2024/36.

الجمهورية التونسية
مجلس نواب الشعب
كتلة لينتصر الشعب

مشروع قانون يتعلق بالأمن السيبراني

الباب الأول
أحكام عامة

الفصل الأول:

يضبط هذا القانون:

- قواعد ومقتضيات الأمن المنطبقة على النظم المعلوماتية للإدارة العمومية والجماعات المحلية والمؤسسات والمنشآت العمومية وكل شخص معنوي آخر خاضع للقانون العام، يشار إليهم في هذا القانون بـ **"الهينة"**؛
- قواعد ومقتضيات الأمن المطبقة على البنية التحتية ذات الأهمية الحيوية؛

قواعد ومقتضيات الامن المنطبقة على مستغلي الشبكات العمومية للموصلات ومسدي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنات، يشار إليهم في هذا القانون بـ ***"المتعهد"***؛

- الإطار الوطني لحوكمة الأمن السيبراني؛
- إطار التعاون وتبادل المعلومات بين السلطة الوطنية للأمن السيبراني المحددة بنص ترتيبي، والمشار إليها في القانون بـ **"السلطة الوطنية"** والمصالح المختصة للدولة المكلفة بمعالجة الجرائم التي تمس بنظم المعالجة الآلية للمعطيات.
- المساهمات التي تقدمها السلطة الوطنية للهيئات المختصة من أجل تعزيز الثقة الرقمية، وتطوير رقمنة الخدمات المسداة من طرف الدولة، وحماية المعطيات الشخصية؛
- اختصاصات السلطة الوطنية لا سيما فيما يتعلق بتطوير الخبرة الوطنية والتحسيس في مجال الأمن السيبراني لفائدة الهيئات والفاعلين في القطاع الخاص والأفراد، وتعزيز التعاون مع المؤسسات الوطنية والأجنبية.

2024/36.

الفصل 2:
يقصد بالعبارات التالية على معنى هذا القانون ما يلي:

- **"الأمن السيبراني":** مجموعة التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقاوم أحداثا مرتبطة بالفضاء السيبراني، من شأنها أن تمس بسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلة، والخدمات ذات الصلة التي يقدمها هذا النظام أو تسمح الولوج إليه؛

- **"جرائم سيبرانية":** مجموعة الأفعال المخالفة للتشريع الوطني أو الاتفاقيات الدولية التي صادقت عليها الجمهورية التونسية، 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 بسريتهما؛

- **"أخلاقيات سيبرانية":** مجموعة المعايير والقواعد التي تحدد السلوك المسؤول في الفضاء السيبراني:

- **"بنى تحتية ذات أهمية حيوية":** التجهيزات والمنشآت والأنظمة الضرورية للحفاظ على استمرارية الوظائف الحيوية للمجتمع والصحة والأمن والدفاع والسلامة والتقدم الاقتصادي أو الاجتماعي حيث إن أي ضرر أو إتلاف أو ضياع قد يصيبهما يترتب عنه خلل في هذه الوظائف؛

- **"قطاع الأنشطة ذات الأهمية الحيوية":** مجموعة الأنشطة التي تقوم بها البنية التحتية ذات الأهمية الحيوية وتساهم في تحقيق نفس الهدف ولها علاقة إما بإنتاج وتوزيع السلع أو الخدمات الضرورية لتلبية الحاجات الأساسية لعيش المواطنين، أو ممارسة الدولة لصلاحيتها أو بالحفاظ على قدراتها الأمنية والدفاعية أو بسير النشاط الاقتصادي، على اعتبار أن هذه الأنشطة غير قابلة للاستبدال أو التعويض، أو بالنظر للخطر الجسيم الذي قد تشكله على المواطنين؛

- **"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 شأنها المساس بسريتها أو بسلامة محتواها أو بتوافرها أن يلحق ضررا بهيئة ما أو ببنية ذات أهمية حيوية؛

- **"خدمة لأمن السيبراني"**: كل خدمة أمن مقدمة من قبل مسدي خدمات الأمن السيبراني لفائدة هيئة ما أو بنية ذات أهمية حيوية تهم رصد وتشخيص حادث أمن سيبراني وتقوية أمن نظم معلوماتها؛

-**"مسدي خدمات رقمية"**: كل شخص مادي أو معنوي 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 التي يمكن تقاسمها، بما فيها مستضيفي المعطيات أو نظم المعلومات أو هما معا ومسدي الخدمات الرقمية السحابية؛

- **"إيواء"**: كل خدمة لتخزين إشارات أو كتابات أو صور أو أصوات أورسائل بمختلف أنواعها، مقدمة بعوض أو بدون عوض من لدن مسدي 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 خاصة في مستوى الخدمات ومدة الإسناد؛

- **"حادث أمن سيبراني"**: واقعة أو وقائع غير مرغوب أو غير متوقعة، مرتبطة بأمن نظم المعلومات، والتي يحتمل جدا أن تعرض للخطر أنشطة هيئة ما أو بنية ذات أهمية حيوية أو متعهد أو 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 والتدابير المتخذة للتدخل والمعالجة المتعلقة بها.

الباب الثاني
إجراءات حماية أمن نظم المعلومات

الفرع الأول
أحكام خاصة بالهيئات

الفصل 3:

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

الفصل 4:

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

يتعين على كل هيئة تحديد المخاطر التي تهدد أمن نظم معلوماتها واتخاذ الإجراءات التقنية والتنظيمية اللازمة لإدارة هذه المخاطر، من أجل تجنب الحوادث.

يتعين أن يخضع كل نظام معلومات هيئة تقدم خدمات رقمية للغير لتدقيق أمني قبل الشروع في استغلاله.

يتعين على كل هيئة إجراء تدقيق لنظم معلوماتها بانتظام.

الفصل 5:

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

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

ويضبط بأمر الدليل المرجعي لتصنيف أصول المعلومات ونظمها.

الفصل 6:

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.

الفصل 7:

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 المتحصل عليها بواسطة الوسائل المذكورة إلا لغرض تحديد ومعالجة الخطر الذي يمس بأمن نظم معلومات الهيئة المعنية.

الفصل 8:

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 معلوماتها.

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

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

الفصل 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 هذ الوظائف في أقرب الآجال.

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

الفصل 10:

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

الفصل 11:

إيواء المعطيات الحساسة، تتم حصريا، داخل التراب الوطني.

الفصل 12:

يتعين أن يكون كل إسناد خارجي لنظام معلومات حساس موضوع عقد خاضع للقانون التونسي يتضمن وجوبا الإلتزامات المتعلقة بحماية المعلومة وقابليتها للتدقيق واستعادتها، ومتطلبات الأمن ومستوى الخدمة المرغوب فيها.

الفصل 13:

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

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

الفصل 14:

تسري أحكام الفرع الأول من هذا الباب على البنى التحتية ذات الأهمية الحيوية.

الفصل 15:

تضبط بأمر قائمة قطاعات الأنشطة ذات الأهمية الحيوية والسلطات الحكومية والمؤسسات العمومية وباقي الأشخاص المعنويين الخاضعين للقانون العام المشرفين على تنسيق هذه القطاعات.

الفصل 16:

يتم تحديد البنى التحتية ذات الأهمية الحيوية لكل قطاع أنشطة ذات أهمية حيوية، بعد أخذ رأي السلطة الوطنية، من طرف السلطة المعنية أو المؤسسة العمومية أو الشخص المعنوي الخاضع للقانون المشرف على تنسيق هذا القطاع.

تظل قائمة هذه البني التحتية سرية، ويتم تحيينها على فترات منتظمة لا تتعدى سنتين.

الفصل 17:

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

الفصل 18:

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

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

تظل قائمة نظم المعلومات الحساسة سرية.

الفصل 19:

يخضع أمن نظام معلومات حساس للمصادقة قبل الشروع في استغلاله.

وتحدد السلطة الوطنية دليل المصادقة على نظم المعلومات الحساسة.

الفصل 20:

على المسؤولين عن البنية التحتية ذات الأهمية الحيوية، بناء على طلب من السلطة الوطنية، إخضاع نظم المعلومات الحساسة الخاصة بها إلى تدقيق تقوم به السلطة أو متعهدي التدقيق المؤهلين من قبلها.

تضبط بآمر معايير تأهيل متعهدي التدقيق وطرق إجراء التدقيق.

الفصل 21:

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

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

الفصل 22:

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

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

الفصل 23:

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

الفصل 24:

على كل مسؤول عن بنية ذات أهمية حيوية تم تدقيقها وضع برنامج عمل لتنفيذ التوصيات الواردة في تقارير التدقيق، وإرساله إلى السلطة الوطنية قصد متابعة تنفيذه.

الفصل 25:

يتعين أن يلجأ المسؤولون عن البنى 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، يتعين على المسؤولين عن البنية التحتية ذات الأهمية الحيوية اللجوء إلى مسدي خدمات مؤهلين من طرف السلطة الوطنية.

تضبط بأمر معايير تأهيل مسدي خدمات الأمن السيبراني.

الفرع الثالث
أحكام خاصة بالمتعهدين

الفصل 26:

على مستغلي الشبكات العمومية للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الإنترنات 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 الحاصلة عليها بواسطة نظم الاستغلال والتطبيقات ومنتوجات الأمن.

تحدد مدة الاحتفاظ بالمعطيات التقنية اللازمة لتحديد وتحليل الحادث في سنة واحدة، ويمكن تغيير المدّة بمقتضى أمر.

الفصل 27 :

يخطر مستغلو الشبكات العامة للمواصلات ومزودو خدمات الإنترنت ومقدمو خدمات الأمن السيبراني ومقدمو الخدمات الرقمية وناشرو منصات الإنترنت حرفائهم بهشاشة نظم معلوماتهم أو الاختراق الذي قد تتعرض له.

الفصل28 :

لضمان أمن نظم المعلومات الخاصة بالهيئات والبيات 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 ومسدي خدمات الأمن السيبراني ومسدي 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 والبنى التحتية ذات الأهمية الحيوية.

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

الفصل 29 :

على مستغلي الشبكات العمومية للمواصلات ومزودي خدمات الإنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري الإنترنت، في إطار توجيهات السلطة الوطنية، اتخاذ التدابير الحمائية اللازمة للوقاية وإبطال مفعول التهديدات أو الإختراقات التي تمس نظم معلومات حرفائهم.

الفصل 30 :

يتعين على مستغلي الشبكات العمومية للمواصلات ومزودو خدمات الإنترنت ومقدمو خدمات الأمن السيبراني ومقدمو الخدمات الرقمية وناشرو منصات الإنترنت حال رصد أحداث قد تؤثر على أمن نظم معلومات حرفائهم إخبار السلطة الوطنية فورا بذلك.

الفصل 31 :

على مستغلي الشبكات العمومية 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.

الفصل 32 :

على مسدي الخدمات الرقمية تحديد المخاطر التي تهدد 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 أدني حد ممكن من أثر هذه المخاطر ضمانا لاستمرارية هذه الخدمات.

الفصل 33:

على مسدي 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.

الفصل 34:

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

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

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

الباب الثالث
حوكمة الأمن السيبراني

الفرع الأول
اللجنة الاستراتيجية للأمن السيبراني

الفصل 35 :

تحدث **"لجنة استراتيجية للأمن السيبراني"**، يعهد إليها القيام بالمهام التالية:

- ضبط التوجهات الاستراتيجية للدولة في مجال الأمن السيبراني والسهر على ضمان صمود نظم معلومات الهيئات والبنى التحتية ذات الأهمية الحيوية والمتعهدين المشار إليهم في الفرع الثالث من الباب الثاني من هذا القانون؛
- التقييم السنوي لأنشطة السلطة الوطنية؛
- تقييم عمل اللجنة الوطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة، المنصوص عليها بالفصل 36 وما بعده؛
- حصر نطاق تدقيقات 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 والبنى التحتية ذات الأهمية الحيوية؛
- إبداء الرأي في مشاريع القوانين والنصوص الترتيبية المتعلقة بمجال الأمن السيبراني.

وتضبط بأمر تركيبة وطرق سير اللجنة الاستراتيجية للأمن السيبراني.

الفصل 36 :

تحدث لدى اللجنة الاستراتيجية للأمن السيبراني، **لجنة لإدارة الأزمات والأحداث السيبرانية الجسيمة**، تكلف بضمان التدخل والتنسيق في مجال الوقاية وإدارة الأزمات على إثر وقوع حوادث أمن سيبراني.

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

وتضبط بأمر تركيبة اللجنة وطرق سيرها ومجال تدخل كل عضو من أعضائها.

الفصل 37 :

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

الفرع الثالث
السلطة الوطنية للأمن السيبراني

الفصل 38:

يعهد إلى السلطة الوطنية مهمة تنفيذ استراتيجية الدولة في مجال الأمن السيبراني.

ولهذا الغرض، تتولى السلطة الوطنية، علاوة على المهام الأخرى المسندة إليهما 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؛

- ضبط 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 والبنى التحتية ذات الأهمية الحيوية؛

- تأهيل مقدمي خدمات تدقيق نظم المعلومات الحساسة للبنى التحتية ذات الأهمية الحيوية ومقدمي خدمات الأمن السيبراني؛

- وضع تصور للوسائل اللازمة لضمان أمن الاتصالات الإلكترونية بين الوزارات وتنسيق تفعيلها؛

- القيام بأعمال المراقبة المنصوص عليها في هذا القانون؛

- السهر على ضمان إجراء عمليات تدقيق أمن نظم معلومات الهيئات والبنى التحتية ذات الأهمية الحيوية؛

- تدقيق متعهدي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية الذين يقدمون خدمات للبنى التحتية ذات الأهمية الحيوية المتوفرة على نظم معلومات حساسة؛

- تقديم المساعدة والنصائح إلى الهيئات والبنى التحتية ذات الأهمية الحيوية قصد تعزيز أمن نظم معلومتها؛

- مساعدة مرافقة الهيئات والبنى التحتية ذات الأهمية الحيوية لوضع أجهزة لرصد أحداث مست أوقد تمس بأمن نظم معلوماتها و تنسيق إجراءات التصدي لهذه الأحداث؛

التعاون، مع الهيئات والبنى التحتية ذات الأهمية الحيوية، من خلال إعداد نظام خارجي لليقظة والرصد والإنذار بأحداث مست أو قد تمس بأمن نظم معلوماتها وتنسيق إجراءات التصدي لهذه الأحداث؛

- القيام بأنشطة البحث العلمي والتقني في مجال الأمن السيبراني وتشجيعها.

الفصل 39:

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

الفصل 40:

تحدد السلطة الوطنية قواعد الأمن اللازمة لحماية نظم معلومات الهيئات والبنى التحتية ذات الأهمية الحيوية والمتعهدين المشار إليهم في الفصل الأول من هذا القانون.

تحدد السلطة الوطنية قواعد أمن خاصة بقطاع أنشطة ذي أهمية حيوية معين.

وتقوم بتبليغ هذه القواعد وطرق وآجال تطبيقها إلى مسؤولي البنية التحتية ذات الأهمية الحيوية التابعين للقطاع المعني.

على المسؤولين سالفي الذكر تطبيق هذه القواعد على نفقتهم.

الفصل 41:

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

الفصل 42:

تتعاون السلطة الوطنية مع السلطات 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، يتعين عليها إحالة الأمر إلى السلطات المختصة.

يتعين على السلطات المختصة إعلام السلطة الوطنية بمآل الإحالة

الباب الرابع
التكوين والتحسيس والتعاون

الفصل 43:

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

وتحدث لهذا الغرض مدرسة عليا للأمن السيبراني.

الفصل 44:

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

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

الفصل 45:

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

الفصل 46:

تقوم السلطة الوطنية، بعد التشاور مع الوزارات المعنية، بتطوير علاقات التعاون مع المنظمات الوطنية والأجنبية في مجال الأمن السيبراني وتنسيقها.

الفصل 47:

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

الباب الخامس
معاينة المخالفات والعقوبات

الفصل 48:

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

توجه محاضر معاينة المخالفات إلى النيابة العمومية المختصة.

الفصل 49:

مع مراعاة العقوبات الجزائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بغرامة من 30 ألف دينار إلى 60 ألف دينار؛

- كل مسؤول عن هيئة أو بنية تحتية ذات أهمية حيوية قام بإيواء المعطيات الحساسة خارج التراب الوطني، خرقا لأحكام الفصل 11 المشار إليه أعلاه؛

- كل مسؤول عن بنية تحتية ذات أهمية حيوية تتوفر على نظام معلومات حساس شرع في استغلاله دون إخضاعه للمصادقة المنصوص عليها في الفصل 19 المشار غليه أعلاه،

- كل مسؤول عن بنية تحتية ذات أهمية حيوية عهد إليه بتدقيق آمن نظم المعلومات الحساسة الخاصة ببنيته تحتية إلى متعهد تدقيق غير مؤهل، خرقا لأحكام الفصل 20 المشار إليه أعلاه.

- كل من قدم خدمات تدقيق أمن نظم المعلومات الحسّاسة للبنى التحتية ذات الأهمية الحيوية دون أن يكون مؤهلا من قبل السلطة الوطنية أو استمر في تقديم هذه الخدمات رغم سحب تأهيله من قبل السلطة.

كل مسؤول عن بنية تحتية ذات أهمية حيوية أسند خدمات الأمن السيبراني إلى مسدي خدمات غير مؤهل، خرقا لأحكام الفصل 25 المشار إليه 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.

الفصل 50:

مع مراعاة العقوبات الجزائية الأشد المنصوص عليها في التشريع الجاري به العمل، يعاقب بغرامة من 20 آلاف إلى 40 ألف دينار:

- كل من أخل بالالتزامات المتعلقة بإبلاغ السلطة الوطنية عن الحوادث، خرقا لأحكام الفصول 8 و30 و33 المشار إليهم أعلاه؛

- كل من قام، باي وسيلة كانت، بعرقلة أو بمنع إجراء عمليات تدقيق أمن نظم المعلومات الحساسة للبنية التحتية ذات الأهمية الحيوية، المنصوص عليها بالفصل 20 المشار إليه أعلاه؛

- كل متعهد لشبكة عمومية للمواصلات أو مزود خدمات الإنترنت أو مقدم خدمات الأمن السيبراني أو مقدم الخدمات الرقمية أو ناشر منصات الإنترنت أخل بالالتزامات المنصوص عليها بالفصل 26 المشار إليه أعلاه؛

- كل متعهد لشبكة عمومية للمواصلات أو مزود خدمات الإنترنت أو أعوانهم، عرقل أعمال السلطة الوطنية أو أعوانها المنصوص عليها في الفصل 28 المشار إليه أعلاه؛

- كل مسدي خدمة رقمية امتنع عن اتخاذ التدابير المنصوص عليها بالفصل 32 المشار إليه أعلاه أو عرقل عمليات المراقبة المنصوص عليها بالفصل 34 المشار إليه أعلاه.

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

الفصل 51:

يمكن للمحكمة أن تحكم بمصادرة المواد والوسائل التي أستعملت لإرتكاب أفعال مخالفة لأحكام هذا القانون.

الفصل 52:

في حالة العود، تضاعف العقوبات المنصوص عليها في هذا القانون.

ويعتبر في حالة عود كل من سبق الحكم عليه بعقوبة من اجل ارتكاب إحدى المخالفات المنصوص عليها في هذا القانون بحكم قضائي بات ثم ارتكب نفس المخالفة قبل مضي أربع سنوات من تمام تنفيذ تلك العقوبة أو تقادمها.

الباب السادس
أحكام ختامية

الفصل 53:

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

الفصل 54:

ينشر هذا القانون بالرائد الرسمي للجمهورية التونسية وينفذ كقانون من قوانين الدولة.

2024/36.

وردات عدد .....
30 افريل 2024 B
مجلس نواب الشعب
مكتب الضبط المركزي

الجمهورية التونسية
مجلس نواب الشعب
كتلة لينتصر الشعب

شـــــرح الأسبـــاب

• • •

تبعا للإعتماد المتزايد على تكنولوجيات المعلومات والاتصالات من قبل الحكومات والشركات والمؤسسات والأفراد، أضحى ضمان الاستخدام الآمن والمناسب للفضاء الرقمي أحد التحديات التي يواجهها العالم اليوم للوقاية من المخاطر السيبرانية.

ولهذا الغرض، قامت العديد من الدول بتبني التدابير الرامية إلى تعزيز الإطار التشريعي والتنظيمي لمواكبة هذا التقدم التكنولوجي، بغية تعزيز الأمن السيبراني الذي يشكل عاملا أساسيا لحماية الامن القومي ولتحقيق التنمية الاقتصادية والاجتماعية.

فالتقدم الكبير الذي عرفه التحول الرقمي، والإعتماد المتزايد على البنيات التحتية التكنولوجية، جعل من الضروري اليوم وضع إطار قانوني لحماية الأنشطة التي تتم ممارستها في الفضاء السيبراني عبر تعزيز الثقة في المعاملات الالكترونية سواء من طرف الأشخاص الطبيعيين أو المعنويين، ولذلك اضطرت مجموعة من الدول إلى اتخاذ تدابير تشريعية وتنظيمية ملزمة في مجال الامن السيبراني من أجل تأمين نظم المعلومات وإنجاح عملية التحول الرقمي والحماية من مخاطر الجرائم السيبرانية وإساءة استخدام المعطيات الشخصية والحساسة.

في هذا السياق وعلى سبيل المثال، عززت فرنسا في سنة 2013 ترسانتها القانونية في مجال الامن السيبراني بمقتضيات تفرض على المتعهدين ذوي الأهمية الحيوية، من خلال قانون البرمجة العسكرية، تعزيز امن نظم المعلومات التي يستعملونها. حيث يفرض هذا القانون على مستغلي شبكات الاتصالات بأن يشاركوا بفعالية في رصد الهجمات السيبرانية التي تستهدف حرفائها ويقر عقوبات على الأجهزة التي تخل بالتزاماتها.

كما وضعت الولايات المتحدة الامريكية أيضا في سنة 2015 إطارا قانونيا يحدد قواعد الحماية من التهديدات السيبرانية.

أما في الإتحاد الأوروبي، فقد تم على التوالي خلال سنتي 2016 و2018 اعتماد توجيه بشأن أمن الشبكات وأنظمة المعلومات وتوجيه خاص بحماية البيانات

2024/36

والمعطيات الشخصية لمواطني الاتحاد من سوء الإستخدام. كما ساهمت الأمم المتحدة سنة 2013 من خلال مجهودات فريق الخبراء الحكوميين التابع للمنظمة في إقرار تطبيق مبادئ وقواعد القانون الدولي في الفضاء السيبراني.

أما في الدول العربية فقد أصدرت كل من الأردن القانون رقم 16 لسنة 2019 والمغرب القانون رقم 5 لسنة 2020 حول الأمن السيبراني .

وبالنظر للتطورات التي يشهدها مجال الأمن السيبراني، فقد أصبح ضروريا أكثر من أي وقت مضى،ادارك هذا الفراغ لدينا وضرورة وضع إطار قانوني شامل يمكن من تعزيز أمن نظم معلومات الدولة والبنى التحتية ذات الأهمية الحيوية، والقيام بعمليات التحسيس لفائدة هيئات القطاع الخاص والأفراد.

و وفقا لما تقدم، واستئناسا بمختلف التشريعات والتجارب الدولية المقارنة الناجحة في مجال الأمن السيبراني، وفي ظل ما راكمته بلادنا من تجربة على المستوى الوطني في هذا الميدان، تم إعداد القانون المتعلق بالأمن السيبراني، الذي يهدف إلى ما يلي:

*** تعزيز حماية وصمود نظم المعلومات**

تتجلى الأهداف الأساسية لهذا القانون في وضع قواعد قانونية بشأن وسائل الحماية الرامية إلى تعزيز الثقة ودعم الاقتصاد الرقمي، وبشكل أعم ضمان استمرارية الأنشطة الاقتصادية والاجتماعية لبلادنا.

ولهذا الغرض، وتحقيقا لأهداف الاستراتيجية الوطنية للأمن السيبراني، لا سيما التي تهم تعزيز حماية وصمود نظم معلومات الدولة والجماعات المحلية والبنى التحتية ذات الأهمية الحيوية، يتضمن هذا القانون تدابير أمنية تهدف إلى تقوية القدرات الوطنية في هذا المجال والمساهمة في تأمين عملية التحول الرقمي بتونس وكذلك تنسيق إجراءات الوقاية والحماية في مواجهة هجمات وحوادث الأمن السيبراني.

وفي هذا الصدد، يضع القانون إطارا تشريعيا يلزم الإدارات العمومية والجماعات المحلية والمؤسسات والمنشآت العمومية وكل شخص معنوي آخر خاضع للقانون العام، المشار إليهم فيما بعد بالهيئات، باحترام التوجيهات والقواعد والأنظمة والمراجع والتوصيات الصادرة عن السلطة الوطنية في هذا المجال.

كما يفرض هذا القانون على الهيئات تنفيذ التدابير والتقنية والتنظيمية لإدارة المخاطر السيبرانية وتجنب الحوادث التي قد تؤثر على نظم المعلومات والالتزام بإبلاغ السلطة الوطنية للأمن السيبراني بأي حادث يؤثر على أمن أو سير نظم

المعلومات الخاصة بها وذلك حتى يتسنى للسلطة الوطنية إيجاد الحلول الناجعة من أجل تجاوز هذا الحادث.

ويلزم هذا القانون كل هيئة بتعيين مسؤول عن أمن نظم المعلومات وإعداد مخططات ضمان استمرارية واستئناف الأنشطة في أقرب الآجال لإبطال مفعول انقطاعاتها.

وبالإضافة إلى الإجراءات الأمنية التي تخضع لها تلك الهيئات والتي تسري أيضا على البنيات التحتية ذات الأهمية الحيوية، ينص القانون على أحكام إضافية خاصة بالبنيات التحتية ذات الأهمية الحيوية التي تتوفر على نظم معلومات حساسة، لا سيما تلك المتعلقة بالمصادقة على نظم المعلومات الخاصة بها، وإخضاع هذه النظم لتدقيقات أمنية من قبل الأعوان المعتمدين من طرف السلطة الوطنية أو من قبل متعهدي التدقيق المؤهلين من طرف السلطة الوطنية.

*** توسيع نطاق الحماية بدمج فئات فاعلة أخرى**

ينص القانون المتعلق بالأمن السيبراني على اتخاذ التدابير التقنية والتنظيمية اللازمة لحماية شبكات ونظم معلومات فئات فاعلة أخرى تشمل مستغلي الشبكات العمومية للمواصلات، ومزودي خدمات الانترنت، ومقدمي خدمات الأمن السيبراني، ومقدمي الخدمات الرقمية وناشري منصات الانترنت.

ويعتبر هؤلاء المتعهدون طرفا استراتيجيا في تعزيز أمن نظم معلومات الهيئات والبنى التحتية ذات الأهمية الحيوية ومتعهدي القطاع الخاص والأفراد. وينص هذا القانون كذلك على احتفاظ المتعهدين سالفي الذكر بالمعطيات التقنية الكفيلة بتحديد حوادث الأمن السيبراني والإبلاغ عن أي حادث قد يؤثر على نظم معلومات حرافائهم واتخاذ التدابير الوقائية اللازمة لمنع وتخفيف وقع التهديدات أو المساس بهذه النظم.

كما يولي هذا القانون أهمية كبيرة للوقاية والتحسيس بشأن تحديات الأمن السيبراني، حيث يعهد للسلطة الوطنية بأن تنشر بانتظام على موقعها الالكتروني النصائح والتوصيات الوقائية المتعلقة بالأمن السيبراني لفائدة الإدارات العمومية والجماعات المحلية والمؤسسات والمنشآت العمومية والبنى التحتية ذات الأهمية الحيوية ومتعهدي القطاع الخاص والمواطنين.

*** مواجهة الهجمات السيبرانية وتعزيز الرقمنة وحماية المعطيات الشخصية والحساسة**

تلعب جودة تبادل المعلومات والمعطيات بين المصالح المختصة للدولة دورا هاما في مكافحة الهجمات السيبرانية. ولهذا الغرض، يضع القانون إطارا للتعاون

وتبادل المعلومات بين السلطة الوطنية للأمن السيبراني والمصالح المختصة في الدولة المكلفة بالتصدي للجرائم التي تخل بسير نظم المعالجة الآلية للمعطيات.

كما تسهم السلط الوطنية، وفقا لهذا القانون، في دعم البرامج التي تعدها الهيئات المختصة في الدولة من أجل تعزيز الثقة وتطوير رقمنة الخدمات وحماية المعطيات ذات الطابع الشخصي.

ومن أجل مضاعفة قدرات التصدي للهجمات السيبرانية، فإن هذا القانون يعطي أولوية هامة لتعزيز التعاون وتطوير تبادل التجارب والخبرات مع المنظمات والمؤسسات الأجنبية المماثلة.

*** تخويل اللجنة الاستراتيجية والسلطة الوطنية صلاحيات ووسائل الاضطلاع بمهمة حماية نظم المعلومات**

يولي هذا القانون أهمية بالغة لحوكمة الأمن السيبراني من خلال تحديد المهام الموكلة إلى اللجنة الاستراتيجية للأمن السيبراني، والسلطة الوطنية للأمن السيبراني واللجنة الوطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة.

كما ينص القانون على إمكانية إجراء عمليات تدقيق لضمان تنفيذ قواعد أمن وحماية نظم المعلومات.

*** تعزيز وتطوير البيئة الوطنية للأمن السيبراني**

إضافة إلى التأثير المباشر على سير الاقتصاد والمجتمع، سيمكن هذا القانون من تعزيز البيئة الوطنية للأمن السيبراني، وهو ما سيعزز ويطوّر الخدمات في مجال الاستشارة والتدقيق والرصد ومعالجة حوادث الأمن السيبراني المنتوجات التي تسمح بتأمين الشبكات ونظم المعلومات.

ولضمان تطبيق أحكام هذا القانون، تضمنت أحكامه مقتضيات زجرية عند الإخلال بها، مثل عدم الإبلاغ عن الحوادث التي تؤثر على نظم المعلومات، أو إيواء المعطيات الحساسة خارج التراب الوطني، أو إعاقة إجراء عمليات تدقيق أمن نظم المعلومات، أو عدم تنفيذ القرارات والتدابير الأمنية الصادرة عن السلطة الوطنية للأمن السيبراني.

تلك هي الغاية من هذا القانون.

الجمهورية التونسية
مجلس نواب الشعب

2024/36.

واردات عدد .....
30 أفريل 2024
مجلس نواب الشعب
مكتب الضبط المركزي

قائمة الإمضاءات حول

"مشروع قانون يتعلّق بالأمن السيبراني"

ع/ر	الإسم واللقب	الإمضاء
1	علي زعدود	
2	عبد العزيز	
3	المختار عبد الله	
4	لطفي السعداوي	
5	أمنة البوغنيوا	
6	محمد ماجدا	
7	محمد سنا	
8	النوري جريدي	
9	عادل البوسالمي	
10	محمد هنو	
11		
12		
13		
14		
15		
16		

2024/36.

2024/36.

الجمهورية التونسية

مجلس نواب الشعب

باردو في، 2024/04/29

وارد بمكتب الضبط عدد .....
30 أفريل 2024
B
مجلس نواب الشعب
مكتب الضبط

تصـريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله علي زغدود .....
عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء

2024/36.

2024/36.

الجمهورية التونسية

مجلس نواب الشعب

باردو في، 29/04/2024

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله عماد الحمروني

عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضاء

02693296

2024/36

الجمهورية التونسية

مجلس نواب الشعب

باردو في، 2024 01 29

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله ..... المختار عبد الموى .....

عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــام العلم **بمضمونه** وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء

الجمهورية التونسية
مجلس نواب الشعب

2024/36

باردو في، 05/04/2024

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله ..... لطفي العداوي .....
عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء

الجمهورية التونسية
مجلس نواب الشعب

2024/36

باردو في، 2024/04/29

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله ..... أمينة الجندوبي .....
عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء

الجمهورية التونسية
مجلس نواب الشعب

2024/36.

باردو في، 29/04/2024

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله ..... محمد الماجدي .....
عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء

2024/36.

الجمهورية التونسية
مجلس نواب الشعب

باردو في، 2024/04/29

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله محمد سمّاعي
عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء

الجمهورية التونسية
مجلس نواب الشعب

2024/36 م

باردو في، 2024/04/29

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله ..... النّوري جريبي .....
عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء

الجمهورية التونسية
مجلس نواب الشعب

2024/36

باردو في، 2024/04/29

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله عادل البوسالمي
عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54

وإنّي على تمـــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء

2024/36.

الجمهورية التونسية
مجلس نواب الشعب

واردات عدد .....
30 افريل 2024 B
مجلس نواب الشعب
مكتب الضبط المركزي

باردو في، 2024/04/29

تصـــريح

بتبنّي مقترح قانون

إنّي الممضي (ة) أسفله .....محمد عمّو.....
عضو مجلس نوّاب الشّعب،

وعملا بأحكام الفصل 68 من أحكام دستور الجمهوريّة التّونسيّة لسنة 2022 والفصل 122 من النّظام الدّاخلي لمجلس نوّاب الشّعب،

أصرّح وأنّي أتبنّى عرض مقترح القانون حسب البيانات التّالية:

عنوان مقترح القانون	مشروع قانون يتعلق بالأمن السيبراني
عدد الفصول المضمّنة بمقترح القانون	54 فصلا

وإنّي على تمـــام العلم بمضمونه وأطلب عرضه وفق الشّروط القانونيّة قصد النّظر في إمكانيّة المصادقة عليه

الإمضـاء