المغرب وتحديات الأمن السيبراني

ياسين الفشتالي
طالب باحث بسلك الدكتوراه
كلية العلوم القانونية والاقتصادية والاجتماعية بفاس
المغرب

المقدمة

نعيش اليوم في خضم مجتمع المعرفة والمعلومات، مجتمع الاتصال الشبكي أين أصبح التدفق المعلوماتي أسرع من أي تدفق آخر عرفته البشرية، فصارت مستحدثات هذه المرحلة تفوق بأشواط كبيرة المراحل الإنسانية السابقة جودة وسرعة وسعة وثراء. وهو ما نقل العالم من التقارب إلى التلاحم الجغرافي هذا التدفق ساهم في غزارة ووفرة معلوماتية غير مسبوقة أفضت إلى ظاهرة الانفجار المعلوماتي بما له وعليه من إيجابيات وسلبيات على المجتمع الدولي، كما تسبب من جهة أخرى في مشاكل أمنية كثيرة متفاوتة الخطورة والضرر على الأفراد والدول، استدعت في الكثير من الحالات التدخل لحماية البيانات والمعلومات الشخصية والمشتركة خاصة تلك المتعلقة بالسيادة الوطنية والأمن القومي وهو ما يطلق عليه تسمية الأمن السيبراني.[1]

فإذا كان الأمن يعتبر الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيدا عن تحققه سواء أكان ذلك على المستوى التقني، أم على المستوى القانوني. فقد تحول الأمن مع بروز مجتمع المعلومات والفضاء السيبراني إلى واحد من قطاع الخدمات التي تشكل قيمة مضافة ودعامة أساسية لأنشطة الحكومات والأفراد على السواء كما هو الحال مع التطبيقات الخاصة بالحكومة الإلكترونية والصحة الإلكترونية وغيرها.

فلقد بات الأمن السيبراني يشكل جزءا من أي سياسة أمنية وطنية، حيث أصبح معلوما أن صناع القرار في الولايات المتحدة الامريكية والاتحاد الأوربي والصين وغيرهم من الدول يصنفون مسائل الدفاع السيبراني كأولوية في سياستهم الدفاعية الوطنية بحيث أعلنت العديد من الدول تخصيص أقساما خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني.

و لمواكبة هذه المتغيرات، أعطت المملكة المغربية أهمية كبرى لورش الرقمنة من خلال تنفيذ العديد من البرامج مثل المغرب الرقمي ، و من أجل دعم هذا التحول اختارت المملكة المغربية أن تتجاوب بصورة مناسبة مع المخاطر و التحديات الناجمة عن التهديدات من خلال تحديث استراتيجيتها الوطنية للأمن السيبراني "الاستراتيجية الوطنية للأمن السيبراني2030"، و إصدار القانون رقم 05.20 المتعلق بالأمن السيبراني.[2] إضافة إلى إنشاء المديرية العامة لأمن نظم المعلومات[3] واللجنة الاستراتيجية للأمن السيبراني[4]، ناهيك عن سن مجموعة من القوانين المهمة[5].

وعلى هذا الأساس من الأهمية، وقع اختيارنا على موضوع المغرب وتحديات الأمن السيبراني كنواة لورقتنا البحثية التي نحاول من خلالها الإجابة عن الإشكالية التالية: **ما هي أهم التحديات التي تواجه المغرب لتحقيق الأمن السيبراني بالرغم من جهوده المبذولة؟**

تحقيقا لإشكالية الدراسة وموضوعها، تم طرح العديد من التساؤلات الفرعية، جاءت كالتالي:

- ✓ ما المقصود بالأمن السيبراني؟
- ✓ ما هي الجهود المبذولة من طرف المغرب بمواجهة الجريمة السيبرانية؟
- ✓ ما هي التحديات التي تواجه مساعي إقرار الأمن السيبراني بالمملكة المغربية؟

وابتغاء تحليل ومناقشة الموضوع سنعمل إلى تقسيمه إلى محورين على النحو التالي:

المحور الأول: الأحكام العامة للأمن السيبراني بالمغرب

المحور الثاني: تحديات المغرب في مجال الأمن السيبراني

المحور الأول: الأحكام العامة للأمن السيبراني بالمغرب

لقد أدى التحول الرقمي المتسارع عبر العالم[6]، إلى ضرورة تحقيق الأمن السيبراني، الذي يعد ركيزة أساسية لحماية الأفراد والمؤسسات والدول، من هنا يمكن تعريف الأمن السيبراني أنه مجموعة من الأدوات والسياسات والتقنيات الهادفة إلى حماية الأنظمة والشبكات والبيانات من الهجمات الرقمية، التي تشير التقديرات إلى تعرض العالم لأكثر من 21 مليار هجمة سيبرانية يوميا مع خسائر متوقعة تقدر ب 10.5 تريليون دولار بحلول عام[20257]، مقارنة ب 3 تريليونات في 2015.

فالأمن السيبراني يعتبر مصطلحا جديدا نسبيا لمجموعة من الممارسات القديمة حول أمان شبكة المعلومات إلا أنه يتسم بوجود تعارض في تعريفاته ويتجلى ذلك في رفض بعض الجهات الحكومية في عدد من الدول الاتفاق على مفردات مشتركة.

فقد عرف المشرع المغربي الأمن السيبراني من خلال المادة الثانية من القانون رقم 20-05 بأنه:" مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقاوم أحداثا مرتبطة بالفضاء السيبراني من شأنها أن تمس بتوافر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلة والخدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالولوج إليه".

وحسب الاتحاد الدولي للاتصالات فالأمن السيبراني هو" مجموعة من الأدوات والسياسات والمفاهيم الأمنية والتحفظات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب، وغيرها من الممارسات وآليات الضمان والتكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسات والمستعملين من المخاطر الأمنية ذات الصلة في البيئة السيبرانية.[8]

كما عرفه المركز الوطني البحريني للأمن السيبراني بأنه عملية حماية الأنظمة والبيانات والاتصالات والشبكات الموجودة والمتصلة بالإنترنيت ضد الهجمات الرقمية. فهذه الهجمات التي يشار إليها باسم "الهجمات السيبرانية"، ما هي إلا محاولة اختراق أو تعديل أو تعطيل أو دخول أو استخدام غير مشروع وبالتالي يمكن أن تتراوح الهجمات السيبرانية من تثبيت رموز برمجية ضارة على جهاز حاسوب شخصي وصولا إلى محاولة تدمير البنية التحتية لدول بأكملها.[9]

يمكن القول إذا أن مفهوم الأمن السيبراني بالرغم من كونه مفهوم معقد حيث يحمل الكثير من المعاني والتعريفات المختلفة إلا أن جل التعريفات تتفق على وظيفته العامة تقريبا.

يعتبر الأمن السيبراني قطاع استراتيجي في مجال حماية الرقمنة والفضاء الرقمي، وتسعى الدول في الوقت الحالي إلى إيلائه العناية الفائقة على غرار الأوجه الأخرى من الأمن الشامل كالأمن الداخلي والخارجي، الأمن السياسي، الأمن الغذائي وكذلك لارتباط الأمن السيبراني بحماية البيانات والمعطيات بكل أنواعها. لهذا عمل المغرب على مكافحة الجريمة السيبرانية وبذل مجهودات كبيرة في سبيل تحقيق الأمن السيبراني.

إذ تظهر ملامح هذا الاهتمام والجهود المبذولة على مستويين:

أولا: على المستوى الدولي

نلامس ذلك من خلال وعي المغرب بأهمية التعاون الدولي في مجال الأمن السيبراني والعمل على تحسين آليات هذا التعاون، ولعل أهم هذه الآليات الاتفاقيات والمعاهدات الدولية.

فاتفاقية بودابست المتعلقة بالإجرام السيبراني والاتفاقية العربية لمكافحة جرائم تقنية المعلومات تشكل حجر الزاوية في شأن التعاون الدولي في مجال الأمن السيبراني ومكافحة الجريمة السيبرانية، إذ أن الاتفاقية الأولى خصصت الباب الثالث منها كاملا للتعاون الدولي في مجال الأمن السيبراني، بينما خصصت الاتفاقية الثانية أحكام الفصل الرابع منها للتعاون القانوني والقضائي في مجال مكافحة جرائم تقنية المعلومات.

إلى جانب هاتين الاتفاقيتين تم كذلك إبرام مجموعة من الاتفاقيات الثنائية في هذا المجال كتوقيع المغرب مذكرة تفاهم للتعاون في مجال الأمن السيبراني مع دولة الإمارات بتاريخ 19 أكتوبر 2023 بدبي، وذلك على هامش معرض "جيتكس جلوبال 2023"، بحيث التزم البلدان بالتعاون لمواجهة المخاطر المتزايدة في المملكة المغربية ومجلس الأمن السيبراني الإماراتي.

ثانيا: على المستوى الوطني

حقق المغرب تقدما ملحوظا في ميدان الأمن السيبراني، في انعكاس لاعترافه المتزايد بأهمية بنيته التحتية الرقمية وبياناته. فقد أظهر التزاما واضحا عبر إنشاء هيئات وأطر متخصصة مثل المديرية العامة لأمن نظم المعلومات، والوكالة الوطنية لتقنين المواصلات، وفريق الاستجابة لطوارئ الحاسوب المغربي، واللجنة الوطنية لحماية المعطيات الشخصية، والمركز المغربي للبحث والابتكار المتعدد التقنيات.[10]

من خلال سنه لمجموعة من الإجراءات الوقائية والأمنية وهيئات الحكامة الكفيلة بضمان حماية فعالة من مختلف التهديدات التي ممكن أن تطال الأنظمة المعلوماتية، بالإضافة إلى القوانين المرتبطة بالمجال الإلكتروني، فضلا عن التوجهات والاستراتيجيات في هذا المجال.

فعلى المستوى التشريعي أولى المشرع المغربي لإجراءات حماية نظم المعلومات أهمية بالغة حيث من خلال القانون رقم 05.20 المتعلق بالأمن السيبراني الذي ينص على مجموعة من تدابير الأمان ذات الطبيعة التنظيمية والتقنية التي تهدف إلى تعزيز القدرات الوطنية في مجال الأمن السيبراني، وتنسيق جهود الوقاية والحماية من الهجمات والحوادث المتعلقة بالأمن السيبراني. خصص لها الفصل الثاني منه وهذا الفصل مقسم إلى ثلاث فروع، الفرع الأول[11] خصصه لأحكام خاصة بالهيئات، أما الفرع الثاني فخصصه للأحكام الخاصة بالبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة،[12] وأخيرا الفرع الثالث من هذا الفصل خصص للأحكام الخاصة بالمتعهدين.[13]

فبالإضافة إلى القانون 05.20 نجد المشرع المغربي واجه الجريمة السيبرانية بإصدار مجموعة من النصوص التشريعية لمواكبة هذا النوع من الإجرام. ولعل أبرز مظاهر المواجهة التشريعية للإجرام السيبراني يتمثل في المقتضيات التشريعية الواردة في مجموعة القانون الجنائي، ثم المقتضيات الواردة في القوانين المتعلقة بالمعاملات الإلكترونية.[14]

في نفس السياق، لتأمين حماية الفضاء الرقمي وضمان تطبيق مقتضيات القانون رقم 05.20 ومراسيمه التطبيقية، في هذا المجال تم إنشاء مجموعة من الهيئات والمؤسسات التي لها اختصاصات رقابية وضبطية وتنظيمية تتمثل في:

- **اللجنة الاستراتيجية للأمن السيبراني**

تم إحداث اللجنة بموجب القانون 05.20 وذلك بهدف تأمين البيئة الرقمية الحاضنة للبنيات التحتية من التهديدات الداخلية والخارجية كقرصنة البيانات أو تهديدات سيبرانية، ويترأس هذه اللجنة الوزير المنتدب لدى رئيس الحكومة المكلف بإدارة الدفاع الوطني، وقد حدد المشرع مهامها بمقتضى المادة 35 من نفس القانون.

- **لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة**

أحدثت لدى اللجنة الاستراتيجية للأمن السيبراني لجنة يصطلح عليها بلجنة إدارة الأزمات والأحداث السيبرانية الجسيمة تترأسها المديرية العامة لأمن نظم المعلومات، فهي تعمل على إعداد إطار لإدارة الأزمات والأحداث السيبرانية الجسيمة يحدد مجال تدخل كل عضو من أعضاء هذه اللجنة فضلا عن الإجراءات والتدابير المرتبطة بإدارتها وكيفية التواصل وتبادل المعلومات يتم عرضه على اللجنة الاستراتيجية للأمن السيبراني قصد المصادقة عليه.[15]

- **السلطة الوطنية للأمن السيبراني**

لم يعرف المشرع المغربي ما المقصود بالسلطة الوطنية في إطار القانون 05.20 وهو أمر كان لابد منه، وذلك من أجل فك الغموض بشأن هذا الجهاز الذي يجب على كافة الهيئات المشار إليها في المادة الأولى من القانون المذكور أن تتبع إرشاداتها وأن تتواصل معها بخصوص المخاطر أو العوارض التي قد تصادفها، واستنادا إلى الصلاحيات المخولة لها في المواد 38 وما يليها يمكن القول بأن السلطة الوطنية عبارة عن جهاز إداري يمكن نعته كذلك بدركي الفضاء السيبراني يختص قانونا بمهام الرقابة والتوجيه والتتبع لكافة الهيئات.[16]

بالرغم من المجهودات المبذولة من قبل المغرب سواء على المستوى الدولي أو الوطني إلا أنه لازال أمامه العديد من التحديات لتحقيق الأمن السيبراني بشكل فعال.

المحور الثاني: تحديات المغرب في مجال الأمن السيبراني

ارتباطا بالسياق الاستراتيجي، فإن المغرب يمثل حالة دراسية متميزة و معقدة في نفس الوقت في مجال الأمن السيبراني بمنطقة شمال إفريقيا، يتمثل ذلك في التناقض بين التقدم المؤسساتي، و بين التحديات الهيكلية، حيث أنه من جهة، يحتل المرتبة الأولى إفريقيا والعاشرة عالميا في مؤشر الأمن السيبراني العالمي[17] (GCI 2024) بحصوله على 100/97.5 نقطة، ومن جهة أخرى، يصنفه الإنتربول[18] كأكثر دولة إفريقية تعرضا لهجمات أحصنة طروادة المصرفية[19] (18,827 هجمة في 2022)، هذا التناقض يفرض تحليلا شاملا لأسس النجاح، ومعيقات التطور، واستشراف المستقبل في ظل تصاعد الهجمات المرتبطة بالتوترات الجيوسياسية، خاصة مع الجزائر.

أولا: الفجوات التشريعية:

كما هو متعارف عليه، يعتبر التنظيم القانوني، الإطار الذي يتم فيه تحديد القواعد والإجراءات التي تنظم سلوك الأفراد أو المؤسسات في مجال معين، و المغرب بخصوص مجال الأمن السيبراني، نص على مجموعة من القوانين من قبيل القانون 08.09 المتعلق بحماية المعطيات الشخصية، بالإضافة إلى القانون 20.43 المتعلق بالتوقيع الالكتروني، و نص أيضا على القانون 05.20 المتعلق بالأمن السيبراني، هذا الأخير الذي يشكل الإطار الأساسي في المجال السيبراني، حيث وضع مجموعة من القواعد والتدابير الأمنية الرامية إلى تعزيز أمن وصمود نظم معلومات إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري آخر خاضع للقانون العام وكذا البنيات التحتية ذات الأهمية الحيوية التي تتوفر على نظم معلومات حساسة.

لكن بالرغم من هذه النصوص التشريعية وخاصة القانون 05.20، يلاحظ مجموعة من السلبيات المسجلة بخصوصها، تتمثل في وجود ثغرات قانونية وتنظيمية، وذلك بغياب إطار قانوني متكامل يتماشى مع المعايير الدولية[20]، مثل GDPR الأوروبي، والتي تتميز بمجموعة من التعديلات المستمرة باستمرار تطور التهديدات، ما يفرض على القوانين الوطنية هي الأخرى مواكبة التحديثات العالمية في هذا المجال.

إن ما يزيد من فقامة التنظيم القانوني هو تعقيدات الامتثال لهذه القوانين المتعددة، والذي يرجع بالدرجة الأولى أن النصوص القانونية قد تكون غير واضحة أو غير محددة، مما يجعل من الصعب على المؤسسات فهم ما هو مطلوب منها، ما يتطلب الأمر إلى وضع استراتيجيات

قانونية مخصصة، بالإضافة إلى خلق آليات الاستشارات القانونية المتخصصة لتقديم استشارات دورية لضمان أن تظل المؤسسات والشركات الكبرى على دراية بالتطورات القانونية المستمرة في مجال الأمن السيبراني.

كما يشكل ضعف العقوبات الزجرية للجرائم الالكترونية، ثغرة قانونية كبيرة في التنظيم التشريعي المتعلق بالأمن السيبراني، ما يعزز فرص ارتكاب الجرائم الالكترونية و الانفلات من العقاب، فسياسة التجريم و العقاب في مجال الجرائم السيبرانية يجب أن يكون متشددة، بهدف تحقيق الردع الاستباقي، فعلى الرغم من تنصيص المشرع الجنائي على مجموعة من النصوص التي تعاقب على الجرائم الالكترونية، من خلال القانون رقم 03-07 بشأن تتميم مجموعة القانون الجنائي فيما يتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات، هذا فضلا عن الأخرى المتفرقة في نصوص خاصة، إلا أنه يبقى غير كافي و غير مواكب لتطور الجرائم الالكترونية التي تتسم بخصائص[21] تميزها عن غيرها من الجرائم.

ثانيا: التحديات ذات الأبعاد الجيوسياسية:

إن من أكبر التحديات التي يعرفها الأمن السيبراني، هي التهديدات السيبرانية، وتتنوع أشكال الهجمات السيبرانية وتختلف باختلاف التقنيات الحديثة، وقدرات المهاجمين والمخترقين الذين يحرصون ويحاولون دائما الالتفاف على الأنظمة الأمنية السيبرانية واختراقها وابتداع وتطوير أساليب جديدة لتحقيق أهدافهم.

من فإن أسباب هذه التهديدات تتعدد وتختلف في الزمان والمكان، وتلعب الدوافع الجيوسياسية دورا كبيرا في تكريس الهجمات من قبيل صراع المغرب والجزائر حول الصحراء المغربية، أو دعم القضية الفلسطينية، وقد يكون الهاجس الاقتصادي دافعا في كبيرا لتوجيه الهجمات.

لا يخفى على الجميع في وقتنا الراهن أن الفضاء السيبراني أصبح ساحة لـ"الحرب بالوكالة"[22]، حيث تنفد هجمات انتقامية كما يقع في معظم دول العالم خاصة تلك التي تعرف صراعات جيوسياسية، و قد أشارت العديد من التقارير الدولية[23] و الوطنية أن المغرب من بين البلدان المتصدرة في تلقي الهجمات السيبرانية إفريقيا، و التي ترشح حسب مجموعة من المؤشرات أن سبب وقوع الهجمات السيبرانية في المغرب مثل الهجوم الأخير (أبريل 2025)، على مواقع وزارة الداخلية المغربية و التسريبات التي طالت الموقع الصندوق الوطني للضمان الاجتماعي (CNSS)، يرجع أساسا للصراعات الجيوسياسية المرتبطة بالمغرب[24].

وقد سجلت أبرز الهجمات في الفترة ما بين (2012–2025)[25]:

- سنة 2012: ضد بنك المغرب المركزي " اختراق الموقع " من طرف: "أنونيموس"[26].
- سنة 2014: ضد وزارة الخارجية ومواقع حكومية "تشويه المحتوى " قراصنة.
- سنة 2018: ضد القناة التلفزيونية الثانية" تعطيل البث " جماعات "هاكتيفيست"[27].
- سنة 2019: ضد بورصة الدار البيضاء "تسريب بيانات "مجموعات مجهولة.
- سنة 2025: ضد الصندوق الوطني للضمان الاجتماعي " تسريب 44 ألف وثيقة " جماعات (DDOS54).

ثالثا: تحديات ذهنية أو بشرية

من بين التحديات التي يعرفها الأمن السيبراني في المغرب، تلك المتعلقة بالجانب البشري، إذ تتمظهر في نقص الكفاءات المتخصصة، في مجال الأمن السيبراني، و إن وجدت فهي تحتاج إلى التطور و التدريب المستمر، بالإضافة إلى التأهيل لمواكبة التحديات الجديدة، كما يتطلب

إنشاء بيئة تعليمية وثقافية تعزز الفهم والالتزام بممارسات الأمان، و في ميدان الوظائف تثقيف الموظفين حول التهديدات المحتملة، مثل التصيد الاحتيالي والبرامج الضارة، بالإضافة إلى ذلك، تعزيز ثقافة الأمان عبر تشجيع الموظفين على الإبلاغ عن الحوادث والمخاوف.

خاتمة

من المؤكد أن المغرب قد أدرك أهمية تعزيز قدراته في مجال الأمن السيبراني لتحقيق الرفاهية الاقتصادية، وابدى يقظة مستمرة تجاه المشهد المتغير للتهديدات السيبرانية والتحديات الجديدة التي تطرحها التطورات التكنولوجية مثل "إنترنت الأشياءIOT، و الحوسبة السحابية، و التقنيات المحمولة، و غيرها". وأدى هذا الوعي إلى جهود متواصلة للتكيف وتعزيز التدابير السيبرانية مع الامتثال للقوانين والبقاء على اطلاع دائم بأحدث التطورات التقنية.[28]

وفي الأخير يتضح جليا أن تحديات المغرب في مجال الأمن السيبراني ليس هو غياب النصوص القانونية، ولا حتى غياب التعبير عن الإرادات ووضع الاستراتيجيات والبرامج، بل هو التنزيل السليم لهذه التوجهات، وهذه بعض التوصيات لتعزيز الأمن السيبراني في البلاد:

- القيام بحملات التوعية العامة بهدف تثقيف المواطنين بأهمية الأمن السيبراني؛
- دعم حكومي للمؤسسات الصغيرة والمتوسطة لتحسين وضعها في نجال الأمن السيبراني؛
- الشراكة بين القطاع العام والخاص لتعزيز التعاون بين الجهات الحكومية ومنظمات الأمن السيبراني لتقوية القدرات وتبادل الموارد من أجل الدفاع الجماعي؛
- الاستثمار في التقنيات الحديثة.

الهوامش:

[1] – حميدي حياة–طايلب نسيمة، مدخل مفاهيمي حول الأمن السيبراني، مدار للدراسات الاتصالية الرقمية، المجلد الثاني، العدد 2، نونبر 2022، ص.2.

[2] – القانون رقم 05.20 المتعلق بالأمن السيبراني، الصادر بتنفيذه ظهير شريف رقم 69. 1.20 بتاريخ 4 ذي الحجة 1441 (25 يوليو 2020.

[3] المديرية العامة لأمن نظم المعلومات (DGSSI): تم إحداث المديرية العامة لأمن نظم المعلومات سنة 2011، التابعة لإدارة الدفاع الوطني للمملكة المغربية بموجب المرسوم رقم 2.11.509 الصادر في 21 سبتمبر 2011. تعتبر المديرية العامة لأمن نظم المعلومات، هي الهيئة الوطنية المكلفة بحماية نظم المعلومات ضد التهديدات السيبرانية في المغرب، وتضم المديرية العامة لأمن نظم المعلومات أربع مديريات:

- مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية(ماسيرت)؛
- مديرية الاستراتيجية والتقنين؛
- مديرية المساعدة والتكوين والمراقبة والخبرة؛
- مديرية نظم المعلومات المؤمنة.

[4] اللجنة الاستراتيجية للأمن السيبراني: تم إحداث اللجنة الاستراتيجية للأمن السيبراني (المسماة سابقا باللجنة الاستراتيجية لأمن نظم المعلومات) بموجب القانون رقم 20.05 بتاريخ 25 يوليوز 2020، وهي السلطة المسؤولة عن:

- اعداد التوجهات الاستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان صمود نظم معلومات الهيئات والبنى التحتي ة ذات الأهمية الحيوية والمتعهدين، المشار إليهم في الفرع الثالث من الفصل الثاني من القانون رقم 20.05 المذكور أعلاه.
- إجراء تقييم سنوي لأنشطة المديرية العامة لأمن نظم المعلومات.
- تقييم عمل اللجنة الوطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة المنصوص عليها في المادة 36 من القانون رقم 20.05 المذكور أعلاه.
- حصر نطاق افتحاصات أمن نظم المعلومات التي تنجزها المديرية العامة لأمن نظم المعلومات.

- تشجيع البحث والتطوير في مجال الأمن السيبراني.
- تشجيع برامج وأنشطة التحسيس وتعزيز القدرات في مجال الأمن السيبراني لفائدة الهيئات والبنيات التحتية ذات الأهمية الحيوية.
- ابداء الرأي في مشاريع القوانين والنصوص التنظيمية المتعلقة بمجال الأمن السيبراني.

[5] _قانون رقم 20.05 المتعلق بالأمن السيبراني؛

_قانون حماية المعطيات الشخصية رقم 08.09؛

_قانون المتعلق بالتوقيع الإلكتروني رقم 20.43؛

_ القانون رقم 53.05 إلى القانون المتعلق بالمصادقة الإلكترونية والتوقيع الرقمي.

[6]– تتجلى بعض مؤشرات التطور العالمي في المجال السيبراني، في اعتبار الفضاء السيبراني "المجال الخامس" للحروب بعد البر والبحر والجو والفضاء، كما نجد من مؤشرات التطور، اعتماد البنى التحتية الحيوية مثل: الطاقة، النقل، الاتصالات... على الأنظمة الرقمية، ما يجعل اختراقها تهديدا للأمن الوطني والدولي.

[7] – خالد سمير، الأمن السيبراني: تعريفه وأهميته وكيف يعمل ومجالاته وأنواع التهديدات والتقنيات الحديثة، مقال منشور بالموقع الإلكتروني "زامن" : https://zamn.app/blog/ _ تم الاطلاع عليه بتاريخ: 22 /2025/02 على الساعة 14:20.

[8] – الموقع الرسمي للاتحاد الدولي للاتصالات.

[9] – الموقع الرسمي للمركز الوطني البحريني للأمن السيبراني.

[10] – هند الإدريسي، الأمن السيبراني في المغرب: بين الإنجازات والتحديات، مقال منشور بالموقع الرسمي للمعهد المغربي لتحليل السياسات، تم الاطلاع عنه بتاريخ 2025/06/02، على الساعة العاشرة صباحا.

[11] – هذا الفرع تم التنصيص عليه من المادة 3 إلى المادة 13 من القانون 05.20.

[12] – هذا الفرع تم التنصيص عليه من المادة 14 إلى المادة 25 من القانون 05.20

[13] – هذا الفرع تم التنصيص عليه من المادة 26 إلى المادة 34 من القانون 05.20.

[14] – على سبيل المثال لا الحصر نجد القانون رقم 03.03 المتعلق بمكافحة الإرهاب والقانون رقم 43.20 المتعلق بخدمات الثقة بشأن المعاملات الإلكترونية والقانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين اتجاه معالجة المعطيات ذات الطابع الشخصي.

[15] – حدد المشرع مهام اللجنة من خلال مقتضيات المادة 36 من القانون 05.20.

[16] – بالعودة للمواد 38 إلى 52 من القانون 05.20 نجد أن مهام السلطة تتنوع بين ما هو استراتيجي وتنظيمي.

[17]– مؤشر الأمن السيبراني وفقاً للهيئة الوطنية للأمن السيبراني هو أداة قياسية تهدف إلى تقييم وقياس مستوى استعداد المؤسسات والجهات الحكومية والخاصة لمواجهة التهديدات السيبرانية. يُستخدم هذا المؤشر لتحديد مدى تطبيق السياسات الأمنية، فعالية الإجراءات الوقائية، والقدرة على الاستجابة للحوادث والتهديدات الإلكترونية.

يتم تحديث هذا المؤشر بشكل دوري لتشمل مختلف التهديدات والتطورات في مجال الأمن السيبراني، كما يساعد في تقييم مدى التزام الجهات بالممارسات المثلى والالتزامات القانونية والتنظيمية في هذا المجال. يهدف إلى تعزيز مستوى الأمان الإلكتروني وضمان حماية البيانات والمعلومات الحساسة على جميع الأصعدة.

[18]– المنظمة الدولية للشرطة الجنائية، والمعروفة باسم الإنتربول، [1]هي منظمة دولية تأسست بهدف تسهيل التعاون الشرطي في جميع أنحاء العالم ومكافحة الجريمة. وهي أكبر منظمة شرطة دولية في العالم. يقع مقرها الرئيسي بليون فرنسا، ولها سبعة مكاتب إقليمية في جميع أنحاء العالم، ومكتب مركزي وطني في جميع الدول الأعضاء البالغ عددها 195 دولة.

[19]– أصبحت هجمات طروادة المصرفية مصدر قلق كبير في مجال الأمن السيبراني، مما يشكل تهديداً خطيراً للأفراد والشركات والمؤسسات المالية على حدٍ سواء. تم تصميم هذه البرامج الضارة المتطورة خصيصاً لاستهداف الأنظمة المصرفية عبر الإنترنت، بهدف سرقة المعلومات المالية الحساسة وبيانات اعتماد تسجيل الدخول، وفي النهاية الوصول غير المصرح به إلى الحسابات المصرفية .

[20] تشير تقارير المعهد المغربي لتحليل السياسات (MIPA) إلى هذه الإشكالية المتمثلة في غياب مواءمة ومواكبة للمعايير الدولية.

[21] تتسم الجرائم الالكترونية او السيبرانية بمجموعة من الخصائص من بينها: أنها عابرة للحدود وأنها تتميز بالتعقيد والتنوع، كما أنها تمس الأفراد والمؤسسات، بالإضافة إلى أنها تتسم بصعوبة الإثبات والاكتشاف.

[22]– يقصد بالحرب بالوكالة (Proxy Warfare): هي استراتيجية سياسية وعسكرية تستخدم فيها دولة أو مجموعة دول أخرى من أجل تحقيق أهدافها في دولة أو منطقة أخرى، بدلًا من أن تكون هي من تتولى هذه المهمة بشكل مباشر. وفي المجال السيبراني هذا يعني أن الدولة أو الجهة السياسية تستخدم أفرادًا أو جماعات أو دولًا أخرى لمهاجمة خصم سياسي أو منافس سياسي عبر الإنترنت، بدلاً من أن تكون هي من تشن الهجوم السيبراني بشكل مباشر.

[23]– أكد تقرير لشركة "كاسبرسكي" لحلول الأمن السيبراني، الذي عُرضت نتائجه خلال معرض "جيتيكس" بمراكش، اكتشاف أكثر من 131 مليون تهديد إلكتروني عبر عموم القارة الإفريقية سنة 2024، بالتوازي مع ارتفاع وتيرة التهديدات السيبرانية ضد الشركات العاملة في المنطقة بأكثر من 1 في المائة مقارنة بالأرقام المسجلة عام 2023، كما أكد التقرير أن المغرب تعرّض لـ 12 مليونًا و600 ألف تهديد على هذا المستوى العام الماضي وحده، فيما تعرّضت دولة كينيا لقرابة 20 مليون محاولة هجوم سيبراني، تلتها جنوب إفريقيا بنحو 17 مليونًا.

[24]- RAOUF RIAHI, Comprehensive Analysis of the April 2025 Cyberattacks on Morocco.

_ مقال منشور بالموقع الإلكتروني "لينكيد اين" على الرابط الآتي: تم الاطلاع عليه بتاريخ 2025/05/2.

https://www.linkedin.com/pulse/comprehensive-analysis-april-2025-cyberattacks-raouf-riahi-mbci-whinf.

KHADIJA TACHFINE, Report warns Morocco is becoming fertile ground for cyberattacks amid geopolitical tensions.

_ مقال منشور بالموقع الالكتروني "هيسبريس" على الرابط الآتي: تم الاطلاع عليه بتاريخ 2025/05/4.

https://en.hespress.com/108504-report-warns-morocco-is-becoming-fertile-ground-for-cyberattacks-amid-geopolitical-tensions.html .

[25]– هند الإدريسي، الأمن السيبراني في المغرب: بين الإنجازات والتحديات؛ مرجع سابق.

[26]– قراصنة " أنونيموس تونس" اخترقت موقع بنك المغرب المركزي.

[27]– هاجمت جماعات "هاكتيفيست" موالية لإسرائيل مؤسسات مغربية ردًّا على موقف المغرب الداعم لفلسطين.

[28] – هند الإدريسي، مرجع سابق.