الجريمة الالكترونية وتحديات الأمن السيبراني في الجزائر

Cybercrime and cybersecurity challenges in Algeria
La Criminalité électronique et les défis de la cybersécurité en Algérie

د.يحي مجيدي/ جامعة الوادي

Yahia108@gmail.com

د.سليمان نبار/ جامعة الوادي

slimane-nebbar@univ-eloued.dz

ملخص:

يهدف البحث إلى وصف وتحليل تجربة الجزائر في مواجهة الجريمة الالكترونية والتحديات التي واجهتها لتحقيق الأمن السيبراني. أدى ارتفاع حجم الجرائم الالكترونية في الجزائر خلال العقد الأخير إلى وضع الأطر القانونية التي تعاقب سوء استخدام التكنولوجيات الحديثة.كما بادرت الجزائر في تشريع وتأسيس العديد من المصالح والهيئات المكلفة بعمليات التحري والمتابعة. هذه الهيئات تختلف مهامها حسب الجهات الأمنية التابعة لها. وبينت النتائج أن تطور الجرائم الالكترونية وأشكالها خلال السنوات الأخيرة صاحبه أيضا تشكيل هيئات متخصصة.

الكلمات المفتاحية: الجريمة الالكترونية؛ الأمن السيبراني ؛التحديات؛ المؤسسة الأمنية.

Abstract:

The research aims to describe and analyze Algeria's experience in confronting cybercrime and the challenges it faced in achieving cybersecurity. The increase in cybercrimes' ratio in Algeria during the last decade has led to the establishment of legal institutes that penalizes the misuse of modern technologies. Algeria has also initiated the legislation and establishment of several entities and agencies responsible for investigation and monitoring. These units have varied responsibilities depending on the security authorities they are affiliated with. The results have shown that the evolution of cybercrimes and their forms in recent years has led to the formation of specialized establishments.

Keywords:cybercrime; cyber security; challenges; security establishment.

Résumé:

La recherche vise à décrire et analyser l'expérience de l'Algérie face à la cybercriminalité et les défis rencontrés pour réaliser lacybersécurité. L'augmentation du volume des cybercrimes en Algérie au cours de la dernière décennie a conduit à la mise en place de cadres juridiques sanctionnant l'abus des technologies modernes. L'Algérie a également initié la législation et la création de plusieurs entités et organismes chargés d'enquêtes et de suivi. Ces entités ont des tâches variées en fonction des autorités de sécurité auxquelles elles sont affiliées. Les résultats ont montré que l'évolution des cybercrimes et de leurs formes au cours des dernières années a également entraîné la formation d'organismes spécialisés.

Mots-clés: criminalité électronique; Cybersécurité; les défis ; corps sécuritaire.

مقدمة

قدمت الانترنت والتكنولوجيات الحديثة خدمة للإنسانية عن طريق منحها تأشيرة للانفتاح على العالم، كما أتاحت لها أشكال جديدة من الاتصال والتعامل مع البيانات والمعلومات، وسهلت من مستوى الخدمات الالكترونية وسرعتها، في المقابل أفرزت هذه البيئة الرقمية العديد من المشاكل غير أخلاقية وغير قانونية كثيرا ما أثرت على النفس والعقل وسلوك الفرد والجماعة.

صاحب تطور الأجهزة الرقمية وشيوع الانترنت عبر العالم تغيرا في منظومة القيم والمفاهيم والسلوك، وباتت البيئة الالكترونية تشكل تهديدا على أمن الفرد والمجتمع، بفضل ميزة الشعور بالحرية والتخفي والتعدي على الآخرين التي أتاحتها لمستخدمي الانترنت، الأمر الذي أدى إلى تطور في نسب ومستوى أشكال الجريمة الالكترونية التي مست أمن الفرد والمجتمع والدولة.

تزامن تطور التكنولوجيا مع نمو الجرائم المستحدثة عبر العالم، الأمر الذي شكل تهديدا على الدول واجبرها على وضع استراتيجيات وضوابط تقلل من الجريمة الالكترونية وتفرض الأمن السيبراني. والجزائر كغيرها من الدول أخذت على عاتقها مجابهة هذه الظاهرة عن طريق صياغة منظومة قانونية وأطر تشريعية تعاقب كل من يهدد أمن الأفراد وأمن الدولة، كما أسست مراكز متخصصة مهمتها التقصي ومتابعة المجرمين والوقاية من الجريمة الالكترونية ومجابهتها.

1- إشكالية البحث

تعتبر الجزائر واحدة من الدول التي مستها الجريمة الالكترونية بكل أشكالها، وظلت تشكل تهديدا الكترونيا يضر بالأمن السيبراني والأمن الوطني. ولمواجهة هذا النوع من الجرائم تبنت جملة من الآليات تمثلت في صياغة النصوص التشريعية، و تأسيس هيئات أمنية مكلفة بعمليات التحري والمتابعة لضبط الجريمة الالكترونية وتحقيق الأمن السيبراني. وهذا المقال هو عبارة عن دراسة وصفية تحليلية لواقع الجريمة الالكترونية في الجزائر والآليات التي تبنتها الدولة الجزائرية لمواجهتها وجاء التساؤل الرئيسي التالي.

- **ما هي الآليات التي تبنتها الجزائر لمواجهة تحديات الجريمة الالكترونية وتحقيق الأمن السيبراني؟**

وللإجابة على الإشكالية المطروحة قسمت الدراسة إلى العناصر التالية :

- تحديد لمفهومي الجريمة الالكترونية و الأمن السيبراني.
- نسبة الجريمة الالكترونية وأشكالها في الجزائر خلال السنوات الأخيرة.
- الأطر القانونية المستحدثة التي تعاقب المجرم الالكتروني.
- مهام المراكز والهيئات الأمنية التي أسستها الجزائر لمواجهة تحديات الجريمة الالكترونية.

2- تعريف الجريمة الالكترونية

الجريمة المعلوماتية أو الرقمية أو الإلكترونية أو السيبرانية (Cybercrime) هي مصطلح حديث يتألف من مصطلحين، الأول إجرام أو جريمة (Crime) والمصطلح الثاني سيبراني أو إلكتروني (Cyber)، ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسوب أو عصر المعلومات. وهي كما يصفها الدكتور طارق عبد الوهاب سليم "**الجرائم الهادئة**" التي لا تتطلب القوة أو العنف أو السلاح (سليم، 1997، صفحة 150). فالجريمة الإلكترونية تعرف بأنها " أي سلوك غير مشروع يرتبط بإساءة استخدام الحاسب الآلي ويؤدي إلى تحقيق أغراض غير مشروعة " (المحلاوي، 2016، صفحة 40).

وقع على عاتق الفقه مسؤولية ضبط تعريف للجريمة الالكترونية، انطلاقا من القواعد العامة واستنادًا إلى النقاط المستحدثة في الجريمة الإلكترونية. وهو الأمر الذي ترتب عنه ظهور العديد من التعريفات منها التي تضيق من نطاق الجريمة الإلكترونية وتركز على نوعها، ومنها التي تستند إلى الفاعل مرتكب الجريمة، كما أن هناك تعريفات توسعت في تعريف الجريمة الإلكترونية لتدخل ضمن نطاقها كافة العمليات والممارسات غير مشروعة المرتبطة بتكنولوجيا الإعلام والاتصال واستخدام الحاسوب الآلي والوسائل الإلكترونية وشبكة الانترنت (بهلول، 2018، صفحة 283).

تعرف الجريمة الالكترونية على أنها الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال بالإنترنت، ويكون هدفها اختراق الشبكات وتخريبها والتحريف والتزوير والسرقة والاختلاس والقرصنة وسرقة حقوق الملكية الفكرية. تعرف أيضا " الجريمة الناجمة عن إدخال بيانات مزورة في الأنظمة، وإساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم أكثر تعقيدا من الناحية التقنية مثل تعديل الكومبيوتر" (عريان، 2010، صفحة 03).

نلاحظ أن التعدد في تحديد مفاهيم الجريمة الإلكترونية مرتبط باختلاف الزاوية التي ينطلق منها الباحثين في تحليلاتهم فهناك مفاهيم قانونية، وأخرى تتحدد حسب أنماط الجريمة أو آلياتها أو مواضيعها؛ أو حتى حسب مرتكبيها (سواء كانت أفراد أو منظمات أو حكومات)، أو تفسيرات اخرى تركز على الهدف من الجريمة مثل التعدي على الغير وإلحاق الضرر به معلوماتيا وماديا وفكريا.

3- تعريف الجريمة الإلكترونية في التشريع الجزائري

انتشرت الجرائم الإلكترونية- اليوم- وأصبح من الضروري التصدي لهذه الظاهرة التي تمس بالأمن الوطني، الأمر الذي ترتب عنه تعديل الكثير من التشريعات الوطنية والدولية، وصنف هذا النوع من الجرائم ضمن الأفعال المجرمة التي يعاقب عليها القانون وفرضت عقوبات تحد من انتشارها .

عمل المشرع الجزائري بموجب تعديل قانون العقوبات لسنة 2004 (قانون العقوبات، 10 نوفمبر2004) على تجريم الجرائم الإلكترونية التي أصبحت تنتشر في المجتمع الجزائري ،واستحدث بذلك قسما خاصا بالعقوبات المطبقة على الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات. فأصدر سنة 2009 أول نص قانوني متعلق بالجرائم الإلكترونية ومكافحتها والذي قدم من خلاله مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهي " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات؛ وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصال الإلكترونية .

أضاف أيضا سنة 2021 تعريفا آخر:" بأنها الجريمة المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا، بمفهوم هذا القانون، الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضرين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة، أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود و الوطنية، أو لمساسها بالنظام والأمن العموميين. تتطلب استعمال وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي".(أمر رقم21-11 المؤرخ في 25 غشت سنة 2021يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الاجراءات الجزائية ،المادة 211 مكرر25). وبمقارنة هذا النص بسابقه تضمن هذا التعريف إضافة أكثر دقة تؤكد على الاهتمام بعدد أطراف الجريمة ومجالها الجغرافي ومستوى أضرارها على الفرد والمؤسسة والأمن العام، ووسائل التحري المتخصصة، والتعاون الدولي لمواجهة أشكال الجريمة الالكترونية المتعددة.

4- تعريف الأمن السيبراني

يُعرف بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية، والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات، وضمان أصالة وصحة هذه الاتصالات مع الحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام (شوابكة، 2019).

5- مكونات الأمن السيبراني

توحي كلمة الأمن السيبراني والجرائم الالكترونية بأنه تم الكشف عن معلومات كان يجب أن تبقى سراً، والحقيقة أن الحفاظ على سرّية المعلومات هو أحد جوانب الأمن، بيد أن المتخصصين يرون أن لأمن الحواسيب والمعلومات مكونات ثلاثة على درجة واحدة من الأهمية تتمثل في: **سرّية المعلومات** (**Data Confidentiality** و**سلامة المعلومات** (**Data Integrity**)

6- القواعد الإجرائية للوقاية من الجريمة الإلكترونية ومكافحتها في التشريع الجزائري

صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، واعتبر في تلك الفترة الخطوة الأولى للحكومة الجزائرية لمواجهة الجريمة الإلكترونية؛ حيث أشرف على إعداده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات. يتكون القانون من (19 مادة) موزعة على 06 فصول، تضمن أحكام خاصة في مجال التطبيق، وأخرى خاصة بمراقبة الاتصالات الإلكترونية، وحدد الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية، بالإضافة إلى القواعد الإجرائية للتفتيش الإلكتروني.

حدد المشرع الجزائري- في إطار كشف الجرائم الإلكترونية ومحاربتها- جملة من القواعد الإجرائية محددة بموجب القانون 09-04 وتتمثل في:

6-1- مراقبة الاتصالات الإلكترونية

يعمل المشرع وفق مبدأ الحماية القانونية للبيانات ذات الطابع الشخصي من خلال أسمى نص في القانون ألا وهو الدستور وهذا في إطار القواعد العامة التي تعنى بالحماية القانونية للحياة الخاصة للأفراد، وهو ما يفرض ضرورة حماية بياناتهم الشخصية من انتهاكات المعالجة الآلية (أمحمدي، 2017، صفحة 73)، وحدد على سبيل الحصر الحالات التي يسمح فيها باللجوء إلى المراقبة الإلكترونية والمتمثلة في:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توافر 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 إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة (المادة (04) من القانون 09-04).

ونظرا لخطورة هذا الإجراء لما له من انتهاك للحياة الخاصة للأفراد، فقد نص المشرع على عدم جوز إجراء عمليات المراقبة الإلكترونية إلا بإذن مكتوب من السلطة القضائية المختصة، كما خص الحالة الأولى المتعلقة بالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، بإجراءات خاصة تدخل ضمن اختصاص النائب العام لدى مجلس قضاء الجزائر وضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

6-2- تفتيش المنظومة المعلوماتية

أجاز المشرع للسلطات القضائية وضباط الشرطة القضائية في سبيل مكافحة الجرائم الإلكترونية وفي إطار نصوص قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد إلى:

* منظمة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
* منظمة تخزين معلوماتية (المادة (05) من قانون 09-04).

وحرص في هذا المجال على فتح باب التعاون الدولي وأشار إلى أهمية فتح مجال المساعدة الدولية في مجال مكافحة الجرائم الإلكترونية وفق ما تقتضيه الاتفاقيات الدولية ومبادئ المعاملة بالمثل.

تدارك المشرع الجزائري الفراغ القانوني نسبيا في مجال الإجرام المعلوماتي عموما، والإجرام عبر الإنترنت خصوصا بموجب القانون 04-15 المتضمن تعديل قانون العقوبات، الذي بموجبه جرم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات وهي:

- **جريمة التوصل أو الدخول غير المصرح به:** تقوم هذه الجريمة بمجرد ما يتم الدخول غير المرخص به، وعن طريق الغش إلى المنظومة المعلوماتية، سواء مس ذلك الدخول أو البقاء لكامل المنظومة أو جزء منها فقط. وهو ما أشارت إليه المادة (394) مكرر من قانون العقوبات.
- **جريمة التزوير المعلوماتي:** النشاط الإجرامي في هذه الجريمة ينحصر في أفعال الإدخال والمحو والتعديل، ولا يشترط اجتماعهما معا حتى يتوافر النشاط الإجرامي فيها، إذ يتوفر الركن المادي للجريمة بمجرد القيام بفعل واحد على حدا. لكن القاسم المشترك في هذه الأفعال جميعا، هو انطوائها على التلاعب في المعطيات، التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل آخر. (خثير، 2010، صفحة 123). وأكد المشرع على معاقبة هذه الجرائم في المادة (394) مكرر1.
- **جريمة الاستيلاء على المعطيات:** تعد هذه الجريمة من بين أكثر الجرائم وقوعا في العالم الافتراضي، وهي ما أقرته المادة (394) مكرر2.
- **جريمة إتلاف وتدمير المعطيات:** تطرق إليها المشرع الجزائري بالمادة (394) مكرر1 من قانون العقوبات.
- **جريمة الاحتيال المعلوماتي:** تطرقت إليه فحوى المادة (394) مكرر1/2.
- **أنشطة الإنترنت المجسدة لجرائم المحتوى الضار والتصرف غير القانوني:** نصت مواد القسم السابع مكرر من قانون العقوبات وخاصة المادة (394) مكرر2/2 على تجريم أفعال الحيازة، الإفشاء والنشر التي ترد على المعطيات الآلية بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق، وجميع الأفعال غير المشروعة، وذلك

بعقوبتي الحبس والغرامة، إضافة إلى ما نصت عليه المادة (394) بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات (قانون 04-15 ، 10 نوفمبر2004).

6-3- حجز المعطيات المعلوماتية

فتح المشرع الجزائري للسلطة التي تباشر التفتيش عندما تكتشف في منظومة معلومات معطيات مخزنة تكون مفيدة في الكشف عن الجرائم الإلكترونية أو مرتكبيها، المجال لنسخ المعطيات محل البحث. والمعطيات اللازمة لفهمها تكون قابلة للحجز وفقا للقواعد المقررة قانونا، في حال ما لم يكن من الضروري حجز كامل المنظومة (المادة (06) من القانون 09-04).

يتضح من خلال هذه القوانين أن الجزائر كغيرها من الدول بذلت جهودا تشريعية لمواجهة الجريمة الالكترونية، إلا أن هناك من يرى أن تجسيد بنود هذا القانون على أرض الواقع يبقى نسبي بسبب إهماله للجوانب التقنية الكفيلة بتصنيف هذه الجرائم، وتحديد العقوبة المناسبة في حق مرتكبيها. واقتصرت العقوبات في أغلب الأحيان على الغرامة المالية. وخلص أحد الباحثين أنه على الرغم من الجهود الجبارة التي بذلها المشرع الجزائري في سبيل التصدي لظاهرة الإجرام الالكتروني إلا أنها غير كافية لبلوغ الهدف، نظرا للتطورات السريعة والمستمرة التي تعرفها الظاهرة، لذلك لا بد من اللجوء إلى التعاون الدولي. (عيمور، 2022)،

يرى البعض أن القصور في البنية التشريعية والتنظيمية، وعدم إلمام قوانينها بمختلف الأجزاء المكونة للفضاء الرقمي والتوجه نحو الإجراءات الردعية والتدابير الوقائية للحد من القرصنة، أثبت عدم التحكم في تكنولوجيات الإعلام والاتصال (بوازدية، 2019). لذا يمكن القول أن التطور التكنولوجي أسرع بكثير من الأطر التشريعية وأساليب الردع القانونية. الأمر الذي يفرض على الفاعلين الاهتمام بعملية تحيين التكوين ،وتوفر عنصر الكفاءة والتخصص.

7- أشكال الجريمة الالكترونية في الجزائر

أسست الجزائر سنة 2009 قسم خاص لمكافحة الجريمة المعلوماتية متخصص في استغلال الأدلة المعلوماتية ضمن المديرية الفرعية للشرطة العلمية والتقنية، وتمكنت مصالح المديرية العامة للأمن الوطني من تسجيل عدد من القضايا المتعلقة بالجريمة الالكترونية ؛حيث تم معالجة 515 قضية خلال سنة 2012، ويتعلق الأمر بـ 126 قضية خاصة بالاستغلال غير القانوني للأداة المعلوماتية، و154 تتعلق بالهاتف النقال، و103 تخص الصور الفوتوغرافية والفيديو.

عالجت الخلية المركزية لمكافحة الجريمة الالكترونية خلال السداسي الأول من نفس السنة 15 قضية تتعلق بانتهاك خصوصية الحياة الشخصية (معالجة 6 قضايا سنة 2012) وأربعة خاصة بالتشهير (8 قضايا سنة 2012) و11

بسبب الابتزاز (4 قضايا سنة 2012) وواحدة خاصة بانتحال الشخصية (4 قضايا سنة 2012) و24 تتعلق بالقرصنة (10 قضايا سنة 2012)، ويشير القسم المختص في استغلال الأدلة المعلوماتية أن غالبية المخالفات تتعلق بالتكنولوجيات الجديدة؛ سيما بواسطة الحواسيب والانترنت والهواتف النقالة. وتم تسجيل أزيد من 100 قضية خلال 9 أشهر من سنة 2014 ومعظمها تتعلق بالنصب والاحتيال على الأشخاص.

سجلت مصالح الأمن في السداسي الأول من سنة 2015 ما يعادل 417 قضية تتعلق بالجريمة الالكترونية، شملت انتحال الشخصية، النصب والاحتيال التزوير الإلكتروني تخريب بيانات شخصية وعامة، الابتزاز بصور أو معلومات مقرصنة، التشهير، السرقة الالكترونية، وانتشار مثل هذه القضايا يعود الى الاستخدام المتزايد لشبكة الانترنت من قبل جميع الفئات الاجتماعية، وبالتالي ازدياد عدد ضحايا القرصنة والنصب والاحتيال ومختلف أشكال الجرائم الالكترونية الأخرى وكذلك ارتفاع عدد مجرمي الانترنت (لطرش و بن عزوز، 2016).

بينت عملية تحليل المعطيات للجرائم المسجلة أن القذف والسب عبر الفضاء السيبراني احتل الصدارة بنسبة تفوق 55 بالمائة، تليها الجرائم ضد الأمن العمومي، ثم الأفعال الماسة بالحياة الخاصة وإفشاء الأسرار، وأخيرا الابتزاز والنصب والاحتيال والاستغلال الجنسي والأفعال المخالفة للآداب العامة وقضايا مشابهة (باشوش، 2021). كما بينت دراسة "جميلة بن عابد وفطيمة بن عابد" أنه تم إحصاء 126 جريمة الكترونية سنة 2017 بولاية الأغواط، من بينها جرائم القذف والإغراء والتهديد بمعدل 20% ،مصنفة ضمن صنف المساس بالمصلحة العليا للبلاد. تليها نسبة 15.87% بمجموع 20 جريمة تمثلت في قضايا عدم الانجاز؛ وهي القضايا التي تم رفع شكوى ضد مرتكبيها وتم التنازل عنها مثل: قضايا الإغراء والسب والتشهير. وهذا لأن مرتكب الجريمة يكون من أقارب المدعي أو احد معارفه. (بن عابد و بن عابد، 2022).

سجلت احصائيات سنة 2018 أكبر نسبة في "قضايا القذف" حيث احتلت نسبة 13.54% بمجموع 42 جريمة شملت قذف أشخاص وتشويه سمعتهم، تليها نسبة 7.41% بمجموع 23 جريمة تمثلت في قضايا السب سواء بطريقة كتابية أو عن طريق رسوم ومطبوعات عبر البريد الالكتروني أو الصوتي، واحتلت قضايا التشهير نسبة 6.77 بمجموع 21 قضية وذلك بنشر معلومات مغلوطة عن أشخاص أو مؤسسات للتشهير بهم ونشر إشاعات و17 قضية بنسبة 5.58% من صنف المساس بخصوصية الأشخاص دون علمه ورضاه ووضع تعليقات مسيئة لهم أو التهديد والابتزاز (بن عابد و بن عابد، 2022).

يتضح من خلال قراءة النسب أن "جريمة القذف والسب"هي الجريمة الأكثر انتشارا في السنوات الأخيرة، وهذا بسبب خاصية التخفي التي يمنحها الفضاء الالكتروني للمجرمين، وكذا خوف الضحية من التبليغ عن الجريمة وترددهم،

خاصة إذا كان الجناة من فئة أقارب الضحية، بالإضافة إلى نقص الوعي بالقوانين التي تشرع للأمن السيبراني، وتعاقب كل من يسيء استخدام التكنولوجيا الحديثة.

8- تأسيس هيئة رسمية مختصة في الأمن السيبراني

تتطّلب مكافحة الجريمة الإلكترونية إحداث هيئة مختصة في الأمن والسلامة المعلوماتية. ويعدّ اعتماد هيئة مختصة في دعم ومساندة الجهات الأمنية عند مكافحتهم للجريمة الإلكترونية أمرا ضروريا، نظرا لصعوبة إثبات الجريمة المعلوماتية. وقد أنشأت عدة دول في العالم وحدات متخصصة في مكافحة جرائم الإنترنت مثل: الصين، والولايات المتحدة، وبريطانيا، وفرنسا، وكذلك الجزائر. وتعتمد مواجهة مخاطر الجريمة الإلكترونية بشكل كبير على تبني إستراتيجية- أمنية مجتمعية متكاملة، والتي تعمل فيها أجهزة مكافحة الجريمة الرسمية في الدولة جنبا إلى جنب مع- أفراد المجتمع ومؤسسات القطاع الخاص مثل:

- مزودو خدمة الإنترنت الذين يملكون القدرة على تحديد ما يعرف بـ (IP- Internet Protocol) للمشتركين، ما يتيح إمكانية مراقبة الأنشطة الخطرة على الإنترنت، وتقييد اشتراك المستخدمين المنخرطين في تلك الأنشطة.
- يمكن للمواطن العادي تحمل مسؤولية حماية نفسه من الوقوع ضحية لجرائم الإنترنت، وذلك باقتناء برمجيات الحماية من الفيروسات.
- المصارف التجارية وشركات البطاقات الائتمانية عليها أيضا مسؤولية كبيرة في حماية عملائها من خلال تطبيق برامج إجرائية وقائية ضد الاحتيال، وكذلك وضع برمجيات مراقبة لتعقب النشاطات غير المعتادة على حسابات العملاء، ووضع أنظمة لتنبيه العميل على كل عملية تتم على حسابه.
- دور المحققين المختصين الذين يعملون بالتنسيق مع أجهزة العدالة الجنائية في مكافحة جرائم الإنترنت (بن خليفة و عبد القادر، 2017).

9- آليات مكافحة الجريمة الالكترونية وتحقيق الأمن السيبراني في الجزائر:

استعدادا لمواجهة الجريمة الالكترونية التي شهدت اكتساحا للفضاء السيبراني شرعت الجزائر على غرار كل الدول في صياغة أطر قانونية تضبط سرعة انتشار الظاهرة وتوسعها، وكذا تأسيس هيئات مختصة في المتابعة والتقصي للجريمة الالكترونية. وعليه فقد أنشأت هيئات ومصالح تابعة لجهاز الأمن، وأخرى تابعة للدرك الوطني، ومصالح تابعة لقيادة أركان الجيش الوطني الشعبي.

9-1- الهيئات التابعة لسلك الأمن الوطني

انبثق عن القانون الصادر في الجريدة الرسمية للجمهورية الجزائرية في العدد 47 يوم 16 غشت 2009؛ والذي نص في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

أنشأت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته وحددت مهامها في الفصل الخامس من خلال المواد من (14-17) والمتمثلة في:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها.
- أكد القانون في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية في إطار مبدأ المعاملة بالمثل، وتبادل المعلومات مع نظيرتها في الخارج، قصد جمع كل المعطيات المفيدة للتعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم "

أمام زيادة أهمية استخدام تكنولوجيا الاتصال الحديثة لدى الأفراد أو المؤسسات (عامة أو خاصة)، ومع تطور نسبة الجرائم السيبرانية تم إنشاء هذه الهيئة بأمر من رئيس الجمهورية سنة 2009 ،بهدف التعامل الجيد مع هذه الجرائم والتمكن من مواجهة التهديدات الالكترونية مهما كان مصدرها. والتصدي للأضرار التي قد تمس أمن المعلومات، أو نشر الإشاعات أو أي ضرر قد يلحق بالبنية التحتية، أو التجسس، أو استخدام الفضاء السيبراني لتجنيد الإرهابيين، أو إعطاء تقارير للجهات المختصة. تعمل الهيئة بالتنسيق مع المؤسسات الوطنية المعنية بالأمن السيبراني (الجيش الوطني الشعبي، الشرطة، القضاء)، وكذا التعاون مع الهيئات المماثلة في الخارج، سواء تلك التي تنتمي إلى الدول أو التنظيمات (إقليمية، دولية)، كما أن هناك هيئات تابعة للجهاز الأمني مكلفة بالتدخل للمواجهة العملية على المستوى التطبيقي للجرائم المعلوماتية.

يوجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي المخبر المركزي للشرطة العلمية بالجزائر، المخبر الجهوي للشرطة العلمية بقسنطينة، المخبر الجهوي للشرطة العلمية بوهران... كل هذه الهيئات تتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها (رابح، 2004).

تم استحداث مصالح على مستوى مديريات الأمن في كل ولاية تهتم بالجرائم الالكترونية، ومن أهمها ما يلي:

ب- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني:

استجابة لمطلب الأمن السيبراني ومكافحة التحديات الأمنية الناجمة عن الجرائم الالكترونية، وبقرار من المدير العام للأمن الوطني قامت مصالح الأمن سنة 2011 بإنشاء المصلحة المركزية للجريمة الالكترونية على مستوى المديرية العامة للأمن الوطني، وقد أضيفت للهيكل التنظيمي في 2015 ليشمل جميع الولايات.

تعمل المصلحة من خلال محققتين مختصتين يتكفلون بالشكاوي المتعلقة بالجريمة الالكترونية على مستوى الولايات باستخدام أحدث المعدات، إضافة إلى معالجة نفس نوعية هذه القضايا على المستوى الدولي من خلال التعاون بين هذه المصلحة والعديد من المصالح المشابهة في العديد من الدول (المصلحة المركزية للجريمة الالكترونية في مواجهة مجرمي العالم الافتراضي، 2016). من مهام هذه المصلحة:

- حماية المعلومات حماية جنائية.
- العمل وفق الاختصاص (محلي ووطني)، وإمكانية التعاون الدولي في مجال مكافحة الجريمة الالكترونية من خلال تحديد دائرة الاختصاص.
- مراقبة ومواكبة التطور التكنولوجي المحدد من الجريمة الالكترونية.
- الوقوف ضد الاختراقات والقرصنة والتجسس.
- التفتيش في المنظومة المعلوماتية بناء على أوامر قضائية.
- مكافحة الانتهاكات للمراسلات الشخصية.
- برمجة دورات تكوينية داخليا وخارجيا.
- التحقيق في القضايا المتعلقة بالجريمة الالكترونية.

احتلت الجزائر المرتبة 23 عالميا من أصل 29 في مستوى التأهب في مجال الأمن السيبراني، أما على المستوى العربي فقد صنفت في المرتبة العاشرة حسب التزامها بالتدابير التي يحددها الرقم القياسي العالمي للأمن السيبراني (بن جدو، 2022). وعموما يمكن القول أن الهيئات جاءت كرد فعل لتزايد نسبة الجريمة الالكترونية بكل أشكالها خلال العقد الأخير.

9-2- الهيئات والوحدات التابعة للقيادة العامة للدرك الوطني

تقدم الهيئات التابعة للدرك الوطني ومختلف المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني دورا هاما في مجال مكافحة الجريمة المعلوماتية، وتضم موارد بشرية تتميز بالخبرة والكفاءة. وعلى المستوى المركزي تشكلت هيئات متخصصة يمكن إجمالها في الآتي:

أ- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني:

يتكون المعهد من إحدى عشر دائرة متخصصة في عدة مجالات متباينة، تضمن جميعها الخبرة والتكوين والتعليم، وتقديم جميع المساعدات التقنية. تقوم دائرة الإعلام الآلي والالكتروني المكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما يقدم المساعدة للمحققين. يتوفر على عدة تجهيزات مثل محطة ترميم وتصليح الأجهزة المعطلة، الشبكات الإعلامية، والتجهيزات البيانية.

يعتبر المعهد مؤسسة عمومية تحت الوصاية المباشرة لوزير الدفاع الوطني، من مهامه إجراء الفحوص العلمية في إطار التحريات الأولية، وإجراء بحوث متعلقة بالكشف عن الإجرام باللجوء إلى التكنولوجيا الدقيقة. يضم العديد من المصالح منها مصلحة الإعلام الآلي تقوم برصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية، وتفكيك البرامج المعلوماتية " (رابح، 2004).

أنشئ المعهد بموجب مرسوم رئاسي 133/04 المؤرخ في 26 جوان 2004 ودخل حيز الخدمة ابتداء من الفاتح جانفي 2009، أما الفترة الممتدة بين 2004 و2009 كرست لتكوين المورد البشري، واقتناء المعدات العلمية والتقنية الضرورية. يقوم المعهد بتلبية الطلبات الواردة من السلطة القضائية، ضباط الشرطة القضائية والسلطات المؤهلة قانونيا خاصة أثناء معالجة القضايا المعقدة.

يعنى بتحقيق الأمن السيبراني باستخدام أحدث البرامج والوسائل وتوظيف المورد البشري المختص في تكنولوجيا الاتصال والشبكات والمعلومات، وكشف عمليات القرصنة. يقوم المعهد بتنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية، ويحتوي على العديد من الأقسام والمصالح المختصة أين يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية؛ وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية (عطية، 2019).

من أهم اختصاصاته في مجال الأمن السيبراني:

- تعميم وانجاز بنوك المعطيات.
- إجراء الخبرات والفحوص العلمية في إطار التحريات الأولية والتحقيقات القضائية.
- ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية.
- العمل على ترقية البحوث التطبيقية وأساليب التحريات التي أثبتت فعاليتها.
- المشاركة في الملتقيات والمحاضرات والندوات على الصعيدين الوطني والدولي (بارة، 2017).

فرضت التهديدات الالكترونية إنشاء كل هذه المصالح والهيئات وتجنيد كافة الإمكانيات المادية والبشرية للتصدي لمخاطر الجريمة الالكترونية التي تهدد الأمن الوطني.

ب- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني:

أنشأ هذا المركز سنة 2008 من مهامه تأمين منظومة المعلومات لخدمة الأمن العمومي، وهو بمثابة مركز توثيق يهدف إلى تحليل معطيات وبيانات الجرائم المعلوماتية، وتحديد هوية أصحابها مما يؤمن الأنظمة المعلوماتية للمؤسسات الرسمية أو البنوك أو الشركات أو حتى الأفراد، كما يهدف إلى مساعدة باقي الأجهزة الأخرى في أداء مهامها وخاصة فيما يلي:

- ضمان المراقبة الدائمة والمستمرة على شبكة الانترنت.
- القيام بمراقبة الاتصالات الالكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية.
- مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة.
- المشاركة في عمليات التحري عبر شبكة الانترنت لفائدة وحدات الدرك الوطني والسلطات القضائية.
- المشاركة في قمع الجرائم المعلوماتية من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

عالج المركز سنة 2015 ما يقارب 240 قضية متعلقة بالجرائم المعلوماتية، شملت جرائم التهديد، المساس بالنظام العام، جرائم الاختراق، التحرش الجنسي بالقصر وتحريضهم على مخالفة الآداب العامة، إهانة هيئات ورموز وطنية، النصب والاحتيال الاعتداء على حرمة الحياة الخاصة (بارة، 2017).

9-3- الهيئات التابعة لقيادة أركان الجيش الوطني الشعبي

أ- مصلحة الدفاع السيبراني ومراقبة أمن الأنظمة:

أنشأت المصلحة سنة 2015 ومن مهامها الحرص على وضع وتنفيذ السياسة العامة للدفاع السيبراني، والرفع من مستوى أمن الأنظمة المستحدثة؛ بالإضافة إلى تحيين وتطبيق الإطار التنظيمي المحدد لمجال الدفاع السيبراني، وحماية منظومة الأسلحة، والتنسيق مع الهيئات الوطنية المعنية" (جنادي، 2020).

ويمكن تحديد مهام هذه المصلحة في:

- حماية منظومة الدفاع العسكرية (أسلحة، اتصالات، رادارات...) من الاختراق والهجمات السيبرانية.
- تأمين المنشآت العسكرية والمجال الجغرافي (بر، جو، بحر).
- التنسيق مع الهيئات المدنية المختصة في تحقيق الأمن السيبراني (اقتصادية، مالية، سياسية...).
- الكشف عن عمليات التجسس.

- محاربة الإرهاب السيبراني مهما كانت الفواعل (دول، تنظيمات، أفراد).
- المشاركة في إعداد السياسية العامة للدولة في مجال مكافحة تحقيق الأمن السيبراني.

ومن بين النتائج المتوصل إليها من طرف هذه المصالح، اتضح أن الجرائم الإلكترونية بالجزائر تتضاعف بطريقة سريعة جدا، وهذا ما كشفت عنه الأرقام المسجلة التي تم البت فيها، حيث سجلت سنة 2017 أكثر من 2500 جريمة ويتعلق أبرزها (70%) انتهاك الحريات الشخصية والتهديد عبر الانترنت، ونشر صور فاضحة، الابتزاز، والقرصنة الإلكترونية وغيرها (بوازدية، 2019). فبالرغم من تأسيس كل هذه الهيئات الأمنية وأمام تصاعد أرقام الجريمة الالكترونية التي ظلت تهدد الأمن الوطني والسيبراني، وفي ظل عدم كفاية هذه المؤسسات للتصدي للاعتداءات التي تمس بمؤسسات الدولة، كان لابد من تبني إستراتيجية فعالة وطويلة المدى قادت لانشاء قطب جزائي وطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

9-4- القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

في ظل تطور الجريمة السيبريانية وتنوع أشكالها وتنامي خطورتها على النظام والأمن الوطني والمجتمع ككل، أحدث المشرع الجزائري في آخر تعديل لقانون الإجراءات الجزائية بموجب الأمر 21-11 المؤرخ في 2021/08/25 القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. يمثل هذا القطب يمثل جهة قضائية مكلفة بالنظر في الجرائم السيبريانية. حيث نصت المادة 211 مكرر22 "ينشأ على مستوى محكمة مقر مجلس قضاء الجزائر، قطب جزائي وطني متخصص في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والجرائم المرتبطة بها، كما تختص بالحكم في الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحا. يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي ورئيس ذات القطب، بالمتابعة والتحقيق والحكم في الجرائم المتصلة حصريا بتكنولوجيا الإعلام والاتصال وكذا الجرائم المرتبطة بها وهي:

- الجرائم التي تمس بأمن الدولة وبالدفاع الوطني.
- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية.
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.
- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.
- جرائم التمييز وخطاب الكراهية.

وضمان الفعالية في التصدي وكيفية التعامل مع هذا النوع من الجرائم لا يتأتى إلا بالرفع من فعالية الجهات المكلفة بمكافحة الجريمة الالكترونية؛ مما يستلزم توفير فرق خاصة من الشرطة القضائية، والتكوين المستمر والتأهيل. (بن يونس، 2022).

إنشاء هذا القطب فرضته جملة من التحولات الاجتماعية والسياسية التي عرفها المجتمع الجزائري خاصة بعد الحراك الشعبي منذ 2019، وتصاعد موجات الغضب وانتشار فكرة الحرية التي تميز بها مضمون الخطاب الالكتروني لدى فئة الشباب خاصة، مما أدى إلى تسجيل العديد من القضايا من صنف المساس بأمن الدولة، بالإضافة إلى انتشار واسع لأشكال التعدي على خصوصية الأفراد والخصوصية الاجتماعية والثقافية وحتى التاريخية للمجتمع الجزائري وأدى إلى المساس بأمن الدولة ورموزها ومؤسساتها الرسمية.

وبالنظر إلى المعطيات التي قدمها تقرير الاتحاد الدولي السنوي (نوفمبر2017) الذي صنف دول العالم في مجال الأمن السيبراني وفق مقياس "مدى التزام الدول في جميع أنحاء العالم بتفعيل وتطوير مختلف تقنيات الأمن السيبراني"، فقد صنفها الى ثلاث فئات، دول متخلفة، الناضجة والمتقدمة، وهنا احتلت الجزائر المرتبة الثامنة والستون عالميا من مجموع 164 دولة شملها التقرير واحتلت المرتبة التاسعة من مجموع 22 دولة عربية (بوازدية، 2019). ومنه يمكن القول أن التأهب وتحقيق الأمن السيبراني مشروط باقتناء التكنولوجيات الحديثة ومعرفة دقيقة بأنظمتها الأمنية.

10- خاتمة:

تعددت تعريفات الجريمة الالكترونية بتباين الزاوية التي ينظر منها كل باحث، فهناك من يركز على الوسيلة المستخدمة في الجريمة وهي جهاز الكمبيوتر لكونها زاوية التفرقة بين الجريمة الإلكترونية وغيرها من الجرائم التقليدية، وهناك من يركز على مرتكب الجريمة، أو التركيز على الهدف من الجريمة وهو التعدي على الغير وإلحاق الضرر به معلوماتيا وماديا وفكريا.

تتزايد التهديدات الالكترونية نتيجة التطور في الأساليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية بهدف تعديلها أو سرقتها أو حتى تدميرها، ويمكن تصنيف أساليب التهديد إلى ثلاث : اختراق الشبكات، والهندسة الاجتماعية، والبرمجيات الضارة. وعرّف التشريع الجزائري الجريمة الالكترونية بأنها الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات؛ وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصال الإلكترونية.وأكد في القانون الصادر سنة 2021 على ضرورة الاهتمام بعدد أطراف الجريمة، ومجالها الجغرافي، ومستوى أضرارها على الفرد والمؤسسة والأمن العام، ووسائل التحري المتخصصة، والتعاون الدولي لمواجهة أشكال الجريمة الالكترونية المتعددة.

تتميز خصوصية الجريمة الإلكترونية بقدرة مرتكبيها على التخّفي والإفلات من العقاب، الأمر الذي يتطلب اعتماد آليات وطرق لمكافحة الجريمة الالكترونية، ومن أكثر أشكال الجرائم الالكترونية انتشارا في الجزائر "جريمة القذف والسب" بسبب القدرة على التخفي وكذلك عزوف الضحايا عن التبليغ. حيث بينت التحريات أن اغلب الجناة من فئة أقارب الضحية، أيضا نقص الوعي بالقوانين التي تشرّع للأمن السيبراني وتعاقب كل من يسيء استخدام التكنولوجيا الحديثة.

شرعت الجزائر في صياغة أطر قانونية تضبط سرعة انتشار الظاهرة وتوسعها، وأنشأت هيئات تابعة لأسلاك الدولة مختصة في المتابعة والتقصي للجريمة الالكترونية وهي هيئات تابعة لجهاز الأمن الوطني، وأخرى تابعة لجهاز الدرك الوطني، كما أنشأت القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال الذي يهتم بالمتابعة والتحقيق والحكم في الجرائم.

أخيرا يمكن القول أنه على الرغم من تطور وسائل الاتصال الحديثة، إلا أن هذا التطور صاحبه من جهة ثانية استخدام واسع للتكنولوجيات الحديثة من قبل الأفراد والمؤسسات، فأصبحت بذلك الجريمة الإلكترونية ظاهرة إجرامية تتطور بتطور وسائل التكنولوجيا خاصة مع ضعف المعرفة بآليات أمن المعلومات أو القوانين التي تعاقب سوء استخدامها لذلك لابد من:

- تطوير التشريعات السيبرانية تماشيا مع التطورات الحاصلة في عالم التكنولوجيا.
- الانضمام إلى الاتفاقيات الدولية في مجال حماية الأنظمة المعلوماتية، مما يحفز على التنسيق والتعاون مع الناشطين من خبراء في مجال الأمن السيبراني إقليميا ودوليا، وعقد مؤتمرات علمية ودورات تكوينية للاستفادة من الخبرات.
- ضمان التكوين المتواصل للمورد البشري المكلف بعمليات التحري والمتابعة من مهندسي الإعلام الآلي ورجال القانون والقضاة.
- التوعية والتحسيس خاصة في المؤسسات التربوية، وإدراج مضامين تعليمية تحث على مخاطر التكنولوجيا الحديثة وخاصة تلك التي تهدد المنظومة القيمية للطفل.
- تشكيل قنوات إعلامية مهمتها نشر الوعي في كل مؤسسات التنشئة الاجتماعية وخاصة الأسرة والمدرسة.
- إشراك وتفعيل دور مؤسسات المجتمع المدني في مكافحة الجريمة الالكترونية وأضرارها على الفرد والمجتمع.

11- المراجع:

أمحمدي، آمنة بوزينة. (2017). " إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائرية وقانون الوقاية من جرائم الإعلام) ". الملتقى الوطني الأول حول آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، 29 مارس، الجزائر العاصمة: مركز جيل البحث العلمي.

بارة، سمير. (2017). " الأمن السيبراني في الجزائر: السياسات والمؤسسات ". المجلة الجزائرية للأمن الإنساني، الجالد02(ع02)، ص273.

باشوش، نوارة. (2021). الإجرام الالكتروني.. أرقام مرعبة. https://www.echoroukonline.com.

بن جدو، بن علية. (2022). " تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية ". المجلة الجزائرية للأمن الإنساني، الجولد07(ع02)، ص317.

بن خليفة، أحمد والأمير عبد القادر، محفوظة. (2017). " الجريمة الإلكترونية وآليات التصدي لها. مجلة الامتياز لبحوث الاقتصاد والإدارة "، المجلد01(ع01)، ص163.

بن عابد، جميلة وبن عابد، فطيمة. (2022). " الالكترونية في المجتمع الجزائري: دراسة وصفية عن تطور الظاهرة في ولاية الأغواط". مجلة البحوث القانونية والاقتصادية، المجلد05(ع02)، ص.ص272، 275-276.

بن يونس، فريدة. (2022). " استحداث قطب جزائي وطني لمكافحة الجرائم السيبريانية ومتابعتها- قراءة في الأمر21-11 ". مجلة الدراسات القانونية والاقتصاد، المجلد05(ع01)، ص.ص1709-1710.

بهلول، سمية. (2018). دور الإدارة الالكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر. رسالة دكتوراه غير منشورة في العلوم القانون (تخصص إدارة محلية)، جامعة الحاج لخضر باتنة، الجزائر.

بوازدية، جمال. (2019). " الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والآفاق المستقبلية ". مجلة العلوم القانونية والسياسية، المجلد10(ع01)، ص1280.

الجمهورية الجزائرية الديمقراطية الشعبية. (16 أوت 2009). الجريدة الرسمية، (ع47).

جنادي، إسماعيل. (أوت 2020). " الدفاع السيبراني من أهم تحديات الجيش الوطني الشعبي ". مجلة الجيش الشعبي الجزائري، (ع635)، ص31.

خثير، مسعود. (2010). الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات. الجزائر: دار الهدى.

رابح، سعاد. (2004). " ضوابط مكافحة الجريمة المعلوماتية. مجلة القانون العام الجزائري والمقارن "، المجلد02(ع01)، ص.ص266-288.

سليم، طارق عبد الوهاب. (1997). الجرائم المرتكبة بواسطة الانترنت وسبل مكافحتها. تونس: د.د.ن.

شوابكة، عدنان عواد. (2019). "دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف". مجلة دراسات وأبحاث، المجلد11(ع04)، ص168.

عريان، أمير الفونس. (2010). " الجرائم الالكترونية في البنوك- وكيفية معالجتها ". ورقة مقدمة للمؤتمر الثاني حول الجرائم المستحدثة: كيفية إثباتها ومعالجتها. مصر: المركز القومي للبحوث الاجتماعية والجنائية.

عطية، إدريس. (2019). "مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري". مجلة مصداقية، المجلد01(ع01).

عيمور، راضية. (2022). " الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري ". المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد06(ع01)، ص106.

الغثير، خالد بن سليمان. (2009). أمن المعلومات: بلغة مسيرة، تقديم محمد بن إبراهيم السويل. الرياض: مكتبة الملك فهد الوطنية.

قانون 04-15. (10 نوفمبر2004). المواد (394) مكرر2، (394) مكرر6.

قانون العقوبات. (10 نوفمبر2004). القانون 04-15 المؤرخ في 10 نوفمبر2004، المعدل والمتمم للأمر 66-156، المؤرخ في 08 جوان 1966. الجريدة الرسمية، (ع71).

القواعد الخاصة بالوقاية. (05 أوت 2009). المادة (02) الفقرة الأولى من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. الجريدة الرسمية، (ع47)، 05.

لطرش فيروز وبن عزوز حاتم. (2016). " الجريمة الالكترونية في الجزائر من جريمة فردية إلى جريمة منظمة ". مجلة آفاق للعلوم، المجلد01(ع1)، ص.ص330-331.

المادة (04) من القانون 09-04.

المادة (05) الفقرة الأخيرة من القانون 09-04.

المادة (05) من قانون 09-04.

المادة (06) من القانون 09-04.

المحلاوي، أنيس حسيب السيد. (2016). الخبرة القضائية في الجزائر المعلوماتية. الإسكندرية: دار الفكر الجامعي.

المصلحة المركزية للجريمة الالكترونية في مواجهة مجرمي العالم الافتراضي. (2016). https://www.djazairess.com/essalam/52564.

نافع زينب وشعباني، مجيد. (2020). " تحديات الحكومة الالكترونية في الجزائر: الجريمة الالكترونية نموذجا ". مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، المجلد12(ع01)، ص.ص783-784.