القانون المتعلق بالأمن السيبراني

adala.justice.gov.ma

ظهير شريف رقم 1.20.69 صادر في 4 ذي الحجة 1441(25 يوليو 2020) بتنفيذ القانون رقم 05.20 المتعلق بالأمن السيبراني[1]

الحمد لله وحده،

الطابع الشريف- بداخله:

(محمد بن الحسن بن محمد بن يوسف الله وليه)

يعلم من ظهيرنا الشريف هذا، أسماه الله وأعز أمره أننا:

بناء على الدستور ولا سيما الفصلين 42 و50 منه،

أصدرنا أمرنا الشريف بما يلي:

ينفذ وينشر بالجريدة الرسمية، عقب ظهيرنا الشريف هذا، القانون رقم 05.20 المتعلق بالأمن السيبراني، كما وافق عليه مجلس النواب ومجلس المستشارين.

وحرر بتطوان في 4 ذي الحجة 1441 (25 يوليو 2020).

وقعه بالعطف:

رئيس الحكومة،

الإمضاء: سعد الدين العثماني.

1 - الجريدة الرسمية عدد 6904 بتاريخ 9 ذو الحجة 1441 (30 يوليو 2020) ، ص 4160.

قانون رقم 05.20 يتعلق بالأمن السيبراني

الفصل الأول: أحكام عامة

المادة الأولى

يحدد هذا القانون:

- قواعد ومقتضيات الأمن المطبقة على نظم معلومات إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري آخر خاضع للقانون العام، يشار إليهم في هذا القانون ب «الهيئة»؛
- قواعد ومقتضيات الأمن المطبقة على البنيات التحتية ذات الأهمية الحيوية؛
- قواعد ومقتضيات الأمن المطبقة على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت، يشار إليهم في هذا القانون ب «المتعهد»؛
- الإطار الوطني لحكامة الأمن السيبراني؛
- إطار التعاون وتبادل المعلومات بين السلطة الوطنية للأمن السيبراني المحددة بنص تنظيمي، والمشار إليها في هذا القانون ب «السلطة الوطنية »والمصالح المختصة للدولة المكلفة بمعالجة الجرائم الماسة بنظم المعالجة الآلية للمعطيات؛
- المساهمات التي تقدمها السلطة الوطنية للهيئات الوطنية المختصة من أجل تعزيز الثقة الرقمية، وتطوير رقمنة الخدمات المقدمة من طرف الدولة، وحماية المعطيات ذات الطابع الشخصي
- اختصاصات السلطة الوطنية لا سيما في ما يتعلق بتطوير الخبرة الوطنية والتحسيس في مجال الأمن السيبراني لفائدة الهيئات والفاعلين في القطاع الخاص والأفراد، وتقوية التعاون مع المؤسسات الوطنية والأجنبية.

المادة 2

يقصد في مدلول هذا القانون بما يلي:

- «الأمن السيبراني»: 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؛

- « جرائم سيبرانية»: مجموعة من الأفعال المخالفة للتشريع الوطني أو الاتفاقيات الدولية التي صادقت عليها المملكة المغربية، التي تستهدف شبكات ونظم المعلومات أو تستعملها كوسيلة لارتكاب جنحة أو جناية؛
- «تهديد سيبراني»: كل عمل يهدف إلى الإخلال بأمن نظام للمعلومات من خلال المساس بتوافر النظام أو المعلومة التي يتضمنها أو بتماميتهما أو بسريتهما؛
- «أخلاقيات سيبرانية»: مجموعة من المعايير والقواعد التي تحدد السلوك المسؤول في الفضاء السيبراني؛
- «بنيات تحتية ذات أهمية حيوية»: التجهيزات والمنشآت والأنظمة الضرورية للحفاظ على استمرارية الوظائف الحيوية للمجتمع والصحة والأمن والسلامة والتقدم الاقتصادي أو الاجتماعي حيث إن أي ضرر أو إتلاف أو ضياع قد يصيبها يترتب عنه خلل في هذه الوظائف؛
- «قطاع الأنشطة ذات الأهمية الحيوية»: مجموعة من الأنشطة التي تقوم بها البنيات التحتية ذات الأهمية الحيوية وتساهم في تحقيق نفس الهدف ولها علاقة إما بإنتاج وتوزيع السلع أو الخدمات الضرورية لتلبية الحاجيات الأساسية لعيش المواطنين، أو بممارسة الدولة لصلاحيتها أو بالحفاظ على قدراتها الأمنية أو بسير النشاط الاقتصادي، على اعتبار أن هذه الأنشطة غير قابلة للاستبدال أو التعويض، أو نظرا للخطر الجسيم الذي قد تشكله على الساكنة؛
- «نظام معلومات»: مجموعة منظمة من الموارد كالمستخدمين والمعدات والبرامج والمعطيات والإجراءات التي تسمح بتجميع المعلومة في بيئة معينة وتصنيفها ومعالجتها ونشرها؛
- «نظام معلومات حساس »: نظام معلومات يعالج معلومات أو معطيات حساسة من شأن المساس بسريتها أو بسلامة محتواها أو بتوافرها أن يلحق ضررا بهيئة ما أو ببنية تحتية ذات أهمية حيوية؛
- «خدمة للأمن السيبراني»: كل خدمة أمن مقدمة من لدن مقدمي خدمات الأمن السيبراني لفائدة هيئة ما أو بنية تحتية ذات أهمية حيوية تهم رصد وتشخيص حادث أمن سيبراني وتقوية أمن نظم معلوماتها؛
- «مقدم خدمات رقمية»: كل شخص ذاتي أو اعتباري يقدم عن بعد وبطريقة إلكترونية، وبناء على طلب مستفيد ما، إحدى الخدمات التالية:

- خدمة رقمية تسمح لمستهلكين أو لمهنيين بإبرام عقود بيع أو خدمة عبر الإنترنت؛
- خدمة رقمية تسمح للمستعملين القيام بأبحاث على مواقع الإنترنت؛
- خدمة رقمية تسمح بالولوج إلى مجموعة مرنة ومتنوعة من الموارد المعلوماتية التي يمكن تقاسمها، بما فيها مستضيفي المعطيات أو نظم المعلومات أو هما معا ومقدمي الخدمات الرقمية السحابية؛

- «إيواء»:كل خدمة لتخزين إشارات أو كتابات أو صور أو أصوات أو رسائل بمختلف أنواعها، مقدمة بعوض أو بدون عوض من لدن مقدمي الخدمات الرقمية؛

- «إسناد نظام المعلومات لجهة خارجية»: كل عملية تتمثل في الإسناد الجزئي أو الكلي لنظام معلومات هيئة ما إلى مقدم خدمات معين في إطار عقد يحدد بدقة على الخصوص مستوى الخدمات ومدة الإسناد؛

- «المصادقة على نظم المعلومات»: وثيقة يشهد بواسطتها المسؤول عن البنية التحتية ذات الأهمية الحيوية على اطلاعه على نظام المعلومات والتدابير الأمنية التقنية أو التنظيمية أو القانونية المتخذة وعلى تحمله للمخاطر المتبقية؛

- «حادث أمن سيبراني»:واقعة أو وقائع غير مرغوب فيها أو غير متوقعة، مرتبطة بأمن نظم المعلومات، والتي يحتمل جدا أن تعرض للخطر أنشطة هيئة ما أو بنية تحتية ذات أهمية حيوية أو متعهد أو أن تهدد سلامة نظمهم المعلوماتية

- «أزمة أمن سيبراني»: حالة ناتجة عن وقوع حدث أو عدة أحداث متعلقة بالأمن السيبراني، يمكن أن يكون لها وقع خطير على حياة الأفراد أو على ممارسة الدولة لسلطاتها أو سير الاقتصاد أو على المحافظة على القدرات الأمنية والدفاعية للبلاد؛

- «إدارة حوادث الأمن السيبراني»: عمليات رصد حوادث الأمن السيبراني والتبليغ عنها وتقييمها وكذا التدابير المتخذة للتدخل والمعالجة المتعلقة بها.

الفصل الثاني: إجراءات حماية أمن نظم المعلومات

الفرع الأول: أحكام خاص بالهيئات

المادة 3

يجب على كل هيئة أن تسهر على أن تكون نظم معلوماتها مطابقة للتوجيهات والقواعد والأنظمة والمراجع والتوصيات الصادرة عن السلطة الوطنية.

المادة 4

يجب على كل هيئة أن تضع وتنفذ سياسة لأمن نظم معلوماتها وفق التوجيهات الصادرة عن السلطة الوطنية.

يجب على كل هيئة تحديد المخاطر التي تهدد أمن نظم معلوماتها واتخاذ الإجراءات التقنية والتنظيمية اللازمة لإدارة هذه المخاطر، من أجل تجنب الحوادث التي من شأنها المساس بنظم المعلومات وكذا التقليل إلى أدنى حد ممكن من الآثار التي قد تنجم عن هذه الحوادث.

يجب أن يخضع كل نظام معلومات هيئة تقدم خدمات رقمية للغير لا فتحاص أمني قبل الشروع في استغلاله.

يجب على كل هيئة إجراء افتحاص لنظم معلوماتها بانتظام.

المادة 5

يجب على كل هيئة أن تقوم بتصنيف أصولها المعلوماتية ونظم معلوماتها حسب مستوى حساسيتها من حيث السرية والتمامية والتوافر، كما يتعين أن تكون تدابير حماية الأصول المعلوماتية ونظم المعلومات متناسبة مع مستوى التصنيف المخصص لها.

يجب على كل هيئة أن تحدد إجراءات تأهيل الأشخاص الذين يمكنهم الولوج إلى المعلومات المصنفة وشروط معالجة هذه المعلومات أو تبادلها أو تخزينها أو نقلها.

يحدد بنص تنظيمي الدليل المرجعي لتصنيف أصول المعلومات ونظم المعلومات.

المادة 6

يجب على كل هيئة أن تعين مسؤولا عن أمن نظم المعلومات، يتولى السهر على تطبيق سياسة أمن نظم المعلومات.

يعتبر المسؤول عن أمن نظم المعلومات مخاطب السلطة الوطنية للأمن السيبراني، ويتعين أن يتمتع بالاستقلالية اللازمة لممارسة مهامه.

المادة 7

يجب على كل هيئة أن توفر الوسائل المناسبة لمراقبة ورصد الأحداث التي قد تمس بأمن نظم معلوماتها ويكون لها وقع بالغ على استمرارية الخدمات التي تقدمها.

لا يمكن للسلطة الوطنية استغلال المعطيات التقنية المحصل عليها بواسطة الوسائل المذكورة إلا لغرض تحديد ومعالجة الخطر الذي يمس بأمن نظم معلومات الهيئة المعنية.

المادة 8

يجب على كل هيئة فور علمها بأي حادث يؤثر على أمن أو سير نظم المعلومات الخاصة بها أن تقوم بإبلاغ السلطة الوطنية.

تقوم كل هيئة بإبلاغ السلطة الوطنية، بناء على طلب هذه الأخيرة، ودون تأخير، بالمعلومات الإضافية المتعلقة بالحوادث التي تؤثر على أمن أو سير نظم معلوماتها.

تبين السلطة الوطنية المعطيات التقنية والمعلومات المتعلقة بالحوادث، التي يجب إبلاغها، وكذا كيفيات إرسالها.

ترسل السلطة الوطنية إلى الهيئة المعنية تقريرا تركيبيا يتضمن التدابير والتوصيات لمعالجة الحادث.

المادة 9

تعد كل هيئة مخططا لضمان استمرارية أو استئناف الأنشطة يتضمن مجموع الحلول البديلة لإبطال مفعول انقطاعات الأنشطة وحماية الوظائف المهمة والحساسة من الآثار الناجمة عن الاختلالات الأساسية لنظم المعلومات أو عن الكوارث، وضمان استئناف عمل هذه الوظائف في أقرب الآجال.

يتعين اختبار مخطط ضمان استمرارية أو استئناف الأنشطة بصفة منتظمة من أجل تحيينه حسب التطورات الخاصة بالهيئة وتطور التهديدات.

المادة 10

في حالة إسناد نظام معلومات حساس لجهة خارجية، يجب على هذه الجهة احترام القواعد والأنظمة والدلائل المرجعية التقنية المتعلقة بأمن نظم المعلومات، والتي تضعها السلطة الوطنية.

المادة 11

يجب أن يتم إيواء المعطيات الحساسة، حصريا، داخل التراب الوطني.

المادة 12

يجب أن يكون كل إسناد خارجي لنظام معلومات حساس موضوع عقد خاضع للقانون المغربي، يتضمن وجوبا الالتزامات المتعلقة بحماية المعلومة وقابليتها للافتحاص واستعادتها، وكذا متطلبات الأمن ومستوى الخدمة المرغوب فيها.

المادة 13

تحدد السلطة الوطنية القواعد والدليل المرجعي التقني المنظم لشروط الأمن المتعلقة بالإسناد الخارجي لنظم المعلومات.

الفرع الثاني: أحكام خاصة بالبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة

المادة 14

تسري أحكام الفرع الأول من هذا الفصل على البنيات التحتية ذات الأهمية الحيوية.

المادة 15

تحدد بنص تنظيمي لائحة قطاعات الأنشطة ذات الأهمية الحيوية وكذا السلطات الحكومية والمؤسسات العمومية وباقي الأشخاص الاعتباريين الخاضعين للقانون العام المشرفين على تنسيق هذه القطاعات.

المادة 16

يتم تحديد البنيات التحتية ذات الأهمية الحيوية لكل قطاع أنشطة ذات أهمية حيوية، بعد استطلاع رأي السلطة الوطنية، من طرف السلطة الحكومية أو المؤسسة العمومية أو الشخص الاعتباري الخاضع للقانون العام المشرف على تنسيق هذا القطاع.

تظل لائحة هذه البنيات التحتية سرية، ويتم تحيينها على فترات منتظمة لا تتعدى سنتين.

المادة 17

يقوم المسؤول عن البنية التحتية ذات الأهمية الحيوية، بناء على نتائج تحليل المخاطر، بإعداد لائحة نظم المعلومات الحساسة، وإرسالها في صيغتها المحينة إلى السلطة الوطنية.

المادة 18

يمكن للسلطة الوطنية توجيه ملاحظات إلى المسؤول عن البنية التحتية ذات الأهمية الحيوية بخصوص لائحة نظم المعلومات الحساسة التي تمت موافاتها بها.

في هذه الحالة، يتعين على المسؤول عن البنية التحتية ذات الأهمية الحيوية تعديل لائحتها وفقا لهذه الملاحظات، وإرسال اللائحة المعدلة إلى السلطة الوطنية داخل أجل شهرين من تاريخ التوصل بالملاحظات.

تظل لائحة نظم المعلومات الحساسة سرية.

المادة 19

يجب أن يخضع أمن كل نظام معلومات حساس للمصادقة قبل الشروع في استغلاله.

تحدد السلطة الوطنية دليل المصادقة على نظم المعلومات الحساسة.

المادة 20

يجب على المسؤولين عن البنيات التحتية ذات الأهمية الحيوية، بناء على طلب من السلطة الوطنية، إخضاع نظم المعلومات الحساسة الخاصة بها إلى افتحاص تقوم به هذه السلطة أو متعهدي الافتحاص المؤهلين من قبلها.

تحدد بنص تنظيمي معايير تأهيل متعهدي الافتحاص وكذا كيفيات إجراء الافتحاص.

المادة 21

يجب على المسؤولين عن البنيات التحتية ذات الأهمية الحيوية مد السلطة الوطنية أو متعهد الافتحاص المؤهل بالمعلومات والعناصر اللازمة لإجراء الافتحاص، بما في ذلك الوثائق المتعلقة بسياستها الأمنية، وعند الاقتضاء، نتائج الافتحاص الأمني السابقة، والسماح لهم بالولوج إلى الشبكات ونظم المعلومات موضوع المراقبة قصد إجراء التحليلات واستخراج بيانات المعلومات التقنية.

يجب أن يلتزم متعهدو الافتحاص المؤهلون ومستخدموهم، تحت طائلة العقوبات المنصوص عليها في مجموعة القانون الجنائي، باحترام السر المهني طيلة مدة مهمة الافتحاص وبعد الانتهاء منها، بشأن المعلومات والوثائق التي تم تجميعها أو اطلعوا عليها أثناء القيام بهذه المهمة.

المادة 22

في حالة إجراء الافتحاص من طرف متعهد افتحاص مؤهل، يقوم المسؤول عن البنية التحتية ذات الأهمية الحيوية بإرسال تقرير الافتحاص إلى السلطة الوطنية.

يجب على متعهد الافتحاص المؤهل أن يسهر على ضمان سرية تقرير الافتحاص.

المادة 23

عند إجراء عمليات الافتحاص من طرف متعهدي الافتحاص المؤهلين، يتحمل المسؤول عن البنية التحتية ذات الأهمية الحيوية المعنية مصاريف هذه العمليات.

المادة 24

يجب على كل مسؤول عن بنية تحتية ذات أهمية حيوية تم افتحاصها وضع برنامج عمل لتنفيذ التوصيات الواردة في تقارير الافتحاص، وإرساله إلى السلطة الوطنية قصد تتبع تنفيذه.

المادة 25

يجب أن يلجأ المسؤولون عن البنيات التحتية ذات الأهمية الحيوية إلى الخدمات أو المنتوجات أو الحلول التي تسمح بتعزيز الوظائف الأمنية، والتي تحددها السلطة الوطنية.

في حالة إسناد خدمات الأمن السيبراني لجهة خارجية، يجب على المسؤولين عن البنيات التحتية ذات الأهمية الحيوية اللجوء إلى مقدمي خدمات مؤهلين من طرف السلطة الوطنية.

تحدد بنص تنظيمي معايير تأهيل مقدمي خدمات الأمن السيبراني.

الفرع الثالث: أحكام خاصة بالمتعهدين

المادة 26

يجب على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت التقيد بتوجيهات السلطة الوطنية، لا سيما تلك المتعلقة بالمحافظة على المعطيات التقنية اللازمة لتحديد أي حادث أمن سيبراني.

تتضمن هذه المعطيات التقنية على الخصوص، بيانات الربط والنشرات المعلوماتية وآثار أحداث الأمن المحصل عليها بواسطة نظم الاستغلال والتطبيقات ومنتوجات الأمن.

تحدد مدة الاحتفاظ بالمعطيات التقنية اللازمة لتحديد وتحليل الحادث في سنة واحدة، ويمكن تغيير هذه المدة بنص تنظيمي.

المادة 27

يخطر مستغلو الشبكات العامة للمواصلات ومزودو خدمات الإنترنت ومقدمو خدمات الأمن السيبراني ومقدمو الخدمات الرقمية وناشرو منصات الإنترنت زبناءهم بهشاشة نظم معلوماتهم أو الانتهاك الذي قد يطالها.

المادة 28

من أجل ضمان أمن نظم المعلومات الخاصة بالهيئات والبنيات التحتية ذات الأهمية الحيوية، يسمح لأعوان السلطة الوطنية المعتمدين حصريا بهدف الوقاية وتحديد خصائص التهديد السيبراني، بتجميع وتحليل المعطيات التقنية، دون أي استغلال آخر، لدى مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت.

تؤهل السلطة الوطنية لوضع أجهزة تقنية على الشبكات العامة للمواصلات وشبكات مزودي خدمات الإنترنت حصريا بهدف رصد الأحداث التي قد تؤثر على أمن نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية.

توضع هذه الأجهزة حصريا خلال المدة وفي الحدود التي يتطلبها تحديد خصائص التهديد.

المادة 29

يجب على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنت، في إطار توجيهات السلطة الوطنية، اتخاذ التدابير الحمائية اللازمة لأجل الوقاية وإبطال مفعول التهديدات أو الانتهاكات التي تمس نظم معلومات زبنائهم.

المادة 30

عندما يقوم مستغلو الشبكات العامة للمواصلات ومزودو خدمات الإنترنت ومقدمو خدمات الأمن السيبراني ومقدمو الخدمات الرقمية وناشرو منصات الإنترنت برصد أحداث قد تؤثر على أمن نظم معلومات زبنائهم، وجب عليهم إخطار السلطة الوطنية فورا بذلك.

المادة 31

يجب على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت أن يستعملوا، في شبكات الاتصالات الإلكترونية التي يستغلونها، أجهزة للرصد تشتغل بعلامات تقنية توفرها السلطة الوطنية، وذلك فقط بهدف رصد الأحداث التي قد تؤثر على أمن نظم معلومات مشتركيها.

المادة 32

يجب على مقدمي الخدمات الرقمية تحديد المخاطر التي تهدد أمن نظم معلوماتهم، واتخاذ التدابير التقنية والتنظيمية اللازمة لإدارة هذه المخاطر، وذلك لمنع وقوع الحوادث التي قد تؤثر سلبا على هذه الشبكات ونظم المعلومات، والتقليل إلى أدنى حد ممكن من أثر هذه المخاطر ضمانا لاستمرارية هذه الخدمات.

المادة 33

يجب على مقدمي الخدمات الرقمية، فور علمهم بأي حوادث تؤثر على الشبكات ونظم المعلومات اللازمة لتوفير خدماتهم، أن يقوموا بإبلاغ السلطة الوطنية بها، وذلك حينما يتبين من المعلومات المتوفرة لديهم أن لهذه الحوادث وقع بالغ يؤثر على تقديم هذه الخدمات.

المادة 34

إذا تم، بأي وسيلة كانت، إخبار السلطة الوطنية بأن أحد مقدمي الخدمات الرقمية لا يفي بأحد الالتزامات المنصوص عليها في هذا القانون، أمكن لهذه السلطة أن تخضعه للمراقبة من أجل التحقق من تقيده بهذه الالتزامات، وكذا من مستوى أمن الشبكات ونظم المعلومات اللازمة لتقديم خدماته.

تتم المراقبة من قبل السلطة الوطنية أو من قبل متعهدي الافتحاص المؤهلين من قبل هذه السلطة. وفي هذه الحالة الأخيرة، يتحمل مقدم الخدمات الرقمية مصاريف عمليات المراقبة.

إذا تبين أثناء إجراء المراقبة وجود أي إخلال بالالتزامات الملقاة على عاتق مقدم الخدمات بموجب هذا الفرع، أمكن للسلطة الوطنية إعذار مسيري مقدم الخدمات المعني بالتقيد بهذه الالتزامات، وذلك داخل أجل تحدده هذه السلطة.

الفصل الثالث: حكامة الأمن السيبراني

الفرع الأول: اللجنة الاستراتيجية للأمن السيبراني

المادة 35

تحدث لجنة استراتيجية للأمن السيبراني، يعهد إليها بالقيام بما يلي:

- إعداد التوجهات الاستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان صمود نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية والمتعهدين المشار إليهم في الفرع الثالث من الفصل الثاني من هذا القانون؛
- التقييم السنوي لأنشطة السلطة الوطنية؛
- تقييم عمل اللجنة الوطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة، المنصوص عليها في المادة 36 بعده؛
- حصر نطاق افتحاصات أمن نظم المعلومات التي تنجزها السلطة الوطنية؛
- تشجيع البحث والتطوير في مجال الأمن السيبراني؛
- تشجيع برامج وأنشطة التحسيس وتعزيز القدرات في مجال الأمن السيبراني لفائدة الهيئات والبنيات التحتية ذات الأهمية الحيوية؛
- إبداء الرأي في مشاريع القوانين والنصوص التنظيمية المتعلقة بمجال الأمن السيبراني.

يحدد بنص تنظيمي تأليف وكيفيات سير اللجنة الاستراتيجية للأمن السيبراني.

المادة 36

تحدث لدى اللجنة الاستراتيجية للأمن السيبراني، لجنة لإدارة الأزمات والأحداث السيبرانية الجسيمة، تكلف بضمان تدخل منسق في مجال الوقاية وتدبير الأزمات على إثر وقوع حوادث أمن سيبراني.

ولهذا الغرض، يتعين على مستغلي الشبكات العامة للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية الامتثال للأوامر الصادرة عن لجنة إدارة الأزمات والأحداث السيبرانية الجسيمة والاستجابة لطلباتها المتعلقة بالدعم والمساعدة التقنية.

يحدد بنص تنظيمي تأليف اللجنة وكيفيات اشتغالها ومجال تدخل كل عضو من أعضائها.

المادة 37

يمكن للجنة إدارة الأزمات والأحداث السيبرانية الجسيمة، من أجل التصدي لحوادث الأمن السيبراني الجسيمة، أن تحدد التدابير التي يتوجب على مسؤولي الهيئات والبنيات التحتية ذات الأهمية الحيوية تنفيذها وأن تقدم توصيات ونصائح إلى متعهدي القطاع الخاص والأفراد.

الفرع الثاني: السلطة الوطنية للأمن السيبراني

المادة 38

يعهد إلى السلطة الوطنية بتنفيذ استراتيجية الدولة في مجال الأمن السيبراني.

ولهذا الغرض، تتولى السلطة الوطنية، علاوة على المهام الأخرى المسندة إليها بمقتضى هذا القانون، القيام بالمهام التالية:

- تنسيق الأعمال المتعلقة بإعداد وتنفيذ استراتيجية الدولة في مجال الأمن السيبراني والسهر على ضمان تطبيق توجيهات اللجنة الاستراتيجية للأمن السيبراني؛
- تحديد تدابير حماية نظم المعلومات والسهر على ضمان تطبيقها؛
- تقديم اقتراحات إلى اللجنة الاستراتيجية للأمن السيبراني بخصوص تدابير التصدي للأزمات التي تمس أو تهدد أمن نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية؛
- تأهيل مقدمي خدمات افتحاص نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية ومقدمي خدمات الأمن السيبراني؛

- وضع تصور للوسائل اللازمة لضمان أمن الاتصالات الإلكترونية بين الوزارية وتنسيق تفعيلها؛
- القيام بأعمال المراقبة المنصوص عليها في هذا القانون؛
- السهر على ضمان إجراء عمليات افتحاص أمن نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية؛
- افتحاص متعهدي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية الذين يقدمون خدمات للبنيات التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة؛
- تقديم المساعدة والنصائح إلى الهيئات والبنيات التحتية ذات الأهمية الحيوية قصد تعزيز أمن نظم معلوماتها؛
- مساعدة ومواكبة الهيئات والبنيات التحتية ذات الأهمية الحيوية لوضع أجهزة لرصد أحداث مست أو قد تمس بأمن نظم معلوماتها وكذا تنسيق إجراءات التصدي لهذه الأحداث؛
- القيام، بتعاون مع الهيئات والبنيات التحتية ذات الأهمية الحيوية، بإعداد نظام خارجي لليقظة والرصد والإنذار بأحداث مست أو قد تمس بأمن نظم معلوماتها وكذا تنسيق إجراءات التصدي لهذه الأحداث؛
- القيام بأنشطة البحث العلمي والتقني في مجال الأمن السيبراني وتشجيعها.

المادة 39

يتعين على السلطة الوطنية ضمان سرية المعلومات الحساسة التي تجمعها في إطار هذا القانون.

المادة 40

تحدد السلطة الوطنية قواعد الأمن اللازمة لحماية نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية والمتعهدين المشار إليهم في المادة الأولى من هذا القانون.

تحدد السلطة الوطنية قواعد أمن خاصة بقطاع أنشطة ذي أهمية حيوية معين. وتقوم بتبليغ هذه القواعد وكذا كيفيات وآجال تطبيقها إلى مسؤولي البنيات التحتية ذات الأهمية الحيوية التابعين للقطاع المعني.

يجب على المسؤولين سالفي الذكر تطبيق هذه القواعد على نفقتهم.

المادة 41

لأجل التصدي لأي هجوم إلكتروني يستهدف نظم المعلومات ويمس بالوظائف الحيوية للمجتمع أو الصحة أو السلامة أو الأمن أو التقدم الاقتصادي أو الاجتماعي، يقوم أعوان السلطة الوطنية بالتحريات التقنية اللازمة لتحديد خصائص الهجوم ويسهرون على ضمان تنفيذ التدابير والتوصيات المتعلقة بها.

المادة 42

تتعاون السلطة الوطنية مع المصالح المختصة في الدولة من خلال تبادل أي معطيات أو معلومات قد تساعدها على معالجة الجرائم التي تخل بسير نظم المعالجة الآلية للمعطيات.

إذا تبين للسلطة الوطنية، أثناء ممارسة مهامها، وجود فعل يشتبه في مخالفته للقانون، فإنها تحيل الأمر إلى السلطات المختصة.

يتعين على السلطات المختصة إخبار السلطة الوطنية بالمآل المخصص للإحالة.

الفصل الرابع: التكوين والتحسيس والتعاون

المادة 43

تقوم السلطة الوطنية، بتعاون مع الفاعلين والمهنيين في مجال الأمن السيبراني، بتنظيم دورات تكوينية وتمارين لفائدة مستخدمي الهيئات والبنيات التحتية ذات الأهمية الحيوية من أجل تطوير وتعزيز القدرات الوطنية في هذا المجال.

المادة 44

تقوم السلطة الوطنية بتحديد وتنفيذ برامج تحسيسية بشأن الأخلاقيات السيبرانية والتحديات المتعلقة بتهديدات ومخاطر الأمن السيبراني لفائدة مستخدمي الهيئات والبنيات التحتية ذات الأهمية الحيوية والقطاع الخاص والأفراد.

تنشر بانتظام على الموقع الإلكتروني للسلطة الوطنية النصائح والتوصيات الوقائية المتعلقة بالأمن السيبراني لفائدة مستخدمي الهيئات والبنيات التحتية ذات الأهمية الحيوية والقطاع الخاص والأفراد.

المادة 45

تسهم السلطة الوطنية في دعم البرامج التي تعدها الهيئات المختصة في الدولة من أجل تعزيز الثقة الرقمية وتطوير رقمنة الخدمات وحماية المعطيات ذات الطابع الشخصي.

المادة 46

تقوم السلطة الوطنية، بتشاور مع الإدارات المعنية، بتطوير علاقات التعاون مع المنظمات الوطنية والأجنبية في مجال الأمن السيبراني وتنسيقها.

المادة 47

تقوم السلطة الوطنية بربط علاقات التعاون على الصعيدين الوطني والدولي لمعالجة حوادث الأمن السيبراني وتطوير تبادل التجارب والخبرات في هذا المجال.

الفصل الخامس: معاينة المخالفات والعقوبات

المادة 48

يؤهل للبحث عن المخالفات لأحكام هذا القانون والنصوص المتخذة لتطبيقه ومعاينتها بواسطة محاضر، علاوة على ضباط الشرطة القضائية، أعوان السلطة الوطنية المنتدبون لهذا الغرض والمحلفون وفق التشريع الجاري به العمل.

توجه محاضر معاينة المخالفات إلى النيابة العامة المختصة.

المادة 49

دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بغرامة من 200.000 إلى 400.000 درهم:

- كل مسؤول عن هيئة أو بنية تحتية ذات أهمية حيوية قام بإيواء المعطيات الحساسة خارج التراب الوطني، خرقا لأحكام المادة 11 أعلاه؛
- كل مسؤول عن بنية تحتية ذات أهمية حيوية تتوفر على نظام معلومات حساس شرع في استغلاله دون إخضاعه للمصادقة المنصوص عليها في المادة 19 أعلاه؛
- كل مسؤول عن بنية تحتية ذات أهمية حيوية عهد بافتحاص أمن نظم المعلومات الحساسة الخاصة ببنيته التحتية إلى متعهد افتحاص غير مؤهل، خرقا لأحكام المادة 20 أعلاه؛
- كل من قدم خدمات افتحاص أمن نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية دون أن يكون مؤهلا من قبل السلطة الوطنية أو استمر في تقديم هذه الخدمات رغم سحب تأهيله من قبل هذه السلطة؛
- كل مسؤول عن بنية تحتية ذات أهمية حيوية أسند خدمات الأمن السيبراني إلى مقدم خدمات غير مؤهل، خرقا لأحكام المادة 25 أعلاه؛

- كل من قدم خدمات الأمن السيبراني دون أن يكون مؤهلا من قبل السلطة الوطنية أو استمر في تقديم هذه الخدمات رغم سحب تأهيله من قبل هذه السلطة.

المادة 50

دون الإخلال بالعقوبات الجنائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بغرامة من 100.000 إلى 200.000 درهم:

- كل من أخل بالالتزامات المتعلقة بإبلاغ السلطة الوطنية عن الحوادث، خرقا لأحكام المواد 8 و30 و33 أعلاه؛
- كل من قام، بأي وسيلة كانت، بعرقلة أو بمنع إجراء عمليات افتحاص أمن نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية، المنصوص عليها في المادة 20 أعلاه؛
- كل متعهد لشبكة عامة للمواصلات أو مزود خدمات الإنترنت أو مقدم خدمات الأمن السيبراني أو مقدم الخدمات الرقمية أو ناشر منصات الإنترنت أخل بالالتزامات المنصوص عليها في المادة 26 أعلاه؛
- كل متعهد لشبكة عامة للمواصلات أو مزود خدمات الإنترنت أو أعوانهم، عرقل أعمال السلطة الوطنية أو أعوانها المنصوص عليها في المادة 28 أعلاه؛
- كل مقدم خدمة رقمية امتنع عن اتخاذ التدابير المنصوص عليها في المادة 32 أعلاه أو عرقل عمليات المراقبة المنصوص عليها في المادة 34 أعلاه.

يعاقب بالغرامة نفسها كل شخص اسْتُخْدِم نظام معلوماته دون علمه لنشر البرمجيات الخبيثة أو للقيام بأعمال مخالفة للقانون، امتنع عن تنفيذ توجيهات السلطة الوطنية بعد إخباره بها.

المادة 51

يجوز للمحكمة أن تحكم بمصادرة المواد والوسائل التي استعملت لارتكاب أفعال مخالفة لأحكام هذا القانون.

المادة 52

في حالة العود، ترفع العقوبات المنصوص عليها في هذا القانون إلى الضعف.

يعتبر في حالة العود كل من سبق الحكم عليه بعقوبة من أجل ارتكاب إحدى المخالفات المنصوص عليها في هذا القانون بمقرر قضائي مكتسب لقوة الشيء المقضي به، ثم ارتكب نفس المخالفة قبل مضي أربع سنوات من تمام تنفيذ تلك العقوبة أو تقادمها.

الفصل السادس: أحكام ختامية

المادة 53

يدخل هذا القانون حيز التنفيذ ابتداء من تاريخ نشر النصوص المتخذة لتطبيقه بالجريدة الرسمية.

adala.justice.gov.ma