المملكـــة المغـــربيـة
إدارة الدفاع الوطني

مذكـرة تقديمية للقانون رقم 05.20 المتعلق بالأمن السيبراني

مع الاعتماد المتزايد على تكنولوجيات المعلومات والاتصالات من قبل الحكومات و الشركات و المؤسسات و الأفراد، أضحى ضمان الاستخدام الآمن و المناسب للفضاء الرقمي أحد التحديات التي يواجهها العالم للوقاية من المخاطر السيبرانية. ولأجل ذلك، قامت العديد من الدول بتبني التدابير الرامية إلى تعزيز الإطار التشريعي والتنظيمي لمواكبة هذا التقدم التكنولوجي، بغية تعزيز الأمن السيبراني الذي يشكل عاملا أساسيا لتحقيق التنمية الاجتماعية والاقتصادية.

فالتقدم الكبير الذي عرفه التحول الرقمي، والاعتماد 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 الذاتيين أو الاعتباريين. ولذلك، اضطرت مجموعة من الدول إلى اتخاذ تدابير تشريعية وتنظيمية ملزمة في مجال الأمن السيبراني من أجل تأمين نظم المعلومات وإنجاح عملية التحول الرقمي والحماية من مخاطر الجرائم السيبرانية وإساءة استخدام المعطيات الشخصية والحساسة.

1. تعزيز الدول لتشريعاتها المتعلقة بالأمن السيبراني

في هذا السياق و على سبيل المثال، عززت فرنسا في سنة 2013 ترسانتها القانونية في مجال الأمن السيبراني بمقتضيات تفرض على المتعهدين ذوي الأهمية الحيوية، من خلال قانون البرمجة العسكرية، تعزيز أمن نظم المعلومات التي يستعملونها. حيث يفرض هذا القانون على مستغلي شبكات الاتصالات بأن يشاركوا بفعالية في رصد الهجمات السيبرانية التي تستهدف زبنائها، ويقر عقوبات على الأجهزة التي تخل بالتزاماتها. كما وضعت الولايات المتحدة الأمريكية أيضا في سنة 2015 إطارا قانونيا يحدد قواعد الحماية من التهديدات السيبرانية.

وعلى مستوى الاتحاد الأوروبي، تم على التوالي خلال سنتي 2016 و2018 اعتماد توجيه بشأن أمن الشبكات وأنظمة المعلومات وتوجيه خاص بحماية البيانات والمعطيات الشخصية لمواطني الاتحاد من سوء الاستخدام. كما ساهمت الأمم المتحدة سنة 2013 من خلال مجهودات فريق الخبراء الحكوميين التابع للمنظمة في إقرار تطبيق مبادئ وقواعد القانون الدولي في الفضاء السيبراني.

2. الأمن السيبراني بالمغرب: تجربة غنية انطلقت منذ سنة 2011

انخرط المغرب منذ سنة 2011، تحت **القيادة الرشيدة لصاحب الجلالة الملك محمد السادس نصره الله وأيده**، في مسار تطوير القدرات الوطنية لأمن نظم المعلومات وتعزيز الثقة الرقمية، حيث اعتمدت بلادنا سنة 2012 الاستراتيجية الوطنية للأمن السيبراني، وكذا التوجيهات الوطنية لأمن نظم المعلومات التي بدأت في تطبيقها الإدارات والمؤسسات العمومية منذ سنة 2014.

وتنزيلا لهذه الاستراتيجية ، قامت إدارة الدفاع الوطني سنة 2016 بإعداد مرسوم بشأن تحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية، بالإضافة إلى إصدار قرار لرئيس الحكومة سنة 2018 يحدد شروط اعتماد المتعهدين الخواص لافتحاص نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية وكذا كيفيات إجراء هذا الافتحاص.

وبالنظر للتطورات التي يشهدها مجال الأمن السيبراني، فقد أصبح ضروريا أكثر من أي وقت مضى، التوفر على إطار قانوني شامل يمكن من تعزيز أمن نظم معلومات الدولة والبنيات التحتية ذات الأهمية الحيوية، والقيام بعمليات التحسيس لفائدة هيئات القطاع الخاص والأفراد.

3. القانون رقم 05.20 لتعزيز الثقة والأمن الرقمي

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، قامت إدارة الدفاع الوطني، بعد **الموافقة الملكية السامية**، بإعداد القانون رقم 05.20 المتعلق بالأمن السيبراني بتنفيذ الظهير الشريف رقم 1.20.69 الصادر في 4 ذي الحجة 1441 (25 يوليو 2020)، 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 الترابية وكذا البنيات التحتية ذات الأهمية الحيوية، يتضمن هذا النص التشريعي تدابير أمنية تهدف إلى تقوية القدرات الوطنية في هذا المجال والمساهمة في تأمين عملية التحول الرقمي بالمغرب وكذا تنسيق إجراءات الوقاية والحماية في مواجهة هجمات وحوادث الأمن السيبراني.

وفي هذا الصدد، يضع القانون رقم 05.20 إطارا قانونيا يلزم إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية وكل شخص اعتباري 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 التقنية 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 رقم 05.20 على أحكام إضافية خاصة بالبنيات التحتية ذات الأهمية الحيوية التي تتوفر على نظم معلومات حساسة، لا سيما تلك المتعلقة بالمصادقة على نظم المعلومات الحساسة الخاصة بها، وإخضاع هذه النظم لإفتحاصات أمنية من قبل الأعوان المعتمدين من طرف السلطة الوطنية أو من قبل متعهدي الإفتحاص المؤهلين من طرف السلطة الوطنية.

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

ينص القانون رقم 05.20 المتعلق بالأمن السيبراني على اتخاذ التدابير التقنية والتنظيمية اللازمة لحماية شبكات ونظم معلومات فئات فاعلة أخرى تشمل مستغلي الشبكات العامة للمواصلات، ومزودي خدمات الانترنيت، ومقدمي خدمات الأمن السيبراني، ومقدمي الخدمات الرقمية وناشري منصات الانترنيت.

ويعتبر هؤلاء المتعهدون طرفا استراتيجيا في تعزيز أمن نظم معلومات الهيئات والبنيات 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 أمن نظم معلومات زبنائهم واتخاذ التدابير الوقائية اللازمة لمنع وتخفيف وقع التهديدات أو المساس بهذه النظم.

كما يولي هذا القانون كذلك 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 إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية والبنيات التحتية ذات الأهمية الحيوية ومتعهدي القطاع الخاص والمواطنين.

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

تلعب جودة تبادل المعلومات و المعطيات بين المصالح المختصة للدولة دورا هاما في مكافحة الهجمات السيبرانية. ولأجل ذلك، يضع القانون رقم 05.20 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 السلطة 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 لتنمية التعاون وتطوير تبادل التجارب والخبرات مع المنظمات والمؤسسات الأجنبية المماثلة.

- ✓ **تخويل اللجنة الاستراتيجية و السلطة الوطنية صلاحيات ووسائل الاضطلاع بمهمة حماية نظم المعلومات**

يولي هذا القانون أهمية بالغة لحكامة 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 رقم 05.20 على إمكانية إجراء عمليات افتحاص 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 سيعطي دفعة لتطوير الخدمات في مجال الاستشارة والافتحاص والرصد ومعالجة حوادث الأمن السيبراني وكذا المنتوجات التي تسمح بتأمين الشبكات ونظم المعلومات.

ولضمان تطبيق وتنفيذ أحكام هذا القانون، يتضمن هذا النص التشريعي مقتضيات زجرية في حالة الإخلال، مثل عدم الإبلاغ عن الحوادث التي تؤثر على نظم المعلومات، أو إيواء المعطيات الحساسة خارج التراب الوطني، أو إعاقة إجراء عمليات افتحاص أمن نظم المعلومات، أو عدم تنفيذ القرارات والتدابير الأمنية الصادرة عن السلطة الوطنية للأمن السيبراني.

تلكم هي الغاية من هذا القانون.