

تعزيز الأمن السيبراني كعنصر أساسي للتحويل الرقمي في القضاء الإداري *Enhancing Cybersecurity as a Fundamental Pillar of Digital Transformation in Administrative Judiciary*

الشريف وكواك

عبد النور بوهالي *

Ouakouak Cherif

Abdenmour Bouhali

مختبر السياسات العامة وتحسين الخدمة العمومية في الجزائر

Public Policy and Public Service Improvement in Algeria Laboratory

جامعة الوادي - الجزائر

University of El Oued, (Algeria)

Ouakouak-cherif@gmail.com abdenmour-bouhali@univ-eloued.dz

تاريخ النشر: 2025/12/31

تاريخ القبول للنشر: 2025/12/09

تاريخ الاستلام: 2025/10/08

ملخص:

للأمن السيبراني دور كبير في إنجاح مسار التحويل الرقمي في القضاء باعتباره ركيزة أساسية لضمان استمراره، حيث ظهرت الحاجة إلى حماية المعطيات القضائية من المخاطر السيبرانية التي تهدد سلامة الإجراءات، وثقة المتقاضين. كما أنه يساهم في تجويد الأحكام والقرارات القضائية، بحماية الأدلة الإلكترونية، والإجراءات والأحكام، واستمرارية عمل الأنظمة الرقمية. فالتحديات التي تواجه القضاء الرقمي هي ضمان أمن قواعد البيانات، والمنصات الإلكترونية، فقصور الأطر التشريعية والتنظيمية يعرقل مواكبة التطور التكنولوجي المتسارع. ولمعالجته يتطلب وضع مقاربة تجمع بين الآليات التقنية والتشريعية والتنظيمية لردع الاعتداءات السيبرانية، فالأمن السيبراني لم يعد مجرد عنصر تقني داعم للتحويل الرقمي في القضاء الإداري، بل أصبح شرطاً جوهرياً لحماية الحقوق، وضمان فعالية العدالة. والجزائر تسعى إلى تحقيق أمن سيبراني لمنظومة القضاء من خلال تصميم بنية تحتية تقنية وتشريعية قوية وفعالة.

الكلمات المفتاحية: الأمن السيبراني، التحويل الرقمي، القضاء الإداري، التشريع.

Abstract:

Cybersecurity plays a pivotal role in ensuring the success of digital transformation within the judiciary, as it constitutes a fundamental pillar for its sustainability. The need has emerged to safeguard judicial data against cyber threats that jeopardize the integrity of procedures and the

* المؤلف المراسل.

trust of litigants. Moreover, Cybersecurity contributes to enhancing the quality of judicial rulings and decisions by protecting electronic evidence, judicial procedures, and the continuity of digital systems. The challenges facing digital justice revolve mainly around securing databases and electronic platforms, as deficiencies in legislative and regulatory frameworks hinder the ability to keep pace with rapid technological advancements. Addressing these challenges requires an integrated approach that combines technical, legislative, and regulatory mechanisms to deter cyberattacks. Cybersecurity is no longer merely a supportive technical element of digital transformation in administrative justice; rather, it has become an essential condition for safeguarding rights and ensuring the effectiveness of justice. Algeria, in particular, seeks to achieve a secure judicial system by establishing a robust and efficient technical and legislative infrastructure.

Keywords: Cybersecurity, Digital Transformation, Administrative Judiciary, Legislation.

مقدمة

في إطار سياسات التحول الرقمي الذي تشهده الدول في مختلف المجالات والقطاعات، ومنها قطاع العدالة. وفي مجال القضاء الإداري الذي يهدف إلى عصنة العمليات القضائية وتجويد الأحكام الصادرة عنه، وتحسين الخدمات ورفع كفاءتها، إلا أن هذا التحول يرافقه تحديات كبيرة، أهمها المخاطر السيبرانية المتزايدة التي تهدد سلامة الأنظمة القضائية ونزاهتها. حيث أن الهجمات الإلكترونية تستهدف البنى التحتية للقطاع العام، بما فيها الأنظمة القضائية. وتشمل هذه المخاطر، الاختراق الإلكتروني للأنظمة القضائية، وتسريب البيانات الحساسة والمعلومات الشخصية للمتقاضين، تزوير المستندات والأحكام القضائية، وتعطيل الخدمات الإلكترونية للقضاء.

هذه التهديدات لا تقوض فقط سرية وسلامة البيانات والإجراءات القضائية، بل تضعف ثقة المتقاضين في النظام القضائي الرقمي، مما يعرض مشاريع العصرية وتحسين الجودة للخطر. فبحسب تقرير صادر عن الوكالة الأوروبية للأمن السيبراني (ENISA) تسبب الهجمات الإلكترونية خسائر تقدر بـ 10.5 تريليون دولار سنوياً بحلول سنة 2025، مع ارتفاع ملحوظ في الهجمات المستهدفة للقطاع العام¹.

يواجه القضاء الإداري في عصر التحول الرقمي كما هو الحال في باقي القطاعات الأخرى، مجموعة من التهديدات السيبرانية الفريدة والمتخصصة، والتي تختلف في طبيعتها عن تلك التي

تواجهها المؤسسات الأخرى. فبينما تستهدف الهجمات التقليدية البيانات المالية أو المعلومات الشخصية، فإن الهجمات على القضاء الإداري تهدف إلى تقويض أسس العدالة والنظام القانوني نفسه. ومن أبرز هذه التهديدات هجمات تعطيل والحرمان من الخدمة (DDoS) التي تهدف إلى تعطيل سير العمل القضائي وإبطاء التقاضي، مما يناقض مبدأ سرية الفصل في الدعاوى الإدارية، واختراق قواعد البيانات القضائية والتلاعب في الأحكام والسجلات القضائية، وهو ما يهدد مبدأ نزاهة الوثائق القضائية الذي يشكل عماد الثقة في القضاء²، وهجمات التصيد الاحتمالي المتخصصة التي تستهدف القضاة وموظفي القضاء الإداري للوصول إلى المعلومات السرية الخاصة بالقضايا، وهو ما يشكل انتهاكا لمبدأ سرية العمل القضائي للعديد من الدول³.

وبناء على ما سبق ذكره نطرح الإشكالية التالية:

ما مدى إمكانية تعزيز الأمن السيبراني باعتباره عنصرا محوريا في مسار التحول الرقمي للقضاء، وضمانه كآلية عملية لتحقيق مقاصده، فنجاح هذا التحول يظل رهينا بقدرة المنظومة القضائية على حماية بياناتها ومعطياتها الرقمية من المخاطر السيبرانية التي تهدد الثقة في العدالة، كما أن قصور الأطر التشريعية والتنظيمية إذا لم تتم معالجته بفعالية، قد يقف عائقا أمام بلوغ الأهداف المرسومة للتحول الرقمي في القضاء الإداري؟

تمت الدراسة بالاعتماد على المنهج الوصفي التحليلي كأداة رئيسية لوصف وتحليل واقع الأمن السيبراني وتحدياته في بيئة القضاء الإداري الرقمي. الذي يتيح فهم الظاهرة المدروسة من خلال جمع البيانات والمعلومات الدقيقة عنها، وتحليلها لتحديد العلاقة بين متغيراتها المختلفة. حيث تهدف الدراسة إلى:

- ✓ تحليل مفهوم الأمن السيبراني وعلاقته بالتحول الرقمي في القضاء الإداري.
- ✓ تقييم المخاطر السيبرانية النوعية المهددة للعمل القضائي الرقمي.
- ✓ تحليل المعايير والممارسات الدولية والإقليمية في مجال أمن القضاء الرقمي.
- ✓ تحديد الآليات العملية لتعزيز الأمن السيبراني كعامل تمكين للتحول الرقمي الفعال والأمن في القضاء الإداري.

انطلاقا من الفرضيات المطروحة في الإشكالية تم انتاج خطة عمل مقسمة إلى مبحثين:

- المبحث الأول: الإطار المفاهيمي للأمن السيبراني والعلاقة العضوية التي تربطه بالتحول الرقمي في القضاء الإداري.

● المبحث الثاني: آليات تعزيز الأمن السيبراني في القضاء الإداري الرقمي، المعايير والتطبيق.

المبحث الأول

الإطار المفاهيمي للأمن السيبراني والعلاقة العضوية بالتحول الرقمي في القضاء الإداري

يعد الأمن السيبراني في العصر الرقمي حجر الزاوية لضمان استمرارية الأنظمة الإلكترونية وحماية المعطيات الحساسة، وهو ما يجعله مرتبطاً عضوياً بالتحول الرقمي في مختلف القطاعات، وعلى رأسها القضاء الإداري الذي يعتمد بشكل متزايد على الوسائل التكنولوجية في إدارة الدعاوى والفصل فيها. فبينما يهدف التحول الرقمي إلى تحديث البنية القضائية عبر توظيف التقنيات الحديثة لتسريع الإجراءات وتعزيز الشفافية، يبرز الأمن السيبراني كضمانة أساسية لصيانة هذه المكاسب من التهديدات السيبرانية. ومن ثم، فإن فهم الإطار المفاهيمي للأمن السيبراني وعلاقته العضوية بالتحول الرقمي في القضاء الإداري يشكل مدخلاً ضرورياً لتقييم فعالية هذا التحول، ومدى قدرته على تحقيق عدالة إدارية آمنة، حديثة، وذات موثوقية عالية، حيث نتطرق في هذا المبحث إلى المفاهيم الأساسية والعلاقة التكاملية للأمن السيبراني والتحول الرقمي الذي يعتبر ركيزة لتحول رقمي فعال وآمن.

المطلب الأول: المفاهيم الأساسية والعلاقة التكاملية للأمن السيبراني والتحول الرقمي

يظل تحقيق التكامل الفعال بين الأمن السيبراني والتحول الرقمي في القضاء الإداري تحدياً معقداً يتطلب مقاربة شاملة تجمع بين الجوانب التقنية والقانونية والبشرية. ومن خلال تبني الإطار المقترح في هذا التحليل، يمكن للقضاء الإداري أن يحقق التحول الرقمي المنشود مع الحفاظ على أمن وسلامة بياناته، حيث نبين مفهوم التحول الرقمي في القضاء الإداري وأهدافه، والأمن السيبراني وأبعاده الأساسية.

الفرع الأول: مفهوم التحول الرقمي في القضاء الإداري وأهدافه

1. تعريف التحول الرقمي في القضاء الإداري: التحول الرقمي هو أحد المفاهيم المحورية الناتجة عن التطورات المتسارعة في مجال التكنولوجيا الحديثة، لاسيما في ظل ما يعرف بالثورة الصناعية الرابعة، وهذا التحول غير المجتمع بشكل كبير كما هو الحال لما حدث في الثورة الصناعية في القرن التاسع عشر الميلادي⁴.

يقصد بالتحول الرقمي في القضاء الإداري تبني التقنيات الرقمية لتحسين كفاءة الخدمات القضائية وضمان استمرارية الأعمال في بيئة رقمية تتطور باستمرار⁵. ويشمل تحولاً شاملاً في العمليات والإجراءات القضائية من الشكل التقليدي إلى الشكل الرقمي، لضمان تجويد خدماته وتحقيق العدالة الإدارية من خلال تحقيق السرعة والشفافية المطلوبة مع الحفاظ على المبادئ الأساسية للعدالة والنظام القانوني.

2. أهداف التحول الرقمي في القضاء الإداري: يسعى التحول الرقمي في القضاء الإداري إلى تحقيق عدة أهداف رئيسية:

- أ- تحسين كفاءة الخدمات القضائية من خلال أتمتة العمليات والإجراءات⁶.
- ب- تعزيز الشفافية والنزاهة في العمل القضائي من خلال توثيق الإجراءات رقمياً⁷.
- ج- ضمان استمرارية العمل القضائي حتى في الظروف الطارئة مثل ما حدث في جائحة كورونا⁸.
- د- تجويد الأحكام القضائية من خلال توفير خدمات قضائية رقمية سريعة وميسرة للمتقاضين⁹.

الفرع الثاني: مفهوم الأمن السيبراني وأبعاده الأساسية

1. التعريف القانوني والمفاهيمي للأمن السيبراني: يعرف الأمن السيبراني وفقاً للقانون الأردني رقم (16) لسنة 2019 بأنه تلك الإجراءات التي يجب القيام بها والتي تهدف إلى حماية البنى التحتية للشبكات والأنظمة المعلوماتية من أخطار الأمن السيبراني، وكذلك والقدرة على إعادة تشغيلها في حالة تعرضها لهجوم سيبراني، والمحافظة على استمرار نشاطها، وتأمينها من سوء الاستخدام ومن اختراقها أو نتيجة الفشل في اتباع إجراءات الحماية والأمن أو تعرضها لأي تشويش مخادع¹⁰.

أما القانون المغربي رقم 05-20 المتعلق بالأمن السيبراني، بأنه مجموع التدابير والأعمال المتخذة ومفاهيم الأمن سبل إدارة المخاطر والتدريبات والتكوينات وأحسن الممارسات، والتقنيات التي تسمح لنظام المعلومات بمقاومة الأحداث المرتبطة بحماية الفضاء السيبراني¹¹.

عندما نذكر الأمن السيبراني نتكلم عن مجموعة من الإجراءات المتبعة لحماية الأنظمة والشبكات والبنى التحتية من الهجمات السيبرانية، ومنع الدخول غير المصرح به أو سوء

الاستخدام، ويعني أيضا استعادة العمل إذا فشلت إحدى الإجراءات المتخذة، أو تعرض للخداع أو الاختراق، ولكن بالإمكان أن يؤدي هذا إلى فقدان الثقة الكاملة في هذا النظام.

من ناحية المفهوم، يشمل الأمن السيبراني جملة المهام والأدوات والطرق والاستراتيجيات والمبادئ والإجراءات الأمنية والمبادئ التوجيهية والمقاربات الخاصة بإدارة المخاطر، والتدريبات والممارسات المثلى والتكنولوجيا التي يكون في مقدورها أن تواجه وتحمي البيئة السيبرانية وموجودات المؤسسات والمستخدمين¹².

2. الأبعاد الأساسية للأمن السيبراني: يحتوي الأمن السيبراني على أبعاد أساسية تشكل الأسس الرئيسية لحماية الأنظمة الرقمية، ومن أبرزها¹³:

أ- البعد الوقائي الذي يشمل التدابير الاستباقية لمنع الوصول غير المصرح به وإفشال الاختراقات المحتملة، مثل جدران الحماية وأنظمة كشف التسلل.

ب- البعد الكشفى المتعلق برصد التهديدات المحتملة ومراكز الضعف داخل النظام من خلال أدوات المراقبة المتقدمة وأنظمة كشف الاختراق.

ج- البعد العلاجي المتمثل في اتخاذ الإجراءات الضرورية لاحتواء حوادث الاختراق الأمني، استرجاع الأنظمة المتأثرة به وإعادة وضعها في حالة عمل.

المطلب الثاني: الأمن السيبراني ركيزة لتحول رقمي فعال وآمن

في ظل تسارع عملية التحول الرقمي، أضحت الأمن السيبراني أكثر من مجرد أداة تقنية، بل هو ضرورة استراتيجية لضمان نجاح التحول الرقمي في القضاء. وعلى ضوء ذلك، فإن أي تحول رقمي في عمل مرفق القضاء يجب أن يكون محمي بشبكة من الأمن السيبراني، انطلاقا من بنية تحتية تشمل قاعدة رقمية وتشريعية تساهم في أمن وسلامة المعطيات، وتضمن سرية البيانات والحياة والحرية الخاصة لمستخدمي مرفق القضاء¹⁴. سنعالج في هذا المطلب، متطلبات الأمن السيبراني كعنصر أساسيا للتحول الرقمي في القضاء، وتعزيز الأمن السيبراني لأهداف التحول الرقمي.

الفرع الأول: متطلبات الأمن السيبراني كعنصر أساسيا للتحول الرقمي في القضاء

1. المتطلبات التقنية لحماية المعطيات والبيانات الرقمية: محدودية الوصول إلى بعض قواعد البيانات القومية أو إتاحتها بشكل محدود مثل حماية مصالح الأمن القومي أو الخصوصية الشخصية أو الحفاظ على الملكية الفكرية على سبيل المثال، أو تطبيق التشريعات الوطنية للحصول على هذه

البيانات وإزالة القيود غير الضرورية¹⁵. كما هو الحال بالنسبة للجانب القضائي تحديد الولوج إلى قواعد البيانات للمعطيات الخاصة بالمتقاضين أو الأحكام والقرارات الصادرة عن المحاكم والمجالس، والمحاكم الإدارية ومحاكم الاستئناف أو المحكمة العليا ومجلس الدولة، لحماية أمن وسرية المعلومات، بتطبيق أطر عمل معيارية مثل إطار للأمن السيبراني ISO 27001 لأنظمة إدارة أمن المعلومات¹⁶.

كما أن استخدام تقنيات متقدمة يمكنها كشف التهديدات في وقت زمني قصير، ولها استجابة دفاعية سريعة تقلل من الهجمات الإلكترونية للمنظومة الرقمية¹⁷. واستخدام نظم التشفير المتقدمة خصوصا مع التقنيات المتطورة للحوسبة الكمومية التي تهدد نظام الشفرة التقليدية¹⁸. يشير دليل "Cybersecurity Basics for Courts" الصادر عن اللجنة التقنية المشتركة بالتعاون مع NCSC وConférence of State Court Administrators إلى أن القضاء يجب أن ينشئ فرق استجابة للحوادث دورها تقييم مخاطر الأنظمة بالنظام، وتفعيل آليات الاستجابة السريعة عند وقوع خروقات سيبرانية¹⁹.

إضافة إلى ذلك يجب على القضاء أن يدمج آليات الكشف المبكر عن الولوج غير المصرح به إلى النظام الرقمي، فمن غير هذه الآليات، قد يبقى النظام معرض لاختراقات بطيئة كالهجمات التي تثبت نفسها تدريجيا داخل الشبكة الرقمية ويصعب اكتشافها حالا، حيث أنه لا يكفي تحويل إجراءات التقاضي إلى شكل إلكتروني، بل يجب أن تنشأ بنية تحتية تقنية تضمن سلامة هذه الإجراءات في جميع مراحلها.

2. المتطلبات التشريعية: لا يمكن أن يكون للتحويل الرقمي القضائي فعالية إن لم تؤطره تشريعات تحمي البيانات، وتجرم انتهاكات الأمن السيبراني ويعاقب عليه القانون. تعد اتفاقية بودابست لمكافحة الجريمة المعلوماتية (Budapest Convention on Cybercrime) لمكافحة الاختراق، والتجسس الرقمي، ومسائل الأدلة الإلكترونية²⁰، وللتعاون الدولي في هذا المجال إطارا قانونيا يمكن للدول التي تراعيه أن تدججه ضمن تشريعاتها الوطنية لتأمين البيئة الرقمية القضائية. على مستوى القارة الإفريقية تعتبر اتفاقية مالابو للأمن السيبراني، مرجعية إقليمية، حيث دعت الدول الأعضاء إلى وضع أطر تنظيمية تهدف إلى حماية البيانات الشخصية وتعزيز البنى القانونية لمكافحة الجرائم الإلكترونية²¹.

وعلى الصعيد الوطني، على الدولة وضع تشريعات خاصة بالأمن السيبراني أو تضمين قانون العقوبات فصولاً متخصصة تجرم الوصول غير المرخص إلى أنظمة المعلومات، والاستغلال غير المشروع للبيانات، أو التجسس على المعطيات القضائية، وتحدد العقوبات الرادعة لكل فعل مجرم، على غرار، القانون رقم 09 - 04 مؤرخ 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها²²، القانون رقم 18-04 المؤرخ في 10 مايو، 2018 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية²³، والقانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي²⁴.

إن تطوير أطر قانونية لحماية البيانات الرقمية الشخصية العادية كالاسم واللقب، العمر ورقم الهاتف²⁵، أو الحساسية كالبيانات المتعلقة بالصحة النفسية أو الجسمية أو البيانات الجينية أو البيومترية²⁶، أو البيانات والمعلومات المالية أو الانتماءات والآراء السياسية، أو الحالة الأمنية أو المعتقدات الدينية للأشخاص²⁷، ومنع الاطلاع عليها إلا برخصة من مركز حماية البيانات الشخصية، وبموافقة الشخص المعنى الحامل لهذه البيانات. كما يجب إنشاء آليات خاصة بمراقبة تنفيذ معايير الأمن السيبراني.

فالتشريع القويم يعطي الإطار القانوني الذي يجبر الجهات القضائية ويخلق التوازن بين الحق في الوصول إلى العدالة وحق المتقاضين في الحماية الرقمية.

3. المتطلبات التنظيمية: إلى جانب المتطلبات التقنية والتشريعية، لا بد للقضاء الرقمي أن يتوفر على مجموعة من الضوابط التنظيمية التي تشغل الهيئات القضائية بآليات ملموسة لدعم الأمن السيبراني نذكر منها:

أ- إنشاء دائرة مركزية متخصصة في الأمن السيبراني داخل الجهاز القضائي، تعمل على مراقبة النظام السيبراني، وإدارة الحوادث، وتقوم بالتنسيق مع الجهات الأمنية الوطنية لحماية وصد أي اختراق سيبراني، وتحدد المعايير والتوجيهات الفنية والقانونية داخل المؤسسة القضائية²⁸.

ب- وضع إجراءات صارمة تنظم الصلاحيات، وحقوق النفاذ، وتدابير السرية، وإجراءات التدخل في حالة وجود اختراق²⁹.

ج- التكوين التقني والنفسي الدوري والمستمر للقضاة وموظفي المنظومة الرقمية في الجهاز القضائي، لتمكينهم من الاحاطة بمبادئ الأمن المعلوماتي، وبالخطر السيبراني، وطرق التصدي له

مثل تجنب الوقوع في فخ التصيد أو استخدام كلمات مرور غير آمنة، هذا التدريب يعتبر عاملاً محوري للحد من الثغرات البشرية التي كثيراً ما يستغلها المهاجمون³⁰.

د- إنشاء آليات الرقابة والتدقيق المستقل على نظم الأمان داخل الجهات القضائية، مهمتها العمل على التقييم الدوري لاكتشاف نقاط الضعف، والتأكد من الالتزام بالمعايير بحياد والمصادقية³¹.

هـ- وضع خطة، تكون جاهزة للتفعيل لحماية استمرار العمل القضائي في مواجهة الهجمات السيبرانية أو الأعطال الكبرى، على سبيل المثال، توفير نسخ احتياطية في مواقع موازية، آليات استعادة النظام، ونماذج بديلة لتسيير العمل إذا تعطل النظام الرقمي الأصلي، إضافة إلى الشراكة والتنسيق مع الجهات الأمنية الوطنية، والمؤسسات المختصة في الأمن السيبراني مثل وكالات الأمن السيبراني، لتبادل المعلومات والتحذيرات الأمنية، والتعاون في التحقيق عند وقوع اختراق³². بفضل هذه المتطلبات التنظيمية، يكون الجهاز القضائي قادراً على ترجمة النصوص التقنية والتشريعية إلى واقع ملموس يحمي النظام الرقمي ويعزز قدرته على الصمود أمام التحديات السيبرانية.

الفرع الثاني: تعزيز الأمن السيبراني لأهداف التحول الرقمي

الأمن السيبراني ليس غاية بحد ذاته، بل هو وسيلة ضرورية لتحقيق أهداف التحول الرقمي في القضاء الإداري، وهي مكاملة لضمان عمل النظام الرقمي بكفاءة وبمصادقية، وبما يحفظ الحقوق والالتزامات القانونية لجميع الأطراف. وفيما يلي نسلط الضوء على كيفية مساهمة الأمن السيبراني في تحقيق هذه الأهداف:

1. يعزز من جودة القرارات القضائية الرقمية: الأمن السيبراني يعزز من جودة القرارات القضائية الرقمية من خلال ضمان أن المعلومات التي تستخدم كدليل لم يعبث بها، وأن وثائق الإثبات محمية بالكامل من لحظة جمع الأدلة حتى عرضها أمام المحكمة³³؛ الجودة تعني أدلة دقيقة، ونظام معلومات موثوق، وتكنولوجيا تساعد في تحليل القضايا بكفاءة وأمان.
2. ضمان صحة الأدلة الرقمية: أحد الأهداف الأساسية لأي نظام قضائي رقمي هو أن تقبل الأدلة الرقمية أمام القضاء كأدلة موثوقة، أي أنها حقيقية (authentic)، كاملة (complete)، ودقيقة (accurate)، وخاضعة لآليات لمنع التلاعب أو التزيف أو

الضياح. الأمن السيبراني يوفر آليات التوقيع الرقمي، الأختام الزمنية (timestamping)، وسجل الوصول والتعديل، وتكنولوجيا التشفير، لضمان هذه الشروط³⁴.

3. سرية المداولات: في القضاء الإداري كما في غيره، هناك جلسات تحقيق أو مداولات لا يجب أن تعرض إلا لأهلها، أو معلومات لا يحق نشرها إلا بعد صدور الحكم أو وفق إجراءات قانونية. الأمن السيبراني يوفر الحماية لهذه السرية من خلال التشفير، والأذونات (permissions)، والتقسيم المنطقي للشبكات، وسياسات سرية ملزمة قانونياً. هذا يضمن أن المداولات لا تتعرض للتفتيش أو الوصول غير المصرح به³⁵.

4. حماية النزاهة الإجرائية: النزاهة الإجرائية تعني أن كل إجراء قانوني يتم وفقاً للمعايير القانونية المقررة، وألا يكون هناك تحيز أو تلاعب، وأن يكون الوصول إلى العدالة متاحاً على قدم المساواة. الأمن السيبراني يجعل الإجراءات الرقمية شفافة وقابلة للتدقيق، ويسجل كل نشاط ضمن النظام مما يمنع التلاعب، أو التغيير في الأحكام الرقمية، ويوفر إمكانية مراجعة شاملة³⁶.

5. ضمان توفر الأنظمة: كباقي الأنظمة يحتاج النظام القضائي الرقمي إلى أن يكون متاحاً باستمرار للمستخدمين والمتقاضين، والقضاة، والموظفين المؤهلين. توفر الأنظمة (availability) يعني أن المنصات الإلكترونية، أنظمة إدارة القضايا، بوابات المرافعة الإلكترونية، وأنظمة الأرشفة الرقمية تعمل دون انقطاع أو مع انقطاع محدود وخطة استعادة فورية. الأمن السيبراني يدعم ذلك عبر حماية ضد هجمات الحرمان من الخدمة (DDoS)، صيانة خطط التعافي من الكوارث، نسخ احتياطية آمنة، واستراتيجيات توزيع الخطر³⁷.

يشكل الأمن السيبراني ركيزة أساسية لضمان نجاح التحويل الرقمي في القضاء الإداري، إذ لا يقتصر دوره على حماية البيانات والأنظمة، بل يتجاوز ذلك ليعزز جودة الأحكام الرقمية، ويكفل صحة الأدلة، ويحافظ على سرية المداولات، ويضمن النزاهة الإجرائية واستمرارية عمل المنصات القضائية. ومن ثم، فإن تحقيق عصريّة القضاء الإداري وجودة خدماته مرهون بمدى صلابة البنية السيبرانية التي تؤطره وتؤمنه ضد مختلف المخاطر والتحديات.

المبحث الثاني:

آليات تعزيز الأمن السيبراني في القضاء الإداري الرقمي المعايير والتطبيق

لتعزيز الأمن السيبراني وضع مركز "بلفر" عدة أهداف رئيسية تسعى كل الدول إلى تحقيقها لحماية أمنها السيبراني، بعضها قد ينطوي على انتهاكات لحقوق الإنسان أو يشكل تهديدا للنظام الدولي، وبدلا من دعم السلام والأمن الدوليين، قد تؤدي هذه الأهداف إلى تقويض الاستقرار العالمي، وتشمل مراقبة المجموعات المحلية إلكترونيا من أفراد وجاعات، تحت دريعة حماية الأمن القومي، بجمع المعلومات الاستخبارية عن التهديدات المحلية واكتشاف الأنشطة المحتملة. تقوية الدفاعات السيبرانية داخل الدولة، بتقوية الأنظمة الدفاعية للبنية التحتية لمؤسساتها الوطنية. التحكم في بيئة المعلومات بالتحكم في تدفقها داخليا وخارجيا باستخدام الوسائل الإلكترونية، مع محاولة التوفيق بين حماية خصوصية الإنترنت وحرية التعبير للمواطنين.

جمع المعلومات الاستخبارية الإلكترونية من دول أخرى من خصوم أجنب عن طريق اختراق الاتصالات أو سرقة ملفات حساسة في مختلف المجالات.

تحقيق مكاسب تجارية وصناعة وتنمية محلية باستخدام الأنشطة السيبرانية لتطوير الصناعات المحلية، بالطرق المشروعة أو غير المشروعة، كالنحسس الصناعي لنقل التكنولوجيا من الشركات الأجنبية. تخطيم أو تعطيل البنية التحتية للخصم باللجوء إلى استخدام تقنيات إلكترونية مدمرة لإضعاف قدراته في المجالات السيبرانية أو التقليدية. وضع معايير إلكترونية دولية، حيث تساهم الدول في صياغتها تقنيا وقانونيا من خلال المشاركة في التحضيرات والمناقشات، وهو الهدف الأكثر مثالية لتعزيز السلام والأمن الدوليين³⁸.

حتى ينتقل القضاء الإداري إلى قالب رقمي آمن وفعال، لا بد من تفعيل آليات سيبرانية عملية وفعالة، ومعايير واضحة تترجم إلى ممارسات على أرض الواقع داخل الأجهزة القضائية. سنتناول في هذا المبحث، الأخطار السيبرانية المحيطة بالقضاء الإداري الرقمي، والإطار التشريعي والتنظيمي لتعزيز الأمن السيبراني في القضاء الإداري العربي والجزائري.

المطلب الأول: الأخطار السيبرانية المحيطة بالقضاء الإداري الرقمي

تعد المنظومة القضائية الرقمية، لاسيما في ميدان القضاء الإداري، من الأهداف الحساسة للهجمات السيبرانية لما تحتوي عليه من بيانات موثوقة تخص جهاز القضاء والمتقاضين، ومن استحقاقات قانونية، حق الوصول السريع إلى العدالة. حيث أن هذه الهجمات يكون هدفها سرقة المعطيات أو تزوير الأحكام والقرارات القضائية، أو تعطيل القضايا والإضرار بمصالح المتقاضين، أو تعطيل مرفق القضاء، وبالتالي خلق عدم الأمن والاستقرار القضائي. تنطرق في هذا المطب

إلى، استهداف قواعد البيانات وسرقة المعلومات أو التشويش عليها، والآليات العملية لحماية البيانات الرقمية للقضاء الإداري من الهجمات السيبرانية.

الفرع الأول: استهداف قواعد البيانات وسرقة المعلومات أو التشويش عليها

تعتبر من أخطر العمليات التي تمكن المهاجمين من الوصول غير المرخص إلى قواعد معطيات القضاء، وسرقة الوثائق القضائية، أو ملفات المتقاضين، أو المراسلات الإلكترونية، ما يفتح الباب أمام الابتزاز، أو الكشف عن أسرار المرافعات، أو تسريب معلومات حساسة قبل صدور الأحكام ما يؤثر سلباً على سرية القضايا ومصداقية النظام القضائي³⁹.

كما قد تلجأ بعض الجهات إلى زرع برمجيات خبيثة داخل أنظمة القضاء الرقمي، أو استخدام هجمات الفدية التي تقوم بقفل وتشفير غير مرخص لملفات، وبالتالي طلب فدية مقابل فك التشفير. هذا النوع من الهجمات يمكن أن يشل النظام القضائي ويمنع القضاة من الوصول إلى الدعاوى المرفوعة من طرف المتقاضين والوثائق التي تحتوي على الأدلة⁴⁰. حيث ينبغي على المحاكم أن تكون على استعداد لهجمات الفدية، من خلال القيام بإنشاء نسخ احتياطية مؤمنة ووضع خطط الاستجابة للحوادث الطارئة.

التصيد الاجتماعي الذي يستهدف فيه المهاجمون المورد البشري، من قضاة وموظفي القضاء، عبر رسائل بريد إلكتروني تستدرجهم للإفصاح عن بيانات دخول النظام. هذه الهجمات تعكس أن الثغرة الأهم قد تكون العنصر البشري، لا التقنية وحدها، يعتبر التصيد من الأساليب الأكثر استخداماً للوصول إلى معلومات قضائية حساسة، خصوصاً حينما يتم خداع الموظف أو الشخص المرتبط بالقضية⁴¹.

كما يمكن للمهاجم الختلق لنظام القضاء دون أن يسرق البيانات، فإنه قد يغير في الأدلة أو يدخل بيانات مزيفة، أو يحرف تواريخ التعديلات، مما يضعف قبول الوثائق الرقمية أمام القضاء ويهدد نزاهة الأحكام⁴². ويمكن له توجيه هجوم على الخادم الرقمي حيث يغرقه بطلبات ضخمة تتسبب في تعطيل الوصول إلى منصة المرافعة الإلكترونية أو نظام إدارة القضايا، الشيء الذي يؤدي إلى عرقلة مواعيد الجلسات أو تعطيل التواصل القضائي هذا ما يطلق عليه بهجمات الحرمان من الخدمة. وكذلك على ذلك، واجهت محكمة ولاية بنسلفانيا بالولايات المتحدة الأمريكية هجوم تعطيل الخدمة على موقعها القضائي، مما أثر سلباً على الوصول إلى الدعاوى الإلكترونية⁴³.

وقد يكون التهديد من داخل الجهاز القضائي نفسه، بسبب موظف له صلاحيات قد يستغلها عمداً أو عن طريق الخطأ بطريقة تهدد أمن المعلومات والبيانات القضائية، حيث يصعب اكتشاف هذا النوع من التهديدات، وعواقبه غالباً ما تكون أخطر من الهجمات الخارجية. إن البنى التحتية القديمة أو البرمجيات التي لم يتم تحديثها بصفة دورية تجعل ثغرات في منظومة القضاء تكون عرضة لكثير من الهجمات التي تستغل نقاط ضعف في أنظمة قديمة لا تتلقى تحديثات أمنية حديثة. حيث أشارت بعض التقارير الإعلامية أن النظام القضائي الفيدرالي في الولايات المتحدة الأمريكية استخدم كنقطة اختراق بسبب أن بعض الأنظمة كانت قديمة وغير محدثة.⁴⁴

يمكن أن تنطلق الهجمات السيبرانية من خارج حدود الدولة أو عن طريق شبكات دولية، مما يطرح مسائل قانونية حول الاختصاص، وتنفيذ الأحكام، والتعاون بين الدول لملاحقة المهاجمين، حيث تثار أبعاد الاختصاص القانوني عند هجمات تطل أنظمة مشتركة عبر الدول، وكيف تتدخل التشريعات المحلية والدولية لمعالجتها، وهو ما يصطلح عليه بتعدد الاختصاصات ومسائل القضاء العابر للحدود.⁴⁵

الفرع الثاني: الآليات العملية لحماية البيانات الرقمية للقضاء الإداري من الهجمات السيبرانية

1. آلية تشفير البيانات القضائية أثناء عملية النقل والتخزين: القيام بعملية التشفير لكل البيانات الحساسة أثناء نقلها سواء بين المستخدمين والخوادم الرقمية أو أثناء تخزينها في قواعد البيانات وأرشفتها. حيث يجب استعمال تشفير قوي باستخدام خوارزميات حديثة مع إدارة مفاتيح مؤمنة تحمي من الولوج غير المصرح به، ويكون هذا التشفير كدليل مقبول على سرية الوثائق الرقمية عند القيام بالطعن أو حماية الخصوصية.⁴⁶

2. اعتماد مصادقة إلكترونية متعددة العوامل: تعتمد مصادقة متعددة العوامل (Multi-factor authentication) للمستخدمين ذوي الصلاحيات كالقضاة، المحامون، والموظفون الذين يتعاملون مع البيانات القضائية، الشيء الذي يقلل من مخاطر الولوج غير المصرح به إلى قاعدة البيانات حتى إذا تم تسريب كلمات المرور. كما يجب تبني سياسات إدارة هويات مركزية (Identity & Access) تركز على مبادئ أقل صلاحية ممكنة وسجلات تفويض دقيقة.⁴⁷

3. آلية الفصل بين الشبكات وتصميم بنية تعتمد على صفر ثقة: تقسيم الشبكة (network segmentation) وفصل بيئات الموظفين في المحاكم عن خوادم القضايا

والأرشفة، واعتماد طريقة صفر ثقة (Zero Trust) الذي يطلب تحققاً مستمراً قبل السماح للمستخدم بالدخول إلى أي شبكة، هذا ما يمنع من قدرة المهاجم السيرياني على الانتشار داخل جهاز القضاء إذا تمكن من اختراق نقطة معينة⁴⁸، استراتيجية آلية الفصل بين الشبكات، وتصميم بنية تعتمد على صفر ثقة تخفض نطاق الضرر وتسهل الاستجابة السريعة للتصدي للاختراق السيرياني.

4. مراقبة التسجيلات (logging) وأنظمة الكشف: تفعيل نظام التسجيلات (system/application logs) بجميع وسائلها، بالفيديو، الأوديو أو أي نوع آخر، وتحليلها مع أنظمة كشف منع التسلسل، يمكن من خلالها رصد أنماط النفاذ الشاذة واكتشاف الحوادث مبكراً، فالتسجيلات الجيدة لا يقتصر دورها على الاكتشاف فقط، بل تعد دليلاً رئيسياً في التحقيق الجنائي الرقمي⁴⁹.

5. آلية إنشاء نسخ احتياطية مشفرة: يعتبر إنشاء نسخ دورية احتياطية مع تشفيرها، آلية منتظمة لعمليات الاستعادة (recovery drills)، تضمن بواسطتها استمرارية العمل القضائي عند حدوث أعطال البنية التحتية، أو هجمات الفدية. حيث يجب توثيق إجراءات استعادة البيانات واختبارها بانتظام وإدراجها ضمن خطة استمرارية أعمال الجهاز القضائي⁵⁰.

6. آليات حفظ الأدلة وسلسلة الحماية الرقمية: إنشاء بروتوكولات مشددة لاستلام، توثيق، تأمين ونقل الأدلة الرقمية يضمن قبوليتها أمام القضاء، هذه الإجراءات تتضمن توثيقاً زمنياً دقيقاً، نسخاً مؤمنة، وطرقاً واضحة لحفظ وإثبات عدم التلاعب بالأدلة. كذلك من الضروري تدريب فرق الاستجابة الرقمية للحفاظ على أثر الدليل⁵¹.

7. آلية الاختبار الدوري للاختراق وتقييم الثغرات الأمنية: القيام بإجراء اختبارات اختراق مجدولة وفحص نقاط ضعف تقنية والاستجابة لتقاريرها، مع معالجة الثغرات ضمن أطر زمنية محددة، يساعد في تقليل المساحات الهجومية والاستعداد لهجمات متقدمة. ويفضل أيضاً إسنادها إلى مختصين خارجيين مستقلين لضمان حياد التقييم⁵².

8. التكوين والتوعية والتدريب المستمر للقضاة والموظفين: تخطط برامج تدريب منهجية تركز على مخاطر الهندسة الاجتماعية (phishing)، إدارة كلمات السر، التعامل الآمن مع المرفقات والوسائط، وإجراءات الاستجابة للحوادث؛ لأن العنصر البشري غالباً هو الحلقة الأضعف. كما يجب أن يتضمن التدريب على أحداث عملية قريبة للواقع ومحاكاتها دورياً⁵³.

9. وضع قوانين وسياسات داخلية واضحة للتبليغ والامتثال وحماية البيانات: يعتبر التبليغ عن المخروقات من الواجبات الأساسية وقواعد الامتثال لحماية المعطيات الشخصية، وضوابط قانونية للتعامل مع البيانات القضائية متمثلة في (مدة الاحتفاظ، شروط النشر، حق الوصول)، يوفر ضامنا قانونيا للتدابير التقنية ويحد من التجاوزات. ووجود سياسات معلنة يزيد من الشفافية والمسؤولية ويسهل التعاون مع أجهزة التحقيق عند حوادث سببرانية⁵⁴.
إن تطبيق هذه الآليات يمثل مجموعة متكاملة من عناصر تقنية، تنظيمية، وتشريعية. عندما تدمج هذه الآليات داخل استراتيجية متماسكة مع إدارة مخاطر واضحة (risk management)، يصبح القضاء الإداري الرقمي قادرا على حماية بياناته الحساسة، الحفاظ على نزاهة الإجراءات، وضمان استمرار تقديم خدمات قضائية ذات جودة عالية، وله القدرة على مواجهة التهديدات السببرانية المحتملة.

المطلب الثاني: الإطار التشريعي والتنظيمي لتعزيز الأمن السببراني في القضاء الإداري العربي

أصبح الأمن السببراني في عصر التحول الرقمي مطلبا تشريعيا وتنظيميا لا يقل أهمية عن كونه بنية تقنية، خاصة في مرفق القضاء الإداري الذي يعد ضامنا لشرعية أعمال الإدارة وحامي الحقوق والحريات. وإذا كان البعد التقني يشكل خط الدفاع الأول ضد التهديدات السببرانية، فإن المنظومة القانونية هي التي تمنح هذا الدفاع طابعا إلزاميا وشرعية مؤسسية.
ومن هنا برزت الحاجة إلى بناء إطار تشريعي وتنظيمي متكامل في الدول العربية، والجزائر على وجه الخصوص، يواكب التطورات التكنولوجية ويؤسس لآليات حماية البيانات القضائية، وضمان أمن المنصات الرقمية، ويحقق التوازن بين متطلبات النجاعة القضائية وحماية الحقوق الأساسية للأفراد.

ويثار التساؤل حول مدى كفاية النصوص التشريعية والتنظيمية المعتمدة في العالم العربي والجزائر لمواجهة المخاطر السببرانية، وقدرتها على دعم التحول الرقمي للقضاء الإداري وضمان استمراريته بثقة وشفافية. تشمل دراسة هذا المطلب على المرجعيات التشريعية والتنظيمية للأمن السببراني لبعض الدول العربية، والإطار القانوني والتنظيمي الجزائري.

الفرع الأول: المرجعيات التشريعية والتنظيمية للأمن السببراني لبعض الدول العربية

نظرا لما وصلت إليه مخاطر الأمن السيبراني، فإن المنظومات القضائية في الدول العربية مطالبة بتكييف تشريعاتها مع التحديات الرقمية الجديدة. وقد خطت بعض الدول العربية خطى نسبية معتبرة في هذا المجال:

1. دولة الإمارات العربية المتحدة: أقر القانون الاتحادي رقم 5 لسنة 2012 بشأن مكافحة جرائم تقنية المعلومات، المعدل سنة 2018، حيث وضع قواعد صارمة لحماية البيانات ومنع التلاعب بالأنظمة القضائية الرقمية⁵⁵.

2. المملكة المغربية، قامت باعتماد القانون 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، والذي يرسخ مبدأ الشرعية والشفافية في معالجة البيانات القضائية⁵⁶.

3. المملكة العربية السعودية، اعتمدت نظام مكافحة الجرائم المعلوماتية بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8 الذي يشكل مرجعا إقليميا لمكافحة الهجمات السيبرانية على المؤسسات العامة، بما في ذلك القضاء⁵⁷.

هذه المرجعيات تبين أن الأمن السيبراني له أهمية بالغة في التشريع العربي، حيث أصبح ينظر إليه في الوطن العربي كشرط أساسي لبناء ثقة المواطن في المنصات القضائية الرقمية.

الفرع الثاني: الإطار القانوني والتنظيمي الجزائري

تزايد الاهتمام بالتحول الرقمي والأمن السيبراني في الجزائر، خصوصا بعد صدور القانون 05-18 المؤرخ في 10 مايو 2018 المتعلق بالتجارة الإلكترونية⁵⁸، والذي نص على ضمان أمن المعاملات الإلكترونية وحماية البيانات الشخصية. كما جاء المرسوم الرئاسي 05-20 المؤرخ في 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية⁵⁹، الموضوع لدى وزارة الدفاع الوطني، حيث جاء في المادة 3 أنها تشمل على:

1. مجلس وطني لأمن الأنظمة المعلوماتية: الذي يضطلع بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها، ومن بن أعضائه الوزير المكلف بالعدل. من بين مهام المجلس، يفصل في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة، وأيضا دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليها، كما يقوم بدراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها، ومن بين مهامه كذلك أنه يقدم الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في

مجال أمن الأنظمة المعلوماتية، وكذلك الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني، كما يقوم بالموافقة على تصنيف الأنظمة المعلوماتية، واقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية، عند الحاجة، كما يبدي أيضا المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي له علاقة بأمن الأنظمة المعلوماتية⁶⁰.

2. وكالة لأمن الأنظمة المعلوماتية: وتكلف بتنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، يحدد تنظيمها ومكوناتها، وكيفية سيرها وكذلك مهامها وصلاحياتها، بموجب قرار من وزير الدفاع الوطني، وبموجب المادة 18 تكلف الوكالة بتحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس، كما تقوم بتنسيق وتنفيذ الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية المحددة من قبل المجلس، وتقرّر كيفية اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية، كما تقوم بإجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية. وتسهر على جمع وتحليل وتقييم البيانات المتصلة بمجال أمن الأنظمة المعلوماتية وتستخلص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية، وتقوم أيضا بمتابعة عمليات التدقيق لأمن الأنظمة المعلوماتية، وتقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية. ومن مهامها ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية. ومراقبة الإدارات والمؤسسات والهيئات، بالتشاور مع الهياكل المتخصصة في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية، بعد رأي للمجلس، وتقوم بإعداد وتحديث المرجعيات والإجراءات والأدلة العملية وتقديم توصيات في ميدان أمن الأنظمة المعلوماتية، كما تعتمد منتجات أمن الأنظمة المعلوماتية والتصديق عليها، واعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني، المعمول، وتحديد معايير وإجراءات منح علامة الجودة و/ أو التصديق و/ أو اعتماد المنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية طبقا للتشريع والتنظيم الساري⁶¹.

إضافة إلى الهياكل المختصة لوزارة الدفاع الوطني في المجال أمن الأنظمة المعلوماتية حسب ما جاء في المادة 3 من المرسوم الرئاسي 05-20.

أما في مجال حماية البيانات، فقد تم اعتماد القانون 07-18 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي⁶²، الذي يؤسس

لأول مرة في الجزائر إطارا قانونيا قريبا من اللائحة الأوروبية (GDPR)، يضع قائمة التحقق من الامتثال لللائحة العامة لحماية البيانات⁶³.

كما نص القانون رقم 04-09 لسنة 2009 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها⁶⁴، بتجريم الأفعال الماسة بسرية النظم المعلوماتية والبيانات المخزنة فيها، وهو ما يعد أداة مهمة لحماية المعطيات القضائية الرقمية من القرصنة. رغم هذا التطور، فإن الإطار التشريعي الجزائري والعربي يواجه تحديات مرتبطة أساسا بضعف التطبيق العملي، ونقص التنسيق بين مختلف الهيئات، إضافة إلى الحاجة إلى تدريب القضاة وموظفي المحاكم على الأمن الرقمي، وتطوير بنية تحتية متوافقة مع المعايير الدولية مثل: شهادة ISO/IEC 27001 لأمن أنظمة المعلومات، هو معيار عالمي شهير لأنظمة إدارة أمن المعلومات الذي يحدد المتطلبات التي يجب أن يفي بها نظام إدارة أمن المعلومات⁶⁵. والمعهد الوطني للمعايير والتكنولوجيا NIST⁶⁶، الذي يطور معايير وإرشادات وممارسات وموارد للأمن السيبراني.

من خلال التجربة العربية والجزائرية يتضح أن تعزيز الأمن السيبراني في القضاء الإداري الرقمي لا يقتصر على وضع النصوص القانونية، بل يتطلب إرادة سياسية، وتنسيقا مؤسسيا، وتبني معايير تقنية وتنظيمية صارمة ومن ثم، فإن نجاح التحول الرقمي في القضاء الإداري مرهون بمدى قدرة التشريع والتنظيم الوطني على مواكبة المعايير العالمية، وتوفير بيئة قضائية آمنة وموثوقة، وتبادل التجارب والخبرات بين مختلف الدول العربية للوصول إلى الهدف المنشود هو الحماية السيبرانية لمختلف المؤسسات والمنظومات، ومن بينها منظومة القضاء الإداري.

الخاتمة

من خلال دراسة موضوع تعزيز الأمن السيبراني كعنصر أساسي للتحول الرقمي في القضاء الإداري، تبين أن نجاح عملية الرقمنة في المجال القضائي لا يقتصر على الجانب التقني فقط، بل يبقى مرهونا بوجود إطار قانوني وتنظيمي متكامل يوفر الحماية للمعطيات القضائية والبيانات الشخصية، ويضمن في الوقت ذاته نزاهة الإجراءات القضائية وصحة الأدلة الرقمية. كما بينت الدراسة أن التحول الرقمي في القضاء الإداري، على الرغم من فوائده البارزة في تسريع الفصل في المنازعات وتحسين الشفافية وتقليل التكلفة، يظل عرضة لمخاطر الهجمات السيبرانية المتعددة، مثل اختراق قواعد البيانات، أو تزوير الأدلة الإلكترونية، أو تعطيل المنصات الرقمية

المخصصة للتقاضي. هذه المخاطر لا تمس فقط بحقوق المتقاضين الدستورية، بل قد تهدد الثقة العامة في العدالة إذا لم تواجه باليات وقائية وردعية فعالة.

كما خُصّ البحث إلى أن التشريعات الجزائرية والعربية وإن كانت قد خطت خطوات مهمة بإصدار تشريعات متعلقة بحماية البيانات ومكافحة الجرائم الإلكترونية، إلا أنها ما تزال بحاجة إلى لوائح تنظيمية متخصصة تعنى بخصوصية القضاء الإداري الرقمي، وتعالج قضايا دقيقة مثل سلسلة الحياة الرقمية للأدلة، والمعايير التقنية لتأمين جلسات التقاضي الإلكترونية، والالتزامات المفروضة على القضاة والموظفين في مجال الأمن السيبراني.

وبناء على هذه الدراسة، نقدم جملة من المقترحات العملية التي من شأنها تدعيم الأمن السيبراني في القضاء الإداري:

1. تكييف التشريعات السارية، والوطنية مع المستجدات التكنولوجية التي تواكب تطور الأمن السيبراني، لتوفير حماية أكثر نجاعة للقضاء الإداري الرقمي.
 2. وضع لوائح تنفيذية متخصصة ضمن التشريعات الوطنية تنظم بوضوح قواعد حماية البيانات الرقمية في القضاء الإداري، وتحدد التزامات ومسؤوليات كل جهة فاعلة.
 3. اعتماد معايير دولية في تصميم وتشغيل المنصات القضائية الرقمية، بما يضمن انسجام القضاء الإداري مع أفضل الممارسات العالمية.
 4. تفعيل التعاون المؤسسي بين المجالس القضائية والهيئات الوطنية للأمن السيبراني لتبادل الخبرات ووضع بروتوكولات استجابة سريعة للهجمات الإلكترونية.
 5. تعزيز التكوين المستمر للقضاة والموظفين في مجال الأمن السيبراني والأدلة الرقمية، باعتبار المورد البشري نقطة ضعف رئيسية يمكن استغلالها في الاختراقات.
 6. إرساء آليات رقابية مستقلة لمتابعة مدى احترام المحاكم لمعايير حماية البيانات، على غرار هيئات حماية المعطيات الشخصية في الأنظمة المقارنة.
 7. تطوير بنية تحتية رقمية حديثة للحد من مخاطر الهجمات السيبرانية حتى في حالة حدوث اختراق جزئي للمنظومة الرقمية للقضاء.
- وخلاصة يمكن القول إن الأمن السيبراني ليس خيارا مكملًا للتحويل الرقمي في القضاء الإداري فحسب، بل يمثل شرطا وجوديا لضمان عدالة فعالة، نزاهة، وأمانة في العصر الرقمي.
- الهوامش:

1 Mouhammed Al-Amiri, *Artificial Intelligence in Cybersecurity and Digital Governance*, 2025 19, July, accessed on 13/08/2025 at 11:42, <https://www.mohammedaameri.com/blog/282>.

2 ما المقصود بالأمن السيبراني، دون مؤلف، تاريخ الاطلاع 2025/08/16، الساعة 13:17، [/https://aws.amazon.com/ar/what-is/cybersecurity](https://aws.amazon.com/ar/what-is/cybersecurity)

3 محمد المطري، أهمية الأمن السيبراني في العصر الرقمي، تاريخ النشر 29 ديسمبر 2024. تاريخ الاطلاع 2025/08/12، الساعة 17:12، <https://tinyurl.com/23e37a3v>.

4 كمال بداري، التحول الرقمي حجر الأساس من أجل بناء اقتصاد قوي، تاريخ النشر 2022/03/10، تاريخ الاطلاع 2025/05/10، الساعة 18:14، <https://tinyurl.com/bdzj8d32>.

5 Hafiz Gaffar, *Implications Of Digitalization And Ai In The Justice System A Glance At The Socio-Legal Angle*, *International Journal of Law "Law And World"* Volume 10, Issue 3, September 2024, Page15.

6 ساره حسن ناجي، إسهام التحول الرقمي في دعم القضاء الإداري -دراسة تطبيقية-، رسالة ماجستير، كلية الحقوق جامعة الملك عبد العزيز، المملكة العربية السعودية، 2024، ص 215.

7 نهي القحطاني، إصلاح القضاء ركيزة العدالة والتنمية، تاريخ النشر 2025/03/28، تاريخ الاطلاع 2025/06/16، الساعة 11:17، <https://www.alriyadh.com/2124978>.

8 غريبي بشري، جائحة كورونا تحد جديد على ضمان استمرارية سير المرافق العامة، مجلة الاجتهاد لقضائي، جامعة محمد خيضر بسكرة، المجلد 13، العدد 28، سنة 2021، ص ص 360 -361.

9 فهد ال خفير، التقاضي الإلكتروني في المحاكم السعودية، تاريخ النشر 2024/09/13، تاريخ الاطلاع 2025/06/16، الساعة 19:28.

[/https://www.fklaw.sa/electronic-litigation](https://www.fklaw.sa/electronic-litigation)

10 المادة 2، قانون رقم 16 لسنة 2019 الخاص بالأمن السيبراني، ج ر للمملكة الأردنية الهاشمية، رقم 5595، الصادرة بتاريخ 2019-09-16، ص 5143.

11 المادة 2، ظهير شريف رقم 1.20.69، المؤرخ في 4 ذي الحجة 1441 (25) يوليو 2020، بتنفيذ القانون رقم 05.20 المتعلق بالأمن السيبراني، ج ر المملكة المغربية، عدد 6904، الصادرة بتاريخ 9 ذو الحجة 1441، الموافق لـ 30 يوليو 2020.

12 فريق sebrany، أساسيات الأمن السيبراني وأهميته، تاريخ النشر 2025/7/11، تاريخ الاطلاع 2025/06/4، الساعة 23:37، <https://tinyurl.com/39y4h652>.

13 فريق Rmg team، عناصر الأمن السيبراني الأساسية، دليلك الشامل لبناء دفاع رقمي متين، تاريخ الاطلاع 2025/5/20، تاريخ الاطلاع 2025/06/4، الساعة 23:37، [/ https://tinyurl.com/32eajxbb](https://tinyurl.com/32eajxbb)

- 14 محمد محمد جمعه، التحول الرقمي وكفاءة الأنظمة القانونية والقضائية (دراسة تحليلية مقارنة تضم 40 دولة)، دار الأهرام للنشر والتوزيع والإصدارات القانونية مصر، الطبعة الأولى، سنة 2023، ص 12.
- 15 محرم الحداد، محمد إبراهيم، الثورة الصناعية الرابعة (الذكاء الاصطناعي - التحول الرقمي)، معهد التخطيط القومي، الإصدار رقم 8، الطبعة الأولى، سنة 2021، ص 29.
- 16 فريق afnor، شهادة- ISO/IEC 27001 أمن نظم المعلومات، تاريخ الاطلاع 13\08\2025، الساعة 20:31، <https://tinyurl.com/kau254mu>
- 17 مصطفى قطب، الأمن السيبراني، أهمية حماية البيانات في العصر الرقمي، تاريخ النشر 08\11\2024، تاريخ الاطلاع 13\08\2025، الساعة 20:44، <https://tinyurl.com/2fymfnee>
- 18 دون مؤلف، مستقبل الأمن السيبراني في العصر الرقمي، تاريخ النشر 12\03\2025، تاريخ الاطلاع 13\08\2025، الساعة 22:02، <https://tinyurl.com/zv89s7xd>
- 19 Joint Technology Committee, Resource Bulletin Cybersecurity Basics for Courts, NCSC, 2021, p12.
- 20 Conventions on cybercrime: The Budapest Convention and the draft UN treaty, Council of Europe, published 27/08/2024, Accessed on 15/08/2025 at 20h36, <https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a>.
- 21 AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, MALABO, EQUATORIAL GUINEA, 27TH JUNE 2014, p2, accessed on 15/8/2025, at 20h50, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
- 22 قانون رقم 09-04، المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47، الصادرة بتاريخ 16 أوت 2009.
- 23 القانون 18-04، المؤرخ في 10 مايو 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية، عدد 27، الصادرة بتاريخ 13 مايو 2018.
- 24 القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات طابع شخصي، الجريدة الرسمية، عدد 34، الصادرة بتاريخ 10 يونيو 2018.
- 25 سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة القانون الكويتية العالمية، عدد 99، سنة 2015، ص 401.
- 26 محمد حماد مرهج الهيتي، البحث عن حماية جنائية للبيانات والمعلومات الشخصية الأسمية المخزنة في الحاسب الآلي، مجلة كلية الشريعة والقانون، الامارات، عدد 27، سنة 2016، ص 401.

27 هبه رمضان رجب، الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية، مجلة العلوم القانونية والاقتصادية، سنة 2024، ص 424.

28 Without an author, Long Range Plan for Information Technology in the Federal Judiciary: Fiscal, Judicial Conference of the United States, 2024, pp 12-13.

29 Brian J. McLaughlin, Cybersecurity Protecting Court Data Assets, AMERICAN SOCIETY FOR PUBLIC ADMINISTRATION, 2018, p71.

30 Renato Solimar Alves, Jady Pamella Barbacena da Silva, Luiz Antonio Ribeiro Junior, Rafael Rabelo Nunes, Enhancing cybersecurity in the judiciary: Integrating additional controls into the CIS framework, Computers & Security, Volume 157, 2025, p.9

31 Brian J. McLaughlin, op sit, p70.

32 Renato Solimar Alves, Jady Pamella Barbacena da Silva, Luiz Antonio Ribeiro Junior, Rafael Rabelo Nunes, op sit, p.9

33 Yeboah-Ofori, Brown AD, Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence, Forensic Legal & Investigative Sciences, 2020, p6.

34 Sean E. Goodison, Robert C. Davis, Brian A. Jackson, Digital Evidence and the U.S. Criminal Justice System, 2015, p13.

35 Deepti Vaddey, Cybersecurity in criminal trial: Protecting sensitive data in the digital courtroom, INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS], Volume 3, Issue 1, 2025, p 405.

the digital courtroom, INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS], Volume 3, Issue 1, 2025, p 405.

36 Yeboah-Ofori, Brown AD, op sit, p6.

37 Jeff Kosseff, Defining Cybersecurity Law, IOWA LAW REVIEW, Vol 103, 2018, pp 11-13.

38 Julia Voo, Irfan Hemani, Simon Jones, Winona DeSombre, Daniel Cassidy, Anina Schwarzenbach, National Cyber Power Index 2020 Methodology and Analytical Considerations, China Cyber Policy Initiative, Harvard Kennedy School, Belfer Center for science and International Affaires, published September 2020, accessed on 12/9/2025 at 16:52. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf,

39 Fedbarblog, Cybersecurity Challenges for Federal Attorneys and Judges, 2025, NCSC Associations, published 04/03/2025, accessed on 12/9/2025 at 16:57, <https://www.fedbar.org/blog/cybersecurity-challenges-for-federal-attorneys-and-judges/>

40 Joint Technology Committee, Cybersecurity basics for courts, JTC Resource Bulletin, published 2022, accessed on 12/9/2025 at 19:34, <https://www.ncsc.org/resources-courts/cybersecurity-basics-courts>.

41 Fedbarblog, Cybersecurity Challenges for Federal Attorneys and Judges, op. sit, accessed on 13/9/2025 at 23:11.

42 Deepthi Kallahakalu Vijay Dev, Securing Justice: Enhancing Cybersecurity in the Criminal Justice System, published August 2024, accessed on 12/9/2025 at 19:42, https://www.researchgate.net/publication/383007192_Securing_Justice_Enhancing_Cybersecurity_in_the_Criminal_Justice_System,

43 MARC LEVY, Cyberattack on Pennsylvania courts didn't appear to compromise data, officials say, published February /6/2024, accessed on 12/9/2025 at 19:42,

<https://apnews.com/article/cyberattack-pennsylvania-courts-hackers-cybersecurity-187de27a9d4eab485b56a65e869bf298>.

44 David DiMolfetta, *US court system to boost cyber posture after hack of electronic case management tool*, published August/ 8/2025 2025, accessed on 13/9/2025 at 00:42 https://www.nextgov.com/cybersecurity/2025/08/us-court-system-boost-cyber-posture-after-hack-electronic-case-management-tool/407321/?utm_source=chatgpt.com

45 Feras A. Batarseh, *Cyber Threats Jurisdiction and Authority – A Legal Discussion*, Antonin Scalia Law School, George Mason University, published 2022, accessed on 13/9/2025 at 00:56, <https://arxiv.org/pdf/2206.09465>

46 Joint Technology Committee, *op. cit*, 2021, p5.

47 Paul A. Grassi, and Other, *Digital Identity Guidelines Authentication and Lifecycle Management*, National Institute of Standards and Technology, U.S. Department of Commerce, 2025, pp 16-18.

48 Scott Rose, and Other, *Zero Trust Architecture*, NIST Special Publication 800-207, 2020, p4.

49 Joint Technology Committee, *op. cit*, 2021, p9.

50 Joint Technology Committee, *op. cit*, 2021, p9.

51 Sean E. Goodison, Robert C. Davis, Brian A. Jackson, *op. cit*, p11.

52 Joint Technology Committee, *op. cit*, 2021, p22.

53 Sean E. Goodison, Robert C. Davis, Brian A. Jackson, *op. cit*, p16.

54 Joint Technology Committee, *op. cit*, 2021, p22.

55 مرسوم بقانون اتحادي رقم 5 لسنة 2012، في شأن مكافحة جرائم تقنية المعلومات، بتاريخ 13 أغسطس 2012، الجريدة الرسمية لدولة الإمارات العربية المتحدة، العدد 540 ملحق، الصادر بتاريخ 26 أغسطس 2012، مرسوم بقانون اتحادي رقم 2 لسنة 2018، بتعديل بعض أحكام المرسوم بقانون اتحادي رقم 5 لسنة 2012، في شأن مكافحة جرائم تقنية المعلومات، بتاريخ 24 يوليو 2018، الجريدة الرسمية لدولة الإمارات العربية المتحدة، العدد 633، الصادرة بتاريخ 31 يوليو 2018.

56 قانون رقم 09.08، يتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية للمملكة المغربية، عدد 5711، الصادرة بتاريخ 23 فبراير 2009.

57 مرسوم ملكي رقم م / 17 بتاريخ 8 / 3 / 1428، قرار مجلس الوزراء رقم 79 بتاريخ 7 / 3 / 1428، نظام مكافحة جرائم المعلوماتية، تاريخ الإصدار 08/03/1428 هـ الموافق: 2007/03/27 م، هيئة الخبراء بمجلس الوزراء، المملكة العربية السعودية. تاريخ الاطلاع 2025/9/21، الساعة 20:37،

<https://laws.boe.gov.sa/Boelaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1>

58 قانون رقم 05-18، مؤرخ 10 مايو سنة 2018، يتعلق بالتجارة الإلكترونية، الجريدة الرسمية، عدد 34، الصادرة بتاريخ 10 يونيو سنة 2018.

59 المرسوم الرئاسي رقم 05-20، المؤرخ في 20\01\2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية، عدد 04، الصادرة بتاريخ 26 جانفي سنة 2020.

- 60 حزام فنيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي 20-05، مجلة الحقوق والعلوم الإنسانية، عدد 03، تاريخ النشر 30\10\2020، ص 182.
- 61 المادة 5 من المرسوم الرئاسي رقم 20-05، المرجع السابق.
- 62 قانون رقم 07-18، مؤرخ 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، عدد 28، الصادرة بتاريخ 16 مايو سنة 2018.
- 63 اللائحة العامة لحماية البيانات الأوروبية (GDPR)؛ قانون للاتحاد الأوروبي يهدف إلى حماية البيانات الشخصية للأفراد في المنطقة الاقتصادية الأوروبية، ويفرض التزامات صارمة على المؤسسات التي تعالج هذه البيانات. تعطي اللائحة الأفراد حقوقاً على بياناتهم، مثل الحق في الوصول إليها وتصحيحها وحذفها، وتلزم المؤسسات بالشفافية والأمن في معالجة البيانات. تفرض عقوبات مالية كبيرة، تصل إلى 4% من الإيرادات السنوية للمؤسسة، على الجهات غير الملتزمة،
- Matt Kosinski, GDPR compliance checklist, IBM, 2024*، تاريخ الاطلاع 2025/9/21، الساعة 21:44،
<https://www.ibm.com/think/topics/gdpr-compliance-checklist>
- 64 قانون رقم 04-09، مؤرخ في 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر، عدد 47، الصادرة بتاريخ 5 غشت سنة 2009.
- 65 شهادة ISO/IEC 2700 أمن أنظمة المعلومات، *certification. afnor*، تاريخ الاطلاع 2025/9/21، الساعة 21:58،
<https://certification.afnor.org/numerique/certification-iso-27001>
- 66 الأمن السيبراني والخصوصية، NIST، تاريخ الاطلاع 2025/9/21، الساعة 22:16،
<https://www.nist.gov/cybersecurity-and-privacy>