الأمن السيبراني ورهانات التحول الرقمي في المغرب
–التأصيل المفاهيمي والإستراتيجية التشريعية–

الباحث سعيد أوغان
كلية العلوم القانونية والاقتصادية والاجتماعية سلا
جامعة محمد الخامس الرباط
المغرب

مقدمة:

لا شك أنّ أمن الدول هو محور وغاية كل سياسة أمنية أو دفاعية، غير أنّ الرهانات والتحديات التي يطرحها هذا الهدف تبدو في غاية الأهمية والحساسية، إذا ما أخذنا في الحسبان التطور التكنولوجي والثورة الرقمية الهائلة التي جعلت من العالم قرية صغيرة، وحتّمت على الدول انتهاج سياسات أمنية ودفاعية تأخذ في الاعتبار الفضاء الافتراضي المفتوح بكل ما يحتويه من زخم، وكل ما يتعرض له من أخطار وتحديات في عالم توحدت فيه البنى التحتية المعلوماتية على المستويات الوطنية والإقليمية والدولية.

ففي الوقت الذي تتحوّل فيه مفاهيم الأمن والقوة والجريمة والحروب التقليدية، نتيجة العولمة والاتصالات واختراق حدود الدول، يفرض إيجاد بنية تحتية معلوماتية قوية، تجعل مسؤولية حماية الأمن السيبراني مسؤولية دولية، وتتعزز من خلالها القوانين العالمية.

فبالقدر الذي تطوّرت فيه الخدمات الإلكترونية، تطوّرت المخاطر والجرائم السيبرانية، وظهرت طرق جديدة لارتكاب الجرائم على الفضاء السيبراني. مما يفرض اتخاذ التدابير اللازمة لمواجهتها، وتعزيز الجهود الوطنية والإقليمية والدولية لمواكبة التحولات في مفهوم الأمن الدولي، وسياسات الدفاع ومفاهيم الجريمة والإرهاب الإلكتروني والتجارة الإلكترونية والبحث العلمي، بغرض التفاعل مع المفاهيم الحديثة للأمن السيبراني وانعكاساتها الخطيرة التي لا تقف عند حدود تهديد الأفراد والمؤسسات، بل تتعداها إلى تهديد أمن الدول والمجتمعات. مما يستدعي وضع مقاربة شاملة لجميع التحديات التي يطرحها الفضاء السيبراني، مع إعادة النظر في مفهوم السيادة الوطنية والأمن الإلكتروني للدول، ووضع آليات قانونية واتفاقية تواكب هذا التحوّل وتحدّ من مخاطر الفضاء السيبراني المتعددة.

أهمية الدراسة

تظهر أهمية هذه الدراسة في إطار الاهتمام الرسمي الذي توليه المملكة المغربية لتأمين فضائها السيبراني من الهجمات السيبرانية التي قد تتعرض لها من بعض الدول من جهة، ومن جهة أخرى ضرورة مواكبة السباق السريع نحو استغلال مساحات الفضاء السيبراني من أجل مواجهة مخاطر هذا الفضاء المفتوح على برامج الاختراق والقرصنة وكافة أشكال التهديدات السيبرانية داخلياً وخارجياً، مما أدى إلى تحول في مفهوم الأمن للدول الذي لم تعد فيه

مكانة للمفاهيم التقليدية مع بروز ثورة المعلومات؛ الأمر الذي يتطلب من الدول الأقل أمنا إلكترونياً وسيبرانياً، انتهاج استراتيجيات أمنية جديدةوتوحيد الجهود الإقليمية والدولية لمواجهة مخاطر الفضاء السيبراني.

إشكالية الدراسة:

في ظل ما يشهده العالم من اختلالات في موازين القوى وإعادة رسم خارطة القوة الدولية، يطرح التساؤل التالي: إلى أي حد يمكن إعادة النظر في الاستراتيجيات الأمنية والدفاعية للدول في مجال الأمن السيبراني الوطني للحفاظ على السيادة الوطنية والمصالح الاقتصادية والمعطيات الحساسة ضد الأخطار والتهديدات الالكترونية المحدقة، في ظل الانتشار الواسع للجرائم السيبرانية والقرصنة؟ وما طبيعة الآليات والاستراتيجيات التشريعية الكفيلة بضمان الأمن السيبراني للدول، وسبل التنسيق الإقليمي والدولي ومدى فاعليتها؟

منهج الدراسة:

اعتمدنا في هذه الدراسة على المنهج الوصفي، من خلال مناقشة الظاهرة السيبرانية وتأصيلها معرفياً وفقهياً، وبيان ارتباطاتها ببعض المفاهيم التقليدية كالأمن، والحرب. كما اعتمدنا أيضاً على المنهج التحليلي لدى مناقشة وتقييم وتحليل السياسات الأمنية والاستراتيجيات التشريعية لمواجهة الخطر السيبراني المتصاعد في ظل تحديات الواقع وتجليات المستقبل. واستخدمنا كذلك المنهج المقارن لدى مقاربة الاستراتيجية الوطنية ومقارنتها بالاستراتيجيات الإقليمية والدولية في مجال أمن الفضاء السيبراني.

خطة البحث:

تقوم خطة هذه الدراسة على مبحثين، حيث خصصنا فيها المبحث الأول لاستعراض التأصيل المفاهيمي والمعرفي للأمن السيبراني والجريمة السيبرانية في ظل المخاطر المحدقة في الفضاء الرقمي، في حين كان المبحث الثاني عبارة عن قراءة في الجهود الوطنية والدولية لتأمين الفضاء السيبراني من خلال بعض الآليات التشريعية والمؤسساتية والاتفاقيات.

المبحث الأول: التأصيل المفاهيمي والمعرفي للأمن السيبراني والجريمة السيبرانية في ظل المخاطر المحدقة في الفضاء الرقمي.

المبحث الثاني: الاستراتيجية الوطنية والإقليمية والدولية لمواجهة المخاطر والتهديدات السيبرانية.

المبحث الأول: التأصيل المفاهيمي والمعرفي للأمن السيبراني والجريمة السيبرانية في ظل المخاطر المحدقة في الفضاء الرقمي

لا شك أن انتشار ثورة المعلوماتية وتطور التكنولوجيا الرقمية واستخدامها من طرف الدول والمنظمات والأفراد انعكست على موازين القوى في العلاقات الدولية، وأحدث نمطاً جديداً في مقاربات أمن الدول، في اتجاه انتهاج الخيارات المعلوماتية في خوض سباق التفوق الدولي، ويحتم أيضاً إعادة النظر في المفاهيم التقليدية للأمن والجريمة والحرب والصراع والقوة، وهو ما سيتم التطرق إليه من خلال هذا المبحث.

المطلب الأول: مفهوم الأمن السيبراني وماهية الجريمة السيبرانية

أصبحت السياسات الأمنية والدفاعية للدول اليوم مرتبطة بمدى قدرتها على توظيف الفاعل الرقمي في حماية مجالها السيبراني من كل الجرائم الداخلية والاعتداءات الخارجية، مما يستلزم معه تحديد مفهوم الأمن السيبراني، وماهية الجريمة السيبرانية ومدى تأثيراتها على الأمن الداخلي للدول، والاستراتيجيات الكفيلة لمواجهتها.

الفرع الأول: تعريف الأمن السيبراني

الأمن السيبراني هو عبارة عن مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرّح له بالدخول إلى شبكات الكمبيوتر، أو سوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية وخصوصية البيانات الخاصة بفواعل الفضاء السيبراني1، وبالتالي فهو المجال المتعلق بمعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات أو للحد من آثارها.

وقد عرّفه ريشارد كوموري بأنّه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة"2. أمّا إدوارد أومورسو فعرّفه بأنّه: "وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها"3.

وبحسب تعريف الاتحاد الدولي للاتصالات في تقريره حول اتجاهات الإصلاح في الاتصالات للعام **2010 – 2011**، فإنّه:" مجموعة من المهمات كتجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين"4، وهو المفهوم نفسه تقريباً الذي أخذت به وكالة الأمن الرقمي الأوروبية في أول تشريع أصدرته في هذا الشأن سنة **2001** ، أنه: "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق أو الحوادث غير المتوقعة، التي تستهدف البيانات المتداولة أو المخزنة وفق إطار توافقي"5، تنتظم فيه الأدوات القانونية والسياسات الأمنية ووسائل الدفاع الإلكتروني لتحقيق أهداف الأمان السيبراني المنشودة وطنياً وإقليمياً ودولياً.

وما يمكن استنتاجه بخصوص هذا المفهوم هو أن الأمن السيبراني يضيف إلى البعد المادي والتكنولوجي لأمن المعلومات كلا من البعد القانوني المتعلق بوسائل الحماية القانونية من كل ما من شأنه أن يشكل جريمة، وبعد سياسي يندرج في إطار السياسة الأمنية الداخلية والخارجية، وما تتطلبه من تعزيز وسائل وأدوات الدفاع من جهة، وتعاون بين الدولة والقطاع الخاص والمحيط الإقليمي والدولي من جهة أخرى.

الفرع الثاني: ماهية الجريمة السيبرانية وأشكالها

نظراً لحداثة النظام السيبراني واتساع نطاق الاعتماد على المعلوماتية في المجالات التقنية والاقتصادية والعسكرية والشخصية؛ فإنّه صار من الضروري وضع تعريف دقيق لكل نشاط يأخذ توصيف الجريمة ينتهك ضمن نطاق الفضاء السيبراني بكل مكوناته، وهو ما يعرف بالجرائم السيبرانية التي ما زال تحديد مفهومها وأشكالها ونطاقها محل جدل فقهي، فالجريمة السيبرانية هي: كل ما يقع على الشبكات وأنظمة تقنية المعلومات والأنظمة التشغيلية ومكوناتها(الأجهزة والبرمجيات والخدمات) من اختراق أو تعطيل أو تعديل أو استخدام أو استغلال غير مشروع6، ومن جهة أخرى هي: الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضد الأشخاص كجريمة السب أو القذف عبر الإنترنت**7**.

وعموما، يصعب التمييز بين الجريمة الإلكترونية والجريمة السيبرانية من الناحية النظرية على الأقل. لذلك يستخدم المفهوم الأول في الغالب عند التطرق للجرائم السيبرانية، خاصة أنّه لم يتم حسم الجدل الفقهي حول تحديد تعريف ونطاق واضح لهذا المفهوم، وهو ما يمكن فهمه من خلال بعض الاتفاقيات الدولية التي جاءت بعنوان مكافحة الجريمة المعلوماتية، أو التشريعات الوطنية التي تطرقت لتحديد مفاهيم الأمن والجريمة الإلكترونية، مرتكزة على الأبعاد التقنية والمادية والجرائم ذات الصلة.

وقد اجتهدت بعض الدول في تعريفها منعا لأي مغالطات في تفسير وتحديد أركان وأشكال ونطاق هذه الجرائم، من بينها المغرب الذي حيزا مهما للجرائم الماسة بنظم المعالجة الآلية للمعطيات من خلال القانون 07.03 8، والتي تدخل ضمن فصول القانون الجنائي، انطلاقا من المادة 3-607 والتي تنص في الفقرة الأولى على جريمة الولوج عن طريق الاحتيال إلى نظام المعالجة الآلية للمعطيات، ومن خلال الفقرة الثانية من نفس المادة على جريمة البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات. كما تطرق المشرع من خلال الفصل 5-607 إلى كل من جريمة عرقلة سير نظام المعالجة الآلية للمعطيات وإحداث خلل في نظام المعالجة الآلية.

ومن هنا يتضح لنا أن المشرع المغربي انخرط في مصاف الدول التي جرمت المس بنظم المعالجة الآلية للمعطيات، او ما يعرف بالجريمة المعلوماتية، وبالتالي أضحى المس بسرية النظام المعلوماتي وسلامته، وسلامة المعطيات المعلوماتية جرائم تستوجب العقاب.

وعليه تعد جريمة سيبرانية كل فعل يأخذ وصف الجريمة في القانون الجنائي العام يرتكب في الفضاء السيبراني من قبل أشخاص، أو جماعات، أو منظمات، أو دول بواسطة أجهزة الحاسوب وبرامج الإعلام الآلي وشبكة الإنترنت، أو الاعتداء عليها أو بها، مما يهدد حق الأفراد في الخصوصية وقواعد البيانات الخاصة وأنظمة المعلومات والاتصالات، وقد يأخذ بعداً أمنياً وعسكرياً حينما يتعلق الأمر بأنظمة الدفاع والتسلح.

الفرع الثالث: أشكال الجرائم والتهديدات السيبرانية

تتنوع الجرائم والتهديدات السيبرانية بتنوع الأشخاص أو الكيانات المرتكبة لها، والأدوات المستعملة والأهداف المتوخاة، وبحسب كونها وطنية أو عابرة للحدود، منها على سبيل المثال:

كل ما يعرّض الأمن القومي والعسكري والاقتصادي والاجتماعي، ويهدد البنية التحتية للدول وأسواق المال والقطاعات المصرفية، والسلم الدولي، والمنشآت النووية، والمؤسسات الصحية، وقطاعات النقل بكل أنواعها**9**.

المساس بسرية الاتصالات على الوسائط الإلكترونية، وسرقة البيانات الشخصية وتسريبها واستخدامها دون إذن، ودون وجه حق، وسرقة الأموال، واختراق أنظمة المعلومات، والاعتداء على الملكية الفكرية، والصناعية والعلامات التجارية.

الجرائم العادية التي تستخدم الإنترنت في تنفيذها، كالسرقة والغش والخداع، والتغرير بالقاصرين، وتسهيل الدعارة، والترويج لنشاطات مخالفة للقانون.

التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو إتلافها، سواء عبر الاقتحام اليدوي، أو عبر إرسال برامج وفيروسات مخصصة بذلك.

إتلاف المعطيات والبيانات المخزّنة الرقمية أو تشويهها، والتجسس على الشبكات، بالإضافة إلى تدمير الأصول والمعلومات10 بواسطة الأنظمة الخبيثة والفيروسية بأهداف إجرامية أو إرهابية.

الإرهاب الإلكتروني، ويأخذ شكل التهديدات القائمة على مهاجمة أنظمة الحواسيب، بغرض الترويع أو الابتزاز أو إجبار الحكومات أو الأفراد على تحقيق أهداف سياسية أو دينية أو عقائدية11، وينبغي أن يكون الهجوم مدمراً وتخريبياً لتوليد الخوف، بحيث يكون مشابهاً للأفعال المادية للإرهاب.

المطلب الثاني: المخاطر والتهديدات السيبرانية في الفضاء الرقمي

يعد الفضاء السيبراني ساحة للعديد من المخاطر التي تعتبر في الأساس جرائم تقليدية، أسهم التحول الرقمي وتنوع الفاعلين وصعوبة الإثبات وتعدد آليات المواجهة في فداحتها، وهو ما سيتم تبيانه من خلال هذا المطلب.

الفرع الأول: التهديدات السيبرانية

لا تقتصر التهديدات والمخاطر في الفضاء السيبراني على الحروب السيبرانية والصراعات غير المرئية بين الدول سعياً منها نحو تأمين مجالها السيبراني وتعزيز منظومتها الدفاعية الرقمية، فهذا الفضاء السيبراني مجال لأشكال أخرى من التهديدات التي يرتكبها الأفراد والجماعات والمنظمات، على غرار الإرهاب السيبراني والقرصنة الإلكترونية، وهذا ما يجعل بعض الدول تقوم باستكشاف إمكانية اتباع نهج حربي تقليدي عندما يتعلّق الأمر بمناورات سيبرانية، مما يجعلها تصمّم أسلحة سيبرانية هجومية وقدرات دفاعية أيضاً، وهي تعتبر الأسلحة السيبرانية بمثابة(مضاعِفات القوة)، التي ينبغي استعمالها في المقام الأول بالاقتران مع الأعمال العسكرية الأكثر تقليدية من أجل تعزيز قدراتها الحربية بشكل كبير12، حيث يمكن اعتبار هذه المناورات حرباً معلوماتية وتهديداً للأمن القومي تضاهي الأعمال العسكرية، سواء أسفرت عن خسائر أم لا13، وبهذا الصدد فإنّ العديد من البلدان تعتبر إتلاف المعلومات على الإنترنت شكلاً من أشكال الاعتداء العسكري ضد معنويات الجمهور، ومن ثم تكون مستعدة للتصدي للتهديدات السيبرانية باستخدام القوة العسكرية14.

الفرع الثاني: القرصنة الإلكترونية

تعد القرصنة الإلكترونية جريمة مكتملة الأركان في معظم التشريعات الجزائية، فهي ترتكب من طرف أشخاص هواة أو محترفين لتحقيق أهداف إجرامية، وإحداث تلف بالأجهزة والبرمجيات الرقمية الحديثة، والمساس بأمن الشبكات وسريتها، فهي عبارة عن عملية دخول غير مشروع، إلى أجهزة الغير وشبكاتهم الإلكترونية؛ أي أن توجه هجمات إلى معلومات الكمبيوتر أو خدماته، بقصد المساس بالسرية أو المساس بسلامة المحتوى والتكاملية، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها15، ويقول محمد أمين الشوابكة بأنّها: "جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك النتيجة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"16. والواقع أنّ أي محاولة لتحديد مفهوم القرصنة الإلكترونية يجب أن تأخذ في الحسبان المعطيات المتعلقة بموضوع الجريمة أو نمط السلوك محل التجريم، والوسيلة المستخدمة في ارتكابها، وكذا صفات القرصان، وهدفها.

ورغم أنّ التشريعات الجنائية سبقت في أحكامها الجزائية التقليدية عصر الإنترنت، إلاّ أنّ الكثير منها حاول تدارك الأمر، من خلال استحداث جرائم وعقوبات تواكب الثورة الرقمية، وتستهدف تجريم كل ما من شأنه المساس، أو الاعتداء على أنظمة المعلومات وقواعد البيانات، وهو ما ذهب إليه المشرع المغربي، حيث ينص الدستور المغربي على أنه " لا يجوز إلقاء القبض على أي شخص أو اعتقاله أو متابعته أو إدانته، إلا في الحالات و طبقا للإجراءات التي ينص عليها القانون"17، تلته بعد ذلك مجموعة من النصوص القانونية التي تجرم وتعاقب على الجريمة الالكترونية خاصة القانون رقم 03-07 المتعلق بجرائم المس بنظم المعالجة الآلية للمعطيات. حيث نصت المادة 3 من الفصل 607 من القانون الجنائي على أنه: "يعاقب بالحبس من شهر على ثلاثة أشهر و بالغرامة

من 2000 إلى 10000آلاف درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات عن طريق الاحتيال...". وأضافت المادة ذاتها على أنه: ...ويعاقب بنفس العقوبة من بقي في نظام المعالجة الآلية للمعطيات أو جزء منه، كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله، وتضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية أو اضطراب في سيره".

كما عمل المشرع المغربي في قانون حماية حقوق المؤلف على وضع مرجعية جنائية خاصة بدل الإحالة إلى فصول القانون الجنائي وذلك راجع إلى خصوصية هذه المادة، فنص في المادة 64 على: يعاقب بالحبس من شهرين إلى ستة أشهر وبغرامة تتراوح بين 10.000 إلى 100.000 درهم أو بإحدى هاتين العقوبتين فقط، كل من قام بطريقة غير مشروعة وبأي وسيلة كانت بقصد الاستغلال التجاري بخرق معتمد لحقوق المؤلف المشار لها في المادتين 9 و10 لحقوق فناني الأداء في المادة 50 لحقوق منتجي المحلات الصوتية (المادة 51) لحقوق هيئات الإذاعة (المادة 52).

والملاحظ أن الحبس والغرامة هنا عقوبتان أصليتان الأولى سالبة للحرية والثانية عقوبة مالية، مع السلطة التقديرية للقضاء في تكريس العقوبتين أو إحداهما تتناسب مع خطورة الفعل الجرمي. وعلى العموم نجد المشرع المغربي متجاوبا مع اتفاقية (التربيس) التي حثت الدول على تبني نظام إجرائي رادع للمخالفين18.

كما تأخذ القرصنة الإلكترونية عدة توصيفات منها :الاحتيال المعلوماتي، والاختراقات وجرائم التقنية العالية، وجرائم أصحاب الياقات البيضاء، والأنونيموس(الهاكرز المتخفون)، الذين يشنون منذ أكثر من عقدين حرباً لا هوادة فيها ضد المواقع الرسمية والسرية للدول والجماعات وفق منطلقات أيديولوجية معيّنة لتحقيق أهداف خاصة، أو في إطار التوظيف لفائدة جهات رسمية أو استخباراتية أو بدوافع شخصية، غير أنّ جميع السياسات التشريعية وآلياتها الردعية وحتى الجهود التنسيقية عجزت عن مواجهة هذا النوع من الجرائم في ظل ثورة رقمية مهولة، وفضاء افتراضي مفتوح على كل المخاطر والابتكارات، وفي عالم افتراضي يتجدد ويتطور ويتأقلم مع كل الآليات المستخدمة لمواجهته.

ومن أشهر هذه التحديات والصعوبات التي تواجه مكافحة القرصنة الإلكترونية نذكر ما يلي19:

الصبغة العالمية للجريمة الإلكترونية المرتكبة عبر الإنترنت.

صعوبة إثبات الجريمة الإلكترونية.

عدم قدرة نصوص التجريم التقليدية على مسايرة تطور الجريمة الإلكترونية.

وبالتالي فالقرصنة الإلكترونية هي عملية تقنية بحتة تقوم أهدافها على الأغراض الاقتصادية والتجارية، حينما يتعلق الأمر ببراءات الاختراع الإلكترونية والحروب التجارية الدولية كما هو الشأن بين الصين والولايات المتحدة الأمريكية، أو بين شركتي آبل وسامسونج وبين شركتي هواوي وآبل.

وعليه، فالأمن السيبراني يتطلب استراتيجية متعددة الأهداف تقوم على التعاون الدولي ولا يجب أن ينحصر على الصعيد الوطني، لأنّ التهديد السيبراني ينعكس بالضرورة على الأمن القومي للدول. فالجريمة السيبرانية (إرهاب، اختراق، قرصنة...إلخ)هي جريمة ذات امتدادات خارجية والعكس صحيح، والفاعل الرقمي في الفضاء السيبراني ليس حكراً على الدول المتطوّرة تكنولوجياً وليس محصوراً في أيدي الأنظمة الاستخباراتية، أو ما يسمى بالجيوش الإلكترونية، مما يتطلب انتهاج استراتيجية وطنية وإقليمية ودولية لمواجهة المخاطر والتهديدات السيبرانية وانعكاساتها على الأمن القومي.

الفرع الثالث: الإرهاب السيبراني

على الرّغم من الاختلاف في تحديد مفهوم الإرهاب، إلاّ أنّ هناك اجتهادات حول تحديد مفهوم الإرهاب السيبراني، حيث عرفته الأمم المتحدة بأنّه: «استخدام الإنترنت لنشر الأعمال الإرهابية». أما مكتب التحقيقات الفدرالي الأمريكي (**F.B.I**) فيعرفه بأنّه: «كل اعتداء قصدي ذي دوافع سياسية على المعلومات، أو النظام المعلوماتي، أو البرامج، أو البيانات ينتج عنه أعمال عنف ضد المدنيين، سواء ارتكبت من قبل مجموعة وطنية أو عملاء غير مرئيين»20. في حين يعرّفه حلف شمال الأطلسي بأنّه: «أي هجوم سيبراني، يستخدم أو يستغل شبكات المعلوماتية أو شبكات الاتصال، لإحداث تدمير كاف لإثارة الرعب وإرهاب مجتمع، لأهداف إيديولوجية»21.

ويعود أصل الربط بين مفهوم الإرهاب والسيبرانية إلى استخدام وسائل ووسائط التكنولوجيا المعلوماتية والاتصالية في تنفيذ أعمال إرهابية تتجاوز تداعياتها الأبعاد المحلية والوطنية لتؤثر بشكل كبير على الأمن القومي والإقليمي والدولي.

ويتضمن الإرهاب الإلكتروني أو الرقمي بهذا المعنى ما يلي22:

أعمال اختراق المواقع وأنظمة المعلومات، وكافة أشكال القرصنة.

نشر الرعب وأشكال التهديد الموجّهة نحو الأفراد أو الدول.

استقطاب الأفراد للانخراط في التنظيمات الإرهابية والجهادية والجريمة عبر الوطنية.

محاولة السيطرة الكاملة على المؤسسات والهياكل الاستراتيجية للدول عن طريق استعمال أسلحة تكنولوجيا المعلومات والاتصالات، أو مواجهة المعلومات من خلال الوسائط الإلكترونية، وهو ما يؤدي في نهاية المطاف إلى شلل هذه الأنظمة.

والإرهاب في الفضاء السيبراني يعد معضلة حقيقية تواجه الدول وتهدّد الأمن والعلاقات الدولية، مما يتطلب حشد الجهود الدولية للحد من انتشاره، بانتهاج سياسات أمنية واستراتيجيات شاملة، وتنسيق إقليمي ومتعدد الأطراف، في ظل الفضاء الإلكتروني المفتوح الذي يتغير كل يوم ويتطوّر في كل لحظة، ويهدّد مباشرة الأمن القومي للدول، من خلال الهجوم على أنظمة صنع القرار والأنظمة الدفاعية للدولة، والسعي للسيطرة على قواعد المعلومات، واستهداف الاتصالات وأنظمة المواصلات والخدمات العامة للمواطنين والدولة.

ولما كان الإرهاب الرقمي يندرج في إطار الحرب الرقمية، التي تعرف من خلال الإجراءات التي يتم اتخاذها بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت ذاته الدفاع عن هذه المعلومات والنظم التي تحتويها، فإنّه يتطلب جهوداً فردية ودولية لمكافحته، حيث خلص التقرير رقم (98 -2013/**A**/**68**) الصادر عن فريق الخبراء الحكومي المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية التابع للجمعية العامة للأمم المتحدة في سياق الأمن الدولي إلى أنّ: " القانون الدولي وبخاصة ميثاق الأمم المتحدة ينطبق على استخدام الدول لتكنولوجيات المعلومات والاتصال، وهو عنصر لابد من المحافظة عليه من أجل حفظ السلام والاستقرار، وتهيئة بيئة تكنولوجية منفتحة ومأمونة23، وهي مسؤولية دولية تنطلق من الوعي بخطورة الظاهرة والآثار الوخيمة التي تهدد استقرار الدول والأمن والسلم الدوليين" .

المبحث الثاني: الاستراتيجية الوطنية والإقليمية والدولية لمواجهة المخاطر والتهديدات السيبرانية

مع كل الصعوبات في تحديد مفهوم الأمن وطرق مواجهة الإجرام السيبراني العابر للحدود الذي تجاوز حدود فكرة القوة العسكرية إلى مفهوم القوة السيبرانية؛ فإنّه ينبغي تعزيز البيئة التشريعية الوطنية والاتفاقية الإقليمية بالآليات اللازمة للردع والمواجهة، وتعاوناً دولياً في نفس مستوى التعاون الدولي لمكافحة الإرهاب والجريمة المنظمة، وهو ما سوف نتطرق إليه من خلال المطلبين التاليين.

المطلب الأول: الاستراتيجية الوطنية لحماية الأمن السيبراني

إن تزايد التهديدات والتحديات المرتبطة بالمجال السيبراني لم يستثن أي دولة تعتمد في أنشطتها الاقتصادية والاجتماعية والثقافية على شبكة الأنترنت، ولرصد ومجابهة المخاطر والتهديدات المستمرة، عمل المغرب على وضع استراتيجية وطنية للأمن السيبراني سنة 2012 للحفاظ على أمنه وبنياته التحتية ومصالحه الاقتصادية والسياسية.

الفرع الأول: أهداف الاستراتيجية المغربية للأمن السيبراني

تهدف الاستراتيجية المغربية للأمن السيبراني إلى تقييم المخاطر للوقاية من التهديدات السيبرانية، وحماية نظم المعلومات والبنيات التحتية.

تقييم المخاطر

يعد الهدف الأساسي للأمن السيبراني في القدرة على مقاومة المخاطر السيبرانية التي تهدد الدولة، وبالتالي التحرر من الخطر أو الأضرار الناجمة عن إساءة استخدام تكنولوجيا المعلومات والاتصالات مما يتطلب حماية الشبكات وأجهزة الكمبيوتر، والبرامج والبيانات من الهجوم أو الضرر أو الوصول غير المصرح به24. كما يشكل ارتباط البنى التحتية الخاصة بتقنيات المعلومات والاتصالات، كما الاعتماد المتزايد عليها، من قبل الدول والأفراد والمؤسسات، عاملا محفزا لتصاعد نسبة المخاطر، ما يفرض اتخاذ تدابير وإجراءات، تضمن إدارة فاعلة للمخاطر التقنية والسيبرانية، تعتمد على منهجية تتناسب والأبعاد الواسعة لهذا الارتباط، ما ينسحب على البلدان أجمع25.

من بين المحاور الأساسية التي جاءت بها الاستراتيجية المغربية للأمن السيبراني نجد تقييم المخاطر بالنسبة لنظم المعلومات الخاصة بالإدارات والمؤسسات الحكومية والبنيات التحتية ذات الأهمية، والشك إن هذا الأمر يتطلب التنفيذ المنسجم والفعال للأنظمة الآمنة داخل الدولة من خلال تبني مناهج تحليل المخاطر والسياسات ومعايير أمنية متجانسة. وقد تم تحديد برنامجين أساسين لتنفيذ هذا المحور وهما:

وضع خطط لتقييم المخاطر والتهديدات من خلال تحديد شبكة تقييم لدرجة أهمية نظم المعلومات للإدارات والمؤسسات العمومية والبنيات التحتية الحيوية وإحصاء وتعريف وتصنيف هذه الأنظمة، وإجراء تقييم دوري لمستوى الخطر التي قد تتعرض لها وكذا تقييم مخططات تدبير المخاطر التي تتبناها هذه الإدارات والمؤسسات العمومية والبنيات التحتية الحيوية.

وضع الأدوات الضرورية للمساعدة في اتخاذ القرار وذلك بالقيام بتحقيقات لجمع بيانات ذات طبيعة قانونية وتقنية وإجرائية التي لها علاقة بنظم المعلومات، وكذا إنتاج البيانات الإحصائية ومؤشرات المراقبة، ثم ضمان المراقبة التكنولوجية والقانونية والتنظيمية26.

إن التقييم الدوري للمخاطر المرتبطة بالنظم تحتاج إلى تحديد طبيعة المخاطر التي يشكلها التهديد المتوقع والثغرات الموجودة. وهذا الأمر يحتاج إلى فهم التهديدات وتحديد أولوياتها ومعالجتها27، ويمكن لعملية وضع نماذج للتهديدات أن تمثل وسيلة مفيدة لتعيين البنية التحتية المعلوماتية المهمة وحمايتها. ذلك لأنها تنظر إلى البنية التحتية 3من وجهة نظر المهاجم لتحديد أسباب التهديد المرجح استخدامه وأهدافه المحتملة28.

إن خطة الاستجابة للحوادث السيبرانية تستلزم مراقبة تدفقات المعلومات المدخلة والمخرجة. فمن المهم تحديد الحادث في أقرب وقت ممكن من خلال إضفاء الطابع الرسمي على التعامل مع الحوادث انطلاقا من الكشف إلى المعالجة29. وهذا الأمر يتطلب إنشاء مركز للاستجابة السريعة لطوارئ الحاسوب، الذي يشكل الأداة الأساسية لحماية البنية الأساسية الحساسة للمعلومات. ومن مهامه العمل بسرعة على رصد المخاطر المعلوماتية المستجدة، مثل الفيروسات والديدان وبرامج التجسس ومكامن الضعف في الأنظمة التشغيلية، والتعامل معها، وإعطاء الحلول والتدابير اللازمة بشأنها، ونشر المخاطر المعلوماتية على موقعه على الأنترنت، وإطلاق حملات إعلامية عنها، وتحذير المواطنين منها، وإعطائهم الإرشادات والتوجيهات حول سبل حماية أنظمتهم المعلوماتية وبياناتهم، وتنفيذ برامج توعية شاملة للمواطنين30.

وفي هذا الإطار تم إحداث مركز اليقظة والرصد والتصدي للهجمات المعلوماتية بالمغرب سنة 2011 التابع للمديرية العامة لأمن نظم المعلومات بإدارة الدفاع الوطني، وعهد إلى هذا المركز القيام بالمراقبة والكشف والرد على الهجمات السيبرانية.

حماية أمن نظم المعلومات والبنيات التحتية

عند ذكر كلمة أمن المعلومات وجرائم الحاسوب، فإن ما يتبادر إلى الذهن هو كشف معلومات كان يجب أن تبقى سرا، والحقيقة أن الحفاظ على سرية المعلومات لا يعدو أن يكون جانبا واحدا من جوانب الأمن المعلوماتي، فهذا الأخير يتحقق إذا تم الحفاظ على ثالثة عناصر رئيسة، وهي:

سرية المعلومات. (**confidentialité**)

سلامة المعلومات من التعديل من قبل أشخاص غير مصرح لهم بذلك.(**intégrité**)

إتاحة المعلومات بمعنى حماية المعلومات من الفقدان أو التلف. (**availability**)

وارتباطا بهذا فقد فصل المشرع المغربي بين "نظام معلومات" و"نظام معلومات حساس"، وأفرد لكل واحد منهما تعريفا خاصا، إذ عرف "نظام المعلومات" بأنه مجموعة منظمة من الموارد كالمستخدمين والمعدات والبرامج والمعطيات والإجراءات التي تسمح بتجميع المعلومة في بيئة معينة وتصنيفها ومعالجتها ونشرها. في حين عرف "نظام معلومات حساس" بأنه نظام معلومات يعالج معلومات ومعطيات حساسة من شأن المساس بسريتها أو بسلامة محتواها أو بتوافرها أن يلحق ضررا بهيئة ما أو ببنية تحتية ذات أهمية حيوية**31**.

من المعلوم أن غالبية الوزارات وغيرها من المؤسسات العمومية في المغرب تتوفر اليوم على نظم معلوماتية تتيح لها تقديم جزء من خدماتها على الخط. إلا أن نظم المعلوميات هذه غالبا ما تكون هدفا لهجمات مغرضة غالبا ما يتم توجيهها من الخارج من قبل أجهزة المخابرات أو الجماعات الإرهابية. ومن بين أهم المعلومات الحساسة التي

تتعرض لهجمات سيبرانية من الخارج نجد المعطيات ذات الطابع الشخص ي والأسرار الصناعية. وبطبيعة الحال، فإن الجرائم التي تقع على نظم المعلومات الحساسة تكون لها قطعا تأثيرات سلبية على ثقة المواطنين والمؤسسات في الدول32.

لحماية نظم المعلومات حدد المغرب في استراتيجيته33 للأمن السيبراني ثلاثة برامج تتمحور حول:

إعداد المرجعيات والمعايير الوطنية لنظم المعلومات.

تأمين أمن نظام المعلومات للإدارات والهيئات العمومية والبنى التحتية ذات الأهمية الحيوية.

تعزيز هياكل لليقظة والكشف والاستجابة لحوادث أمن المعلومات.

وقد أصبح المغرب شأنه شأن أغلب دول العالم يعتمد أكثر فأكثر على الفضاء الإلكتروني(**Cyberspace**) لاسيما في البنى التحتية المعلوماتية العسكرية والمصرفية والحكومية، إضافة إلى المؤسسات والشركات العامة والخاصة. ولاشك أن ازدياد الهجمات الإلكترونية والتي نشهدها اليوم يرتبط أيضا بازدياد هذا الاعتماد على شبكات الكومبيوتر والأنترنيت في البنية التحتية الوطنية الأساسية، وهو ما يعني إمكانية تطور الهجمات الإلكترونية اليوم لتصبح سالحا حاسما في النزاعات بين الدول في المستقبل، علما أن أبعاد مفهوم الحرب الإلكترونية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين وحتى العامة34.

ويروم المغرب في استراتيجيته لحماية نظم المعلومات والبنيات تحتية ذات أهمية حيوية، التي حددها المشرع في التجهيزات والمنشآت والأنظمة الضرورية للحفاظ على استمرارية الوظائف الحيوية للمجتمع والصحة وألأمن والسلامة والتقدم الاقتصادي أو الاجتماعي35، إلى مواجهة المخاطر السيبرانية وتعزيز الثقة في البنيات التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في شتي المجالات الحيوية من خلال تأمينها من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المغربي بمختلف أطيافه.

الفرع الثاني: آليات تنفيذ الاستراتيجية الوطنية للأمن السيبراني

تستلزم الأهداف المرسومة للاستراتيجية المغربية للأمن السيبراني إيجاد وسائل ضرورية لتحقيقها من خلال تعزيز القدرات الوطنية والتعاون الوطني والدولي.

أولا: تعزيز القدرات الوطنية في مجال الأمن السيبراني

من أجل تحقيق الأهداف المرسومة الاستراتيجية الأمن السيبراني يعمل المغرب على تعزيز القدرات الوطنية في هذا المجال بشكل منسجم ومتكامل من أجل التصدي والتخفيف من المخاطر السيبرانية وذلك عبر الوسائل التالية:

الإطار القانوني

يعتبر الإطار القانوني والتنظيمي حاجة ملحة، نظرا لكونه عاملا مؤسسا لعنصر الثقة، ليس فقط في دعم الاستثمار وتقديم نوعية أفضل من الخدمات بكلفة وأسعار تنافسية، وإنما أيضا في إرساء أسس ثقة المواطن في مجتمع المعلومات، وذلك انطلاقا من أن القانون هو ضمانة الحقوق والحريات36.

إن استراتيجية المغرب للأمن السيبراني، شأنها شأن الدول ألاخرى، لم تغفل مسألة تأهيل الإطار التشريعي والتنظيمي في هذا المجال، وهذا الأمر بدأ حتى قبل أن يتم وضع هذه الاستراتيجية وبالضبط سنة 2003 مع إصدار القانون رقم 07.03 بتتميم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات37. وهذا القانون ملأ الفراغ التشريعي بشأن الأنشطة المعلوماتية، والذي سمح لأول مرة بمعاقبة الدخول الاحتيالي إلى نظام للمعالجة الآلية للمعطيات.

وفي سنة 2009 تم إصدار القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي38، الذي يهدف إلى حماية الأشخاص الذاتيين ضد الانتهاكات أثناء هذه المعالجة، كما أحدث هذا القانون اللجنة الوطنية مراقبة حماية المعطيات ذات الطابع الشخصي، التي عهد إليها المشرع إعمال أحكام ما جاء به هذا القانون ونصوصه التطبيقية، من قبيل تلقي الشكايات، والإدلاء بالآراء القانونية ذات الصلة بمعالجة المعطيات ذات الطابع الشخصي، وتسليم الأذون الضرورية39.

وتبقى أقوى نقلة تشريعية في مجال الأمن السيبراني هو إصدار القانون رقم 05.20 المتعلق بالأمن السيبراني40 عام 2020، الذي حدد:

قواعد ومقتضيات الأمن المطبقة على نظم معلومات إدارات الدولة والجماعات الترابية والمؤسسات والمقاولات العمومية، وعلى البنيات التحتية ذات الأهمية الحيوية وعلى مستغلي الشبكات العامة للمواصلات ومزودي خدمات الأنترنت ومقدمي خدمات الأمن السيبراني ومقدمي الخدمات الرقمية وناشري منصات الأنترنت.

الإطار الوطني لحكامة الأمن السيبراني؛

إطار التعاون وتبادل المعلومات بين السلطة الوطنية للأمن السيبراني 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 لاسيما في ما يتعلق بتطوير الخبرة الوطنية والتحسيس في مجال الأمن السيبراني لفائدة الهيئات والفاعلين في القطاع الخاص والأفراد، وتقوية التعاون مع المؤسسات الوطنية والأجنبية.

إن تطبيق هذا القانون يتوقف على مدى إصدار النص أو النصوص التنظيمية المتعلقة أساسا بتحديد الدليل المرجعي لتصنيف أصول المعلومات ونظم المعلومات الواردة في المواد 4 و5 من هذا القانون فيما يخص وضع وتنفيذ سياسة ألمن نظم المعلومات لكل هيئة معنية وتحديد المخاطر التي تهدد أمن نظم معلوماتها واتخاذ الإجراءات التقنية والتنظيمية اللازمة لإدارة هذه المخاطر. ثم تصنيف أصولها المعلوماتية ونظم معلوماتها حسب مستوى حساسيتها من حيث السرية والتمامية والتوافر وكذا تحديد إجراءات تأهيل الأشخاص الذين يمكنهم الولوج إلى المعلومات المصنفة وشروط معالجة هذه المعلومات أو تبادلها أو تخزينها أو نقلها. هذا بالإضافة إلى ما جاءت به المادة 6 حول تعيين الهيئة المعنية للمسؤول عن أمن نظم المعلومات يتولى السهر على تطبيق سياسة أمن نظم المعلومات. وإجمالا فإن المواد التي أحالت على النص التنظيمي بلغت 14 مادة من أصل 53 مادة التي جاء بها القانون المذكور.

التكوين

أوردت الاستراتيجية المغربية للأمن السيبراني تحديد خصوصيات الكفاءة المناسبة في مجال الأمن السيبراني، وتنظيم دورات تكوينية لفائدة مستخدمي الهيئات والبنيات التحتية ذات الأهمية الحيوية من أجل تعزيز القدرات الوطنية في هذا المجال41.

التحسيس

من خلال تحديد وتنفيذ برامج تحسيسية بشأن الأخلاقيات السيبرانية والتحديات المتعلقة بتهديدات ومخاطر الأمن السيبراني لفائدة مستخدمي الهيئات والبنيات التحتية ذات الأهمية الحيوية والقطاع الخاص والأفراد، خاصة الأطفال ومستعملي شبكات الانترنت42.

دعم البحث العلمي في مجال الأمن السيبراني

تهدف هذه الآلية إلى ضمان الاستقلالية العلمية والتقنية، ولن يتأتى ذلك إلا من خلال تشجيع تطوير الحلول الوطنية في مجال الأمن المعلوماتي، سواء تعلق الأمر بالبحث الجامعي أو ما يقدمه الخبراء الوطنيين أو الدوليين الذين يمكنهم القيام بمساعدة لحل المشاكل المرتبطة بالأمن السيبراني43.

المطلب الثاني: التعاون الدولي في مجال الأمن السيبراني

إن المجال السيبراني وما ينتج عنه من تهديدات على موازين القوى الدولية، يحتم على المجتمع الدولي التعاون والتنسيق من أجل الحد من هذه المخاطر والتهديدات، وتأمين حقوق الأفراد والمصالح الاستراتيجية للدول. وهذا التعاون ينبغي أن يتم على المستويين الإقليمي والدولي.

الفرع الأول: على المستوى العربي

راهنت الدول العربية في مسعاها لضمان أمنها القومي على اعتماد الأمن السيبراني وتعزيز القدرات الدفاعية الإلكترونية كمرتكز أساسي لضمان أمنها الداخلي والإقليمي، وفي هذا الصدد تم على مستوى جامعة الدول العربية تبني اتفاقية تهدف إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات44 لدرء أخطار هذه الجرائم، حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها، وضماناً للحفاظ على القوى الوطنية والعربية من أي اعتداءات أو اختراقات إلكترونية، والإسهام في حفظ الثروات الإنسانية والمالية والتقنية والمعلوماتية للمؤسسات الحكومية والخاصة والأفراد من الهجمات والقرصنة الإلكترونية، بالإضافة إلى تأمين حماية البيانات والبُنى التحتية ضد أي هجوم إلكتروني أو اختراقات، مما يقتضي وضع آليات قانونية وتشريعية تضمن الاستخدام السيبراني الآمن.

وفي هذا الصدد شددت الاتفاقية العربية لبناء الثقة في مجال الأمن السيبراني **45** على ضرورة تعزيز التعاون العربي البيني والدولي، حيث نصت المادة (**13**) منها على ضرورة تعاون الدول الأعضاء، مع الهيئات الدولية والإقليمية، المتخصصة في قضايا حماية الفضاء السيبراني، لاسيما اللجان التابعة للأمم المتحدة، والاتحاد الدولي للاتصالات، والآيكان(هيئة الإنترنت للأسماء والأرقام)، وجامعة الدول العربية، وهيئات الاتحاد الأوروبي، ومجموعة دول الكومنولث، ومنظمة التعاون والتنمية الاقتصادية، وأي هيئة دولية أخرى ذات اختصاص وصلة بمسائل الأمن السيبراني، كما نصت المادة(**14**) على ضرورة تعاون الدول العربية الأعضاء، لحماية الفضاء السيبراني، والخدمات الإلكترونية، في منع ومكافحة الجرائم السيبرانية، طبقاً للقوانين والإجراءات الداخلية لكل دولة منها، من خلال الآتي:

تبادل المعلومات المتعلّقة بأنشطة وجرائم الجماعات التي تنظّم الاعتداءات والهجمات على الأنظمة المعلوماتية والبُنى التحية للاتصالات والمعلومات والمواقع الإلكترونية، وتتبُّع مواقعها ووسائل اتصالاتها ودعاياتها المستخدمة.

التحرّيات وتقديم المساعدة في مجال القبض على الهاربين من المتهمين أو المحكوم عليهم بجرائم سيبرانية وفقاً لقانون وأنظمة كل دولة.

تبادل الخبرات والدراسات والبحوث وتوفير المساعدات الفنّية المتاحة لإعداد برامج ودورات تدريبية مشتركة خاصة بكل دولة، أو بين الدول المتعاقدة للعاملين في مجال مكافحة الجرائم السيبرانية لرفع مستوى أدائهم.

الفرع الثاني: على الصعيد الدولي

من الواضح أن هناك صعوبة في وضع تعريف موحد للحرب السيبرانية، الشيء الذي يحد من جهود المنظمات الدولية والمراكز البحثية لوضع الآليات الناجعة لمواجهة هذا التهديد، على الرغم من وجود بعض الدلائل مثل الهجمات السيبرانية التي تستهدف المصالح الحيوية(المنشآت النووية، والعسكرية) لبعض الدول، على غرار ما حصل

في كل من إستونيا وجورجيا والعراق وإيران46. ذلك أنّ ثغرات الأمن والدفاع أصبحت من الأزمات الدائمة التي لم تجد طريقها إلى الحل في كبرى الدول رغم الإمكانيات المادية والبشرية والتقنية التي تتمتع بها، ذلك أن الفجوة تكمن في عدم احترام لقواعد حماية الأنظمة المعلوماتية من طرف المستخدمين؛ لذا نجد أنّ أنظمة الأمن والدفاع كثيراً ما تقف عاجزة أمام الاختراقات47. كما حذر خبراء في أمن المعلومات48 من خطورة الاستمرار في تطوير الأسلحة السيبرانية.

وفي هذا الإطار، هناك العديد من الجهود الدولية والتنسيق المشترك لمكافحة الجرائم السيبرانية، من بينها:

اتفاقية بودابست لمكافحة الجريمة المعلوماتية

تعد اتفاقية بودابست إحدى أهم الاتفاقيات في مجال التعاون الدولي لمكافحة الإجرام السيبراني، حيث اعتمدت هذه الاتفاقية مصطلح جرائم الإنترنت على نطاق واسع49، وهي ترمي بشكل أساسي إلى مواءمة عناصر القانون الموضوعي الجنائي المحلي والأحكام المتصلة بالجرائم في مجال الجريمة الإلكترونية، والتنصيص على صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم، ومتابعتها قضائياً، علاوة على الجرائم الأخرى التي ترتكب عن طريق الكمبيوتر، أو التي تكون الأدلة المتصلة بها في شكل إلكتروني، وإلى إنشاء نظام سريع وفعّال للتعاون الدولي، وهي بمثابة صك دولي ملزم بشأن هذه المسألة، أو مبدأ توجيهي لأي بلد لوضع تشريع وطني شامل لمكافحة جرائم الإنترنت، وإطار للتعاون الدولي بين الدول الأطراف في هذه الاتفاقية50. وقد تضمنت هذه الاتفاقية مجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في مجال الشؤون الجنائية، وحدّدت الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول في غياب الاتفاقيات الدولية51، وقد وقّعت على هذه الاتفاقية **30** دولة، ولأهمية هذه الاتفاقية انضمَّ إليها العديد من الدول من خارج المجلس الأوروبي، وأبرز هذه الدول الولايات المتحدة الأمريكية، التي صادقت عليها في **22** سبتمبر **2006** ، ودخلت حيّز النفاذ في الأول من يناير522007، وتهدف الاتفاقية إلى التالي53:

توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

توفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة إلكترونياً بواسطة الكمبيوتر.

تعيين نظام سريع وفعّال للتعاون الدولي.

الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.

مجموعة الدول الثماني**G8**

اعتمد وزراء العدل والداخلية التابعين لبلدان ال **G8** وهي: (الولايات المتحدة الأمريكية، اليابان ألمانيا، روسيا الاتحادية، إيطاليا، المملكة المتحدة، فرنسا، وكندا) في اجتماعاتهم المختلفة، سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى المبادئ التالية:

عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات.

التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت، ومحاكمتهم بغض النظر عن مكان حدوث الضرر.

تدريب الموظفين المكلفين بتنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية.

بالإضافة لذلك، دعت هذه الدول إلى مواصلة العمل حتى يتم التوصل إلى حلول دولية ناجعة، حيث تبنت في هذا الإطار عدة مبادئ وتوصيات من أبرزها:

مبادئ وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر **1997**.

مبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول**1999**.

توصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية**2002**.

مبادئ توافر البيانات الأساسية لحماية السلامة العامة **2002**، وإعلان بيان دول مجموعة الثمانية فيما يتعلق بحماية نظم المعلومات **2002**، ناهيك عن مجموعة من البروتوكولات والإعلانات الدولية، نذكر منها على سبيل المثال لا الحصر: إعلان فيينا لسنة 2000، وإعلان بانكوك لسنة**2005** ، وبروتوكول ستراسبورغ لسنة **2003** .

الخاتمة:

في خضم التحولات الدولية الراهنة وما نتج عنها من تغيرات في موازين القوى الدولية، أصبح من الضروري إعادة النظر في خارطة المفاهيم الجيو-سياسية والاستراتيجية تأخذ بعين الاعتبار التحولات الحاصلة في موازين القوى الدولية بين الدول القوية صاحبة الريادة في مجال تكنولوجيا الاتصال والمعلومات من أجل تأمين مصالحها الوطنية والاقتصادية وضمان أمنها القومي؛ الأمر الذي أدى إلى إعادة النظر في كثير من المفاهيم التقليدية(الأمن والقوة والحرب والصراع والسيادة)، حيث طرحت الدراسات الاستراتيجية والأمنية الجديدة نمطاً جديداً من الحروب لا مكان فيه للمفاهيم التقليدية، وأشكالا جديدة من النظم الدفاعية الأمنية يحتل فيها المجال الرقمي الأهمية القصوى فيما يسمى بالدفاع السيبراني وتأثيراته على مفاهيم السيادة السيبرانية، في ظل فضاء رقمي مفتوح وغير آمن متعدد المخاطر والتهديدات الأمنية. كما طرح هذا الوضع أشكالاً جديدة من الصراعات الدولية والإقليمية ساهمت فيها الثورة الرقمية بشكل واضح في تغيير موازين القوى بين الدول، معتمدة في ذلك على استراتيجيات أمنية ودفاعية قوية في حروبها المعلوماتية تحت غطاء" البقاء لمن يحسن استخدام تكنولوجيا المعلومات والاتصالات، ويوظفها لخدمة أهدافه الدفاعية أو الهجومية".

وعليه، ونتيجة للتطور المتسارع في المجال الرقمي والصراع على الفضاء السيبراني، تغيرت العديد من المفاهيم التقليدية السائدة، بحيث لم تعد القوة العسكرية وحدها كافية لضمان الأمن القومي نتيجة امتلاك منظمات وكيانات مجهولة مكانا في هذا الفضاء مما مكن من بروز التهديدات والجرائم السيبرانية، الشيء الذي يتطلب معه تعزيز آليات المواجهة من خلال التنسيق الاستراتيجي الأمني بين الدول، وتكثيف الجهود التشريعية للحد من المخاطر والتهديدات السيبرانية التي أصبحت أكثر فتكا وتدميرا من الحروب التقليدية.

الهوامش:

1- يوسف بوغارة، الأمن السيبراني :الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، برلين، ألمانيا، المجلد1 ، العدد3 ، سبتمبر 2018 ، ص: 106 .

2 -Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science, 2003, p.3.

3 -Edward Amoroso, Cyber Security, Silicon Press, 2007, p.1.

4 -ITU, Cyber security, Geneva: International Telecommunication Union (ITU), 2008.

5 – جمال بوازدية، الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية – التحديات والآفاق المستقبلية، مجلة العلوم القانونية والسياسية، جامعة الوادي، الجزائر، المجلد 10 ، العدد1 ، أفريل/أبريل 2019 ، ص : 1266 .

6 – عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية :دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تمنراست، الجزائر، المجلد9 ، العدد3 ، سنة 2020 ، ص: 149.

7 – نبيل إدريس، الجريمة السيبرانية بين المفاهيم والنصوص التشريعية – الجزائر نموذجاً، مجلة القانون والمجتمع، جامعة أحمد دراية، أدرار، الجزائر، المجلد 5، العدد2 ، سنة 2007 ، ص : 30.

8 – القانون رقم 07.03 المتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات الصادر بتنفيذه الظهير الشريف رقم 197.03.1 بتاريخ 26 رمضان 1424 الموافق 11 نوفمبر 2003، المنشور بالجريدة الرسمية عدد 5171 بتاريخ 27 شوال 1424 الموافق 22 ديسمبر 2003، ص: 4284.

9 – منى الأشقر جبور، الأمن السيبراني :التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الندوة الأولى للمختصين في أمن وسلامة الفضاء السيبراني، بيروت، 28 / 27 أغسطس 2012 ، ص : 4.

10 – محمد مختار، هل يمكن أن تتجنب الدول مخاطر الهجمات الإلكترونية، مجلة اتجاهات الأحداث، مركز المستقبل للأبحاث والدراسات المتقدمة، العدد6 ، جانفي /يناير 2015 ، ص: 5-6.

11 - Dorothy E. Denning, Cyber terrorism, Global Dialogue, Autumn, 2000, p.1, Available at: https://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf

12 - Kevin Coleman, Russia's Cyber Forces, Available at:
https://www.military.com/defensetech/2022/11/17/russias-cyber-forces.

13 – حمدون إ .توريه، الاستجابة الدولية للحرب السيبرانية :البحث عن السلام السيبراني، الاتحاد الدولي للاتصالات، يناير 2011 ، ص – 79
. 80تاريخ الزيارة 2022 /11 / 17 : متاح على الرابط الآتي:
https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-A.pdf

14 - Gregory Asmolov, "Russia: New Military Doctrine and Information Security": Global Voices

تاريخ الزيارة 2022/11/17، متاح على الرابط الآتي:
https://globalvoices.org/2010/02/23/russian-military-doctrine/

15– فتيحة ليتيم ونادية ليتيم، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، جامعة محمد خيضر، بسكرة، الجزائر، المجلد 10 العدد 12 ، سنة 2015 ، ص: 242.

16 – سالم مدني، مدى إمكانية تطبيق الحدود على الجرائم الإلكترونية، ورقة عمل مقدمة إلى ندوة المجتمع والأمن : الجرائم الإلكترونية الملامح والأبعاد، الرياض،2007 ، ص: 516.

17 – الفصل 23 من دستور 2011.

18 -
https://www.droitetentreprise.com/%d8%a7%d9%84%d8%ad%d9%85%d8%a7%d9%8a%d8%a9-%d8%a7%d9%84%d9%82%d8%a7%d9%86%d9%88%d9%86%d9%8a%d8%a9-%d9%84%d8%ad%d9%82%d9%88%d9%82-%d8%a7%d9%84%d9%85%d8%a4%d9%84%d9%81-%d9%81%d9%8a-%d8%a7%d9%84%d9%86/

19 – أنيس العذار، مكافحة الجريمة الإلكترونية، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمن ميرة، بجاية، الجزائر، المجلد 17 ، العدد1 ، سنة 2018 ، ص : 430-727 .

20 – إسحاق العشعاش، الإرهاب السيبراني وتحديات الدول :دراسة مقارنة مع الاتفاقيات الدولية، مجلة بحوث، جامعة بن يوسف بن خدة، الجزائر، المجلد 12 ، العدد1 ، سنة 2018 ، ص: 178 .

21 -NATO Glossary of Terms and Definitions, AAP-06 Edition 2012Version 2. (NATO) defines terrorism as "the unlawful use Or, threatened use of force or violence against individuals or property tocoerce or intimidate governments or societies to achieve political, religious or ideological objectives".

https://ccdcoe.org/cyberdefinitions.html. Accessed on: 30/12/2022.

22 – حكيم غريب، الإرهاب السيبراني والأمن الدولي :التهديدات العالمية الجديدة وأساليب المواجهة، المجلة الجزائرية للدراسات السياسية، المدرسة الوطنية العليا للعلوم السياسية، الجزائر، المجلد5 ، العدد2 ، سنة 2018 ، ص : 106 .

23 – إسحاق العشعاش، مرجع سابق، ص :192.

24 – أميرة عبد العظيم محمد عبد الجواد: المخاطر السيبرانية وسبل مواجهتها في القانون الدولي، مجلة الشريعة والقانون، العدد 35، الجزء الثالث 2020 ص، 437-438.

25 – منى الأشقر جبور: السيبرانية هاجس العصر، المرجع السابق، ص: 165.

26 -Stratégie nationale en matière de cyber sécurité: Administration de la défense Nationale, p: 12, Voir le lien suivant: https://www.dgssi.gov.ma/sites/default/files/attached_files/strategie_nationale.pdf

27 -Référentiel de gestion des incidents de cyber sécurité : : Administration de la défense Nationale, édition 2017, p : 6. Voir le lien suivant : https://www.dgssi.gov.ma/sites/default/files/attached_files/referentiel_de_gestion_des_incidents_de_
Cyber sécurite.pdf

28 – المبادئ التوجيهية المتعلقة بأمن البنية التحتية للأنترنت في الدول العربية، المرجع السابق، ص: 25.

29 -Ali El Azzouzi: les enjeux cybersécurité au Maroc, livre blanc, DATAPROTECT/AUSIM, Septembre 2018, P: 26.

30 – تقرير صادر عن اللجنة الاقتصادية والاجتماعية لغربي آسيا حول "الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية"، الأمم المتحدة 2015، ص:21.

31 – القانون رقم 05.20 يتعلق بالأمن السيبراني، الجريدة الرسمية عدد 6904 بتاريخ 30 يوليوز 2020 ،ص: 4160.

32 – فؤاد بصغير: الأمن السيبراني بالمغرب، مقال نشر على الرابط التالي:
https://www.hespress.com/517499-الامن-السيبراني-في-المغرب؟. html

33 -Stratégie nationale en matière de cybersécurité : Administration de la défense Nationale, p : 12-13. Voir le lien suivant : https://www.dgssi.gov.ma/sites/default/files/attached_files/strategie_nationale.pdf

34 – فيصل محمد عبد الغفار: الحرب الإلكترونية، الجنادرية للنشر والتوزيع، الطبعة الأولى 2016،ص: 9.

35 – القانون رقم 05.20 (المرجع السابق).

36 – منى الأشقر جبور: السيبرانية هاجس العصر، المرجع السابق، ص: 18.

37 – ظهير شريف رقم 1.03.197 صادر في 16 من رمضان 1424(11 نوفمبر 2003) بتنفيذ القانون رقم 07.03 بتتميم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، الجريدة الرسمية عدد 5171 بتاريخ 22 ديسمبر 2003.

38 – ظهير شريف رقم 1.09.15 صادر في 22 من صفر 1430 (18 فبراير 2009) بتنفيذ القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه المعالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية عدد 5711 بتاريخ 23 فبراير 2009.

39 -Ali El Azzouzi : les enjeux cybersécurité au Maroc, Op. Cit, P : 10.

40 – ظهير شريف رقم 1.20.69 صادر في 04 ذي الحجة 1441(25 يوليو 2020) بتنفيذ القانون رقم 05.20 المتعلق بالأمن السيبراني، الجريدة الرسمية عدد 6909 بتاريخ 17 أغسطس 2020.

41 -Stratégie nationale en matière de cybersécurité, Op. Cit, P: 15.

42 -op.cit, P: 15

43 -op.cit, P: 15.

44 – الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، جامعة الدول العربية، مجلس وزراء العدل العرب، القاهرة، 2010 / 12 / 21 ، والتي وافق عليها المغرب بموجب القانون رقم 75.12 بتاريخ 2012/12/18.

45 – الاتفاقية العربية لحماية الفضاء السيبراني بين الواقع والطموح، جامعة الدول العربية، مجلس وزراء العدل العرب، بيروت، 23 – 25 يوليوز 2018.

46– جمال بوازدية، مرجع سابق، ص. 1272 .

47– عبد الله بن عبد العزيز بن فهد العجلان، الإرهاب الإلكتروني في عصر المعلومات، المؤتمر الدولي الأول حول حماية المعلومات والخصوصية في قانون الإنترنت، القاهرة، 4 -2 جوان/يونيو 2008.

48 – منهم الخبير الروسي يوجين كاسبرسكي Eugene Kaspersky المدير العام لشركة كاسبرسكي لاب Kaspersky Lab المتخصصة في مجال أمن الحواسيب، الذي حذّر من أنّ استمرار تطوير الأسلحة السيبرانية وانتشارها Cyber Weapons من شأنه أن يغيّر وجه العالم الذي نعرفه، وأنّ البنية التحتية للعالم ليست مستعدة بعد لحماية نفسها من مثل هذه الأسلحة .مشار إليه لدى :ربيع محمد يحي، إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط :دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الإنترنت2002-2013، ، ص 77 ، تاريخ الاطلاع :2023/03/15 متاح على الرابط الآتي:

http://strategicvisions.ecssr.com/ECSSR/ECSSR_DOCDATA_PRO_EN/Resources/P

49- Jan-Jaap Oerlemans, Investigating cybercrime, Doctoral Thesis, Leiden University, Netherlands, 2017, p. 20, Available at :https://scholarlypublications.universiteitleiden.nl/handle/1887/44879.

50-Cybercrime-Budapest Convention and related standards-Council of Europe 17.1.2017, Available at: http://www.coe.int/en/web/cybercrime/the-budapest-convention.

51 – عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الإلكترونية، ط1 ، المركز القومي للإصدارات القانونية، القاهرة، 2012 ، ص8 .

52 – ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، مجلة الحوار المتمدن، العدد 34 ، سنة 2017 ، ص 24 – 23 ، تاريخ الاطلاع :2023/05/11 ، متاح على الرابط الآتي :

http://www.ahewar.org/debat/show.art.asp?aid=571423&r=0

53 – جورج لبكي، المعاهدات الدولية للإنترنت، مجلة الدفاع الوطني اللبناني، بيروت، العدد 83 ، كانون الثاني/يناير 2013، تاريخ الاطلاع: 2023/05/11، متاح على الرابط الآتي:

https://www.lebarmy.gov.lb/ar/content/%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%87%D8%AF%D8%A7%D8%AA-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9%D9%84%D9%84%D8%A5%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AD%D9%82%D8%A7%D8%A6%D9%82-%D9%88%D8%AA%D8%AD%D8%AF%D9%91%D9%8A%D8%A7%D8%AA