكترونية بكفاءة، مع العمل على تحديث الأدوات القانونية لتظل قادرة على التعامل مع كافة أشكال الجرائم الرقمية الحديثة.

في الختام، تبقى الجريمة المعلوماتية من القضايا المحورية التي تتطلب جهودًا مستمرة من المشرع الجزائري لتوفير حماية قانونية فعالة، وخصوصًا في ظل التطور المستمر للتكنولوجيا. إن مواجهة هذه التحديات تستلزم أيضًا التعاون الدولي الفاعل في محاربة الجرائم الإلكترونية والحفاظ على أمان الشبكات والبيانات.

أهم النتائج:

1. **غموض المفهوم القانوني للجريمة المعلوماتية** :لا يزال المفهوم القانوني لهذه الجريمة يعاني من تباين في التعريف بين التشريعات، كما أنه في الجزائر لا توجد مادة قانونية موحدة تُعنى بهذا النوع من الجرائم بشكل مستقل، وإنما وردت أحكامها متفرقة في قوانين مختلفة (مثل قانون العقوبات، قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 2023).
2. **ضعف آليات الكشف الرقمي والتكوين** :تعاني الجهات المكلفة بإنفاذ القانون من نقص في الكوادر المؤهلة تقنيًا، إضافة إلى محدودية الوسائل التقنية المخصصة لرصد وتتبع الجرائم الإلكترونية، مما يؤثر على فعالية الكشف والملاحقة.
3. **الطابع العابر للحدود** :تمثل الطبيعة العابرة للحدود تحديًا كبيرًا أمام الأجهزة القضائية، لا سيما في غياب اتفاقيات ثنائية أو إقليمية فعالة في ميدان التعاون القضائي الرقمي.

الآفاق المستقبلية للتشريع الجزائري:

1. **تطوير تشريع خاص بالجريمة المعلوماتية** :من الضروري إصدار قانون شامل خاص بمكافحة الجريمة المعلوماتية يتضمن تعريفًا دقيقًا لها، وتصنيفًا واضحًا لصورها، وإجراءات خاصة بالتحقيق والمحاكمة والحماية الإلكترونية.

2. **تعزيز التعاون الدولي** :يجب على الجزائر الانخراط بشكل أكبر في الاتفاقيات الدولية (مثل اتفاقية بودابست) وتحديث آليات التعاون القضائي في ميدان الجريمة السيبرانية.

3. **تعزيز قدرات أجهزة إنفاذ القانون** :من خلال التكوين المستمر للضباط والقضاة، وتوفير وسائل متطورة للتحقيق الرقمي والردع الإلكتروني.

4. **تكريس التوعية الرقمية** :ينبغي إشراك المؤسسات التربوية والإعلامية في حملات توعية موجهة للمجتمع حول مخاطر الجريمة المعلوماتية وسبل الوقاية منها.

5. **ضمان التوازن بين الحماية والعقاب** :يجب أن يتوازن التشريع بين ضمان الأمن السيبراني وحقوق الأفراد في الخصوصية وحرية التعبير، وفقًا للمعايير الدولية لحقوق الإنسان.

قائمة المصادر والمراجع

I. المصادر

أولًا: النصوص القانونية

1. الأمر 66-156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم، ج.ر.ع 49 الصادرة بتاريخ: 1966/07/11.
2. القانون رقم 04-15 المؤرخ في 10نوفمبر 2004، الجريدة الرسمية، العدد 71.
3. المرسوم الرئاسي رقم 06-03 المؤرخ في 19جانفي 2006، يحدد قواعد التعاون الدولي في مكافحة الجرائم الإلكترونية.
4. قانون رقم 09-04 المؤرخ في 5أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
5. القانون رقم 15-03 المؤرخ في 1فيفري 2015، المتعلق بعصرنة العدالة في الجزائر.
6. القانون رقم 18-04 المؤرخ في 10ماي 2018، المتعلق بالبريد والاتصالات الإلكترونية، الجريدة الرسمية عدد 27.
7. القانون رقم 18-07 المؤرخ في 10جوان 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات.
8. القانون رقم 20-05 المؤرخ في 28أفريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.
9. الأمر رقم 21-09 المؤرخ في 8جوان 2021، المتعلق بحماية المعلومات والوثائق الإدارية.
10. المرسوم الرئاسي رقم 22-187 المؤرخ في 18ماي 2022، يتعلق بتعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات.
11. قانون العقوبات الجزائري.
12. قانون الإجراءات الجزائية.

ثانيًا: الوثائق الرسمية والتقارير

1. وزارة الداخلية والجماعات المحلية، *دليل الشرطة الجزائرية في مكافحة الجرائم الإلكترونية*، ط1، الجزائر، 2020.

2. قيادة الدرك الوطني، *التقرير السنوي حول الجرائم الإلكترونية في الجزائر*، الجزائر، 2022.]تم الاطلاع عليه من موقعwww.mdn.dz :، قسم الأمن السيبراني، بتاريخ 02 أبريل 2025.[

ثالثًا: الوثائق الدولية

1. قرارات الجمعية العامة للأمم المتحدة 63/55 (2000) و121/56 (2001) بشأن "مكافحة استخدام نظم المعلومات لأغراض إجرامية."

2. المادة 50 من العهد الدولي الخاص بالحقوق المدنية والسياسية.

3. أنظر مسودة مشروع قانون يقضي بتغيير وتتميم قانون المسطرة الجنائية المتاح على الموقع الإلكتروني لوزارة العدل المغربية: www.justice .gov.ma والذي تم الإطلاع عليها بتاريخ 27/06/2017 على الساعة 22:00 ، كما تجدر الإشارة إلى أن مسودة المشروع منبثقة عن توصيات الحوار الوطني الشامل والعميق لإصلاح منظومة العدالة الذي أصدرته مؤخرا وزارة العدل والحريات المغربية الذي جاء ليعدل ويتمم القانون الحالي رقم 01-22 المتعلق بالمسطرة الجنائية الصادر بتنفيذه الظهير الشريف رقم 1.02.255 الصادر في 25 ديجنبر 1432 الموافق 03 أكتوبر 2002 الجريدة الرسمية عدد 5078 بتاريخ 27 ذي القعدة الموافق 30 يناير 2003، هي مسودة شبه نهائية تم إقرارها سنة 2014 وغير مصادق عليها بعد في إنتظار المصادقة عليها لتعد بمثابة قانون معدل ومتمم للقانون رقم 01-22 المتعلق بالمسطرة الجنائية.

II. المراجع

أولاً: الكتب

1. أحسن بوسقيعة، الوجيز في القانون الجنائي العام، الطبعة 14، دار هومة، الجزائر، 2014.

2. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي للنشر والتوزيع، مصر، 2006.

3. بلعيد رشيد، الجرائم الإلكترونية في القانون الجزائري، دار النسر، 2020.

4. خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، 2008.

5. محمد أمين أحمد الشوابكة، جرائم الحاسوب الأولى والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2004.

6. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة.

7. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.

8. نهلا عبد القادر المومني، الجرائم المعلوماتية، ط2، دار الثقافة للنشر والتوزيع.

9. يونس عرب، موسوعة القانون وتقنية المعلومات: دليل أمن المعلومات والخصوصية، الجزء الأول، منشورات اتحاد المصارف العربية، 2002.

ثانياً: الرسائل الجامعية

1. مجراب الذوادي، الأساليب الخاصة للبحث والتحري في الجريمة المنظمة، أطروحة لنيل شهادة دكتوراه علوم في القانون العام. جامعة الجزائر 01 بن يوسف بن خدة كلية الحقوق السنة الجامعية 2015 2016.

2. عمار حشمان، *الجريمة المعلوماتية في التشريع الجزائري*، مذكرة ماستر، جامعة قاصدي مرباح، ورقلة، 2018–2019.

3. سعيدان نعيم، *آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري*، ماجستير، جامعة الحاج لخضر، باتنة، 2012–2013.

4. صغير يوسف، *الجريمة المرتكبة عبر الإنترنت*، ماجستير، جامعة مولود معمري، تيزي وزو، 2013.

5. عبد الكريم شيباني، *الحماية الإجرائية والموضوعية للجريمة المعلوماتية*، ماستر، جامعة د. الطاهر مولاي، سعيدة، 2015–2016.

6. مسعود شهيرة، *الجريمة الإلكترونية في التشريع الجزائري*، ماستر، جامعة عبد الحميد بن باديس، 2020–2021.

7. يوسف جفال، *التحقيق في الجريمة الإلكترونية*، مذكرة ماستر، 2016–2017.

ثالثًا: المقالات والدوريات العلمية

1. زهير خريبط خلف، "الجريمة الإلكترونية كوجه مستحدث من وجوه الجريمة"، *مجلة القرار للبحوث العلمية*، العدد 6، المجلد 2، 2024.

متاح على: https://www.elqarar.com/

2. عفاف بعون، نسيمة أولاد سالم، "الجريمة الإلكترونية – قراءة سوسيوتاريخية"، مجلة القبس للدراسات النفسية والاجتماعية، مجلد 5، عدد 20، 2023.

3. طيبي رتيبة، "العولمة وأثرها في بروز الجرائم المعلوماتية المستحدثة"، مجلة سوسيولوجيا الجريمة، جامعة البليدة2، 2021.

4. حمز خضري، عشاش حمزة، "خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري"، مجلة الدراسات القانونية والسياسية، مجلد 6، عدد 2، 2020.

5. محمود محمد صفاء الدين على شرشر، "الجهود الدولية والتشريعية لمكافحة جرائم الانترنت"، مجلة البحوث القانونية والعلوم الاقتصادية، المنوفية.

رابط: https://jslem.journals.ekb.eg/article_202042_ed932acc3346987c283aee46f8d66c2a.pdf

رابعاً: مراجع باللغة الأجنبية

coordonne l'opération, qui comprend les éléments strictement nécessaires a la constatation des infractions et ne mettant pas en danger la sécurité de l'agent infiltré et des personnes requises au sens de l'article 706-82 - << art 706-81-3 "l'infiltration fait l'objet d'un rapport rédigé par l'officier de police judiciaire ayant

فهرس المحتويات

الفصل الثاني: الحماية القانونية والكشف عن الجرائم المعلوماتية

ملخص:

يتناول هذا البحث الجريمة المعلوماتية من خلال محورين أساسيين، حيث يخصص الفصل الأول للإطار المفاهيمي للجريمة المعلوماتية، موضحًا مفهومها، خصائصها، أنواعها، وأسباب انتشارها في ظل تطور التكنولوجيا الرقمية. أما الفصل الثاني، فيركز على سبل الحماية القانونية المقررة في التشريع الجزائري، إضافة إلى الآليات التقنية والقضائية للكشف عنها ومتابعة مرتكبيها. يسلط البحث الضوء على التحديات التي تواجه الأجهزة الأمنية والقضائية، ويبرز أهمية التحديث التشريعي والتعاون الدولي في مكافحة هذا النوع من الجرائم المعقدة والعابرة للحدود.

الكلمات المفتاحية:

الجريمة المعلوماتية، الحماية القانونية، التشريع الجزائري، الأدلة الرقمية،الأمن السيبراني.

Abstract :

This research addresses cybercrime through two main axes. The first chapter is dedicated to the conceptual framework of cybercrime, explaining its definition, characteristics, types, and the reasons behind its spread in light of the development of digital technology. The second chapter focuses on the legal protection measures established in Algerian legislation, in addition to the technical and judicial mechanisms used to detect and prosecute perpetrators. The study highlights the challenges faced by security and judicial authorities and emphasizes the importance of legislative updates and international cooperation in combating this complex and transnational type of crime.

Keywords:

Cybercrime, Legal Protection, Algerian Legislation, Digital Evidence, Cybersecurity