

## الجريمة الإلكترونية والجهود الدولية لمكافحتها

د. حكيم غريب،

أستاذ محاضر - ب -

المدرسة الوطنية العليا للعلوم السياسية

### مقدمة:

عرفت الإنسانية عبر القرون الماضية ثورتين غيرت وجه التاريخ وطبيعة الحياة البشرية، وهما الثورة الزراعية والثورة الصناعية، وما هو مؤكد -اليوم- أن المجتمع الدولي أضحي يعيش الثورة الثالثة (أو بالأصح الموجة الثالثة)، وهي تعبير عن ثورة تكنولوجيا المعلومات، لأن هذه الموجة الجديدة أساسها جهاز الكمبيوتر والإنترنت والمعرفة، التي أصبحت ركيزة للمشاريع التنموية في عالم اليوم، ويعتبر هذا التقدم المعلوماتي الإلكتروني الهائل -الذي نشهده اليوم- نتيجة لثمرة المزوجة بين تقنيات الإعلام الآلي وتكنولوجيا الاتصالات، وهو ما أدى إلى ميلاد الثورة الإلكترونية، وأمام تسارع إيقاع التقدم التكنولوجي والتقني الهائل، وظهور الفضاء الإلكتروني ووسائل الاتصال الحديثة، كالفكس والإنترنت وسائر صور الإتصال الإلكتروني عبر الأقمار الصناعية قد أدى إلى إستغلاله من قبل مرتكبوا الجرائم الإلكترونية وتوظيفه في تنفيذ عملياتهم الإجرامية التي لم تعد تنحصر على مستوى الدولة الواحدة، بل تجاوزت حدود البلدان، وهي جرائم حديثة وجديدة تمثل ضرباً من الذكاء الخارق، وإستعماله لإلحاق الضرر بالآخرين.

وتعد ظاهرة الجرائم الإلكترونية، أو جرائم التكنولوجيا العالية، أو السيبركرايم Cyber Crime، أو جرائم أصحاب الباقات البيضاء White Collar، من الظواهر الإجرامية مستحدثة وهو ما دفع إلى تفرع أجراس الخطر لتنبيه المجتمع الدولي لحجم التهديدات الخطيرة الناجمة عنها، بإعتبارها تستهدف الإعتداء على الأنظمة الإلكترونية للمواقع الحساسة والإستراتيجية للدولة، فهي جرائم إلكترونية تنشأ في الخفاء يقتربها مجرمون أذكاء، يمتلكون تقنيات التكنولوجيا الحديثة، والتي يوجهونها إلى إختراق الحق في المعلومات، وتطال آثارها نظام المعلوماتية، وفي مقدمتها المواقع الرسمية للدولة. وتدفع هذه المعطيات للبحث بوساطة هذه الدراسة عن هذه الظاهرة المستحدثة، على صعيد المتابعة الجنائية، سواءاً في إطار القوانين الوطنية أو الدولية.

● **إشكالية الدراسة:** تعود إشكالية الدراسة إلى ما يتصل بها من مفردات ومفاهيم جديدة كالبيانات وشبكات الإتصال الإلكتروني، والشبكات العنكبوتية، وحول التساؤل عن الآليات والتدابير المناسبة لمكافحة الجريمة الإلكترونية وطنياً ودولياً؟

● ولهذا بات لا يكفي أن يكون الدارس متخصصاً في القانون وفي السياسة الجنائية، بل يجب عليه أن يكون ذو دراية كافية بتقنيات إستخدام الكمبيوتر والإنترنت، ليستطيع إيجاد الحلول المناسبة للرهانات والتحديات الأمنية والإقتصادية والإجتماعية، التي تنيرها هذه التكنولوجيا بكل أبعادها الإيجابية، وما أكثرها والسلبية وما أخطرها على الأفراد وتهدد الأمن الوطني والسيادة الوطنية، وفقدان الثقة في التقنيات التكنولوجية الحديثة، وعلى رأسها شبكة الإنترنت، لذا فإن معرفة ماهية الجريمة الإلكترونية، والطبيعة الموضوعية لهذه الجرائم، وإظهار تداعياتها ومخاطرها الإقتصادية والأمنية والإجتماعية والثقافية، ضرورة لتحقيق الأمن الشامل.

## • 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 إنتشار الجريمة بمختلف أشكالها، حتى أصبحت تسمى بعولمة الجريمة الإلكترونية.

وأمام تعدد الآراء بشأن مفهوم الجريمة الإلكترونية، تبني كل رأي مفهوماً مرتبطاً 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 إستناداً لمعايير أخرى حسب القائلين بها<sup>(1)</sup>. وهذا ما أعاق منظمة الأمم المتحدة إلى عدم التوصل لتعريف متفق عليه دولياً، 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 بـ: "نشاط جنائي يمثل إعتداء على برامج وبيانات الحاسب الإلكتروني"، وأيضاً بأنها: "كل إستخدام في صورة فعل أو إمتناع غير مشروع للتقنية المعلوماتية ويهدف إلى الإعتداء على أية مصلحة مشرعة، سواء أكانت مادية أو معنوية"<sup>(2)</sup>. 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 والانترنت) 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 وخطرها حالياً عن الحروب العسكرية، إلا أنها تتحقق عبر شبكات الإنترنت.

والظاهر أن كل الدراسات والنظريات الخاصة بالجريمة الإلكترونية تلتقي عند نقطة مركزية، تنحصر - عموماً - 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 إقتحام موقع البنتاغون الأمريكي، لتعود في صورة جديدة على شاكلة ما يعرف بالإرهاب الإلكتروني<sup>(3)</sup> الذي بات خطراً حقيقياً يهدد سلامة وأمن المجتمع الدولي، عن طريق التهديد بنسف المعلومات وتدمير إستراتيجية الدفاعات الإقتصادية والأمنية للبدان وعوائدها المالية، بإستعمال أنواع الفيروسات المدمرة والخطط التخريبية لتدمير العديد من البرامج المعلوماتية الحساسة للدول.

## • خصائص الجرائم الإلكترونية:

إن أهم ما تتصف به هذه الجرائم الإلكترونية سهولة ارتكابها بعيداً عن الرقابة الأمنية، وصعوبة التحكم في تحديد حجم الضرر الناتج عنها قياساً بالجرائم التقليدية، وأن مرتكبيها هم من بين فئات مختلفة تجعل من التنبؤ بالمشتبه بهم أمراً في غاية الصعوبة وتنطوي على سلوكيات غير مؤلفة عن الأفراد، وسهولة إنتلاف 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 Chachers 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 بوساطة إيجاد الوسيلة التي تمكنهم من تحطيمها، بل والتفوق عليها<sup>(4)</sup>.

ولقد تعددت الدراسات التي تتحدث عن سمات مرتكبي الجرائم الإلكترونية وشخصيتهم، ومدى جسامه 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 الشفرات، ويسبح في عالم الشبكات ليحصل على كل غالي وثمان 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<sup>(5)</sup>، 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 يمتلك 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 حالياً 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 أمنياً وقضائياً في العديد من البلدان والمدرجون على قوائم الإرهابيين من إدارة المواقع على شبكات الأنترنت.

ويعد الإرهاب الإلكتروني نمطاً جديداً 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، وإن الهدف الرئيسي للإرهابيين في السيطرة على القناة، يكمن في مقدرتهم على بث أفلام تنظيم "داعش" الدعائية.

#### • مظاهر تحديات الجريمة الإلكترونية:

ترتب على ظاهرة الجريمة الإلكترونية رهانات وتحديات عديدة، ومن أفدحها تنامي الأنشطة الإجرامية الإلكترونية، وتوصل مرتكبوها بتقنيات عالية التكنولوجيا غير مسبوقة، 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 شيئاً من الواقعية، أن معظم النصوص الموجودة تواجه بعض الأنشطة المجرمة التي ترتكب عن طريق الإنترنت، فإنه ينبغي ألا ننكر أن هناك نصوصاً قانونية لم تعد تتماشى مع تطور الجريمة الإلكترونية، وظهور الإرهاب الإلكتروني كمبدأ لشرعية الجرائم المستحدثة والعقوبات والتفسير الضيق والمحدود لأبعادها<sup>(6)</sup>.

#### • الجريمة الإلكترونية والإرهاب:

لقد استغلت العديد من التنظيمات الإرهابية الطبيعة الإتصالية لشبكة الإنترنت من أجل نشر أفكارها ومعتقداتها، بل تعداه الأمر إلى ممارسات تهدد أمن الدول الذي أخذ منحى خطيراً في استخدام الإنترنت في ارتكاب جرائم غاية في الفتك في حق المجتمعات، وبث ثقافة الإرهاب عبر الإنترنت عن طريق تصميم مواقع إفتراضية تمثل الجماعات الإرهابية، وهي مواقع آخذة في تنامي وإرتفاع مع زيادة عدد الجماعات الإرهابية، حيث تطلن عبر هذه المواقع تحملها مسؤولية إحدى العمليات الإرهابية التي تم إرتكابها بها، ويبقى خير مثال في استخدام الإنترنت بصورة مؤثرة وعالية الدقة في تصوير الجرائم المتوحشة والخطيرة، هو تنظيم داعش، فقد استطاع هذه التنظيم من خلال الإنترنت تجنيد المقاتلين الأجانب، وهم في أغليبيتهم 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، فدائماً ما تصف الأهداف التي تستهدف عملياتهم بالكافرة، وتقوم بدعوة الشباب إلى الجهاد وحثهم على الإستشهاد في سبيل الله، والفوز بالجنة<sup>(7)</sup>.

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 قيوداً على إفادة التنظيمات الإرهابية من نشر وسائل الإعلام عنها، بينما في المقابل تتيح المواقع الإلكترونية للتنظيمات الإرهابية قدراً كبيراً من التحكم في نظام المعلومات، ونشر رسائلها الإعلامية التي تود ترويجها، بل أيضاً تتيح لها المرونة في توجيه الرسائل لفئات مختلفة من الجمهور المستهدف، ورسم صورة ذهنية عن الجماعة وعن أعدائها أيضاً.

وتستعمل الجماعات الإرهابية -الإنترنت إلى جانب أغراض الدعاية والترويج- في نشر معلومات مضللة أو مغلوطة، ونشر تهديدات وصور ولقطات فيديو مرعبة<sup>(8)</sup>. 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 الإنحراف الفكري، من خلال

تعرض فئات الشباب –على الخصوص- إلى الكثير من المؤثرات الفكرية والإيديولوجية، وبالتالي تهدد الأمن بكل أبعاده ومستوياته<sup>(9)</sup>.

### • تنظيم داعش والجيل الجديد من الجهاديين الأجانب:

لقد بدأت علاقة تنظيم "داعش" بالإنترنت مبكراً، ووفق قاعدة أن "الحاجة هي أم الاختراع" خاصة من خلال مواقع التواصل الاجتماعي "فيسبوك"، بشكل خاص، وكذا موقع "خلافة بوك" الذي أعلن انتماءه التام والمطلق لما يسمى بالدولة الإسلامية، ويبقى الهدف من هذه الوسائط الإعلامية هو السماح للتنظيم وأنصاره بالتواصل في مواجهة الحظر، الذي يواجهونه من الشبكات الاجتماعية الأخرى.

وتشكل شبكة الإنترنت عاملاً مركزياً في عمل التنظيم ونشاطه وخطابه الإعلامي، ونشره عملياته المتوحشة، وقدرته على التجنيد خاصة الجيل الرابع من الجهاديين: "المقاتلون الأجانب" وقد تجاوز تنظيم داعش التنافس الإلكتروني والنجاح في خوض الحرب الإعلامية – النفسية مع أكثر الأجهزة الأمنية على الشبكة العنكبوتية، ومن أبرز أسرار نجاحه في التفوق والصمود والتواصل والتحايل على المعارك الكبرى التي يخوضها في بلاد الرافدين، وأصبح مفهوم "الجهاد الإلكتروني" راسخاً في أيديولوجيته القتالية، في ظل عمل التنظيم على عولمة حركته وفعاليته في سياق الاستجابة والرد على عولمة سياسة الحرب على الإرهاب، ولقد أظهر تنظيم داعش قدرة فائقة على التكيف والتجدد والتطور في عرض عملياته الوحشية ضد الأبرياء في العراق وسوريا وليبيا، عبر مواقعه في شبكات الإنترنت، وقد رسخت تلك العمليات المتداولة عبر شبكات التواصل الاجتماعي، ولادة أنموذج جديد غير تقليدي يرهق أقوى وأذكى الأجهزة الاستخباراتية الدولية، وقد نشرت في الآونة الأخيرة وكالة الأنباء الأمريكية "أسوشيتد برس" أن عشرين ألف مقاتل أجنبي جاؤوا من كل دول المعمورة، وانظموا إلى صفوف تنظيم الدولة الإسلامية الإرهابي، ويتفق عديد من الخبراء والمحللين الأمنيين على أن الاعتماد على شبكات التواصل الاجتماعي في تجنيد واستقطاب المقاتلين الأجانب من أسباب نجاح تنظيم داعش الإرهابي، لأنه بنى حاضنة مستمرة لاستقطاب مستمر ومتواصل في العديد من المواقع على شبكة الإنترنت، من أبرزها: موقع يوتيوب، موقع تويتر وشبكة فين (VINE) لمقاطع الفيديو.

ويعد المقاتلون الأجانب الأصلح لبعض المهمات الخاصة، كالعمليات الانتحارية المدمرة، ويرجع ذلك لكون التنظيم يجد سهولة أكبر في إقناع هذا الجيل الجديد من الجهاديين الأجانب، بالإقدام على مثل هذا النوع من العمليات النوعية، نظراً لشدة حماسهم القوي والمرتفع، وتشبعهم بمعتقدات الجهاد الإلكتروني من خلال شبكات التواصل الاجتماعي، والمدونات المُنَعْنَة بالانتصارات الزائفة التي تسهل عملية إقناعهم أكثر من المقاتلين العرب من تونس وليبيا والعراق ... إلخ، ومن جهة أخرى فإن نجاح هذا التنظيم في تنفيذ استراتيجيته يبرز في لفت انتباه الإعلام الأجنبي إلى الحد المبالغ فيه، ولعل أوضح مثال على ذلك هو التهويل الإعلامي الذي تقوده الوسائل الغربية كالترويج لهذه المجموعات المرتزقة، والتأطير لميلاد جيل جديد من المقاتلين الأجانب الذين سيكونون مستقبلاً عبئاً كبيراً وخطراً محدقاً في حالة عودتهم إلى ديارهم الأصلية، وفي هذا الصدد يبدو أن أبناء الجيل الجديد من هؤلاء المقاتلين الأجانب يشعرون بالوحدة والغربة في بلدانهم الأصلية، فوجدوا في الفضاء الإلكتروني الملاذ الآمن لتحقيق نزعتهم الانتقامية في (الحج) إلى تنظيم داعش.

### • موقف النظام القانوني العربي من حماية نظام المعلومات:

توصف قوانين العقوبات العربية بالمتعلقة بحماية نظام المعلومات بالعمومية (ما عدا تشريعات حماية المصنفات الرقمية في نطاق الملكية الفكرية فقط)، أما الجرائم الإلكترونية (بالمعنى والمستوى القانوني المقرر في التشريعات المقارنة) هناك فإن نصوصاً ضيقة قد وردت في تشريعات التجارة الإلكترونية التي تم إقرارها في كل من الأردن والإمارات المتحدة وتونس، بخصوص تجريم التلاعب برسائل البيانات، أو إرتكاب الجرائم عبر الوسائل الإلكترونية.

والملاحظ، أن مثل هذا المستوى من التدخل التشريعي لا يتوافق البتة مع الموضوع محل التنظيم، ولا مع الأحكام المتعين أن تتضمنها التدابير التشريعية في حقل جرائم الكمبيوتر، وعلى الرغم من هذا القصور التشريعي الذي أصبح واقعاً ملموساً، إلا أنه لا يحول دون الإجهاد في تفسير النصوص العقابية التقليدية التي تعاقب على صور الإعتداءات المختلفة على المال، بحيث يمكن تطبيقها على الجرائم المستحدثة التي فرضتها ثورة الاتصالات والمعلوماتية.

ولكن هناك محاولات قامت بها الدول العربية لمعالجة نقص التشريعات والأنظمة الخاصة بالجريمة الإلكترونية، وذلك بوضع أطر عامة حول ضوابط استخدام وأمن شبكة الإنترنت، عن طريق تحديد بعض النشاطات الإجرامية، التي يمكن أن توظف الشبكة والكمبيوتر عموماً فيها، كما تشمل هذه المحاولات على العديد من تعليمات أمن المنشآت الحاسوبية والأجهزة والبرامج، وبعض القواعد العامة المنظمة لإرتباط المنشآت الحكومية بالشبكة العالمية<sup>(10)</sup>.

للإشارة أن كل هذه الجهود لم تخرج في نصوصها عن مجال تعدد الجرائم المرتكبة عبر الإنترنت، مما يتطلب من الدول العربية المزيد من الجهود والتعاون من أجل مكافحة هذه الظاهرة الخطيرة.

#### • الجرائم الإلكترونية والمشرع الجزائري:

لقد عمل المشرع الجزائري على مواكبة مختلف التطورات التشريعية التي تم سنّها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الإلكترونية، بما فيها شبكة الإنترنت، تلك خاصة التي تسعى إلى الحد من الاستخدام غير المشروع لها، وذلك مراعاةً منه لما يشهده العالم من تطورات حديثة في مجال تكنولوجيا الاتصالات والمعلومات، وكذلك إيماناً 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 الاسم كعلامة تجارية للبرنامج، وذلك لما يتضمنه هذا النوع من أهمية في الحماية.

ولقد تدارك المشرع الجزائري خلال الأعوام الأخيرة، ولو نسبياً، الفراغ القانوني في مجال الإجرام الإلكتروني، خصوصاً بموجب (القانون 04-15) المتضمن تعديل 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، لأن المجرمين يسعون بشتى الوسائل لكي لا يتركوا ورائهم آثاراً تدل على إرتكابهم 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<sup>(11)</sup>.

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 الأذكياء 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، فضلاً عن إستغلال العديد من المواقع من طرف الجماعات الإرهابية<sup>(12)</sup>.

### • الجهود الدولية في مكافحة:

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 أنموذج موحد للنشاط الإجرامي، الأمر الذي يقتضي توحيد هذه النظم القانونية، وإستحالة 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 غالباً ما تشجع الأطراف فيها على السماح بإستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من الفوارق وأوجه الإختلاف بين الأنظمة القانونية والإجرائية، ويفتح المجال أمام تعاون دولي فعال، فمثلاً المادة (20) من إتفاقية 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، لإستخدامها 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 يومياً، طوال أيام الأسبوع، لكي تؤمن المساعدة المباشرة للتحقيقات 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 إستقطاب المتخصصين والكفاءات في المجال الإلكتروني والمعلوماتي وضمهم إلى مصالحهما.

## التعاون الأمني على المستوى الدولي:

تستدعي 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 بجهودها المنفردة القضاء على الجريمة بكل أشكالها، في ظل التطور المذهل في كافة مجالات الحياة، خاصة في ميدان الإتصالات وتكنولوجيا المعلومات وظهور الإنترنت، ولأن الإنتشار الكبير والسريع لها قد أدى إلى ظهور أشكال وصور جديدة من الجرائم الإلكترونية، التي أصبحت خطراً على سرية النظم الحاسوبية، بل تعدت إلى أمن البنى الأساسية والإستراتيجية للدول، نظراً 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 بإستخدام التقنيات، إلا أن لا تكفل لها أمناً فعالاً، ويتاح في ظلها التلاعب -عبر الحدود- بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أضراراً خطيرة، خاصة في ظل عدم وجود نموذج موحد للنشاط الإجرامي.

### الخاتمة:

يتجلى لنا من خلال هذه الدراسة للجريمة الإلكترونية، أنها 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 هذه التكنولوجيات والإلمام بها، حتى يمكن التصدي لهذه الجرائم التي صاحبتهام ومواجهتهام، 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) لمجلس وزراء الداخلية العرب 2015 بالجزائر العاصمة: في كلمة مفادها: "وفي هذا المقام، أود أن أخص بالذكر الجريمة الإلكترونية نظراً لإرتباطها بظاهرة الإرهاب، إستحداث الصيغ والآليات 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 وتجنيب 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 والإستقرار.

## الهوامش:

1. تعريف خبراء منظمة التعاون الإقتصادي والتنمية وتم مناقشة هذا التعريف في إجتماع المنظمة بباريس سنة 1990.
  2. CHERNAOUTI HELI SLANGE, "Comment lutter contre la cybercriminalité?" reveille Science, N°=391, Mai 2010.
  3. عبد الصبور عبد القوي، الجريمة الإلكترونية، الطبعة الأولى، دار العلوم للطباعة والنشر، القاهرة 2007.
  4. محمود أحمد عابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، 2005.
  5. MASCALA CORINE, criminalité et contrat électronique, IN, le contrat électronique, travaux de l'association CAPITANT HENRI, journées national; Paris, 2000.
  6. محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الحديثة للنشر، الإسكندرية، 2001.
  7. محمد السيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار سر ناشري للنشر الإلكتروني، 2012.
  8. مها عبد الكجيد صلاح، إستراتيجيات الإتصال في مواقع الجماعات المتطرفة على شبكة الإنترنت دراسة تحليلية، الندوة العلمية "إستعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين"، قسم الندوات واللقاءات العلمية، الرياض، 2010.
  9. ناصر بن محمد اليقي، أثر التحول إلى مجتمع معلوماتي على الأمن الفكري، المؤتمر الوطني الأول للأمن الفكري المفاهيم والتحديات، جامعة الملك سعود، المملكة السعودية.
  10. فايز بن عبد الله الشهري، التحديات الأمنية المصاحبة لوسائل الإتصال الجديدة، مقال متوفر على الموقع التالي: <http://www.Osamabahar.com>.
  11. غازي عبد الرحمن هيان الرشيد، الحماية القانونية من جرائم المعلوماتية، أطروحة دكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.
- <<http://Forum.Edudz.com>> الجريمة الإلكترونية جريمة العصر، للمزيد أنظر الموقع الإلكتروني: