وزارة التعليم العالي والبحث العلمي

جامعة الشهيد حمه لخضر- الوادي

كلية العلوم الإنسانية والإجتماعية

مخبر التنمية الإجتماعية وخدمة المجتمع

الملتقى الوطني

الأمن السيراني

ورهانات الأمن الشامل في الجزائر

المحور: جهود الدولة الجزائرية في مواجهة تهيدات الأمن السيبراني

سياسيا/قانونيا/إستراتيجيا

يوم14/13 ماي2024

إستراتيجية المشرع الجزائري في مواجهة الجرائم السيبرانية التي تهدد أمنها السيبراني

من إعداد/أ:هادفي تاج الدين

التخصص: علم إجتماع الحضري

جامعة الشهيد حمه لخضر بالوادي

الإيمايل:tajmoumni60@gmail.com

أ/ هادفي محمد عبد المناف

جامعة المنار- تونس

الإيمايل:hadfi.manef@gmail.com

الملخص: إهتمت هذه الدراسة بالإستراتيجية التي وضعها المشرع الجزائري في التصدي للجرائم السيبرانية التي تهدد أمنها السيبراني، والتي تركت أثارها خاصة على مستوى الأمن الوطني، لأن الجزائر وبموقعها الإسترتيجي تعد مجالا مفتوح الإتجاهات ومركزا حيويا مغاربيا، ومتوسطيا، وإفريقيا، وهذا بدوره أدى إلى إختراقات وتجسسات عديدة بداية من أمن الأشخاص، مما جعل حياتهم وخصوصياتهم ملاذ للإبتزاز، سواء كان مسئولا أو مواطنا عاديا، ليتعدى الأمر بالتجسس والتهديدات التي لم تسلم منها المؤسسات الحكومية والأمنية والعسكرية في البلاد، وهذا مما أدى إلى دق ناقوس الخطر لإعادة وضع حواجزتقنية لمنع

هذه التجاوزات والهجمات التي تمس بالأمن الوطني، لذلك نطرح الإشكالية التالية: ماهي الإستراتيجية القانونية التي وضعها المشرع الجزائري لمواجهة تهديدات الجرائم السيبرانية ومخاطرها ؟

الكلمات المفتاحية: المشرع الجزائري، الأمن السيبراني، الجريمة السيبرانية، المخاطر.

Abstract: This study focused on the strategy developed by the Algerian legislator in confronting cybercrimes that threaten its cybersecurity, which left its effects, especially at the level of national security, because Algeria, with its strategic location, is considered an open field and a vital center in the Maghreb, the Mediterranean, and Africa, and this in turn led to hacking and espionage. Many things, starting with the security of people, making their lives and privacy a haven for blackmail, whether an official or an ordinary citizen It goes beyond espionage and threats from which governmental, security and military institutions in the country were not spared. This led to sounding the alarm to re-establish technical barriers to prevent these transgressions and attacks that affect national security. Therefore, we pose the following problem: What is the legal strategy that the Algerian legislator has developed to confront the threats of cybercrimes? And its risks?

Keywords: Algerian legislator, cybersecurity, cybercrime, risks.

مقدمة:

لقد شهد المجتمع الدولي في منتصف القرن العشرين ثورة تكنولوجية هائلة، فكان لها أثر إيجابيا على حياة الأشخاص والدول، لكن من الناحية السلبية فقد أفرز الإستخدام السيئ للأنظمة المعلوماتية للشبكات العنكوبتية العديد من الجرائم والتهديدات التي تستخدم فيها الأساليب التقنية العالية بفعل التطور التكنولوجي والتي مست عديد من الأفراد والمؤسسات بجميع أشكالها المادية والإلكترونية كالتجسس والتخريب والتهديد وكذلك الهجمات اللاذعة في عالم "يشهد تحولا رقميا متسارعا.... مما وصل إلى الأمر بالتجسس على الأمن الوطني والدولي، وعليه فالجزائر وموقعها الإستراتيجي فقد عرفت أيضا مخاطر سيبرانية من طرف دول خارجية التي تحاول تحديد أمنها وتعطل إستقراره إلى جانب القرصنة وعلاقتها بالإجرام والتجسس والتخريب، وهذا بأرقام مخيفة ومرعبة من حيث العدد الكبير للتهديدات المتعلقة بالأمن السيبراني باستخدام أدوات متطورة، حيث تترتب عن هذه الهجمات والتهديدات خسائر مادية ومعنوية معتبرة، وللتصدي لهذه التجاوزات والإختراقات فقد وضعت الحكومة الجزائرية

إستراتيجية محكمة لحماية منظومتها المعلوماتية، وتأمينها، وكذا الاستجابة للحوادث السيبرانية عن طريق التحقيق والمساعدة والتحسيس بصفة دورية، وهذا بإستخدام العديد من القوانين والتصورات بإستراتيجية الأمن السيبراني والتي ترتكز أساسا على بناء حواجز وجدران تقني لمنع هذه الهجمات، وبالتالي التحكم في انظمة المراقبة لحماية المنظومة المعلوماتية للمؤسسات والأشخاص، وهذا الأمر جعل الدولة الجزائرية حارسة على تأمين أنظمتها المعلوماتية، خاصة الحيوية منها، وبناءا على ما تقدم في هذا الطرح سوف نعالج الإشكالية من خلال سؤال التالي:

ماهي الإستراتيجية القانونية التي وضعها المشرع الجزائري لمواجهة تهديدات جرائم أمنها السيبراني ومخاطره؟

- وعليه في هذه الدراسة سوف نحاول التطرق إلى موضوع الأمن السيبراني عامة، وذلك من خلال تناول العناصر التالية: خصائص الجرائم السيرانية، والإجرام السيبراني، وكذلك دوافع الإجرام السيبراني، وأبعاد الأمن السيبراني، وأهم وسائل تهديدات الجرائم السيبرانية، وكذلك أبرز تهديدات الإجرام السيبراني التي تواجه الجزائر، وفي الأخير إستراتيجية الدولة الجزائرية في مواجهة جرائم الأمن السيبراني وتهديداته.

1-مفهوم الأمن السيبراني بإختصار:

الأمن السيبراني هو عبارة عن مجموعة من الوسائل التقنية والتنظيمية المستخدمة لحماية الأنظمة والشبكات الإلكترونية من التهديدات والهجمات السيبرانية المتطرفة.

2-**مفهوم الإجرام السيبراني:** هو كل عمل يريد به الإنسان الوصول إلى تخريب وعرقلة شبكات الاتصال الخاصة بمكونات الحاسب المادية والمعنوية سوى للإشخاص أو المؤسسات.(الشوابكة،2011، ص09)

وتعرف بأنها " نوع من السلوك الغير مشروع يرتكب بإستخدام الحاسب عبر أجهزة إلكترونية بهدف إلحاق الضرر بالأفراد أو المؤسسات من خلال الولوج إلى النظم المعلوماتية الخاصة بهم". **(- Klaus, , 1993, p.61.)**

ومن الناحية القانونية العامة (هي القيام بفعل أو تركه بإرادة جنائية، لإضرار أي مصلحة جنائية ما حماها القانون بمواد تجرمه وتعاقب عليه جزائيا) **(سامي، 2007، ص 134)**

وعرفها قانون المشرع الجزائري بموجب المادة 01 من القانون رقم 09-04 بمصطلح " المساس بأنظمة المعالجة الألية للمعطيات "

وعرفها: " بأنها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصالات الالكترونية من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها"(**زيدان،2011، ص 42.)**

3-خصائص الجرائم السيبرانية:

1-**جرائم مختفية:** يصعب اكتشافها، وهذا راجع لضعف القدرة الفنية للضحية من جهة ، ومن جهة أخرى خبرة المجرم الفنية والعلمية المتقدمة لقدرته على إخفائها.

2-**جرائم لها سرعة التنفيذ:** قد لا تتطلب وقت في الإعداد قبل التنفيذ، وفي معظم الأحيان يكون إرتكابها خلال جزء من الثانية.

3-**جرائم عن بعد:** ينفذ المجرم جريمته وهو بعيدا عن المجني عليه وحتى في دول بعيدة.

4- **جرائم ناعمة:** أي لا تمارس بالعنف، ولا بأدنى مجهود عضلي، عكس الجرائم التقليدية.

5- **جرائم عابرة للحدود:** ليس لها حدود جغرافية للدول، وهذا راجع لإرتباط العالم بشبكة أنترنت موحدة .

6- **جرائم يصعب إثباتها:** جرائم لا يمكن إثباتها، ومن الصعب حصرها في مكان معين بحيث لا تترك أثر ولا تشاهد بالعين المجردة، وهذا راجع لعدة أسباب:

- لا تترك هذه الجريمة أثر بعد إرتكابها من المجرم.
- تعتمد على ذكاء خارق حين إرتكابها.
- تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها.
- تعتمد على الخداع في إرتكابها، والتمويه على مرتكبيها.

صعوبة الإحتفاظ الفني لأي أثر منها. **(القرعان، 2217، ص 11.)**

4- دوافع الإجرام السيبراني:

نلاحظ بأن المجرم السيبراني يتميز بمهارات عالية عندما يريد تنفيذه أي إجرام سيبراني، فهو يعتمد على قدراته العقلية بالذكاء والدهاء ومعرفة الطرق السيبرانية لإتلاف البرامج واختراق

الحواجز الأمنية ، ولعل الدافع للمجرمين السيبرانيين قد يكون بدافع المال بالدرجة الأولى، وهذا بلجوئهم إلى الطرق الغير مشروعة، وذلك بسبب ما يعانوه من البطالة ، وقد يكون بدوافع عقائدية وسياسية ، وقد يكون بدوافع شخصية كقيام الموظف بالإنتقام من المؤسسة أو الشركة التي قامت بفصله ، أو للتجسس وانتهاك خصوصية الأشخاص أو المؤسسات.

5-**أبعاد الأمن السيبراني:** هناك العديد من الأبعاد للأمن السيبراني، ونحصرها فيمايلي:

أ- البعد القانوني: : أكد المستشار القانوني للجنة الدولية للصليب الأحمر، لوران جيسل بأن المادة 36 من البروتوكول لعام 1977 تلزم الدول بتصنيع الأسلحة الجديدة وفقاً للقوانين الدولية، إلا أن هناك قواعد أخلاقية وإنسانية عامة يجب الالتزام بها، وقد كشفت التسريبات عن إنفاق الحكومة الأمريكية مبالغ كبيرة على العمليات السيبرانية في عام 2011، وقد أعلنت أكثر من 130 دولة عن تخصيص أقسام قانونية خاصة بالتهديدات السيبرانية. **(المجذوب، 2014، ص58)**

ب- البعد الإقتصادي: ويكمن ذلك في حماية المورد الإقتصادي، وتفادي خسارته أو فقدانه بحيث تعمل المؤسسة جاهدة على حماية الموجودات الاقتصادية من الأضرار الناجمة عن عدم كفاية الأمن والإحتمال التعرض لهجمات أو أي إختراقات التي تضعف القيمة الأقتصادية لأي مؤسسة أو دولة ما. **(العوادي، 2016، ص 06)**

ج - البعد الإجتماعي: إن تقرير مؤسسة Sosial Are we يشير إلى أن حوالي 2.5 مليار شخص، أي ما يعادل 35%من سكان العالم، يستخدمون الإنترنت، ويظهر لها دورًا هامًا في تعبير المواطنين عن آرائهم وتطلعاتهم في مختلف المجالات، بينما تمثل الأخرى تهديدات، مثل الإرهاب ونشر الفكر المتطرف وتجنيد الشباب والترويج للاتجار بالممنوعات.

البعد السياسي: ويكمن هذا بمسؤولية الدولة وسيادتها في تحقيق الأمن السيبراني، بحيث تتطلب جهوداً شاملة، فلا يجب أن تقتصر على دعم البحث والتطوير فحسب، بل يجب أيضاً تعزيز الثقافة الأمنية وتنفيذ استراتيجيات لإدارة الوقاية والإبلاغ وتبادل المعلومات وزيادة الوعي بأفضل الممارسات وإدارة المخاطر. **(حمدون، 2006، ص 15)**

هـ- البعد العسكري: تطوّرت بدايات الإنترنت في بيئة عسكرية، ثم امتدّت إلى البيئة الأكاديمية والأبحاث التي خدمت تطوير القدرات العسكرية والإنجازات العلمية. تتمثل خطورة

الهجمات السيبرانية في التجسس والسرقة والاختراق، حيث تؤدي إلى نتائج مادية مثل اندلاع صراعات مسلحة. **(جبور، 2012، ص16)**

6- وسائل تهديدات الجرائم السيبرانية:

أ- **التجسس التقني والمعلوماتي:** تشكل أسلحة حرب سيبرانية مهمة تهدد الدول، وتتضمن أشكالًا متعددة مثل التجسس على المعلومات من أجهزة الحواسيب والأقمار الصناعية والهواتف المحمولة. **(عبد الصادق،2017، ص02)**

ب- **الإختراق الإلكتروني:** هي جريمة الكترونية تشمل إنشاء نظام أو برنامج للاستيلاء على معلومات الخصم وتدميرها، مع فساد النظام الحاسوبي والآلي، بهدف التفوق في الجوانب الأمنية والعسكرية والاقتصادية والسياسية.**(الشهري نوال، 2024)**

القرصنة الإلكترونية: هي سلاحًا فتّاكًا في الفضاء الرقمي، حيث يتضمن هذا السلاح تقنيات الصراع الإلكتروني الحديثة، وتعتمد على تجنيد أفراد ماهرين في التعامل مع الحواسيب والأنظمة التقنية، لاختراق الأنظمة التكنولوجية، يُطلق على هؤلاء الأفراد الماهرين باسم "الهاكرز"**(جلعود، ،2013، ص111)**

ت- **الرسائل الصامتة:** هي برامج تقنية تستخدم في الهواتف المحمولة من الجيل الرابع والخامس، تُرسل دون أن يلاحظ صاحب الهاتف وتُساعد على تحديد موقعه بدقة.

ث- **شبكات التواصل الإجتماعي:** هي منصات رقمية تربط الأفراد والمجتمعات مع بعضها البعض في مجالات مثل العمل والدين وغيرها، تجمع بين مختلف الفئات العمرية والاجتماعية والاقتصادية والثقافية والتعليمية، وتلعب دوراً هاماً في الصراع التقني عبر الإنترنت بما يسمى الجرائم السيبرانية.

ج- **الحقيبة الكهروستاتيكتة:** هي عبارة عن تكنولوجيا عسكرية تُشكل أجهزة صغيرة تولّد نبضات كهرومغناطيسية فائقة القوة، تُستخدم لتعطيل الوحدات الإلكترونية في أي نظام أو محطة إرسال، مما يؤدي إلى فقدان قدراتها العلمية والإنتاجية والتشغيلية.

ح- **الأسلحة النانو تكنولوجية:** تشمل تصميم أجهزة دقيقة جدًا في المجال العسكري تتسلل إلى أنظمة الحواسيب والتقنيات، حيث تُستخدم لتدمير البنية المعلوماتية بسرعة عالية. مثل آليات عمل الفيروسات، بواسطة ما يُعرف بالميكروبات الرقمية.

7-أبرز تهديدات الإجرام السيبراني التي تواجهه الجزائر:

أ- **التهديدات السياسية:** الدراسات الأمنية تميز بين أمن النظام وأمن المجتمع، حيث تركز الدول التسلطية على حماية النظام، بينما تسعى الدول المدنية لتحسين مبادئ الديمقراطية في بعض الأنظمة التسلطية، ويمكن للنظام أن يشكل تهديدًا للمجتمع خلال الأزمات، مما يستدعي اتخاذ إجراءات أمنية قد تؤثر سلباً على أمن المجتمع.(**الخلفي،2024**)

ب- التهديدات الإجتماعية: إن تأثيرات العولمة جعلت هذه القضايا تشكل تهديداً جنائياً حقيقياً للأمن القومي، كما تمثل رغبات المشروع المجتمعي تحدياً حقيقياً للأمن الاجتماعي والثقافي، حيث تستخدم الهوية والوطنية لأغراض سياسية سواء من قبل النخب الحاكمة أو القوى المعارضة. التعامل السلبي مع هذه المكونات يؤدي إلى عدم تجسيد المشروع المجتمعي، ويعيق جهود تحديث الأمن والمجتمع الجزائري. لحماية الأفراد والمؤسسات والدولة من تهديدات الجرائم السيبرانية.

ج- التهديدات الإقتصادية: إن التحديات الاقتصادية تتجلى في قلة تنوع مداخيل الجزائر والاعتماد الكبير على القطاع النفطي، إذا استمرت الجزائر في تصدير النفط بهذا الوتيرة، فقد لا يكون هناك ما يتبقى للتصدير بعد ربع قرن من الآن، مما يكشف عن فجوة في الاستراتيجية الاقتصادية لتأمين مستقبل الأجيال القادمة.

د- التهديدات التكنولوجية: في مجال التهديدات التكنولوجية، يشكل التقدم السريع في هذا المجال تهديداً للأمن القومي الجزائري، حيث تؤثر هذه التهديدات على المؤسسات والأفراد على حد سواء، وتشمل هذه التهديدات الجرائم المتعلقة بالمواقع المعادية، وخاصة المواقع السياسية التي قد تكون مصدرًا للأخبار الفاسدة التي تفتح فجوة بين النظام السياسي والمواطنين. **(زياني،2014، ص ص.294-293)**

أهم الجرائم السيبرانية التي تعرضت لها الجزائر:

أ- **الإرهاب السيبراني:** يُعَد من بين التهديدات والجرائم الرئيسية للأمن الجزائري في عصر التكنولوجيا الحديثة، حيث تشكل وسائل التواصل الاجتماعي والمواقع الإلكترونية منبرًا لنشر الأفكار المتطرفة والعنيفة، ويتضمن الإرهاب الإلكتروني العديد من المخاطر مثل التهديدات بالعنف والتخريب والتخويف باستخدام الوسائل الإلكترونية للإضرار بالأفراد والمجتمع بأكمله. **(بن مرزوق، د.س، ص67)**

ب- القرصنة السيبرانية: سجلت الجزائر أكثر من 900 جريمة إلكترونية في عام 2017، حسب مركز الوقاية ومكافحة الجريمة الإلكترونية، التابع لمصالح الدرك الوطني، وتشمل هذه الجرائم المساس بحياة الأشخاص، والتهديد والابتزاز، والتشهير بالإرهاب، وقرصنة البيانات ونظم الكمبيوتر، وسرقة الهوية وتحريض القصر على الدعارة.

ويمكن أن نجمل أخطر التهديدات الالكترونية فيما يلي: تعطيل الخدمة، إتلاف المعلومات أو تعديلها، التجسس على الشبكات، وعليه سجلت الجزائر أزيد من 900 جريمة إلكترونية خلال سنة 2017 حسب ما أعلنه مركز الوقاية ومكافحة الجريمة الإلكترونية.

8-**استراتيجية الدولة الجزائرية في مواجهة جرائم الأمن السيبراني :** تتبوأ الجزائر موقعًا مهمًا في مواجهة جرائم الأمن السيبراني، حيث اتخذت خطوات جادة لمواجهة الزيادة الملحوظة في الجرائم الإلكترونية، بتجهيز أكثر من 24 ألف مهندس وتقني مختص في الأمن السيبراني، وبدء تدريب أعداد أخرى ذات كفاءة عالية في هذا المجال، كما تعاقدت الجزائر مع شركات عالمية مثلHuawei ، Microsoft، Cisco، في إطار استراتيجيتها الوطنية لتطوير الاقتصاد الرقمي والأمن السيبراني.

وعليه تمتلك الجزائر جهوداً مكثفة لحماية نظامها السيبراني، وتعمل على تطوير البنية الجهود بتشديد الرقابة وتطبيق التشريعات والتقنيات الملائمة لمواجهة التهديدات الإلكترونية، وقد تمكن الجيش الوطني الشعبي من مواكبة التطورات التكنولوجية وتأمين نطاقه المعلوماتي وأمنه السيبراني من خلال الناشطين فيه، ومن خلال التركيز على إستراتيجية محكمة تعتمد فيها على مرتكزات رئيسية وقوفا ضد الجرائم السيبرانية وهي:

أ- نص القانون الجزائري: تمحور التركيز أساساً حول اتخاذ التدابير القانونية في مكافحة الجرائم السيبرانية ، كما يظهر من صدور القانون رقم -09 04 بتاريخ 05أوت 2009، الذي يحدد القواعد للوقاية من جرائم التكنولوجيا الإعلامية والاتصال، بما في ذلك الإجراءات المتاحة لمراقبة الاتصالات الإلكترونية، وعليه قد أخص المشرع الجزائري بتنظيم قوانين عامة عامة وخاصة، حيث تمثلت القوانين العامة بناءا على ما ورد في المادة 4 التي نصت على ما يلي: (الجمهورية الجزائرية،2009،ص 06)

- تُعتبر الإجراءات الوقائية ضرورية لمكافحة الأنشطة المصنَّفة كجرائم إرهابية أو تخريبية، وكذلك لمواجهة الجرائم التي تهدد أمن الدولة.

– إذا كانت هناك معلومات تشير إلى احتمال تعرض منظومة معلوماتية لاعتداء يشكل تهديدًا للنظام العام، أو الدفاع الوطني، أو مؤسسات الدولة، أو الاقتصاد الوطني.

– تتطلب عمليات التحقيق القضائي في بعض الأحيان استخدام المراقبة الإلكترونية، عندما يكون من الصعب الوصول إلى نتائج تُعزز جهود البحث الحالية، وذلك في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

– تم إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وفقًا للمادة 13، وصدر المرسوم الرئاسي رقم 261–15 المؤرخ في08 أكتوبر 2015 لتنظيم عمل هذه الهيئة، ويحدد هذا المرسوم التشكيلة والتنظيم وكيفية سير العمل داخل الهيئة، بحيث تتضمن مهام الهيئة، كما هو مذكور في المادة 4 من المرسوم، مع القيام بالأنشطة التي تهدف إلى الوقاية من هذه الجرائم ومكافحتها.

– يتضمن اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المرتبطة بتقنيات الإعلام والاتصال ومكافحته.

– تعزيز وتنسيق جهود الوقاية من الجرائم المرتبطة بتقنيات الإعلام والاتصال ومكافحتها.

– تقديم الدعم للسلطات القضائية ومصالح الشرطة القضائية في مكافحة الجرائم المرتبطة بتقنيات الإعلام والاتصال، بما في ذلك جمع المعلومات وتقديمها بمساعدة الخبراء القضائيين.

– المساهمة في تحسين القوانين المنظمة لمجال اختصاصها

– ضمان المراقبة الاحترازية للاتصالات الإلكترونية للكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والتي تهدد أمن الدولة، وذلك بموجب قرارات صادرة عن القاضي المختص، مع استثناء أي هيئات وطنية أخرى.

– تعزيز الدور في تدريب المحققين المتخصصين في التحقيقات التقنية المتعلقة بتقنيات الإعلام والاتصال.

– توسيع مشاركة فاعلين جدد من خارج الجهاز العسكري، الذين يستطيعون المساهمة في تعزيز عقيدة الدفاع الوطن فقد أصبح الفضاء السيبراني أحد أهم المجالات، حيث يحتل المرتبة الخامسة بعد الأرض والبحر والجو والفضاء، وبالتالي يشكل مجالاً حيويًا للانخراط والتأثير.

-تنظيم مديرية الاتصال والإعلام والتوجيه مع أركان الجيش الوطني الشعبي سلسلة من الندوات حول تداول المعلومات عبر شبكات التواصل الاجتماعي، وتحديات الجيش الوطني الشعبي، حيث تم التأكيد على ضرورة تعزيز الوعي الأمني والسيطرة على التقنيات الحديثة في إطار العقيدة الأمنية الجزائرية. (بوعلام، 2016، ص39)

كما كفل الدستور الجزائري خلال سنة 2016 بالتعديل الطارئ على حماية الحقوق الأساسية و الحريات الفردية، وذلك عن طريق أهم المبادئ الدستورية في مواده.

- **المادة38:** الحريات الأساسية وحقوق الإنسان والمواطنة مضمونة.

المادة44: حرية الإبتكار الفكري مضمونة للمواطن، أما حقوق المؤلف يحميها القانون

وتتمثل القوانين الخاصة التي أقرها المشرع الجزائري في مجال الجريمة الإلكترونية، وأهمها:

(القانون 15-04من الجريدة الرسمية رقم 14 المؤرخة في 7 مارس .2016)

أ- قانون البريد والاتصالات السلكية واللاسلكية: حيث نصت عدة مواد منه فيما يخص المجال السيبراني المادة 87، والتي نصت على سهولة التحويلات المالية الكترونيا، والمادة 2/84 على استعمال حوالات الدفع العادية والالكترونية، كما نصت المادة 105 على احترام المراسلات، أما المادة 127 بجزاء كل من يفتح أو يخرب بريد.

ب- قانون التأمينات: وقد نص هذا القانون على تنظيم الجريمة الالكترونية من خلال مؤسسات وهيئات الضمان الاجتماعي ،وذلك في عدة نصوص تخص بطاقة الكترونية.

ج- القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: حيث جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكل ماله علاقة بالمنظومة المعلوماتية.

كما تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة القانونية 394 مكرر بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية، وعقوبة الاشتراك في الاتفاق تكون نفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تكون العقوبة هي عقوبة الجريمة الأشد. **(بوغرارة، 2018، ص110)**

خاتمة:

لقد تبنت الحكومة الجزائرية استراتيجيات أمنية سيبرانية لمواجهة التهديدات الجرائمية في الفضاء الرقمي، التي تشكل تهديدًا للأفراد والمجتمع والأمن الداخلي، وهذا بإستخدام المجرمون أحدث التقنيات في تنفيذ هجماتهم، وبالتالي فإن الدولة اضطرت إلى مواكبة

التطورات في مجال السيبراني وتطوير القوانين والأنظمة اللازمة لمكافحة هذه الجرائم وفرض العقوبات على المتسببين بها، بالإضافة إلى الابتزاز والتهديد والتشهير، واختراق الخصوصية الشخصية عبر منصات التواصل الاجتماعي، ويتمثل هذا في نشر المعلومات الكاذبة والمضللة، بما في ذلك القرصنة والتحرش الإلكتروني، ورغم الجهود المبذولة في سبيل تحقيق ذلك إلا أن المراتب التي تحتلها الجزائر عربيا ودوليا تشير إلى أنها بحاجة إلى المزيد من الجهود لمواجهة الجرائم السيبرانية سواء على الأفراد أو المؤسسات، وهذا من خلال تفعيل الجهود التشاركية من فواعل أفراد المجتمع، وهذا يتمثل في:

– للقضاء على الجرائم السيبرانية يتطلب ضرورة نشر الوعي المجتمعي بخطورتها.

–تشجيع التكوين العلمي والجامعي المتخصص في دراستها من أجل إيجاد حلول متطورة لفك هذه الجرائم.

–العمل على تشجيع وسائل الإعلام، وذلك بفتح مواضيع متعلقة بهذه الجرائم الجرائم الخطيرة، وتوضيح أليات الوقاية منها.

– تمكين وحدات عسكرية وأمنية خاصة تتولى بالتعاون على المستوى الخارجي، مع الهيئات العاملة على مكافحة المخاطر والحد منها ومن أثارها.

–يجب الإستفادة من التجارب الدولية الرائدة في هذا المجال.

– كما أن للتنشئة الإجتماعية دورا مهم في مكافحة مختلف الجرائم السيبرانية، سواء التقليدية أو الإلكترونية، وهنا وجب الإهتمام بالأسرة، المدرسة، الجامعة، المسجد، وكذلك تنظيمات المجتمع المدني من أجل المشاركة معا في بناء مجتمع خال من التطرف والإرهاب.

قائمة المراجع:

1- محمد أمين الشوابكة، (2011)، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع.

2- عبد الستار فوزية،(1982) شرح قانون العقوبات، دارالنهضة، القاهرة.

3- Klaus TIEDEMANN,(1993) Fraude et autres délits d’affaires commis à l’aide d’ordinateurs électroniques, Dalloz, France.

4- سامي علي حامد عياد،(2007) الجريمة المعلوماتية وإجرام الأنترنت، دار الفكر الجامعي، دط، الإسكندرية،مصر.

5- زيدان ربيحة،(2011)،الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر.

6- القرعان محمود أحمد، (2017)، الجرائم الإلكترونية ، دار وائل للنشر والتوزيع، عمان ، ط1.

7- المجذوب طارق،(2014)"ساحة "خفية" لحرب "ناعمة" قادمة"!، منشورات الدفاع الوطني اللبناني، العدد ،89، لبنان
8- (العوادي أوس مجيد غالب،(2016)، الأمن المعلوماتي السيبراني، بيروت، مركز البيان للدراسات والتخطيط،.
9- حمدون توريه،(2006)، الأمن السيبراني في البلدان النامية، الاتحاد الدولي للاتصالات.
10- جبور منى الأشقر،(2012)، الأمن السيبراني التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية.
11- عبد الصادق عادل،(2017)، الحروب السيبرانية: تصاعد القدرات والتحديات للأمن العالمي، المركز العربي لأبحاث الفضاء الإلكتروني، د.ش، القاهرة.
12- الشهري نوال، حرب المعلومات، في مركز تميز الأمن المعلوماتي، (جامعة الملك سعود)، دن، من الرابط :
www.coeia.edu.sa/index.php/ar/assur_awess/data_privacy/1263_influance warfare.html_تاريخ التصفح 08/03/2024)
13- فاروق حسين،(1999)، فيروسات الحساب الآلي، العربية للطباعة والنشر، ط،1، القاهرة.
14- جلعود وليد غسان سعيد،(2013) دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، أطروحة ماجستير في التخطيط والتنمية السياسية، بكلية الدراسات العليا، جامعة نابلس، فلسطين.
15- الرسائل الصامتة،(2016) سلاح الرقابة السرية، 23 يونيو/ حزيران ، من الرابط : www.almaged.ps/3 ،تاريخ التصفح،2024/03/07.
16- شبكة النبأ المعلوماتية، حرب الفضاء والأقمار الصناعية، من رالرابط : www.annaba.org/nbanes/69/022/htmتاريخ التصفح 2024/03/19
17- الخلفي مصطفى، أزمة العلاقات المغربية الجزائرية ومشكلة الصحراء المغربية، الرابط : http://www.aljazeera.net.التصفح تاريخ:2024/03/08
18- زياني صالح، تحولات العقيدة الأمنية الجزائرية في ظل تنامي تهديدات العولمة، مجلة الفكر، عدد 5، د.س.ن، ص ص.294-293، الجزائر.
19- بن مرزوق عنتر، الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية، محاضرة مقدمة لطلبة جامعة محمد بوضياف المسيلة، كلية الحقوق والعلوم السياسية، د.س، ص67.
20- محمود خليل،50 ألف موقع الكتروني لداعش والإرهاب يحاصر الانترنيت، من الرابط : www.alittihad.ae/details.php=120lتصفح في تاريخ: 2024/04/09

21- فضيلة غاقلي،الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مركز جيل البحث العلمي، على الرابط.http://jilrc.com : التصفح في 2024/04/07

22- ب. بوعلام، (2016)،ملتقى حول الجيش الوطني الشعبي ورهانات تداول المعلومات عبر شبكات التواصل الاجتماعي، مجلة الجيش، مؤسسة المنشورات العسكرية، العدد ،630، الجزائر.

23- يوسف بوغرارة،(2018) الأمن السيبراني الإستراتجية الجزائرية للأمن والدفاع في الفضاء السيبيري، مجلة الدراسات الإفريقية، العدد الثالث، الجزائر.