

آليات التصدي للجرائم السيبرانية في القانون الجزائري

مليلة أوباية⁽¹⁾

ناصر زورور⁽²⁾

(2) أستاذ، كلية الحقوق والعلوم السياسية، جامعة

(1) أستاذ محاضر قسم "أ"، كلية الحقوق والعلوم

مولود معمري تيزي وزو، الجزائر.

السياسية، جامعة مولود معمري تيزي وزو، الجزائر.

البريد الإلكتروني: malika.oubaya@ummtto.dz

البريد الإلكتروني: Nacer.zerourou@ummtto.dz

الملخص:

تواجه الجزائر على غرار باقي دول العالم مخاطر الهجمات السيبرانية التي تشكل تهديدات بمصالحها وبسيادتها الرقمية، الأمر الذي دفعها للتصدي لهذه المخاطر من خلال تبني مجموعة من النصوص القانونية التي تجرم العديد من الجرائم السيبرانية على غرار الولوج إلى الأنظمة المعلوماتية بطريقة غير قانونية، اختراقها، إحداث تغيير أو تزوير فيها، التعدي على أنظمة المعلومات أو التلاعب بالمعطيات، في إطار قانون العقوبات باعتباره الإطار العام للجرائم وفي قوانين خاصة وضعت من أجل حماية أنظمة الإعلام والاتصال على غرار القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

إلى جانب استحداث مؤسسات لتفعيل هذا الإطار القانوني وضمان التصدي للجرائم السيبرانية والوقاية منها على غرار الوكالة الوطنية لأمن المعلوماتية، اللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي والقطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

رغم أهمية هذه الآليات القانونية والمؤسسية في التصدي للجرائم الإلكترونية، إلا أنه يتعين تعزيزها باعتماد قانون موحد ينظم كل مستلزمات الأمن السيبراني وكذا الانخراط في بعض التكتلات الدولية للتصدي لهذه الجرائم باعتبارها في الغالب جرائم عابرة للحدود.

الكلمات المفتاحية:

الجريمة، الأمن السيبراني، أنظمة المعلومات، الاتصالات الإلكترونية، البيانات الشخصية.

تاريخ إرسال المقال: 2025/12/09، تاريخ قبول المقال: 2026/05/23، تاريخ نشر المقال: 2026/06/30

المؤلف المراسل: أوباية مليلة، oubaya_malika@yahoo.fr

المجلد 17، العدد 01-2026

أوباية مليلة، زورور ناصر، "آليات التصدي للجرائم السيبرانية في القانون الجزائري"، ص ص

Mechanisms for Combating Cybercrime in Algerian Law

Abstract:

Like other countries around the world, Algeria faces the risks of cyberattacks that may pose threats to its economic, political, and security interests, as well as to its overall digital sovereignty. This situation has led the country to address such risks through the adoption of a set of legal instruments criminalizing various cybercrimes, such as illegal access to information systems, hacking, alteration or falsification of data, infringement of information systems, and manipulation of data. These offences are covered under the Penal Code as the general framework for criminalization, as well as under specific laws designed to protect information and communication systems, notably Law No. 09-04 laying down specific rules on the prevention and combating of offences related to information and communication technologies, and Law No. 18-07 on the protection of natural persons with regard to the processing of personal data.

In addition, Algeria has established institutions to implement this legal framework and ensure the prevention and suppression of cybercrime, such as the National Agency for Information Security, the National Commission for the Protection of Personal Data, and the National Judicial Hub for Combating Cybercrime.

Although these legal and institutional mechanisms are important in addressing cybercrime, there remains a need to strengthen them through the adoption of a unified law governing all aspects of cybersecurity, as well as through participation in international cooperation mechanisms to combat these crimes, given their often transnational nature.

Keywords:

Crime, cybersecurity, information systems, electronic communications, personal Data.

Les mécanismes de lutte contre la cybercriminalité en droit Algérien

Résumé :

A l'instar des autres pays du monde, l'Algérie fait face aux risques des cybers attaque qui menacent ses intérêts ainsi que sa souveraineté numérique. Cela l'a conduite à lutter contre ces risques en adoptant un ensemble de textes juridiques incriminant plusieurs formes de cybercriminalité, telles que l'accès illégal aux systèmes d'information, leur intrusion, la modification ou la falsification de leurs contenus, l'atteinte aux systèmes d'information ou la manipulation des données.

Ces mesures ont été prises dans le cadre du code pénal , considéré comme le cadre général des actes répréhensibles, ainsi que dans des lois spéciales adoptées pour protéger les systèmes d'information et de communication , à l'instar de la loi N°09-04 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication , et la loi N°18-07 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.

Par ailleurs, des institutions ont été créées afin de mettre en œuvre ce cadre juridique et d'assurer la lutte contre la cybercriminalité, telles que l'Agence Nationale de la Sécurité des Systèmes d'Information, la Commission National de Protection des Données à caractère personnel et le pole pénal national de lutte contre les infractions liées aux technologies de l'information et de la communication. Malgré l'importance de ces mécanismes juridiques et institutionnels dans la lutte contre la cybercriminalité, il demeure nécessaire de les renforcer, notamment par l'adoption d'une loi unifiée régissant les exigences du cyber sécurité, ainsi par l'adhésion à certains conventions internationaux visant à lutter contre ces infractions, considérées le plus souvent comme des crimes transfrontaliers.

Mots-clés :

Crime, cyber sécurité, systèmes d'information, communications électroniques, données personnelles.

مقدمة

تعتبر الجرائم السيبرانية من الجرائم الحديثة التي ارتبط ظهورها ارتباطا وثيقا بالتطور التكنولوجي واتسع نطاق انتشارها وازدادت وتيرتها بشكل كبير في السنوات الأخيرة إذ أصبحت تندرج ضمن المخاطر الداخلية والدولية وتشكل تهديدا حقيقيا للأمن الوطني والاقتصادي وللمصالح الحيوية لمختلف الدول، الأمر الذي دفع بالمجتمع الدولي للاهتمام بالمسألة والتكثف من أجل إرساء أطر قانونية لتوفير الأمن السيبراني والتصدي لكل أشكال هذه الهجمات والوقاية منها. من أبرز هذه الأطر التوقيع على اتفاقية بودابست لمكافحة الجرائم السيبرانية التي وضعها المجلس الأوروبي سنة 2001 والتي تعد الإطار القانوني الدولي الأول الذي اجتمعت بشأنه الدول لمواجهة الجرائم التي ترتكب عبر الوسائط الالكترونية¹.

رغم أهمية هذه الاتفاقية وتأثيرها في توجيه التشريعات الداخلية للدول المنخرطة في توفير الأمن السيبراني إلا أن طابعها الإقليمي في البداية جعل عددا من الدول تحفظت عن الانضمام إليها واختارت التصدي لهذه الجرائم باعتمادها على قوانينها الداخلية وعلى مؤسساتها الخاصة.

تعد الجزائر واحدة من هذه الدول، لكن رغم عدم انضمامها للاتفاقية بودابست، إلا أنها تأثرت بمضمون الاتفاقية وبالمبادئ والقواعد التي أرستها، لذلك تبنت منظومة قانونية دعمتها بنصوص خاصة ومؤسساتية للتصدي للجرائم السيبرانية والوقاية منها لتوفير الأمن السيبراني لكل الاتصالات الالكترونية.

من هذا المنطلق نسعى من خلال هذا المقال للبحث عن مدى فعالية المنظومة القانونية والمؤسساتية المعتمدة في الجزائر لمواكبة التحديات التي يفرضها التصدي للجرائم السيبرانية والوقاية منها في ظل التطور السريع والطابع العابر للحدود لهذه الجرائم؟

للإجابة على هذه الإشكالية يتعين اعتماد المنهج التحليلي، يتم بمقتضاه دراسة وتحليل ما اعتمدته الجزائر من آليات في إطار سياستها للتصدي للجرائم السيبرانية المتمثلة في إرساء أطر قانونية دعمت من خلالها منظومتها الجزائية بقواعد جرمت من خلاله العديد من الجرائم السيبرانية (المبحث الأول)، وعلى

¹ مجلس أوروبا: الاتفاقية المتعلقة بالجريمة الالكترونية، الموقعة في بودابست يوم 23/11/2001 متاحة على الموقع الرسمي للمجلس الأوروبي على الرابط : <http://www.conventions.coe.int>

استحداث مجموعة من المؤسسات والهيئات على مستويات عدة للتدخل في مواجهة هذه الجرائم والوقاية منها (المبحث الثاني).

المبحث الأول: إرساء إطار قانوني للتصدي للجرائم السيبرانية في الجزائر

تعمل السلطات الجزائرية جاهدة لمواكبة التغيرات والمستجدات العالمية التي يشهدها المجتمع الدولي باستمرار من خلال الانضمام إلى اتفاقيات ثنائية ومتعددة الأطراف، لكن في مجال مكافحة الجرائم السيبرانية ورغم تكييف هذه جرائم بالخطيرة والعابرة للحدود مما يستدعي التعاون الدولي لمجابهتها²، اختارت عدم الانضمام لاتفاقية بودابست لمواجهة الجرائم الالكترونية³ حفاظا على سيادتها الرقمية وتحفظها عن بعض القواعد الإجرائية التي تضمنتها الاتفاقية⁴. إلا أنها تأثرت كثيرا بالقواعد الموضوعية وبالمبادئ التي جاءت بها، فجرمت العديد من الأفعال التي تشكل الهجمات السيبرانية من خلال التعديل الذي أدخل على قانون العقوبات في سنة 2004 (المطلب الأول) ومن خلال اعتماد نصوص قانونية خاصة وسعت من خلالها الإطار القانوني الرادع للجرائم السيبرانية (المطلب الثاني).

المطلب الأول: تجريم بعض الهجمات السيبرانية في قانون العقوبات

لم يعتمد المشرع الجزائري بشكل صريح مصطلح الجرائم السيبرانية في المنظومة القانونية الجزائرية، إلا أنه تأثر بالتدابير المقررة على المستوى الدولي للتصدي لهذه الجرائم لاسيما القواعد الموضوعية التي أقرتها اتفاقية

² تم تكييف الجرائم المعلوماتية لأول مرة بالعبارة للحدود في القضية المعروفة برنامج بنقص المناعة المكتسبة التي وقعت في المملكة المتحدة في 1989 والتي قام في إطارها شخص يدعى جوزيف بوب بتوزيع عدد من النسخ في عدة دول من برنامج يحتوى نصائح وإرشادات للوقاية ومواجهة المرض، لكنه ضمن البرنامج فيروس من خلاله تم السطو على حسابات مالية للأشخاص الذين حملوا البرنامج وانخرطوا فيه، تم القبض عليه في الولايات المتحدة ثم تم تسليمه لبريطانيا بناء على طلبها باعتبار أنه أرسل البرنامج من إقليمها، فبذلك اعتبر أول مجرم معلوماتي يتم تسليمه ويحاكم بتهمة جريمة معلوماتية، للمزيد من التوضيح حول هذه القضية ومفهوم الجرائم المعلوماتية راجع: المومني نهلا عبد القادر، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان 2010، ص 52 وما يليها

³ إذ تسمح المادة 32 من الاتفاقية لدولة عضو من الولوج مباشرة لبيانات كمبيوتر متاحة للعموم موجودة في دولة أخرى دون إذن مسبق منها في حالات محددة، كما أنها تلزم مقدمي خدمات الانترنت بتسليم البيانات للدولة عضو من دون الرجوع إلى دولته الأصلية، وهو ما تعتبره السلطات الجزائرية مساسا بالسيادة الرقمية للدول الأعضاء وكان من أبرز أسباب عدم انضمامها للاتفاقية ⁴ فطاف سليمان، بوقرين عبد الحليم، "آليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري"، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 6، العدد 01، 2022، ص 338.

بودباست التي من خلالها فرضت على الدول الأعضاء إدخال تعديل على قوانينها العقابية وتجريم الأفعال التي تشكل هجمات سيبرانية، لذلك مباشرة بعد دخول الاتفاقية حيز التنفيذ في جويلية 2004، تبنى بموجب القانون رقم 15-04 المؤرخ في 10 نوفمبر 2004⁵ نوعا جديدا من الجرائم تدخل في إطار مفهوم الجرائم السيبرانية (الفرع الأول)، من خلال تجريمه لمجموعة من الأفعال التي تشكل اعتداءات على أنظمة المعالجة الآلية للمعطيات والإقرار لها بعقوبات جزائية (الفرع الثاني).

الفرع الأول: تكريس مفهوم الجرائم السيبرانية في قانون العقوبات

تعتبر الجرائم السيبرانية شكلا متطورا من أشكال الجريمة العابرة للحدود المرتبطة بالفضاء الإلكتروني والرقمي والتي يترتب عنها أضرار جسيمة بمصالح الأشخاص أو المصالح الحيوية للدولة⁶، تندرج هذه الجرائم تحت مظلة المفاهيم الشديدة التعقيد التي لم تحظ بتكييف موحد، إذ ينظر إليها البعض على أنها مجرد انتقال لمفهوم الجريمة التقليدية إلى العالم الافتراضي، فيما يعتبرها البعض الآخر شكلا جديدا من الجرائم المستحدثة ظهرت نتيجة التفاعل الديناميكي بين الفرد وتكنولوجيا المعلومات⁷. أما مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة فقد اعتبر الجرائم السيبرانية مفهوما غير قانوني قائم بذاته، بل تعبير جامع يشمل مجموع الأفعال المرتكبة ضد البيانات أو نظم الحاسوب أو باستخدامها⁸.

كما لم يتفق الفقه ولا التشريعات حول تعريف موحد للجريمة السيبرانية، ففي ظل أزمة المصطلحات وبروز العديد من الجهود لضبط معناها على المستوى الداخلي وعلى المستوى الدولي، ألحقت بها العديد من التعاريف، فهناك من ركز في تعريفها على كونها جرائم مستحدثة ظهرت كأثر سلبي للتطور الذي شهدته وسائل الإعلام

⁵ قانون رقم 15-04 مؤرخ في 10 نوفمبر 2004، يعدل ويتم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، ج ر عدد 71، صادر في 10 نوفمبر 2004.

⁶ محسن عباس محسن، الهجمات السيبرانية ومنطقة الفراغ التشريعي، دراسة في ميثاق الأمم المتحدة والقانون الدولي، الفا للوثائق، عمان، 2021، ص ص 65-66.

⁷ بوبكر رشيدة، الجرائم السيبرانية وتكنولوجيا الذكاء الاصطناعي بين تصاعد التهديدات وفرص تعزيز الأمن السيبراني، دار ايلياء للنشر والتوزيع، الجزائر، 2024، ص 35.

⁸ تقرير مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال إفريقيا، من 12 إلى 19 أبريل 2010، الدوحة، ص ص 08-09. متاح على

الموقع: www.unodc.org/romeria/ar/cybercrime.htm/

والاتصال واستخدامات الانترنت في السنوات الأخيرة⁹. وهناك من ركز على الفعل الإجرامي المشكل لركنها المادي فاعتبرها تلك السلوكات الإجرامية التي تستهدف البيانات والنظم الحاسوبية، أو على الوسائل المعتمد عليها في ارتكاب الجريمة، فاعتبرها كل سلوك غير مشروع يرتكب باستخدام الحاسوب والانترنت¹⁰. فيما كيفها البعض الآخر على أنها صورة متطورة للجرائم الالكترونية تستهدف زعزعة الأمن والاستقرار في الفضاء السيبراني عن طريق الدخول غير المشروع لشبكات الاتصالات والمعلومات بهدف تحقيق مصالح غير مشروعة¹¹.

الفرع الثاني: حصر التجريم في قانون العقوبات على الجرائم السيبرانية التقليدية

لم يضع المشرع الجزائري تعريفا للجرائم السيبرانية، لكنه تماشيا مع تجريمها على المستوى الدولي وفي العديد من الدول أدخل إصلاحا جوهريا على قانون العقوبات الجزائري، استحدث من خلاله القسم السابع مكرر المعنون المساس بأنظمة المعالجة الآلية للمعطيات، فجرم من خلال مواده مجموعة من الجرائم السيبرانية، تعتبر تقريبا نفس الجرائم التي اعتبرت اتفاقية بودابست جرائم الكترونية في إطار المجموعتين الأولى والثانية من مجموع الجرائم التي عدتها ضمن فئة الجرائم التي تتضمن مساسا بالخصوصية وسلامة الأنظمة والبيانات والجرائم ذات الصلة بالكمبيوتر¹².

جرم المشرع الجزائري مجموعة من الأفعال التي تشكل هجمات سيبرانية تقليدية وتتمثل هذه الأفعال في:

- فعل الدخول أو البقاء عن طريق الغش في جزء من منظومة المعلومات.
- كل حذف أو تغيير في معطيات المنظومة عن طريق الغش.
- كل فعل يهدف إلى إدخال بطريق الغش معطيات في نظام لمعالجة المعطيات أو يهدف إلى إزالة المعلومات منه أو تغييرها أو تزيفها¹³.

⁹ محمد علي قطب، الجرائم المستحدثة وطرق مواجهتها، دار الفجر للنشر والتوزيع، القاهرة، 2009، ص ص 130-133.

¹⁰ محمد أمين السويكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، 2004، ص ص 29-30.

¹¹ محسن عباس محسن، مرجع سابق، ص ص 45-47.

¹² تتمثل هذه الجرائم أساسا في: النفاذ غير المشروع للأنظمة، الاعتراض غير المشروع، التدخل في البيانات أو النظام إساءة استخدام الأجهزة والتزوير والاحتيايل المرتبط بالكمبيوتر، للمزيد من التوضيح بشأن الجرائم الالكترونية التي عدتها الاتفاقية انظر المواد من 2 إلى 8 من اتفاقية بودابست المتعلقة بالجريمة الالكترونية، مرجع سابق.

¹³ انظر المادة 394 مكرر 1 من القانون 04-15 المتضمن تعديل قانون العقوبات، مرجع سابق.

- كل فعل تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار بمعطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية.

كيفّ المشرع الجزائري كل هذه الأفعال جنحا وقرر لها عقوبات متباينة تختلف من جريمة إلى أخرى تتراوح ما بين الحبس من شهرين إلى خمس سنوات وغرامات مالية تتراوح ما بين 50.000 إلى 5000.000 دج¹⁴، وعندما يكون مرتكب الجريمة شخصا معنويا فإن الغرامة التي تفرض عليه في هذه الحالة تعادل 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي بشأن نفس الفعل الإجرامي.

كما اعتبر المشرع مجرد الشروع في هذه الأفعال جريمة قائمة بذاتها ويعاقب مرتكبها بنفس العقوبة المقررة في الجريمة التامة، كما تطبق ذات العقوبات على الشريك في جميع أشكال الجرائم السيبرانية المذكورة سابقا. عندما تستهدف هذه الهجمات مؤسسة من مؤسسات القانون العام يعد ذلك ظرفا مشددا، فيكتسب الفعل طابعا أكثر خطورة لذلك تضاعف العقوبة على مرتكبيه وعلى الشريك فيها¹⁵. لكن تجدر الإشارة إلى أن المشرع الجزائري في إطار تجريمه لهذه الأفعال لم يراع أنواع مرتكبي هذه الجرائم ولا تصنيفهم وفقا لأغراض الاعتداء، فاعتمد نفس العقوبة سواء كان مرتكبها من المتطفلين الهاكرز والكراز أو المحترفين الذين يهدفون من اعتداءاتهم أساسا إلى تحقيق مكسب مادي أو أغراض سياسية أو مجرد حاقدين لا يسعون إلى إثبات قدراتهم الفنية ولا إلى تحقيق مكاسب مادية فدافعهم لارتكاب الفعل الإجرامي مجرد الانتقام. كما أغفل المشرع في إطار قانون العقوبات الإشارة إلى صغار نوابغ المعلوماتية الذين عادة ما يرتكبون هذه الجرائم بدفع المغامرة فقط دون أي قصد جنائي¹⁶، مما يعنى إخضاعهم لنفس العقوبة مع البالغين دون الاستفادة من أي ظرف مخفف، لذلك يتعين على المشرع مواكبة المستجدات وتعديل أحكام قانون العقوبات تماشيا معها، لأنه منذ 2004 تطورت بكثير الجرائم السيبرانية وظهرت أشكال جديدة لتنفيذ الهجمات السيبرانية لا تعتمد فقط على الأفعال التقليدية المحددة في إطار القسم السابع مكرر من قانون العقوبات.

¹⁴ انظر المواد 394 مكرر إلى المادة 394 مكرر 4 من القانون 04-15، مرجع سابق.

¹⁵ انظر المادة 394 مكرر 3 من نفس القانون.

¹⁶ بوبكر رشيدة، مرجع سابق، ص ص 43-44.

كما أنه عند التدقيق في هذه الأفعال يتبين أنها تتدرج أكثر في صنف الجرائم الالكترونية أكثر منها جرائم سيبرانية وأن نية المشرع من خلال هذا الإصلاح القانوني اتجهت أكثر للتصدي للجرائم الالكترونية دون باقي الجرائم السيبرانية.

المطلب الثاني: تجريم بعض الأفعال المشككة لهجمات سيبرانية بموجب قوانين خاصة

لم يكتف المشرع الجزائري بتجريم بعض الأفعال المشككة لهذه الهجمات في قانون العقوبات، فبهدف التوسيع من نطاق التصدي لأشكال الهجمات السيبرانية، بل دعمه بتبني عدة نصوص قانونية خاصة سعى من خلالها لضمان الأمن السيبراني وحماية أنظمة الاتصال ومعالجة المعطيات، فجرم من خلالها مجموعة أخرى من الأفعال التي تشكل هجمات سيبرانية، من أهم هذه النصوص قانون البريد والاتصالات الالكترونية (الفرع الأول)، القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (الفرع الثاني) القانون الخاص بحماية المعطيات ذات الطابع الشخصي (الفرع الثالث).

الفرع الأول: بموجب قانون البريد والاتصالات الالكترونية

اعتمد المشرع الجزائري سنة 2018 قانونا جديدا لتحديد القواعد العامة للبريد والاتصالات الالكترونية¹⁷، أكد من خلاله على التزام الدولة وسهرها على توفير أمن وسلامة شبكات الاتصالات الالكترونية في الجزائر، وضمانا لذلك تم تحديد ولأول مرة في القانون الجزائري مفهوم الأمن السيبراني، حيث اعتمد بشأنه مدلولاً أوسع بكثير من مجرد تجريم الجرائم الالكترونية، فاعتبره مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية ضد أي حدث من شأنه المساس بتوفير وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسل¹⁸. ضمانا لتجسيد هذا المدلول للأمن السيبراني تم تجريم مجموعة أخرى من الأفعال تتمثل أساسا في:

- جريمة انتهاك سرية المراسلات الالكترونية.

- جريمة تحويل المراسلات أو خطوط الاتصالات الالكترونية.

¹⁷ قانون رقم 18-04 مؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر عدد 27، صادر في 13 ماي 2018.

¹⁸ انظر المادة 394 مكرر 3 من نفس القانون.

-جريمة إتلاف أو تخريب الأجهزة والمنشآت ووسائل الاتصال الالكترونية.

ويندرج في إطار هذه الإشكال من الجرائم العديد من الجرائم السيبرانية المستحدثة كهجمات البرمجيات الخبيثة والبرمجيات الضارة، الهندسة الاجتماعية¹⁹.

على غرار التكييف المعتمد في قانون العقوبات للجرائم السيبرانية، اعتبرها المشرع في هذا النص جنحا، وأقر لها عقوبات حبس متفاوتة تتراوح ما بين سنة إلى خمس (5) سنوات وغرامات مالية متباينة تتراوح ما بين 1000000 إلى 5000000 دج، ولكن عندما تتخذ الجريمة السيبرانية شكل فعل مادي يتمثل في قطع أو إتلاف كابل بحري عمدا من أجل توقيف أو تعطيل الاتصالات الالكترونية كليا أو جزئيا يتغير تكييف الجريمة من جنحة إلى جناية وقد تصل عقوبتها إلى السجن 10 سنوات²⁰. كما تم التركيز على مسؤولية المتعاملين في مجال الاتصالات الالكترونية عندما لا يتدخلون رغم إغذراهم من قبل سلطة الضبط القطاعية لمنع النفاذ إلى شبكة الاتصالات الالكترونية.

الفرع الثاني: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

إلى جانب القواعد الردعية السابق الإشارة إليها تبني المشرع بمقتضى القانون 04-09 قواعد خاصة للوقاية من جرائم تكنولوجيا الإعلام والاتصال²¹، استحدثت الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال، وأسند لها مهمة تنسيق عمليات الوقاية من الجرائم السيبرانية والاتصالات الماسة بأنظمة الاتصالات الالكترونية وتقديم العون للسلطات القضائية والأمنية في التحري بشأن هذه الجرائم.

رغم عدم الانضمام إلى اتفاقية بودابست إلا أن المشرع الجزائري أظهر تأثره ببعض بنود الاتفاقية من خلال هذا القانون فأقر بآلية المساعدة القضائية الدولية المتبادلة في مجال التحري والتحقيقات القضائية للكشف عن مرتكبي الجرائم السيبرانية وجمع الأدلة حولها²²، مثلما أكدت عليه الاتفاقية بالنسبة للدول الأعضاء في إطار الفصل الأول من الباب الثالث المتعلق بالتعاون الدولي²³.

¹⁹ بوبكر رشيدة، مرجع سابق، ص ص 51-52.

²⁰ انظر المادة 179 من القانون 04-18، مرجع سابق.

²¹ قانون رقم 04-09 مؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 47، صادر في 16 أوت 2009.

²² انظر المادة 16 من نفس القانون 04-09، مرجع سابق.

²³ انظر المادة 23 من الاتفاقية المتعلقة بالجريمة الالكترونية، مرجع سابق.

الفرع الثالث: القانون الخاص بحماية المعطيات ذات الطابع الشخصي

اعتمد القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي²⁴، بغرض تعزيز الأمن السيبراني في مجال حماية الخصوصية الرقمية فجرم، على غرار ما تضمنته اتفاقية بودابست، بعض الأفعال التي تشكل جرائم اعتداء على الخصوصية.

ألزم مقدمي خدمات الاتصالات الالكترونية المفتوحة للجمهور بإبلاغ فوراً السلطة الوطنية لحماية المعطيات الشخصية والمعني عن كل تلف أو ضياع أو إفشاء أو ولوج غير مرخص به إلى البيانات الشخصية وعن كل انتهاك أو تغيير في المعطيات ذات الطابع الشخصي.

كما اعتبر كل فعل من شأنه أن يؤدي إلى جمع المعطيات ذات الطابع الشخصي ونقلها نحو دولة أجنبية دون الحصول على ترخيص مسبق من السلطات الوطنية المختصة جريمة سيبرانية ويعاقب عليها قانوناً، تقدر هذه الأخيرة عند نقل المعطيات إلى دولة أجنبية أو منظمة دولية المستوى الكافي من الحماية الذي يجب أن توفره الجهة التي يتم إليها نقل هذه البيانات على أن ينتفي عن الفعل الصفة الإجرامية²⁵.

إلى جانب كل هذه النصوص القانونية التي قام من خلالها المشرع الجزائري بتجريم أشكال عديدة للهجمات السيبرانية، صنفت الهجمات السيبرانية ضمن المخاطر والكوارث التي يتعين التصدي لها في إطار ضمان التنمية المستدامة²⁶، لذلك يتم التحضير حالياً لقانون شامل للأمن السيبراني لتوفير حماية متكاملة للأنظمة المعلوماتية من كل أشكال الهجمات السيبرانية وتعزيز من خلاله البنى التحتية وإرساء نظام التبليغ السريع عن المجرمين وتعزيز حماية المعطيات ذات الطابع الشخصي وتوفير الأمن السيبراني لكل الاتصالات الالكترونية

²⁴ قانون رقم 07-18، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر عدد 34، صادر في 10 جوان 2018، معدل ومتمم بالقانون رقم 11-25، المؤرخ في 24 جويلية 2025، ج ر عدد 48، صادر في 24 جويلية 2025.

²⁵ انظر المادة 45 مكرر 13 من القانون رقم 11-25، المعدل والمتمم للقانون 07-18، المرجع نفسه.

²⁶ انظر المادة 55 من القانون رقم 04-24 المؤرخ في 26 فيفري 2024، يتضمن قواعد الوقاية والتدخل والحد من أخطار الكوارث في إطار التنمية المستدامة، ج ر عدد 16، صادر في 6 مارس 2024.

وتأمينها من أية اختراقات أو هجمات، يتم إعداد هذا القانون من قبل خبراء ومختصين²⁷. وبالاطلاع على تجارب الدول الرائدة في مجال الأمن السيبراني²⁸.

المبحث الثاني: إرساء إطار مؤسساتي متعدد لمواجهة الجرائم السيبرانية في الجزائر

إلى جانب تجريم العديد من الأفعال التي تشكل هجمات سيبرانية وإقرار عقوبات جزائية ردعية على مرتكبيها، دعمت الجزائر ذرعها الوافي من هذه الجرائم باعتماد إطار مؤسساتي يتكون من عدة أجهزة وهيكل لضمان توفير الأمن السيبراني والتصدي للهجمات التي يمكن أن تزعزعه وللوقاية منها ومن أبرز هذه المؤسسات استحداث سلطات ضبط قطاعية في القطاعات ذات الصلة بالأنظمة المعلوماتية هما: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (المطلب الأول)، اعتماد إستراتيجية وطنية لأمن الأنظمة المعلوماتية يتولى تجسيدها مجلس وطني لأمن الأنظمة المعلوماتية ووكالة لأمن الأنظمة المعلوماتية (المطلب الثاني) إلى جانب استحداث جهة قضائية خاصة لمتابعة مرتكبي الجرائم السيبرانية تتمثل في القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (المطلب الثالث).

²⁷ القانون ما يزال قيد الإعداد لم يتم نشر بعد المسودة الخاصة به، للمزيد من التوضيح حول هذا المشروع راجع: بهلولي أسماء، "مشروع قانون للأمن السيبراني على طاولة الحكومة قريبا"، مجلة الشروق، العدد الصادر في 2025/06/30، متاح على الموقع

www.echorokonline.com

²⁸ لاسيما قانون الاتحاد الأوروبي والقانون الفرنسي والألماني.

المطلب الأول: استحداث هيئات إدارية مستقلة لضمان الأمن السيبراني

تبنى المشرع الجزائري منذ مطلع التسعينات نموذج السلطات الإدارية المستقلة في العديد من القطاعات الاقتصادية الحيوية كالقطاع المصرفي، الإعلام، البورصة، التأمينات، المناجم...، فأسند لها مهمة المراقبة والإشراف على هذه القطاعات بالاعتماد على آليات الضبط الاقتصادي²⁹.

نقل هذا النموذج من السلطات الإدارية لمجال ضمان الأمن السيبراني، فاستحدثت سلطتي ضبط في مجال الأنظمة المعلوماتية ومكافحة الجرائم السيبرانية هما الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام، والاتصال ومكافحتها (الفرع الأول) والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (الفرع الثاني).

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

استحدثت بموجب القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في البداية في شكل مؤسسة عمومية ذات طابع إداري وزودها بالشخصية المعنوية والاستقلال المالي³⁰، تتولى الهيئة تنسيق وتنشيط عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتساهم في التصدي لها، من خلال تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية عند مباشرتها التحريات وتجميع المعلومات وإعداد الخبرات القضائية بشأن مختلف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

نظرا للطابع العابر للحدود للجرائم السيبرانية، تم التوسيع من صلاحيات الهيئة لاستيعاب هذه الخصوصية، لذلك أسندت لها صلاحية التعاون الدولي مع نظيراتها في الخارج وتبادل المعلومات بغرض التعرف على مرتكبي الجرائم السيبرانية وتحديد أماكنهم على أن يتم هذا التبادل للمعلومات وفقا لما هو مقرر في الاتفاقيات الدولية والثنائية ذات الصلة ومراعاة لمبدأ المعاملة بالمثل³¹.

²⁹ Pour plus informations sur les autorités administratives indépendantes en Algérie voir : ZOUAIMIA Rachid, *Les autorités administratives indépendantes et la régulation économique en Algérie*, Éditions HOUMA, Alger, 2005.

³⁰ مرسوم رئاسي رقم 19-172 مؤرخ في 6 جوان 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 37، صادر في 9 جوان 2019 (ملغى).

³¹ انظر المادتين 14 و 17 من القانون 04-09، مرجع سابق.

لكن في سنة 2020 أعيد النظر في المركز القانوني للهيئة، فألحقت بطائفة السلطات الإدارية المستقلة، مما عزز من مكانتها ووسع أكثر من صلاحيتها في مجال الأمن السيبراني واعتبرها المكلفة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال³².

الفرع الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تم بموجب القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، استحداث سلطة إدارية ثانية ذات علاقة بالأمن السيبراني هي السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، على خلاف هيئة الاتصالات الإلكترونية، اعتبر المشرع هذه السلطة منذ إنشائها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، كما تولى مباشرة تحديد تشكيلتها والصلاحيات الموكلة إليها على غرار غالبية السلطات الإدارية المستقلة الأخرى.

تتشكل السلطة من تركيبة جماعية متنوعة تضم شخصيات من ذوي الاختصاص في مجال معالجة المعطيات ذات الطابع الشخصي، قضاة، ممثلين برلمانيين، إلى جانب ممثلين عن مجموعة من الوزارات ذات العلاقة بالأمن السيبراني وممثل للمجلس الوطني لحقوق الإنسان³³.

تسهر السلطة على ضمان معالجة المعطيات ذات الطابع الشخصي في الإطار الذي يسمح به القانون من جهة ومن جهة أخرى تضمن حماية لهذه المعطيات الشخصية من الهجمات والاعتداءات السيبرانية من خلال ضمان عدم انطواء استعمال تكنولوجيا الإعلام والاتصال على أي أخطار تجاه الأشخاص حقوقهم وحياتهم الخاصة، لذلك تتولى وضع المعايير في مجال حماية المعطيات ذات الطابع الشخصي وتطور علاقات التعاون مع الهيئات القضائية، في هذا الإطار تعلم النائب العام فوراً بالوقائع المحتمل أن تشكل هجوماً سيبرانياً بمجرد اكتشافه، كما تتعاون مع السلطات والهيئات الأجنبية المماثلة لها في الحدود المقررة في الاتفاقات الدولية ذات الصلة³⁴.

³² مرسوم رئاسي رقم 20-183 مؤرخ في 13 جويلية 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر عدد 40، صادر في 18 جويلية 2020.

³³ انظر المادة 23 من القانون 07-18، مرجع سابق.

³⁴ انظر المادة 25 من القانون 07-18، مرجع سابق.

المطلب الثاني: اعتماد استراتيجية وطنية لأمن الأنظمة المعلوماتية وقطب جزائي خاص

بغرض تدعيم المنظومة الوطنية لأمن الأنظمة المعلوماتية تم اعتماد استراتيجية وطنية لأمن الأنظمة المعلوماتية في 2020، يركز تجسيد هذه الاستراتيجية على هئتين أساسيتين هما المجلس الوطني لأمن الأنظمة المعلوماتية وكالة أمن الأنظمة المعلوماتية (الفرع الأول) إلى جانب كل هذه الهيئات الإدارية تدعم الإطار المؤسسي الوافي والمتصدي للجرائم السيبرانية باستحداث جهة قضائية خاصة تتمثل في القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (الفرع الثاني).

الفرع الأول: الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية

إدراكا من السلطات الجزائرية بخطورة الجرائم السيبرانية وجسامة التحديات التي تفرضها على السيادة الوطنية وعلى المصالح الحيوية للدولة، تبنت بموجب المرسوم الرئاسي رقم 05-20 منظومة وطنية لأمن الأنظمة المعلوماتية³⁵ تشرف عليها وترعاها مباشرة وزارة الدفاع الوطني، بعد مشاورات موسعة مع العديد من الفاعلين الوطنيين والجهات ذات الصلة بالأمن السيبراني.

تعتبر هذه المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية والإطار التنظيمي الذي سيتولى إعداد استراتيجية وطنية لأمن الأنظمة المعلوماتية، تجسدت هذه الاستراتيجية في شكل خطة حكومية شاملة شاركت فيها مختلف الجهات الفعالة ذات العلاقة بالأمن السيبراني، تهدف الاستراتيجية إلى تعزيز السيادة الرقمية وحماية الأنظمة المعلوماتية والبنية التحتية الهامة من الجرائم السيبرانية، من خلال إرساء أنظمة قانونية واضحة لردع هذه الجرائم وأطر مؤسسية تركز على تضافر جهود جهات عديدة ومتباينة قادرة على الصمود في مواجهة كل أشكال الهجمات السيبرانية التي تتطور باستمرار وتتعد أكثر فأكثر.

تندرج هذه الاستراتيجية في إطار تعزيز الإطار المؤسسي الوطني الموجه للتصدي للجرائم السيبرانية وتعزيز قدرته على الوقاية منها، تركز المنظومة الوطنية للأمن السيبراني على هئتين هما:

-المجلس الوطني لأمن الأنظمة المعلوماتية: يعتبر الأداة المحورية في المنظومة الوطنية للأمن السيبراني والهيئة العليا في الدولة في مجال توفير الأمن السيبراني. يتأسس المجلس وزير الدفاع الوطني أو ممثله، يضم ممثلا لرئيس الجمهورية إلى جانب عدد من الوزراء الممثلين للوزارات الحساسة والهامة في الدولة وذات الصلة

³⁵ مرسوم رئاسي رقم 05-20 مؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر عدد 04، صادر في 26 جانفي 2020.

بالأمن السيبراني هم: الوزير المكلف بالشؤون الخارجية، الوزير المكلف بالداخلية، الوزير المكلف بالمالية، وزير العدل، الوزير المكلف بالاتصالات، وزير التعليم العالي والوزير المكلف بالطاقة. يتولى المجلس إعداد استراتيجية أمن الأنظمة المعلوماتية والموافقة عليها وتوجيهها³⁶، في إطار ذلك يضطلع بالعديد من المهام تتمثل أهمها فيما يلي:

-الفصل في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية التي تقترحها الوكالة.

-إبداء الآراء في مشاريع النصوص القانونية ذات الصلة بأمن الأنظمة المعلوماتية.

-دراسة التقارير المتعلقة بالاستراتيجية والموافقة عليها.

-الموافقة على اتفاقيات التعاون المتبادل مع الهيئات الأجنبية في مجال الأمن السيبراني.

لضمان أداء المجلس لمهامه هذه يمكنه الاستعانة بأي شخص أو مؤسسة من شأنها أن تساعد وتتيه في أداء مهامه³⁷.

-وكالة أمن الأنظمة المعلوماتية: تعتبر الوكالة الأداة التنفيذية للاستراتيجية، وهي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، يدير الوكالة لجنة التوجيه ويسيرها مدير عام، كما تم تزويدها بلجنة علمية ومركز وطني عملياتي لأمن الأنظمة المعلوماتية وعدد من المديريات والمصالح الإدارية والتقنية³⁸.

تضطلع الوكالة بمهام عديدة في إطار ضمان الأمن السيبراني والتصدي للجرائم السيبرانية تتمثل أساسا في: تحضير عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، ثم تنفيذها بعد اعتمادها من المجلس، إجراء تحقيقات رقمية في حالة الهجمات والحوادث السيبرانية التي تستهدف المؤسسات الوطنية، السهر على جمع وتحليل المعطيات لتوفير المعلومات الملائمة لتأمين منشآت المؤسسات الوطنية، ضمان اليقظة التكنولوجية في مجال أمن الأنظمة، مراقبة المؤسسات في معالجة آثار الهجمات السيبرانية، اقتراح مشاريع للتعاون مع هيئات أجنبية لتعزيز التعاون في مجال توفير أمن الأنظمة المعلوماتية للتصدي لكل أشكال الهجمات السيبرانية، تنظيم التظاهرات العلمية والتقنية للتحسيس بخطورة الهجمات السيبرانية وتعزيز آليات التصدي لها، في هذا الإطار

³⁶ انظر المادة 3 من المرسوم الرئاسي رقم 20-05، مرجع سابق .

³⁷ للمزيد من التوضيح حول طريق عمل هذا المجلس راجع: حزام فتحة "حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية -قراءة في أحكام المرسوم الرئاسي 20-05"، مجلة الحقوق والعلوم الإنسانية، العدد 3، 2020، ص 182.

³⁸ انظر المادة 20 من المرسوم الرئاسي رقم 20-05، مرجع سابق .

نشير إلى الورشة التي نظمتها الوكالة في الفترة الممتدة من 28 إلى 30 أبريل 2024 والموسومة "الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية" للتعريف من خلالها بالإستراتيجية والتأكيد على الأهمية القصوى التي توليها الدولة لتوفير أمن أنظمة المعلومات. تم في إطارها مناقشة العديد من المحاور الكبرى ذات الصلة بالاستراتيجية لاسيما: آليات توفير الحماية للبنى التحتية الحساسة، قدرة الاستجابة للهجمات السيبرانية، تعزيز القدرات أكثر في مجال التكوين والبحث لمواكبة المستجدات في مجال الأمن السيبراني³⁹ نشير في هذا الإطار إلى أنه تم إنشاء المدرسة الوطنية العليا للأمن السيبراني في سنة 2024 من أجل ضمان تكوين إطارات متخصصة ذات كفاءات عالية في مجال الأمن السيبراني، يتم إعداد برامج التكوين فيها للحصول على شهادة المهندس والدكتوراه في الأمن السيبراني بالتنسيق بين وزارة التعليم العالي ووكالة أمن الأنظمة المعلوماتية⁴⁰.

رغم حداثة هذه الهيئات مقارنة بنظيراتها في الدول الأخرى، إلا أنها أثبتت فعاليتها وزودت الدولة الجزائرية بمؤسسات قادرة على حماية سيادتها الرقمية وضمان الأمن السيبراني في أنظمتها المعلوماتية.

الفرع الثاني: القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

نظرا لخطورة وتشعب الجرائم السيبرانية وتعدد آثارها وتأثيرها العابر للحدود، مما يتطلب وسائل بشرية وفنية وقدرات وكفاءات علمية وتكنولوجيا عجزت الأقسام الجزائية ومحاكم الجنايات على توفيرها، على الرغم من استحداث في الجزائر ستة أقطاب جزائية متخصصة للفصل في مجموعة من الجرائم الخطيرة، إلا أن الجرائم السيبرانية لم تكن ضمن اختصاصاتها، لذلك استحدث المشرع الجزائري هيئة متخصصة وليس استثنائية على مستوى مجلس قضاء الجزائر العاصمة أطلق عليه القطب الجزائري الوطني خاص بمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب الأمر 11-21 المعدل والمتمم لقانون الإجراءات الجزائية⁴¹، الملغى بموجب القانون رقم 14-25 المتضمن قانون الإجراءات الجزائية⁴²، الذي احتفظ بهذا القطب ونظمه من خلال المواد من 338 إلى 342 و التي تكاد تكون مجرد نقل للمواد 211 إلى 211 مكرر 29 من النص السابق.

³⁹ للمزيد من التوضيح حول هذه الورشة اطلع على موقع وزارة الدفاع الوطنية : www.mdn.dz.

⁴⁰ مرسوم رئاسي رقم 181-24 مؤرخ في 5 جوان 2024، يتضمن إنشاء مدرسة وطنية عليا في الأمن السيبراني، ج ر عدد 39، صادر في 8 جوان 2024.

⁴¹ أمر رقم 11-21 مؤرخ في 25 أوت 2021، يتم الأمر رقم 66-155 المؤرخ في 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية، ج ر عدد 65، صادر في 26 أوت 2021 (ملغى).

⁴² قانون رقم 14-25 مؤرخ في 3 أوت 2025، يتضمن قانون الإجراءات الجزائية، ج ر عدد 54، صادر في 13 أوت 2025.

من شأن هذا القطب الجزائي الخاص أن يضمن قضاء متخصصا يملك المعرفة القانونية والفنية والمهارات في التحقيق والتحري وأدوات التحليل الجنائي الضرورية لمواجهة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال بكل أشكالها وأنواعها⁴³، وأن يكون الدرع القضائي للوقاية منها وحماية الأفراد وخصوصياتهم وممتلكاتهم وحماية المصالح العليا الأمنية والسياسية والاقتصادية والاجتماعية للدولة.

يتمتع هذا القطب الجزائي باختصاص إقليمي وطني يمتد لكل جريمة مرتبطة بأي مكان من الإقليم البري أو الجوي أو البحري الوطني، وباختصاص نوعي حصري يتمثل في المتابعة والتحقيق والفصل في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكذا مجموعة من الجرائم المرتبطة بها، إن هذه الجرائم في الأصل أفعال مجرمة بموجب نصوص أخرى وتخضع لاختصاص قضائي متباين من جريمة إلى أخرى، لكنها متى ارتبطت بجريمة متصلة بتكنولوجيا الإعلام والاتصال نقل اختصاص البحث والتحري والحكم فيها لهذا الطلب الجزائي الخاص، تتمثل هذه الجرائم في: الجرائم الماسة بأمن الدولة وبال دفاع الوطني، جريمة نشر وترويج أخبار كاذبة بين الجمهور من شأنها أن تزعزع الأمن والسكينة العامة، وكذا تلك الجرائم ذات الطابع المنظم والعابر للحدود والتي من شأنها أن تشكل مساسا بالأمن والنظام العام العمومي، الجرائم الماسة بأنظمة المعلومات الخاصة بالهيئات العمومية، جرائم التمييز وخطاب الكراهية إلى جانب جرائم الاتجار بالبشر والأعضاء البشرية وتلك المتعلقة بتهريب المهاجرين⁴⁴، إلى جانب الجرائم التكنولوجية الأكثر تعقيدا أي الجرائم المعلوماتية العابرة للحدود وتلك التي تتطلب استعمال وسائل وخبرة متخصصة أو تستدعي اللجوء إلى التعاون الدولي للتصدي لها.

عند التدقيق في مضمون المواد المحددة لاختصاصات القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا المعلومات والاتصال وعلاقته بالجرائم السيبرانية ينتهي بنا الأمر إلى إبداء الملاحظات التالية:

- على غرار النصوص التي تجرم بعض الأفعال المشكلة جرائم سيبرانية السابق الإشارة إليها لم يستعمل المشرع في إطار هذا النص الإجرائي الجديد مصطلح الجرائم السيبرانية بل اعتمد مصطلح الجرائم المتصلة بتكنولوجيا المعلومات والاتصال، التي خصها من خلال نص المادة 335 منه بتعريف موسع كما يلي "أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية

⁴³ سوماتي شريفة، "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص"، مجلة الدراسات القانونية، المجلد 08، العدد 02، 2022، جامعة لمدينة، ص 487.

⁴⁴ انظر المادة 337 من القانون رقم 25-04، مرجع سابق.

ذات الصلة بتكنولوجيا الإعلام والاتصال"، سمح اعتماد هذا التعريف الموسع للجرائم المتصلة بتكنولوجيا الإعلام والاتصال أن يشمل التجريم كل من الجرائم الالكترونية والسيبرانية لأنه دمج المعيارين المعتمدين في القوانين المقارنة في تحديد الجرائم السيبرانية وهما وسيلة ارتكاب الجريمة وهي نظم المعلوماتية ومعيار موضوع الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات⁴⁵.

-أصاب المشرع في اختيار تسمية الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال لتحديد الاختصاص النوعي الأصلي لهذا القطب الجزائي الخاص، عوضا من الاستناد إلى مفاهيم ضيقة كالجرائم الالكترونية، لكونها الأكثر اعتمادا في القوانين المقارنة ولأن هذه التسمية احتوت كل أنواع الجرائم الجديدة المستحدثة التي تتخذ من وسائل الإعلام والاتصال بيئة لارتكابها أو لقيام أحد أركانها⁴⁶، مما يجعل الجرائم السيبرانية مهما كان الفعل المجسد لها تتدرج ضمن الاختصاص النوعي لهذا القطب الجزائي.

- كما يشكل منح هذا القطب الاختصاص في النظر والبحث والتحري في الجرائم المرتبطة بأنظمة الإعلام والاتصال تكريس صريح لاختصاصه الحصري⁴⁷ في الهجمات السيبرانية التي قد تستهدف الأنظمة المعلوماتية للمؤسسات والمنشآت العمومية أو بأمن الدولة والدفاع الوطني.

-لكن عندما يتزامن اختصاص هذا القطب الجزائي مع اختصاص القطب الجزائي الوطني الاقتصادي والمالي أو مع اختصاص القطب الجزائي الوطني لمكافحة الإرهاب والجريمة المنظمة عبر الوطنية ينزع الاختصاص من القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ويؤول إلى إحدى هذه الأقطاب بحسب الحالة⁴⁸.

⁴⁵ انظر: المومني نهلا عبد القادر، مرجع سابق، ص 100 وما يليها.

⁴⁶ POINSOT Laurent, Introduction à la sécurité informatique, Thèse de doctorat en droit, Université Paris 13, pp. 25-26.

⁴⁷ سوماتي شريفة، مرجع سابق، ص 494.

⁴⁸ انظر المادتين 341، 342 من القانون رقم 14-25، مرجع سابق.

خاتمة

أدركت السلطات الجزائرية حجم التهديدات التي تفرضها التكنولوجيا الحديثة على أمن الأفراد والمؤسسات الحيوية للدولة لذلك أظهرت إرادة سياسية قوية كلها عزم على مواكبة التغيرات والمستجدات الدولية والوطنية في مجال التصدي للجرائم السيبرانية، وتحسين الأنظمة المعلوماتية من هذا الشكل الجديد للإجرام، في إطار رفض كل أشكال المساس بالسيادة الرقمية باعتبارها جزء لا يتجزأ من السيادة الوطنية.

حاولت التصدي لهذا الشكل الجديد من الجرائم العابرة للحدود بشكل يتوافق مع احترام سيادتها الرقمية، فاستطاعت أن تضع أسسا قوية لبناء منظومة قانونية ومؤسسية لمواجهة الجرائم السيبرانية، تم في إطارها استحداث قسم خاص لتجريم العديد من الأفعال التي تشكل جرائم سيبرانية في قانون العقوبات والإقرار لها بعقوبات ردية، تجريم أفعال أخرى في قوانين خاصة بغرض مواكبة الوتيرة المتسارعة لتطور هذا النوع من الجرائم.

تدعيما لهذا الإطار القانوني، تم استحداث العديد من الأجهزة والهيكل الإداري لتفعيل درع الدولة الواقية من الجرائم السيبرانية ولمساعدة الهيئات القضائية في التصدي لها على غرار الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ومن أجل خلق التكامل وسد الثغرات في المنظومة الوطنية الخاصة بالأمن السيبراني تم اعتماد في سنة 2020 الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، انبثقت عنها استحداث هيئتين أكثر تخصصا في مجال توفير الأمن السيبراني والتصدي لكل الجرائم المرتبطة به هما: المجلس الوطني لأمن الأنظمة المعلوماتية ووكالة أمن الأنظمة المعلوماتية.

حققت بذلك الجزائر إنجازات هامة في إرساء منظومة قانونية ومؤسسية لمكافحة الجريمة السيبرانية، رغم حداثة النسبية. لكن الوتيرة التقنية التي تتطور بها هذه الجرائم يفرض تحديات مستمرة عليها تستوجب تطوير أكثر آليات الاستباق والتحقيق والتعاون الدولي بما يضمن ليس فقط التصدي للجرائم السيبرانية ولكن الوقاية منها أيضا، غير أن تحقيق ذلك يستدعي مواصلة الجهود أكثر لذلك يتعين:

-الإسراع في إصدار القانون الخاص بالأمن السيبراني، حتى يضمن توفير إطار قانوني متكامل يدمج بين الردع الجنائي حماية البيانات والأنظمة المعلوماتية ويواكب تطور الجرائم السيبرانية.
-تعزيز التكامل والتنسيق بين الهيئات والمؤسسات المتدخلة في مجال ضمان وتوفير الأمن السيبراني.

- تطوير البنية التحتية الوطنية للإنذار المبكر بشكل يسمح للأجهزة المتخصصة برصد أي هجوم سيبراني والتعامل معه في الوقت المناسب.
- تدعيم التكوين أكثر في مجال الأمن السيبراني بتوفير كل الإمكانيات المادية والبشرية الضرورية لذلك والاستفادة من تجارب الدول الرائدة في المجال.
- تعزيز التعاون القانوني والقضائي الدولي لتسهيل تتبع المجرمين خارج الحدود الوطنية.