

التكريس التشريعي للأمن السيبراني في الجزائر

Legislative Entrepreneurship of Cybersecurity in Algeria

حابت أمال*

Amel Habet

جامعة تيزي وزو - الجزائر

University of Tizi Ouzou -Algeria-

habet_amel@yahoo.fr

تاريخ الاستلام: 2026/06/01 تاريخ القبول للنشر: 2026/09/17 تاريخ النشر: 2026/10/01

ملخص:

يعد التكريس التشريعي للأمن السيبراني ضرورة حتمية لضمان نجاح التحول الرقمي ، حيث انتقلت الدولة من المقاربة التقنية الكلاسيكية المعتمدة على تأمين الأجهزة والشبكات ببرمجيات الحماية والتشفير، إلى تبني استراتيجية سيبرانية شاملة تعتمد على "الدفاع في العمق" عبر هيئات سيادية متخصصة. وقد واکب هذا التطور التقني زخم تشريعي ، بدأ بتعديل قانون العقوبات انتهى إلى حين كتابة هذا المقال إلى إصدار قانون 02-26 المتعلقة بالثقة في المعاملات الالكترونية، مما يعكس رغبة المشرع في خلق بيئة رقمية آمنة، مؤكداً أن الأمن المعلوماتي لم يعد مجرد إجراء تقني فقط بل أصبح ركيزة قانونية استراتيجية.

الكلمات المفتاحية: أمن، سيبراني، معاملات، الكترونية، ثقة، رقمية

Abstract:

Legislative entrepreneurship of cybersecurity is an imperative for ensuring the success of digital transformation. The state has moved from the classical technical approach, which relies on securing devices and networks with protection and encryption software, to adopting a comprehensive cybersecurity strategy based on "defense in depth" through specialized sovereign bodies. This technological development has been accompanied by legislative momentum, beginning with amendments to the Penal Code and culminating, at the time of writing, in the enactment of Law 26-02 concerning trust in electronic transactions. This reflects the legislator's desire to create a secure digital environment, confirming that information security is no longer merely a technical procedure but has become a strategic legal pillar.

Keywords: Security, cybersecurity, electronic transactions, trust, digital

* المؤلف المراسل.

مقدمة:

يمر العالم اليوم بتحولات رقمية متسارعة جعلت من الفضاء السيبراني وطننا ثانيا للبشرية ومحركا أساسيا لاقتصاديات الدول واستقرارها، هذا الانفتاح الرقمي الواسع أدى إلى نشوء مساحات شاسعة من الضعف التقني مما جعل المعلومات عرضة لاعتداءات مختلفة، من هنا برز للوجود مفهوم أمن المعلومات الذي تطور فيما بعد إلى مفهوم الأمن السيبراني كضمان لاستمرارية هذا التحول مع حماية الخصوصية والسيادة الرقمية.

يعتبر تحدي الأمن السيبراني أعلى تحديات الأمن الوطني والدولي في القرن الواحد والعشرين، مع الإشارة إلى أن المفهوم الحديث للأمن لا يقتصر فقط على الجوانب العسكرية، بل يواكب كل التهديدات والتحديات التي يمكن أن تشكل حجر عثرة أمام الاقتصاد الرقمي وتدفق المعرفة، فقد أسقطت تكنولوجيا المعلومات والاتصالات مفهوم الحدود الجغرافية بين الدول مما يضع السيادة الوطنية على المحك، خاصة مع اختراق المواقع الحكومية الرسمية والتجسس المعلوماتي على الدول.

للاّمن السيبراني مفهومين أحدهما كلاسيكي والثاني حديث، و التعريف الكلاسيكي للأمن المعلوماتي يركز على أنه نشاط يؤمن حماية الأنظمة المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن.

بينما التوجه الحديث في تعريف الأمن السيبراني انتقل من مجرد مجموع الاجراءات التقنية لحماية البيانات إلى مفهوم أكثر شمولية حيث أنه انتقل من الاستجابة لرد الفعل- الطابع الدفاعي- إلى الأمن الإستباقي، فيعرف الأمن المعلوماتي اليوم على أنه منظومة ذكية قادرة على التنبؤ بالهجمات قبل وقوعها عبر تحليل السلوك باستخدام خوارزميات التعلم الآلي بدلا من الاعتماد فقط على قواعد البيانات التقليدية للفيروسات ومن ثمة التصدي لها مع ضمان إستمرارية الأنظمة وسرعة التعافي، وهو بذلك مجموعة من الاجراءات تتخذ في الدفاع ضد الهجمات السيبرانية وعواقبها وتنفيذ التدابير المضادة المطلوبة¹

الأمن السيبراني ليس مجرد تطور تقني فقط بل هو قضية أمن قومي ذو بعد دولي بامتياز، فيكفي أن نعلم أن الهجمات السيبرانية المختلفة كلفت الاقتصاد العالمي العام الماضي 2025 أكثر من 10.5 تريليون دولار لنستوعب حجم هذه المعضلة، فمع كل تقدم نحزله في رقمنة الخدمات

والمعاملات يتولد معه تحديات وتهديدات عابرة للحدود لا تعترف بالحواز الجغرافية ولا بالسيادة الوطنية للدول.

عليه، وجدت الدول نفسها مضطرة أن تهتم بتأمين الفضاء السيبراني، ولقد خطت الجزائر خطوات جبارة في هذا المضمار من خلال ترسانة قانونية مستحدثة ومؤسسات وطنية متخصصة إدراكا منها بأن السيادة الرقمية هي الوجه الآخر للسيادة الوطنية في القرن الحادي والعشرين. وضع المشرع الجزائري نصوص قانونية بشكل متشعب تضمن أمن الانظمة المعلوماتية بدء بقانون العقوبات²، قانون الاجراءات الجزائية³، قانون رقم 04-09 المتعلق بالوقاية من جرائم تكنولوجيايات الاعلام والاتصال ومكافحتها⁴، قانون رقم 04-18 المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية⁵، قانون رقم 05-18 المتعلق بالتجارة الالكترونية⁶ قانون رقم 07-18 المتعلق بحماية الاشخاص الطبيعيين في مجال معالجة البيانات ذات الطابع الشخصي⁷ المعدل والمتمم⁸، القانون النقدي والمصرفي⁹ الى جانب المرسوم الرئاسي رقم 05-20 المتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية¹⁰ المعدل والمتمم بالمرسوم الرئاسي رقم 25-298، قانون الثقة في المعاملات الالكترونية¹¹ و المرسوم الرئاسي رقم 07-26¹²، خاصة أمام اعتماد الجزائر على رقمنة جميع مصالحها وانشاء محافظة سامية للرقمنة بموجب مرسوم رئاسي رقم 23-314¹³ المعدل بالمرسوم الرئاسي رقم 24-1463.

انطلاقا من هذه المعطيات نتساءل: ماهي التدابير التشريعية التي وضعها المشرع الجزائري لتحقيق مستويات أمان قصوى للبيانات في ظل بيئة افتراضية مليئة بالتهديدات ؟ تبعا لصيغة هذا الاشكال فان المنهج المناسب للدراسة هو المنهج الاستدلالي الاستقرائي نطلق فيه من تحليل النصوص القانونية كقضايا جزئية أولية لنخلص في الأخير إلى القاعدة الكلية التي تحكم التكريس التشريعي للأمن السيبراني .

يوجد علاقة طردية بين التوسع الرقمي وزيادة المخاطر، عليه لابد من مجابهة هذه المخاطر من خلال آليات مختلفة منها المؤسساتية (مبحث أول)، بالإضافة إلى آليات قانونية يتوزع الاطار التشريعي لها على عدة نصوص (مبحث ثان).

المبحث الأول: الاطار المؤسساتي للأمن السيبراني

الأمن السيبراني منظومة متكاملة مكونة من تقنيات عملية وبرامج متطورة واطار قانوني رادع، كما أن النصوص القانونية أصلا لا تستقيم إن لم تستند إلى قاعدة تقنية صلبة ووعي مجتمعي يقظ، فلا يتوقف تحقيق الأمن السيبراني على وجود التشريع بقدر ما يتوقف على الكفاءة البشرية للمؤسسات المكلفة بأمن الأنظمة المعلوماتية، وقد شهد الإطار المؤسساتي للأمن السيبراني في الجزائر تطوراً جذرياً خاصة مع مطلع عام 2026، حيث تم الانتقال من مجرد هيئات مكافحة الجريمة الإلكترونية إلى رؤية استراتيجية شاملة تقودها وزارة الدفاع الوطني بالتنسيق مع أعلى سلطات الدولة، و عليه تتمثل هيكلية الإطار المؤسساتي للأمن السيبراني في الجزائر في أجهزة مكلفة بوضع استراتيجيات الأمن السيبراني (مطلب أول) وأجهزة أخرى عملانية وتقنية تعمل على تنفيذ هذه الاستراتيجيات (مطلب ثان).

المطلب الأول: الهيئات المكلفة بوضع استراتيجيات الأمن السبراني

يعتبر محور الهياكل المكلفة بوضع استراتيجيات الأمن السيبراني الركيزة الأساسية في بناء جدار الصد الرقمي لأي دولة، فلا يقتصر الأمر على الجوانب التقنية فحسب، بل يمتد ليشمل صناعة القرار السيادي وحماية مصالح الدولة والافراد، لذلك كان من المستحسن لو تم دسرة مبدأ الأمن السيبراني مثلما فعلته بعض الدساتير كالمشرع المصري مثلاً¹⁵.

الفرع الأول: القيادة الاستراتيجية العليا

تتمثل في رئيس الجمهورية، القائد الأعلى للقوات المسلحة، وزير الدفاع الوطني الذي يشرف مباشرة على اعتماد الاستراتيجيات الكبرى وقد نشرت وكالة أمن الأنظمة المعلوماتية لوزارة الدفاع الوطني، يوم الثلاثاء 03 مارس 2026، الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية للفترة 2025-2029¹⁶، في نسختها الأولى، والتي صادق عليها السيد رئيس الجمهورية القائد الأعلى للقوات المسلحة وزير الدفاع الوطني بموجب المرسوم الرئاسي رقم 25-321 مؤرخ في 30 ديسمبر 2025 والتي تعتبر "خارطة الطريق" للسيادة الرقمية الجزائرية من أجل تحصين وحماية مؤسسات الدولة والهيئات الوطنية من كافة أشكال التهديدات التي قد تواجهها في فضاءها السيبراني، تمثل هذه الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية الإطار الشامل الذي يهدف إلى ضمان المرونة السيبرانية الوطنية وحماية البنية التحتية الرقمية للدولة وبياناتها، وكذا حماية المواطنين

من التهديدات التي قد تواجههم في الفضاء السيبراني، خاصة في ظل توجه السلطات العليا للبلاد الرامي إلى التسريع من وتيرة التحول الرقمي على مستوى كافة مؤسسات الدولة، كما تعد ورقة طريق من شأنها المحافظة على السيادة الرقمية الوطنية وضمان الخدمات العمومية الأساسية وتعزيز ثقة المواطن في بيئته الرقمية.

تمثل المحاور الاستراتيجية الوطنية الجديدة (2025-2029) في أربعة أعمدة رئيسية تم إقرارها في عام 2026:

1. القدرات التقنية العملية: تعزيز وسائل الكشف والاستجابة للحوادث السيبرانية.
2. الإطار القانوني والتنظيمي: تحديث التشريعات لتواكب التطورات التكنولوجية المتسارعة (مثل الذكاء الاصطناعي والحوسبة السحابية)
3. التكوين والبحث والتحصين: ترسيخ ثقافة أمنية لدى المواطن والموظف الحكومي.
4. التعاون الدولي: بناء شراكات استراتيجية لحماية الفضاء السيبراني الجزائري من التهديدات العابرة للحدود.

الفرع الثاني: المجلس الوطني لأمن الأنظمة المعلوماتية

يعتبر المجلس الوطني لأمن الأنظمة المعلوماتية في الجزائر حجر الزاوية في منظومة الحكم الرقمي، و هو "العقل المدبر" الذي يقرر كيف تحمي الجزائر فضاءها الرقمي، ومن هم الحلفاء، وما هي الخطوط الحمراء التي لا يمكن تجاوزها في التعامل مع البيانات الوطنية، و يمثل السلطة المسؤولة عن رسم السياسات وتنسيق الجهود بين مختلف القطاعات (المدينة والعسكرية) لضمان السيادة الرقمية.

يخضع المجلس مباشرة لرئاسة الجمهورية، وترجع قيادته وتنسيقه العملياتي إلى وزارة الدفاع الوطني، هذا الربط يعكس نظرة الدولة للأمن السيبراني كجزء لا يتجزأ من الأمن القومي الشامل.

يتولى المجلس القيام بعدة مهام استراتيجية¹⁷، أبرزها:

- رسم الاستراتيجية الوطنية: إعداد وتحيين الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والإشراف على تنفيذها.
- تحديد المعايير التقنية: وضع المقاييس الأمنية التي يجب على المؤسسات الحكومية والخاصة (الحساسة) اتباعها لحماية بياناتها.
- المصادقة على المخططات الاستيعالية: اعتماد خطط التدخل في حالة وقوع هجمات سيبرانية كبرى تهدد استقرار المنشآت الحيوية (الطاقة، الاتصالات، المالية)

- التنسيق بين الهيئات: الربط بين "وكالة أمن الأنظمة المعلوماتية" (الجانب التقني) وبين الهيئات الوزارية الأخرى (الجانب الإداري)

المطلب الثاني: الهيئات العملية والتقنية لتنفيذ استراتيجية الأمن السيبراني

تمثل أبعاد الأمن المعلوماتي في حماية البنى التحتية الحيوية للدولة من اصابتها بشلل أو تدمير أنظمة التشغيل الخاصة بها، بما يؤدي إلى إرباك عملها و تعطيل العديد من مرافق الحياة وسيادة الفوضى، مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات، وإذا كانت الأجهزة المذكورة في الفرع الأول تضطلع بوضع استراتيجيات الأمن السيبراني لا بد من وجود أجهزة عملاتية وتقنية تكلف بتنفيذ هذه الاستراتيجيات فهي إذن المحرك الفعلي للأمن السيبراني في البلاد، ويضم أجهزة إدارية مستقلة (فرع أول) وهيكل داخل كل الإدارات العمومية (فرع ثان).

الفرع الأول: الأجهزة الإدارية – المستقلة- المكلفة بتحقيق الأمن السيبراني وتضم كل من:

أولاً: وكالة أمن الأنظمة المعلوماتية¹⁸

تتبع وزارة الدفاع الوطني، وهي الهيئة المحورية المسؤولة عن تنفيذ الاستراتيجية الوطنية، وحماية البنى التحتية الحساسة للدولة، وضمان "المرونة السيبرانية" للمؤسسات الرسمية. وهناك تكامل وظيفي بينها وبين المجلس الوطني لأمن الأنظمة المعلوماتية فبينما يضع المجلس الوطني السياسات والقرارات الكبرى (المستوى الاستراتيجي)، تقوم الوكالة بتنفيذ تلك القرارات ومراقبة تطبيق المعايير على أرض الواقع (المستوى العملي)

يتولى إدارة الوكالة لجنة توجيه وتزود بلجنة علمية، كما يكلف بتسييرها مدير عام وتتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات و مصالح تقنية وإدارية موضوعة تحت سلطته.

ما يمكن تسجيله على هذا المرسوم الرئاسي تضارب في اختصاص فيما يخص اعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني كمهمة من مهام وكالة أمن الأنظمة المعلوماتية والتي حددت مسبقاً كصالحية من صلاحيات سلطات التصديق الإلكتروني سواء في ظل القانون 04-15 الملغى أو القانون رقم 02-26

يقع على عاتق المؤسسات والادارات والهيئات العمومية والخاصة التزام تعيين مسؤول مكلف بالأنظمة المعلوماتية لتمتكن الوكالة من التعامل معه وذلك في اجل سنة من نشر المرسوم الرئاسي 05-20.

ثانيا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها : والتي أعطى لها المرسوم الرئاسي رقم 15-261 صفة السلطة الإدارية المستقلة التي تراجع عنها لاحقا بموجب المرسوم الرئاسي 19-172 واعتبرها مؤسسة عمومية ذات طابع إداري توضع تحت سلطة وزارة الدفاع ليعيد إليها المرسوم الرئاسي رقم 20-183 صفة السلطة الإدارية المستقلة والموضوعة تحت سلطة رئيس الجمهورية بعدما كانت تحت وصاية وزارة العدل في 2015 ثم وزارة الدفاع في 2019 وأخيرا رئاسة الجمهورية في 2020.

وتضطلع هذه الهيئة بدورين، دور وقائي بصدد الجرائم الإرهابية أو التخريبية والماسة بأمن الدولة ودور مكافح لباقي جرائم تكنولوجيا الإعلام والاتصال ومساعد للهيئات القضائية بعد حدوث الجريمة¹⁹ فهي تعمل كمنسق بين الجهات القضائية والأمنية لمواجهة التهديدات الرقمية.

ثالثا: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني أنشئ منذ 2008، ويختص بالرقابة التقنية، تحليل البيانات الرقمية، وتتبع عمليات الاختراق والقرصنة.

رابعا: المصلحة المركزية لمكافحة الجريمة المعلوماتية بالمديرية العامة للأمن الوطني: تختص بملاحقة الجرائم السيبرانية التي تستهدف الأشخاص والممتلكات وتأمين الفضاء الرقمي العام.

و لضمان استدامة الأمن السيبراني، استثمرت الجزائر في تكوين العنصر البشري من خلال:

المدرسة الوطنية العليا للأمن السيبراني (ENSCS) بقطب سيدي عبد الله، وهي المؤسسة الأكاديمية الرائدة لتخريج مهندسين متخصصين في حماية الأنظمة الرقمية وتطوير الحلول الأمنية المحلية.

الفرع الثاني: انشاء هيكل مسؤولة عن أمن الأنظمة المعلوماتية وحماية المعطيات داخل كل الهيئات العمومية

جاء انشاء هذه الهياكل بموجب المرسوم الرئاسي رقم 26-07²⁰، ويهدف هذا الأخير إلى إحداث نقلة نوعية في حوكمة الأمن المعلوماتي داخل المؤسسات العمومية ، من خلال إنشاء كيان تنظيمي متخصص يدعى "الهيكال". وقد نصت المادة 2 بوضوح على ضرورة أن يكون هذا الهيكال مستقلاً عن الهيكال المكلف بالأنظمة المعلوماتية (الرقمنة والإعلام الآلي)، لضمان عدم تضارب المصالح بين جهة التشغيل وجهة التأمين والرقابة، على أن يلحق الهيكال مباشرة بالمسؤول الأول للمؤسسة (الوزير، الوالي، المدير العام...) لضمان النفاذ المباشر وصلاحيات اتخاذ القرار .

بالنسبة للاختصاصات والمهام الرئيسية للهيكل²¹ :

يتولى الهيكل مهامًا تقنية واستراتيجية، أبرزها :

- رسم السياسات : إعداد سياسة أمن الأنظمة المعلوماتية للمؤسسة والسهر على تطبيقها .
- إدارة المخاطر : إعداد خريطة المخاطر المرتبطة بالأمن وحماية المعطيات ذات الطابع الشخصي .

• المرونة السيبرانية : إدارة حلول الأمن واليقظة المستمرة وضمان المرونة في حالة وقوع حوادث .

- التدقيق والمراقبة : القيام بعمليات تدقيق دورية بالتعاون مع الجهات المختصة .
- الامتثال القانوني : السهر على تطبيق القانون رقم 07-18 المتعلق بحماية المعطيات الشخصية .

أما بشأن التنظيم الداخلي والموارد البشرية: حدد المرسوم الوظائف الأساسية التي يجب أن يتضمنها الهيكل وهي :

1. مسؤول الهيكل.

2. المكلف بعمليات الأمن واليقظة.

3. المكلف بالتدقيق وتسيير المخاطر.

4. المكلف بحماية المعطيات ذات الطابع الشخصي.

5. المكلف بالتحسيس والتكوين.

يمكن الدمج بين بعض هذه المناصب حسب حجم المؤسسة ودرجة حساسية أنظمتها .

لضمان تفعيل الهيكل سريعاً، أقر المرسوم طرقاً مرنة للتوظيف²²:

إعادة التوزيع الداخلي للموظفين.

النقل أو الانتداب من إدارات أخرى للموظفين ذوي الكفاءة والإشهاديات.

التوظيف الخارجي عند الضرورة.

الإلزامية استفادة الموظفين من تكوين تحضيري قبل مباشرة مهامهم .

كما يفرض المرسوم نظاماً تنسيقياً مع جهات خارجية لضمان التكامل²³ وهما:

- وكالة أمن الأنظمة المعلوماتية: للتنسيق التقني والبرامج التكوينية.
- السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي: لضمان قانونية معالجة البيانات.

المبحث الثاني:

الأطر القانونية الجزائرية لتحقيق الامن السيبراني

عرف المشرع الجزائري الامن السيبراني في القانون رقم 04-18 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية في مادته 10 / 3 بأنه: مجموع الادوات والسياسات ومفاهيم الامن والاليات الامنية والمبادئ التوجيهية وطرق تسيير المخاطر والاعمال والتكوين والممارسات الجيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الالكترونية ضد اي حادث من شأنه المساس بتوفر وسلامة وسرية البيانات المخزنة او المعالجة او المرسلة، ما يلاحظ على هذا التعريف تناوله للشق المتعلق بالحماية من الاعتداءات فقط ولم يتضمن الشق الحديث والمتمثل في الأمن السيبراني الاستباقي، ولتحقيق هذا الأمن السيبراني وضع المشرع مجموعة من القوانين لها علاقة بامن الانظمة المعلوماتية وتتوزع بين تلك التي أهتمت بالجانب الجزائي الاجرائي والعقابي (مطلب أول) و اخرى ذات طابع مدني إهتمت بحماية البيانات والمعاملات (مطلب ثان).

المطلب الأول: القوانين الجزائية وتنظيمها للامن السيبراني

أصبح الإطار الجزائي أكثر صرامة ووضوحا، مع التركيز ليس فقط على معاقبة القرصنة، بل أيضا على حماية البيانات الشخصية والسيادة الرقمية، و الجزائر في تنظيمها للأمن السيبراني تعتمد على بعدين : دولي و وطني ، بالنسبة للبعد الدولي صادقت الجزائر على كل من: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب مرسوم رئاسي رقم 14-252²⁴ اضافة الى معاهدة الأمم المتحدة لمكافحة الجرائم السيبرانية والتي وقعت الجزائر عليها في أكتوبر 2025، وتعد هذه الاخيرة إطارا قانونيا ملزما للاستجابة الجماعية للمخاطر المتعددة الأوجه المرتبطة بالجرائم السيبرانية، حيث تنص على استحداث آليات لتكثيف التحقيقات الجنائية التقليدية مع بيئة تكنولوجيا المعلومات بالإضافة إلى وضع آلية عالمية لتبادل الأدلة الإلكترونية حول الجرائم الخطيرة. أما داخليا فتعتمد الجزائر على ترسانة قانونية جزائية تجمع بين قوانين عامة تضم كل من قانون العقوبات وقانون الاجراءات الجزائية وقوانين خاصة استحدثت لمواكب التطور الرقمي

الفرع الأول: القوانين الجزائية العامة

تضم كل من:

أولا: قانون العقوبات:

حيث تضمن فصلا خاصا بالمساس بانظمة المعالجة الالية للمعطيات جرم فيها افعال منها الدخول أو البقاء غير المصرح بهما الى كل أو جزء من انظمة معلوماتية، مع مضاعفة العقوبة اذا

ترتب عن هذا الدخول حذف أو تغيير في معطيات المنظومة، وإذا ترتب على الدخول تخريب المنظومة تشدد العقوبة²⁵.

تجريم الادخال عن طريق الغش أو الازالة أو التعديل للمعطيات ، تجريم تصميم، البحث، التجميع، التوفير، النشر، أو الاتجار في معطيات يمكن استخدامها لارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما جرمت حيازة البيانات فيعاقب أيضاً على حيازة، إفشاء، أو استعمال المعطيات التي تم الحصول عليها نتيجة هذه الجرائم²⁶.

ثانياً: قانون الاجراءات الجزائية

يساهم هذا القانون في تحقيق أمن الأنظمة المعلوماتية من خلال عدة آليات إجرائية وتقنية متطورة:

- اعتبار الجرائم المتصلة بتكنولوجيا الاعلام والاتصال²⁷ جرائم خاصة²⁸ ، ووجه الخصوصية يمكن في خطورتها لذلك خصها المشرع بعدة اجراءات تختلف عن الجرائم العادية منها قواعد التفتيش الذي يتم في أي وقت وفي أي مكان، التوقيف للنظر الذي يمكن تجديده ثلاث مرات²⁹، كما لا يمكن للمشتبه فيه في هذا النوع من الجرائم ان يتصل بمحاميه الا بعد مرور نصف المدة القوي المقررة لوقفه للنظر أي بعد 96 ساعة من توقيفه³⁰

- آليات التحقيق الرقمي الحديثة: القانون سمح بالتعامل مع "الدليل الرقمي" الذي يتميز بالسرعة وسهولة المحو بعدة اليات ، ومن أبرزها:

1- التفتيش الإلكتروني:منح صلاحيات لتفتيش الأنظمة المعلوماتية أو الحوامل الإلكترونية (سواء كانت مادية كالأقراص الصلبة أو سحابية) وضبط البيانات المخزنة فيها.

2- الاعتراض الرقمي :إمكانية اعتراض المراسلات بما فيها الالكترونية وتسجيل الاصوات و التقاط الصور في الوقت الحقيقي تحت إشراف قضائي³¹

3- الحجز الرقمي :لم يعد الحجز يقتصر على الأجهزة المادية فقط، بل امتد ليشمل "نسخ البيانات" أو تجميدها لمنع تغييرها، فتتص المادة 119 من قانون الاجراءات مثلاً انه يتم نسخ المراسلات والصور والمحدثات المسجلة والمفيدة في اظهار الحقيقة في محضر يودع بالملف وترفق به الدعامة الالكترونية.

- تخصيص قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال³² وهو قطب مخصص بالمتابعة والتحقيق والحكم في هذا النوع من الجرائم ويوجد في دائرة اختصاص مجلس قضاء الجزائر العاصمة³³ فيكون كل من وكيل الجمهورية وقاضي التحقيق في هذا القطب اختصاص وطني.

- الاعتراف الصريح بالدليل الالكتروني في الاثبات وقد جاء النص عليه في المادة 349 من قانون الاجراءات الجزائية الجديد.

- إلزامية التعاون: يلزم القانون شركات الإنترنت والاتصالات بالمساهمة في التحقيقات، وتزويد السلطات بالبيانات اللازمة لتعقب الجناة، مع الحفاظ على سرية التحقيق.

الفرع الثاني: القوانين الخاصة

وتشمل عدة نصوص حاولت تحقيق الامن المعلوماتي من خلال تجريم بعض الاعتداءات ونصوص اخرى تضمنت اجراءات خاصة .

أولاً: قانون حق التأليف:

المشرع الجزائري في ظل الأمر رقم 05-03 المتعلق بحقوق المؤلف والحقوق المجاورة³⁴، جرم الاعتداء على البرامج الالكترونية لكنه لم يعرف المصنفات الرقمية إنما ذكرها على سبيل المثال لا الحصر³⁵، إلا انه قام بتجريم كل إعتداء على الحق الأدبي و المالي للمؤلف تحت مسمى جريمة التقليد وذلك في المادتين 151 و152 من الأمر 05/03 ، يتحقق السلوك الإجرامي في جريمة التقليد بتحقيق أحد الأفعال التي تمس بالحقوق الإستثنائية وهذه الأفعال تتمثل في:

- الكشف غير المشروع للمصنف³⁶

- المساس بسلامة المصنف³⁷

- الاعتداء على حق النسخ³⁸

- الاعتداء على حق المؤلف في إبلاغ المصنف للجمهور³⁹

- الاعتداء على حق المؤلف في تحويل البرنامج: أي حق المؤلف في استغلال مصنفه وفي

ترخيص انجاز مصنفات مشتقة كالاقتباسات والترجمات والتعديلات الخ

- الاستيراد أو التصدير لنسخ مقلدة

- بيع نسخ مقلدة لمصنف

- تأجير نسخ مقلدة او عرضها للتداول

ثانيا: قانون 04-09 المتعلق بالوقاية من جرائم تكنولوجيايات الاعلام والاتصال ومكافحتها:

ومن اهم ماجاء في هذا القانون انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيايات الاعلام والاتصال، و اجرائي المراقبة الالكترونية والتفتيش الالكتروني.

نعني بالمراقبة الالكترونية للاتصالات وضع تقنيات لازمة لتجميع وتسجيل محتوى الاتصالات الالكترونية بما فيها تلك التي تتم على شبكة الانترنت أو الفاكس أو التلكس أو الهاتف...أو أي وسيلة أخرى الكترونية تنقل معلومات في أي شكل كانت، على أن يتم هذا التجميع والتسجيل في حينه أي أثناء إجراء الاتصال، أما إذا تم الاطلاع هذه المعلومات في وقت لاحق فذلك لا يعد عملية مراقبة للاتصال بل يعد تفتيشاً⁴⁰.

ولهذه المراقبة طابعين: طابع وقائي فنعني به أن هذا الإجراء يتخذ من دون حدوث أي جريمة، بل تفاديا لحدوثها. ونظرا لمساسه مجرمة وسرية المراسلات والاتصالات حصره المشرع في حالة الوقاية من الجرائم الإرهابية والتخريبية والماسة بأمن الدولة وكذا احتمال اعتداء على أنظمة معلوماتية تمس بالنظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني

- طابع تحقيقي أي بعد حدوث الجريمة تضمثها الحالتين ج ود وهما متعلقتين ب لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية.

- في إطار المساعدة الدولية المتبادلة.

أما اجراء تفتيش المنظومة المعلوماتية ،فحسب المادة 05 من القانون 04-09 يجوز للسلطات القضائية المختصة وضباط الشرطة القضائية الدخول بغرض التفتيش إلى:

- منظومة معلوماتية أو جزء منها والمعطيات المعلوماتية المخزنة فيها.
- منظومة تخزين معلوماتية.

هذا التفتيش له حالات وهي ذاتها التي تسمح باللجوء إلى المراقبة الالكترونية، كما تجمد القواعد الإجرائية للتفتيش والمنصوص عليها في قانون الإجراءات الجزائية باستثناء الحصول على إذن ، وتضيف المادة 05 من قانون رقم 04-09 انه في صدد الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب والمساس بأمن الدولة يجوز تمديد التفتيش بسرعة إلى منظومة معلوماتية لم يشملها الإذن إذا كانت هناك أسباب تدعو إلى الاعتقاد أن المعطيات المبحوث عنها مخزنة فيها مع إعلام السلطة القضائية المختصة ، وإذا كانت هذه المنظومة خارج الإقليم الوطني يمكن أن تطلب مساعدة السلطات الأجنبية للوصول إليها⁴¹.

بالإضافة الى الزام مقدمي خدمات الانترنت بالتعاون مع السلطات لتسهيل جمع الادلة.

المطلب الثاني: القوانين ذات الطابع المدني وعلاقتها بالأمن السيبراني

ضمت هذه الطائفة مجموعة من القوانين تسعى لحماية البيانات والمعاملات (فرع أول) وأخرى اهتمت بالأمن المالى وخدمات الثقة في المعاملات الالكترونية (فرع ثان)

الفرع الأول: قوانين ذات الصلة بحماية البيانات والمعاملات

زيادة للقانون المدني والقانون التجاري كأولى القوانين المنظمة لبعض احكام التعاملات الالكترونية، وبعض المراسيم التنفيذية مثل المرسوم التنفيذي رقم 16-142 مؤرخ في 5 مايو سنة 2016، يحدد كيفيات حفظ الوثيقة الموقعة إلكترونيا، صدرت قوانين جديدة تسعى لتكريس الامن السيبراني ويندرج ضمنها كل من:

أولا: قوانين الانترنت والرقمنة:

المشروع الجزائري وضع التزامات على عاتق مقدمي خدمات الانترنت في كل من المرسوم التنفيذي 98-257 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها المعدل بموجب مرسوم تنفيذي رقم 2000-307 المؤرخ في 14 أكتوبر سنة 2000 وفي قانون رقم 04-09 تحقق نوع من الامن المعلوماتي بحيث :

- نصت المادة 14 من المرسوم التنفيذي 98-257 المعدل والمتمم على التزامات مقدمي الانترنت بحيث يجب على المتعامل اتخاذ التدابير اللازمة لضمان المراقبة الدائمة والدقيقة للمحتويات التي يتم بثها أو استضافتها أو الوصول إليها عبر شبكته، والامتنثال فورا لأي طلب حجب أو منع يصدر عن السلطات المختصة، لا سيما عندما يتعلق الأمر بحماية النظام العام أو الآداب العامة، وعليه أبرز الالتزامات القانونية المقررة في المادة: 14 من المرسوم التنفيذي 98-257 هي:

- **المراقبة والمسؤولية:** إلزام متعاملي ومزودي خدمات الإنترنت بمراقبة المحتوى والخدمات التي تمر عبر شبكاتهم .

- **الامتنثال لأوامر السلطات:** منح السلطات العمومية والمختصة الحق في مطالبة المزود بحجب أي موقع أو منع وصول للمحتويات التي تعتبر مخالفة للقانون .

- **حماية الصالح العام:** تحديد معايير الحجب ب النظام العام، والآداب العام أو الأخلاق.

كذلك القانون رقم 04-09 نص على واجب التدخل الفوري لسحب المحتويات غير مشروعة أو جعل الدخول إليها غير ممكن. إلى جانب وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام والآداب العامة وإخبار المشتركين لديهم بوجودها .

- أما بشأن المرسوم الرئاسي رقم 23-314 المتعلق بإنشاء المحافظة السامية للرقمنة المعدل والمتمم ، فقد جاء في نص المادة 4 منه والمتضمنة صلاحيات هذه المحافظة والتي منها: ضمان توافق الاستراتيجية الوطنية للرقمنة مع متطلبات أمن الأنظمة المعلوماتية بالتنسيق مع الجهات المختصة.

أولاً: قانون 04-18 تتجلى علاقة هذا القانون بالأمن السيبراني في المحاور الأساسية التالية:

- إلزامية تأمين الشبكات والأنظمة
- فرض القانون على متعاملي الشبكات (مثل شركات الاتصالات ومزودي الإنترنت) التزامات صارمة تتعلق بأمن البنية التحتية:
- سلامة الشبكات: يلزم القانون المتعاملين باتخاذ كافة التدابير التقنية لضمان استمرارية الخدمة وحماية الشبكات من الاختراقات.
- سرية المراسلات: يضع إطاراً قانونياً تحت طائلة المساءلة الجزائية يمنع التجسس أو اعتراض المراسلات الإلكترونية إلا في الحالات التي يحددها القانون (تحت إشراف قضائي)⁴² ، مما يعزز ثقة المستخدم في المنظومة الرقمية
- دور سلطة الضبط (ARPCE) في الرقابة، بحيث منح القانون سلطة ضبط البريد والاتصالات الإلكترونية صلاحيات واسعة تؤثر مباشرة على الأمن السيبراني، منها:
- المصادقة والاعتماد: مراقبة الأجهزة والأنظمة التي تدخل السوق الجزائرية للتأكد من مطابقتها للمعايير التقنية والأمنية، لضمان عدم وجود ثغرات "خلفية" (Backdoors) في المعدات.
- فرض العقوبات الإدارية: يحق للسلطة سحب التراخيص أو فرض غرامات مالية ضخمة على المتعاملين الذين يهملون في تأمين بيانات المشتركين أو يفشلون في حماية أنظمتهم من الهجمات

ثانياً: قانون رقم 05-18 المتعلق بالتجارة الإلكترونية

حيث تضمن احكاماً متعلقة بالأمن المعلوماتي أهمها:

- إلزامية تأمين المواقع الإلكترونية وتأكيد صحتها⁴³

- الزامية تأمين المعاملات حيث فرض القانون على الموردين حفظ سجل المعاملات وتواريخها وارسالها الى المركز الوطني للسجل التجاري⁴⁴
- الزامية اتخاذ تدابير تقنية عالية لضمان امن التبادل الالكتروني وسرية المعلومات⁴⁵
- الزامية اخذ موافقة المستهلكين لجمع بياناتهم
- الزامية تأمين الدفع الالكتروني بنظام للتصديق الالكتروني و فرض شروط تقنية لربط المنصات التجارية بمنظومات الدفع التابعة للبنوك عبر منصات دفع مؤمنة الى جانب خضوع منصات الدفع لرقابة بنك الجزائر لتأمين سلامة وسرية وامن البيانات عند تبادلها
- استخدام بروتوكولات تشفير قوية لحماية البيانات مثل ارقام البطاقات البنكية والمعلومات الشخصية اثناء انتقالها من الزبون الى الموقع
- سلامة المحتوى حيث لا يتم تعديل او تحريف العرض التجاري او العقد الالكتروني اثناء عملية الارسال⁴⁶
- لضمان وجود كيان قانوني يمكن محاسبته فرض القانون التسجيل في السجل التجاري الالكتروني وتوطين المواقع⁴⁷.

ثالثا: قانون رقم 07-18 المعدل والمتمم بقانون 11-25 المتعلق بحماية البيانات الشخصية :

البيانات الشخصية هي تلك المعلومات التي تسمح بالتعريف بالشخص (اسم ، رقم تعريف، بصمة، صورة، معطيات طبية...الخ) حيث اوجب القانون على المؤسسات اتخاذ كافة الاحتياطات التقنية والتنظيمية من اجل حماية المعطيات من التلف العرضي او الغير مشروع مثل الحرائق واعطال الاقراص الصلبة ، منع الضياع العرضي عن طريق انظمة النسخ الاحتياطي مثلا، منع الوصول الغير مصرح به عبر تقنيات مختلفة كالجدران النارية- التشفير...الخ، منع أي شكل من اشكال المعالجة الغير مشروعة كتسريب او بيع البيانات.

انشأ القانون 07-18 السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وهي هيئة ادارية مستقلة تتمتع بصلاحيات منها: منح التراخيص: لا يمكن لاي مؤسسة معالجة بيانات حساسة دون ترخيص بذلك من السلطة ، سلطة الرقابة والتفتيش حيث يمكن لاعوان السلطة الدخول لمقرات والاطلاع على الانظمة المعلوماتية للتأكد من فاعلية اجراءات الامن ، كما منح القانون للمواطن بعض الحقوق في سبيل الرقابة على بياناته منها: حق الاعتراض لأسباب مشروعة، حق الحصول على نسخة من البيانات التي يمتلكها النظام عنه، حق التصحيح والمسح من خلال اجبار صاحب النظام على تعديل المعلومات الخاطئة او حذفها اذا انتهى الغرض من معالجتها.

- بعدها جاء القانون 11-25 المعدل للقانون 07-18 بأحكام جديدة أهمها:
- تعزيز الاطار المفاهيمي والمؤسسي لحماية المعطيات من خلال عرض مفاهيم مستحدثة كالبيانات البيومترية، التمييز، تجهيل البيانات...الخ
 - تعزيز دور السلطة الوطنية لحماية المعطيات الشخصية من خلال توسيع صلاحياتها كالرقابة القبلية الصارمة واجراء التوقيف الفوري لعمليات المعالجة اذا ثبت وجود ثغرات امنية تهدد خصوصية المواطن⁴⁸
 - تفعيل دور مندوب حماية المعطيات
 - النص على واجب التوثيق والشفافية من خلال مسك سجل نشاطات المعالجة ودفتر العمليات
 - نظام التبليغ عن اختراقات البيانات وضوابط النقل الدولي للمعطيات⁴⁹
 - الزم الجهات التي تعالج البيانات تبني تقنيات التشفير متوافقة مع المعايير الوطنية التي تحددها وكالة امن الانظمة المعلوماتية
 - النص على العقوبات المالية و الجزائية في حال عدم الالتزام بالتدابير الامنية التقنية التي تحمي البيانات من الاختراق مسؤولية الشخص المعنوي (البنوك، شركات الاتصالات...الخ) الذي سرب البيانات
 - الحق في النسيان الرقمي، الزم القانون المؤسسات بحذف كافة البيانات الشخصية فور انتهاء الغرض الذي جمعت من اجله وجرت الاحتفاظ بها وارشفتها دون مبرر قانوني.
 - التكامل مع قانون العقوبات بحيث أي اعتداء سبراني يؤدي الى تسريب بيانات شخصية يعاقب عليه مرتين:
 - باعتباره مساسا بنظم المعالجة الالية للمعطيات بموجب قانون العقوبات
 - باعتباره انتهاكا لخصوصية البيانات الشخصية بموجب قانون 07-18 المعدل والمتمم بقانون 11-25.

الفرع الثاني : القوانين ذات الصلة بالأمن المالي وخدمات الثقة

يندرج ضمنها كل من:

أولا:قانون رقم 09-23 المتعلق بالقانون النقدي والمصرفي

يعمل القانون 09-23 على تأمين معلوماتي مالي من خلال:

- الزام بنك الجزائر بوضع معايير امنية مشفرة لمنع تزوير او اختراق العملة الرقمية⁵⁰.

- استحداث لجنة الاستقرار المالي مكلفة بمراقبة المخاطر التي تهدد النظام المصرفي ومن ضمن صلاحياتها: مواجهة المخاطر السيبرانية وذلك بالتنسيق بين الهيئات لضمان صمود الانظمة المعلوماتية البنكية امام مختلف الهجمات

- تنظيم مقدمي خدمات الدفع والتي تزاوّل نشاطها بعد حصولها على ترخيص ولا يمنح هذا الاخير الا اذا اثبت امتلاكه لانظمة معلوماتية محصنة ضد الاختراق ، مع خضوع هذه الشركات لعمليات تدقيق امني من طرف بنك الجزائر

- شدد القانون على حماية البيانات المالية للزبائن من خلال الزام البنوك بوضع بروتوكولات صارمة للوصول للبيانات وفرض عقوبات ادارية ومالية على المؤسسات التي تتعرض لاختراقات ناتجة عن اهمال في تحديث الانظمة الامنية

- ادخال مفهوم المختبر التنظيمي الذي يسمح بتجريب الحلول التقنية المتكررة في بيئة مراقبة مما يسمح باختبار الثغرات الامنية في التطبيقات البنكية الجديدة قبل طرحها للجمهور وكذا ضمان ان الابتكارات المالية لا تأتي على حساب امن الانظمة المعلوماتية الوطنية.

ثانيا: قانون رقم 02-26 المتضمن خدمات الثقة للمعاملات الالكترونية والهوية الالكترونية

وهو مكمل جوهري لمنظومة امن الانظمة المعلوماتية وقد ساهم في تأمين انظمة المعلومات من خلال:

- وضع معايير الثقة الرقمية فلا يمكن لاي نظام معلوماتي ان يكون امنا دون وجود الية للتحقق هذه الثقة وعليه نظم التوقيع الالكتروني، الختم الالكتروني، الهوية الالكترونية، الوسم الزمني، شهادات الاعتماد....الخ

- تأمين الادلة الرقمية من خلال اعطاء حجية كاملة للمحررات الالكترونية المعتمدة⁵¹

- تنظيم نشاط مزود خدمات الثقة بفرض التزامات عليه ورقابة من خلال التدقيق الامني الذي يثبت ان الانظمة المعلوماتية للمزود محصنة ووفق معايير وطنية قررتها وكالة امن الانظمة المعلوماتية - التأكيد على توطين البيانات داخل التراب الوطني

الخاتمة:

بناءً على التطورات التشريعية والمؤسسية التي شهدتها الجزائر حتى مطلع عام 2026، وتماشياً مع إطلاق الاستراتيجية الوطنية للأمن السيبراني (2025-2029)، يمكن استخلاص النتائج التالية وتقديم حزمة من التوصيات لتعزيز هذا التكريس التشريعي:

أولاً: النتائج المحققة

- الانتقال من "المكافحة" إلى "الاستباقية": "نجح التشريع الجزائري في الانتقال من مجرد نصوص تعاقب الجريمة بعد وقوعها (قانون 04-15 وقانون 09-04) إلى نصوص تفرض "الحوكمة الوقائية"، مثل المرسوم الرئاسي 26-07 الذي ألزم كل المؤسسات العمومية بإنشاء وحدات خاصة للأمن السيبراني مستقلة عن أقسام الإعلام الآلي.
 - مركزية القرار السيادي: أدى وضع الأمن السيبراني تحت إشراف رئاسة الجمهورية ووزارة الدفاع الوطني إلى تسريع وتيرة إصدار النصوص القانونية وضمان التزام كافة القطاعات (المالية، الطاقة، النقل) بمعايير أمنية موحدة.
 - السيادة الرقمية (الحوسبة السحابية): توقيع المراسيم المتعلقة بـ "حوسبة المعطيات الوطنية" (2025) أدى إلى فرض توطين البيانات الحساسة داخل التراب الوطني، مما أغلق ثغرة قانونية كانت تسمح بتخزين بيانات سيادية في خوادم خارج الحدود.
 - مواءمة القوانين مع المعايير الدولية: التعديلات الأخيرة على قانون حماية المعطيات الشخصية جعلت التشريع الجزائري يقترب من المعايير العالمية مثل GDPR ، مما يسهل التعاون الدولي والمبادلات الاقتصادية الرقمية الآمنة.
- ثانياً: التوصيات المقترحة
- لتعزيز الفعالية ورغم القفزة النوعية، تتطلب المرحلة القادمة (ما بعد 2026) التركيز على المحاور التالية:
- الجانب التشريعي والقضائي:
- استحداث "قانون إطاري شامل للأمن السيبراني: "بدلاً من تشتت النصوص بين قانون العقوبات وقانون حماية البيانات ومراسيم رئاسية، يفضل جمعها في قانون واحد موحد يسهل الرجوع إليه.
 - التكوين المتخصص للقضاة: تكثيف برامج التدريب للقضاة في مجالات "الأدلة الرقمية المعقدة" و"الجرائم المرتكبة عبر الذكاء الاصطناعي".
- الجانب المؤسسي والتقني:
- تحفيز القطاع الخاص و تشجيع المؤسسات على تطوير "حلول أمنية جزائرية" (برامج مضادة للفيروسات، جدران نارية) لتقليل التبعية للتكنولوجيا الأجنبية.

- إنشاء "نظام وطني للتوسيم (Labeling)" وضع قانون يفرض وسم "آمن سيرانياً" على كل الأجهزة والبرمجيات التي يتم استيرادها أو استخدامها في الإدارات العمومية. الجانب البشري والاجتماعي:
- قانون "التبليغ المحمي": توفير حماية قانونية للمبلغين عن الثغرات الأمنية لتشجيعهم على المساهمة في تأمين الأنظمة الوطنية دون خوف من الملاحقة القضائية.
- الثقافة الرقمية: إدراج مادة "المواطنة الرقمية والأمن السيبراني" في المناهج التعليمية في كامل أطواره (الابتدائي والمتوسط والثانوي والجامعي) بنص تنظمي لضمان نشوء جيل محصن رقمياً.

الهوامش:

1 أنظر في ذلك : راشد محمد المري، الأمن السيبراني وحماية الأنظمة الالكترونية، مجلة الدراسات القانونية والاقتصادية ، متاح على الموقع:

https://jdl.journals.ekb.eg/article_288640_499c1f37202cfd81125efc4525698e0.pdf

2 أمر رقم 156-66 مؤرخ في 8 جوان 1966 ، يتضمن قانون العقوبات ، معدل ومتمم بقانون 06-24 مؤرخ في 28 أفريل 2024 ، الجريدة الرسمية عدد 30 الصادرة في 30 أفريل 2024.

3 قانون رقم 14-25 مؤرخ في 3 أوت 2025 ، يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 54 الصادرة في 13 أوت 2025.

4 قانون رقم 04-09 مؤرخ في 5 أوت 2009 ، يتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيايات الاعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47 الصادرة في 16 أوت 2009.

5 قانون رقم 04-18 مؤرخ في 10 ماي 2018 ، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية عدد 27 الصادرة في 13 ماي 2018.

6 قانون رقم 05-18 مؤرخ في 10 ماي 2018 ، يتعلق بالتجارة الالكترونية، الجريدة الرسمية عدد 28 الصادرة في 16 ماي 2018

7 قانون رقم 07-18 مؤرخ في 10 جوان 2018 ، يتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 34 الصادرة في 10 جوان 2018.

8 قانون رقم 11-25 مؤرخ في 24 جويلية 2025 ، يعدل ويتمم القانون رقم 07-18 مؤرخ في 10 جوان 2018 والمتعلق بحماية الاشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 48 الصادرة في 24 جويلية 2025.

9قانون رقم 09-23 مؤرخ في 21 جوان 2023، يتضمن القانون النقدي والمصرفي، الجريدة الرسمية عدد43 الصادرة في 27 جوان 2023

10مرسوم رئاسي رقم 05-20 المؤرخ في 20 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية عدد4 الصادرة في 26 جانفي 2020

11قانون رقم 02-26 مؤرخ في 17 فيفري 2026، يحدد القواعد العامة المتعلقة بخدمات الثقة للمعاملات الالكترونية وبالتعريف الالكتروني، الجريدة الرسمية عدد14 الصادرة في 18 فيفري 2026.

12المرسوم الرئاسي رقم 07-26 المؤرخ في 7 جانفي 2026 يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والادارات والهيئات العمومية وتحديد مهامه وتنظيمه وسيره، الجريدة الرسمية عدد04 الصادرة في 18 جانفي 2026.

13مرسوم رئاسي رقم 314-23 مؤرخ في 6 سبتمبر 2023، يتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها، الجريدة الرسمية عدد59 الصادرة في 10 سبتمبر 2023

14مرسوم رئاسي رقم 63-24 مؤرخ في 1 فيفري 2024، يعدل مرسوم رئاسي رقم 314-23 مؤرخ في 6 سبتمبر 2023، يتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها، الجريدة الرسمية عدد 8 الصادر في 4 فيفري 2042.

15افتتص المادة 31 من الدستور المصري (يناير 2014) على أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون، انظر في ذلك الاستراتيجية الوطنية للأمن السيبراني 2023-2027. على الموقع:

https://egcert.eg/wp-content/uploads/2024/02/Publications_1412024000_ar_National_Cybersecurity_Strategy_2023_2027.pdf

16يمكن الاطلاع على هذه الاستراتيجية على الموقع: https://www.mdn.dz/assi/nsiss_ar.pdf

17حددت المادة16 من المرسوم الرئاسي رقم 05-20 مهام المجلس الوطني لأمن النظم المعلوماتية، أماالأهداف الاستراتيجية للمجلس (رؤية 2026) في ظل التحولات التي شهدتها الجزائر في مطلع عام 2026، يركز المجلس حالياً على:

1. السيادة على البيانات: ضمان تخزين البيانات الحساسة داخل التراب الوطني (الحوسبة السحابية الوطنية)
2. حماية المنشآت الحيوية: تأمين أنظمة التحكم الصناعي في قطاع المحروقات والمياه والكهرباء.

3. الدفاع السيرياني الاستباقي: تطوير قدرات الرصد المبكر للهجمات المعقدة قبل وصولها للأهداف.
- 18الوكالة فتعتبر حسب نص المادة 17 من المرسوم الرئاسي، مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية وتمثل مماتها في:
 - تحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس.
 - تنسيق تنفيذ الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية المحددة من قبل المجلس
 - اقتراح كينيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.
 - إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيريانية التي تستهدف المؤسسات الوطنية..
 - السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية.
 - متابعة عمليات التدقيق أمن الأنظمة المعلوماتية.
 - تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية.
 - ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية.
 - مرافقة الإدارات والمؤسسات والهيئات بالتشاور مع الهياكل المختصة ف هذا المجال في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية، بعد الرأي المطابق للمجلس.
 - إعداد وتحديث المرجعيات والإجراءات والأدلة العملية وتقديم توصيات في ميدان أمن الأنظمة المعلوماتية.
 - اعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها.
 - اعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني
 - تحديد معايير وإجراءات منح علامة الجودة و/أو التصديق و/أو اعتماد المنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية طبقاً للتشريع والتنظيم المعمول بهما
 - القيام بنشاطات التكوين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية.
- 19لأكثر تفصيل انظر مقالنا بعنوان دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، المجلد 5 ، العدد3، 2021، ص 470 وما يليها.

20 وذلك بموجب المرسوم الرئاسي 07-26 المؤرخ في 7 جانفي 2026 يتضمن إنشاء هيكل مسؤول عن أمن الأنظمة المعلوماتية وحماية المعطيات في المؤسسات والادارات والهيئات العمومية وتحديد مهامه وتنظيمه وسييره، الجريدة الرسمية عدد 04 الصادرة في 18 جانفي 2026.

21 انظر المادة 4 من المرسوم الرئاسي 07-26 السالف الذكر

22 انظر المادة 10 من المرسوم الرئاسي 07-26

23 انظر المادة 5 من المرسوم الرئاسي 07-26 المذكور سابقا.

24 مرسوم رئاسي رقم 14-252 مؤرخ في 8 سبتمبر سنة 2014 يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 الجريدة الرسمية للجمهورية الجزائرية عدد 57 / 2014.

25 لتصل الى حد حبس من عام لثلاث سنوات وغرامة بين 100000 الى 3000000 دج

26 نص على احكام تجريم هذه الافعال في قانون 04-15 المعدل لقانون العقوبات وقد رفع من حجم العقوبات بموجب القانون 24-06 المعدل لقانون العقوبات.

27 عرف قانون الاجراءات الجزائية جرائم تكنولوجيا الاعلام والاتصال في المادة 3/335 وهو نفس التعريف الذي جاء في قانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا الاعلام والاتصال، ويلاحظ على هذا القانون انه جاء بمفهوم الجرائم الاكثر تعقيدا وبالنسبة لجرائم تكنولوجيا الاعلام والاتصال تكون اكثر تعقيدا اذا

-تعدد الفاعلين او الشركاء او المتضررين

-اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامته اثارها او الاضرار المترتبة عليها

- لطابعها المنظم او العابر للحدود الوطنية

-مساسها بالنظام والامن العموميين

- تطلبها وسائل خاصة أو خبرة فنية متخصصة أو تعاون قضائي دولي

يكفي ان تتحقق احد هذه الاسباب كي تتحول الجريمة المتصلة بتكنولوجيا الاعلام والاتصال من جريمة بسيطة الى جريمة أكثر تعقيدا.

28 انظر المادة 3/78 من قانون 14-25

29 انظر الفقرة 7 من المادة 83 من قانون 14-25

30 انظر المادة 4/85 من قانون 14-25

31 انظر المادة 114 من قانون 14-25

32 لأكثر تفصيل أنظر: عبد النبي سلمى، دور القطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في مواجهة الاعتداءات الواقعة على المعطيات المعلوماتية، مجلة الحقوق والعلوم السياسية، مجلد 11، العدد 2، 2024، ص 18 وما يليها.

33 انظر المادة 335

34 أمر رقم 05-03 مؤرخ في 19 يوليو 2003 يتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية للجمهورية الجزائرية عدد 2003/44.

35 وتندرج ضمن المصنفات الرقمية كل من البرامج الحاسوب، قواعد البيانات، المصنف متعدد الوسائط، انظر في ذلك:

حواس فتيحة، حماية المصنفات المنشورة على الأنترنت، مذكرة لنيل شهادة الماجستير، كلية الحقوق، فرع الملكية الفكرية، جامعة الجزائر، 2003.

36 نصت على هذا الحق المادة 22 من أمر رقم 05-03 وهو حق محول للمؤلف أو ورثته في الكشف عن المصنف وقت ما يريد

37 يعود الحق في تعديل وتحوير أو تغيير أو حذف أو إضافة ترد على البرنامج إلى المؤلف فقط ولا يمكن إدخال تعديلات على البرنامج سواء بالتصحيح أو التعديل أو الحذف إلا بموافقة المؤلف تستثنى حالة ما إذا كانت هذه التعديلات لا تمس بسمعة أو شرف أو مصالح المؤلف طبقا لنص المادة 90 من الأمر رقم 05-03 السالف الذكر

38 وقد نص المشرع الجزائري في المادتين 52 و 53 من الأمر 05-03 على استثناءات هذا الحق، بحيث يجوز النسخ بدون إذن في الحالتين التاليتين:

الاستنساخ بغرض استعمال البرنامج للغرض الذي اكتسب من أجله، وهو متعلق بالنسخ الشخصي.

أن يكون النسخ تعويضا لنسخة مشروعة الحياة من البرنامج، مخافة من ضياعها أو إتلافها وهذا الأمر أيضا متعلق بالنسخ الشخصي.

39 المادة 150 الأمر رقم 05/03 السالف الذكر.

40 وهو ما اقره القضاء الأمريكي حيث اعتبر ان مراقبة الاتصالات الالكترونية هي تلك التي تتم عندما يتم التقاطها في

زمن البث، أما الذي يطلع على نسخة من اتصال مخزن لا يعد عمله مراقبة للاتصال بل تفتيشا، انظر في ذلك د/ سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار الكتب القانونية، مصر، 2011، ص.284.

41 لأكثر تفصيل انظر: مرتيز فاطمة، التفتيش الافتراضي كإجراء استدلاي في ضوء القانون 09 /04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات والإعلام والاتصال ومكافحتها دراسة مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، مجلد10، العدد2، 2021، ص 239 وما يليها

42 لأكثر تفصيل انظر كتابنا بعنوان، الأمن السيبراني: الجريمة السيبرانية ومكافحتها ، كوكب العلوم ، الجزائر، 2023، ص 247

43 انظر المادة2/8 من قانون رقم 05-18

44 لأكثر تفصيل أنظر المرسوم التنفيذي رقم 19-89 مؤرخ في 5 مارس سنة 2019، يحدد كفاءات حفظ سجلات المعاملات التجارية الإلكترونية وإرسالها إلى المركز الوطني للسجل التجاري.

45 انظر المادة 3/26 من قانون 05-18

46تعرف هذه التقنية بتقنية تكامل المعطيات

47 انظر المادة 9 من قانون 05-18

48دون انتظار صدور حكم قضائي

49حيث قام المشرع بتقييد النقل العابر للحدود بعد ان كان محضورا

50فتح القانون امام بنك الجزائر اصدار عملة رقمية وطنية وهذا التوجه فرض ضرورة وجود بنية تحتية تقنية فائقة الامان

51منح حجية نسبية للبيانات والوثائق الالكترونية الغير معتمدة بشرط الحفظ وامكانية العودة اليها في أي وقت