

الآليات القانونية لمكافحة الجرائم السيبرانية في التشريع الجزائري: دراسة تحليلية.***Legal Mechanisms for Countering Cybercrimes in Algerian Legislation:
An Analytical Study.*****محمد صالح بن أمود*****Mohammad Salah ben Amoud****جامعة تامنغست - الجزائر -****University of Tamanrasset - Algeria -****sallahtinza@gmail.com**

تاريخ الاستلام: 2026/06/15 تاريخ القبول للنشر: 2026/09/18 تاريخ النشر: 2026/10/01

ملخص:

شهدت الجزائر في السنوات الأخيرة تقدماً ملموساً في مواجهة الجرائم السيبرانية من خلال إنشاء إطار قانوني متكامل يشمل تعديل أحكام قانون العقوبات، وإصدار نصوص قانونية خاصة، وتنظيم الإجراءات المتعلقة بالتحري والبحث عن الجرائم الرقمية، إلى جانب تأسيس مؤسسات وطنية متخصصة لمكافحة الجرائم الإلكترونية وحماية الأمن الرقمي. وأظهرت الدراسة أن هذه الآليات القانونية ساهمت في حماية الأفراد والمؤسسات وضمان الأمن الاقتصادي والاجتماعي في الفضاء الرقمي، رغم التحديات القائمة مثل سرعة التطور التكنولوجي، وتعقيد الجرائم السيبرانية، ووجود بعض الثغرات القانونية، بالإضافة إلى الحاجة لتعزيز قدرات الجهات المكلفة بالتحري والبحث. وتعتمد الدراسة على المنهج التحليلي لتحليل النصوص القانونية وتقييم فعاليتها تطبيقاً، مع تقديم توصيات عملية تشمل تطوير التشريع، تعزيز قدرات التحري، تفعيل التعاون الدولي، ورفع وعي المجتمع الرقمي، بما يضمن مكافحة فعالة للجرائم السيبرانية وحماية الحقوق الرقمية.

الكلمات المفتاحية: جريمة سيبرانية؛ حماية البيانات؛ الأمن الرقمي؛ قانون العقوبات؛ المصنفات الرقمية؛

Abstract:

In recent years, Algeria has made notable progress in confronting cybercrime through the establishment of a comprehensive legal framework, including amendments to the Penal Code, the issuance of specialized legal texts, the regulation of digital crime investigation procedures, and the creation of specialized national institutions for combating electronic crime and protecting digital security. The study found that these legal mechanisms

*** المؤلف المراسل**

have contributed to protecting individuals and institutions and ensuring economic and social security in the digital space, despite ongoing challenges such as the rapid pace of technological progress, the complexity of cybercrime, the existence of certain legal loopholes, and the need to strengthen the capacity of investigative entities. The study employs an analytical-descriptive methodology to analyse legal texts and assess the effectiveness of their application, while offering practical recommendations including legislative development, enhanced investigative capacity, strengthened international cooperation, and raising digital society awareness; all aimed at ensuring effective combating of cybercrime and the protection of digital rights.

Keywords: Cybercrime; data protection; digital security; Penal Code; digital works.

مقدمة:

شهد مجال تقنيات المعلومات تطورًا سريعًا ومستمرًا، ما يؤدي إلى ظهور جرائم جديدة تختلف أركانها عن الجرائم التقليدية، أو إلى تطور صور قائمة من حيث ركنها المادي أو المعنوي، مما يصعب تطبيق النصوص القانونية الحالية عليها¹. وتتميز هذه الجرائم بذكاء وفطنة مرتكبيها، الأمر الذي يفرض على المشرعين تحديثًا مستمرًا لمواكبة هذا التطور وإصدار قوانين حديثة تلبي المتطلبات المستجدة².

وأمام تنامي هذه الجرائم، سعى المشرع الجزائري إلى وضع إطار قانوني لمواجهةها، من خلال تجريم الأفعال المرتكبة في البيئة الرقمية، وتنظيم إجراءات البحث والتحري، وتوفير آليات خاصة للتعامل مع الأدلة الإلكترونية. وعليه، تتمثل أهمية دراسة الآليات القانونية لمكافحة الجرائم السيبرانية في الجزائر في حماية حقوق الأفراد والمؤسسات ضمن فضاء رقمي سريع التطور، وضمان سلامة المعاملات الإلكترونية، وضبط الجريمة الرقمية والتصدي للتهديدات المتجددة على الأمن الوطني والاقتصادي. كما أن فهم الإطار القانوني وأدوات تطبيقه يمثل أساسًا لتقييم مدى فعالية التشريعات الحالية وكشف مواطن القصور والتحديات العملية في مواجهة هذه الجرائم³.

وبذلك تتمحور الإشكالية حول السؤال التالي: ما مدى كفاية الآليات القانونية التي أقرها التشريع الجزائري لمواجهة الجرائم السيبرانية في ظل التطور المستمر للبيئة الرقمية؟ وتهدف هذه الدراسة إلى:

1. تحليل الإطار القانوني الجزائري المتعلق بالجرائم السيبرانية.

2. تقييم مدى فعالية الآليات القانونية الحالية في مواجهتها.

3. تحديد الثغرات والتحديات في التشريعات القائمة.

4. تقديم توصيات لتطوير الآليات القانونية بما يتوافق مع التطورات الرقمية الحديثة.

اعتمدت الدراسة على المنهج التحليلي، من خلال استعراض النصوص القانونية الوطنية المتعلقة بالجرائم السيبرانية وتحليل مضمونها وتطبيقاتها العملية. كما شملت دراسة الفقه القانوني والتجارب المقارنة لتحديد نقاط القوة والضعف في الآليات القانونية الحالية، وتقديم تصور موضوعي لتطويرها بما يضمن مكافحة فعالة للجرائم الرقمية.

المبحث الأول:

الإطار العلمي والقانوني لمكافحة الجريمة السيبرانية

تُعَدّ الجريمة السيبرانية من أبرز صور الإجرام المستحدث المرتبطة بالتطور الرقمي، لما تتميز به من خصوصية تقنية وتنوع في صورها ووسائل ارتكابها. وقد فرضت هذه الخصوصية ضرورة إحاطتها بدراسة علمية تحدد مفهومها وخصائصها، إلى جانب وضع إطار قانوني ملائم يجرّم أفعالها وينظم آليات مكافحتها.

المطلب الأول: التأصيل العلمي للجرائم السيبرانية:

أدى التحول الرقمي المتسارع إلى بروز أنماط إجرامية جديدة اتخذت من الفضاء السيبراني مجالاً لارتكابها، وتميزت بخصوصية في طبيعتها ووسائل تنفيذها مقارنة بالجرائم التقليدية. لذلك، تبرز أهمية التأصيل العلمي لهذه الجرائم من خلال ضبط مفهومها، وتحديد خصائصها، وبيان أهم صورها، بما يساهم في تحديد طبيعتها القانونية وتمييزها عن الأنماط الإجرامية الأخرى.

الفرع الأول: مفهوم الجريمة السيبرانية:

أفرز التحول الرقمي المتسارع بيئة إجرامية مغايرة للأنماط التقليدية، أصبح الفضاء السيبراني فيها مجالاً لارتكاب أفعال تمس الأفراد والبيانات والأنظمة المعلوماتية. وقد فرض هذا التحول تحديات قانونية خاصة، بالنظر إلى الطبيعة التقنية لهذه الجرائم وتعدد صورها ووسائل ارتكابها. ومن ثم، يكتسي تحديد مفهوم الجريمة السيبرانية وبيان خصائصها أهمية أساسية في ضبط نطاقها وتمييزها عن الجريمة التقليدية، بما يسمح بتحديد القواعد القانونية الملائمة لمواجهتها.

أولاً- تعريف الجريمة السيبرانية.

اهتمّ المشرع الجزائري بتنظيم الجرائم المرتبطة بالبيئة الرقمية من خلال القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها⁴، حيث تناولت المادة الثانية منه مفهوم هذه الجرائم باعتبارها كل فعل إجرامي يمس أنظمة المعالجة

الآلية للمعطيات، أو يرتكب أو يُسهّل ارتكابه بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية. ويُستفاد من ذلك أن المشرّع لم يَحصر الجريمة الرقمية في الاعتداء المباشر على الأنظمة المعلوماتية، وإنما وسّع نطاقها ليشمل كذلك الجرائم التقليدية التي تُستخدم فيها التكنولوجيا الرقمية وسيلةً لارتكابها أو تسهيل تنفيذها.

كما عرّف المشرّع المنظومة المعلوماتية باعتبارها نظاماً أو مجموعة من الأنظمة المترابطة التي تقوم، كلياً أو جزئياً، بالمعالجة الآلية للمعطيات من أجل تنفيذ برنامج محدد، في حين تشمل المعطيات المعلوماتية مختلف الوقائع أو المعلومات أو المفاهيم المدّعة للمعالجة داخل هذه المنظومة، بما في ذلك البرامج التي تمكّن النظام من أداء وظائفه.

ويتكامل هذا الإطار مع أحكام المواد (394 مكرر إلى 394 مكرر 2 ق.ع)، التي جرّمت جملة من الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، من أبرزها الدخول أو البقاء غير المشروع في النظام، وإدخال أو حذف أو تعديل المعطيات بطريق الغش، فضلاً عن التعامل غير المشروع في المعطيات والبرامج التي يمكن استخدامها في ارتكاب الجرائم، وحياسة أو إفشاء أو استعمال البيانات المتحصّل عليها بصورة غير مشروعة.

ويُستخلص من مجموع هذه الأحكام أن المشرّع الجزائري اعتمد أساساً على طبيعة محل الاعتداء والبيئة المعلوماتية التي تُرتكب فيها الجريمة؛ فهناك جرائم تستهدف النظام المعلوماتي أو البيانات ذاتها، وأخرى تُتخذ فيها التكنولوجيا وسيلة لارتكاب أفعال إجرامية مختلفة. ومع ذلك، لم يقدّم المشرّع تعريفاً جامعاً مانعاً لمفهوم الجريمة الإلكترونية، وإنما عالجها من خلال تحديد نطاقها وصورها ووسائل ارتكابها، بما يسمح بإخضاع الأفعال المستحدثة للقواعد الجزائية المقررة، ومراعاة الخصوصية التقنية للبيئة الرقمية.

ثانياً- خصائص الجريمة السيبرانية.

تستمد الجريمة الإلكترونية خصوصيتها من البيئة الرقمية التي تنشأ في نطاقها، ومن الأدوات التقنية التي تُوظف في تنفيذها، الأمر الذي جعلها تختلف في طبيعتها وآثارها عن الجرائم التقليدية. ولا تقتصر خصوصيتها على وسيلة ارتكابها، وإنما تمتد إلى كيفية وقوعها واكتشافها وإثباتها وملاحقة مرتكبيها، وهو ما أفرز مجموعة من الخصائص التي يمكن بيان أهمها فيما يأتي:

1- تجاوزها للحدود الإقليمية للدول:

تنسّم الجريمة الإلكترونية بقدرتها على تجاوز الحدود الجغرافية والإقليمية، بحيث يمكن أن يقع السلوك الإجرامي في إقليم دولة، بينما تظهر نتيجته أو آثاره في إقليم دولة أخرى، وقد تمتد تلك

الآثار إلى عدة دول في الوقت ذاته. ويترتب على ذلك تعدد الروابط الإقليمية للجريمة، وما ينشأ عنها من صعوبات في تحديد الاختصاص القضائي والقانون الواجب التطبيق، فضلاً عن تعقيد إجراءات البحث والتحري عندما تكون البيانات أو الخوادم أو الأطراف المرتبطة بالجريمة موزعة بين دول مختلفة. ومن ثم، أصبحت مكالحة هذا النوع من الجرائم تستلزم تعزيز التعاون الدولي وتبادل المعلومات والمساعدة القضائية في مجال الأدلة الرقمية.⁵

2- الطبيعة الرقمية للأدلة وصعوبة الكشف والإثبات:

تطرح الجريمة الإلكترونية تحديات خاصة في مجال الإثبات، ذلك أن آثارها لا تكون بالضرورة محسوسة أو ظاهرة بالصورة التي تكون عليها في الجرائم التقليدية، وإنما تتجسد غالباً في بيانات وملفات وسجلات إلكترونية يمكن تغييرها أو نقلها أو حذفها بسرعة. كما يستطيع مرتكب الجريمة استخدام وسائل تقنية متعددة لإخفاء نشاطه أو طمس آثاره الرقمية، مما يصعب عملية تحديد مصدر الفعل الإجرامي ونسبته إلى فاعله. ولذلك يتطلب التعامل مع هذا النوع من الجرائم وسائل فنية متخصصة وخبرات قادرة على ضبط الأدلة الرقمية واستخراجها وتحليلها والمحافظة على سلامتها بما يضمن إمكانية الاستناد إليها في المجال القضائي.⁶

3- سهولة ارتكابها واتساع نطاق آثارها:

لا يرتبط ارتكاب الجريمة الإلكترونية في كثير من صورها بتوافر إمكانيات مادية كبيرة، إذ يمكن أن تُنفذ بواسطة أجهزة وتقنيات متداولة، مع الاستفادة من شبكة الإنترنت والبرمجيات والخدمات الرقمية المختلفة. كما أن الطبيعة غير المادية للبيئة الرقمية تتيح للجاني تنفيذ الفعل عن بُعد دون الحاجة إلى الوجود في المكان الذي تتجسد فيه النتيجة الإجرامية. ويؤدي ذلك إلى إمكانية استهداف عدد كبير من الأشخاص أو الأنظمة خلال مدة زمنية قصيرة، بما يجعل نطاق الضرر الناتج عنها قابلاً للامتداد بصورة تفوق في بعض الحالات نطاق الجريمة التقليدية.⁷

4- الخفاء وسرعة التنفيذ والتطور المستمر لأساليبها:

تتصف الجريمة الإلكترونية بدرجة عالية من الخفاء، إذ قد يتم تنفيذها دون أن يدرك المجني عليه وقوع الاعتداء في حينه، ولا تظهر آثارها إلا بعد اكتشاف فقدان البيانات أو تغييرها أو الوصول غير المشروع إليها. كما تتميز بسرعة تنفيذها، إذ يمكن إتمام بعض الأفعال الإجرامية في وقت وجيز باستخدام الوسائل الرقمية. وإلى جانب ذلك، فإن أساليب ارتكابها ليست ثابتة، بل تتطور بصورة مستمرة بالتزامن مع تطور التكنولوجيا، الأمر الذي يدفع مرتكبيها إلى ابتكار وسائل جديدة لتجاوز أنظمة الحماية وإخفاء هوياتهم وآثار أنشطتهم. ويشكل هذا التطور المتواصل تحدياً أمام أجهزة

البحث والتحري والجهات القضائية، ويفرض ضرورة تحديث الوسائل القانونية والتقنية لمواجهة المستجدات الإجرامية في البيئة الرقمية⁸.

5- طبيعة مرتكبي الجريمة السيبرانية:

يتميز مرتكب الجريمة الإلكترونية بخصوصية تميزه عن النمط المألوف للجاني في الجرائم التقليدية، إذ يرتبط ارتكاب هذا النوع من الجرائم، في كثير من الحالات، بتوافر قدرات تقنية ومعارف متخصصة في مجال تكنولوجيات الإعلام والاتصال. فالجاني قد يمتلك خبرة في التعامل مع أنظمة المعلومات وقواعد البيانات، وفهماً لآليات تشغيلها وإدارتها، بما يمكنه من الوصول غير المشروع إلى البيانات أو تعديلها أو نسخها أو استغلالها بوسائل يصعب اكتشافها بالطرق التقليدية. ولا تقتصر خطورة هذا الجاني على الجانب التقني فحسب، وإنما تتعزز بقدرته على التخطيط الدقيق واستغلال مواطن الضعف والثغرات الأمنية التي قد تشوب الأنظمة المعلوماتية، فضلاً عن قدرته على توظيف الوسائل الرقمية الحديثة في تنفيذ أفعاله وإخفاء آثارها. كما أن مظهره الخارجي أو وضعه الاجتماعي لا يشكل، في الغالب، مؤشراً كافياً على نشاطه الإجرامي، الأمر الذي قد يجعل التعرف عليه وتعقبه أكثر تعقيداً⁹.

الفرع الثاني: أركان الجريمة السيبرانية.

أولاً: الركن الشرعي للجريمة المعلوماتية

يُعدّ الركن الشرعي الأساس الذي تستند إليه المسؤولية الجزائية، إذ لا يمكن إضفاء الصفة الإجرامية على أي سلوك إلا إذا كان المشرّع قد نصّ على تجريمه وحدد له الجزاء المقرر قانوناً، تكريماً لمبدأ الشرعية الجزائية المقرر في المادة الأولى من قانون العقوبات الجزائري، والتي تقضي بأنه: «لا جريمة ولا عقوبة أو تدابير أمن بغير قانون». ويكتسي هذا المبدأ أهمية خاصة في مجال الجرائم المعلوماتية، بالنظر إلى حداثة صورها وتطور الوسائل التقنية المستخدمة في ارتكابها. وفي هذا السياق، تدخل المشرّع الجزائري بتجريم عدد من الأفعال التي تستهدف أنظمة المعالجة الآلية للمعطيات، وذلك من خلال إدراج أحكام جزائية خاصة ضمن قانون العقوبات، لاسيما في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، حيث حدد صور الأفعال المجرّمة والعقوبات المقررة لها، بما يضمن خضوع التجريم والعقاب لقاعدة قانونية سابقة على ارتكاب الفعل¹⁰.

وإلى جانب الأحكام الموضوعية الواردة في قانون العقوبات، اعتمد المشرّع الجزائري إطاراً قانونياً خاصاً للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال وضع مجموعة من القواعد ذات الطابع الإجرائي والتقني التي تستجيب لخصوصية البيئة الرقمية. وتشمل

هذه القواعد، على وجه الخصوص، آليات مراقبة الاتصالات الإلكترونية واعتراضها وتسجيل محتواها، فضلاً عن إجراءات التفتيش والبحث داخل الأنظمة المعلوماتية، وغيرها من التدابير التي تسمح بجمع الأدلة الرقمية وكشف الأفعال الإجرامية المرتكبة في البيئة السيبرانية. وعليه، فإن الركن الشرعي للجريمة المعلوماتية في التشريع الجزائري لا يقتصر على مجرد النص على الأفعال المحرمة والعقوبات المقررة لها، وإنما يقوم ضمن منظومة قانونية متكاملة تجمع بين التجريم والعقاب من جهة، والوقاية والكشف والتحري عن الجرائم المعلوماتية من جهة أخرى، بما يراعي خصوصية هذا النوع من الجرائم وطبيعة الأدلة المرتبطة بها¹¹. وسيتم بيان مختلف مكونات هذه المنظومة القانونية وآلياتها بصورة أكثر تفصيلاً ضمن المطلب الثاني المتعلق بالإطار القانوني لمكافحة الجريمة السيبرانية في الجزائر.

ثانياً: الركن المادي.

تتسم الجرائم السيبرانية بارتباطها الوثيق بالوسائل التكنولوجية، ولا سيما أجهزة الحاسوب والهواتف الذكية وشبكات الإنترنت، التي تشكل أداة أساسية في تنفيذ السلوك الإجرامي. ويتميز هذا السلوك بطابعه غير المادي والخفي، الأمر الذي يجعل تحديد مظاهره وحدود تحققه أكثر تعقيداً مقارنة بالجرائم التقليدية. وقد يسبق التنفيذ الفعلي للجريمة نشاطٌ تحضيري يتمثل في إعداد الوسائل التقنية، كقنناء البرمجيات أو تطويرها وإنشاء المواقع والصفحات الوهمية واستغلالها للوصول إلى الأنظمة أو البيانات. وتثير هذه الأفعال صعوبة في التمييز بين مجرد التحضير وبدء التنفيذ، خاصة أن بعض الأفعال التقنية قد تشكل، بالنظر إلى طبيعتها وخطورتها، جرائم مستقلة بذاتها. كما يختلف السلوك الإجرامي باختلاف طبيعة الجريمة السيبرانية؛ فقد يقتصر في بعض الحالات على فعل واحد، كالدخل غير المشروع إلى نظام معلوماتي، بينما يتخذ في جرائم أخرى صورة أفعال متتابعة ومتزايدة تتدرج من التحضير إلى التنفيذ وتحقيق النتيجة الإجرامية¹².

وتختلف الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات عن الجرائم التقليدية من حيث صور السلوك الإجرامي، إذ تتخذ أساساً شكل الاعتداء غير المشروع على النظام أو البيانات التي يتضمنها، ومن أبرز صورها¹³:

1- الدخول أو البقاء غير المشروع في النظام

يتحقق هذا الفعل بمجرد الدخول إلى نظام المعالجة الآلية للمعطيات أو البقاء فيه دون إذن من صاحبه أو خارج الحدود المسموح بها، وهو ما جرمته المادة 394 مكرر (ق.ع). ويتخذ هذا السلوك صورتين:

أ- الصورة البسيطة: تتمثل في الدخول غير المشروع إلى النظام أو البقاء فيه رغم عدم توافر الإذن، أو بعد تجاوز المدة أو الحدود المقررة للاستعمال.

ب- الصورة المشددة: تقوم عندما يترتب على الدخول أو البقاء غير المشروع إتلاف المعطيات أو تغييرها أو تعطيل النظام عن أداء وظائفه.

2- إدخال المعطيات بطريق الغش

يقصد به إضافة معطيات جديدة إلى نظام المعالجة الآلية أو تعديل المعطيات الموجودة فيه بصورة غير مشروعة، بما يؤدي إلى تغيير محتواه أو وظائفه، ومن أمثلته الاستعمال الاحتيالي لبطاقات السحب أو الائتمان، سواء من صاحبها أو من الغير.

ثالثا- الركن المعنوي في الجرائم السيبرانية

يتميز الركن المعنوي في الجرائم السيبرانية بخصوصية تفرضها طبيعة البيئة الرقمية، إذ يتعين التحقق من الحالة الذهنية للجاني والغاية التي اتجه إليها سلوكه، سواء تعلق الأمر بإتلاف البيانات أو تغييرها أو التجسس عليها أو تعطيل النظام. ويقوم هذا الركن أساسًا على العلم والإرادة¹⁴.

1- العلم: يقصد به إدراك الجاني للعناصر الجوهرية المكونة للجريمة، ولا يتحقق القصد الجنائي إذا انتفى علمه بأحد العناصر التي يتطلبها القانون، ما لم يكن الجهل بها غير مؤثر قانونًا.

2- الإرادة: تتمثل في اتجاه إرادة الجاني إلى ارتكاب السلوك المجرّم عن وعي واختيار، بحيث تنصرف إلى الفعل والنتيجة متى كانت هذه الأخيرة عنصرًا لازمًا لقيام الجريمة.

وفي الجرائم السيبرانية، لا يشترط دائمًا تحقق ضرر فعلي لقيام القصد الجنائي، إذ قد يكتمل بمجرد تعمد الولوج أو البقاء غير المشروع في النظام المعلوماتي، متى توافرت باقي العناصر القانونية، وهو ما يعكس حرص المشرع على توفير حماية جنائية مبكرة للأنظمة والبيانات المعلوماتية¹⁵.

المطلب الثاني: الإطار القانوني لمكافأة الجريمة السيبرانية في الجزائر

فرض التطور الرقمي المتسارع تحديات إجرامية جديدة، في مقدمتها الجرائم السيبرانية التي تتميز بتنوع صورها وصعوبة الكشف عنها وإثباتها. واستجابةً لذلك، أرسى المشرع الجزائري إطارًا قانونيًا لمكافئتها، من خلال تجريم الأفعال السيبرانية وتنظيم إجراءات البحث والتحري وجمع الأدلة الرقمية، بما يتلاءم مع خصوصية البيئة الرقمية.

الفرع الأول: مكافئة الجريمة السيبرانية في قانون العقوبات

نتيجة للتطور التكنولوجي وظهور جرائم مستحدثة تعتمد على التكنولوجيا أساسا لها، اهتم المشرع الجزائري بإدخال تعديلات على قانون العقوبات الأمر رقم 66-156 تتضمن تلك التعديلات نصوصا قانونية تنظم هذه الجرائم وتعمل على مكافئتها.

أولا: القانون رقم 01-09 المؤرخ في 26 جوان 2001¹⁶.

تضمن هذا القانون استحداث عقوبات جزائية جديدة تُطبَّق على بعض الجرائم المرتبطة بإهانة أو سب الموظف العمومي أو الضابط العمومي أو القاضي أو أحد رجال وضباط القوات العمومية أو القادة التابعين لها، وذلك باستعمال أي وسيلة، لاسيما الوسائل الرقمية، متى ارتكبت هذه الأفعال أثناء تأدية مهامهم الوظيفية أو بمناسبة، وبقصد الاعتداء على شخصهم أو المساس بشرفهم واعتبارهم، أو إهانتهم، أو التقليل من الاحترام الواجب لأداء واجبه الوظيفي¹⁷.

وقد قرر المشرع لهذه الجرائم عقوبة الحبس التي تتراوح مدتها بين شهرين وستين، وغرامة مالية تتراوح بين 1.000 دينار جزائري و500.000 دينار جزائري، أو إحدى هاتين العقوبتين. ويلاحظ في هذا السياق أنَّ هذه الغرامات قد تم تحيينها بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2016، وذلك فيما يخص جريمة إهانة الموظف في مؤسسات الدولة، حيث أصبحت الغرامة تُقدَّر بين 20.000 دينار و100.000 دينار جزائري¹⁸.

وبالرجوع إلى أحكام (المادة 144 مكرر ق رقم 01-08)، يتبيّن أنّها استحدثت تجريم أفعال جديدة تتمثل في سب وشم رئيس الجمهورية أو إهانتته، و لاسيما عبر وسائل الاتصال المختلفة، من بينها الوسائل الرقمية، حيث زُيِّت على هذه الأفعال عقوبة الحبس من ثلاثة (03) أشهر إلى اثني عشر (12) شهرا، وغرامة مالية تتراوح بين 50.000 و250.000 دينار جزائري، أو إحدى هاتين العقوبتين.

وتجدر الإشارة إلى أنَّ قيمة هذه الغرامة قد تم رفعها لاحقا بموجب القانون رقم 11-14، لتتراوح بين 100.000 و500.000 دينار جزائري¹⁹.

ثانيا: القانون رقم 04-15، المؤرخ في 10/12/2004، المعدل والمتمم لقانون العقوبات.

يعدّ هذا القانون من أهم النصوص القانونية في مجال حماية حرمة الحياة الخاصة للأشخاص، إذ تضمّن عقوبات مستحدثة تهدف إلى مكافئة جرائم الاعتداء على هذه الحرمة عبر الوسائل الرقمية. وفي هذا الإطار، استحدث المشرع (المادة 303 مكرر من ق.ع) بموجب المادة 34 منه، والتي تُجرّم كل اعتداء على حرمة الحياة الخاصة يتم عن طريق التقاط الصور أو التسجيلات أو

إجراء المكالمات أو نقل الأحاديث السرية دون الحصول على إذن مسبق من الشخص المعني. وقد قررت هذه المادة عقوبة الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، بالإضافة إلى غرامة مالية تتراوح بين 50.000 و 300.000 دينار جزائري²⁰.

ثالثا: القانون 02-16، المؤرخ في 19 جوان 2016²¹.

تضمن هذا القانون بدوره أحكامًا مستحدثة تتعلق بمكافحة الإرهاب الإلكتروني وتنظيم الجماعات الإرهابية عبر الوسائط الرقمية، حيث نصّت المادة 87 مكرر 11 على تجريم كل من يعتمد وسائل تكنولوجيا الإعلام والاتصال في ارتكاب أفعال تُصنّف من قبيل الأعمال الإرهابية، سواء من خلال المشاركة فيها، أو التدبير لها، أو الإعداد أو التنفيذ الفعلي، أو التدريب عليها، أو نشر مضامين مخصصة لها. وقد رتب المشرع على هذه الأفعال عقوبة السجن من خمس (5) إلى عشر (10) سنوات، وغرامة مالية تتراوح بين 100.000 و 500.000 دينار جزائري. كما جرّم المشرع، بموجب المادة 87 مكرر 12، كل من يعتمد وسائل التكنولوجيا والاتصال للدعوة إلى تجنيد الأفراد أو استقطابهم للانضمام إلى الجماعات الإرهابية، في إطار تعزيز السياسة الجنائية الرامية إلى الوقاية من أخطار الإرهاب الإلكتروني والحد من انتشاره.

رابعا: القانون رقم 01-20، المؤرخ في 30 جوان 2020²².

هتّم هذا القانون بحماية عمال الصحة والمؤسسات الصحية من مختلف صور الاعتداءات والإهانات التي تُرتكب في حقهم عبر الشبكات الإلكترونية الرقمية، سواء من خلال وسائل التواصل الاجتماعي أو غيرها من الوسائل التكنولوجية. وفي هذا الإطار، استُحدثت (المادة 149 مكرر 3 في ق.ع) والتي قررت عقوبة الحبس من سنتين إلى خمس سنوات وغرامة مالية تتراوح بين 200.000 و 500.000 دينار جزائري ضد كل من يرتكب هذه الجريمة.

وتُشدد العقوبة في حال تم تحويل أو نشر الفيديوها أو الصور أو المعلومات، أو التقاطها خفية في أماكن مفتوحة للجمهور. كما تُشدد العقوبة بصورة أكبر إذا ارتكبت الجريمة خلال فترة الحجر الصحي، حيث يُعاقب مرتكبها بالحبس من خمس سنوات إلى خمس عشرة سنة وبغرامة مالية تتراوح بين 500.000 ومليون وخمسمائة ألف دينار جزائري.

إضافة إلى ذلك، يُجرّم الجاني من استعمال وسائل التواصل الاجتماعي والشبكات الإلكترونية والوسائل التكنولوجية لمدة أقصاها ثلاث سنوات ابتداءً من تاريخ انقضاء العقوبة الأصلية والإفراج عنه. كما يجوز للقاضي أن يحكم بغلق الموقع الإلكتروني أو الحساب الرقمي الذي استخدم في ارتكاب الجريمة²³.

كما اعتبرت المادة 152 مرتكباً لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا القانون، وذلك عن طريق تبليغ المصنف أو الأداء للجمهور عبر التمثيل أو الأداء العلني، أو البث، أو التوزيع بواسطة الكابل، أو أي وسيلة نقل أخرى.

وقد شددت المادة 153 العقوبة على مرتكبي جنحة تقليد المصنف أو الأداء، حيث يعاقب الفاعل بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة مالية تتراوح بين خمسمائة ألف (500.000) دينار ومليون (1.000.000) دينار جزائري، سواء تم نشر المصنف داخل الجزائر أو خارجها.

ثانياً: القانون العضوي رقم 05-12، المؤرخ في 12 جاني 2012 والمتعلق بالإعلام²⁶.

تضمن هذا القانون سرداً للعديد من الجرائم الرقمية والتي من بينها:

1- كشف أسرار التحقيق الابتدائي: تنص المادة 119 من القانون العضوي رقم 05-12 لسنة 2012 على تجريم قيام أي صحفي بفصح أسرار التحقيق الابتدائي عبر الوسائل الإلكترونية، أو الكشف عن أي خبر أو وثيقة قد تؤثر على سير التحقيق. ويُعاقب مرتكب هذا الفعل بغرامة مالية تتراوح بين خمسين ألف دينار (50.000 دج) ومائة ألف دينار (100.000 دج).

2- كشف فحوى المناقشات السرية للجهات القضائية: يحظر القانون الإفصاح عن مضمون الأحكام الصادرة في الجلسات السرية. ويُعاقب كل من يخالف هذا المنع بغرامة مالية تتراوح بين مائة ألف دينار (100.000 دج) ومائتي ألف دينار (200.000 دج)، وفقاً للمادة 120 من القانون ذاته.

3- نشر تقارير المرافعات المتعلقة بحالات الأشخاص والأحداث الخاصة: يعاقب القانون على نشر هذه التقارير عبر الوسائل الرقمية بغرض حماية الخصوصية وسرية المعلومات، وتبلغ الغرامة المالية في هذه الحالة ما بين خمسين ألف دينار (50.000 دج) ومائتي ألف دينار (200.000 دج).

4- نشر وبث الصور والرسومات المتعلقة بالجرائم: يحظر القانون نشر أو إعادة تمثيل الصور والرسومات التي توضح أو تعيد تمثيل ظروف الجرائم والجنح المنصوص عليها في قانون العقوبات. ويعاقب مرتكب هذا الفعل بغرامة مالية تتراوح بين خمسة وعشرين ألف دينار (25.000 دج) ومائة ألف دينار (100.000 دج)، وفق المادة 122 من القانون العضوي رقم 05-12.

5- إهانة رؤساء الدول الأجنبية وأعضاء البعثات الدبلوماسية: يُجرّم القانون أي فعل من شأنه إهانة رؤساء الدول الأجنبية أو أعضاء البعثات الدبلوماسية المعتمدين لدى الجزائر عبر وسائل الإعلام الرقمية، وفقاً للمادة 123 من القانون ذاته.

6- فرض نشر رد الصحفي أو بثه: يعاقب القانون أي صحفي يرفض نشر أو بث الرد المقدم عبر الوسيلة الإعلامية المعنية، وتبلغ الغرامة المالية في هذه الحالة ما بين مائة ألف دينار (100.000 دج) وثلاثمائة ألف دينار (300.000 دج)، وفق المادة 125 من القانون. وتتقادم جميع العقوبات المنصوص عليها أعلاه بعد مرور ستة (06) أشهر كاملة من تاريخ ارتكاب المخالفة.

ثالثاً: القانون رقم 07-18، المؤرخ في 10 جوان 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية.²⁷

تعزيزاً لحزمة الحياة الخاصة وضماناً لحياتها، لا سيما في المجال الإلكتروني، أصدرت الحكومة الجزائرية القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ويهدف هذا القانون إلى تحديد القواعد القانونية الكفيلة بحماية الأشخاص الطبيعيين عند معالجة معطياتهم الشخصية، على أن تتم هذه المعالجة في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، وبما لا يمس بحقوق الأشخاص أو شرفهم أو سمعتهم.²⁸

ويقصد بالمعطيات ذات الطابع الشخصي، وفقاً للفقرة الأولى من المادة الثالثة من هذا القانون، كل معلومة، مهما كان شكلها أو دعمتها، تتعلق بشخص مُعرّف أو قابل للتعرف عليه، بصورة مباشرة أو غير مباشرة، لا سيما بالرجوع إلى رقم تعريف أو عنصر واحد أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

ويُطبق هذا القانون على المعالجة الآلية الكلية أو الجزئية للمعطيات ذات الطابع الشخصي، كما يشمل المعالجة غير الآلية لتلك المعطيات عندما تكون واردة أو قابلة للورود في ملفات يدوية. وقد أقرّ المشرّع الجزائري جملة من المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي، من أبرزها مبدأ الموافقة المسبقة ومبدأ نوعية المعطيات.

وفي هذا السياق، نصّت المادة السابعة من القانون على أنه لا يجوز القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بعد الحصول على الموافقة الصريحة للشخص المعني. وإذا كان هذا الأخير

عدم الأهلية أو ناقصها، فإن الموافقة تخضع للقواعد المقررة في القانون العام. كما خول القانون للشخص المعني حق سحب موافقته في أي وقت، دون أن يترتب عن ذلك أي مساس بحقوقه. ولا يجوز اطلاع الغير على المعطيات ذات الطابع الشخصي محل المعالجة إلا من أجل إنجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة أو المرسل إليه، وذلك بعد الحصول على الموافقة المسبقة للشخص المعني. إضافة إلى ذلك، أخضع المشرع معالجة المعطيات ذات الطابع الشخصي لإجراءات مسبقة تتمثل في التصريح المسبق المودع لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، والمتضمن الالتزام بإجراء المعالجة، وذلك طبقاً لأحكام المادة 13 من القانون. كما قد تستلزم بعض أنواع المعالجة الحصول على ترخيص مسبق تمنحه السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وفقاً لمفهوم المادة 17 من القانون، حيث يجوز لهذه السلطة أن تخضع المعالجة المعنية لنظام الترخيص المسبق إذا تبين لها، عند دراسة التصريح المقدم، أن المعالجة المزمع القيام بها تنطوي على أخطار ظاهرة من شأنها المساس باحترام وحماية الحياة الخاصة أو بالحريات والحقوق الأساسية للأشخاص.

المبحث الثاني:

الآليات الإجرائية والمؤسسية للتحري والبحث عن الجريمة السيرانية

من خلال هذا المبحث سنقوم بالتطرق لكل من إجراءات التحري والبحث عن الجريمة السيرانية (مطلب أول) ومن ثم عرض الآليات المؤسسية المعنية بمكافحة هذه الجريمة في الجزائر (مطلب ثان).

المطلب الأول: إجراءات التحري والبحث عن الجريمة السيرانية.

تتميز الجريمة السيرانية عن الجريمة العادية هي طبيعتها التقنية الخاصة التي تجعل منها صعبة في كشفها، لذلك سخر المشرع الجزائري أعوان مختصين بالتحري والبحث عن هذه الجرائم يتمتعون بالخبرة والكفاءة في المجال التقني المعلوماتي والسيراني²⁹، إضافة لوضعه طرق معينة يتبعها هؤلاء الأعوان في عملية التحري والبحث عنها وهو ما سنقوم بعرضه من خلال هذا المطلب.

الفرع الأول: الجهات المكلفة بالتحري عن الجريمة السيرانية في الجزائر.

سخر المشرع الجزائري جهات معينة تختص بالتحري والبحث عن الجريمة السيرانية، تتمتع هذه الجهات المستخرجة بالخبرة العالية في النظام المعلوماتي والذكاء الصناعي ولها خبرة واسعة في مجال الأمن السيراني، تتمثل هؤلاء الأعوان في كل من رجال الضبطية القضائية (أولا)، ومقدمي الخدمات (ثانيا).

أولاً- الضبطية القضائية.

يعد جهاز الضبطية القضائية الهيئة الهامة المنوط لها باختصاص البحث والتحري في مختلف الجرائم، خاصة السيرانية منها ويتكون هذا الجهاز من ضباط الشرطة القضائية وأعوان الضبط القضائي، إضافة إلى بعض الموظفين والأعوان الذين أسند لهم القانون صلاحيات ضبطية معينة³⁰. وتخضع الشرطة القضائية، في أدائها لمهامها، إلى إشراف النائب العام ضمن نطاق كل مجلس قضائي، بينما يتولى وكيل الجمهورية الإشراف الإداري المباشر عليها على مستوى المحكمة، وذلك كله تحت رقابة غرفة الاتهام باعتبارها الجهة المخولة قانوناً بمتابعة أعمال الضبطية القضائية والتأكد من احترامها للضوابط القانونية. كما تضطلع الشرطة القضائية، استناداً إلى قانون الإجراءات الجزائية، بمهام البحث والتحري في الجرائم المقررة في قانون العقوبات، بما في ذلك الجرائم المعلوماتية، كما تتولى جمع الأدلة والكشف عن هوية مرتكبيها، وذلك ما لم يُفتح بشأن الوقائع محل البحث تحقيق قضائي رسمي³¹.

1. ضباط الشرطة القضائية.

من خلال هذه الجزئية سنقوم بعرض كل من صاحب وصف ضباط الشرطة القضائية، إضافة لاختصاصاتهم.

أ. فئات ضباط الشرطة القضائية:

يُمنح وصف ضابط الشرطة القضائية لفئات محددة بنص القانون، من بينها³²: يكتسب هذه الصفة كلٌّ من رؤساء المجالس الشعبية البلدية، وضباط الدرك الوطني، إلى جانب موظفي الأسلاك الخاصة بالمراقبين، ومحافظي الشرطة وضباطها التابعين للأمن الوطني. كما تُسند الصفة ذاتها لضباط الصف في الدرك الوطني الذين قضوا مدة لا تقل عن ثلاث (3) سنوات خدمة فعلية، وتم تعيينهم بقرار مشترك بين وزير العدل، حافظ الأختام، ووزير الدفاع الوطني، بناءً على رأي لجنة مختصة.

وتشمل صفة ضابط الشرطة القضائية كذلك الموظفين المنتمين لأسلاك المفتشين، والحفاظ، وأعوان الشرطة بالأمن الوطني، ممن أمّوا ثلاث (3) سنوات على الأقل في مناصبهم، وتم تعيينهم بقرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية، بعد موافقة لجنة خاصة. كما تُمنح الصفة نفسها للضباط وضباط الصف العاملين ضمن المصالح العسكرية للأمن، متى تمّ تعيينهم خصيصاً لهذا الغرض، بموجب قرار مشترك بين وزير الدفاع الوطني ووزير العدل.

ب. اختصاصات ضباط الشرطة القضائية:

منح ضباط الشرطة القضائية اختصاص وطني شامل فيما يتعلق بالجرائم المتصلة بأنظمة المعالجة الآلية للمعطيات، بالنظر للطابع العالمي والواسع لهذه الجرائم، ويجوز لهم، بناءً على ترخيص من وكيل الجمهورية المختص، مراقبة المشتبه فيهم في الجرائم الرقمية وتتبع تحركاتهم. كما يتولّى ضباط الشرطة القضائية مهام التحقيق في الجرائم الرقمية، بما في ذلك تنفيذ الإنبات القضائية، وتلقي الشكاوى والبلاغات، وجمع الأدلة وإنجاز التحريات الأولية. ويحق لهم الاستعانة مباشرة بالقوة العمومية، وتوجيه نداءات إلى الجمهور لطلب المعلومات أو الشهادات، كما يمكنهم—بموجب إذن كتابي صادر عن وكيل الجمهورية—طلب نشر إشعارات أو أوصاف أو صور للأشخاص محل البحث. وفي حالات التلبس بجناية أو جنحة رقمية³³، يلتزم ضابط الشرطة القضائية بإخطار وكيل الجمهورية على الفور، ثم الانتقال دون إبطاء إلى مكان ارتكاب الجريمة لاتخاذ التحريات المستعجلة، والمحافظة على الأدلة والآثار، وضبط كل ما من شأنه المساهمة في كشف الحقيقة، وعرض المحجوزات على المشتبه فيهم للتعرف عليها، طبقاً لأحكام المادة 42 من قانون الإجراءات الجزائية. وبعد استكمال المهام المسندة إليهم، يحزّر ضباط الشرطة القضائية محاضر رسمية تتضمن جميع إجراءات التحقيق المتخذة بشأن الجرائم الرقمية، ويقومون بإحالتها بسرعة إلى وكيل الجمهورية مرفقة بنسخة عنها، وذلك وفقاً لما تنص عليه المادة 18 من قانون الإجراءات الجزائية.

2. أعوان الضبط القضائي:

يعدّ أعوان الضبط القضائي - وفقاً لأحكام المادة 19 من قانون الإجراءات الجزائية - كل الموظفين التابعين لجهاز الشرطة، وضباط الصف في الدرك الوطني، وكذا مستخدمي المصالح العسكرية للأمن الذين لا يحملون صفة ضباط الشرطة القضائية. ويختص هؤلاء بمهمة تقديم العون والمساندة لضباط الشرطة القضائية في أداء وظائفهم، وذلك من خلال تنفيذ التوجيهات الصادرة عن رؤسائهم، مع التقيد بالأنظمة الداخلية للهيئة التي ينتمون إليها. كما يكلفون بإثبات الجرائم المنصوص عليها في قانون العقوبات، وجمع كل البيانات والمعلومات التي من شأنها الكشف عن هوية مرتكبها.

ثانياً- مقدمي الخدمات.

يعرّف القانون 09-04 مقدمي الخدمات بأنهم كل كيان عام أو خاص يتيح لمستعملي الإنترنت خدمات الاتصال أو يتولى معالجة أو تخزين المعطيات المعلوماتية لفائدتهم. ويلزم هؤلاء بالتعاون مع السلطات المختصة في عمليات البحث والتحري، من خلال تمكينها من جمع المعطيات الرقمية فوراً

ووضع البيانات المحفوظة تحت تصرفها، مع الالتزام الصارم بسرية الإجراءات والمعلومات تحت طائلة العقوبات. كما يلزم مقدّمو الخدمات بحفظ بيانات حركة المرور، بما في ذلك هوية مستعملي الخدمة، وبيانات الأجهزة الطرفية، والخصائص التقنية للاتصالات، وتواريخها ومددها، إضافة إلى المعطيات المتعلقة بالخدمات التكميلية وعناوين المواقع التي تم الولوج إليها، وذلك لمدة سنة كاملة من تاريخ تسجيلها³⁴.

وبخصوص المحتويات غير المشروعة، يتحمّل مقدّمو الخدمات واجب التدخل الفوري لسحبها أو منع الوصول إليها عند علمهم بمخالفتها للقانون، مع اتخاذ ترتيبات تقنية تحدّ من الوصول إلى الخوادم التي تتضمن محتويات مخالفة للنظام العام أو الآداب العامة، وإعلام المشتركين بوجودها، وفقاً لأحكام المادة 12 من القانون.

الفرع الثاني: اجراءات التحري والبحث عن الجريمة الرقمية.

نتيجة للطبيعة الخاصة التي تتمتع بها الجريمة الرقمية، سخر المشرع الجزائري إجراءات خاصة للتحري والبحث عن هذه الجرائم تتلاءم مع طبيعتها، وتتمثل هذه الإجراءات في التسرب الإلكتروني، اعتراض المراسلات، الإفشاء والإفشاء العاجلان للمراسلات الإلكترونية.

أولاً- التسرب الإلكتروني:

اعتمد المشرع الجزائري هذه الوسيلة للتحقيق والتحري في الجرائم الرقمية لأول مرة في القانون رقم 06-01 من خلال المادة 56 منه³⁵، حيث أقرت بأنه وسيلة تعتمد من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها.

وقد عرف القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية التسرب الرقمي من خلال المادة 65 مكرر 12 والتي أقرت بأن التسرب الإلكتروني أو الرقمي قيام ضابط أو عون للشرطة القضائية، تحت إشراف ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم لجناية أو جنحة من خلال الاندماج في محيطهم وإيهاهم بأنه أحد الفاعلين أو الشركاء في النشاط الإجرامي³⁶، وهذا بناء على إذن مسبق مقدم من وكيل الجمهورية³⁷. يُباشَر إجراء التسرب الإلكتروني بناءً على أمر أو إخطار يصدره وكيل الجمهورية أو قاضي التحقيق بعد إخطار هذا الأخير من طرف وكيل الجمهورية، وذلك وفقاً لأحكام المادة 65 مكرر 11 من قانون الإجراءات الجزائية. ويشترط لصحة هذا الإذن توافر مجموعة من الضوابط الشكلية والموضوعية، يمكن بيانها على النحو الآتي³⁸:

1. **الطابع الكتابي للإذن** يشترط أن يكون الإذن بالتسرب الإلكتروني مكتوباً، تحت طائلة البطلان، نظراً لكونه إجراءً استثنائياً من شأنه المساس بالحقوق والحريات الأساسية للأفراد.

2. **البيانات الإلزامية للإذن** يجب أن يتضمن الإذن جملة من البيانات الجوهرية، أبرزها تحديد نوع الجريمة موضوع عملية التسرب، إضافة لذكر اسم ضابط الشرطة القضائية المسؤول عن تنفيذ الإجراء؛ تحديد مدة تنفيذ العملية، على ألا تتجاوز أربعة (4) أشهر، قابلة للتجديد وفق الشروط والضمانات ذاتها.

3. **مدة الإجراء وإمكانية وقفه** تعين تحديد مدة التسرب بدقة في متن الإذن، مع منح القاضي الذي أصدره سلطة إيقاف هذا الإجراء في أي وقت قبل انتهاء المدة المحددة، إذا اقتضت ذلك ضرورات التحقيق.

4. **الاختصاص النوعي والمكاني** يُراعى في إصدار الإذن بالتسرب الاختصاص النوعي المحدد بحسب طبيعة الجريمة، وكذلك الاختصاص المكاني وفقاً لمكان وقوع الأفعال الإجرامية أو محل إقامة المشتبه فيه.

5. **تسبب الإذن**: يشترط أن يكون الإذن مسبباً تسبباً كافياً، بعيداً عن العبارات العامة أو الفضفاضة القابلة للتأويل. ويتعين أن تتضمن ديباجته الأسباب والدوافع التي حملت الجهة القضائية على الترخيص بهذا الإجراء، استناداً إلى معطيات طلب ضابط الشرطة القضائية، وما تضمنه من مبررات تتعلق بخطورة الإجراء وحساسيته، وضرورته لكشف الحقيقة. ومن بين الأسباب الجدية المبررة للإذن: استحالة أو صعوبة كشف هوية الجناة وضبطهم بالوسائل التقليدية للتحري؛ وجود تحريات أولية جدية تبرر اللجوء إلى هذا الإجراء غير العادي. ويخضع تقدير جدية هذه التحريات إلى كل من وكيل الجمهورية أو قاضي التحقيق، باعتبارهما الجهتين المختصةين قانوناً بإصدار الإذن أو رفضه.

ثانياً- اعتراض المراسلات:

إذا استوجبت ضرورات التحري في حالة التلبس بالجرائم، أو اقتضت متطلبات التحقيق الابتدائي في جرائم المخدرات، أو الجرائم المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أو جرائم تبييض الأموال، أو الإرهاب، أو الجرائم المتعلقة بالتشريع الخاص بالصرف، وكذا جرائم الفساد، فإنه يجوز لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتم عبر وسائل الاتصال السلكية واللاسلكية، واتخاذ الترتيبات التقنية الضرورية دون موافقة المعني،

لالتقاط وتثبيت وبث وتسجيل الكلام الصادر بصفة خاصة أو سرية من شخص أو عدة أشخاص في أماكن خاصة أو عامة، فضلاً عن التقاط صور لأشخاص متواجدين في أماكن خاصة³⁹. يجب أن يتضمن الإذن باعتراض المراسلات جميع العناصر التي تمكن من تحديد الاتصالات المراد التقاطها، وتعيين الأماكن المقصودة سواء كانت سكنية أو غير ذلك، إضافة إلى بيان الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها. ويُسلم الإذن كتابياً لمدة أقصاها أربعة (4) أشهر قابلة للتجديد وفقاً لمقتضيات التحري أو التحقيق، مع احترام نفس الشروط الشكلية والزمنية عند كل تجديد⁴⁰.

ثالثاً- حجز المعطيات.

وفقاً للمادة 06 من القانون 04-09، يتم حجز المعطيات عندما تكتشف السلطات المختصة بالبحث في الجرائم الرقمية وجود بيانات مخزنة لها صلة بكشف الجرائم المعلوماتية أو التعرف على مرتكبيها، حيث يتم نسخ المعطيات محل الفحص على دعامة تخزين إلكترونية قابلة للحجز، مع تكفل السلطة المختصة بالحفاظ على سلامتها. كما يجوز لها إعادة تشكيل تلك المعطيات بما يجعلها قابلة للاستغلال لأغراض التحقيق، شريطة ألا يترتب عن عملية إعادة التشكيل أي مساس بمحتواها الأصلي.

المطلب الثاني: الآليات المؤسسية لمكافحة الجريمة الرقمية.

في سبيل مكافحة الجريمة الرقمية، استحدثت المشرع الجزائري عدة أجهزة وآليات مؤسسية تعمل على حماية مستخدمي الشبكة الرقمية من جهة ومكافحة الجريمة من جهة أخرى، والتي من بينها سنخس الدراسة الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

الفرع الأول: الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.

تم انشاء هذه المؤسسة بموجب القانون 04-09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، بمقتضى المادة 13 منه، وتعتبر هذه الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي على النحو الذي يسمح لها أداء مهامها على أتم وجه، وهذا تحت إشراف وزير العدل.⁴¹ تتمتع الهيئة باختصاص وقائي يُعنى بالحد من الأفعال المصنفة كجرائم إرهابية أو تخريبية أو تلك التي من شأنها المساس بأمن الدولة، وتُكلف حصرياً، في حدود اختصاصها، بمراقبة الاتصالات الإلكترونية وجمع وتسجيل محتواها في الوقت المناسب ضمن نظام معلوماتي، وذلك تحت إشراف

قاضٍ تابع للهيئة. ويتم تنفيذ هذه المهام وفقاً للأحكام المنصوص عليها في المادة 4 من القانون رقم 04-09 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009، كما تخضع عمليات التفتيش والحجز لأحكام قانون الإجراءات الجزائية⁴².

يشتمل الاختصاص الثاني للهيئة في التفتيش والتحري، حيث يخول لها، في إطار تنفيذ عمليات مراقبة الاتصالات الإلكترونية، إنشاء وحدة مراقبة واحدة أو أكثر، تزوّد بالوسائل والتجهيزات التقنية اللازمة. كما يتولى الأعوان المؤهلون التابعون للهيئة، وكذا وحداتها المكلفة بالمراقبة، تقديم الدعم التقني لفائدة ضباط الشرطة القضائية، وذلك في حدود ما تقتضيه أحكام التشريع الساري المفعول، ووفقاً للشروط المحددة في الرخصة المسلمة من السلطة القضائية المختصة. وتُدوّن الأعمال المنجزة عقب ذلك في محاضر رسمية تُحرّر طبقاً لأحكام قانون الإجراءات الجزائية⁴³. أما الاختصاص الأخير للهيئة فيتمثل في حجز المعطيات، حيث تنص المادة 27 من المرسوم التنفيذي رقم 21-439 على أنه يتم حفظ المعلومات والبيانات الملتقطة أثناء عملية المراقبة، طيلة مدة حيازتها من طرف الهيئة، وذلك وفقاً للقواعد المعمول بها في مجال حماية المعلومات المصنفة.

وطبقاً للمادة 28 من المرسوم ذاته، يتم تسجيل الاتصالات الإلكترونية التي تكون محل مراقبة، وتحريرها وفق الشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية. وفي هذه الحالة، تُسلم التسجيلات والمحركات محل الطلب إلى السلطة القضائية المختصة أو إلى مصالح الشرطة القضائية المختصة. وتختص السلطات القضائية وحدها، دون غيرها، بحفظ هذه المعطيات خلال المدة القانونية المحددة في التشريع الساري المفعول.

كما يُحظر، تحت طائلة العقوبات الجزائية المنصوص عليها في التشريع النافذ، استعمال المعلومات والمعطيات المتعلقة بالاتصالات الإلكترونية التي يتم جمعها أو تسليمها لأي أغراض أخرى غير تلك المرتبطة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك وفقاً لأحكام المادة 29 من المرسوم ذاته.

الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي.

تم إنشاء هذه السلطة بموجب القانون رقم 18-07 المؤرخ في 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي⁴⁴، محدثة لدى رئيس الجمهورية، نهبي سلطو وطنية تتمتع بالشخصية المعنوية والاستقلال المالي والإداري يقع مقرها في العاصمة⁴⁵، كرس المشرع الجزائري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي مجموعة من الاختصاصات المحددة في المادة 25 من القانون 18-07 المتعلق بحماية المعطيات ذات الطابع

الشخصي، حيث تتولى هذه السلطة مراقبة مدى مطابقة عمليات معالجة المعلومات الشخصية للأحكام القانونية المقررة، كما تضطلع بضمان عدم توظيف تكنولوجيات الإعلام والاتصال على نحو يمس حقوق الأفراد وحرياتهم الأساسية وحياتهم الخاصة. وتتنوع مهام السلطة بين اختصاصات وقائية ترمي إلى درء المخاطر قبل وقوعها، واختصاصات ردعية تُمارس من خلال التدخل واتخاذ الإجراءات اللازمة عند الإخلال بأحكام التشريع المنظم لحماية البيانات الشخصية⁴⁶.

تتكفل السلطة الوطنية المكلفة بحماية المعطيات ذات الطابع الشخصي، وفقاً لأحكام هذا القانون، بضمان مطابقة معالجة المعطيات للقانون، ومنع أي استخدام لتكنولوجيات الإعلام والاتصال قد يشكل خطراً على حقوق الأشخاص وحرياتهم العامة والحياة الخاصة. وتشمل مهامها، على وجه الخصوص، ما يلي:

1. منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
 2. إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.
 3. تقديم الاستشارات للأشخاص والكيانات التي تتعامل مع المعطيات الشخصية أو التي تنطوي أنشطتها على معالجة مثل هذه المعطيات.
 4. تلقي الاحتجاجات والطعون والشكاوى المتعلقة بتنفيذ عمليات معالجة المعطيات وإعلام أصحابها بنتائجها.
 5. الترخيص بنقل المعطيات الشخصية نحو الخارج وفق الشروط المنصوص عليها في هذا القانون.
 6. اتخاذ الإجراءات اللازمة لحماية المعطيات الشخصية المعالجة.
 7. إصدار أوامر بإغلاق أو سحب أو إتلاف المعطيات عند الضرورة.
 8. تقديم اقتراحات لتبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات الشخصية.
 9. نشر التراخيص الممنوحة والآراء الصادرة في السجل الوطني المشار إليه في المادة 28.
 10. تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة مبدأ المعاملة بالمثل.
 11. إصدار عقوبات إدارية وفق أحكام المادة 46 من هذا القانون.
 12. وضع معايير لحماية المعطيات ذات الطابع الشخصي.
 13. تحديد قواعد السلوك والأخلاقيات التي تحكم معالجة المعطيات الشخصية.
- وفي إطار ممارسة مهامها، تعلم السلطة الوطنية النائب العام المختص فوراً عند معاينة وقائع قد تشكل جرائم جزائية. كما تعد السلطة تقريراً سنوياً عن نشاطها ترفعه إلى رئيس الجمهورية⁴⁷.

الخلاصة:

توصلت الدراسة إلى أن الجزائر أحرزت تقدماً ملحوظاً في مواجهة الجرائم السيبرانية من خلال مجموعة من الإجراءات القانونية والتنظيمية. فقد شملت هذه الجهود تعديل بعض أحكام قانون العقوبات لتجريم الأفعال الرقمية، وإصدار نصوص قانونية خاصة تحدد العقوبات والإجراءات المتعلقة بهذه الجرائم، بالإضافة إلى وضع آليات للتحري والبحث عن الجرائم الرقمية وتحديد الجهات والأعوان المكلفين بها، وإنشاء مؤسسات وطنية متخصصة تعمل على حماية الأمن الرقمي ومكافحة الجريمة الإلكترونية.

كما أظهرت الدراسة أن هذه النصوص والآليات القانونية أسهمت في توفير إطار أولي لحماية الأفراد والمؤسسات وضمان الأمن الاقتصادي والاجتماعي في الفضاء الرقمي، إلى جانب تحديد المسؤوليات والسلطات المتعلقة بالتحري والتحقيق ومتابعة مرتكبي الجرائم. ومن أبرز نتائج الدراسة أن الجرائم السيبرانية تتميز بالتطور المستمر وذكاء مرتكبيها، ما يفرض على السلطات القانونية والأمنية متابعة مستمرة للتطورات التقنية، وتكييف التشريع والإجراءات لضمان فاعلية الردع والكشف والتحقيق.

وعلى الرغم من هذا التقدم، أبرزت الدراسة مجموعة من التحديات التي تواجه مكافحة الجرائم الرقمية في الجزائر، منها:

- سرعة التغير التكنولوجي التي تجعل بعض النصوص القانونية عاجزة عن تغطية جميع أشكال الجرائم الحديثة.
- تعقيد الجرائم السيبرانية التي تتطلب معرفة تقنية متخصصة لا تتوفر دائماً لدى أعوان الضبط القضائي التقليديين.
- وجود بعض الثغرات القانونية في النصوص المتعلقة بالعقوبات والتحريات، مما قد يصعب متابعة بعض الأفعال الرقمية.
- حاجة المؤسسات المكلفة بالتحري والبحث الرقمي إلى تعزيز مواردها البشرية والتقنية، وتحسين التنسيق بين الجهات المختلفة لضمان سرعة الاستجابة وكفاءة التحقيقات.
- استناداً إلى هذه النتائج، تبرز مجموعة من التوصيات لتعزيز مكافحة الجرائم السيبرانية في الجزائر، وهي كالتالي:

1. تطوير التشريع باستمرار لضمان شمول النصوص لجميع صور الجرائم الرقمية، ومراجعة العقوبات لتكون رادعة وملائمة لطبيعة هذه الجرائم المعقدة.

2. تعزيز قدرات أجهزة التحري والبحث الرقمي من خلال برامج تدريب متقدمة على التكنولوجيا الحديثة، وتزويدها بالأدوات الرقمية اللازمة لتحليل الأدلة ومتابعة الجرائم بكفاءة أكبر.

3. تقوية المؤسسات الوطنية المكلفة بالأمن السيبراني عبر زيادة الموارد البشرية والتقنية، وتحسين التنسيق بين الهيئات القضائية والأمنية لضمان فعالية العمل وتوحيد الجهود.

4. تفعيل التعاون الدولي مع السلطات الأجنبية الماثلة لتبادل المعلومات والخبرات ومواجهة الجرائم العابرة للحدود بفاعلية أكبر.

5. رفع مستوى الوعي لدى المستخدمين والمجتمع الرقمي بشأن مخاطر الجرائم السيبرانية وسبل حماية البيانات الشخصية والمؤسسية، من خلال حملات توعية وورش تدريبية.

6. تطوير آليات متابعة وتنفيذ العقوبات لضمان الردع الفعلي وتحقيق العدالة للمجني عليهم، بما يعزز الثقة في القانون وفعالية تطبيقه.

7. تشجيع البحث والدراسة الأكاديمية في مجال الجرائم السيبرانية، بما يساهم في تحديث التشريع والآليات العملية باستمرار لمواكبة الابتكارات الرقمية.

وفي الختام، يتضح أن مكافحة الجرائم السيبرانية تتطلب مقاربة شاملة تجمع بين تشريع منطور، أجهزة تحري وتقنيات متقدمة، مؤسسات وطنية قوية، تعاون دولي، ووعي مجتمعي مستمر. إن تضافر هذه العناصر يضمن فضاءً رقمياً آمناً يحمي الحقوق والمعطيات الشخصية، ويحد من التهديدات الرقمية المتزايدة، ويعزز قدرة الجزائر على مواجهة التحديات الجديدة في عالم رقمي متصل بشكل متسارع.

الهوامش:

1 عبد الفتاح بيومي مجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دار الفكر الجامعي، مصر، 2006، ص 44.

2 حنان مهداوي، التنظيم القانوني للجريمة الالكترونية في التشريع الجزائري، مجلة الفكر القانوني والسياسي، المجلد 06، العدد 02، 2022، ص 1060.

3 رحمة نمديلي، خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة، المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية، جامعة طرابلس، 24-25 مارس 2017، ص 101.

4 القانون رقم 04-09، المؤرخ فيلا 05 أوت 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، الجريدة الرسمية عدد 47، الصادرة بتاريخ 16 أوت سنة 2009.

- 5 غادة ناصر، الإرهاب والجريمة الالكترونية، دار العربي للنشر والتوزيع، مصر، 2017، ص 32.
- 6 خالد عبد الحق، الجرائم الالكترونية والتحقيقات الجنائية، دار اليازوري للنشر والتوزيع، الأردن، 2025، ص 18.
- 7 دعاء عبد العال، خالد عبد الحق، الجرائم الالكترونية والتحقيقات الجنائية، دار اليازوري للنشر والتوزيع، الأردن، 2025، ص 19.
- 8 فارس العمارات، جرائم العصر من الرقمية إلى السيبرانية، دار الخليج للنشر والتوزيع، الأردن، 2023، ص 127.
- 9 المرجع نفسه، ص 128.
- 10 حمزة خضري، حمزة عشاش، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، المجلد 06، العدد 02، 2012، ص 173.
- 11 خليفة أحمد الملط، الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2006، ص 12.
- 12 جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار الفكر العربي، مصر، 2001، ص 62.
- 13 حمزة خضري، حمزة عشاش، المرجع السابق، ص 174.
- 14 أحسن بوسقيعة، الوجيز في القانون الجنائي العام، دار هومة للنشر والتوزيع، الجزائر، 2019، ص 143.
- 15 خليفة أحمد الملط، المرجع السابق، ص 13.
- 16 القانون رقم 09-01 المؤرخ في 26 جوان 2001، المعدل والمتمم للأمر رقم 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 34، الصادرة بتاريخ 27 جوان 2001.
- 17 أنظر في ذلك، المادة 144 من القانون رقم 09-01 المؤرخ في 26 جوان 2001، المعدل والمتمم للأمر رقم 66-156.
- 18 القانون رقم 06-23، المؤرخ في 8 جوان 2006، المعدل والمتمم للأمر رقم 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 84، الصادرة بتاريخ 24 ديسمبر 2006.
- 19 القانون 11-14، المؤرخ في 02 أوت 2011، المعدل والمتمم للأمر رقم 66-156، المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 44، الصادرة بتاريخ 10 أوت 2011.
- 20 القانون رقم 04-15، المؤرخ في 10/12/2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية عدد 71، الصادرة في نوفمبر 2004.
- 21 انظر في ذلك الفقرة الأخيرة من المادة 87 مكرر 11، من الامر 16 02، المؤرخ في 19 جوان 2016، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن لقانون العقوبات، الجريدة الرسمية عدد 37، الصادرة بتاريخ 22 جوان 2016.

- 22 الأمر رقم 01-20، المؤرخ في 30 جويلية 2020، المعدل والمتمم للأمر رقم 66-156، المؤرخ في 08 جويلية 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 44، الصادرة بتاريخ 30 جويلية 2020.
- 23 المواد 124 مكرر 08، 09، 12، من الأمر رقم 01-20، المؤرخ في 30 جويلية 2020، المعدل والمتمم للأمر رقم 66-156.
- 24 الأمر 03-05، المؤرخ في 19 جوان 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، عدد 44، الصادرة بتاريخ 23 جويلية 2003.
- 25 Quemener. M, Ferry. J Cybercriminalité, Défi Mondial, Ed Economica, Paris, 2ème Edition 2009 P.05
- 26 قانون عضوي رقم 05-12 مؤرخ في 12 جانفي لسنة 2012، يتعلق بالإعلام، الجريدة الرسمية عدد 02، الصادرة بتاريخ 15 جانفي 2012.
- 27 القانون رقم 07 / 18، المؤرخ في 10 يونيو 2018، الخاص بحماية الاشخاص الطبيعيين في ميدان معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34 المؤرخة في 10 يونيو 2018.
- 28 المادتين: 01، 02، القانون رقم 07 / 18، المؤرخ في 10 يونيو 2018، الخاص بحماية الاشخاص الطبيعيين في ميدان معالجة المعطيات ذات الطابع الشخصي.
- 29 المحمود حسين بوادي، الوسائل التقنية الحديثة في الاثبات الجنائي، منشأة المعارف، مصر، 2005، ص 10.
- 30 المادة 12، الأمر رقم 155/66 المؤرخ في 08/06/1966 المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.
- 31 المادة 14، الأمر رقم 155/66، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، المصدر السابق.
- 32 المادة 15، الأمر رقم 155/66، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم، المصدر السابق.
- 33 المواد 16، 16 مكرر، 17، الأمر رقم 155/66، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم.
- 34 المادتين 10، 11، من القانون 04-09، المؤرخ في 14 شعبان عام 1430، الموافق 5 غشت سنة 2009. يتضمن القواعد الخاصة ب الوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية عدد 47. الصادر بتاريخ 16 اوت 2009.
- 35 القانون رقم 01-06 مؤرخ في 20-02-2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية عدد 14، صادر بتاريخ 03-08-2006.
- 36 القانون رقم 22-06 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 155-66 المؤرخ في 8 جويلية 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 84، لسنة 2006.
- 37 المادة 65 مكرر 11، لقانون رقم 22-06 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 155-66 المؤرخ في 8 جويلية 1966، المتضمن قانون الإجراءات الجزائية.
- 38 فوزي لواتي، التسرب كالية للتحقيق في جرائم الاتجار بالمخدرات في الجزائر: المتطلبات القانونية والاشكالات العملية، مجلة آفاق للعلوم، الجزء 1، العدد 2، 2016، ص 216.

- 39 المادة 65 مكرر 05، القانون رقم 22-06 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 155-66 المؤرخ في 8 جويلية 1966، المتضمن قانون الإجراءات الجزائية.
- 40 المادة 65 مكرر 7، القانون رقم 22-06 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم للأمر 155-66 المؤرخ في 8 جويلية 1966، المتضمن قانون الإجراءات الجزائية.
- 41 المادة الثانية، المرسوم الرئاسي رقم 19-172 مؤرخ في 06 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، جريدة رسمية عدد 37 الصادر في 09 يونيو 2019
- 42 المادة 25، مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية، العدد 86.
- 43 المادة 26، مرسوم رئاسي رقم 21-439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- 44 القانون رقم 18-07، المؤرخ في 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية عدد 34، الصادرة بتاريخ 10 جويلية سنة 2018.
- 45 النظام الداخلي للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، المصادق عليه من طرف أعضاء السلطة الوطنية بتاريخ 26 جويلية 2023.
- 46 القانون 18-07، المؤرخ في 10 جويلية 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، الصادرة بتاريخ 10 جويلية 2018.
- 47 المادة 25، القانون 18-07، المؤرخ في 10 جويلية 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، الصادرة بتاريخ 10 جويلية 2018.