| تاريخ ارسال المقال:2018/11/13 | تاريخ القبول: 2018/12/13 | تاريخ النشر:2019/03/01 |
|---|---|---|

# الجريمة الإلكترونية كتهديد للأمن الوطني الجزائري

د. بلفكرات رشيد
belfekretr@gmail.com
ط/د. بنزعمة عبد القادر
جامعة الجزائر3

**ملخص:**
بالنظر للمعضلات الجيو أمنية، والتحديات متعددة لأبعاد التي باتت تشهدها العديد من دول شمال إفريقيا ومعظم دول الساحل الإفريقي جعلت منها بؤرة توتر وهشاشة تهدد بانفجار الأمن على عدة مستويات من الإقليمي إلى العالمي، فالتطور التكنولوجى على الرغم من آثاره الإيجابية إلا أن له العديد من السلبيات التى تهدد أمن واستقرار المجتمع ليس فى في هذه الدول فقط بل في العالم بأسره والجزائر خاصة. كما أن التطور الهائل فى مجال استخدام الحاسبات الآلية وشبكة المعلومات الدولية على الرغم من إيجابياته المتعددة إلا أنه ينطوى فى داخله على مخاطر تفوق كافة التصورات فى تهديده للأمني، ويكفى بلمسة واحدة لشخص أو مجموعة أشخاص أن يكبدوا بعض المؤسسات أو الشركات الكبرى خسائر مالية كبيرة، أو يهددوا أمن واستقرار المجتمع ككل.
**الكلمات المفتاحية:** الجريمة الالكترونية، تكنولوجيا المعلومات، الأمن الإلكتروني، الحماية المعلومات.

**Résumé:**
Compte tenu des dilemmes de la sécurité géopolitique, et de multiples défis aux dimensions qui ont lieu dans de nombreux pays d'Afrique du Nord et la plupart des pays africains du Sahel ont fait un foyer de tension et de fragilité menace la sécurité d'explosion à plusieurs niveaux de la région à l'avance mondiale, technologique, en dépit des effets positifs, mais il présente de nombreux inconvénients Menace la sécurité et la stabilité de la société non seulement dans ces pays mais aussi dans le monde entier et en Algérie en particulier. Le développement énorme dans l'utilisation des ordinateurs et des réseaux d'information internationaux en dépit de plusieurs aspects positifs, mais il implique dans les risques l'emportent sur toutes les perceptions de la menace à la sécurité, et il suffit d'une simple pression d'une personne ou d'un groupe de personnes qui Aqaibdoa certaines institutions ou grandes entreprises grandes pertes financières, ou Menacer la sécurité et la stabilité de la société dans son ensemble.
**Mots clés:** criminalité électronique, technologie de l'information, sécurité de l'information et protection.

**مقدمة:**

أصبح الاختراع والابتكار والابداع والمعرفة أساس الثروة والنفوذ والأسلحة الرئيسة للريادة الإقتصادية. وأصبح التقدم الحاصل لا يقاس بحجم الصادرات والواردات بقدر ما يقاس بالقدرة على ملاحقة التطور التقني وثورة المعلومات والإتصالات، وهو الأمر الذي أدى إلى فرض تحديات متزايدة على الدول المتقدمة النامية كل على حدى من الناحية الاقتصادية والاجتماعية.

بالنظر للمعضلات الجيو أمنية، والتحديات متعددة لأبعاد التي باتت تشهدها منطقة الساحل الافريقي، جعلت منها بؤرة توتر وهشاشة تهدد بانفجار الأمن على عدة مستويات من الإقليمي إلى العالمي، فالتطور التكنولوجى على الرغم من آثاره الإيجابية إلا أن له العديد من السلبيات التى تهدد أمن واستقرار المجتمع ليس فى دول الساحل الإفريقي فقط بل في العالم بأسره كما أن التطور الهائل فى مجال استخدام الحاسبات الآلية وشبكة المعلومات الدولية على الرغم من إيجابياته المتعددة إلا أنه ينطوى فى داخله على مخاطر تفوق كافة التصورات فى تهديده للأمن فى المستقبل ويكفى بلمسة واحدة لشخص أو مجموعة أشخاص أن يكبدوا بعض المؤسسات أو الشركات الكبرى خسائر مالية كبيرة، أو يهددوا أمن واستقرار المجتمع ككل.

من أهم العوامل التي أدت إلى انتشار الجريمة الالكترونية هي الثورة التكنولوجية وتطور وسائل الاتصالات، فالعالم في الوقت الحالي يشهد ثورة تكنولوجية هائلة تتجلى أبرز مظاهرها في ثورة المعلومات والاتصالات فبفضل التطور الذي شهدته الأنظمة الإلكترونية في مجال البنوك والقطاعات المالية أصبح بالإمكان تحويل مبالغ كبيرة من النقد حول العالم وبسرعة هائلة مما ساعد المنظمات الإجرامية في تبيض وغسل الأموال الناجمة عن أنشطتها الإجرامية، وحدوث جرائم الانتحار الجماعى للمراهقين من جراء شبكات التعارف والتواصل الالكترونية هذا بالإضافة إلى جرائم خطف الأشخاص والطلاق والسرقة والاغتصاب والتهديد والقذف وتشويه السمعة .

بناءا على ما تقدم ذكره يمكن طرح الاشكالية التالية:

**ماهي جهود الدولة الجزائرية لمواجهة الجريمة الالكترونية في ظل تأثيرات التكنولوجية على أمن منطقة الساحل الإفريقي؟**

تم تناول الدراسة من خلال التطرق الى ثلاثة محاور تنطوي على مجموعة من العناصر قابلة للتحليل.

## I. ماهية الجريمة الالكترونية:

لقد عرف مفهوم الجريمة تطورا نتيجة الإكتشافات والتطورات العلمية والتكنولوجية الحديثة فلم يعد يقتصر مفهوم الجريمة على الافعال والتصرفات والسلوكات التقليدية المخالفة للقانون، وإنما تعداها الى اشكل جديدة، حيث أصبحت الجريمة الالكترونية من السمات البارزة للعصر الحديث،وللإطلاع وبشكل أدق على مفهوم الجريمة الالكترونية لابد من التطرق إلى المفاهيم المرتبطة بها وهي: الحاسب الالي، المعلومات، تكنولوجيا المعلومات والاتصالات.

### 1. تعريف الجريمة الالكترونية:

يعتبر مفهوم الجريمة من أكثر المفاهيم التي عرفت اختلافا واسعا بين الفقهاء والباحثين في مجال السلوك الاجتماعي والقانوني وهذا راجع الى اختلاف الزوايا والتوجهات التي ينظر منها كل باحث في هذا المجال، وعموما يطلق لفظ الجريمة على كل فعل أو سلوك غير مشروع مخالف للحق والعدل المستقيم الذي يترتب عنه عقوبه قانونية.[1]

- **الحاسب الالي**: يعرف الحاسوب بأنه: "وسيلة إلكترونية صممت لاستقبال المجاميع الكبيرة من البيانات بشكل ألي ومن ثمة تخزينها ومعالجتها، وتحويلها إلى شكل نتائج ومعلومات مفيدة وقابلة للإستخدام، بموجب مجموعة من التعليمات والإيجازات التي يطلق عليها إسم البرمجيات، ويتألف الحاسوب من قسمين أساسين يكمل كل منهما الآخر: هما المكونات المادية أو الأجهزة (Hard ware) و المكونات البرمجية (Software)".[2]

إذن فالحاسوب هو عبارة عن مجموعة من الآلات التي تعمل في تناسق منظم مصممة أساسا لمعالجة وتشغيل البيانات واستخلاص نتائج العمليات عليها بدقة وسرعة كبيرة من خلال إتباع توجيهات وأوامر المستخدم أومن خلال برامج وتطبيقات معينة، حيث يتميز الحاسوب بعدة خصائص منها:[3]

- الدقة في أداء العمليات.
- السرعة العالية التي تساعد على توفير الوقت والجهد في أداء العمليات.
- المرونة في الأداء بحيث يمكن للحاسب الآلي أداء عدة مهام في وقت واحد.
- السعة الكبيرة في تخزين البيانات وسرعة استرجاعها عند الطلب.
- قابلية التوسع والنمو في ذاكرته الأصلية، وذلك من خلال إلحاق ذاكرة ثانوية وإضافة ملحقات مساعدة.

- **المعلومات**: هي المعرفة التي تستنتج عن عمليات معالجة الحقائق والبيانات والتي تساعد متخذي القرارات في أية منظمة على اتخاذ القرارات اللازمة لهم من خلال الإعتماد على طريقة التخمين والحكم الحدسي والتي تضطر الإدارة إلى اللجوء إليها في غياب المعلومات حيث أن المعلومات تزيد المعرفة.[4]

- **تكنولوجيا المعلومات والإتصال**: وتعرف على أنّها: "جميع الأجهزة والوسائل التي يستخدمها الأفراد في المنظمة من أجل الحصول على البيانات والمعلومات ومعالجتها لغرض خزنها واستخدامها عند الحاجة، وتتكون تكنولوجيا المعلومات من خبرات الأفراد وأجهزة الحاسوب ووسائل الإتصال الأخرى والبرمجيات ونظم تكنولوجيا المعلومات جميع الوسائل والأدوات اللازمة من الحاسبات الإلكترونية، الإتصالات السلكية واللاسلكية، التكنولوجيا المسموعة والمرئية والطباعة والبرمجيات والخبرات والمهارات المتراكمة والمتاحة والوسائل المادية التي يستخدمها الإنسان في الحصول على المعلومات".[5]

❖ **الجريمة الالكترونية**: لا يوجد إجماع على تعريف الجريمة الإلكترونية من حيث كيف تعرف الجريمة الإلكترونية. فهناك غياب لتعريف عام واطار نظري متسق في هذا الحقل من الجريمة... وفي أغلب الأحيان تستخدم مصطلحات الافتراضية والحاسوبيه والإلكترونية والرقمية وكلها تعكس فجوات مهمة في

تعريف الجريمة الإلكترونية وتعريف الجرائم الإلكترونية باختصار على أنها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية الحديثة.

وتعرف الجريمة الالكترونية على انها كل فعل او سلوك يقع ظمن استخدام لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات دورا اساسيا.[6]

ومن الملاحظ أن أعمال الجريمة الإلكترونية تنشأ في شكل من أشكال النشاط المنظم، مع سوق الجرائم الإلكترونية الأسود، على شكل عمل دورة البرمجيات الخبيثة، وفيروسات الكمبيوتر، وإدارة الروبوتات، وحصاد البيانات المالية، وبيع البيانات، وقبض ثمن المعلومات المالية. لم يعد يحتاج مجرمو الجرائم الإلكترونية مهارات أو تقنيات معقدة وهو ما يعكس درجة خطورة وتطور هذا النوع من الجرائم.

## 2. مراحل تطور الجريمة الالكترونية:

لقد شهدت الجرائم المعلوماتية تطورا ملحوظا منذ نشأتها، مارة في ذلك بعدة مراحل، مما جعلها تمتاز بطابع قانوني خاص نظرا لتميزها بمجموعة من السمات أهمها تعديها للحدود الجغرافية كونها تقع في وسط معلوماتي منفتح، مما وسع من مسرح الجريمة المر الذي أثار عدة إشكالات أهمها الإختصاص الزماني و المكاني. كما أسنها جريمة يصعب اكتشافها و إثباتها كونها جريمة تفتقر إلى الدليل المادي الملموس، وقد مرت جرائم الأنترنت بتطور تاريخي تبعا لتطور التقنية وإستخدامها، ولهذا مرت بثلاث مراحل هي:

- **المرحلة الأولى**: من شيوع إستخدام الحواسيب من السيتينات إلى السبعينات من القرن الماضي إقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر؟. وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم شيء عابر أم ظاهرة إجرامية مستحدثة، وإن الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة ، وإن الجدل حول ما إدا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في بيئة أو مهنة الحوسبة ، ومع تزايد إستخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي إهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ الحديث عنها بوصفها ظاهرة إجرامية لامجرد سلوكيات مرفوضة
- **المرحلة الثانية**: في الثمانينات حيث طفا على السطح مفهوم جديد لجرائم الكمبيوتر والأنترنت وإرتبطت بعمليات إقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج. شاع إصطلاح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لإرتكاب هذه الأفعال ظل محظورا في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقني،ولكن هؤلاء المغامرون أصبحوا أداة إجرام، وظهور المجرم المعلوماتي المتفوق المدفوع بأغراض إجرامية خطيرة القدرة على إرتكاب أفعال تستهدف الإستلاء على المال و التجسس أو الاستيلاء على البيانات السرية والإقتصادية والإجتماعية والسياسية والعسكرية .
- **المرحلة الثالثة**: شهدت سنوات التسعينات تناميا هائلا في حقل الجرائم الإلكترونية وتغيير في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الأنترنت من تسهيل لعمليات دخول الأنظمة وإقتحام شبكة

المعلومات ظهرت أنماط تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعملة المعتاد وأكثر ماموست ضد مواقع الأنترنت التسويقية الهامة التي يتسبب إنقطاعها عن الخدمة ساعات في خسائر مالية بالملايين ، ونشطت جرائم نشر الفيروسات عبر المواقع الإلكترونية لما تسهله من إنتقالها إلى ملايين المستخدمين في ذات الوقت وظهرت الرسائل المنشورة على الأنترنت أو المراسلة بالبريد الإلكتروني المنطوية على الأحقاد أو المساس بكرامة وإعتبار الأشخاص أو المروجة لمواد غير القانونية أو غير المشروعة.[7]

### 3. خصائص الجريمة الإلكترونية:

لقد تعددت صور الجرائم المعلوماتية وتنوعت، وانقسمت في مجملها إلى قسمين جرائم واقعة ضد النظام المعلوماتي كجريمة الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي، وجريمة سرقة المال المعلوماتي وجريمة التلف المعلوماتي، وتتميز الجريمة الالكترونية بعدة خصائص اهمها:[8]

- **جريمة عالمية:** بمعنى انها تتعدى الحدود الجغرافية للدول،إنها جرائم عابرة للقارات ، لأنه مع إنتشار شبكة الاتصالات العالمية والانترنت أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة حيث يمكن ان يكون الجاني في بلد و المجني عليه في بلد آخر.
- **جرائم صعبة الإثبات:** صعوبة متابعتها واكتشافها بحيث لا تترك أثرا فهي مجرد أرقام تتغير في السجلات، فمعظم الجرائم الالكترونية تم إكتشافها بالصدفة وبعد وقت طويل من ارتكابها، ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها على أساس أنها تفتقر إلى الدليل المادي التقليدي كالبصمات. كما يصعب الاحتفاظ الفني بآثارها أن وجدت، تحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي منالها أو التعامل معها،لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع و التضليل بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول الى الدليل وقد يلجا مرتكبيها لتشفير التعليمات لمنع إيجاد أي دليل يدنيه.
- **جرائم ناعمة:** إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة ،وغيرها ، فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي ممكن ، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما.
- **عدم التبليغ:** عند وقوع الجريمة بواسطة الانترنت نجد ان بعض المجني عليهم يمتنعون عن ابلاغ السلطات المختصة خشية على السمعة و المكانه ،و عدم اهتزاز الثقة في كفاءته خاصة اذا كان كيان او هيئة معينة وقد اقترح في و م أ بان تفرض النصوص المتعلقة بجرائم الحاسوب التزاما على عاتق موظفي الجهة المجني عليها، بالإبلاغ عما يقع عليها من جرائم متى وصل الى علمهم ذلك مع تقرير جزاء في حالة إخلالهم بهذا الالتزام.

تعد الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية: إن هذه الجريمة تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على معرفة بتقنيات الحاسب الآلي ، وفي الواقع ليس هناك شعور بعدم أمان تجاه المجرمين في مجال المعرفة المعلوماتية لأن مرتكبيها ليسوا محترفي الإجرام.

### 4. أنواع الجرائم الإلكترونية:

إن الجرائم الالكترونية جرائم متعددة ومتنوعة، ويستعصي حصرها بسهولة ،بحيث توجد عدة تصنيفات لجرائم الحاسب الآلي والانترنت فهناك من يصنفها بحسب الفئات مثل جرائم ترتكب على نظم الحاسب الآلي، أو بحسب الأسلوب المتبع في الجريمة أو الباعث الدافع لارتكابها ،غير أننا يمكن أن نجمل الجرائم التي وردت في أغلب التشريعات على النحو الآتي[9]:

- جريمة الدخول غير المشروع :معناه دخول الشخص إلى شبكة الانترنت بدون ترخيصا من الجهة المخولة منح هذه الصلاحية ،هذا الفعل يؤكد إرتكاب الجريمة عمدا عن طريق خرق التدابير الأمنية بقصد الحصول على بيانات الكمبيوتر .

- تخريب أو إتلاف أجهزة المعلومات أو احدي مكوناتها: إن حماية شبكة المعلوماتية يستلزم التدخل لتجريم الأفعال التي تهدف إلي تخريب أو تعطيل أو إتلاف الأجهزة المادية و المتمثلة في الحاسوب أو البيانات و المعلومات الموجودة بداخله لأن علة التجريم هي حماية المعلومات والأجهزة المادية من أفعال التخريب.

- صناعة الفيروسات أو نشرها: هي وسيلة تستخدم لتدمير المعلومات و البيانات و البرامج و تعطيل شبكة المعلومات.

- الغش أو التغيير في مواصفات و خصائص تقنية المعلومات: تتحقق الجريمة بتغير الخصائص أو المواصفات بسلوك إيجابي يأتيه الفاعل بطرق تدليسية إحتيالية بحيث تعرض تقنية المعلومات أو مكوناتها وما في حكمها إلى الغش الذي يعد انتهاكا لحقوق الملكية الفكرية.

- سرقة الأجهزة والمكونات أو المعلومات: تعتبر جريمة سرقة وإخلال بحقوق الملكية الفكرية أو براءة الاختراع أو العلامات المسجلة على أساس أن محل السرقة الحاسوب ككيان مادي.

- جرائم النظام العام والآداب العامة الاتجار في الجنس البشري: الإخلال بالنظام العام والآداب، إنشاء أو نشر مواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام الآداب، انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة، الإساءة إلى السمعة،والدعارة والمخدرات وغسيل الأموال.

- الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية: إن التمعن في قراءة النصوص المنظمة لجرائم الانترنت في التشريعات العربية تكشف عن حقيقة متواترة في جل هذه التشريعات، ألا وهي اهتمامها الكبير عند تنظيم الانترنت وضبطه، بجعل حماية الدولة وأمنها كهدف أسمى من طرف المشرع قبل حماية أمن المواطن، وهذه مسألة واضحة على مستوى النصوص.

- جرائم الإرهاب الاعتداء على الملكية الفكرية: إن المتضرر الأول من إساءة إستخدام شبكة المعلوماتية حقوق الملكية الفكرية سواء ما يتعلق منها بحقوق المؤلف أو الحقوق المجاورة والمتعلقة بالبرامج والإصدارات الخاصة

بنظم المعلومات أو بالمصنفات الفكرية أو الأدبية أو الأبحاث العلمية التي باتت متاحة على شبكة المعلوماتية ويتم نسخها و تداولها دون أن تنسب إلي صاحبها الأصلي وهو ما يلحق ضررا بليغا بهذه الطائفة من الحقوق التي تعرف بالذهنية أو الفكرية.

- تزوير أو تقليد التوقيع الإلكتروني: الذي هو عبارة عن رموز تميِّز صاحب هذا التوقيع، وهو بهذا المعنى يعد وسيلة تعتمد في المعاملات الإلكترونية ويقوم مقام التوقيع الكتابي.

إنَّ ظاهرة الجرائم الإلكترونية ظاهرة إجراميّة مُستجدَّة نِسبيًّا تقرع في جنباتها أجراس الخطر لتنبِّه مجتمعات العصر الرّاهن لحجم المخاطر، وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة من بيانات، ومعلومات، وبرامج بكافّة أنواعها؛ فهي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون أذكياء، يمتلكون أدوات المعرفة التقنية، تُوَجَّه للنَّيْل مِنَ الحق في المعلومات، وتَطَال اعتداءاتها معطيات الكمبيوتر المخزَّنة، والمعلومات المنقولة، عبر نُظُم وشبكات المعلومات، وفي مقدمتها الإنترنت.

## II. مظاهر التعاون الدولي في مكافحة الجريمة الالكترونية:

إن الطبيعية الدولية للجريمة المعلوماتية استوجبت تعياون دولي من أجل مكافحة فعالة، و لعل من أهم مظيياهر التعاون الدولي التعاون القضائي، ففعالية التحقيق و الملحقة القضائية غالبا ما تقتضي تتبع أثر النشاط الإجرامي، لذلك فان أجهزة إسنفاذ القانون تكون أحيانا بحاجة إلى مساعدة نظرائها في وليات قضائية و من أهم مصادر التعاون القضائي التعاون الأمني والمساعدة القضائية الدولية.[10]

هذه الجرائم و غيرها أدت إلى ظهور تحديات جديدة للمنظومة القانونية على المستوى الدولي، خاصة بعدما ألقت بظلها على العالم بأسره، فتضافرت الجهود من أجل كبح هذه الظاهرة بنجاعة و فعالية، و في إطار الجهد المبذول فان هناك العديد من الهيئات الدولية التي تلعب دورا ملحوظا في هذا المجال على رأسها منظمة الأمم المتحدة التي بذلت جهودا لا يستهان بها، مؤكدة على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون على الحد من انتشار الجريمة المعلوماتية، و هذا من خلال مؤتمراتها لمنع الجريمة و معاملة المجرمين بدءا بالمؤتمر السابع عام 1985 إلى غاية المؤتمر الثاني عشر عام 2010.

إضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات و ذلك تحت إشراف الأمم المتحدة عام 1994 ،الذي نتج عنه عدة توصيات و قرارات ذات صلة بالجرائم المعلوماتية، و قد تضمنت شقين اثنين واحد موضوعي يتناول الفعال التي تقع تحت طائلة الإجرام المعلوماتي، و ثاني إجرامي يتضمن الإجراءات الواجب إتباعها لتطبيق القواعد الموضوعية.

كما كان للمنظمة العالمية للملكية الفكرية دور بارز في هذا المجال، و ذلك من خلل خلقها لنصوص قانونية خاصة بحماية برامج الحاسب الألي و هذا من خلل المادة 04 و 05 من اتفاقية تريبس.

هذا إلى جانب الجهد الكبير المبذول من قبل الإتحاد الدولي للاتصالات وكذا في إطار برنامج الأمن المعلوماتي العالمي المعلن عنه من قبيل الأمين العام للإتحاد عام 2007 ،و الذي يرمي إلى تحقيق عدة أهداف أبرزها

استحداث تشريع نموذجي لمكافحة الجريمة المعلوماتية يمكن تطبيقه عالميا ويكون قابل للاستخدام مع التدابير التشريعية القائمة على الصعيدين الوطني و الإقليمي.

أما من جانب المنظمات الإقليمية فقد كان للإتحاد الأوروبي دور فعال في هذا المجال حيث أثمرت جهوده عن ميلاد أولى المعاهدات الدولية الخاصة بمكافحة الجرائم المعلوماتية بالعاصمة المجرية بودابست عام 2001 ،و قد سعت هذه الإتفاقية إلى بناء سياسية جنائية مشتركة من أجل مكافحة الجرائم المعلوماتية في جميع أنحاء العالم من خلال تنسيق و انسجام التشريعات الوطنية ببعضها البعض، و تعزيز قدرات القضاء و كذا تحسين التعاون الدولي في هذا الإطار، إضافة إلى تحديد عقوبات الجرائم المعلوماتية في إطار القوانين المحلية . كما أنشأ الإتحاد الأوروبي أجهزة تساعد على مكافحة هذا النوع من الجرائم، من بينها جهاز الأيوروبول والمركز الأوروبي لمكافحة الجريمة المعلوماتية و الذي أفتتح في جانفي 2013.

## III. جهود الدولة الجزائرية في مواجهة الجريمة الإلكترونية:

### 1. القوانين المنظمة والعقابية لأشكال الجريمة الالكترونية:

ذهبت الجزائر إلى صياغة مشروع قانون مكافحة الجرائم الكترونية الذي ينص علي جملة اجراءات التي تحدد اليات الرقابة علي الانترنت ومحاربة الجنح المرتبطة بالشبكة الافتراضية وتشمل اجراء المزمع تطبيقها علي الفاعلين في قطاع الانترنت بفرض شروط ورخص جديدة لمولي الانترنت وإلزام هذه الشركات بالحفاظ علي المراسلات الإلكترونية وإجبار مقاهي الانترنت علي التجهيز بكامرات مراقبة وتفعيل حملات تفتيش يقوم بها مصالح الامن بالاضافة الى العقوبة للمخالفات، بالنسبة للتشريع الجزائري فقد احدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات و الجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394المادة مكرر7.[11]

وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون- رقم 06-23 المؤرخ في 20 ديسمبر 2006 حيث مس هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص ، الواردة في هذا القسم من القانون 04-15 وربما يرجع سبب هذا التعديل إلى إزدياد الوعي بخطورة هذا النوع المستحدث من الإجرام بإعتباره يؤثر على الإقتصاد الوطني بالدرجة الأولى وشيوع إرتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وإنتشار الأنترنت كوسيلة لنقل المعلومات.

طبقا لقانون العقوبات المعدل والمتمم الذي أستحدث فيه المشرع الجزائري قسما خاصا في القسم السابع مكرر من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات وعلى هذا الأساس يمكن تصنيفها إلى:

الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات،حذف أو تغيير لمعطيات المنظمة،اد خال او تعديل في نظام المعطيات، تصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار،حيازة أو

إفشاء أو نشر أو استعمال المعطيا، تكوين جمعية أشرار، وتتمثل العقوبات الواردة في نص القانون من خلال المواد التالية:

- المادة 394 مكرر يعاقب بالحبس من ثلاثة اشهر الى سنة و بغرامة من خمسين ألف الى مائة ألف دينار كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الالية للمعطيات أو يحاول ذلك .تضاعف العقوبة اذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظمة . و إذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من 06 اشهر الى سنتين و غرامة من 50000 الى 150000 ألف دينار جزائري.

- المادة394 مكرر1 يعاقب بالحبس من06 اسهر الى03 سنوات وبغرامة من500.000 دج الى2000.000 كل من ادخل بطريقة الغش معطيات في نظام أو أزال او عدل بطريقة الغش المعطيات التي يتضمنها.

- المادة 394 مكرر2 يعاقب بالحبس من شهرين الى03 سنوات وبغرامة من1000.000 دج الى5000.000 دج كل من يقوم عمدا وعن طريق الغش بتصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن ترتكب بها الجرائم المنصوص عليها في هذا القسم. أو حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

- المادة 394 مكرر3 تضاعف العقوبة المنصوص عليها في هذا القسم اذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات اشد.

- المادة 394 مكرر4 يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الاقصى المقرر للشخص الطبيعي

- المادة 394 مكرر5 كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم و كان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.

- المادة 394 مكرر6 مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة و البرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.

- المادة 394 مكرر7 يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها .

إن متابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة. غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية[12] كما نص على التفتيش في المادة

45 الفقرة 7من نفس القانون [13] المعدلة حيث أعتبر إن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطته المشرع بقواعد صارمة،وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم ألكترونية. ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 [14]وكذا على "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5/ 10.[15]كما أن قانون الإجراءات الجنائية نص على ألا يجوز ضبطها إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة. غير أنه طبقا لقانون الإجراءات المعدل و المتمم في الفصل الرابع تحت عنوان "في إعتراض المراسلات و تسجيل الأصوات و إلتقاط الصور". نصت المادة (65 مكرر5/3)على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن بالإعتراض و وضع ترتيبات تقنية دون موافقة المعنيين من أجل إلتقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة[16]. أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية.

كما جاء القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها منظما للجرائم المتصلة بتكنولوجيا الإعلام والإتصال وكل ما يتعلق بالمنظومة المعلوماتية، والمعطيات المعلوماتية، ومقدمو الخدمات، والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية.من مراقبة و تفتيش المنظومات المعلوماتية عند الضرورة،و حجز المعطيات المعلوماتية،و حفظ المعطيات المتعلقة بحركة السير.على الإلتزامات الخاصة بمقدمي خدمة الإنترنت ،وأخيرا على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[17] بالاظاثة إلى العديد من القوانين الأخرى التي تنظم الجريمة الإلكترونية وتحمي التحويلات المالية كقانون البريد والاتصالات السلكية واللاسلكية(رقم 03- 2000 المؤرخ في2000/08/05 )، وقانون التأمينات.

## 1. هياكل والهيئات القائمة للمواجهة الجرائم الإلكترونية:

**+الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:** وأنشئت بموجب القانون رقم04-09 المؤرخ في 5 أوت 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقاية، ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية،في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية أللاقتصاد الوطني.

**+الهيئات القضائية الجزائية المتخصصة:**أنشئت بموجب القانون 14/04المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد329،37،و40 من ق.إ.ج.ج.تتمتع اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في 2006/01/05.بحيث تنظر فيالقضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى

ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04.

+**المعهد الوطني للأدلة الجنائية وعلم الجرائم**: يتكون من احدى عشرة دائرة متخصصة في مجالات مختلفة ، جميعها تضمن إنجاز الخبرة ، التكوين والتعليم و تقديم المساعدات التقنية ،و دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات.

+**المديرية العامة للأمن الوطني**: تتصدى هذه المديرية للجريمة الإلكترونية من عدة جوانب وأ منها الجانب التوعوي بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعية وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

ودائما في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم ،أكدت الجزائر عضويتها الفعالة في:

- المنظمة الدولية للشرطة الجنائيةINTERPOL هذه الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا.
- منظمة الشرطة الجنائية الإفريقيةAFRIPOL بعد نشأتها وتدشين مقرها بالجزائر يوم 13 ديسمبر2015 ، سعيا لتسهل تبادل المعلومات بين قوات الشرطة الوطنية بخصوص الجريمة الدولية والارهاب والمخدرات والاتجار بالأسلحة في أفريقيا.

**الخاتمة:**

جاء انتشار الجريمة الإلكترونية وتطوّر هذا النوع من الجرائم بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا التي يسرت سبل التواصل وانتقال المعلومات بين مختلف الشعوب والحضارات وسهلت حركة المعاملات ما أدى إلى إستخدامها في الجوانب السلبية والإجرامية من طرف بعض الأشخاص والتنظيمات. فجرائم الإنترنت ذات بعد دولي ولا تحدها حدود وطنية أو قومية مما يتطلب تعاونا دوليا للحد منها خاصة اذا تعلق الأمر بدول الساحل الإفريقي في ظل غياب سيطرة كاملة على هذا النوع من الجرائم والتي تكاد تنعدم فيه آليات التصدي من طرف هذه الدول وتصبح التنظمات والفئات الإجرامية تنشط بكثرة، ما ينعكس بالضرر الكبير على دول الجوار منها الجزائرفرغم صعوبة ضبط و مكافحة جرائم الانترنت على الصعيد الوطني أيضا إلا أن هناك جهود معتبرة قام بها المشرع الجزائري في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم حاول المشرع الجزائري، إصدار قوانين عامة وخاصة وهياكل وأجهزة للتصدي للجرائم الإلكترونية. ومن التوصيات التي من شأنها محاربة مثل هذه الجرائم المستحدثة والمنجرة عن التطور التكنولوجي والتي تأثر بطريقة أو بأخرى على الأمن الدولي والإقليمي:

-ضرورة مراجعة التشريعات الوطنية لهده الدول من خلال تشديد العقوبات على المتسببين والمشاركين في الجريمة الالكترونية.

-تعديل التشريعات بما يتلائم مع طبيعة جرائم الإنترنت والتقنية، تتناسب والتطورات التكنولوجية الحاصلة.

-إبرام اتفاقات دولية وإقليمية في مجال مكافحة الجرائم المعلوماتية،

-فتح أبواب التعاون فيما بين هذه الدول في الكشف وإثبات الجريمة الالكترونية وتبادل المعلومات وتسليم المجرمين.

-انشاء مركز معلومات وهيئة مشرفة على مثل هذه الجرائم بين مختلف الدول توفير كافة الوسائل المادية والتقنية اللازمة.

-تفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكة الاتصالات العالمية وحثهم على الاستخدام الأمثل لهذه التقنيات.

-تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة الجريمة الالكترونية والحد من أثارها.

## الهوامش:

[1] نجيب بوالماين،"الجريمة والمسألة السوسيولوجية"،(أطروحة دكتوراه، جامعة قسنطينة، كلية العلوم الإنسانية والاجتماعية، 2008)، ص32.

[2] عامر ابراهيم قندلجي، إيمان فاضل السمرائي، تكنولوجيا المعلومات وتطبيقاتها. عمان: مؤسسة الوراق للنشر والتوزيع، 2009، ص 120.

[3] محمد محمد الهادي، "نحو توظيف تكنولوجيا المعلومات لتطوير التعليم في مصر"، أبحاث المؤتمر الثاني لنظم المعلومات وتكنولوجيا الحاسبات، 13-15 ديسمبر1994، القاهرة : المكتبة الأكاديمية، ص 273.

[4] علاء عبد الرزاق السالمي، نظم إدارة المعلومات، ط3، الدوحة: المنظمة العربية للتنمية الإدارية، 2013، ص 4.

[5] محمد الهاشمي حجاج، حسام مسعودي، "دور تحديث أنظمة المعلومات في تفعيل الممارسة المحاسبية"، الملتقى الوطني حول واقع وأفاق النظام المحاسبي المالي قي المؤسسات الصغيرة والمتوسطة في الجزائر، كلية العلوم الإقتصادية والتجارية وعلوم التسيير، جامعة الوادي الجزائر،05- 2013، ص5.

[6] Leukfeldt, R. and Veenstra S., & Stol W. High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 January – June 2013, Vol 7 (1): 1–17

[7] بوعزة سعيدة، الجريمة الإلكترونية في التشريع الجزائري"، مذكرة ماستر، جامعة محمد خيضر- بسكرة كلية الحقوق والعلوم السياسية، تخصص قانون ال، 2016)، ص 16.

[8] عبد الفتاح مراد، شرح التحقيق الجنائي الفني والبحث الجنائي. القاهرو: دار الكتب والوثائق المصرية،2006 ، ص 46.

[9] محمد السعيد رشدى ، الانترنت والجوانب القانونية لنظم المعلومات، جامعة حلوان: المؤتمر العلمي الثاني حول الاعلام والقانون ، كلية الحقوق، من 14-15 مارس 1999، ص 3 -5.

[10] قداري امان، مكافحة الجرائم المعلوماتية في القانون الدولي، في الموقع الالكتروني: http://rdoc.univ-sba.dz/handle/123456789/665?mode=full&submit_simple=Affichage+d%C3%A9taill%C3%A9

[11] القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم- 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات.

[12] المادة 37 من قانون الإجراءات الجنائية المعدل والمتمم بأمر رقم 15-02 مؤرخ في 23 يوليو سنة 2015 ،يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية،الجريدة الرسمية عدد 40.

[13] المادة 45 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 ص 6.

[14] المادة 51 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84،ص7.

[15] فصل رابع بعنوان "في اعتراض المراسلات و تسجيل الأصوات والتقاط الصور المواد من 65 مكرر5 حتى 65 مكرر10. بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006، الجريدة الرسمية عدد84، ص8.

[16] القانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر 2006، يعدل و يتمم الأمر رقم 155-66، المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966. و المتضمن قانون الإجراءات الجنائية الجزائري. المادة 65 مكرر 3/5 "إذا أقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أوالإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص بأن يأذن بما يأتي : – وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية...

[17] قانون رقم04-09 المؤرخ في 2009/08/05 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، المواد من 2 إلى 14.