

حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية

- قراءة في أحكام المرسوم الرئاسي 20-05

Information systems security between technical mechanisms and protection devices

Read the provisions of Presidential Decree 20-05

حزام فتيحة*

Fatiha Hazam

جامعة بومرداس، الجزائر، f.hazem@univ-boumerdes.dz

تاريخ الإرسال: 2020-05-03 تاريخ القبول: 2020-10-28 تاريخ النشر: 2020-10-30

ملخص:

في إطار السعي لحماية المعلومات والبيانات الخاصة بمختلف القطاعات التي تشهد حركية في إطار رقمنة مصالحها في مواجهة مخاطر الإعتداءات السيبرانية، تدخل المشرع الجزائري لمحاولة تأمينها تأميناً فعالاً وذلك من خلال إصداره للمرسوم الرئاسي رقم 20-05 المتعلق بأمن الأنظمة المعلوماتية، لذا تسعى الدراسة لبيان أهم الآليات الفنية لحماية المعلومات من جهة، وتبسيط الضوء على أهم الأحكام التي تضمنها هذا المرسوم من جهة ثانية لا سيما من خلال تبيان مهام وصلاحيات الهيئات التي استحدثها والمتمثلة في المجلس الوطني لأمن الأنظمة المعلوماتية وكذا الوكالة الوطنية لأمن الأنظمة المعلوماتية.

الكلمات المفتاحية: أنظمة معلوماتية، حماية المعلومات، رقمنة، أمن البيانات.

Abstract:

In an effort to ensure the security of information and data for the various sectors witnessing dynamism within the framework of digitizing their interests in facing the dangers of cyber attacks, the Algerian legislator intervened to try to secure them effectively through the issuance of Presidential Decree No. 20-05 related to the security of information systems, so the study seeks to demonstrate the most important technical mechanisms To protect the information on the one hand, and highlight the most important provisions included in this decree on the other hand, particularly by clarifying the tasks and powers of the bodies that he created, which are represented in the National Council for Information Systems Security as well as the National Agency for Systems Security Informatics.

*Corresponding author, e-mail: f.hazem@univ-boumerdes.dz.

Key words: information systems, data protection, digitization, data security.

1- مقدمة

إنَّ التقدم التكنولوجي الكبير، وتطوُّر وسائل الإتصالات المتنوعة، وانفتاح العالم على بعضه، واعتماده على إرسال شتى أنواع البيانات خلال الشبكات، كل ذلك أدى إلى إحداث خطر على تسرُّب هذه البيانات، ووصولها للأشخاص الخاطئين، أو المنافسين، وبالتالي أصبحت الحاجة الملحة للحفاظ على أمن المعلومات.

يقصد بأمن المعلومات هو السيطرة التامة على المعلومات، من حيث تحديد من سيستلم هذه البيانات، وتحديد صلاحيات الوصول إليها، واستخدام مجموعة من التقنيات من أجل ضمان عدم اختراقها من قبل أي جهة، وتتضاعف أهميتها من الحفاظ على الخصوصية، إلى الحفاظ على بيانات هامة مثل حسابات العملاء في البنوك، حيث يوجد في شبكة الإنترنت الاعتيادية مجموعة كبيرة من نقاط الضعف التي تمكّن أشخاص غير مخوّلين من الوصول إلى هذه البيانات، ومنها الأخطاء البرمجية التي يقوم بها المبرمجون أثناء بناء الشبكات، أو تصميم التطبيقات المختلفة، مثل أخطاء في كيفية تعامل التطبيق مع الإدخال الخاطئ، أو بسبب سوء توزيع الذاكرة، كما أنّ هناك العديد من المبرمجين الذين يقومون بتصميم برامج مخصّصة لاختراق الأنظمة، والبحث عن نقاط ضعفها، لذا يتحدد مفهوم الأمن المعلوماتي من زاوية أكاديمية هو العلم الذي يبحث في نظريات و استراتيجيات توفير الحماية للمعلومات من المخاطر- التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.¹

أمّا من الناحية القانونية فالأمن المعلوماتي هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة.²

فنظرا لأهمية قضايا الأمن السيبراني وتداركا للمخاطر التي يمكن أن تتعرض لها المعلومات والبيانات في البيئة الرقمية ناهيك عن الحوادث السيبرانية التي تستهدف المؤسسات الوطنية، أصدر المشرع مرسوما رئاسيا تحت رقم 05-20 يتعلق برسم ووضع منظومة وطنية لأمن الأنظمة المعلوماتية موكلة لوزارة الدفاع الوطني، وحسب المرسوم فإنّ المنظومة أداة الدولة في مجال أمن الأنظمة المعلوماتية، وتشكل الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وتنسيق تنفيذه.

اعتبارا لكون الأمن المعلوماتي هو علم مختص بتأمين المعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الإعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفرها لحماية المعلومات.³ تأسيسا على ما تقدم نطرح الإشكالية:فيما تتمثل أهم الآليات الفنية لحماية وضمان أمن المعلومات؟وما هي أهم صلاحيات أجهزة الحماية التي حملها المرسوم الرئاسي 05-20؟. للإجابة عن ذلك اخترنا اتباع المنهجين الوصفي والتحليلي ف دراسة الموضوع مقسمين الدراسة للمبحثين المواليين:

المبحث الأول:الآليات التقنية لأمن الأنظمة المعلوماتية

يتم اللجوء لمجموعة من طرق الحماية من أجل الحفاظ على أمن المعلومات، ومنها طرق الحماية المادية فهناك العديد من الطرق البسيطة التي يجب اتباعها من أجل الحفاظ على أمن المعلومات الحفاظ على جهاز الحاسوب في مكان آمن، ووضع كلمة سرّ عليه لمنع عبث المتطفلين، وأن تكون كلمة السر تحتوي على أحرف، وأرقام، ورموز؛ كي يصعب التنبؤ بها، وتغييرها بشكل دوري.

المطلب الأول: آليات تأمين الدخول لشبكة المعلومات

تتعلق بالآليات التي عن طريقها يتم التأكد من عدم تعرض المعلومات للأخطار المتمثلة في إمكانية الكشف عنها أو الاطلاع عليها من قبل أشخاص غير مسموح لهم بذلك وفي الحالة التي يكون فيها مالكي هذه المعلومات يرغبون في حفظ سرّيتها . لذا فإن هذا الجانب الذي يتطلب الوثوقية أو الأمانة يتطلب في ذات الوقت اتخاذ التدابير اللازمة لحماية سرية المعلومات الحساسة وضمان التوصل إلى المعطيات حصرياً من قبل المستعملين المرخصين أو عدا مالكيها ، وهذا كما سبق بيانه يعد جانب من الجوانب للأمن المعلوماتي أو السلامة المعلوماتية مع ضمان سلامة المعلومات أو المحتوى ويعني ذلك اتخاذ التدابير اللازمة و الضرورية لحماية المعلومات من التعديل، لكن سلامة المعلومات لا يعني فقط تعديلها بل سلامتها من أي استخدام غير مشروع بفعل تعرض محتواها إلى الانتهاك سواء بالتعديل أو المحو أو التدمير ، مع ضمان الوصول إلى المعلومات واستمرارها فمن شروط السلامة المعلوماتية وأهدافها التأكد من استمرار التفاعل مع المعلومات واستمرار عمل النظام المعلوماتي من خلال التصدي لأعمال وهجمات التي يقوم بها الجاني المعلوماتي لحرمان المستفيدين من الوصول إلى المعلومات فضلاً عن عدم إنكار التصرف الذي يتم من خلال هيئات التصديق الإلكتروني وتتمثل وظيفته في أن يمنع من خلالها أي كيان أو مستخدم من أن ينكر أي عمل سابق تم إجرأه كأن يتم إنكار إرسال المعلومات أو رسالة معينة ، لذلك عند وقوع مثل هذا الخلاف بين الأطراف المتصلة يجب توفر إجراء معين أو وسيلة محددة لحل هذا النزاع ويتم ذلك من خلال إشراك طرف محايد وموثوق ، وهذا ما تحققه وظائف التوقيع الإلكتروني من خلال هيئات التصديق وبالتالي لا يمكن لأي طرف إنكار أي تصرف صادر منه⁴.

الفرع الأول: عن طريق الجدران النارية

نظراً للانتشار الواسع حالياً لقرصنة المعلومات والتجسس المعلوماتي وذلك بسبب إنتشار برامج القرصنة ووجودها في الكثير من المواقع أصبح من الممكن إختراق أي جهاز أو نظام معلوماتي و بدون عناء فور إنزال إحدى البرامج و خاصة مع وجود ثغرات في الأجهزة أو الأنظمة ومن أثار تلك التهديدات، التعرض للسرقة والاحتيال عن طريق تغيير المعلومات التي يتم إدخالها في النظام أو تغيير المخرجات التي تخرج منه التجسس الصناعي عن طريق تنزيل الأسرار الصناعية من الكمبيوتر إلى إحدى الشركات وإرسالها عبر البريد الإلكتروني مباشرة إلى منافستها، الأمر الذي يستدعي ضرورة إيجاد آليات لمواجهتها من بينها الجدران النارية.

إنّ الجدار الناري هو عبارة عن جهاز، أو تطبيق، ويتمّ وضعه عند الخادم، وعند مصافي الشبكة، كل حسب احتياجاته، وقد جاءت فكرة الجدار الناري من الطريقة الأمنية المعروفة قديما وهي عبارة عن حفر خندق حول قلعة لمنع أي شخص من الدخول أو الخروج من القلعة، ويمكن تفتيشه من قبل الحراس على القلعة، لذا يقصد بالجدار الناري: «مجموعة أنظمة توفر سياسات أمنية بين الإنترنت والشبكة الخاصة لتصبح جميع عمليات العبور إلى الشبكة أو الخروج منها تمر من خلال الجدار الناري الذي يصعد المستعملين غير المرغوب فيهم، فالجدار الناري يقوم بالتحقق من صلاحية المستعمل المحلي والمستعمل الخارجي، ونظام الدخول والخروج، وتشفير المعلومات، وإجراءات الحماية من الفيروسات»⁵.

من مزايا الجدار الناري: توفير الحماية اللازمة للشبكة والمعلومات. -توفير خدمات التشفير في تكنولوجيا الجدار الناري. -تخزين العمليات والمعلومات التي تمر من طريق الجدار الناري. -متابعة المستخدمين للشبكة ومن يحاول العبث بها. وعليه على المستخدم الذي يريد الدخول إلى شبكة الأنترنت أن يحصن جهازه بالجدار الناري⁶، ويمكن الحصول عليه من الأنترنت عن طريق زيارة موقع (WWW.DOWNLOAD.COM).

الفرع الثاني-عن طريق البرامج الكاشفة:

إنّ مسألة تعرض جهاز الحاسب الآلي للهجمات الفيروسية أمر وارد والذي بالنتيجة يؤدي حتما لتلف المحررات الإلكترونية بسبب العدوى التي تحدثها تلك الفيروسات، لذا كان من الضروري التفكير في إيجاد آليات تحول دون حصول ذلك، وعليه، فقد أنشئت برمجيات تحتوي عددا من الموظفين من إداريين ومحلي نظم ومبرمجين لتصميم وإعداد وكتابة برامج الكشف عن الفيروسات، ومن ثم تدميره قبل أن يبدأ عمله في النظام. نجد أغلب برامج الكشف عن الفيروسات ومكافحتها تستطيع التعرف إلى ملفات التجسس وتقوم بإزالتها من الجهاز، لكن هناك ملفات التجسس قد لا تستطيع برامج مكافحة الفيروسات إكتشافها. رغم كل تلك التدابير إلا أنّ الجهاز لا يزال غير آمن، لهذا يجب تجنب وضع قوائم بكلمات السر أو الإستخدام على الجهاز، وخصوصا أرقام الحسابات البنكية، وبطاقات الإئتمان، مع التقليل من الدخول على الحسابات البنكية عبر الأنترنت، وعدم الإحتفاظ بتقارير سرية تحوي أرقاما مهمة على القرص الصلب، لكون المخترقين يعملون بجهد لإختراق كل الأنظمة والبرامج⁷.

الفرع الثالث: إستعمال تقنية التشفير الإلكتروني للتوقيعات الرقمية:

يقصد بالتشفير " تلك الطريقة التي تعتمد على الخوارزمات الرياضية الذكية التي تسمح لمن يمتلك مفتاحا سريا أن يحول رسالة مقروءة لرسالة غير مقروءة أو العكس⁸.

لم يعرف المشرع الجزائري تقنية التشفير لكنه تطرق من خلال نص المادة الثانية الفقرتين الثامنة والتاسعة من القانون 04-15 المتعلق بالتوقيع والمصادقة الإلكترونيين⁹، للإشارة لمفتاحي التشفير العمومي والخاص والتي سنأتي على بيانها لاحقا، خلافا للمشرع التونسي الذي قام بتعريفه في المادة 5/3 بانه: «إستعمال رموز أو إشارات غير متداولة تصلح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها غير قابلة للفهم من قبل الغير، أو

إستعمال رموز أو إشارات لا يمكن الوصول إلى المعلومات بدونها»¹⁰.

ثانيا- خصائص نظام التشفير: يحتل نظام التشفير مفهومين أحدهما مفهوم واسع والآخر مفهوم ضيق، ومقتضى المفهوم الواسع لنظام التشفير، عدم خضوع أدوات ووسائل التشفير لأية قيود عند إستخدامها وقد أخذت بهذا المفهوم الولايات المتحدة الأمريكية، أما المفهوم الضيق لنظام التشفير، يقصد به وضع إجراءات مشددة على إستعمال أدوات ووسائل التشفير، ليس فقط على تصدير واستيراد هذه الوسائل والأدوات، وإنما تتخذ هذه الإجراءات حتى على بيع وإستخدام هذه الوسائل داخل أراضي الدولة نفسها، ومن هذه الأنظمة النظام الفرنسي¹¹، فالتشفير إذن هو تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من إطلاع الغير عليها أو من تعديلها أو تغييرها، فهذا النظام يتمتع بالخصائص التالية:

1- أن تشفير البيانات والمعلومات التي يتم تدوينها أو التعامل فيها يتم من خلال الوسائط الإلكترونية.
2- إحترام سرية البيانات المشفرة والإعتراف بحق أصحابها في خصوصية البيانات المشفرة المرسله عبر الأنترنت وتجريم الإعتداء عليها.

3- أن نظام التشفير من أصل عسكري: فإحداث التوقيع الإلكتروني والتدقيق فيه يرتبط ارتباطا وثيقا بعناصر التشفير «فهو يعتمد أساسا على أساليب التشفير باستعمال المفاتيح الألفروتمية للترقيم والتشفير نظام عرفه منذ القدم الجيش الفرنسي وقد استعمل القائد العسكري Jules César نظام التشفير في مراسلاته، وقد تم تقنين ألفتورتمات التشفير من طرف السلطات العسكرية سنة 1991 بصدور قانون التشفير»¹². تأسيسا على ذلك، يمكننا القول أن التشفير هو ذلك الإجراء الذي يؤدي إلى توفير الثقة في المعاملات الإلكترونية وذلك باستخدام أدوات أو وسائل أو أساليب لتحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها غير المشروع.

ثالثا- كيفية إجراء التشفير: «يسمح التشفير كإجراء بتوفير الثقة في المعاملات الإلكترونية حيث يسهم من خلال أدوات ووسائل وأساليب تحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو إستخدامها غير المشروع بحيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي ذات البيانات التي قام المرسل بالتوقيع عليها»، ويتم تشفير التوقيع الإلكتروني باستخدام نظامي هما السيمتري وهونوع من البرامج يعتمد على الرموز الهندسية المعقدة والآخر هو النظام البيومتري والذي يعتمد على مواصفات شخصية تتعلق بصاحب التوقيع ذاته»¹³.

الفرع الثاني: صور التشفير

رغم حداثة تقنية التشفير في المجال التكنولوجي إلى أنها تشهد تطورات سريعة نظرا لأهميتها البالغة في تأمين وموثوقية المحررات الإلكترونية، لذا فقد ظهر لأول وهلة نظام التشفير المتماثل لكنه أثبت عجزه نظرا لبعض العيوب التي لحقت به وهو ما سوف نتطرق له من خلال العنصر الأول، أما العنصر الثاني فنتطرق فيه للنظام

البديل المقترح وهو نظام التشفير اللاتماثل مع تبيان الخصوصية التي يتمتع بها بفضا إعماده على المفتاحين العام والخاص، ونطرق في عنصر أخير لنوع مستحدث من التشفير وهو البصمة الإلكترونية.

أولا- التشفير المتماثل أو الأحادي أو ذو المفتاح الواحد: في هذا النظام نفس المفتاح يستعمل للتشفير من ناحية ولفك التشفير من ناحية ثانية، لكن الإشكالية بالنسبة لهذا النظام تتمثل في إيجاد وسيلة موثوق بها لتبليغ المفتاح للطرف الموجهة إليه.

ثانيا- التشفير اللاتماثل أو الثنائي Cf: (ذو المفتاح الثنائي) إنّ التشفير غير المتماثل يعتمد على زوج من المفتاح غير المتماثلة (مفتاح عام ومفتاح خاص) الأول يكون معروفا للجميع ويحتفظ به سرا والثاني فهو خاص بصاحبه وعليه الإحتفاظ به سرا ، ومالك هذا الزوج من المفتاح عليه الإحتفاظ بالمفتاح الخاص سريا حيث من خلاله يستطيع تشفير رسالته وبالتالي عدم قدرته على رفض ما جاء فيها، وتكمن ميزة هذا النظام في أنّ معرفة المفتاح العام لا يمكن منه معرفة أو تشكيل المفتاح الخاص، وأنّ كل مفتاح يقوم بعكس عمل الآخر بمعنى أن ما يشفره الأول يقوم الآخر فقط بحله لبيان كيفية استخدام التوقيع الرقمي من خلال عملية التشفير، «كما يجب تزامن عميتي التشفير وفكه». إنّ تقنية التشفير كما سبق بيانه، تقسم إلى تشفير متماثل وآخر غير متماثل ، أما الأول يعتمد وجود مفتاح وحيد فالرقم السري معلوم بين صاحبه والجهاز فقط، أما الثاني فهو التشفير غير المتماثل الذي يعتمد زوج مفتاح غير متماثل (مفتاح عام ومفتاح خاص) الأول يكون معلوم للكل، والثاني معلوم فقط لصاحبه ويلتزم بالإحتفاظ به سرا، فلا يمكن بأي حال معرفة المفتاح الخاص انطلاقا من المفتاح العام نظرا لكون ذلك يتطلب وقتا طويلا لاعتماده على صيغ رياضية، كما سبق بيانه، أما الكيفية التي تنشأ فيها المحررات الإلكترونية، وآلية إرسال الرسالة واستخدام المفتاح العام والخاص فتتمثل في أنّ المرسل يقوم بترميز الرسالة باستخدام «دالة البعثرة»¹⁴، وينتج عن ذلك ما يعرف باختصار الرسالة أو بصمة الرسالة، وباستخدام المفتاح الخاص للموقع تحول برمجيات الموقع نتيجة البعثرة إلى توقيع رقمي.

ثالثا- إعماد التشفير على المفتاح الخاصة والعمومية:

1-المفتاح الخاص : فحسب نص المادة الثانية الفقرة الثامنة من القانون 04-15 المتعلق بالتوقيع والمصادقة الإلكترونية، عرفت مفتاح التشفير الخاص على أنه: «هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي»، فهو بذلك يكون تحت السيطرة والسلطة المطلقة لصاحب التوقيع الإلكتروني الذي يتعين عليه توفير شروط السلامة لحماية المفتاح من مخاطر استعمالهم طرف الغير خاصة بعدم الكشف عنه لأي شخص آخر، وهذا المفتاح يستعمل لتشفير الوثائق وإمضاءها.

2-المفتاح العمومي : حسب نص المادة الثانية الفقرة التاسعة من القانون المتعلق بالتوقيع والمصادقة الإلكترونية فإنّ مفتاح التشفير العمومي «هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور

يهدف تمكينهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني». فكما يدل عليه اسمه هو مفتاح يمكن لكل شخص الإطلاع عليه واستعماله للتأكد من أن الإمضاء المضمن بالوثيقة الإلكترونية هو صادر عن الشخص المنسوب إليه الإمضاء»، والمفتاح العام يتم نشره في الدليل وهو متاح للعامة من الناس. هناك من اقترح ما يعرف بـ «نظام الغير الثقة» بحيث يوجد مفتاحين مفتاح عام وخاص ويحمل كل مفتاح علاقة رياضية غير مفهومة ويبقى المفتاح الخاص مع المستخدم أو العميل بحيث لا يستعمله إلا هو فإذا استعمله في أية عملية قانونية وصدر منه توقيع يعد ذلك قرينة عن أنه شخصيا استعمل المفتاح، فوجود المفتاح سرا معه يعطي الثقة والأمان في أي توقيع يصدر منه ومهمة المفتاح العام هو التحقق من صحة التوقيع الإلكتروني الصادر من صاحب المفتاح الخاص. كما يجب أن تكون العناصر البرمجية والمعدات المستخدمة للغرض مؤمنة من الناحية التقنية بطريقة تمنع استعمالها إلا من قبل صاحبها كما أنها يجب أن تضمن الارتباط بين الإمضاء والوثيقة المتعلقة به بحيث أن كل تغيير يطرأ على الوثيقة يمكن التفتن إليه آليا (وهو جوهر ما اشترطه المادة 453 من مجلة الالتزامات والعقود التونسية وذلك في فقرتها الثانية).

هناك العديد من البروتوكولات المعدة لتشفير البيانات، بحيث تمنع أي أحد يصلها من فهمها، وتختلف درجة التعقيدات في هذا التشفير، فهناك بعض الأنظمة التي يمكن حلها بالعودة لقواعد تشفيرها، ولذلك يجب اعتماد طريقة معقدة، تصعب قدر الإمكان إمكانية إعادة النص للغته قبل التشفير، وبالطبع فإن مفتاح فك التشفير يمتلكه الجهاز المستقبل لهذه البيانات. مراقبة البيانات (Packet Sniffers): يوجد العديد من التطبيقات التي تتمكن من معرفة حركة البيانات الخارجة، والداخلية إلى الشبكة، وعن طريق تحليلها يمكن التوصل للاختراقات التي حدثت لهذه الشبكة، ومعرفة مكانها. كلما زادت أهمية البيانات وسريتها، زادت الوسائل المتبعة لحمايتها، من مادية، وبرمجية، فمثلاً أجهزة الخوادم توضع في مكان محمي بشئ الطرق الفيزيائية، ومن ضمنها الحراس¹⁵.

المطلب الثاني: آليات منع إفشاء المعلومات

نظرا للآخطار التي تهدد خصوصية المعلومات وانتهاك السرية المعلوماتية، توفر تقنية المعلومات الجديدة إمكانية تخزين أو حفظ واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة. وأكثر من هذا فإنه يمكن خزن وحفظ المعلومات والبيانات الشخصية في قاعدة مؤمنة هي قاعدة البيانات ويمكن نقلها عبر مختلف مناطق البلد في ثوان معدودة وبتكاليف منخفضة نسبيا، إن هذا يبين بوضوح كيفية أو إمكانية تهديد الخصوصية و تزايد مخاطر التقنيات الحديثة على حماية الخصوصية كتقنيات الرقابة وبطاقات الهوية وقواعد البيانات الشخصية وغيرها، فوسائل أمن المعلومات والأنظمة المعلوماتية عبارة عن آليات وإجراءات وأدوات ومنتجات تستخدم للوقاية وللتقليل من مخاطر المعلوماتية والتهديدات التي تتعرض لها الأنظمة المعلوماتية.

الفرع الأول: أنظمة الحماية التقنية في المصارف الإلكترونية:

سعيًا من المصارف الإلكترونية في توفير الحماية التقنية لعمليات الدفع الإلكتروني ووسائله فقد أوجدت لنفسها بعض الأنظمة التي تمكنها من أداء مهامها بأكثر سرية وموثوقية بحيث تمكنها من التحقق من شخصية العميل، وتؤكد في حالة التحكم في استخدامها بشكل صحيح أنّ المتعامل بها هو فعلاً صاحب الحساب وتعد هذه الأنظمة من قبيل التوقعات الإلكترونية المؤمنة ومن بينها:

أولاً - نظام هوية المستخدم وكلمة السر: نجدها أكثر رواجاً في المعاملات المصرفية الإلكترونية، فعند دخول العميل لموقع البنك على الأنترنت بقصد الاستفادة من الخدمات الإلكترونية، فإنّ أول ما يصادفه طلب إدخال هوية المستخدم وكلمة السر حتى يتمكن من الوصول لحسابه، وبالتالي فإنّ إدخالهما يشكل وسيلة للتحقق من الشخصية ودليلاً على أنّ الذي قام بالعملية هو صاحب الحساب، وإذا كان موقع البنك يسمح بإجراء العمليات بمجرد الدخول إليه باستخدام الهوية وكلمة السر فإنّ ذلك يشكلان دليلاً على إتجاه إرادة العميل إلى الالتزام بمقتضى العملية التي أجراها.¹⁶ يعتبر هذا النظام بمثابة توقيع إلكتروني لأنه لا يمكن إجراء أي العملية إلاّ بإدخال كلمة السر وهوية المستخدم وهي بذلك تكون مرتبطة برسالة المعلومات المتضمنة للعملية المجراة، وباعتبارها خاصة بالعمل وحده فإنّها تميز شخصه وتدل على إرادته في الالتزام بمضمونها.

ثانياً - نظام كلمة السر التي لا تتكرر: سيمت هذه الطريقة بكلمة السر التي لا تتكرر لأنّ كلمة السر المستخرجة من جهاز التوثيق لا تكون صالحة إلاّ لعملية واحدة وخلال مدة محددة بدقيقة واحدة فقط، وهي شأنها شأن الكلمة المستخرجة بطريقة خوارزمية القيمة الاختبارية تعتبر بمثابة توقيع إلكتروني.

يستخدم هذا النظام كوسيلة إضافية للنظام السابق، حيث تقوم بعض البنوك بإستخدامه مع عملائها عند إجراء العمليات التي تتضمن أوامر الدفع والتي تؤثر على الذمة المالية للعميل، ويتم ذلك بإشتراك كل من العميل والبنك للتوصل لكلمة سر التي لا تتكرر، حيث يتم تزويد كل منهما في البداية بنفس جملة المرور وعدد مرات إدخال البيانات لخوارزمية القيمة الاختبارية التي تعد عبارة عن مجموعة من العمليات الحسابية يتم من خلالها توليد مجموعة من الحروف ذات طول معين مستنتجة رياضياً من مجموعة أخرى من الحروف أطول بكثير وتمثل الرسالة المراد تشفيرها، كما تستخدم هذه العملية لاكتشاف تزوير البيانات

حيث أنّ أي تغيير ولو كان بسيطاً في الرسالة الأصلية يؤدي إلى تغيير كبير في القيمة الاختبارية، فيبدأ العميل بإرسال رسالة البداية، فيرد البنك برقم عشوائي يتم إستخدامه في إستخراج كلمة السر التي لا تتكرر عبر المرور بثلاث خطوات:

1- الخطوة التمهيديّة: حيث يدخل العميل جملة المرور ويتم إضافتها إلى الرقم العشوائي ثم ترسل للبنك.

2- خطوة التوليد: حيث يتم تنفيذ خوارزمية القيمة الاختبارية عدة مرات على هذه الجملة لإنتاج أو أكثر، هذا العدد من المرات هو المخزن في جهّازي العميل والبنك. Bit كلمة سر ذات 64 خانة "يعتمد عمل الحاسب الآلي على تحويل المعلومات بكافة أشكالها (بيانات مكتوبة، صوت، صورة) إلى أرقام ثنائية وتسمى بذلك لأنها مؤلفة على

وجه الحصر من أصفار واحد ويسمى كل صفراً واحداً بت ، وما أن يتم تحويل المعلومات إلى أرقام فإنه يصبح بالإمكان تخزينها في الكمبيوتر على شكل صفوف طويلة من البتات وهذه الأرقام هي ما يطلق عليها (المعلومات الرقمية).

3-خطوة العرض: حيث تأخذ كلمة السر المنتجة من المرحلة السابقة وتعرض بصورة مقروءة وفي المرحلة النهائية يستخدم العميل هذه الكلمة مرة واحدة بإرسالها للبنك الذي يتأكد من صحتها وبعد أن تتم العملية المراد إنجازها تصبح هذه الكلمة غير صالحة للاستعمال¹⁷ ، وإذا أراد العميل القيام بعملية بنكية أخرى يجب عليه إتباع نفس الخطوات السابقة .

الفرع الثاني-البصمة الإلكترونية:

ظهرت البصمة الإلكترونية بمناسبة ظهور التوقيع الإلكتروني، وبوجه التحديد التوقيع الرقمي، وهي نوع من أنواع التشفير باتجاه واحد، فتؤخذ الرسالة المراد تشفيرها وتحوّل للحصول على ما يسمى المفتاح الشفرة، وميزة هذا المفتاح أنه لا توجد طريقة فيه لفك التشفير والحصول على الرسالة الأصلية منه، ولهذا السبب سمي هذا الأسلوب بأسلوب التشفير باتجاه واحد، وهو يستخدم في الأنظمة التي تحتاج فيها للتحقق من صحة المعلومات دون الحاجة لمعرفة فحوى هذه المعلومات، وذلك لأنّ تشفير نفس الرسالة بنفس الخوارزمية ينتج مفتاح الشفرة نفسه في كل مرة، فهو يستخدم للتحقق من عدم التلاعب ببيانات أو ملفات معينة، فمثلاً إذا حصلنا على بيانات من أحدهم، فإنّ هناك احتمالاً بأنها قد تمّ التلاعب بها عمداً أو أنها أصيبت بفيروس ما، أو أنها حدث بها تغيير غير متعمد أثناء تنزيلها من الإنترنت بسبب عطل ما في الإتصال، فنحن بحاجة هنا لطريقة ما نتأكد فيها من تطابق نسخة البيانات التي لدينا مع البيانات الأصلية. إنّ البصمة الإلكترونية أو التشفير باتجاه واحد يستخدم غالباً في التوقيع الرقمي للتأكد من صحة البيانات المنقولة عن طريق وسيط إلكتروني.¹⁸

المبحث الثاني: الآليات القانونية لأمن الأنظمة المعلوماتية (هيئات الحماية)

أدى ظهور المعلوماتية وتطبيقاتها المتعددة إلى بروز مشاكل قانونية جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية ففرض حلها ضرورة البحث في الأوضاع القانونية القائمة ومدى ملائمتها لمواجهة هذه المشاكل ، ولما كان القاضي الجزائي مقيداً عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم فإنه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا على مستوى عال من الخطورة الإجرائية وتمس بالأمن السيبراني عامة.

رغم أنّ المشرع الجزائري حاول المواجهة من خلال حماية المعطيات عند معالجتها بالطرق الإلكترونية وذلك من خلال القانون 15-04 المعدل والمتمم للأمر 66-156 المتضمن قانون العقوبات، القسم السابع المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات، وأحكام قانون الإجراءات الجزائية الذي كرس ضمانات لعدم إساءة استخدام السلطة بانتهاك الحق في الحياة الخاصة في ما 44 وما يليها التي تكفل تلك الحماية هذا كأصل

عام ، وكذا من خلال القانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، فهي حماية ذات طابع عام لكل الإعتداءات الواقعة على البيانات الشخصية مهما كانت الوسائط المتدخلة في تداولها شبكات عامة أو خاصة، وتكريسا لأحكام المادة 4/46 من دستور 2016 التي تحمي المعطيات الخاصة في مجال المعالجة الآلية فقد صدر القانون 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الذي أقر ضمانات قانونية تشكل شكلا جديدا من أشكال الحماية.

كما خصّص الفصل الأول من الباب الثالث من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة أحكاما لحماية حقوق المؤلف تمكنه من حماية منتوجه الفكري، فللمؤلف بعض الحقوق عند تعرض برنامجه الحاسوبي للتغيير أو التحريف كحق سحب برنامجه شرط إلزامه بدفع تعويض عن الأضرار اللاحقة بالمستفيدين منه، الحق في إنتساب البرنامج له، الحق في الحفاظ لضمان سلامته من التعديل والتشويه (المادة 25 من الأمر أعلاه)، إلا أنّ كل تلك الجهود التشريعية لأمن الأنظمة المعلوماتية لم تثبت قدرتها للتصدي لقضايا الأمن السيبراني.¹⁹

لذا يحاول المشرع الجزائري التدخل بآليات مستحدثة ترعاها وزارة من بين الوزارات السيادية وهي وزارة الدفاع الوطني كون قضايا الأمن السيبراني يمس بسيادة الدولة الجزائرية ككل وذلك بناء على أحكام المرسوم الرئاسي رقم 05-20 لا سيما المادة الثالثة منه التي نصت «تشمل المنظومة الوطنية لأمن الأنظمة المعلوماتية الموضوعة لدى وزارة الدفاع الوطني ما يأتي:- مجلس وطني لأمن الأنظمة المعلوماتية، يدعي في صلب النص «المجلس»، ويكلف بإعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والموافقة عليها وتوجيهها، وكالة الأمن الأنظمة المعلوماتية تدعي في صلب النص «الوكالة»، وتكلف بتنسيق تنفيذ الاستراتيجية الوطنية الأمن الأنظمة المعلوماتية، ولممارسة مهامه يتوفر المجلس، بالإضافة إلى الوكالة على الهياكل المختصة لوزارة الدفاع الوطني في هذا المجال. لذا سنسعى من خلال هذا المحور لبيان مهام وتشكيلة كلا الهيئتين من خلال المطلبين المواليين:

المطلب الأول: المجلس الوطني لأمن الأنظمة المعلوماتية

إنّ المجلس الوطني لأمن الأنظمة المعلوماتية هيئة مستحدثة على غرار هيئات التصديق الإلكتروني التي أقرها القانون 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين، لذا سنتناول تحديد مهامها وتشكيلتها وطرق سيرها من خلال الفروع الموالية:

الفرع الأول: تشكيلة المجلس الوطني لأمن الأنظمة المعلوماتية

تضم تشكيلة المجلس الوطني لأمن الأنظمة المعلوماتية رئيسا يتمثل في وزير الدفاع الوطني أو ممثله ويتكون المجلس من تشكيلة تضم: ممثل عن رئاسة الجمهورية - ممثل عن الوزير الأول- الوزير المكلف بالشؤون

الخارجية - الوزير المكلف بالداخلية - الوزير المكلف بالعدل، - الوزير المكلف بالمالية، - الوزير المكلف بالطاقة، - الوزير المكلف بالاتصالات، - الوزير المكلف بالتعليم العالي.

كما يمكن أن يستعين المجلس بأي شخص أو مؤسسة من شأنه تنويره في أعماله.²⁰

الفرع الثاني: مهام المجلس الوطني لأمن الأنظمة المعلوماتية

يتولى المجلس، في إطار إعداد الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، على الخصوص المهام الآتية:- البت في عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديد.

- دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليهما.- دراسة التقارير المتعلقة بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها.- الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.- الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني.- الموافقة على تصنيف الأنظمة المعلوماتية - اقتراح لائحة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية، عند الحاجة، ويبيدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية.²¹

الفرع الثالث: سير المجلس الوطني لأمن الأنظمة المعلوماتية

يصادق المجلس على نظامه الداخلي بحيث يجتمع كلما دعت الضرورة إلى ذلك والهيئات العمومية والخاصة من أجل وضع إستراتيجية بناء على استدعاء من رئيسه،²² كما يتولى رئيس المجلس إعداد جدول أعمال مع ضمان اليقظة التكنولوجية في مجال أمن الأنظمة كما ينظم اجتماعات المجلس ويحدد تاريخها.²³

ترسل الإستدعاءات و جدول الأعمال إلى الأعضاء قبل خمسة (5) أيام، على الأقل، من تاريخ الاجتماع، وفي حالات الاستعجال، يمكن تبليغ جدول الأعمال خلال انعقاد الجلسة. أما فيما يخص قرارات المجلس فتتخذ بالأغلبية، وفي حال تساوي عدد الأصوات، يكون صوت الرئيس مرجحا²⁴، لذا تدون نتائج أشغال اجتماعات المجلس في محضر.²⁵ كما تتوج أعمال المجلس، حسب الحالة، بقرارات وتوصيات وآراء وتقارير، كما تفرد وتسجل الاعتمادات اللازمة لسير المجلس في ميزانية وزارة الدفاع الوطني.²⁶

المطلب الثاني: وكالة أمن الأنظمة المعلوماتية

كان للمشرع التونسي السبق في إنشاء الوكالة الوطنية للسلامة المعلوماتية التي استحدث بموجب القانون المتعلق بالسلامة المعلوماتية سنة 2014²⁷، وهي في تحيين مستمر فهي سنة 2019 شرعت في تنظيم ورشات تعنى بحماية البنى التحتية المعلوماتية الحيوية وآلية المراكز القطاعية للاستجابة للطوارئ المعلوماتية والسلامة العملياتية.

أما تبني المشرع الجزائري لوكالة أمن الأنظمة المعلوماتية جاء متأخرا مقارنة مع نظيره التونسي، حيث تعتبر الوكالة حسب نص المادة 17 من المرسوم الرئاسي، مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية

والاستقلالية المالية ويحدد مقر الوكالة في مدينة الجزائر.

الفرع الأول: مهام وكالة أمن الأنظمة المعلوماتية

يحدد تنظيم مكونات الوكالة وكيفية سيرها وكذا مهامها وصلاحياتها، بموجب قرار من وزير الدفاع الوطني²⁸، وتكلف الوكالة بموجب المادة 18 على الخصوص بما يأتي :

- تحضير عناصر الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس.
- تنسيق تنفيذ الإستراتيجية الوطنية في مجال لأمن الأنظمة المعلوماتية المحددة من قبل المجلس.
- اقتراح كيفية اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.
- إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية 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 لأمن 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 الإيمضاء الإلكتروني.- تحديد معايير وإجراءات منح علامة الجودة و/أو التصديق و/أو اعتماد المنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية طبقا للتشريع والتنظيم المعمول بهما.- القيام بنشاطات التموين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية....²⁹.

الفرع الثاني: تنظيم وسير وكالة أمن الأنظمة المعلوماتية

يتولى إدارة الوكالة لجنة توجيه وتزود بلجنة علمية، كما يكلف بتسييرها مدير عام وتتوفر على مركز وطني عملياتي الأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطته.³⁰

أولا- لجنة التوجيه:

لجنة التوجيه تشكيلة خاصة فضلا عن مهامها وهو ما سنأتي على بيانه من خلال العناصر الموالية:

- 1-تشكيلة لجنة التوجيه: يعين رئيس لجنة التوجيه طبقا للتنظيم المعمول به في وزارة الدفاع الوطني وتتكون لجنة التوجيه من ممثلي: وزارة الدفاع الوطني، - الوزارة المكلفة بالشؤون الخارجية، - الوزارة المكلفة بالداخلية، - الوزارة المكلفة بالعدل، - الوزارة المكلفة بالمالية، - الوزارة المكلفة بالطاقة، - الوزارة المكلفة بالتعليم العالي، - الوزارة المكلفة بالصناعة، - الوزارة المكلفة بالاتصالات، - الوزارة المكلفة بالتجارة، - مصالح الأمن، سلطة ضبط البريد والاتصالات الإلكترونية - السلطة الوطنية للتصديق الإلكتروني، - الهيئة الوطنية لحماية البيانات ذات

الطابع الشخصي،- السلطة الحكومية للتصديق الإلكتروني، وعلى سبيل الاستشارة، المدير العام للوكالة، على أن تتولى مصالح الوكالة أمانة لجنة التوجيه.

كما يمكن أن تستعين لجنة التوجيه بأي شخص أو مؤسسة من شأنها تنويرها في أعمالها³¹.

تحدد القائمة الاسمية لأعضاء لجنة التوجيه بموجب قرار من وزير الدفاع الوطني، بناء على اقتراح السلطات التي ينتمون إليها، ولا يمكن أعضاء لجنة التوجيه انتداب من يمثلهم في حال غيابهم³².

2- مهام لجنة التوجيه: تكلف لجنة التوجيه، على الخصوص بالمهام الآتية :

- دراسة واقتراح عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية.

- دراسة البرامج السنوية والمتعددة السنوات التنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية، والمصادقة عليها، - تقييم نتائج مجموع الأعمال التي قامت بها الوكالة.- تحديد الطرق والوسائل اللازمة للاستجابة للحاجات الوطنية في مجال أمن الأنظمة المعلوماتية.- ضبط الطرق والوسائل اللازمة لترقية البحث والتطوير في مجال أمن الأنظمة المعلوماتية والتطبيقات ذات الصلة بالاحتياجات الوطنية.- التداول في كل المسائل التي تتعلق بتنظيم وسير الوكالة، ولا سيما منها حصائل الأنشطة والتسيير المالي للسنة المالية

المنصرمة والبيانات التقديرية للإيرادات والنفقات ومخطط توظيف وتكوين المستخدمين وكذا مرتبات مستخدمي الوكالة.- الموافقة على النظام الداخلي للوكالة.

3- سير لجنة التوجيه: تجتمع لجنة التوجيه في دورة عادية أربع (4) مرات في السنة، بناء على استدعاء من رئيسها. ويمكنها أن تجتمع في دورة غير عادية كلما دعت الضرورة إلى ذلك حسب الكيفيات التي يسطرها النظام الداخلي، كما تعد لجنة التوجيه نظامها الداخلي وتصادق عليه في اللجنة العلمية في كل دورتها الأولى، كما تدون نتائج أعمال لجنة التوجيه في محضر، وتكون موضوع تقرير يرسل إلى وزير الدفاع الوطني³³.

ثانيا- المدير العام لوكالة أمن الأنظمة المعلوماتية:

يعين المدير العام للوكالة طبقا للتنظيم المعمول به في وزارة الدفاع الوطني وتنتهي مهامه حسب الأشكال نفسها³⁴ ، كما يسهر المدير العام على تنسيق تنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية وينفذ المخططات والبرامج المسطرة من قبل لجنة التوجيه.

1- مهام المدير العام لوكالة أمن الأنظمة المعلوماتية: المدير العام مسؤول عن سير الوكالة وتولى تسييرها ضمن احترام التشريع والتنظيم المعمول بهما، وهذه الصفة:- يعد مخطط عمل وبرامج نشاط الوكالة ويعرضها على لجنة التوجيه للموافقة عليها.- يحضر مشروع الميزانية التقديرية ويعرضه على لجنة التوجيه للمداولة ويتولى تنفيذ ذلك.- يبرم الصفقات ويوقع العقود والاتفاقيات ذات الصلة بمهام الوكالة طبقا للتنظيم المعمول به.- يتصرف باسم الوكالة ويمثلها أمام الهيئات القضائية.- يمارس السلطة السلمية على جميع مستخدمي الوكالة.- يعد النظام الداخلي للوكالة- يسهر على القيام بإجراءات تأهيل مستخدمي الوكالة - هو الأمر بصرف ميزانية

الوكالة.- يعد المدير العام للوكالة تقريراً سنوياً عن نشاطات الوكالة ويرسله إلى رئيس المجلس.- يعين المديرون ورئيس المركز الوطني العملياتي لأمن الأنظمة المعلوماتية ورؤساء المصالح طبقاً للتنظيم المعمول به في وزارة الدفاع الوطني³⁵.- يحدد التنظيم الداخلي للوكالة بموجب قرار من وزارة الدفاع الوطني، بناءً على اقتراح مديرها العام بعد موافقة لجنة التوجيه³⁶.

ثالثاً- اللجنة العلمية للوكالة:

تتكون اللجنة العلمية من عشرة (10) أعضاء يتم اختيارهم لمدة 03 سنوات قابلة للتجديد، من قبل لجنة التوجيه من بين الأساتذة والباحثين والخبراء في مجال أمن الأنظمة المعلوماتية³⁷.

1- مهام اللجنة العلمية للوكالة:

يستشير المدير العام للجنة العلمية في كل مسألة ذات طابع علمي تندرج ضمن إطار مهام الوكالة المتعلقة بنشاطات البحث والتطوير في مجال أمن الأنظمة المعلوماتية.

وتبدي اللجنة رأيها وتوصياتها فيما يأتي:- تجانس البرامج والمشاريع المقترحة من المدير العام للوكالة.

-كيفية تنفيذ برامج ومشاريع البحث والتطوير.- اختيار واقتناء المراجع العلمية.- التنظيم والمشاركة في الأحداث والتظاهرات العلمية المتعلقة بأمن الأنظمة المعلوماتية، - نشاطات التكوين العلمي والإتقان وإعادة التأهيل لفائدة مستخدمي الوكالة، وكذا المستخدمين المكلفين بأمن الأنظمة المعلوماتية في الإدارات والمؤسسات والهيئات العمومية.- كل المسائل ذات الطابع العلمي التي يعرضها عليها المدير العام للوكالة.

تصادق اللجنة العلمية على نظامها الداخلي خلال دورتها الأولى³⁸.

فضلاً عن ذلك، يمكن للجنة العلمية الاستعانة بأي شخصية علمية أو خبير بإمكانه المساهمة مساهمة مفيدة نظراً لكفاءاته في مجال أمن الأنظمة المعلوماتية³⁹.

الخاتمة:

نظراً لكون الآليات التقنية لم تعد كافية لوحدها تدخل المشرع الجزائري بخطوة تشريعية من نوع خاص حيث أناط مهام أمن الأنظمة المعلوماتية لجهاز سيادي وهو وزارة الدفاع الوطني باعتبارها الهيئة العليا الوصية على الهيئات التي استحدثتها بموجب المرسوم الرئاسي رقم 20-05 والمتمثلة أساساً في المجلس الوطني لأمن الأنظمة المعلوماتية إلى جانب وكالة أمن الأنظمة المعلوماتية التي تضم تشكيلة ثلاثية مكونة من لجنة التوجيه، مديراً عاماً ولجنة علمية مختصة تتولى البت في إجراء التحقيقات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية، حيث تمارس الوكالة مهامها تحت إشراف ومتابعة المجلس، وهذا انطلاقاً من كون قضايا الأمن المعلوماتي تكتسي أهمية قصوى خاصة على الصعيد الدولي لكونها تمس بالسيادة الوطنية والأمن السيبراني الذي تسعى كل الدول لتأمينه من كافة النواحي التقنية والهيكلية في مواجهة مختلف الهجمات السيبرانية التي يمكن أن تتعرض لها بنيتها المعلوماتية مما يعرض أمنها المعلوماتي الداخلي والخارجي للخطر، لكن ما يؤخذ على

هذا المرسوم بعض الغموض خاصة فيما يتعلق بـ:

- وجود نوع من التداخل في الصلاحيات بين المجلس والوكالة خاصة فيما يتعلق بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية.
 - تناقض فيما يخص اعتماد منظومات إنشاء وفحص الإيمضاء الإلكتروني كمهمة من مهام وكالة أمن الأنظمة المعلوماتية والتي حددت مسبقا كصلاحيات من صلاحيات سلطات التصديق الإلكتروني الثلاث وكذا الأشخاص المتدخلة في عمليات التصديق (الشخص الثالث الموثوق، مؤدي خدمات التصديق الإلكتروني)، فحاليا ومن الناحية العملية تتمثل السلطة الحكومية للتصديق الإلكتروني في سلطة ضبط البريد والمواصلات السلكية واللاسلكية التي تمارس مهامها لفترة إنتقالية حددها المشرع بخمس سنوات كحد أقصى لحين تنصيب سلطات التصديق الثلاث وهذا ما يتضح من خلال المادتين 78 و79 من القانون 04-15، فهل استحداث المجلس والوكالة بالمرسوم الرئاسي 20-05 يعد إقرارا ضمنيا بإلغاء صلاحيات سلطات التصديق الإلكتروني.
 - أن المرسوم الرئاسي أوكل للمجلس الوطني لأمن الأنظمة المعلوماتية مهمة الموافقة على سياسية التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني التي لم يتم تنصيبها بعد.
- الهوامش:

- 1 - عدنان مريزق، بوقلاشي عمار، «الأمن المعلوماتي في ظل التجارة الإلكترونية»، مجلة الإقتصاد الجديد، عدد3، ماي 2011، ص8.
- 2 - بوربابة صورية، قواعد الأمن المعلوماتي، رسالة مقدمة لنيل شهادة الدكتوراه ، كلية الحقوق و العلوم السياسية ، جامعة الجيلالي اليابس ، سيدي بلعباس، 2015-2016، ص51-53.
- 3 - أحمد بن علي عبد الله طارش، رؤية إستراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والإدعاء العام في المملكة العربية السعودية، مذكرة مقدمة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية ، كلية العلوم الاستراتيجية، 2015 ص44-46.
- 4 - الجواد دلال صادق ، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع ،الأردن، 2008، ص41 وما يليها . الجواد دلال صادق ، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع ،الأردن، 2008، ص41 وما يليها .
- 5 - عبد الرحمان بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، ط2004، 1، ص396.
- 6 - أمان الخالد، «القرصنة.خطوة خطوة» ، مقال بجريدة الرياض ، عدد 12393، سنة2002، ص45.
- 7 - عبد الرحمان بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، المرجع السابق، ص400.
- 8 - ملوم كريم، الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية، مذكرة ماجستير فرع قانون التعاون الدولي، مدرسة الدكتوراه بكلية الحقوق بجامعة تيزي وزو، 2014، ص193.
- 9 - القانون رقم 15. 04 المؤرخ في أول فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج رعد

06، ص 07.

10 - قانون عدد 83 لسنة 2000 مؤرخ في 9 أوت 2000 يتعلق بالمبادلات والتجارة الإلكترونية التونسي على الموقع www.arablawn.com

arablawn.com

- 11 - عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها ط1، منشورات الحلبي الحقوقية، لبنان، 2010، ص236 وما يليها.
- 12 - عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، دون طبعة، دار الفكر الجامعي، الإسكندرية 2002، ص196.
- 13 - خالد مصطفى فهي، النظام القانوني للتوقيع الإلكتروني في ضوء الإتفاقات الدولية والتشريعات العربية-دار الجامعة الجديدة للنشر- 2007، ص101.
- 14 - دالة البعثة: هي عملية رياضية مبنية على خوارزمية تنشئ صورة رقمية للرسالة أو شكلا مضغوطة من الرسالة يشار إليها بعبارة «خلاصة - رسالة و/أو بصمة رسالة، ودالة البعثة لا بد أن تكون ذات إتجاه واحد أي لا بد أن تكون ذات اتجاه واحد أي لا بد من التحقق من استحالة استخراج الرسالة الأصلية إنطلاقا من معرفة دالة البعثة الخاصة بها، دليل الإشتراع الخاص بالقانون النموذجي الخاص بالتوقيع الإلكتروني، منشور بدليل الأمم المتحدة لسنة 2001، ص28-29.
- 15 - إقرأ المزيد على موضوع.كوم <https://mawdoo3.com>
- 16 - أبو فورة محمود: الخدمات البنكية الإلكترونية عبر الأنترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2009، ص86.
- 17 - أبو فورة محمود، نفس المرجع السابق.
- 18 - <http://www.ahmadh.com/weblog/2005/06/27/asymmetric-key-encryption>
- 19 - الأمر 05-03 مؤرخ في 19 يوليو 2003 يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر 44 المؤرخة في 23 يوليو 2003.
- 20 - المادة 05 من المرسوم الرئاسي 05-20 المؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر عدد 04 المؤرخة في 26 جانفي سنة 2020.
- 21 - المادة 04 من المرسوم الرئاسي 05-20.
- 22 - المادة 12 من المرسوم الرئاسي 05-20.
- 23 - المادة 13 من المرسوم الرئاسي 05-20.
- 24 - المادة 14 من المرسوم الرئاسي 05-20.
- 25 - المادة 15 من المرسوم الرئاسي 05-20.
- 26 - المادة 16 من المرسوم الرئاسي 05-20.
- 27 - القانون عدد 5 لسنة 2004، مؤرخ في 3 فيفري 2004 يتعلق بالسلامة المعلوماتية، على الموقع الإلكتروني: <http://legislation-securite.tn>.
- 28 - المادة 34 من المرسوم الرئاسي 05-20.
- 29 - المادة 19 من المرسوم الرئاسي 05-20.
- 30 - المادة 20 من المرسوم الرئاسي 05-20.
- 31 - المادتين 21 و22 من المرسوم الرئاسي 05-20.
- المادة 23 من المرسوم الرئاسي 05-20.

33 - المادة 26 من المرسوم الرئاسي 05-20.

34 - المادة 27 من المرسوم الرئاسي 05-20.

35 - المادة 29 من المرسوم الرئاسي 05-20.

36 - المادة 30 من المرسوم الرئاسي 05-20.

37 - المادة 31 من المرسوم الرئاسي 05-20.

38 - المادة 32 من المرسوم الرئاسي 05-20.

39 - المادة 33 من المرسوم الرئاسي 05-20.

المراجع:

أولا- الكتب:

- أبو فورة محمود: الخدمات البنكية الإلكترونية عبر الأنترنت، ط1، دار الثقافة للنشر والتوزيع، الأردن، 2009.

- الجواد دلال صادق، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2008.

- خالد مصطفى فهمي، النظام القانوني للتوقيع الإلكتروني في ضوء الإتفاقات الدولية والتشريعات العربية-دار الجامعة الجديدة للنشر 2007-.

- عبد الرحمان بن عبد الله السند، الأحكام الفقهية للتعاملات الإلكترونية، ط1، 2004.

- عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها ط1، منشورات الحلبي الحقوقية، لبنان، 2010.

- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الكتاب الأول، دون طبعة، دار الفكر الجامعي، الإسكندرية 2002-.

-الرسائل والمذكرات:

- بوربابة صورية، قواعد الأمن المعلوماتي، رسالة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجليلي اليايس، سيدي بلعباس، 2015-2016.

- أحمد بن علي عبد الله طارش، رؤية إستراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والإدعاء العام في المملكة العربية السعودية، مذكرة مقدمة لنيل شهادة الماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، 2015.

- ملوم كريم، الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية، مذكرة ماجستير فرع قانون التعاون الدولي، مدرسة الدكتوراه بكلية الحقوق بجامعة تيزي وزو، 2014.

-المقالات:

-أمان الخالد، «القرصنة.خطوة خطوة»، مقال بجريدة الرياض، عدد 12393، سنة 2002.

-عدمان مريزق، بوقلاشي عمار، «الأمن المعلوماتي في ظل التجارة الإلكترونية»، مجلة الإقتصاد الجديد، عدد 3، ماي 2011.

-النصوص القانونية:

- القانون رقم 04_15 المؤرخ في أول فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر عدد 06
- الأمر 03-05 مؤرخ في 19 يوليو 2003 يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر 44 المؤرخة في 23 يوليو 2003.
- المرسوم الرئاسي 05-20 المؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج ر عدد 04 المؤرخة في 26 جانفي سنة 2020.
- قانون عدد 83 لسنة 2000 مؤرخ في 9 أوت 2000 يتعلق بالمبادلات والتجارة الإلكترونية التونسية على الموقع www.arablaw.com