الآليات القانونية لمواجهة تحديات الفضاء السيبراني- الجزائر انموذجا –

Legal mechanisms to confront the challenges of cyberspace - Algeria as a model -

عدان نبيلة

كلية العلوم السياسية والعلاقات الدولية - جامعة الجزائر3 –

addane.nabila@yahoo.com

تاريخ الاستلام: 14 /2012/03 تاريخ القبول: 2012/06/23

ملخص: شهدت البشرية وعلى مر العصور تطورات معرفية وتقنية هائلة خاصة مع امتداد العولمة وانعكاساتها أين أصبحت التهديدات الرقمية سمة الألفية الجديدة، الأمر الذي وضع سيادة الدول على محك حقيقي لمواجهة تحديات العصر الرقمي، أين أصبحت الحروب القائمة على المواجهة المباشرة بقوة السلاح طرازا تقليديا، وتحولنا نحو استعمار رقمي تقوده قوة ناعمة تهدد وتداعب حدود الدول بنقرة زر، لدرجة أصبح فيها الأمن السيبراني متطلبا أساسيا لبناء منظومة دفاعية معاصرة في مواجهة التهديدات التي تتربص بأمن وسلامة الدول.

والجزائر على غرار الدول التي قررت التوجه نحو حكومة الكترونية وأتمتة العمل الإداري، وهو ما يشكل تحديا آخر يقع على عاتق الدولة الجزائرية لما يمثله من خطر محدق على الأمن الداخلي ويهدد زعزعة استقرارها خاصة في ظل تصاعد موجات الإرهاب السيبراني، الجريمة السيبرانية وغيرها من تحديات الفضاء السيبراني. وعلى هذا الأساس تسعى هذه الدراسة للوقوف على أهم التهديدات السيبرانية التي تواجهها الجزائر، والتعرف على الاستراتيجيات المتبعة والتشريعات المنتهجة للتصدي لمثل هذه الانتهاكات التي تمس بأمنها وتتعدى على سيادتها.

الكلمات المفتاحية: الفضاء السيبراني، الأمن السيبراني، التهديدات السيبرانية، الجزائر

Abstract: Throughout the ages, humankind has witnessed great knowledge and technological developments, especially with the spread of globalization and its implications, where digital threats have become the characteristic of the new millennium. This evolution put the sovereignty of states face to a new challenge, a war no more based on direct confrontation with armed forces (traditional model) but focused on a "digital colonization" led by soft power that threatens countries' borders at the click of a button, to the extent that cyber security is a prerequisite for building a modern defense system in the face of threats that ambush the states' security and safety.

Algeria is one of many countries that have decided to move towards an electronic government and the automation of administrative work, which pose another challenge for the Algerian state because of its imminent threat to internal security (cyber terrorism, cybercrime and other cyberspace challenges). On this basis, this study seeks to identify the most important cyber threats faced by Algeria, and to identify the strategies and the legislation adopted to address such violations that affect Algerian security and sovereignty.

Keywords: Algeria ,Cyber Space, Cyber Security, Cyber Threats,

*المؤلف المرسل

مقدمة:

يشهد عصرنا الحالي تطورا متزايدا في استخدام تكنولوجيا المعلومات والاتصالات التي أصبحت الدعامة الأساسية لأي مجتمع من المجتمعات نتيجة اتساع وتنوع الخدمات الالكترونية والتي يعتبر الفضاء السيبراني موطنا لها وأساسا لاستمرار عملها، ولأن تكنولوجيا المعلومات والاتصال أضحت متطلبا من متطلبات بناء مجتمع المعرفة الذي تضطلع أمم اليوم للوصول إليه، والقائم على اقتصاد المعرفة، الطفرة التكنولوجية، التنوع، الاستثمار في الرأسمال البشري والإبداع.

ولأجل إرساء مجتمع آمن ومحمي أدركت الدول والحكومات سواء كانت متقدمة أم نامية أهمية بناء قاعدة تشريعية وتهيئة الأطر القانونية لحماية مثل هذه التحولات السيبرانية، والتي بقدر ما تشكل فرصة للدول إلا أنها تحمل في طياتها تهديد لأمن واستقرار وحتى لاستمرار الدول، ذلك أن بناء أي مجتمع مستدام يقوم على المعرفة يحتاج للتقنين والحماية مع بيئة قانونية تؤطر هذه التحولات، وتعالج من خلالها القضايا الناجمة عن استخدام تكنولوجيا المعلومات والاتصالات وخدماتها المقدمة، وتتعامل مع التجاوزات الحاصلة باعتبار أن الفضاء السيبراني أصبح جزء لا يتجزأ من حياة الفرد نظرا لتداخله مع الحياة الاجتماعية، الاقتصادية وحتى السياسية.

وبما أن الجزائر ليست بمعزل عن التطورات الحاصلة فإن تحولها نحو أتمتة العمل الإداري يطرح عدة تحديات خاصة تلك المتعلقة بأمنها وسيادتها، باعتبار أن تهديد الفضاء السيبراني تخطى حدود الدول وهو ما يفضي بضرورة بناء أمن سيبراني قادر على الاستجابة لمثل هذه المخاطر، وعلى هذا الأساس فأن هدف الدراسة الأساسي يكمن في التعرف على أهم التحديات السيبرانية التي تواجهها الجزائر خاصة في السنوات الأخيرة، مع التطرق لأهم الاستراتيجيات المتبناة لبناء نظم دفاعية سيبرانية، إضافة للوقوف عل التشريعات المنظمة لاستخدام تكنولوجيا المعلومات والاتصال في مجال الاتصالات، المعاملات الالكترونية، التواقيع الالكترونية والملكية الفكرية خاصة في ظل تنامي جرائم الفضاء السيبراني كالإرهاب والجرائم السيبرانية، وهو ما يقودنا لطرح التساؤل الرئيسي للدراسة:

فيما تتمثل البيئة القانونية والأطر التشريعية التي أقرتها الدولة الجزائرية لمواجهة تحديات الفضاء السيبراني لاسيما مع تنامي التهديدات الأمنية في ظل اتساع استخدامات تكنولوجيا المعلومات والاتصال؟

وتفصيلا في الدراسة وانطلاقا من التساؤل المطروح سيتم تناول ما يلي:

أولا/ الفضاء السيبراني...كوجه آخر للعالم الافتراضي

ثانيا/ التهديدات السيبرانية وبناء الأمن السيبراني

ثالثا/ التشريعات السيبرانية كآلية لمواجهة التحديات السيبيرية –الجزائر انموذجا-

أولا/ مفاهيم الفضاء السيبراني ...كوجه آخر للعالم الافتراضي

تعريف الفضاء السيبراني:

يمكن اعتبار وزارة الدفاع الأمريكية الأب الروحي للفضاء السيبراني نتيجة تمويله للحوسبة المبكرة والشبكات، يتم وصف الفضاء السيبراني على أنه المجال العالمي في بيئة المعلومات التي تتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الانترنت وشبكات الاتصالات السلكية واللاسلكية وأنظمة الكمبيوتر والمعالجات وأجهزة التحكم المدمجة، فهو البيئة الافتراضية التي يتم فيها نقل المعلومات الرقمية عبر شبكات الكمبيوتر، كما يمكن أن نعتبر أن الفضاء السيبراني هو مجال شبكات الكمبيوتر والمستخدمين الذين يقفون خلفهم، حيث يتم تخزين المعلومات ومشاركتها وتوصيلها عبر الانترنت[1].

فالفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة إضافة إلى القوات الجوية، البرية والبحرية، وهناك من يرى أنه يمثل البعد الخامس للحرب، فالفضاء السيبراني حسب الاتحاد الدولي للاتصالات هو المجال المادي وغير المادي الذي يتكون أو ينتج عن عناصر هي أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر[2]. فالفضاء السيبراني حيز افتراضي للعديد من الفواعل يمكن تصنيفها في[3] :

الفواعل الدولاتية:

تعد فيها الدولة هي السلطة التي تؤثر على الأشخاص في الفضاء السيبراني، باستخدام العديد من الوسائل على غرار قوى الأمن الحكومة...، فالسياسة الداخلية للدولة في مجال الفضاء السيبراني تعتمد على تسيير المنشآت الحيوية والتنظيم الذي تقوم بالتمكين للولوج للشبكة، فالدولة هي الفاعل المحوري في هذا العالم الافتراضي لما لها من مكانة على أساس التفوق التكنولوجي، فالقوة السيبرانية اليوم هي المجال الجديد للخوض في الحروب على غرار القوة العسكرية.

الفواعل غير الدولاتية:

فإذا كانت الدولة مفتوحة على البيئة المحيطة فهذا يعني انفتاحها على العالم الخارجي بما يحمله من شركات متخصصة في تطوير الأمن السيبراني، ومنظمات أمن المنظومات المعلوماتية، وهو ما يؤدي لتفرع فواعل فردية وجماعية وهو ما يظهر من خلال:

الفرد: تؤثر الهجمات السيبرانية التي قد تضع الفرد تحت دائرة الخطر من خلال تسريبها لمعلوماته الشخصية هذا من جهة، ومن جهة أخرى يعتبر الفرد من المؤثرين في الفضاء السيبراني فهو من يحدد تحولات الفضاء السيبراني.

المنظمات غير الحكومية: إذ تسعى هذه المنظمات لوضع برامج تربصات على شكل برامج المساعدة التقنية حول استخدام التكنولوجيا الجديدة.

المجموعات الافتراضية: كالقراصنة الناشطون في الفضاء السيبراني.

وبما أن النظام السيبراني أو المعلوماتي كبيئة افتراضية تتضمن مكونات مادية و معنوية إضافة لشبكات اتصال خاصة ب Net works فان عناصر هذا النظام تتلخص في[4]:

العنصر المادي Hard ware: يتمثل أساسا في جهاز الحاسوب إضافة لملحقاته والوسائط التي توصل به لكي يتلقى من خلالها المعطيات والمعلومات، أو لإخراج النتائج بعد المعالجة، فهو بذلك عبارة عن آلة يمكن برمجتها لتقبل مدخلات وتجري تحويلا لتصبح مخرجات.

العنصر المعنوي Soft ware: ويشمل مجموع البرامج، الأساليب والقواعد، وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات.

وفي ظل عدم التمكن التكنولوجي وعدم القدرة على استيعاب دسائسه، يمكن القول أن الفضاء السيبراني أصبح يشكل مصدرا للتهديدات الأمنية التي تتربص بمستعملي هذا الفضاء(Cybernautes) على اختلاف مراكزهم(دول، منظمات، هيئات شركات....)، ما لم يعمل هؤلاء على تقنين قواعد الاستعمال والوعي بحجم خبايا الفضاء السيبراني[5].

ثانيا/ التهديدات السيبرانية وبناء الأمن السيبراني

التهديدات السيبرانية:

هناك تداخل بين مفهومي الحرب السيبرانية Cyber Warfare والهجمات السيبرانية Cyber Attack فهناك من يرى أنهما يعبران عن نفس المعنى، في حين هناك رأي يسلم بأن الهجمات السيبرانية هو المفهوم الأقرب لاحتواء معنى التهديدات السيبرانية أكثر من مفهوم

الحرب السيبرانية الذي يعتبر مفهوما غير مقبول في القانون الدولي، لأجل ذلك تعبر الهجمات السيبرانية عن تصرف يدور في العالم الافتراضي القائم على استخدام بيانات رقمية ووسائل اتصال تعمل الكترونيا، فهي بذلك هجوم عبر الانترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها بهدف تعطيل أو إتلاف أو الاستحواذ على البيانات المتوفرة فيها[6].

وإذا ما نظرنا للجريمة السيبرانية فإنها ليست مصطلحا قانونيا قائما بذاته، بل هو تعبير جامع يشمل مجموعة أفعال مرتكبة ضد بيانات أو نظم حاسوبية أو باستخدامها، فهي بذلك تشمل الجرائم المرتكبة بحق المعلومات الحاسوبية أو على استخدام موارد المعلومات لأغراض غير مشروعة[7].

تتعدى تهديدات الفضاء السيبراني المجال الافتراضي لتصل حتى للعالم الحقيقي، وهذا ما أثبته برنامج **stuxnet** دودة برامج خبيثة كأول استعراض في العالم الواقعي لقدرة برنامج على تحقيق تأثير مادي خبيث، فلطالما كان شعار العديد من خبراء الصراع السيبراني أن الحرب السيبرانية تقتل فقط الأطفال الالكترونيين إلا أن **stuxnet** أثبت للعالم أن الحرب السيبرانية قد تقتل الأطفال الحقيقيين أيضا، وهو ما أصابته **stuxnet** لما استطاعت توقيف مصنع تصنيع حقيقي لليورانيوم الإيراني ، وبالتالي أثبت أنه لا يوجد على الإطلاق ما يحد من هجوم سيبراني على تقنية اليورانيوم إذا ما أريد استغلالها لأغراض أخرى قد تفتك بالملايين وهو ما يهدد الاستقرار لحد كبير[8].

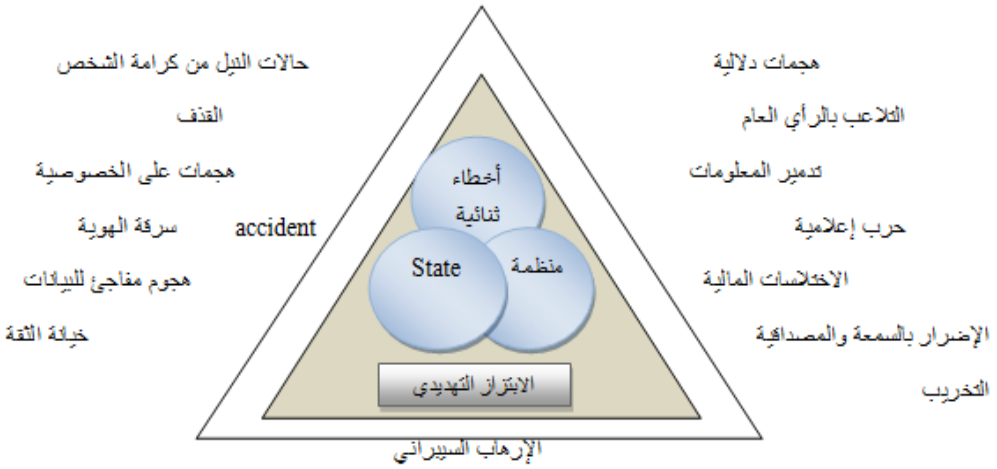
إن ارتفاع حدة القلق والتوتر من إمكانية قيام هجمات سيبرانية على البنية التحتية الحيوية ومستوى التأثير الذي يمكن أن ينعكس على السكان المدنيين يستدعي قيام بيئة وبنية دفاعية سيبرانية، بحيث تعتبر احتمالات الهجمات واستخدام الأسلحة والتقنيات السيبرانية احتمالات واسعة النطاق، وهو ما يبرز تنامي الخوف من القدرة السيبرانية المدمرة التي يمكن تفعيلها لتهديد استقرار وأمن الدول لاسيما مع ضعف نظم الحماية والافتقاد لأمن سيبراني يحتوي مثل هذه التهديدات[9].

إن الفضاء السيبراني كمجال افتراضي تتداخل فيه الأطراف والغايات يتطلب بناء منظومة دفاعية وهو ما يعرف بالأمن السيبراني الذي يضمن للأفراد الحفاظ على خصوصياتهم ويضمن للدولة كيانها ويحفظ سيادتها من الاختراق أو التعدي.

الأمن السيبراني:

يشمل الأمن السيبراني حسب **ريتشارد كمرر** وسائل دفاعية من شأنها الكشف واحباط المحاولات التي يقوم بها القراصنة، وحسب **ادوارد أمورسو** فإن الأمن السيبراني يشمل مجموع الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتتضمن بذلك الأدوات المستخدمة في الكشف عن الفيروسات وتوفير الاتصالات المشفرة، بحيث جوهر الأمن السيبراني يكمن في القدرة على مقاومة التهديدات المتعمدة أو غير المتعمدة، والتحرر من الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو سوء استخدامها[10].

يمس الأمن السيبراني الثورة الرقمية والثقافية للناس والمنظمات وللدول، بل إن التحديات التي ينطوي عليها ذلك معقدة ويحتاج للتصدي لها إلى ضرورة توافر الإرادة السياسية اللازمة لتصميم وتنفيذ إستراتيجية لتطوير بنيات تحتية وخدمات رقمية للأمن السيبراني، وعلى هذا الأساس تتضمن مستويات الأمن السيبراني الأفراد والمنظمات والدول وهو ما يمكن أن يشرحه الشكل التالي[11]:



فالغرض من الأمن السيبراني هو المساعدة على حماية أصول وموارد منظمة ما من المناحي التنظيمية، البشرية والمالية والتقنية والمعلوماتية بحيث تتمكن من أداء المهام الموكلة لها، لأجل ذلك فالأمن السيبراني يعتمد على وجود:

بنيات أساسية للمعلومات الدقيقة والآمنة،

سياسات لخلق الثقة،

أطر قانونية مناسبة،

سلطات قضائية ملمة بالتكنولوجيا الجديدة،

أدوات لإدارة مخاطر وامن المعلومات.

ثالثا/ التشريعات السيبرانية كآلية لمواجهة التحديات السيبيرية- الجزائر انموذجا-:

مفهوم القانون السيبراني:

تشمل قوانين الجرائم السيبرانية على كل عمليات الاقتحام غير المصرح بها في النظم السيبرانية، فبالرغم من اختلاف هذا النوع من الجرائم عن الجرائم التقليدية لكن هذا لا يمنع من إسقاطها أو تناظرها بسهولة مع مفاهيم القانون العام وإدراجها تحت بند التعدي على ممتلكات الغير، وقد تكيفت القوانين لتوضح أن عمليات الاختراق هي جرائم في حد ذاتها، وبالتالي فإن بناء نظام قانوني مناسب للتعامل مع مثل هذه المواقف يعتبر جوهر التشريعات السيبرانية[12].

تعتبر التشريعات السيبرانية مكونا أساسيا ودعامة من دعائم البنية القانونية اللازمة لتطوير مجتمع المعلومات، كما تعد عنصرا حيويا لتوفير الثقة بالخدمات الالكترونية وتأمين الحماية لمستخدمي الفضاء السيبراني[13]، وقد أطلقت الإسكوا عام 2007 مبادرة تحت عنوان "مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة، وقد ركزت على المشاركة الفعلية وقدمت إرشادات لسن قوانين تتماشى مع تحديات الفضاء السيبراني، كما قامت عديد الدول العربية من دراسة واعتماد مثل هذه التشريعات بناء على إرشادات نجد من بينها[14]:

الاتصالات الالكترونية وحرية التعبير،

المعاملات الالكترونية بما فيها التوقيع الالكتروني،

التجارة الالكترونية وحماية المستهلك،

معالجة وحماية البيانات ذات الطابع الشخصي،

الجرائم السيبرانية،

حماية الملكية الفكرية والصناعية.

مضمون التشريعات السيبرانية المنتهجة من قبل الدولة الجزائرية لمواجهة التحديات السيبيرية:

جدول رقم(1) يوضح الترتيب العالمي لقياس الأمن السيبراني للدول وترتيب الجزائر فيه

البلد	الرقم القياسي	الترتيب العالمي
أيسلندا*	0,206	22
أيرلندا*	0,206	22
الأردن	0,206	22
ليبيريا	0,206	22
باراغواي*	0,206	22
تنزانيا	0,206	22
ترينيداد وتوباغو	0,206	22
فنزويلا	0,206	22
الجزائر	0,176	23
أرمينيا	0,176	23
بربادوس	0,176	23
بيلاروس*	0,176	23
بليز*	0,176	23
بنن*	0,176	23
البوسنة والهرسك	0,176	23
بوتسوانا	0,176	23
كازاخستان*	0,176	23

وقد باشرت الدولة الجزائرية في إعداد برامج خاصة لمواجهة الجريمة الالكترونية والحد من انتشارها، وذلك عن طريق إنشاء أجهزة جديدة تنسجم في أدوارها وتجهيزاتها مع المتغيرات الحاصلة، فأصبحت الحماية السيبرانية جزءا مهما في أي منظومة للدفاع وعلى هذا الأساس فإن بناء الأمن السيبراني يضمن بناء بنية تشريعية قوية تدعم تحولها وتقنن مسيرتها نحو الحكومة الالكترونية وأتمتة نشاطها الإداري والحكومي، وعليه تحتل الجزائر من خلال الترتيب العالمي لقياس الأمن السيبراني مرتبة متدنية وهو ما يوضحه الجدول التالي[15]:

وبالنسبة لترتيب الجزائر بين الدول العربية في مجال قياس الأمن السيبراني فيوضح الجدول التالي مكانة الدولة الجزائرية من خلال التطرق للمؤشرات المكونة للمقياس العالمي[16]:

جدول رقم(2) يوضح ترتيب الدول العربية حسب الرقم القياسي العالمي للأمن السيبراني للدول وترتيب الجزائر فيه

الدول العربية	قانونية	تقنية	تنظيمية	بناء القدرات	التعاون	الرقم القياسي	الترتيب الإقليمي
عمان	0,7500	0,6667	1,0000	0,7500	0,6250	0,7647	1
قطر	0,7500	0,8333	0,5000	0,6250	0,5000	0,6176	2
مصر	0,5000	0,5000	0,3750	1,0000	0,5000	0,5882	3
المغرب	0,5000	0,6667	0,7500	0,5000	0,3750	0,5588	4
تونس	1,0000	0,5000	0,6250	0,2500	0,5000	0,5294	5
السودان	0,7500	0,5000	0,5000	0,2500	0,3750	0,4412	6
الإمارات العربية المتحدة*	0,7500	0,3333	0,2500	0,5000	0,1250	0,3529	7
البحرين	0,7500	0,1667	0,1250	0,3750	0,2500	0,2941	8
ليبيا	0,2500	0,3333	0,3750	0,1250	0,3750	0,2941	8
المملكة العربية السعودية*	0,7500	0,3333	0,1250	0,3750	0,1250	0,2941	8
الأردن	0,5000	0,0000	0,5000	0,0000	0,1250	0,2059	9
الجزائر	0,7500	0,0000	0,0000	0,1250	0,2500	0,1765	10
سورية	0,2500	0,3333	0,1250	0,1250	0,1250	0,1765	10
موريتانيا	0,2500	0,1667	0,2500	0,0000	0,1250	0,1471	11
دولة فلسطين*	0,2500	0,0000	0,3750	0,1250	0,0000	0,1471	11
لبنان	0,0000	0,0000	0,0000	0,2500	0,1250	0,0882	12
جيبوتي	0,2500	0,0000	0,0000	0,0000	0,1250	0,0588	13
الكويت*	0,0000	0,0000	0,0000	0,1250	0,1250	0,0588	13
اليمن*	0,2500	0,0000	0,0000	0,0000	0,1250	0,0588	13
جزر القمر	0,0000	0,0000	0,0000	0,0000	0,1250	0,0294	14
العراق*	0,0000	0,0000	0,0000	0,0000	0,1250	0,0294	14

فما يتضح على الصعيد العربي أن الجزائر تحتل من بين الدولة العربية المرتبة 10 بنسبة 0.176 من سلم على 1 وهو ما يوضح النسب المعدومة التي حققتها الجزائر في المجالات التقنية والتنظيمية، والنسب المحتشمة المحققة في مجال بناء القدرات والتعاون، في حين حققت البنية القانونية تطورا ملحوظا في المجال لكن تبقى الفجوة نسبة للدول العربية الأخرى جد مرتفعة.

تتمثل مرتكزات بناء بيئة تشريعية قوية تواجد الأطر القانونية والتشريعية وتدعيمها بمؤسسات وهياكل قادرة على تطبيق السياسات خاصة المتعلقة بالأمن السيبراني وتطبيقها على أرض الواقع، وعلى هذا الأساس نتطرق لأهم التشريعات المنصوص عليها في القانون مع الوقوف على مؤسسات المستحدثة في هذا الصدد، ومن هذا المنطلق تتمثل هذه الآليات في :

النصوص القانونية:

قانون 09-04 المؤرخ في 05 غشت 2009 والذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، كما يبرز القانون المصطلحات الأساسية التي تضمنها القانون والمتعلقة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، منظومة معلوماتية، مقدمو الخدمات، المعطيات المتعلقة بحركة السير، الاتصالات الالكترونية وهو ما يمكن ذكره في[17]:

أ/الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: وتتمثل في جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

ب/منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض والمتعلقة بالمعالجة الآلية للمعطيات تنفيذ لبرنامج معين.

ج/ معطيات معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شانها جعل منظومة معلوماتية تؤدي وظيفتها.

كما حدد القانون أيضا القواعد الخاصة التي تسمح باللجوء إلى مراقبة الاتصالات الالكترونية والتي تتمثل في[18]:

الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة،

في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني،

لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء في المراقبة الالكترونية،

في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

مرسوم رئاسي رقم 15-261 المؤرخ في 8 أكتوبر2015:

والذي اقتضى تشكيل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وحددت مهامها وتشكيلتها بحيث نصت المادة 4 على[19]:

اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

ضمان المراقبة الوقائية الاتصالات الالكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

قانون رقم 18-04 مؤرخ في 13 مايو2018:

يتضمن القانون من خلال نصوصه مواد تركز على جانب تأمين الدولة للانتفاع بخدمات الفضاء السيبراني على غرار الاتصالات الالكترونية وهو ما يظهر من خلال[20]:

المادة4: تنص على أن الدولة تسهر في إطار الصلاحيات المرتبطة بمهامها على مجموعة من المهام أهمها:

أمن وسلامة شبكات الاتصالات الالكترونية

توفير خدمات مطابقة للمقتضيات القانونية والتنظيمية للخدمة الشاملة.

المادة6: تضطلع الدولة في إطار ممارسة صلاحياتها المتعلقة بمراقبة الاتصالات الإلكترونية بما يلي:

ممارسة سيادتها طبقا للأحكام الدستورية على كامل فضائها الهيرتيزي

الانفراد بالاستخدام الحصري لطيف الذبذبات اللاسلكية الكهربائية وضمان التخطيط وتقسيمه إلى حزم ذبذبات ومراقبة والإشراف على استعماله من طرف مختلف المستعملين في ظل احترام مبادئ الفعالية والرشادة في استعمال الذبذبات اللاسلكية الكهربائية.

تساهم هذه الخدمات على الخصوص في مجهود التهيئة الرقمية للإقليم وتقليص الفجوة الرقمية.

المؤسسات والأجهزة المستحدثة لبناء الأمن السيبراني[21]:

مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:

هو الجهاز الوحيد وطنيا أنشئ في 2008 بهدف خدمة الأمن العمومي من خلال تأمين الفضاء السيبيراني واعتبر بمثابة مركز توثيق، يقوم المركز بتحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة وتحديد هوية مرتكبيها، و ذلك لأجل تأمين الأنظمة المعلوماتية والحفاظ عليها لا سيما تلك المستخدمة في المؤسسات الرسمية والبنوك، و قد استطاع المركز معالجة مئات من القضايا لحد الآن.

المعهد الوطني للأدلة الجنائية و علم الإجرام للدرك الوطني:

مؤسسة عمومية تحت الوصاية المباشرة لوزير الدفاع الوطني من مهامها تصميم وانجاز بنوك المعطيات، إجراء البحوث المتعلقة بالإجراء وذلك باللجوء إلى التكنولوجيات الدقيقة إضافة لمهام أخرى ويتضمن المعهد عدة أقسام كمصلحة البصمات، الوثائق، إضافة لمصلحة الإعلام الآلي وهي مصلحة تهتم برصد ومراقبة وتتبع عمليات الاختراق، القرصنة المعلوماتية، وتفكيك البرامج المعلوماتية ...الخ .

المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

وهي نواة محاربة الجريمة الالكترونية في مديرية الأمن الوطني أنشأت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بقرار من المدير العام للأمن الوطني والتي ألحقت بمديرية الشرطة القضائية في جانفي 2015.

الهيئة الوطنية للوقاية من الجرائم بتكنولوجيا الإعلام و الاتصال ومكافحتها:

تشكلت هذه الهيئة سنة 2015 تابعة لوزير العدل، تتضمن قضاة وضباط للشرطة القضائية، كلفت الهيئة باقتراح إستراتيجية وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وذلك عن طريق الاستفادة من الخبرات، وضمان المراقبة الوقائية للاتصالات الالكترونية للكشف عن الجرائم التي تمس بأمن الدولة.

وإذا ما حاولنا المقارنة بين الجزائر والدول العربية على غرار الإمارات العربية المتحدة، نجد أن الإمارات قد سبقت مثيلاتها من الدول العربية في إصدار أول قانونين يدعمان التحول الالكتروني

سنة 2006، فعملت على تجهيز البيئة المثالية لتطبيق مشروع الحكومة الالكترونية وبناء الأمن السيبراني مدعمة ذلك بجملة من القوانين والتشريعات التي تقنن وتحمي البنية التحتية منها :

- قانون الهوية الالكترونية سنة 2006 (يعنى بالمعاملات والتجارة الالكترونية)
- الجرائم الالكترونية 2006(مكافحة جرائم تقنية المعلومات) [22]
- قانون الدفع والتحويل الالكتروني
- نظام ترخيص واعتماد جهات التوثيق الالكتروني والحكومة الذكية
- التصديق الالكتروني[23]

كما أقرت "**حكومة دبي**"، باعتبارها أول حكومة الكترونية قبل تفعيل البرنامج الاتحادي للحكومة الالكترونية) عدد من القوانين القاضية بإنشاء المنطقة الحرة للتكنولوجيا والإعلام وتنظيم المعاملات الإلكترونية بكافة نواحي الحياة لاقتصادية والاجتماعية بالإمارة .

ساعدت التشريعات السيبرانية على تسهيل عمل القطاعات الحكومية وتقديم خدماتها بمرونة عالية، لكن رغم ذلك لازالت تشوب هذه القوانين بعض الثغرات الخاصة ببنية تكنولوجيا المعلومات والاتصالات، ونقص الآليات اللازمة لتنفيذ هذه القوانين بدقة وفاعلية، وتظهر الحاجة الماسة لتطوير التشريعات والقوانين المتعلقة ببعض المجالات كحرية المعلومات وسريتها التي تكفل للأفراد حماية خصوصياتهم .

الخاتمة:

يتبين من خلال ما سبق ذكره أن السياسات السيبرانية المنتهجة من قبل الدولة الجزائرية لا تزال قوانين جد محتشمة ولا تسد الفجوة التشريعية الحاصلة بحيث أن البنية القانونية للدولة الجزائرية لم تتطور بقدر ما تنامت التطورات التكنولوجية والمعلوماتية الحاصلة، فانفتاح الدولة الجزائرية خاصة بعد دخول خدمات الجيل الرابع قد فتح باب الرهانات على مصراعيه مما زاد في حجم التحديات الملقاة على الدولة لبلورة الأمن السيبراني خاصة فيما تعلق ببناء الأطر القانونية الملائمة للتحول الذي تشهده الدولة الجزائرية لا سما تحولها نحو الحكومة الالكترونية وأتمتة العمل الإداري، وهو الأمر الذي يستدعي تحالف النخب خاصة الإطارات التقنية الخبيرة في المجال لتصميم نظم حماية قوية تتماشى مع الرهانات التي تتربص بالدولة، كذلك الاستفادة من التجارب الدولية الرائدة في مجال تحقيق الأمن السيبراني.

وعن أهم التوصيات المقترحة لبلورة البنية التشريعية والقانونية نجد

- لابد أن يكرس الأمن السيبراني كمشروع وطني يتطلب وضوح الرؤية وتوفرموارد تقنية، مادية وبشرية ضخمة لبناء خطة متكاملة تلقى دعما ومتابعة صارمة ودقيقة من قبل القادة السياسيين في الدولة، مع تهيئة بنية تشريعية متينة متكاملة الجوانب تكفل للأفراد حماية خصوصياتهم، وتسهيل تعاملاتهم في ظل العصر الرقمي .
- لا بد أن تعتمد استراتيجيات الأمن السيبراني على أساس دراسات مناسبة من قبل هيئات مختصة وخبيرة في المجال، تنسجم فيها المشاريع مع خصوصيات الدولة وبيئتها الداخلية لا أن تكون تجارب مستوردة من بيئة أجنبية .
- بد وأن ينصب جهد الدولة الأساسي على محو الأمية خصوصا الأمية الرقمية إن صح القول، حيث أن من أهم معيقات تقدم الأمم عموما وفي مجال ضمان الحماية من تهديدات الفضاء السيبراني خصوصا راجع الى تصلب الذهنيات ورفضها التغيير المواكب للعصر الرقمي سواء كان ذلك الرفض نابعا عن جهل بطبيعة التحول الالكتروني الذي انتهجته الدولة أو تخوف نتيجة عدم ثقة في المسؤولين .
- استكمال تجهيز بنية تحتية متينة لتكنولوجيا المعلومات والاتصالات من خلال بناء نظم اتصالات فعالة تترابط من خلالها الجهات الحكومية المركزية والمحلية، وتسمح بانسيابية المعلومات من وإلى المؤسسات الحكومية، المواطن، القطاع الخاص والمجتمع المدني .

قائمة المراجع:

[1] P.W.Singer, Allan Friedman, **Cyber security and Cyber war (what everyone needs to know)**. New York: Oxford University Press, 2014, p13.

[2] ربيع محمد يحي، "إسرائيل وخطوات الهيمنة على ساحة الفضاء السيبراني في الشرق الأوسط : دراسة حول استعدادات ومحاور عمل الدولة العبرية في عصر الانترنت 2002-2013"، **مجلة رؤى إستراتيجية**، المجلد1، العدد3، 2013، ص 67.

[3] يوسف بوغرارة، "الأمن السيبراني: الإستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري"، **مجلة الدراسات الإفريقية وحوض النيل**، المجلد1، العدد3، 2018، ص 104.

[4] نبيل دريس، "الجريمة السيبرانية بين المفاهيم والنصوص التشريعية"، **مجلة القانون والمجتمع**، المجلد5، العدد2، ص ص 25-27.

لطفي لمين بلفرد، "الفضاء السيبراني: هندسة وفواعل"، **المجلة الجزائرية للدراسات السياسية**، العدد5، ص 150. [5]

[6] أحمد أوباس الفتلاوي، "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر"، **مجلة المحقق الحلي للعلوم القانونية والسياسية**، العدد4، ص ص 615-616.

[7] منظمة الأمم المتحدة، مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، الدوحة، 12-19 أفريل 2201، متوفر على الرابط التالي :

https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_a_V1500661.pdf

[8] Paul Rosenzweig, **Cyber Warfare (how conflicts in cyberspace are challenging america and changing the world.** California: Praeger, 2013, p02.

[9] Julian Richards, **Cyber-War (the anatomy of the global security threat),** 1st edition. Hampshire: Palgrave Macmillan, 2012, p04.

[10] عنترة بن مرزوق، محي الدين حرشاوي، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، 2017، ص ص 66-67، متوفر على الرابط : https://manifest.univ-ouargla.dz/documents/Archive/2016-2017/FDSP/%D8%B3%D9%8A%D8%A7%D8%B3%D8%A7%D8%AA%20%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9%20%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A/%D8%AF-%D8%A8%D9%86_%D9%85%D8%B1%D8%B2%D9%88%D9%82_%D8%B9%D9%86%D8%AA%D8%B1%D8%A9.pdf

حمدون أ. توريه، وآخرون، **دليل الأمن السيبراني للبلدان النامية**. جنيف: الاتحاد الدولي للاتصالات، 2006، ص ص 7-8.[11]

[12] Rosenzweig, **Op.Cit**., p 86.

[13] اللجنة الاقتصادية والاجتماعية لغربي آسيا (الاسكوا)، **إرشادات الاسكوا للتشريعات السيبرانية (مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية)**. بيروت: منشورات اللجنة الاقتصادية والاجتماعية لغربي آسيا (الاسكوا)، 2012، ص ج.

[14] اللجنة الاقتصادية والاجتماعية لغربي آسيا (الاسكوا)، **استراتيجيات الحكومة الالكترونية في الدول العربية الواقع وآفاق التطور**. بيروت: اللجنة الاقتصادية والاجتماعية لغربي آسيا، 2013، ص ص 37-38.

[15] الاتحاد الدولي للاتصالات، **تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية**. جنيف: مكتب تنمية الاتصالات، ص4.

الاتحاد الدولي للاتصالات، تقرير حول الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية، **مرجع سابق**، ص 11.[16]

[17] لمزيد من التفصيل أنظر: الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم09-04 المؤرخ في 14 شعبان1430، الموافق ل05 غشت2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **الجريدة الرسمية**، العدد 47، الصادرة بتاريخ 25 شعبان 1430 الموافق ل16 أوت2009، ص 05.

[18]الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم09-04 المؤرخ في 14 شعبان1430، الموافق ل05 غشت2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **مرجع سابق**، ص 06.

[19]

[20] الجمهورية الجزائرية الديمقراطية الشعبية، قانون رقم 18-04 مؤرخ في 24 شعبان 1439 الموافق ل 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، **الجريدة الرسمية**، العدد 27، الصادرة بتاريخ 13 مايو 2018، ص 05.

[21] سمير بارة، "الأمن السيبراني Cyber Security في الجزائر السياسات والمؤسسات"، **المجلة الجزائرية للأمن الإنساني**، العدد4، 2017، ص ص 270-275.

[22] نيفين حسين، **جهود دولة الإمارات العربية المتحدة في مجالات الابتكار واقتصاد المعرفة**. الإمارات العربية المتحدة، وزارة الاقتصاد ، 2016، ص. 7.

[23] اللجنة الاقتصادية والاجتماعية لغربي آسيا، استراتيجيات الحكومة الالكترونية في الدول العربية الواقع وآفاق التطور. **مرجع سابق**، ص ص 38 -40-41.