

الجهود الدولية لمكافحة الجريمة الالكترونية

أ.د. بن عائشة نبيلة^{1*}، أ.د. القينعي بن يوسف²

1. جامعة المدية، الجزائر nabila.benaicha@gmail.com

2. جامعة المدية، الجزائر، benublida@gmail.com

تاريخ الاستلام: 2025/04/20 تاريخ القبول: 2025/05/10 تاريخ النشر: 2025/06/30

ملخص:

تعد ظاهرة الجرائم الالكترونية من الظواهر الاجرامية المتطورة والمتجددة والعابرة للحدود ، وهو ما دفع الى قرع اجراس الخطر لتنبيه المجتمع الدولي نظرا لحجم التهديدات الخطيرة الناجمة عنها، باعتبارها تستهدف الاعتداء على الانظمة الالكترونية للمواقع الاستراتيجية للدولة، فهي جرائم الكترونية تنشا في الخفاء وباستخدام تقنيات تكنولوجية حديثة، والتي يوجهونها الى اختراق الحق في المعلومات وتطال اثارها نظام المعلوماتية و في مقدمتها المواقع الرسمية للدولة، و لهذا اصبحت هذه الجرائم الالكترونية محل متابعة جنائية سواء في اطار القوانين الوطنية والدولية.

وعليه كان التفكير و التخطيط لتعاون السلطات في انحاء العالم بتطوير القدرة على التعاون الدولي الفعال في مجال مكافحة الجريمة الالكترونية من خلال ايجاد ارضية صلبة من التعاون والتفاهم من اجل عالم يسوده الامن و الاستقرار.

الكلمات المفتاحية : الجريمة الالكترونية ، حماية نظام المعلومات، التشريع الجزائري، التعاون الامني الدولي.

Abstract:

Cybercrime is one of the most advanced, renewable and cross-border criminal phenomena, which has sounded the alarm for the international

community due to the scale of the serious threats it poses, as it aims to attack the electronic systems of strategic state sites that they manage in order to penetrate the right to information, and its effects affect the information system, foremost among which are official state sites. For this reason, these electronic crimes have become the subject of criminal prosecution, both under national and international laws. Consequently, thinking about and planning cooperation between authorities around the world involved developing the capacity for effective international cooperation in the fight against cybercrime by finding a solid basis for cooperation and understanding for a world of security and stability.

Keywords: electronic crime, protection of information systems, Algerian legislation, international cooperation on security

مقدمة:

استعمل المشرع في الجريمة الالكترونية مصطلح الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات لتعبير عن الجريمة السيبرانية، وهذا ما يظهر من خلال القانون 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها حيث جاء في المادة 2 منه " يقصد في مفهوم هذا القانون الجرائم المتصلة بتكنولوجيات الاعلام والاتصال : جرائم الماسة بأنظمة المعالجة الآلية للمعطيات..."

واستعمل بموجب الأمر 11-21 المؤرخ في 25 أوت 2021، المتضمن قانون الاجراءات الجزائية، مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية في المادة 211 مكرر 24 .

أما المادة 211 مكرر 22 استعمل الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، كل جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الاعلام والاتصال.

وعليه تطرح الاشكالية التالية : ما مفهوم الجريمة الالكترونية ومدى معالجتها ومكافحتها دوليا ووطنيا ؟.

1. مفهوم الجريمة الإلكترونية:

لقد أدى ظهور شبكات الإعلام الآلي والانترنت وانتشارها إلى العمل على تعزيز التواصل الاجتماعي والثقافي والحضاري، وإلى كسر الحواجز والحدود الجغرافية بين الأمم، إلا أنها من جانب الآخر ساعدت على انتشار الجريمة بمختلف أشكالها، حتى أصبحت تسمى بعوامة الجريمة الإلكترونية. (غريب، ص73)

1.1. تعريف الجريمة الإلكترونية:

أمام تعدد الآراء بشأن مفهوم الجريمة الإلكترونية، تبنى كل رأي مفهوما مرتبطا بالزاوية التي ينظر من خلالها إلى الموضوع، فهناك جانب من المختصين عرفها من زاوية تقنية، وأخرى قانونية، وهناك من عرفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استنادا لمعايير أخرى حسب القائلين بها. وهذا ما أعاق منظمة الأمم المتحدة إلى عدم التوصل لتعريف متفق عليه دولية، ولكن ورغم صعوبة إيجاد تعريف لهذه الظاهرة وحصرها في نطاق محدود وضيق، إلا أن مكتب تقييم التقنية في الولايات المتحدة عرفها من خلال تعريف جهاز الكمبيوتر بأنها: تمثل "الجرائم التي تقوم فيها بيانات الكمبيوتر والبرامج المعلوماتية بدور رئيسي"، كما أنه عرفها ب: "نشاط جنائي يمثل اعتداء على برامج وبيانات الحاسب الإلكتروني"، وأيضا بأنها: "كل إستخدام في صورة فعل أو إمتناع غير مشروع للتقنية المعلوماتية ويهدف إلى الإعتداء على أية مصلحة مشرعة، سواء أكانت مادية أو معنوية. ورغم الفارق بين مجالات جرائم أجهزة الكمبيوتر وشبكات الإنترنت، فبينما تتم الأولى بالإعتداء على مجموعة الأدوات المكونة للكمبيوتر وبرامجه والمعلومات المخزنة به، فإن الثانية تتعلق بجرائم شبكات الإنترنت التي تتم عبر نقل المعلومات والبيانات بين أجهزة الكمبيوتر وخطوط الهاتف. إلا أن الواقع التكنولوجي أدى إلى تزاوج بين المجالين (الكمبيوتر والإنترنت) وظهور مصطلح الجريمة الإلكترونية .

وفي الواقع، فإن هذه الجريمة التي يكون الهدف منها الوصول إلى المعلومات هي في الأغلب تصنف ضمن حالات الجرائم الإقتصادية، وتكون بغرض الحصول على مزايا أو مكاسب إقتصادية، لأن الحرب الإقتصادية لا تقل ضرورتها وخطورها الحالية عن الحروب العسكرية، إلا أنها تتحقق عبر شبكات الإنترنت. والظاهر أن كل الدراسات والنظريات الخاصة بالجريمة الإلكترونية تلتقي عند نقطة مركزية، تنحصر عموما في الغاية المادية البحتة التي يسعى إلى إنجازها هؤلاء المجرمين، بواسطة الإعتداء على البيانات والمعلومات السرية، وتدمير البرامج المعلوماتية لأية دولة لتهديدها وضرب أمنها الوطني، وخلق حالة من الفوضى

الإلكترونية والمعلوماتية في مؤسساتها الحساسة، ولعل خير مثال على ذلك اقتحام موقع البنتاغون الأمريكي، لتعود في صورة جديدة على شاكلة ما يعرف بالإرهاب الإلكتروني الذي بات خطراً حقيقياً يهدد سلامة وأمن المجتمع الدولي، عن طريق التهديد بنسف المعلومات وتدمير استراتيجيات الدفاعات الاقتصادية والأمنية للبدان وعوائلها المالية، باستعمال أنواع الفيروسات المدمرة والخطط التخريبية لتدمير العديد من البرامج المعلوماتية الحساسة للدول. (حكيم غريب : المرجع السابق ، ص 74).

وعليه من خلال ما تقدم تعتبر هذه الجريمة التي ترتكب من تنظيم إجرامي هيكلي يتكون من ثلاثة اشخاص فاكتر ، تحكمه قواعد معينة اهمها قاعدة السرية ، ويعمل بشكل منتظم ، وبشكل مستمر لفترة غير محددة، ويعبر نشاطه حدود الدول، ويستخدم العنف و الفساد و الابتزاز و الرشوة في تحقيق اهدافه للحصول على الربح المادي. (سلمى سبع، ص759).

جرت العادة عند القانونين أن التعاريف من اختصاص الفقه والقضاء ، وبالتالي عادة ما يتجنب المشرع الخوض في التعاريف، غير أن المشرع في الجريمة الالكترونية استعمل مصطلح الجرائم الماسة بأنظمة المعالجة الآلية لمعطيات لتعبير عن الجريمة السيبرانية، وهذا ما يظهر من خلال القانون 04-09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها(القانون 04-09 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال ومكافحتها، الجريدة الرسمية الصادرة بتاريخ 16 اوت 2009 ، العدد 47). حيث جاء في المادة 2 منه " يقصد في مفهوم هذا القانون الجرائم المتصلة بتكنولوجيات الاعلام والاتصال : جرائم الماسة بأنظمة المعالجة الآلية للمعطيات..."

استعمل بموجب الأمر 11-21 المؤرخ في 25 أوت 2021، المتضمن قانون الاجراءات الجزائية، مصطلح الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية في المادة 211 مكرر 24. (الامر 11-21 المؤرخ في 25 اوت 2021، المتتم بالامر 66-155 المؤرخ في 08 جويلية 1966 المتضمن قانون الاجراءات الجزائية).

أما المادة 211 مكرر 22 استعمل الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ، كل جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الاعلام والاتصال.

2.1. خصائص الجرائم الإلكترونية:

إن أهم ما تتصف به هذه الجرائم الإلكترونية سهولة إرتكابها بعيدا عن الرقابة الأمنية، وصعوبة التحكم في تحديد حجم الضرر الناتج عنها قياسا بالجرائم التقليدية، وأن مرتكبيها هم من بين فئات مختلفة تجعل من التنبؤ بالمشتبه بهم أمر في غاية الصعوبة وتنطوي على سلوكيات غير مؤلفة عن الأفراد، وسهولة إئتلاف من قبل الجناة، بالإضافة إلى كونها جريمة عابرة للحدود لا تعترف لا بمكان ولا بالزمان، فهي تتصف بالتباعد الجغرافي بين الجاني والمجني عليه، أما مرتكبيها فهم المحترفون Crachers والقراصنة Hackers، وكذا المخادعون Freudians، وأهم ميزات مرتكبي هذه النوعية من الجرائم هم أشخاص شخص ذوو مهارات فنية عالية متخصصون في الإجرام الإلكتروني وأشخاص قادرين على إستعمال خبراتهم في الإختراقات وتغيير المعلومات.

وفي هذا الإطار، يدرك القراصنة إن الدافع لإرتكاب الجرائم الإلكترونية يغلب عليه الرغبة في قهر النظام، أكثر من شهوة الحصول على الربح، حيث يميل أغلبهم إلى إظهار تفوقهم ومستوى إرتقاء براعتهم وذكائهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة يحاولون بواسطة إيجاد الوسيلة التي تمكنهم من تحطيمها، بل والتفوق عليها).

ولقد تعددت الدراسات التي تتحدث عن سمات مرتكبي الجرائم الإلكترونية وشخصيتهم، ومدى جسامة جرمهم كأساس لتبرير وتقدير العقوبة التي يستحقونها، فنجد أن هناك سمات مشتركة بين هؤلاء المجرمين، أهمها ذلك المجرم المتخصص الذي له قدرة فائقة في المهارة التقنية، ويستغل مداركه ومهاراته في إختراق الشبكات، وإختراق كلمات المرور أو الشفريات، ويسبح في عالم الشبكات ليحصل على كل غالي وثمين من البيانات والمعلومات المتوفرة على أجهزة الكمبيوتر، وهناك أنموذج آخر من المجرمين وهو المجرم العائد للإجرام، حيث يتصف بأنه عائد للجريمة، فهو يوظف مهاراته في كيفية عمل أجهزة الكمبيوتر، وكيفية تخزين المعلومات والبيانات، والتحكم في أنظمة الشبكات والدخول المتكرر وغير المصرح به، فهو قد لا يحقق جريمة الإختراق بهدف الإيذاء وإنما نتيجة شعور بقدرته ومهاراته في الإختراق، إضافة إلى صنف آخر وهو المجرم المحترف، والذي له من القدرات والمهارات التقنية ما يؤهله لأن يوظفها في الإختراق والسرقة والنصب، والإعتداء على حقوق الملكية الفكرية، وغيرها من الجرائم مقابل المال، أما المجرم الذكي، حيث

يملك من المهارات ما يؤهله أن يقوم بتعديل وتطوير في الأنظمة الأمنية حتى لا تستطيع أن تلاحقه وتتبع جرائمه من خلال أجهزة الكمبيوتر.

ومن جانب آخر أكدت بعض الدراسات والأبحاث الأكاديمية على أن فئات المجرمين في عالم الجريمة الإلكترونية تنحدر من:

1 - مستخدموا كمبيوتر البيت.

2- الموظفون الحكوميون الساخطون على مدرائهم ومسؤوليهم.

3- المتسللون، ومنهم الهواة أو العابثون بقصد التسلية.

4- المحترفون الذين يتسللون إلى مواقع مختارة بعناية، ويعبثون أو يتلفون النظام، أو يسرقون محتوياته، وتقع أغلب جرائم الإنترنت حالية تحت طائلة الأعمال الإرهابية.

5- العاملون في الجريمة المنظمة.

ولقد بات الإرهاب الإلكتروني Cyber Terrorism الذي يهدد البنية التحتية للمجتمعات الحديثة من خلال إستخدام التقنيات العالية والمعقدة في الهجمات ضد المؤسسات الحكومية والشركات الإقتصادية أداة في إمكان التنظيمات الإرهابية إستخدامه عبر شبكة الإنترنت وذلك من خلال توسيع أنشطتها الإرهابية في التجنيد والتوجيه، أو التمويل والتغلب على الإجراءات الأمنية والقضائية، والسماح لبعض الأشخاص والهيئات المطلوبة أمنية وقضائية في العديد من البلدان والمدرجون على قوائم الإرهابيين من إدارة المواقع على شبكات الإنترنت.

ويعد الإرهاب الإلكتروني نمطا جديدة من الإرهاب الذي لا يعتمد على إستخدام الأسلحة وإنما عبر توظيف الإرهابيين للأنظمة المعلوماتية للإعلام الآلي ضد الأنظمة المدنية والعسكرية، وهوما يؤدي إلى تهديد الأمن الوطني والدولي على حد سواء، وخير دليل على ذلك إختراق ما يسمى بتنظيم داعش في الآونة الأخيرة مواقع شبكة "تي في 5 موند" وتعطيل شبكات القناة لمدة يوم كامل، والسؤال الذي يطرحه الكثيرون هو كيف يمكن ربط شبكة البث التلفزيوني بشبكة المعلوماتية العادية للشبكة، والتي يسهل النفاذ إليها؟ إلى حد أن الهجوم قد نجح بصورة كبيرة على المستوى الإعلامي في تلميع صورة التنظيم، كما نجح الهجوم الإلكتروني على المستوى التقني في شل قناة تلفزيونية، وهي سابقة خطيرة، ولإن الهدف الرئيسي للإرهابيين في السيطرة على القناة، يكمن في مقدرتهم على بث أفلام تنظيم "داعش" الدعائية. (حكيم غريب ، ص 74).

3.1. مظاهر تحديات الجريمة الإلكترونية:

ترتب على ظاهرة الجريمة الإلكترونية رهانات وتحديات عديدة، ومن أفدحها تنامي الأنشطة الإجرامية الإلكترونية، وتوصل مرتكبوها بتقنيات عالية التكنولوجيا غير مسبقة، في مجال تكنولوجيا المعلومات والاتصالات يسرت لهم القيام بهذه الأعمال الإجرامية والإرهابية، داخل حدود الدولة وخارجها، وهو الأمر الذي أدى إلى دق ناقوس الخطر لدى المنظمات والمؤسسات الدولية والبحث عن الآليات والتدابير لمكافحة هذه الظاهرة، ودعوة المجتمع الدولي إلى التصدي لها ومجابهتها.

وعلى خلفية ما ذهب إليه البعض من أن القوانين القائمة تكفي في حد ذاتها لمواجهة الجرائم الإلكترونية، فالواقع إن كان لهذا الرأي شيئا من الواقعية، أن معظم النصوص الموجودة تواجه بعض الأنشطة المجرمة التي ترتكب عن طريق الإنترنت، فإنه ينبغي ألا ننكر أن هناك نصوص قانونية لم تعد تتماشى مع تطور الجريمة الإلكترونية، وظهور الإرهاب الإلكتروني كمبدأ الشرعية الجرائم المستحدثة والعقوبات والتفسير الضيق والمحدود لأبعادها.

فلقد إستغلت العديد من التنظيمات الإرهابية الطبيعة الإتصالية لشبكة الإنترنت من أجل نشر أفكارها ومعتقداتها، بل تعداه الأمر إلى ممارسات تهدد أمن الدول الذي أخذ منحى خطيرا في إستخدام الإنترنت في إرتكاب جرائم غاية في الفتك في حق المجتمعات، وبث ثقافة الإرهاب عبر الإنترنت عن طريق تصميم مواقع إفتراضية تمثل الجماعات الإرهابية، وهي مواقع أخذت في تنامي وارتفاع مع زيادة عدد الجماعات الإرهابية، حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى العمليات الإرهابية التي تم إرتكابها بها، ويبقى خير مثال في إستخدام الإنترنت بصورة مؤثرة وعالية الدقة في تصوير الجرائم المتوحشة والخطيرة، هو تنظيم داعش، فقد إستطاع هذه التنظيم من خلال الإنترنت تجنيد المقاتلين الأجانب، وهم في أغلبيتهم من فئة الشباب ضعاف العقيدة والفكر، فتعلن الجماعات الإرهابية عبر مواقعها على الإنترنت عن حاجتها إلى عناصر إنتحارية، كما لو كانت تعلن عن وظائف شاغرة للشباب، مستخدمة في ذلك الجانب الديني، فدائما ما تصف الأهداف التي تستهدف عملياتهم بالكافرة، وتقوم بدعوة الشباب إلى الجهاد وحثهم على الإستشهاد في سبيل الله، والفوز بالجنة.

للإشارة، أنه إذا كانت الجماعات الإرهابية تعمل إلى الدعاية والترويج لنفسها عن طريق آليات مختلفة، منها جذب إنتباه وسائل الإعلام المعروفة لتغطية أخبارها وجرائمها، كل ذلك يمثل قيودا على إفادة التنظيمات الإرهابية من نشر وسائل الإعلام عنها، بينما في المقابل تتيح المواقع الإلكترونية للتنظيمات الإرهابية قدرة كبيرة من التحكم في نظام المعلومات، ونشر رسائلها الإعلامية التي تود ترويجها، بل أيضا تتيح لها المرونة في توجيه الرسائل لفئات مختلفة من الجمهور المستهدف، ورسم صورة ذهنية عن الجماعة وعن أعدائها أيضا.

وتستعمل الجماعات الإرهابية - الإنترنت إلى جانب أغراض الدعاية والترويج. في نشر معلومات مضللة أو مغلوطة، ونشر تهديدات وصور ولقطات فيديو مرعبة. وبناء على مميزات الشبكة العالمية للإنترنت التي منحت للجماعات الإرهابية الكثير من المساحات الحرة والخيارات من خلال عدم خضوعها لأي رقابة، وعبرها للحدود الجغرافية بين الدول، ونموها السريع المتواصل، مع ما تمنحه من القدرة للجماعات الإرهابية في التخفي وعدم المواجهة نتيجة للإفتراضية التي تعد من أهم خصائص هذه الشبكة التي باتت من أهم مقومات المجتمع المعلوماتي التي تؤدي إلى الانحراف الفكري، من خلال تعرض فئات الشباب الى الكثير من المؤثرات الفكرية و الإيديولوجية.

2. الجهود الدولية و الوطنية في مكافحة هذه الجريمة:

عملت المجتمعات والدول عبر فترات متلاحقة في سن تشريعات ونصوص من أجل مكافحة الجريمة الإلكترونية، إلا أن هناك صعوبات كثيرة تواجه التعاون الدولي، لاسيما فيما يخص عدم وجود أ نموذج موحد للنشاط الإجرامي، الأمر الذي يقتضي توحيد هذه النظم القانونية، وإلستحالة ذلك فإنه لا مناص من البحث عن وسائل متعددة تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع الجديد من الجرائم، ويخفف من كثرة الفوارق بين الأنظمة القانونية والأمنية بين الدول، وتتمثل هذه الوسيلة في تحديث التشريعات الوطنية المعنية بالجرائم الإلكترونية، وعقد إتفاقات متعددة الأطراف وثنائية، يراعى فيها هذه النوع من الجرائم، إضافة إلى أن وجود الصكوك الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من الفوارق وأوجه الاختلاف بين الأنظمة القانونية والإجرائية، ويفتح المجال أمام تعاون دولي فعال، فمثلا المادة (20) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، تشير في هذا النطاق إلى التسليم المراقب والمراقبة الإلكترونية وغيرها، من أشكال المراقبة والعمليات المخفية، والتي تعد من أهم التقنيات المستخدمة

في التصدي للتنظيمات الإجرامية المنظمة، وذلك بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات، لاستخدامها فيما بعد في المتابعات القضائية الوطنية منها أو الدولية، في دول أطراف في سياق نظم المساعدة القانونية المتبادلة وهذا ما أكدت عليه الإتفاقية الأوروبية للإجرام الإلكتروني، حيث نصت المادة (29) على سرية حفظ البيانات المعلوماتية المخزنة، وأجازت لكل طرف أن يطلب الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك، كما نجد في النص الثاني من المادة (27) من الإتفاقية الأوروبية بشأن الإجرام الإلكتروني، التي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة الإتصال التي تعمل لمدة 24 ساعة يوميا، طوال أيام الأسبوع، لكي تؤمن المساعدة المباشرة التحقيقات المتعلقة بجرائم البيانات والشبكات، هذا بالإضافة إلى القيام ببعض العمليات المشتركة بين الدول، في مجال تدريب مختصين في هذا المجال الواسع.

ولأجل ذلك كان لا بد أن تكون هذه الأجهزة على درجة كبيرة من الكفاءة والمعرفة، والقدرة على كشف غموض هذه العمليات الإجرامية التي قد تمس بكيان الدولة، والقبض على مرتكبيها بسرعة ودقة متناهيين، وهذا لا يتحقق إلا بالتدريب، لأن المواجهة والتصدي لها لا بد أن تركز على كيفية تطوير أساليب العمل والتكوين والتأهيل وكسب الخبرات في إطار التعاون الدولي المكثف والفعال، وليس هذا فحسب، بل يجب على السلطات الأمنية أن تعمل إلى استقطاب المتخصصين والكفاءات في المجال الإلكتروني والمعلوماتي وضمهم إلى مصالحيهما. (حكيم غريب ، ص 78).

1.2. التعاون الأمني على المستوى الدولي:

تستدعى عملية الإستمرار في محاربة هذه الظاهرة المتعددة الأوجه والمخاطر تظافر جميع الدول المساهمة فيها إلى توفير قدر من الأمن والنظام، ولاسيما وأن الواقع العملي قد ظهر أن الدولة لا تستطيع بمجدها المنفردة القضاء على الجريمة بكل أشكالها، في ظل التطور المذهل في كافة مجالات الحياة، خاصة في ميدان الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت، ولأن الإنتشار الكبير والسريع لها قد أدى إلى ظهور أشكال وصور جديدة من الجرائم الإلكترونية، التي أصبحت خطرا على سرية النظم الحاسوبية، بل تعدت إلى أمن البنى الأساسية والإستراتيجية للدول، نظرا لتمييزها بطابع العالمية، وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الأمني، حيث يسمح بالإتصال المباشر بين مختلف مصالح الأمن في الدول، وذلك بتأسيس مكاتب متخصصة لجمع المعلومات عن مرتكبي هذه

الجرائم وتعميمها، ثم التبادل المعلوماتي بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من العقاب.

وعلى الرغم من أن التعاون الدولي بكافة صوره في عالم مزدحم بشبكات إتصالية حساسة ومتطورة تنقل المعلومات والبيانات من مناطق متباعدة باستخدام التقنيات، إلا أن لا تكفل لها أمنا فعالا، ويتاح في ظلها التلاعب - عبر الحدود- بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أضرارا خطيرة، خاصة في ظل عدم وجود أنموذج موحد للنشاط الإجرامي.

2. الجرائم الإلكترونية والمشرع الجزائري:

لقد عمل المشرع الجزائري على مواكبة مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الإلكترونية، بما فيها شبكة الإنترنت، تلك خاصة التي تسعى إلى الحد من الإستخدام غير المشروع لها، وذلك مراعاة منه لما يشهده العالم من تطورات حديثة في مجال تكنولوجيا الإتصالات والمعلومات، وكذلك إيماننا منه أن السلطات الجزائرية ليست بمعزل عن التهديدات الأمنية الجديدة في الفضاء الافتراضي، وقد تطرق المشرع الجزائري إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين أهمها (الأمر 03-06 المؤرخ في 19 جويلية 2003)، والمتعلق بالعلامات التجارية، لذلك نجد أن أصحاب البرنامج عمدوا إلى تسجيل هذا الإسم كعلامة تجارية للبرنامج، وذلك لما يتضمنه هذا النوع من أهمية في الحماية.(الامر 03-06 الجريدة الرسمية العدد 44).

ولقد تدارك المشرع الجزائري خلال الأعوام الأخيرة، ولو نسبياً، الفراغ القانوني في مجال الإجرام الإلكتروني، خصوصاً بموجب القانون 04-15 المتضمن تعديل قانون العقوبات،(القانون 04-15 قانون العقوبات). الذي بموجبه جرم جريمة التوصل أو الدخول غير المصرح به، وجريمة التزوير المعلوماتي وجريمة الإستلاء على المعطيات المخزنة أو المعالجة عن طريق منظمة معلوماتية، إضافة إلى جريمة إتلاف وتدمير المعطيات.

وبالمحصلة، فإن المشرع الجزائري رغم تداركه لهذا الفراغ القانوني في مجال الإجرام المعلوماتي، والجهود المبذولة للحد من هذه الظاهرة، سواء كانت من طرف السلطات الأمنية أو الضبطية القضائية، إلا أن هذه الجهود تصطدم بعدة صعوبات منها التي تظهر من خلال لا مادية الجريمة الإلكترونية، وصعوبة إكتشاف وإثبات الجريمة الإلكترونية يقودنا إلى صعوبة إثباتها، لان المجرمين يسعون بشتى الوسائل لكي لا يتركوا وراءهم آثارا تدل على ارتكابهم للجريمة، وتكمن الصعوبة في نطاق الجرائم المرتكبة عبر الإنترنت في ظل لا ماديتها، وهو الأمر الذي يجعل إسناد الفعل غير المشروع إلى المجرم شبه مستحيل وتبقى الجريمة الإلكترونية من أهم

الجرائم المستحدثة لا تصل إلى علم الجهات الأمنية والقضائية بطريقة إعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية لا تخلف آثار مادية، كذلك التي تخلفها الجريمة العادية. إن العديد من الجرائم المرتكبة عبر الشبكة العنكبوتية تتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية، كجرائم التجسس العسكري والإقتصادي وجرائم الاختلاس، التي تتم عبر تعديل البرامج. والتلاعب بالأنظمة المعلوماتية، فالجناة يعمدون عادة إلى إخفاء جرائمهم، وبوساطة إزالة آثارها عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الحاسوب الآلي والبرامج، ودون ترك أثر، سيما في ظل تطور الوسائل الإلكترونية الحديثة، المعززة بأنظمة متطورة يستغلونها الجناة الأذكى في ضرب حزام أمني على جرائمهم قبل إرتكابها، لكي لا يقعوا تحت طائلة العقاب، وفي هذا المجال حذرت المصالح الأمنية من إرتفاع الجرائم الإلكترونية في الجزائر، حيث إرتفعت من 153 جريمة إلكترونية سنة 2011م، إلى 175 جريمة سنة 2012م، أغلبها تتعلق بالمساس بالحياة الخاصة للأشخاص، على غرار التهديد والتشهير ونشر صور غير لائقة مخلة والنصب والإحتيال، فضلا عن إستغلال العديد من المواقع من طرف الجماعات الإرهابية. (حكيم غريب : المرجع السابق ، ص 79) .

خاتمة:

يتجلى لنا من خلال هذه الدراسة للجريمة الإلكترونية و التي لم يتفق فيها الفقه الجنائي على تسمية موحدة فأحيانا يطلق عليها تسمية: " الجريمة السيبرية" و " الجريمة المعلوماتية " و " الجريمة اساءة استخدام تكنولوجيايات الاعلام و الاتصال " و " جريمة الكمبيوتر و الانترنت "....، ولأنها من أعقد وأخطر الجرائم التي عرفها العالم المعاصر، وذلك لما تتصف به من تحديات وصعوبات في محاربتها ومحاصرتها، في ظل ثورة الإتصالات المتسارعة والتقدم المتواصل في تكنولوجيا الحاسوب الآلي، والإنترنت يفرض على الجهات المعنية أن تسير في خطوات متناسقة مع التطورات السريعة، التي تشهدها هذ التكنولوجيايات والإلمام بها، حتى يمكن التصدي لهذه الجرائم التي صاحبتهامومواجهتهام، هذا من ناحية، كما يستلزم إتخاذ إجراءات قد تتعدى المفاهيم والمبادئ الثابتة في القوانين الوطنية ومن ناحية ثانية لما تتصف به هذه الجرائم من عصرنة وتطور وتحول وسرعة فائقة في أساليبها.

إن غرس الثقافة الحاسوبية وسط المجتمع، وخاصة لدى رجال الأمن والقانون، يمكن أن يحقق للدولة النجاح في مواجهة الجرائم المعلوماتية، التي تبقى من أهم التحديات التي توجه كل الدول، دون إستثناء وفي هذا الصدد يمكن الإشارة إلى موقف الجزائر، المعبر عنه بمناسبة إفتتاح الدورة (32) المجلس وزراء الداخلية

العرب 2015 بالجزائر العاصمة: في كلمة مفادها: "وفي هذا المقام، أود أن أخص بالذكر الجريمة الإلكترونية نظرا لارتباطها بظاهرة الإرهاب، إستحداث الصيغ والأليات الضرورية لتفعيل الرقابة الإلكترونية برفع مستويات التعاون في هذا المجال لسد الثغرات التي قد تستغلها هذه الجماعات لضرب إستقرار دولنا ونشر الفكر المتطرف الدخيل وسط مجتمعاتنا وتجنيد الشباب في صفوفها". وعليه، فلا مفر من مواصلة السلطات المعنية في أنحاء العالم الإلتزام بتطوير القدرة على التعاون الدولي الفعال، في مجال مكافحة الجريمة الإلكترونية، من خلال إيجاد أرضية صلبة من التعاون والتفاهم من أجل عالم يسوده الأمن والاستقرار. لذا لا بد من تعديل القوانين الالكترونية خاصة تعديل القانون 15-04 بما يتماشى مع التطورات الالكترونية.

وكذا إيجاد وحدة البحث و التحري الالكتروني الموحدة دوليا.

دون ان ننسى ضرورة التفاعل الشرطي لكل الدول المنطوية تحت منظمة انتربول ، وذلك بتوحيد الجهود الوطنية مع جهود المنظمة الدولية وخلق جسر تعاون دائم. (حاجي نعيمة ،ص 73).

اهم المراجع المعتمدة :

- الامر 03-06 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات، الجريدة الرسمية الصادرة بتاريخ 23 جويلية 2003، العدد 44.
- القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 66-154 المتضمن قانون العقوبات.
- القانون 09-04 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال ومكافحتها، الجريدة الرسمية الصادرة بتاريخ 16 اوت 2009 ، العدد 47.
- الامر 21-11 المؤرخ في 25 اوت 2021، المتمم بالأمر 66-155 المؤرخ في 08 جويلية 1966 المتضمن قانون الاجراءات الجزائية.
- عبد الصبور عبد القوي: الجريمة الالكترونية، دار العلوم للنشر، طبعة 2007.
- محمد السيد سلطان : قضايا قانونية في امن المعلومات ، دار سر ناشري للنشر الالكتروني، سنة 2012.

- حاجي نعيمة : الجريمة السيبرية و الجهود الدولية لمكافحةها، مجلة النبراس للدراسات القانونية، المجلد 06، العدد 01.
- سبع زيان، المفتي سلمى : الجريمة المنظمة و الجهود الدولية لمكافحةها، مجلة البحوث ، المجلد 06، العدد 01.
- سعيداني نعيم. (2013). اليات بحث و التحري عن الجريمة المعلوماتية في القانون الجزائري. رسالة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة مولود معمري تيزي وزو.
- غريب حكيم: الجريمة الالكترونية و الجهود الدولية لمكافحةها، المجلة الالكترونية للدراسات القانونية، العدد 01 المجلد 02.

قائمة الهوامش:

- حكيم غريب: الجريمة الالكترونية و الجهود الدولية لمكافحةها، المجلة الجزائرية للدراسات السياسية، المجلد 02، العدد 01 الصفحة 73.
- حكيم غريب: المرجع السابق، ص 74.
- سبع زيان، المفتي سلمى : الجريمة المنظمة و الجهود الدولية لمكافحةها، مجلة البحوث ، المجلد 06، العدد 01، ص 759.
- القانون 04-09 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الاعلام و الاتصال و مكافحةها، الجريدة الرسمية الصادرة بتاريخ 16 اوت 2009 ، العدد 47.
- الامر 11-21 المؤرخ في 25 اوت 2021، المتمم بالأمر 66-155 المؤرخ في 08 جويلية 1966 المتضمن قانون الاجراءات الجزائية.
- حكيم غريب: المرجع السابق، ص 74.
- سعيداني نعيم. (2013). اليات بحث و التحري عن الجريمة المعلوماتية في القانون الجزائري. رسالة ماجستير في العلوم القانونية تخصص علوم جنائية، جامعة مولود معمري تيزي وزو.
- عبد الصبور عبد القوي: الجريمة الالكترونية، دار العلوم للنشر، طبعة 2007.
- محمد السيد سلطان : قضايا قانونية في امن المعلومات ، دار سر ناشري للنشر الالكتروني، سنة 2012.

- حكيم غريب: المرجع السابق، ص 78.
- الامر 06-03 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات، الجريدة الرسمية الصادرة بتاريخ 23 جويلية 2003، العدد 44.
- القانون 15-04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 154-66 المتضمن قانون العقوبات.
- حكيم غريب: المرجع السابق، ص 79.
- حاجي نعيمة : الجريمة السيبرية و الجهود الدولية لمكافحةها، مجلة النبراس للدراسات القانونية، المجلد 06، العدد 01.