مجلة الحوكمة والقانون الاقتصادي
المجلد: xx / العدد: xx / السنة: 20xx / ص ص: xxx - xxx

الآليات الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني(الجزائر نموذجا)

Objective and procedural mechanisms used to achieve cyber security (Algeria as a model)

تاريخ الإرسال:2023/06/16 تاريخ القبول:2023/07/26

قطاف سليمان*	Guettaf slimane	بوقرين عبد الحليم	Bougrine Abdel Halim
مخبر البحث الحقوق والعلوم السياسية جامعة عمار ثليجي الأغواط		مخبر البحث الحقوق والعلوم السياسية جامعة عمار ثليجي الأغواط	
جامعة عمار ثليجي الأغواط		جامعة عمار ثليجي الأغواط	
s.guettaf@lagh-univ.dz		Halim.ma@yahoo.fr	

ملخص: يعتبر الأمن السيبراني أحد الركائز الأساسية لتقوية المنظومة الأمنية لسائر الدول، بل أضحى ضرورة حتمية لمواجهة المخاطر السيبرانية التي تهدد كيان الدول وإستقرار سيادتها وذلك لطبيعتها الخاصة التي لا تعترف بالحدود الوطنية وهي مخاطر عابرة للحدود، وصعوبة تعقب مرتكبيها وذلك لسهولة إزالة ادلة الإثبات للإدانة، وقد إقتحمت هذه التهديدات السيبرانية جميع مناحي الحياة نتيجة للتطور السريع والمذهل لتكنولوجيات الإعلام والإتصال، وبالتالي يسهل إختراق خصوصيات المؤسسات والشركات الخاصة، بل وحتى الحياة الخاصة للأفراد.

والجزائر هي أيضا مستهدفة كسائر الدول من التهديد السيبراني، وتداركت الوضع بداية من سنة 2004 بسن القانون 15-04 المعدل والمتمم لقانون العقوبات المتضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والقانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية بإستحداث تدابير الإجرائية لمكافحة الجرائم الإلكترونية، وأيضا سن المشرع نصوص خاصة نذكر أهمها القانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها الذي من مضامينه التشجيع على التعاون الدولي والمساعدة القضائية.

الكلمات المفتاحية: الأمن السيبراني، المنظومة المعلوماتية، الجرائم الالكترونية.

***Abstract**: Cyber security is considered as one of the main pillars for strengthening the security system of all countries. Rather, it has become an imperative necessity to confront cyber risks that threaten the entity, stability and sovereignty of states, due to their special nature, which does not recognize national borders and transcend borders, and the difficulty of tracking down the perpetrators due to the ease of removing evidence of conviction. These cyber threats have invaded All walks of life as a result of the rapid and astounding development of information and communication technologies, thus penetrating the privacy of private institutions and*

*- قطاف سليمان

companies, and even the private mention the most important of them, Law 09-04, which includes the prevention of crimes related to information and communication technologies, which includes encouragement of international cooperation and judicial assistance.

***Keywords**:Cybersecurity, information system, international cooperation.*

lives of individuals.

Algeria, like other countries, was not spared from the cyber threat, and it remedied the situation beginning in 2004 by enacting Law 04-15 amending and supplementing the Penal Code that includes crimes affecting automated data processing systems, and Law 06-22 amending and supplementing the Code of Criminal Procedures by introducing procedural mechanisms to combat cybercrime, with special texts. We

مقدمـة:

يشهد العالم اليوم تطورا غير مسبوق، خاصة المجال التكنولوجي الذي يهتم كثيرا بالحوسبة والحاسبات الآلية، وأضحى العالم مندمجا ومحصورا في عالم إفتراضي، حيث ساعد الإنسان في تقديم خدمات جليلة وتوفير الرفاهية والراحة، وأصبح الإنسان يدير اعماله من خلال شبكات الإلكترونية خصوصا شبكة الأنترنت، لكن هذا التطور بالرغم من إيجابياته إلا أن هناك سلبيات ومخاطر تهدد الأفراد والشركات وحتى الدول نتيجة الإعتداء من المجرمين السيبرانيين على البيانات الشخصية للأفراد والإحتيال على المصارف المالية والتجسس والإرهاب الإلكتروني الذي مس الدول في نظامها العام والأمن الوطني وباتت هذه الدول مهددة في كيانها ووجودها.

والجزائر لم تكن بمنأى من هذه التهديدات السيبرانية وخاصة في المؤسسات الوطنية، والإختراق الأخير لبرنامج "**بيقاسوس**" الإسرائيلي خير دليل على هذا التهديد، ناهيك عن جرائم الإحتيال والنصب على شبكات التواصل الاجتماعي التي تطال الأفراد والمؤسسات يوميا والعدد في تزايد مستمر ومخيف، فالجزائر أصبحت هدف للمخترقين سواء دولا أو أفرادا، وذلك لموقعها الإستراتيجي، مما دفعها في سياستها الأمنية الاهتمام بالأمن السيبراني ومواجهة هذا النوع المستحدث من الإجرام .

إذن نحن أمام الإشكالية التالية: **ما مدى نجاعة وفعالية الأليات الموضوعية والإجرائية المتخذة من قبل الجزائر في تحقيق الأمن السيبراني ومواجهة تحديات الإجرام الإلكتروني؟ .**

وللإجابة عن هذه الإشكالية سنحاول التطرق في هذه الورقة البحثية للخطة التالية: مفهوم الأمن السيبراني (المحور الأول) نتطرق فيه لتعريف الأمن السيبراني وأبعاد الأمن السيبراني ونتطرق للتدابير المتخذة لتعزيز الأمن السيبراني وفق التشريع الجزائري (المحور الثاني) .

المحور الأول: مفهوم الأمن السيبراني

يعتبر الأمن السيبراني من المفاهيم التي أصبحت تتداول في الدراسات الأكاديمية نظرا لأهميتها في الحد من الاختراقات السيبرانية ومواجهة الجرائم الإلكترونية بشتى الطرق والأساليب الموضوعية والإجرائية، وبالتالي كثر إستخدام هذا المصطلح عبر العالم، فعرجنا إلى تعريف الأمن السيبراني (أولا)، وإلى أبعاد الأمن السيبراني (ثانيا).

أولا- تعريف الأمن السيبراني

هناك تعريف منها ما هو فقهي ومنها ما هو قانوني و يا ترى كيف عرف المشرع الجزائري الأمن السيبراني ؟، وهو ما نراه في التعريف الفقهي والقانوني، ثم تعريف المشرع الجزائري للأمن السيبراني.

1- التعريف الفقهي والقانوني للأمن السيبراني:

أ- تعريف الأمن السيبراني ويمكن أن نقارب هذا المفهوم من عدة زوايا **السيبرانية لغة**: وهي مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الإفتراضي، فالسيبرانية تعني (فضاء الأنترنت) وهي كلمة مشتقة من الكلمة اليونانية *Kybernetes* التي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة[1].

السيبرانية إصطلاحا: كلمة سيبرانية في مفهومها الحديث إستعملت لأول مرة من قبل عالم الرياضيات الأمريكي نوربرت وينر *Norbert Winer* وهو أستاذ الرياضيات في معهد ماساشوستس التقني *MIT* الذي أعطاها مفهومها الإصطلاحي الحديث وكان ذلك عام 1948، ومن أجل وصف نظام التغذية الرجعية *Feedback* الإستفادة من مخرجات الأنظمة *out puts* في ضبط مدخلاتها *in puts* وفي التحكم فيها وإستقرار أدائها[2] . وبعد معرفتنا لتعريف السيبرانية لغة وإصطلاحا نعرج إلى التعريف الفقهي.

ب- التعريف الفقهي لأمن السيبراني:

الأمن السيبراني هو "**عبارة عن مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الإستخدام غير المصرح به وسوء الإستغلال واستعادة المعلومات الإلكترونية ونظم الإتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني**"[3].

ثالثا- التعريف القانوني الدولي للأمن السيبراني:

كما نذكر التعريف الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقريره حول" اتجاهات الإصلاح في الاتصالات للعام 2010-2011"، **والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية "هو مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات أمنية، ومبادئ توجيهية. ومقاربات الإدارة المخاطر، وتدريبات، وممارسات فضلي، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين**"[4].

2- تعريف المشرع الجزائري للأمن السيبراني:

أعطى المشرع الجزائري تعريفا في الفقرة الثالثة من المادة العاشرة من القانون رقـــم: 18-04[5] بأنه:" **مجموع الأدوات والسياسات ومفاهيم الأمن والآليات الأمنية والمبادئ التوجيهية وطرق تسيير المخاطر والأعمال والتكوين والممارسات الجـــيدة والضمانات والتكنولوجيات التي يمكن استخدامها في حماية الاتصالات الإلكترونية ضـــد أي حـدث مـــن شأنه المساس بتوفير وسلامة البيانات المخزنة أو المعالجة أو المرسلة**".

كما سعى المشرع في تعديله الأخير لقانون العقوبات للفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر 66-156[6] إلى إضافة قسم سابع مكرر عنوانه: "**المساس بأنظمة المعالجة الآلية للمعطيات**"، بالقانون 04-15[7] ويشمل المواد من 394 مكرر إلى 394 مكرر 7. حيث جاء في هذا القسم بتسطير حماية لأنظمة المعالجة الآلية للمعطيات، وهو ما تركه ينص على بعض من الجرائم و ما يقابلها من عقوبات للحد من إرتكابها[8].

وقد عرف الجريمة السيبرانية في نص المادة 2 الفقرة-أ- من الفصل الأول من القانون 09-04[9] المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تحت عنوان مصطلحات بأنها "**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**"[10] .

ثانيا- أبعاد الأمن السيبراني:

إن للأمن السيبراني أهمية كبيرة في المحافظة والحماية من التعديات السيبرانية التي باتت خطرا يداهم الجميع، ولهذه الأهمية أبعاد شتى للأمن السيبراني، سنتطرق لها وهي خمسة أبعاد وهي الأبعاد القانونية والسياسية والعسكرية ، ثم الأبعاد الإجتماعية والإقتصادية .

1- الأبعاد القانونية والسياسية والعسكرية للأمن السيبراني:

أ- البعد القانوني :

يترتب على النشاط الفردي والمؤسساتي والحكومي في الفضاء السيبراني نتائج قانونية وموجبات تستدعي اهتماما خاصا لحل النزاعات التي يمكن أن تنشأ عنها، وهو ما يستدعي مواكبة التحولات التي رافقت ظهور مجتمع المعلومات، فظهرت حقوق أخرى كحق النفاذ إلى الشبكة العالمية للمعلومات وتوسعت بعض المفاهيم لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية والحق في إنشاء التجمعات على الانترنت والحق في حماية ملكية البرامج المعلوماتية[11].

ب- البعد السياسي :

هناك أمثلة كثيرة تدفع نحو الاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة التي تؤدي إلى مشكلات عويصة جدا على المستوى الداخلي والدولي، كما أنه لا ينكر أحد الدور المتعاظم للشبكات التواصل الاجتماعي على المستوى السياسي خاصة تنظيم الحملات الإنتخابية،

والتظاهرات الافتراضية، والحركات الإحتجاجية الإلكترونية، كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياساتها[12].

ج- الأبعاد العسكرية :

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها ، وكذا السرعة وإعطاء الأوامر العسكرية والقدرة على إيصال الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف لا قوة إن لم تكن شبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي إختراق خارجي قد يتسبب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الإستخبارات، والقيام بعمليات التجسس على أمن العسكري للدول، وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الإتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل وتعطيل عمل أنظمة الدفاع الجوي أو التوجيه الإلكتروني فضلا عن إمكانية فقدان السيطرة على وحدات القيادة[13].

2- الأبعاد الإجتماعية والإقتصادية للامن السيبراني:

أ- الأبعاد الإجتماعية :

تساهم شبكات التواصل الإجتماعي بشكل خاص في فتح المجال للأفراد للتعبير عن تطلعاتهم السياسية وطموحاتهم الإجتماعية بأشكالها المختلفة، كذلك تشكل مشاركة جميع شرائح المجتمع ومكوناته وسيلة لتطوير المجتمع مما يتيح الفرصة للإطلاع على الأفكار والمعلومات وبما تكونه من حاجة لدى المجتمع في الحفاظ على إستقرار الفضاء الإلكتروني والمجتمع الذي يرتكز إليه، كما أن إنفتاح مجتمع ما على المجتمعات الأخرى يؤسس لتبادل خبرات وأفكار وتكوين آفاق للتعاون والتكامل[14].

ب- الأبعاد الإقتصادية:

يرتبط الأمن السيبراني ارتباطا وثيقا بالإقتصاد فالتلازم واضح بين إقتصاد المعرفة وتوسيع إستخدام تقنيات المعلومات والإتصالات بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كل المستويات، كما تتيح تقنيات المعلومات والإتصالات تعزيز التنمية الإقتصادية لدول كثيرة عبر إفادتها من فرص الإستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث في إدارة كلفة إنتاجها بأفضل الشروط، يضاف إلى ذلك دخول العالم عصر المال الإلكتروني ضمن بيئة تقنية متحركة بعد إطلاق الخدمات الإلكترونية، إذ تتزايد إستثمارات المصارف والمؤسسات المالية في مجال المال الرقمي وتتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع آمنة، وقد وضعت بعض الدول تشريعات خاصة بحماية أموالها وما يمكن أن يثيره هذا الأمر من صعوبات وما يتطلبه من تشريعات للحد من بعض الجرائم الإقتصادية والمالية الخطيرة والعابرة للحدود كتبييض الأموال والتهرب من الضريبة. فالأمن السيبراني يضمن تقديم الخدمات التي تقدم بواسطة تقنيات المعلومات والإتصالات، كما يضمن الإقبال عليها بما يترجم عمليا بتطوير أسس إقتصاد سليم[15]

أصبح الامن السيبراني حتمية ضرورية لكل دول العالم وللهيئات العامة والشركات العامة والخاصة وأصبحت الدول تهتم به لحماية نفسها ومواطنيها من التهديدات السيبرانية ومواجهة كافة صور الاجرام السيبراني، فكيف واجه المشرع الجزائري هذا الاجرام المستحدث خاصة في نصوصه القانونية وهو ما سنتطرق له في المحور الموالي.

المحور الثاني: التدابير الموضوعية والإجرائية المتبعة لتحقيق الأمن السيبراني وفق التشريع الجزائري

تفطن المشرع الجزائري للإجرام الإلكتروني وتدارك الوضع فبادر إلى سن مجموعة من القوانين بدأها بتعديل قانون العقوبات بالقانون 04-15 وسماه بالجرائم "**المساس لأنظمة المعالجة الآلية للمعطيات**" وبعدها بالقانون 06-22 لتعديل قانون الإجراءات الجزائية والقانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وإتخاذ عدة تدابير نوضحها كما يأتي: التدابير القانونية والتقنية (أولا)، التدابير الهيكلية والتعاون الدولي (ثانيا).

أولا- التدابير الموضوعية والتقنية للأمن السيبراني:

سار المشرع الجزائري على نهج الدول المتقدمة خاصة فرنسا في سن قوانين خاصة بتجريم السلوكات الماسة بأنظمة المعالجة الآلية للمعلومات، وإستحدات إجراءات مستحدثة في القانون 06-22 وهو ما نراه في التدابير القانونية، ثم التدابير التقنية والإجرائية .

1- التدابير القانونية للأمن السيبراني:

تطرق المشرع الجزائري على غرار الدول الأخرى مثل فرنسا لتجريم أفعال المساس بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، مما دفع بالمشرع إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، والذي أفرد القسم "**السابع مكرر**" منه تحت عنوان "**المساس بأنظمة المعالجة الآلية للمعطيات** " من المادة 394 مكرر إلى 394 مكرر 7، ونص على عدة جرائم،أما في عام 2006 أدخل المشرع الجزائري تعديلا آخر على قانون العقوبات بموجب القانون رقم 06-23[16] حيث مس ذلك التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم من قانون 04-15، وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه، كما أدخل المشرع الجزائري بالقانون رقم 16-02[17] المعدل والمتمم لقانون العقوبات مادتين وهما 87 مكرر11، و394 مكرر 8 فاستعمل في الأولى عبارة (تكنولوجيات الإعلام والاتصال، وفي الثانية عبارة (مقدم خدمات الانترنت)[18].

2- التدابير التقنية والإجرائية للأمن السيبراني:

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها تفادى وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما إستدركه المشرع بتضمين القانون رقم 06-22[19] - المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الإتصالات الإلكترونية وتسجيلها والتسرب. ويقصد بإعتراض المراسلات إعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين الإستقبال والعرض التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها.

ولقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية بموجب هذه المادة فان المشرع الجزائري يسمح لسلطات التحقيق والإستدلال إذا إستدعت ضرورة التحري في الجريمة المتلبس بها أو التحقيق في الجريمة الإلكترونية، اللجوء الى إجراء إعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات و الأصوات و التقاط الصور و الإستعانة بكل الترتيبات التقنية اللازمة لذلك، لأجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة[20].

ومع هذا فان المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الإستدلال والتحري وتصون الحقوق و الحريات العامة والحياة الخاصة للأفراد.

ثانيا- التعاون الدولي والتدابير الهيكلية و لفعالية الأمن السيبراني:

إن المواجهة القانونية لا تكفي لوحدها لمكافحة الجريمة الإلكترونية لأنها جريمة عابرة للحدود ولا تعترف بالحدود الوطنية أيضا يصعب إكتشافها، فبادر المشرع الجزائري إنشاء هياكل مؤسساتية لمجابهتها وشجع على التعاون الدولي في مجال جمع المعلومات والأدلة وتبادل المجرمين بين الدول والمساعدة القضائية بصفة عامة ونوضح ذلك في التعاون الدولي ثم التدابير الهيكلية.

1- التعاون الدولي لمكافحة الاجرام السيبراني:

أصبحت الدولة لوحدها غير قادرة على مواجهة المخاطر السيبرانية ، مما أوجب على الدول التعاون فيما بينها لحصر هذا الإجرام المستحدث والقضاء عليه نهائيا وعليه سنتطرق إلى التعاون الأمني الدولي ثم المساعدة القضائية فيما يلي.

أ- التعاون الأمني الدولي:

ضرورة التعاون الأمني الدولي لقد أثبت الواقع العملي أن الدولة أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة. لذلك أصبحت الحاجة ماسة إلى

وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من وجه العدالة[21].

ب- المساعدة القضائية الدولية:

فتحديث آليات التعاون القضائي دوليا في المادة الجنائية يبدأ بخطوة أولى غايتها ضرورة تطوير القوانين الوطنية على نحو أكثر شمولية ومرونة حتى تواكب القوانين الوطنية حركة التشريع الدولية بشأن مكافحة الجريمة، وأن توثق التعاون بين أجهزة التنفيذية للدول وتنشئ أجهزة متخصصة لمواجهة الإجرام المنظم، و أن تصوغ نظرية متكاملة تستفيد من التطور التكنولوجي في إجراءات جمع الأدلة وتبادل المعلومات، للتصدي للمنظمات الإجرامية، التي تعمل بأسلوب علمي مدروس على تشتيت الأدلة والتخلص منها مما يستدعي تطوير التعاون القضائي في مختلف مراحله ، بما فيها مرحلة تنفيذ الأحكام[22].

ج- تكريس المشرع الجزائري لمبدأ التعاون الدولي والمساعدة القضائية للأمن السيبراني:

بالنسبة للمشرع الجزائري تؤكد المادة (16) من القانون 09-04 سالف الذكر في هذا الجاني على أنه وفي إطار التحقيقات والتحريات التي تمت مباشرتها بخصوص الجرائم الإلكترونية، فيمكن للسلطات القضائية المختصة تبادل المساعدة القضائية على المستوى الدولي قصد جمع الأدلة الخاصة بالجريمة الإلكترونية على أساس ما تشكله هذه الجرائم المستحدثة من صعوبات تقنية بالغة على مستوى كشفها وإثابتها وملاحقة مرتكبيها، إذ لا يمكن لدولة بمفردها القيام بذلك. ونظرا لحالة الاستعجال التي تتطلبها إجراءات التحقيق لجمع الأدلة الخاصة لهذا النوع من الجرائم المستحدثة وما يتطلبه من سرعة لاتخاذ هذه الاجراءات، أقر المشرع قبول طلبات المساعدة القضائية حتى وإن جاءت عن طريق وسائل الاتصال السريعة كالبريد الإلكتروني أو الفاكس بشرط التأكد من صحتها فقط[23]، وتخضع لمبدإ المعاملة بالمثل، احتراما لمبدأ سيادة الدولة حسب المادة17 من القانون 09-04 السالف الذكر[24].

وكما هو معروف لاتستطيع الدولة لوحدها مواجهة الاجرام السيبراني مهما بلغت من تطور في مجال الامن السيبراني، ولا سبيل للمكافحة هذا النوع من الاجرام المستحدث إلا نهج التعاون الدولي خاصة التعاون القضائي الدولي والمساعدة القضائية، وقد نصت على ذلك إتفاقية بودابست لمكافحة الإجرام السيبراني لسنة 2001، وأيضا الاتفاقية العربية لمكافحة تقنية المعلومات2010، اللتان حرصتا على التعاون الدولي وكيفية التصدي للإجرام السيبراني وخاصة إتفاقية بودابست 2001 التي تعتبر إقليميا، لكن هي ذات طابع دولي وهي مصدر ومرجع لدول في رسم سياسة التصدي لهذه المخاطر التي باتت تهديد حقيقي للدول والافراد

2- التدابير الهيكلية لفعالية الأمن السيبراني:

عكف المشرع الجزائري في محاربته للجريمة الإلكترونية بإنشائه لعدة هياكل وظيفتها مكافحة الجريمة السيبرانية نذكر منها:

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال: نصت على إنشاء هذه الهيئة المادة 13 من القانون 09/04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها « **تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته. تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم** »، أما مهامها فقد أوردتها المادة 14 من نفس القانون[25].

ومن مهامها حسب المادة 04 من المرسوم الرئاسي رقم: (21-439)، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي بعدها حول الإشراف على الهيئة إلى أمانة رئاسة الجمهورية، ومن أهم إختصاصاتها مبينة كالتالي[26]:

1- الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال؛
2- مكافحة كافة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال؛
3- تبادل المعلومات مع الدول لأجل تعزيز التعاون الدولي والمساعدة القضائية.

ب- الهيئات القضائية الجزائية المتخصصة :

يقصد بها الأقطاب الجزائية المتخصصة المنشاة بموجب القانون 14-04 المؤرخ في 10 نوفمبر 2014، وتختص هذه الجهات القضائية بموجب المواد 37-40-329 من قانون الإجراءات الجزائية بالنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى الصلاحيات الأخرى الممنوحة للجهات القضائية او للضبطية القضائية في اطار معالجة مثل هذه الجرائم .

ج- جهازي الأمن الوطني والدرك الوطني :

حيث سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني التي إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توفر على هاذين الجهازين من مخبرين علميين للشرطة العلمية والتقنية يتوفران على أحدث الأجهزة ذات تكنولوجيا متطورة لكشف هذا النوع من الإجرام[27].

د- المعهد الوطني للأدلة الجنائية على الإجرام :

يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية ودائرة الإعلام الآلي والإلكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات[28].

يبدو أن الجزائر وتشريعاتها الموضوعية والإجرائية تسعى جاهدة للقضاء على أثار هذا النوع من الإجرام بشتى الطرق والأساليب دون الإصطدام بجدار حقوق الإنسان التي صانها دستور 2020 في مواده والحرص على تطبيقها وإحترام الحياة الخاصة للفرد من أجل التكفل بحياة كريمة مصونة.

خاتمة:

على ضوء ما تقدم خلصنا في هذه الورقة البحثية إلى أنه لابد على الدول والأفراد على حد سواء الاهتمام بالأمن السيبراني خصوصا أننا في زمن الذكاء الإصطناعي، ولاخيار أخر للأمن السيبراني في مواجهة التعديات السيبرانية والإجرام الإلكتروني، والجزائر من خلال إنتهاجها في سياستها الجنائية للتصدي المزدوج للجريمة الالكترونية سواء بالقوانين التقليدية العامة أو بنصوص الخاصة لكل الميدان، بالرغم من المجهود التي تبذله إلا أنها مازالت بعيدة في رسم سياسة جنائية عامة لمواجهتها، لأن هناك عدة عوائق تقف حاجزا في مواجهة الإجرام السيبراني خاصة عند إصطدام الإجراءات المستحدثة في القانون الإجراءات الجزائية بإحترام حقوق الإنسان أيضا عدم الإنضمام للإتفاقيات الدولية خاصة إتفاقية بودابست 2001 الخاصة بمكافحة الإجرام السيبراني **وعليه نقترح بما يلي:**

1- دعوة المشرع الجزائري لتدارك النقائص في القوانين الخاصة بالجريمة الإلكترونية والتعجيل بسن نصوص قانونية تتعلق بالتزوير الإلكتروني خاصة وأن الإتفاقية العربية لمكافحة جرائم تقنية المعلومات2010 تطرقت لها وأن الجزائر صادقت عليها.
2- وضع لجنة قانونية لصياغة النصوص قانونية تتلائم وتتناسب والتطورات التي تعرفها الجريمة الإلكترونية.
3- على المشرع ضبط هذا النوع من الإجرام بقانون خاص وبمحاكم خاصة وتدريب القضاة واعوان الضبطية القضائية على هذا النوع من الإجرام.
4- التشجيع على العمل مع الدول لتقوية التعاون الدولي والمساعدة القضائية لمكافحة الإجرام الإلكتروني وخاصة مع الدول المتقدمة التي لها خبرة في هذا المجال.
5- ضرورة خلق ثقافة سيبرانية لدى أفراد المجتمع والمؤسسات الاقتصادية والمالية ودعوتهم إلى الإستخدام الحسن والجيد لوسائل تكنولوجيات المعلومات والإتصال.
6- على المشرع ترجمة نصوص الإتفاقيات الدولية التي لها علاقة بهذا النوع من الإجرام وتجسيدها في نصوصة الداخلية والإستفادة من مضمونها خاصة إتفاقية بودابست2001، والإتفاقية العربية لمكافحة جرائم تقنية المعلومات2010.
7- دعوة الجامعات والمعاهد لتنظيم تظاهرات وملتقيات للتحسيس بأهمية الأمن السيبراني في دحر الجرائم الإلكترونية.

قائمة المصادر والمراجع:

الوثائق القانونية:

1- المرسوم الرئاسي رقم 21-439، المؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج. ر. ج العدد86، بتاريخ 11 نوفمبر سنة 2021، ص5.

2- القانون 06-23، المؤرخ في 20 ديسمبر 2006، الذي يعدل ويتمم قانون العقوبات المعدل والمتمم (الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، الصادر في الج.ر رقم 84، المنشور بالج. ر.ج عدد 49 مؤرخة في 11 يونيو 1966، ص702)، المنشور بالج.ر.ج بتاريخ 24 ديسمبر سنة 2006.

3- القانون 04-15، المواد من 394 مكرر إلى 394 مكرر 7 ، المؤرخ في 10 نوفمبر 2004، الصادر في الج.ر.ج رقم: 71، المتضمن تعديل قانون العقوبات لسنة 2004، ص. ص: 11 و12.

4- الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات المعدل والمتمم، المنشور بالج.ر.ج عدد 49 مؤرخة في 11 يونيو 1966، الصفحة 702.

5- القانون رقم 06 – 22، المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الصادر في الج.ر.ج عدد رقم 84، المنشور بالج.ر.ج بتاريخ 24 ديسمبر سنة 2006، ص4.

6- القانون رقم 09 - 04، المؤرخ في 14 شعبان عام 1430، الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج.ر.ج العدد 47 بتاريخ 16 غشت سنة 2009.

7- القانون رقم 18-04، المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج.ر.ج العدد 27، بتاريخ 13 مايو 2018، ص 03.

الكتب:

8- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات- قانون العقوبات- قانون الإجراءات الجزائية- قوانين خاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019.

الرسائل والأطروحات الجامعية:

9- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر1 بن يوسف بن خدة ،2018..

10- بلال بن جامع، الجرائم المعلوماتية على شبكة الانترنت دراسة حالة جامعة عبدالحميد مهري قسطنينة2، رسالة دكتوراه، معهد علم المكتبات والتوثيق، جامعة عبدالحميد مهري قسنطينة2، 2016-2017.

المقالات:

11- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية-جامعة العربي التبسي، تبسة، الجزائر، المجلد01، العدد01، 2019، ص103.

12- أسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد03، العدد03، 2018،

13- جمال بوازدية، الإستراتيجية الجزائرية في مواجهة السيبرانية" **التحديات والأفاق المستقبلية**"، مجلة العلوم القانونية والسياسية المجلد10 ،العدد01، أفريل2019.

14- سمير بارة، الأمن السيبراني في الجزائر السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني، المجلد02، العدد04، 2017،.

15- عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد09، العدد03، 2020

16- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية العلوم والدراسات الانسانية بالغاط، جامعة المجمعة، المملكة العربية السعودية، المجلد/14العدد02، 2016،

17- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، المركز الجامعي إيليزي، الجزائر، المجلد02، العدد01، ديسمبر 2017.

18- مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، مجلة القانون المجلد09، العدد01، 2020.

أعمال ملتقى أو مؤتمر:

19- أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة في إطار المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في الفترة من 28 إلى 29 أكتوبر 2009.

الهوامش:

(1) - عبد العزيز بن فهد بن محمد بن داود، الجرائم السيبرانية: دراسة تأصيلية مقارنة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المجلد09، العدد03، 2020، ص148.

(2)- إدريس عطية، مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري، مجلة مصداقية، كلية الحقوق والعلوم السياسية-جامعة العربي التبسي، تبسة، الجزائر، المجلد01، العدد01، 2019، ص103.

(3)- المرجع نفسه، ص104.

(4)- جمال بوازدية، الإستراتيجية الجزائرية في مواجهة السيبرانية" التحديات والأفاق المستقبلية"، مجلة العلوم القانونية والسياسية المجلد10،العدد01، أفريل2019، ص1267.

(5)- أنظر المادة10/3 من القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، الصادر في الج.ر.ج العدد 27، بتاريخ 13 مايو 2018، ص 03.

(6)- الأمر رقم 66-156، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات المعدل والمتمم، المنشور بالج.ر.ج عدد 49 مؤرخة في 11 يونيو 1966، الصفحة 702.

(7) - انظر المواد من 394 مكرر إلى 394 مكرر 7 من القانون 04-15، المؤرخ في 10 نوفمبر 2004، الصادر في الج.ر.ج رقم: 71، المتضمن تعديل قانون العقوبات لسنة 2004، ص. ص: 11 و12.

(8)- بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتوراه علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر1 بن يوسف بن خدة ،2018، ص154.

(9)- أنظر المادة 02/أ من القانون رقم 09 - 04، المؤرخ في 14 شعبان عام 1430، الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج.ر.ج العدد 47 بتاريخ 16 غشت سنة 2009.

(10)- بلال بن جامع، الجرائم المعلوماتية على شبكة الانترنت دراسة حالة جامعة عبدالحميد مهري قسطنينة2، رسالة دكتوراه، معهد علم المكتبات والتوثيق، جامعة عبدالحميد مهري قسنطينة2، 2016-2017، ص116.

(11) - سمير بارة، الامن السيبراني في الجزائر السياسات والمؤسسات، المجلة الجزائرية للآمن الإنساني، المجلد02، العدد04، 2017، ص263.

(12)- المرجع نفسه.

(13)- إدريس عطية، مرجع سابق، ص105.

(14) - المرجع نفسه.

(15)- المرجع نفسه.

(16)- القانون 06-23، المؤرخ في 20 ديسمبر 2006، الذي يعدل ويتمم قانون العقوبات المعدل والمتمم (الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966، الصادر في الج.ر رقم 84، المنشور بالج روج عدد 49 مؤرخة في 11 يونيو 1966، ص702)، المنشور بالج.ر.ج بتاريخ 24 ديسمبر سنة 2006.

(17)- القانون 16- 02 المتضمن تعديل قانون العقوبات.

(18)- مراد مشوش، الجريمة المعلوماتية في ظل قانون العقوبات وقانون الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال، مجلة القانون المجلد09، العدد01، 2020، ص112.

(19)- القانون رقم 06 – 22، المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، الصادر في الج.ر.ج عدد رقم 84، المنشور بالج.ر.ج بتاريخ 24 ديسمبر سنة 2006، ص4.

(20)- أسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد03، العدد03، 2018، ص364.

(21)- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية العلوم والدراسات الانسانية بالغاط، جامعة المجمعة، المملكة العربية السعودية، المجلد/14العدد02، 2016، ص61. ص 52.

(22)- أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة في إطار المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون، أكاديمية الدراسات العليا، طرابلس، ليبيا، المنعقد في الفترة من 28 إلى 29 أكتوبر 2009،ص10.

(23)- يزيد بوحليط، الجرائم الإلكترونية والوقاية منه في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات- قانون العقوبات- قانون الإجراءات الجزائية- قوانين خاصة، دار الجامعة الجديدة، الإسكندرية، مصر، 2019،ص362.

(24)- المرجع نفسه.

(25)- أسمهان بوضياف، مرجع سابق، ص365.

(26)- المرسوم رئاسي رقم 21-439، مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالج. ر. ج العدد86، بتاريخ 11 نوفمبر سنة 2021، ص5.

(27)- محمد السعيد زناتي، الجريمة المعلوماتية في ظل التشريع الجزائري والاتفاقيات الدولية، مجلة إيليزا للبحوث والدراسات، المركز الجامعي إيليزي، الجزائر، المجلد02، العدد01، ديسمبر 2017، ص34

(28)- أسمهان بوضياف، مرجع سابق، ص 370.