

التجربة الجزائرية لتحقيق الأمن السيبراني

The Algerian Experience in Achieving Cybersecurity

تاريخ القبول: 20../..

تاريخ الإرسال: 20../..



<i>Nesrine Mechta</i>	نسرين مشته	<i>Wiam Baghiani</i>	وثام بغياني*
مختبر آفاق الحوكمة للتنمية المحلية المستدامة المركز الجامعي بـبركة-	مختبر آفاق الحوكمة للتنمية المحلية المستدامة المركز الجامعي بـبركة-	مختبر آفاق الحوكمة للتنمية المحلية المستدامة المركز الجامعي بـبركة-	مختبر آفاق الحوكمة للتنمية المحلية المستدامة المركز الجامعي بـبركة-
University Center of Barika	University Center of Barika	University Center of Barika	University Center of Barika
nesrine.mecheta@cu-barika.dz	nesrine.mecheta@cu-barika.dz	wiam.baghiani@cu-barika.dz	wiam.baghiani@cu-barika.dz

والاستجابة للحوادث السيبرانية، بهدف تأمين
البنى التحتية الحيوية.
كما ركزت الجزائر على تطوير المنظومات التقنية
لحماية المواقع الحكومية والخدمات الإلكترونية، واعتماد
حلول متقدمة للكشف المبكر عن الهجمات.
ولم تغفل الدولة جانب التوعية، حيث تم إطلاق
برامج تعليمية وتكوينية لتعزيز الثقافة الرقمية داخل
المؤسسات والمجتمع.
وتبرز هذه الجهود مجتمعة التزام الجزائر ببناء فضاء
رقمي آمن ومتطور قادر على مواجهة التحديات
المتنامية في المجال السيبراني.
الكلمات المفتاحية: الأمن السيبراني، الجزائر، التحول
الرقمي، الأمن القانوني.

Abstract:

The Algerian experience in the field of cybersecurity has become one of the most developed in recent years, as the state has adopted a

ملخص:
تعد التجربة الجزائرية في مجال الأمن السيبراني
من التجارب المتطورة في السنوات الأخيرة، إذ
اعتمدت الدولة مقاربة شاملة تقوم على تعزيز الإطار
القانوني والتنظيمي، وإنشاء مؤسسات مختصة،
وتطوير القدرات التقنية والبشرية.
فعلى المستوى القانوني، تم إصدار تشريعات
تتعلق بمكافحة الجرائم الإلكترونية وحماية المعطيات
الشخصية وتنظيم أنظمة الإعلام والاتصال، مما وفر
أساساً قانونياً لمواجهة التهديدات الرقمية.
أما على الصعيد المؤسسي، فقد تم إنشاء
وحدات متخصصة على مستوى الدرك الوطني
والأمن الوطني، إضافة إلى مراكز اليقظة

comprehensive approach based on strengthening the legal and regulatory framework, establishing specialized institutions, and

*- وثام بغياني

developing technical and human capacities.

At the legal level, several legislations have been enacted concerning the fight against cybercrime, the protection of personal data, and the regulation of information and communication systems, thereby providing a solid legal basis for addressing digital threats.

At the institutional level, specialized units have been created within the National Gendarmerie and the National Police, in addition to cybersecurity monitoring and incident response centers aimed at securing critical infrastructures.

Algeria has also focused on developing technical systems to

protect government websites and electronic services, while adopting advanced solutions for early detection of cyberattacks.

The state has not neglected the awareness aspect, launching educational and training programs to strengthen digital culture within institutions and society.

Together, these efforts reflect Algeria's commitment to building a secure and advanced digital environment capable of facing the growing challenges in the cybersecurity domain.

Keywords: Cybersecurity, Algeria, Digital transformation, Legal security .

مقدمة:

في عصر الثورة الرقمية، أصبح الفضاء السيبراني جزءاً لا يتجزأ من حياتنا اليومية، حيث تعتمد الدول والمؤسسات على نظم معلوماتية متقدمة لتسيير شؤونها الاقتصادية والاجتماعية والسياسية؛ ومع هذا الاعتماد المتزايد، برزت تهديدات جديدة من نوعها، مثل الجرائم الإلكترونية، والهجمات السيبرانية على البنى التحتية الحيوية، وانتهاك الخصوصية، مما جعل الأمن السيبراني أحد الأولويات الاستراتيجية للدول الحديثة.

وتأتي التجربة الجزائرية في مجال الأمن السيبراني في هذا السياق كجهد وطني متكامل يسعى إلى حماية الفضاء الرقمي الوطني وضمان استمرارية الخدمات الحيوية وحماية المعلومات الحساسة؛ حيث اعتمدت الجزائر مقاربة شاملة تشمل تعزيز الإطار القانوني والتنظيمي، من خلال سن تشريعات متطورة لمكافحة الجرائم الإلكترونية وحماية المعطيات الشخصية وتنظيم أنظمة الإعلام والاتصال؛ كما أولت الدولة أهمية بالغة لإنشاء مؤسسات وهيئات مختصة، مثل وحدات الأمن السيبراني في الدرك الوطني والأمن الوطني، إضافة إلى مراكز البقطة والاستجابة للحوادث السيبرانية، لضمان رصد ومواجهة التهديدات بشكل فعال.

ولا تقتصر التجربة الجزائرية على الجانب القانوني والمؤسسي فقط، بل تمتد لتشمل البعد التقني والتكويني، حيث تم تطوير أنظمة حماية متقدمة للمواقع الحكومية والخدمات الإلكترونية، واعتماد حلول ذكية للكشف المبكر عن الهجمات، مع التركيز على تكوين الكفاءات البشرية المتخصصة وتعزيز الوعي الرقمي لدى المواطنين والمؤسسات.

التجربة الجزائرية لتحقيق الأمن السيبراني د.وئام بغياني – د.مشتة نسرين

وتتجلى أهمية هذه المداخلة في أن الأمن السيبراني أصبح عاملا أساسيا لضمان استقرار الدولة الرقمية، وحماية المعلومات الحساسة، وتعزيز الثقة في التحول الرقمي، بما يسهم في التنمية الاقتصادية والاجتماعية المستدامة.

كما تهدف المداخلة إلى دراسة وتحليل التجربة الجزائرية في الأمن السيبراني، مع التركيز على مكوناتها الأساسية، وتقييم مدى فعاليتها.

وبناء على ما سبق نطرح الإشكالية التالية:

ما مدى نجاعة القوانين الجزائرية لتحقيق الأمن السيبراني في ظل ثورة التحول الرقمي؟

للإجابة عن هذه الإشكالية ستعتمد هذه المداخلة على منهجية وصفية تحليلية، حيث يتم أولا تقديم الإطار القانوني والمؤسسي، ثم استعراض الآليات العملية والتدابير التقنية لتحقيق الأمن السيبراني في الجزائر .

وتنقسم هذه المداخلة إلى محورين أساسيين كالتالي:

المحور الأول: الإطار القانوني للأمن السيبراني في الجزائر

أولا: الإطار التشريعي للأمن السيبراني في الجزائر

ثانيا: الإطار المؤسسي لتحقيق الأمن السيبراني في الجزائر

المحور الثاني: الآليات العملية والتدابير التقنية لتحقيق الأمن السيبراني في الجزائر

أولا: آليات الوقاية والحماية السيبرانية

ثانيا: آليات الكشف والاستجابة للهجمات السيبرانية

المحور الأول: الإطار القانوني للأمن السيبراني في الجزائر

مع التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصالات، أصبحت الدول تواجه تحديات متعددة تتمثل في حماية المعلومات الحساسة، ومكافحة الجرائم الإلكترونية، وضمان أمن البنى التحتية الرقمية؛ ومن هذا المنطلق، برزت الحاجة إلى وضع إطار قانوني متكامل ينظم الأنشطة الرقمية ويحدد المسؤوليات القانونية، بما يضمن الأمن السيبراني على المستوى الوطني.

في الجزائر، عملت الدولة على تطوير منظومة تشريعية تهدف إلى تنظيم الأمن السيبراني عبر سن قوانين ومراسم تنظم حماية البيانات الشخصية، ومكافحة الجرائم الإلكترونية، وضبط استخدام شبكات المعلومات والاتصالات؛ كما أسهم الإطار القانوني في تحديد صلاحيات المؤسسات الوطنية المكلفة بحماية الفضاء السيبراني، وتوفير آليات قانونية للتصدي للهجمات السيبرانية، مما يعزز من استقرار البيئة الرقمية ويضمن استمرارية الخدمات الحيوية.

التجربة الجزائرية لتحقيق الأمن السيبراني د. وئام بغياني – د. مشنتة نسرين

وتتميز الجريمة السيبرانية عن الجرائم الأخرى في الوسيلة التي تستعمل في ارتكابها، والتي تتميز في كون مرتكبها يكون على إطلاع ولو بقدر أدنى على الجوانب التقنية والتكنولوجية لعمل الوسائل المستعملة لارتكاب هذه الجريمة، إضافة إلى وجوب توافر الأركان العامة للجريمة المنصوص عليها في قانون العقوبات.¹ كما تتميز الجريمة السيبرانية بأنها جريمة يستخدم فيها الحاسب الآلي وكذا شبكة الإنترنت، وهذا ما يجعلها جريمة صعبة من حيث الإثبات لكون الدليل يمكن التخلص منه بسرعة من طرف الجاني، وبأنه يتطلب خبرة تقنية لإثباتها، لكونها متعلقة بالمعطيات إضافة إلى أنه في أغلب الحالات، فإن الجريمة المرتكبة تكون عبارة عن أرقام وشفرات، ثم إنها جريمة عابرة للحدود وتناحها واسعة النطاق.²

وسنحاول من خلال هذا الجزء من الدراسة تسليط الضوء على الإطار القانوني الجزائري الذي يهدف لتحقيق الأمن السيبراني في ظل التحول الرقمي، وذلك باستعراض الإطار التشريعي والمؤسسي الذي يعمل على تحقيقه.

أولا: الإطار التشريعي للأمن السيبراني في الجزائر

يشكل الإطار التشريعي للأمن السيبراني العمود الفقري لحماية الفضاء الرقمي في أي دولة؛ وفي الجزائر، تم إصدار مجموعة من القوانين التي تهدف إلى مكافحة الجرائم الإلكترونية، وحماية البيانات الشخصية، وتنظيم استخدام شبكات المعلومات والاتصالات؛ ويتيح هذا الإطار القانوني تأسيس قاعدة صلبة لضمان استقرار المنظومة الرقمية الوطنية، وتحديد المسؤوليات، وتوفير آليات قانونية لمواجهة التهديدات السيبرانية الحديثة؛ وفيما يلي استعراض لمجموعة القوانين التي تهدف إلى تحقيق الأمن السيبراني في الدولة الجزائرية:

1- القوانين المتعلقة بالجرائم الإلكترونية:

وهي مجموعة القوانين والتعديلات التي تهدف إلى مكافحة الاعتداءات المعلوماتية وحماية الأنظمة والشبكات الرقمية؛ ومن أهم هذه القوانين مايلي:

أ- **قانون رقم 05-18 المؤرخ في 10 ماي سنة 2018، المتعلق بالتجارة الإلكترونية³**: وهو الإطار التشريعي الذي وضعته الجزائر لتنظيم كل المعاملات التجارية التي تتم عبر الإنترنت، سواء بين التجار أو بين التاجر والمستهلك؛ ويهدف هذا القانون إلى ضبط ممارسة التجارة الإلكترونية من خلال تحديد شروط ممارسة النشاط، وتنظيم العقود الإلكترونية، وفرض التزامات على المتعاملين الإلكترونيين لضمان الشفافية، إضافة إلى حماية المستهلك من الاحتيال والممارسات المنافية للمنافسة.

كما ينظم القانون وسائل الدفع الإلكتروني، ويمنع بيع السلع المحظورة عبر الإنترنت، ويحدد آليات الرقابة والعقوبات، مما يجعل منه أداة أساسية لترسيخ الثقة في المعاملات الإلكترونية وتشجيع الاقتصاد الرقمي في الجزائر.

التجربة الجزائرية لتحقيق الأمن السيبراني د.وئام بغياني – د.مشتة نسرين

ب- القانون رقم 15-04 المعدل والمتمم للأمر 156-66 المتضمن قانون العقوبات⁴: أدخل قسم خاص في قانون العقوبات الجزائري بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات" من المادة 394 مكرر إلى 394 مكرر 7.

ت- قانون رقم 23-06 مؤرخ في 20 ديسمبر سنة 2006 المعدل و المتمم للأمر رقم 156-66 المتضمن قانون العقوبات⁵: عدل قانون العقوبات بحيث أدخل مزيدا من العقوبات على الاعتداءات على الحياة الخاصة عبر الوسائل الرقمية، كما أنه يعترف بمسؤولية الأشخاص المعنويين (مثل الشركات) في الجرائم المعلوماتية.

2- القوانين المتعلقة بحماية المعطيات الشخصية:

وهي القوانين المتعلقة بحماية المعطيات الشخصية في الجزائر؛ وتهدف إلى تنظيم، جمع، معالجة، تخزين، ونقل البيانات الشخصية للأفراد، وذلك من أجل ضمان احترام الخصوصية ومنع إساءة استخدام هذه المعلومات. يمثل مضمونها خاصة في القانون رقم 07-18 مؤرخ في 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي⁶؛ حيث يهدف هذا الأخير إلى حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة بياناتهم الشخصية، من خلال تنظيم جمع، تخزين، استخدام ونقل هذه المعطيات بطريقة قانونية وشفافة، وضمان حقوق الأفراد في الوصول إلى بياناتهم وتصحيحها ومسحها عند الحاجة. كما يلزم الجهات المعنية باتخاذ التدابير الأمنية اللازمة لحماية البيانات من التسريب أو الاستخدام غير المشروع، ويخول للهيئة الوطنية المختصة مراقبة تطبيق القانون وفرض العقوبات على المخالفين.

3- القوانين المتعلقة بأنظمة الإعلام والاتصال:

تتعلق هذه القوانين بتنظيم استخدام وسائل الإعلام التقليدية والرقمية، وضمان تنظيم قطاع الاتصالات وحماية المستخدمين والمعلومات؛ ومن أهمها القانون رقم 04-09 المؤرخ في 05 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها⁷؛ حيث يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، من خلال تنظيم إجراءات التحري والتحقيق في الجرائم المعلوماتية، وتمكين السلطات المختصة من مراقبة الاتصالات الإلكترونية والتفتيش التقني للأنظمة المعلوماتية بإذن قضائي، مع إلزام مزودي خدمات الإنترنت والاتصالات بحفظ بيانات الاتصالات لمدة معينة والتعاون مع الجهات القضائية عند الطلب.

كما ينص القانون على إزالة المحتوى غير القانوني وحماية سرية المعلومات المرتبطة بالتحقيق، إضافة إلى إنشاء هيئة وطنية تعنى بالتنسيق بين مختلف الهيئات في مجال الوقاية من الجريمة الإلكترونية وتبادل المعلومات على الصعيدين الوطني والدولي.

ويحدد كذلك قواعد التعاون الدولي في تبادل الأدلة الرقمية، ويمنح القضاء الجزائري اختصاص متابعة الجرائم المعلوماتية حتى لو ارتكبت من خارج البلاد إذا استهدفت مصالح وطنية، مع فرض عقوبات على الأفراد ومزودي الخدمات عند مخالفة أحكامه.

ثانيا: الإطار المؤسسي لتحقيق الأمن السيبراني في الجزائر

التجربة الجزائرية لتحقيق الأمن السيبراني د.وئام بغياني - د.مشتة نسرين

يشكل الإطار المؤسسي حجر الأساس لتنفيذ السياسات والاستراتيجيات الوطنية للأمن السيبراني في الجزائر؛ وقد أنشأت الدولة عدة هيئات ومؤسسات متخصصة، مثل وحدات الأمن السيبراني في الدرك الوطني والأمن الوطني، ومراكز اليقظة والاستجابة للحوادث السيبرانية (CERT)، بهدف حماية البنى التحتية الحيوية، ورصد التهديدات الرقمية، وضمان استمرارية الخدمات الإلكترونية. ويمكن الهدف من هذا الإطار في توظيف الموارد البشرية والتقنية بشكل منسق لتعزيز الأمن السيبراني الوطني ومواجهة التحديات الرقمية الحديثة.

1- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:

قد أنشئ في سنة 2008، ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، وهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رابح، هذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لا سيما تلك المستعملة في المؤسسات الرسمية والبنوك والبيوت؛ كما يهدف إلى مساعدة باقي الأجهزة الأمنية الأخرى في أداء مهامها.⁸ واستطاعت قيادة الدرك الوطني من خلال التكوين المستمر والمتميز لأفرادها والمفتقيات الدولية والوطنية وتبادل الخبرات مع دول أخرى أن توفر القوى المؤهلة وذات الكفاءة من مهندسي الإعلام الآلي، ورجال القانون، وهذا من أجل الفهم الصحيح للجريمة المعلوماتية والتصدي لها.⁹

2- المصلحة المركزية لمكافحة الجرائم السيبرانية:

أولت القيادة العليا للأمن الوطني أهمية في محاربة ظاهرة الجرائم التي تمس الفضاء الإلكتروني، وجندت إمكانياتها المادية والبشرية في التصدي لمرتكبيها، واستجابت لضرورة الأمن المعلوماتي من خلال إنشاء خلية لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني لسنة 2011، ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بمديرية الشرطة القضائية سنة 2015، تحول فيما بعد إلى مصلحة عملياتية مجهزة بالموارد البشري المتخصص والوسائل التقنية العالية المستوى، لمواجهة التحديات المتزايدة في مجال الجريمة المعلوماتية؛ وتضم الهيكلية الحالية للمصلحة هيكلية متخصصة ومكتب للدعم والتسهيل والتحليل؛ وذلك من أجل أداء مهامها بكل احترافية واستباقية، ومن أجل إمالة اللثام عن أصعب الجرائم السيبرانية؛ كما تضم هذه المصلحة نخبة من الكفاءات الشرطية البحتة، تخرجت من الجامعات الجزائرية، وتلقت تكوينا مكثفا وطنيا ودوليا، حتى يتسنى لهم أداء مهامهم بكل احترافية ومهنية.¹⁰

3- الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال:

أنشئت بموجب المادة 13 من القانون رقم 04-09 المؤرخ في 05 أوت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ وتتولى هذه الهيئة، خصوصا المهام الآتية:

أ- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته،

التجربة الجزائرية لتحقيق الأمن السيبراني د.وئام بغياني - د.مشتة نسرين

- ب- مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجرّها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية،
- ت- تبادل المعلومات قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

ويلاحظ أن المشرع خص الهيئة بالتحري في الجرائم التي تمس أمن الدولة عموماً كالجرائم الإرهابية والتجسس والخيانة العظمى باستعمال وسائط إلكترونية بمعنى كل جريمة متعلقة بالأمن الوطني ومقومات الدولة الجزائرية، غير أنه ونظراً لخطورة هذه الجرائم أعطاه المشرع استمالة أساليب تحري خاصة من بينها تسجيل المعطيات الشخصية في حالة الشك بوجود جريمة إرهابية أو لها علاقة بأمن الدولة، غير أن الإشكال الذي يطرح هو احتمال أن يكون المشتبه فيه بريء، وبالتالي في حالة الحكم بالإدانة فلا مشكلة، غير أنه بعد كل التحريات والإجراءات يحكم القاضي بالبراءة، وهنا تطرح مسألة الحق في حرمة الحياة الخاصة.¹¹

المحور الثاني: الآليات العملية والتدابير التقنية لتحقيق الأمن السيبراني في الجزائر

يمكن اعتبار أن الأمن السيبراني من أولويات الدولة الجزائرية حالياً، خاصة بعدما تبنت خيار الحكومة الإلكترونية من خلال التحول الرقمي التدريجي للعديد من الخدمات العمومية لقطاعات كثيرة (وزارة الداخلية، العدل، التعليم العالي والتربية...); هذا التوجه صاحبه سيبراني سياسات تعني بإدارة المخاطر السيبرانية والمعروفة بحوكمة الأمن السيبراني والتي تشير إلى الأساليب المستخدمة من قبل العديد من أصحاب القرار (حكومات ومؤسسات) لتحديد وتأطير وتنسيق الأمن السيبراني، فلا يمكن تصور تحول رقمي للخدمات العمومية في ظل غياب استراتيجية واضحة وشفافة لضمان الأمن السيبراني.¹²

فبعد ما تم عرض الإطار القانوني والمؤسسي لتحقيق الأمن السيبراني في الجزائر، سنحاول من خلال هذه الجزئية، التطرق للآليات الوقائية من مخاطر التعدي على الأمن السيبراني في الجزائر.

أولاً: آليات الوقاية والحماية السيبرانية

أصبحت الوقاية والحماية السيبرانية اليوم من أهم متطلبات الحفاظ على أمن الدول والمؤسسات والأفراد، في ظل التزايد المستمر للهجمات الإلكترونية وتعقيد أساليب الاختراق؛ وتمثل هذه الآليات مجموعة من الإجراءات التقنية والتنظيمية الرامية إلى حماية الأنظمة الرقمية، وتأمين المعطيات، وضمان استمرارية الخدمات الحيوية؛ ولا تقتصر الحماية على الأدوات التقنية فقط، بل تشمل أيضاً بناء وعي سيبراني، وتطوير سياسات واضحة، وتعزيز قدرة الهياكل على توقع المخاطر قبل وقوعها والحد من آثارها.

1- تعزيز البنى التحتية الرقمية السيادية:

يقصد بتعزيز البنية التحتية السيادية تطوير وبناء أنظمة رقمية وتقنية تكون الدولة هي المتحكم الرئيسي فيها دون الاعتماد على أطراف أجنبية، وذلك لحماية أمنها المعلوماتي وضمان استقلالها الرقمي؛ ويتحقق ذلك عبر:

التجربة الجزائرية لتحقيق الأمن السيبراني د.وئام بغياني – د.مشتة نسرين

أ- إنشاء مراكز بيانات وطنية لتخزين البيانات داخل الدولة: بدل الاعتماد على خوادم خارجية، مما يقلل المخاطر ويحفظ السيادة على المعلومات.

ب- تطوير الشبكات الحكومية الآمنة: عن طريق بناء شبكات اتصال خاصة ومشفرة تستعملها المؤسسات الحساسة لضمان سرية البيانات.

ت- الاعتماد على حلول وبرمجيات وطنية: وذلك بتشجيع تطوير أنظمة تشغيل وبرمجيات محلية أو مفتوحة المصدر بدل الاعتماد على منتجات أجنبية قد تحمل مخاطر تجسسية.

ث- تعزيز القدرة على إنتاج المعدات التقنية: مثل بطاقات التعريف البيومترية، أنظمة المراقبة، وأجهزة التشفير داخل الدولة أو عبر شراكات آمنة.

ج- حماية البنى التحتية الحيوية: مثل الطاقة، الاتصالات، النقل، والقطاع المالي عبر آليات مراقبة دائمة ونظم دفاع سيبراني متقدمة.

وقد قام يوم الأحد 16 مارس 2025، السيد وزير البريد و المواصلات السلكية و اللاسلكية، السيد "علي زروقي"، رفقة السيد وزير اقتصاد المعرفة والمؤسسات الناشئة والمؤسسات الصغيرة، "نور الدين واضح"، زيارة عمل إلى ولاية وهران حيث أجريت جولة ميدانية شملت عدة مشاريع استراتيجية في قطاع الاتصالات والتكنولوجيا؛ من بينها وضع حجر الأساس لمركز بيانات متطور ومركز حوسبة للذكاء الاصطناعي مشروع طموح يعزز البنية التحتية التكنولوجية للجزائر، حيث سيوفر حلول الحوسبة السحابية والذكاء الاصطناعي، مع التركيز على ترشيد استهلاك الطاقة عبر تكنولوجيات مستدامة¹³.

2- اعتماد خدمات الثقة الرقمية:

استعرض وزير البريد والمواصلات السلكية واللاسلكية، سيد علي زروقي، خلال اجتماع مجلس الوزراء، المنعقد في نوفمبر 2025 التدابير الجديدة التي يتضمنها مشروع الإطار القانوني الخاص بخدمات الثقة للمعاملات الإلكترونية والتعريف الإلكتروني، والذي يهدف إلى تمكين الجزائر من مواكبة التطور التكنولوجي وتعزيز استخدام الخدمات الرقمية في بيئة آمنة وموثوقة.

ويأتي هذا النص القانوني الجديد لترسيخ بروز خدمات الثقة والتعريف الإلكتروني، بما يضمن تطوير المعاملات الرقمية ويساهم في تعزيز السيادة الرقمية للبلاد، مع معالجة العراقيل التي واجهت تطبيق القانون 04-15 الصادر في 1 فبراير 2015؛ وقد تضمن المشروع جملة من الأحكام الرئيسية أبرزها:¹⁴

أ- إنشاء السلطة الوطنية للتصديق الإلكتروني: حيث يقترح النص إطارا تنظيميا جديدا يعتمد على هيئة وطنية تتكفل بتقديم خدمات الثقة في المجال الحكومي بصفة دائمة؛ بما يسمح بتوحيد إدارة هذه الخدمات عبر القطاعات الحكومية والاقتصادية.

التجربة الجزائرية لتحقيق الأمن السيبراني د.وئام بغياني - د.مشتة نسرين

- ب- تنظيم خدمات الثقة : من خلال توسيع نطاق الخدمات التي شملها القانون السابق، لتضم التوقيع والخطم الإلكترونيين المعتمدين. وإثبات صحتها وحفظها، إضافة إلى خدمة الإرسال الإلكتروني المعتمد.
- ت- الاعتراف القانوني بالوثائق الإلكترونية : بهدف ضمان مساواة الوثيقة الإلكترونية بنظيرتها الورقية؛ وتعزيز الأمن القانوني في المعاملات الرقمية.

ث- إرساء التعريف الإلكتروني : وذلك عبر إدراج هذا المبدأ لضمان وسيلة موثوقة لإثبات هوية الأفراد والهيئات بما يتيح لهم الولوج الآمن إلى مختلف الخدمات عبر الإنترنت، وبشكل الأساس في منظومة خدمات الثقة.

- ج- تعزيز الرقابة ونظام العقوبات : من خلال تحديد آليات تدقيق ومراقبة أطراف الثقة ومقدمي الخدمات، واعتماد جهات مختصة للتدقيق الدوري؛ فضلا عن مراجعة العقوبات المالية والإدارية والجزائية المتعلقة بمخالفة أحكام خدمات الثقة.

وباعتماد هذا الإطار القانوني، تسعى الدولة إلى بناء بيئة رقمية أكثر موثوقية، وتعزيز أمن الأنظمة المعلوماتية، ودعم التحول الرقمي الوطني بخطوات عملية وفعالة.

3- التعاون الدولي لمكافحة الإجرام السيبراني:

فقد أصبحت الدولة لوحدها غير قادرة على مواجهة المخاطر السيبرانية، مبن ما أوجب على الدول التعاون فيما بينها لحصر هذا الإجرام المستحدث، والقضاء عليه نهائيا؛ سواء من ناحية التعاون الأمني الدولي، أو من ناحية المساعدة القضائية.

- أ- التعاون الأمني الدولي للحفاظ على الأمن السيبراني: فلا بد من ضرورة التعاون الأمني الدولي، حيث أنه أثبت الواقع العملي أن أي دولة لا تستطيع بمجودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة؛ لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة، وتتعاون من خلاله أجهزة الشرطة في جميع الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة.¹⁵

وهذا ما نص عليه المشرع الجزائري من خلال نص المادة 17 من القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ والتي نصت على أنه: "تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات التحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل."

التجربة الجزائرية لتحقيق الأمن السيبراني د. وئام بغياني - د. مشتة نسرين

ب- المساعد القضائية الدولية لمكافحة جرائم الأمن السيبراني: حيث أن تحديث آليات التعاون القضائي دوليا في المادة الجنائية يبدأ بخطوة أولى، غايتها ضرورة تطوير القوانين الوطنية على نحو أكثر شمولية ومرونة، حتى تواكب القوانين الوطنية حركة التشريع الدولية بشأن مكافحة الجريمة، وأن تكون حلقة وصل للتعاون بين الأجهزة التنفيذية للدول، وتنشئ أجهزة متخصصة لمواجهة الإجرام المنظم، وأنت صوغة نظرية متكاملة تستفيد من التطور التكنولوجي في إجراءات جمع الأدلة وتبادل المعلومات، وذلك من أجل التصدي للمنظمات الإجرامية التي تعمل بأسلوب علمي مدروس على تشتيت الأدلة والتخلص منها، مما يستدعي تطوير التعاون القضائي في مختلف مراحله، بما فيها مرحلة تنفيذ الأحكام.¹⁶

وهذا ما كرسه المشرع الجزائري من خلال نص المادة 16 من القانون 04-09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها؛ وذلك بنصها على أنه: " في إطار التحريات أو التحقيقات القضائية الجارية لمعينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن، في حالة الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

ثانيا: آليات الكشف والاستجابة للهجمات السيبرانية:

تعد آليات الكشف والاستجابة للهجمات السيبرانية من الركائز الأساسية لأي منظومة أمن رقمي فعالة، إذ لا يكفي تأمين الأنظمة مسبقا دون امتلاك قدرات تسمح برصد التهديدات فور وقوعها والتعامل معها بسرعة واحترافية.

وتهدف هذه الآليات إلى مراقبة شبكات المعلومات بشكل مستمر، وتحليل المؤشرات الدالة على الاختراق، ثم التدخل لاحتواء الهجوم والحد من أضراره واستعادة الأنشطة بشكل آمن؛ وبذلك تشكل حلقة حيوية في حماية البنى التحتية الرقمية وضمان استمرارية الخدمات الحساسة في مواجهة التهديدات المتزايدة. وفي السنوات الأخيرة، شهدت الجزائر زيادة ملحوظة في حالات الجريمة السيبرانية، وهذا يعود جزئيا إلى الانتشار الواسع لشبكة الإنترنت وقصص المراقبة والمتابعة الدورية لاستخدامها؛ ولكن، حرصا من المشرع الجزائري على مكافحة هذه الجريمة وحماية البيئة الرقمية، حيث قام باتخاذ خطوات جادة لتطوير الإجراءات القانونية والتقنية المناسبة لمواجهة هذا التحدي المتنامي، وتمثل هذه الخطوات في:¹⁷

✓ استحداث آليات إجرائية متقدمة تتناسب مع طبيعة الجرائم السيبرانية: والتي تتميز بتطورها المستمر وتعقيداتها المتزايدة؛

✓ تكثيف الجهود لتطوير القوانين واللوائح ذات الصلة؛

✓ التنسيق بين الهيئات الأمنية، وتعزيز التعاون الدولي في مجال مكافحة الجريمة السيبرانية؛

التجربة الجزائرية لتحقيق الأمن السيبراني د.وئام بغياني – د.مشتة نسرين

✓ تفعيل الأجهزة المكلفة برصد الهجمات والاستجابة لها، وكذلك أنظمة الإنذار المبكر والتشخيص الرقمي للجرائم ومركبيها؛

وتأتي هذه الجهود ضمن استراتيجية شاملة لتحقيق الأمن السيبراني، وتعكس التزام السلطات الجزائرية بمكافحة الجريمة السيبرانية وتعزيز أمن الدولة في العصر الرقمي المعاصر؛ وعليه، فإن الجزائر تسعى جاهدة لتطوير القدرات القانونية والتقنية اللازمة للتصدي للتهديدات السيبرانية وحماية معلوماتها وبنيتها التحتية الرقمية من أجل تحقيق التنمية الشاملة واستقرار الأمن الوطني.

خاتمة:

ختاماً، يمكن القول إن التجربة الجزائرية في مجال حماية الأمن السيبراني قد شهدت تطوراً ملحوظاً خلال السنوات الأخيرة، من خلال تحديث الإطار التشريعي، وتعزيز البنى التحتية الرقمية، واستحداث هيئات ومؤسسات متخصصة في الوقاية والكشف والاستجابة للهجمات السيبرانية. وقد مكنت هذه الجهود من بناء منظومة حماية أكثر تماسكاً، تستجيب لمتطلبات التحول الرقمي الذي يشهده البلد، وتواكب التهديدات الإلكترونية المتزايدة في المحيطين الإقليمي والدولي.

ومع ذلك، تبقى الحاجة ملحة إلى مواصلة تطوير القدرات الوطنية في هذا المجال، سواء عبر تكوين الكفاءات البشرية، أو تعزيز التعاون الدولي، أو تحديث الآليات التقنية والتنظيمية.

وإن تحقيق أمن سيبراني فعال ومستدام يتطلب رؤية شاملة تُدمج بين التشريع والتكنولوجيا والتوعية المجتمعية، بما يضمن حماية الفضاء الرقمي الوطني ويساهم في دعم التنمية الاقتصادية والاجتماعية.

وبناء على ما سبق خرجنا بمجموعة من التوصيات تمثلت أهمها في:

✓ **تعزيز الإطار القانوني:** من خلال تحديث القوانين واللوائح لتواكب التطورات التقنية المستمرة وتحديات الجرائم السيبرانية الجديدة.

✓ **تطوير القدرات البشرية:** عبر تكوين متخصصين في مجال الأمن السيبراني، وإدماج برامج التوعية الرقمية في المؤسسات التعليمية والمجتمع المدني.

✓ **تعزيز التعاون بين المؤسسات الحكومية والقطاع الخاص:** لضمان حماية البنى التحتية الحيوية وتبادل المعلومات حول التهديدات الرقمية.

✓ **اعتماد تقنيات حديثة للوقاية والكشف المبكر عن الهجمات السيبرانية:**، مثل أنظمة الذكاء الاصطناعي والتحليلات التنبؤية.

التجربة الجزائرية لتحقيق الأمن السيبراني د.وئام بغياني – د.مشتة نسرين

✓ **تعزيز الشراكات المولية:** للاستفادة من التجارب العالمية وتطوير استراتيجية وطنية متكاملة للأمن السيبراني.

من خلال هذه التوصيات، يمكن للجزائر تعزيز تجربتها الناجحة وتحقيق فضاء رقمي أكثر أماناً، قادر على مواجهة التحديات المستقبلية في مجال الأمن السيبراني.

الهوامش:

- ¹ لشطر محمد الصالح، الجريمة السيبرانية في ظل القانون الجزائري، مجلة الشرطة، المديرية العامة للأمن الوطني، العدد 158، ماي 2024، ص 22-23.
- ² المرجع نفسه، ص 23.
- ³ قانون رقم 05-18 مؤرخ في 24 شعبان عام 1439 الموافق 10 ماي سنة 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية، العدد 28، صادر بتاريخ: 30 شعبان عام 1439 الموافق 16 مايو سنة 2018، ص 04.
- ⁴ قانون رقم 15-04 مؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2024، يعدل ويتم الأمر رقم 156-66 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 71، صادرة بتاريخ 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، ص 08.
- ⁵ قانون رقم 23-06 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتم الأمر رقم 156-66 المؤرخ في 18 صفر عام 1386 الموافق 08 يونيو سنة 1966 والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، صادرة بتاريخ 4 ذو الحجة عام 1427 الموافق 24 ديسمبر سنة 2006، ص 11.
- ⁶ قانون رقم 07-18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، صادرة بتاريخ 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، ص 11.
- ⁷ قانون رقم 04-09 مؤرخ في 14 شعبان عام 1430 الموافق 05 أوت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، العدد 47، صادرة بتاريخ 25 شعبان عام 1430 هـ الموافق 16 أوت 2009، ص 05.
- ⁸ بارة سمير، الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، العدد الرابع، جويلية 2017، ص 270.
- ⁹ المرجع نفسه، ص 271.
- ¹⁰ حساني غنية، SCLC...العصب الرقمي لصد الجرائم المعلوماتية، مجلة الشرطة، المديرية العامة للأمن الوطني، العدد 158، ماي 2024، ص 22-23.
- ¹¹ سهيلة بوزيرة، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية - جامعة تيزي وزو، المجلد 17، العدد 02، سنة 2022، ص 563.
- ¹² زمورة جبال، بن عيسى ليلي، أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر، مجلة البحوث الاقتصادية المتقدمة، المجلد 07، العدد 02، 2022، ص 415.
- ¹³ وزارة البريد والمواصلات السلكية واللاسلكية، زيارة عمل إلى وهران: تعزيز البنية التحتية الرقمية ودعم الاقتصاد الرقمي، <https://www.mpt.gov.dz>، 20:35، 2025.11.19.
- ¹⁴ الحياة dz، هذا هو مشروع قانون تعزيز الثقة الرقمية والتعريف الإلكتروني في الجزائر، <https://elhayat.dz>، 2025.11.19، 18:49.
- ¹⁵ قطاف سليمان، بوقرين عبد الحليم، الآليات الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني (الجزائر نموذجاً)، مجلة الحوكمة والقانون الاقتصادي، جامعة باتنة 1، 2023، ص 86-87.
- ¹⁶ قطاف سليمان، بوقرين عبد الحليم، مرجع سابق، ص 87.
- ¹⁷ البديل، "الاستراتيجية الوطنية للأمن السيبراني: من أجل جزائر صاعدة سيبرانيا"، <https://elbadilabc-ar.dz/?p=28318>.

2025.11.09، 09:00.