

الإرهاب الإلكتروني وآليات مواجهته في التشريع الجزائري
Cyber terrorism and mechanisms to combat it in Algerian legislation

محمد الصالح روان²
mohamedsalah.rouane@univ-oeb.dz

قارة إيمان¹
I.kara@univ-skikda.dz

تاريخ النشر: 2026/03/15
Received: 28/09/2025

تاريخ الاستلام: 2025/09/28
published: 15/03/2026

ملخص المقال :

يعتبر الإرهاب الإلكتروني تطوراً تقنياً للفعل الإرهابي في ظل العولمة الثقافية وتواجه الدول حالياً تحديات كبيرة في مواجهتها ومكافحتها، نظراً للأساليب التكنولوجية التي يستخدمها من ناحية وتنوع أشكالها وتعددتها من ناحية أخرى، مما يجعل هذه الجرائم تمثل تهديداً خطيراً للأمن الفرد والمجتمع، لذلك فإن المشرع الجزائري يحتاج إلى كثير من العمل لتطوير قدراته للتعامل مع جرائم الكمبيوتر والوقاية منها، فضلاً عن تعديل نصوصها القانونية، واستحداث أخرى تتماشى مع التطور السريع فيها، بما يتماشى مع طبيعة هذه الجريمة العابرة للحدود الوطنية، مما يزيد من خطر اختراقها وتخريبها للأنظمة الحساسة في الدولة كالأجهزة العسكرية والاقتصادية والسياسية.

كلمات مفتاحية: الجرائم الإلكترونية، الحرب الإلكترونية، الإرهاب، التجسس، الاختراق، برمجيات الإعلام، التهديد، الأمن السيبراني.

Abstract:

Terrorist crime is a technical development of the terrorist act in the context of cultural globalization. It is currently facing great challenges in confronting and combating it because of the technical methods it uses on the one hand, and its various forms on the other, making these crimes a serious threat to the security of the individual and society. The Algerian state needs a lot of work to develop its capabilities to deal with computer crimes and prevent them, as well as to amend their legal texts in line with the nature of this transnational crime, which increases the risk of penetration and sabotage of sensitive systems in the country such as military systems Economic and political etc...

Keywords: Electronic, Crimes, Digital War, Terrorism Security, threat, Information Security.

(1) جامعة سكيكدة 20 أوت 1955 (الجزائر)

(2) جامعة أم البواقي العربي بن مهيدي (الجزائر)

مقدمة:

إن التطور التكنولوجي الهائل والثورة المعلوماتية التي جلبتها حضارة التقنية أدت إلى بروز مصطلح الارهاب الالكتروني أو الارهاب الالكتروني وزيادة خطورة الجرائم الارهابية وتعقيدها، سواء من حيث تسهيل الاتصال بين الجماعات الارهابية وتنسيق عملياتها أو من حيث ابتكار أساليب وطرق إجرامية جد متطورة، وهذا الأمر الذي دعا ثلاثين دولة إلى التوقيع على أول اتفاقية دولية لمكافحة الاجرام المعلوماتي في العاصمة المغربية بودابست عام 2004م، ومما لاشك فيه أن الجزائر من الدول التي تعاني من مخاطر وتهديدات هذا النوع الجديد من الإرهاب الذي يشكل خرقا واصحا للأمن القومي أو الداخلي وانتهاكا صارخا للسيادة الوطنية للدولة الجزائرية بصفة خاصة ولأي دولة أخرى بصفة عامة.

إشكالية الدراسة: ومن خلال هذه الدراسة سنحاول الإجابة على الاشكالية التالية: ما مدى فاعلية الآليات التي كرسها المشرع الجزائري لمواجهة جرائم الإرهاب الالكتروني؟ هذه الفاعلية سواء في جودة النص القانوني من حيث وصف أو تكييف الأفعال الجرمية الإرهابية ذات الطبيعة الالكترونية أو من حيث الآليات التي نص عليها في مكافحتها؟ وما مدى مواكبتها للعصرنة في مجال التطور الرهيب للالكتروني، وكذا مدى اتساعها لتحقيق التعاون الأمني والقضائي الإقليمي والدولي؟

أهداف الدراسة:

تهدف الدراسة إلى معرفة جهود الدولة الجزائرية التي بذلتها لمواجهة المخاطر والأضرار الناجمة عن جرائم الإرهاب الالكتروني ومعرفة السياسات والتوجهات القانونية والمؤسسية التي كرسها المشرع الجزائري للتصدي لجرائم الارهاب الالكتروني باعتباره يهدد الأمن الداخلي للدولة والمجتمع، وينخر الأنظمة الحساسة في الدولة سواء كانت عسكرية أو اقتصادية أو سياسية أو مالية...إلخ.

أهمية الدراسة:

يكتسي هذا الموضوع أهمية بالغة، نظرا للتحويلات الجذرية التي عرفها العالم على إثر التطور التكنولوجي الرهيب لاستخدامات وسائط الاعلام و الاتصال في جميع الميادين و المجالات، حيث أصبح العالم قرية صغيرة مما يطرح إشكالية تلاشي الحدود الجغرافية المادية بين الدول، وبرزت هذه الثورة التكنولوجية الالكترونية ظهرت معها العديد من الإشكالات والسلبيات التي تهدد أمن الدول ومن أخطرها هو الحروب الالكترونية أو الارهاب الالكتروني الذي يجد من العالم الافتراضي أو الفضاء السيبراني أرضية خصبة لجرائمه التي تهدد استقرار وسلامة الأنظمة الداخلية للدولة، وفي هاته الدراسة سنعالج الآليات والميكانيزمات التي اعتمدتها الدولة الجزائرية عامة والمشرع الجزائري خاصة لمكافحة المخاطر والأضرار المترتبة عن الإرهاب الالكتروني الشبكي.

فرضية البحث:

تقوم الدراسة على فرضية جهود الدولة الجزائرية لمواجهة المخاطر والأضرار المترتبة عن الإرهاب الالكتروني، وتقييمها والوقوف على قوتها الحمائية من جهة، واستدراك ما يجب تعديله أو استحداثه من جهة أخرى، كل ذلك من أجل الارتقاء بالحماية للأمن والاستقرار السياسي والاقتصادي والمالي والمؤسسي عموما وحماية الأفراد من الاثار المدمرة التي من الممكن تنعكس على قناعاتهم الوطنية والعقائدية وسلوكاتهم الاجتماعية، إذ المستهدف بهذا الإرهاب الالكتروني اثنان الدولة ومؤسساتها ثم الفرد والمجتمع في أفكاره ومعتقداته وانماطه العرفية السلوكية.

خطة الدراسة:

المحور الأول: الآليات النصية لمواجهة جرائم الإرهاب الإلكتروني الشبكي
المحور الثاني: الآليات المؤسسية المكلفة بمواجهة جرائم الإرهاب الإلكتروني الشبكي
الخاتمة والتوصيات.

المحور الأول: الآليات النصية لمواجهة جرائم الإرهاب الإلكتروني

تعتبر الاتفاقيات الدولية للجرائم المعلوماتية مرجعية للقانون الجزائري ومن أهم مصادره، خاصة فيما يتعلق بتحديد المصطلحات التقنية وحسب القانونيين والمختصين والتشريع الجزائري من أحدث التشريعات وأكثرها انسجاما مع المعايير الدولية التي انضمت كل من الولايات المتحدة كندا، اليابان، جنوب إفريقيا، وتمت تكملة الاتفاقية بالبروتوكول الإضافي المتعلق بتجريم الأفعال ذات الطابع المعادي للأجانب والعنصري المرتكبة عن طريق الأنظمة المعلوماتية 2003/09/28م بستراسبورغ، كما تم إعداد مشروع بروتوكول يتعلق بتجريم الرسائل الإرهابية وفك ترميزها (قصعة خديجة، دت، 252)، حيث واجهت الجزائر خطر التهديدات الأمنية الناجمة عن الإرهاب الإلكتروني ووجدت نفسها أمام حتمية التصدي له وذلك بإحداث تغييرات جذرية في المنظومة القانونية والمؤسسية الهيكلية التي تلائم طبيعة هذه المخاطر، وتضع حدا لفتكها بأمن واستقرار الدولة الجزائرية وهذا ما تطرقنا إلى معالجته من خلال هذا المحور من الدراسة.

أولا: المعالجة الجزائية التقليدية للإرهاب في التشريع العقابي الجزائري:

تتصدر المادة 87 مكرر النصوص التشريعية الخاصة بجريمة الإرهاب التقليدي ويمتد أثرها إلى الإرهاب الإلكتروني بما أنها جاءت شاملة وفضفاضة كما ذكرنا أعلاه مختلف الأفعال التخريبية والتهريبية التي تعتبرها إجرامية وماسة بسلامة الأمن الوطني، جاءت المادة 87 مكرر 1 من أجل تبيان العقوبات الواردة والمقررة بموجب قانون العقوبات على الأشخاص المرتكبين لهاته الجريمة كمرجعية عقابية والتي جاء نصها كالاتي: "تكون العقوبات التي يتعرض لها مرتكب الأفعال المذكورة في المادة 87 مكرر أعلاه، كما يأتي:"

أ-الإعدام عندما تكون العقوبة المنصوص عليها في القانون السجن المؤبد،

ب-السجن المؤبد عندما تكون العقوبة المنصوص عليها في القانون السجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة،

ج-السجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة، عندما تكون العقوبة المنصوص عليها في القانون،

ح-السجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات" ()

كما حاول المشرع الجزائري على غرار بقية التشريعات الوطنية معالجة هذه الظاهرة وتنظيمها بموجب قوانين منها ما هو يتعلق بجانب الاتصالات كالقانون رقم 04-09 المؤرخ في 05 أوت 2009م المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كما سيأتي بيانه.

ثانيا: مراقبة الاتصالات الالكترونية

يمكن الخروج على قاعدة سرية الاتصالات والمراسلات وانتهاك الخصوصية الالكترونية حسب مقتضيات النظام العام أو مستلزمات التحريات أو التحقيقات القضائية، وذلك بوضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية وذلك في الحالات التالية:

الحالة الأولى: يمكن القيام بعمليات المراقبة الالكترونية للوقاية من الأفعال الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة؛
الحالة الثانية: توفر معلومات عن اعتداء أو هجوم على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني؛

الحالة الثالثة: من مقتضيات التحريات والتحقيقات القضائية عند ما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية؛

الحالة الرابعة: في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة (المادة 04 من القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، المؤرخ في 16 أوت 2009).

ثالثا: إباحة تفتيش المنظومة المعلوماتية

يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية وكذا ضباط الشرطة القضائية في إطار قانون الاجراءات الجزائية وفي الحالات المبينة في المادة 04 الدخول بغرض التفتيش لو عن بعد إلى:

منظومة معلوماتية او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها (المادة 06 من القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها) وفي حال اكتشاف السلطة التي تبشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها أو نسخ المعطيات محل البحث وذلك للسهر على سلامة المنظومة المعلوماتية والاستعانة بالوسائل التقنية الضرورية.

رابعا: حجز المعطيات المعلوماتية

عندما تكتشف السلطة التي تبشر عملية التفتيش في منظومة معلوماتية معطيات مخزنة، تكون مهمة في الكشف عن الجرائم أو مرتكبيها فليس من الضروري حجز كل المنظومة، فيتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعائم تخزين إلكترونية تكون قابلة للحجز والوضع في أحرارز وفقا للقواعد المقررة في قانون الإجراءات الجزائية، ويجوز للسلطة التي تقوم بعملية الحجز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق (المادة 06 من القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

الجريدة الرسمية عدد 47، المؤرخ في 16 أوت 2009)، فلا يجوز استعمال المعلومات المتحصل عليها بواسطة عمليات المراقبة المنصوص عليها في القانون رقم 04-09 إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية. (المادة 09 من القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، المؤرخ في 16 أوت 2009).

خامسا: حصر الممارسات الغير المشروعة المضرة بالأنظمة المعلوماتية بموجب الأمر رقم 15/04 المتضمن قانون العقوبات جرم المشرع الجزائري في القسم السابع مكرر من قانون العقوبات الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، تم إدراج هذا القسم بموجب 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات ليواجه المشرع الجزائري الجرائم الحديثة المتصلة بتكنولوجيا الإعلام والاتصال، وهي محددة بموجب المواد 394 مكرر إلى 394 مكرر 3 وهي تعاقب على الاختراقات غير المصرح بها داخل نظم المعالجة الآلية للمعطيات (أحمد مسعود مريم، ص 35)، ومنه ما جاء في نص المادة 394 مكرر: (الدخول خلسة للأنظمة المعلوماتية، البقاء غير المشروع في الأنظمة المعلوماتية، تعديل أو حذف معطيات منظومة نتيجة الدخول غير المشروع، الإضرار بنظام التشغيل المنظومة على إثر الدخول أو البقاء غير المشروع)؛

1- الجرائم المنصوص عليها في المادة 394 مكرر 1: (إدخال المعطيات في منظومة معلوماتية خلسة بإزالة أو تعطيل معطيات في منظومة معلوماتية خلسة)؛

من خلال النص أعلاه حصر المشرع الجنائي أهم الممارسات الجرمية الوارد حدوثها في البيئة الالكترونية والتي تتمحور حول الولوج والبقاء غير المشروع في منظومة معلوماتية ولم يبين طبيعة أو نوع هاته المنظومة، كما اعتبر عملية إدخال معطيات في منظومة معلوماتية أو رقمية بقصد الإضرار بها وإتلافها (خلسة) أو خفية كسرقة بيانات رسمية أو حكومية أو حتى شخصية واستعمالها قصد الإضرار بتلك الجهة أي لسبب غير مشروع ودون مبرر قانوني، ولكن ما يعاب على المشرع الجنائي أنه استعمل مصطلحات عامة لا تتوافق ولا تتواءم مع التطور السريع والرهيب لاستخدامات وتقنيات الأجهزة الإلكترونية وتطبيقاتها أو أرضياتها ومواقعها اللامتناهية كما ونوعا، حتى إضفاء وصف التجريم على الممارسات اللاأخلاقية في البيئة والمنظومة المعلوماتية جاء خجولا (كالبقاء غير المشروع، الدخول، خلسة، تعطيل المعطيات)، كما أنه استعمل مصطلحات غامضة وضبابية دون حصر دقيق وشامل لهاته الأفعال الجرمية والتي يلزم من خلالها أنها تجسد الركن المادي للجريمة السيبرانية أو المعلوماتية والالكترونية.

2- الجرائم المنصوص عليها في المادة 394 مكرر 2: (القيام عمدا وخلسة بتصميم أو بحث أو تجميع أو توفير أو نشر معطيات تمكن من ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعلومات)؛ أدرج المشرع الجنائي في هذا النص الركن المعنوي أو القصد الجنائي من

خلال استخدامه لمصطلح (القيام عمدا...)، أي النية السيئة والمبينة للمجرم المعلوماتي من وراء ولوجه لقاعدة بيانات أو أرضية مواقع معلومات إلكترونية تابعة لجهة معينة إما خاصة أو عامة، كما أتبع ركن القصدية العمدية في الفاعل بوجود توفر صفة أو خاصية التخفي فيه أي قيامه بأعمال التصميم أو البحث أو التجميع أو التوفير أو النشر لمعطيات معينة دون إظهار هويته الحقيقية وهاته الأعمال من شأنها أن تمكنه من سرقة أو اختراق محتويات أو إفشاء معطيات المنظومة أو التجسس على أسرار مهنية أو أمنية تخص جهاز حساس من أجهزة الدولة أو مؤسسة استراتيجية تخص قطاع معين، ولما لهذه الأفعال من خطورة التي من شأنها أن تتسبب في خسائر وأضرار جسيمة.

3- الجرائم المنصوص عليها في المادة 394 مكرر3: (ارتكاب الجرائم سالفه الذكر للإضرار بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام)، (القانون رقم 15/04 المؤرخ في 27 رمضان 1425 هـ الموافق ل 10 نوفمبر 2004م المعدل و المتمم لقانون العقوبات رقم 156/66 في 18 صفر 1386 هـ الموافق ل 8 يوليو 1966م، جريدة رسمية، عدد 71 سنة 2004م)، قرن المشرع هنا الأفعال التي أضفى عليها وصف الجريمة في إطار المساس بأنظمة المعالجة الآلية للمعلومات والتي تخص أو تضر بأجهزة أو مؤسسات الدولة بقوله: (... خاضعة للقانون العام)، وهذا ما نلتزمه من خلال تعديل قانون الإجراءات الجزائية بموجب القانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الذي تدارك فيه المشرع الجنائي الجزائري ما كان ينقصه في التشريعات السابقة، كما يلاحظ من خلاله أنه أولى أهمية خاصة بالجرائم المتعلقة بالحياة الخاصة للأشخاص الطبيعية أكثر من الأشخاص المعنوية في إطار المعالجة الآلية للمعطيات الشخصية وخصص لها عقوبات بدنية ومالية إلا أنه لم يركز على الجرائم الإلكترونية والمعلوماتية التي من شأنها أن تفتك بالسيادة والأمن الوطني ضد اعتداءات أو هجمات خارجية ذات نطاق دولي، خاصة في إطار ما يدعى "بالحروب الإلكترونية أو الإلكترونية".

سادسا: الحاجة الملحة إلى إصدار قانون خاص بالأمن السيبراني

بناء على معطيات واقع الحال وما هو حاصل في عالم التكنولوجيا وما أفرزته البيئة الإلكترونية من تحديات مستجدة توجب على الدول بما فيها الدولة الجزائرية والسلطات التشريعية والقضائية المختصة التعامل بجدية صارمة وكفيلة لاستيعاب هاته الممارسات الإجرامية والتجاوزات الخطيرة ذات الطابع المعلوماتي وذات النطاق العالمي الغير محدود، من أجل التصدي للهجمات الإلكترونية السيبرانية مجهولة المصدر والتي يصعب فيها إثبات أو اكتشاف المجرم أو الفاعل الأصلي إلا بعد مرور وقت طويل، كما أن جهود ومحاولات المشرع الجنائي الجزائري انصبت حول حماية المعطيات الشخصية لأفراد دون الدول، ولم يتم التنصيص على الفعل الإرهابي والترهيب باستخدام وسائل التكنولوجيا الإلكترونية على وجه الحصر، كما لم تتضمن هاته التشريعات والأحكام القانونية التوصيف القانوني الجنائي للجرائم الإلكترونية المصحوبة بالممارسات الإرهابية والترهيبية للأفراد والدول، والتي من شأنها زعزعة الأمن القومي

وبث الرعب بقصف وتدمير قواعد البيانات الخاصة بالمؤسسات الحكومية من بنوك ووزارات الدفاع الوطني، فكانت مجرد إشارات فقط دون تخصيص أو تفصيل وعناية كافية بالإرهاب الإلكتروني ووسائله وآليات مكافحته وكيفية التصدي له من طرف خبراء تقنيين أو من قبل خبراء في مجال القانون، وما يمكننا التوصل إليه من أجل الحد من هاته الجريمة التي تتجاوز الحدود الجغرافية للدول وتعتبر القارات في بضع ثوان، هو تعزيز التعاون الدول والإقليمي في هذا الصدد وذلك بتوقيع أشد العقوبات على مرتكبي الجريمة الإرهابية الإلكترونية، كآلية واستراتيجية عقابية ردعية، كما يمكن للمشروع الجنائي الجزائري الاقتداء بالمنطق والمنهج العقابي الأجنبي في هذا الصدد في كل من التشريعات الأمريكية والأوروبية.

المحور الثاني: الآليات المؤسسية المكلفة بمواجهة جرائم الارهاب الالكتروني

توجهت الجزائر في إطار مكافحة ما يسمى بالإرهاب الإلكتروني الشبكي والتهديدات الأمنية الناجمة عنه إلى تفعيل النصوص الجزائية بما يتماشى مع خطورة الارهاب الالكتروني محاولة منها لوضع حد لهذه الظاهرة المتفشية بصورة رهيبية في الآونة الأخيرة، وذلك بتحديد الممارسات الغير المشروعة التي تضر بالأنظمة المعلوماتية وذلك بموجب الأمر رقم 15/04 المتضمن قانون العقوبات وهذا ما خصصناه بالدراسة في الفرع الأول من هذا المطلب، وأما الفرع الثاني من هذا المطلب خصصناه لدراسة الأقطاب الجزائية المتخصصة ودورها في مكافحة جريمة الارهاب الالكتروني خاصة بعد التعديلات الأخيرة التي قام بها المشروع الجزائري.

أولاً: انشاء الأقطاب الجزائية المتخصصة:

في إطار التعديلات الجديدة التي أتى بها المشروع الجزائري فيما يخص مكافحة جرائم المعلوماتية في الجانب التشريعي، عمد إلى إنشاء الأقطاب الجزائية متخصصة وهي جهات قضائية جهوية (الجزائر، العاصمة، وهران، ورقلة، قسنطينة) عُهد إليها اجراءات ذات خصوصية للتفرغ لمواجهة قضايا الاجرام المعاصر ذو التعقيد الكبير، بموجب المرسوم التنفيذي 348/06 المؤرخ في 05 أكتوبر 2006م، وذلك في جرائم تبييض الأموال، جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم الإرهاب، الجرائم المتعلقة بالصرف، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (رابح وهيبة، 2014م، ص 323).

وتم استحداث المحاكم الجنائية ذات الاختصاص الموسع التي أجاز لها تمديد اختصاصها للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المواد (37-40-329) من خلال قانون الاجراءات الجزائية المعدل بموجب قانون 14/04 المؤرخ في 10-2004م تناول موضوع الجرائم الافتراضية من خلال تمديد الاختصاص الإقليمي لضباط الشرطة القضائية بمعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كامل الإقليم الوطني المادة 16.

وتختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال المرتكبة خارج الاقليم الوطني في حالة ما إذا كان مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني (المادة 15 من القانون رقم المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

وعندما يتعلق الامر بالوقاية من الأفعال الموصوفة بجرائم الارهاب أو التخريب أو الجرائم الماسة بأمن الدولة يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته إذنا لمدة ستة أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات الفنية المستعملة والأغراض الموجهة إليها (المادة 04 من المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

ثانيا: تأسيس الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال:

الهيئة هي سلطة ادارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي، توضع لدى الوزير المكلف بالعدل ويقع مقرها في الجزائر العاصمة (المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 53، ص 16)، و تحدد الصلاحيات المخولة للهيئة الوطنية المكلفة بمكافحة جرائم تكنولوجيا الاعلام والاتصال بموجب القانون رقم 04-09 المتعلق ب و كذا المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث تتولى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته بتنشيط عمليات الرقابة من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال، و مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الاعلام والاتصال، كما تسعى إلى تبادل المعلومات مع نظيراتها في الخارج لجمع المعلومات عن مرتكبي الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وتحديد أماكن تواجدهم (المادة 04 من القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها).

تجتمع الهيئة بناء على استدعاء من رئيسها أو بناء على طلب أحد أعضائها إذ تقوم بإعداد نظامها الداخلي والمصادقة عليه حيث يتم تزويدها بقضاة وضباط وأعوان الشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني يتم تحديد عددهم بموجب قرارات مشتركة بين وزير العدل والدفاع والداخلية كما تزود بمستخدمي الدعم التقني والإداري ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني كما يمكن الاستعانة بأي خبير أو أي شخص يمكن تعيينه بشرط الالتزام بالسر المهني (آمال بن صوالح، يومي 11-12 أفريل 2017م، ص 7).

ثالثا: تأسيس السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

تأسست السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بموجب القانون رقم 18-06 المعدل والمتمم للأمر 66-155 المؤرخ سنة 1966 والمتضمن قانون الإجراءات الجزائية، وحسب المادة 22 منه هي تنشأ لدى رئيس الجمهورية كسلطة إدارية مستقلة لحماية المعطيات

ذات الطابع الشخصي ويحدد مقرها بالجزائر العاصمة، وتتمتع بالشخصية المعنوية والاستقلال المالي والإداري، كما تتمثل تشكيلة السلطة الوطنية حسب نص المادة 23 من ذات القانون من ثلاث شخصيات يختارهم رئيس الجمهورية من ذوي الاختصاص في مجال عملها، وثلاث قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة، وعضو عن كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة، بعد التشاور مع رؤساء المجموعات البرلمانية، بالإضافة إلى ممثلين عن الوزارات الحساسة بما فيها وزارة الدفاع ووزارة العدل ووزارة البريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة، ويعين رئيس وأعضاء السلطة الوطنية بموجب مرسوم تنفيذي لعهدته تقدر بمدة 5 سنوات قابلة للتجديد، ومن أهم اختصاصاتها ومهامها ما يلي:

1- السهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون، وضمان عدم استعمال تكنولوجيات الإعلام والاتصال بشكل يهدد حقوق الأشخاص والحريات العامة والخاصة

2- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي

3- إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم...، وفي إطار ممارسة مهامها تعلم السلطة الوطنية النائب العام المختص فورا في حالة معاينة وقائع تحتمل الوصف الجزائي، كما تقوم بإعداد تقرير سنوي حول نشاطها ورفعها لرئيس الجمهورية (القانون رقم 18-06 المعدل والمتمم للأمر 66-155 المؤرخ سنة 1966 والمتضمن قانون الإجراءات الجزائية).

رابعا: إنشاء مصلحة الدفاع عن السيرياني ومراقبة الأنظمة المعلوماتية الالكترونية

اكتفى المشرع الجزائري بذكر مصطلح "الأمن السيرياني" بشكل مقتضب ضمن القانون رقم 04-18 المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، حيث نصّت المادة 10، الفقرة 3 منه على أن: "الأمن السيرياني هو مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية، وطرق تسيير المخاطر، والأعمال، والتكوين، والممارسات الجيدة، والضمانات، والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية من أي حدث قد يمس بتوفر وسلامة وسرية البيانات المخزنة أو المعالجة أو المرسلة".

ورغم أن هذا التعريف يُبرز الإطار العام للأمن السيرياني، إلا أن معالجته ضمن قانون الاتصالات الإلكترونية تبقى غير كافية، في ظل التهديدات المتزايدة والمتطورة التي يشهدها الفضاء السيرياني، والتي قد تمسّ بأمن الدولة واستقرارها.

لذلك، يُعد من الضروري إصدار تشريع خاص ومستقل يُنظم الأمن السيرياني بصورة شاملة، يضبط المفاهيم والآليات والتدابير التقنية والقانونية المعتمدة، ويُحدد بوضوح مجالات التطبيق والجهات المختصة، بما يُسهم في تعزيز الأمن الداخلي، وحماية السيادة الوطنية في البيئة الالكترونية. (القانون رقم 18-04 لسنة 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المؤرخ في 13 مايو 2018، الجريدة الرسمية عدد 27).

تم إنشاء مصلحة الدفاع عن الأمن السيبراني لتتولى مهمة مراقبة الأنظمة المعلوماتية الالكترونية، وضمان حمايتها من مختلف التهديدات التي قد تمس أمن الدولة وسلامتها الالكترونية. وتُعد هذه المصلحة عنصراً محورياً في التصدي للمخاطر السيبرانية التي تستهدف الأمن الوطني وتهدد سيادة الجزائر في الفضاء الالكتروني.

وتُعنى هذه الهيئة بتطوير منظومة دفاعية متكاملة وفعّالة، تشمل حماية وتأمين البنى التحتية الالكترونية والمنشآت الحيوية الحساسة، والتصدي للهجمات الإلكترونية والإرهاب الالكتروني، إضافة إلى إحباط محاولات التجسس أو اختراق أسرار الدولة، بما يعزز من سيادة الجزائر في المجال السيبراني ويصون أمنها الاستراتيجي. (الشروق أونلاين، 2019).

تقوم استراتيجية الدفاع السيبراني للجيش الوطني الشعبي على سبعة محاور رئيسية، تهدف إلى بناء منظومة متكاملة قادرة على حماية الفضاء السيبراني الوطني، وضمان أمن المعلومات واستمرارية أداء البنى التحتية الحيوية:

1. المحور التنظيمي والوظيفي:

يُعنى هذا المحور بوضع إطار تنظيمي فعال يضمن تنسيق الجهود بين مختلف الهيئات والوحدات المعنية بالدفاع السيبراني داخل الجيش، مع اعتماد آليات قيادة وتحكم واضحة، تتيح التدخل السريع والفعال في مواجهة التهديدات السيبرانية.

2. المحور القانوني

يُركز على تطوير الأطر القانونية المتعلقة باستخدام تكنولوجيا الإعلام والاتصال، من خلال تحديث القوانين والتشريعات بصفة مستمرة، بما يتماشى مع المستجدات الالكترونية، ويكفل الحماية القانونية لأنظمة المعلومات الوطنية.

3. محور الموارد البشرية:

4. يُعد العنصر البشري المؤهل ركيزة أساسية في نجاح الدفاع السيبراني، لذا تسعى الاستراتيجية إلى تأهيل الكوادر عبر برامج تكوين متخصصة، وتدريبات مكثفة، بهدف إعداد نخبة ذات كفاءة عالية قادرة على التعامل مع مختلف التحديات السيبرانية.

5. المحور التقني والتكنولوجي:

يرتكز هذا المحور على توفير التجهيزات والمنظومات الالكترونية الحديثة، وتطوير البنية التحتية المعلوماتية، إضافة إلى توطيد التكنولوجيا، بما يعزز من القدرة على صد الهجمات الإلكترونية وضمان الأمن المعلوماتي.

6. محور الرصد واليقظة:

يُعنى بإنشاء منظومات متقدمة للرصد والمراقبة الدائمة للفضاء السيبراني، من خلال مراكز متخصصة تعمل على التحليل المستمر للتهديدات، وتوفير الإنذار المبكر والاستجابة الفورية لأي خرق أو هجوم محتمل.

7. محور التعاون والشراكة:

تدعم الاستراتيجية مبدأ التعاون مع الفاعلين المحليين والدوليين في مجال الأمن السيبراني، بهدف تبادل الخبرات والمعلومات، وتعزيز الجاهزية المشتركة لمواجهة التهديدات العابرة للحدود.

8. محور البحث والتطوير:

يُركّز على دعم الابتكار والبحث العلمي في مجالات التكنولوجيا السيبرانية، من خلال تشجيع المشاريع الوطنية، وتطوير حلول أمنية محلية تضمن استقلالية القرار السيبراني وتعزز من السيادة الالكترونية للدولة. (يوسف بوغرة، 2024، ص 115). وبلغت الأرقام تجهض وزارة الدفاع الوطني يوميا 3500 محاولة اختراق لمواقع قيادات قواتها ومديرياتها المركزية بمعدل 130 ألف محاولة اختراق في السنة من قبل عصابات الماركرز من مختلف دول العالم في إطار ما يعرف بالحرب الالكترونية (الشروق اونلاين، مرجع سابق).

خاتمة:

من خلال ما سبق ذكره في هذه الدراسة توصلنا إلى جملة من النتائج والتوصيات فيما يلي:
- رغم جهود المشرع الجزائري لسد الفراغ التشريعي لمواجهة هذه الجرائم إلا أنه لا تزال ناقصة خاصة فيما يتعلق بالاعتداءات على الأموال المعلوماتية.
- عدم قدرة نصوص التجريم التقليدية على مسايرة تطور الجريمة الالكترونية الالكترونية ففي كل فترة وأخرى تظهر تقنيات جديدة للقرصنة والتحايل والاختراق بشكل يصعب مجاراته من طرف السلطة التشريعية.

التوصيات والاقتراحات:

السعي إلى وضع قانون للأنترنت في أحد جوانبه ينص على جرائم الأنترنت بشقيها، فأما الشق الموضوعي فهو يجرم الأفعال غير المشروعة على الأنترنت ومعاينة مرتكبيها، والشق الإجرائي يوضح إجراءات تفتيش الحاسب وضبط المعلومات التي يحتويها ومراقبة المعلومات أثناء انتقالها والساح للجهات القائمة على التفتيش بضبط برامج الحاسوب والمعلومات الموجودة بالبرامج وفقا للشروط الخاصة بإجراءات التفتيش العادية؛ فرض الرقابة الكافية من قبل الحكومة عن كل ما يقدم من خلال الشبكة لمنع الدخول على بعض المواقع التي تبث الفكر الارهابي والتدميري؛ توحيد الجهود بين الجهات المختلفة للدولة، التشريعية والقضائية والضبطية والفنية من أجل سد منافذ جريمة الارهاب الالكتروني والعمل على ضبطها وثباتها بالطرق القانونية؛ تفعيل التعاون الدولي في المجال الالكتروني والسيبراني لمواجهة جرائم وأضرار الإرهاب الالكتروني الشبكي والالكتروني من خلال الاتفاقيات الدولية وتطوير قدرة الشركات والمنظمات والحكومات على التصدي للتهديدات الأمنية المترتبة عنه وتوفير التقنيات اللازمة لتوجيهها.

المصادر والمراجع:

أولا: النصوص التشريعية

1. الأمر رقم 66-156 المتضمن قانون العقوبات المعدل والمتمم، المؤرخ في 11 جوان 1966، الجريدة الرسمية عدد 49.
2. القانون رقم 18-04 لسنة 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، المؤرخ في 13 مايو 2018، الجريدة الرسمية عدد 27.
3. القانون رقم 15/04 المؤرخ في 27 رمضان 1425 هـ الموافق ل 10 نوفمبر 2004م المعدل و المتمم لقانون العقوبات رقم 66/156 في 18 صفر 1386 هـ الموافق ل 8 يوليو 1966م، جريدة رسمية، عدد 71 سنة 2004م.

4. القانون رقم 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، المؤرخ في 16 أوت 2009.
5. القانون رقم 18-06 المؤرخ في 10 يونيو 2018، المعدل والمتمم للأمر 66-155 المؤرخ في 08 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 34.
6. المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 53.

ثانيا: المراجع

1. آمال بن صوالح، (11-12 أبريل 2017) الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خطوة هامة نحو مكافحة الإرهاب الإلكتروني بالجزائر، مداخلة بالملتقى الدولي حول: الاجرام السيبراني المفاهيم والتحديات، بجامعة قلمة 1945م، الجزائر.
2. رابح وهيب، (2014)، الجريمة المعلوماتية في التشريع الاجرائي الجزائري، مجلة الباحث للدراسات الاكاديمية، عدد 04، جامعة عبد الحميد ابن باديس، مستغانم.
3. الشروق أونلاين، (2019/01/25) الجيش يدخل حرب الفضاء الالكتروني ومكافحة الجوسسة، المقال منشور على الرابط التالي: <https://www.echoroukonline.com/>
4. قصعة خديجة، جمال بن مرزوق، تفعيل آليات الحماية القانونية للحد من انتشار الجريمة الإلكترونية في العالم والجزائر، مجلة تاريخ العلوم، عدد 06.
5. يوسف بوغراة، (2024) الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع الوطني، مجلة الشرطة، المديرية العامة للأمن الوطني، عدد 158.

Les références:

Premièrement : Textes législatifs

1. Ordonnance n° 66-156, contenant le Code pénal modifié et complété, du 11 juin 1966, Journal officiel n° 49.
2. Loi n° 18-04 de 2018 fixant les règles générales relatives à la poste et aux communications électroniques, du 13 mai 2018, Journal officiel n° 27.
3. Loi n° 04/15 du 27 Ramadan 1425 AH correspondant au 10 novembre 2004, modifiant et complétant le Code pénal n° 66/156 du 18 Safar 1386 AH correspondant au 8 juillet 1966, Journal officiel, n° 71 de 2004.
4. Loi n° 04-09 relative aux règles particulières de prévention et de répression des infractions liées aux technologies de l'information et de la communication, Journal officiel n° 47 du 16 août 2009.
5. Loi n° 18-06 du 10 juin 2018, modifiant et complétant l'ordonnance 66-155 du 8 juin 1966, qui comprend le Code de procédure pénale, Journal officiel n° 34.
6. Décret présidentiel n° 15-261 du 8 octobre 2015, fixant la composition, l'organisation et les modalités de fonctionnement de l'Autorité nationale de prévention et de lutte contre les délits liés aux technologies de l'information et de la communication, Journal officiel de la République algérienne, n° 53.



Deuxièmement: Références

1. Ahmed Masoud Maryam, Mécanismes de lutte contre les délits liés aux technologies de l'information et de la communication à la lumière de la loi n° 09/04, référence précédente.
2. Amal Ben Sawalha(11-12 avril 2017), L'Autorité nationale de prévention des délits liés aux technologies de l'information et de la communication est une étape importante dans la lutte contre le cyberterrorisme en Algérie, intervention au Forum international sur: la cybercriminalité, concepts et défis, Université de Guelma 1945, Algérie.
3. Rabah Ouahba(décembre 2014), La cybercriminalité dans la législation procédurale algérienne, Revue du chercheur pour les études académiques, numéro 04, Université Abdelhamid Ibn Badis, Mostaganem.
4. Echourouk Online(25/01/2019), L'armée entre dans la guerre électronique et le contre-espionnage, date de navigation :, l'article est publié sur le lien suivant : <https://www.echoroukonline.com/> .
5. Kassaa Khadidja, Jamal Ben Marzouk, Activation des mécanismes de protection juridique pour réduire la propagation de la cybercriminalité dans le monde et en Algérie, Journal d'histoire des sciences, numéro 06.
6. Youssef Bougrara, Cybersécurité(2024), Stratégie algérienne de sécurité et de défense nationale, Revue de la police, Direction générale de la sécurité nationale, n° 158,.
Traduit avec <https://laratranslate.com/translate?lng=fr>