

الجريمة الإلكترونية والأمن الوطني

أ. خديري عفاف

كلية الحقوق والعلوم السياسية

جامعة عنابة

ملخص:

تميز القرن العشرين باختراعات مذهلة كان أهمها ظهور الحاسب الآلي وتطور شبكات وأنظمة المعلومات حتى أصبحت هذه الأمور من مستلزمات الحياة، وفي ضوء التطور هذا ظهرت مشكلة تتمثل في جرائم الانترنت، هذه الأخيرة تعتبر نوعا شائعا من الجرائم إذ أنها تتمتع بالكثير من المميزات تخص المجرمين تدفعهم إلى ارتكابها، فهي لا تعرف الحدود الجغرافية لأنه يتم ارتكابها بأداة هي الحاسب الآلي وعن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة بهما، كما أن لهذه الجرائم خصائص تنفرد بها، لذا نرى اليوم عدت تشريعات تسعى إلى سن أكبر قدر ممكن من القوانين للقضاء على هذه الظاهرة الإجرامية التي باتت تشكل خطرا كبيرا على الحياة الخاصة للفرد من جهة وعلى أمن الدولة من جهة أخرى.

الكلمات المفتاحية: شبكة الانترنت، الظاهرة الإجرامية، جرائم الهاكرز، غسيل الأموال، الجرائم الأخلاقية...

Abstract:

The twentieth century is characterized by amazing inventions, the most important was the computer emergence and development of networks and information systems so that these things have become necessities of life, and in the light of the evolution, a problem has emerged consisting in online crimes, the latter are considered somewhat common crimes, as they have a lot of specific features to the criminals who are motivated to commit them; they do not know geographic boundaries because they are committed through the computer tool and through the Internet and by someone ultra familiar to them, and that these crimes have unique characteristics, so we see today enumerated legislation seeks to issue as much as possible of laws to eliminate this criminal phenomenon, which has become a major threat to private life of the individual on one hand and to state security on the other one.

Key words: Internet, criminal phenomenon, hacker's crimes, money laundering, moral crimes...

مقدمة

معطيات الكمبيوتر المخزنة والمنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الأنترنت، هذه المعطيات هي مؤشرات هذه الجريمة وما تستهدفه إعتداءات الجناة، وهو ما يظهر مدى خطورة هذا النوع من الجرائم فهي تمس الحياة الخاصة للأفراد، وتهدد الأمن الوطني والقومي والسيادة الوطنية، وتشيع فقدان الثقة بالتقنية، وتهدد إبداع العقل البشري، لذا فإن إدراك ماهية جرائم الانترنت والكمبيوتر والطبيعة الموضوعية لها وإستظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها، وسمات مرتكبها

تعتبر ظاهرة جرائم الانترنت - أو ما يطلق عليه: جرائم التقنية العالية أو جرائم أصحاب الياقات البيضاء - ظاهرة إجرامية مستجدة نسبيا، تفرع على جانبها أجراس الخطر لتنبيه مجتمعات العصر الراهن لحجم المخاطر وفداحة الخسائر الناجمة عنها، باعتبارها تستهدف الإعتداء على المعطيات بدلالاتها التقنية الواسعة، فهي جريمة تنشأ في الخفاء، يقتربها مجرمون أذكى، يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال

جرائم الأنترنت أو ما حمل بعدها من أوصاف كجرائم الهاكرز أو الإختراقات، وآخر السيبركرايم، وجرائم العلم الإفتراضي، بالإضافة لمصطلحات أخرى تبعد قليلا عن التقنية، مثل جرائم الياقات البيضاء⁽¹⁾.

عليه، يمكن تعريف الأنترنت: (Internet) هو اختصار لكلمتين انجليزيتين الأولى هي (international) والثانية (network) وبالتالي هي كلمة مركبة سميت بها شبكة عنكبوتية تتكون من الملايين من قنوات المعلوماتية المتصلة ببعضها البعض، فيصعب إذا تحديد حجمها وكثافتها، والتي تستعمل الحواسيب لإقتناء أغراض المتعاملين وتصرفاتهم القانونية⁽²⁾، أما الجريمة الإلكترونية فقد عرفت بصفة عامة على أنها كل فعل غير مشروع صادر عن إرادة آثمة، يقرر له القانون عقوبة أو تدييرا إحترازيا⁽³⁾.

تعتمد الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت على المعلومة بشكل رئيسي، وهذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم، وقد عرف الفقه⁽⁴⁾ جريمة الأنترنت بأنها: هي نشاط إجرامي تستخدم فيه التقنية الإلكترونية الحاسب الآلي الرقمي وشبكة الأنترنت - بطريقة مباشرة أو غير مباشرة - كوسيلة لتنفيذ الفعل الجرمي المستهدف⁽⁵⁾، ويعرفها البعض الآخر على أنها جرائم تعني الشبكة العالمية التي يستخدم الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة، مثل استخدامه في النصب والاحتيال وغسيل الأموال، وتشويه السمعة والسب...⁽⁶⁾.

يمكن، مما سبق، تعريف جرائم الأنترنت بأنها كل الجرائم التي ترتكب باستخدام شبكة الأنترنت وعلى الرغم من أنها كثيرة ومتنوعة ولا يمكن حصرها، لكنها بصفة عامة هي الجرائم التي تقع على الأموال أو على الأشخاص، أو على الممتلكات الفكرية والعلمية، وقد تصل إلى المساس بأمن الدولة الداخلي والخارجي، وصولا إلى الجرائم ذات البعد الدولي كالجرائم الإرهابية والجرائم الأخلاقية، بالإضافة إلى سرقة المعلومات واختراق المواقع الخاصة وتشويه سمعة أصحابها.

ومن ضمن التعابير التي أطلقت على ظاهرة جريمة الأنترنت، تلك الواردة من قبل خبراء المنظمة الأوروبية

ودوافعهم، يمثل أهمية استثنائية لسلامة التعامل مع هذه الظاهرة، ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية.

وإذا كانت مجتمعاتنا العربية لم تتأثر، بعد، بشكل ملموس بمخاطر هذا النمط المستجد من الجرائم، فإن خطر جرائم الأنترنت والكمبيوتر المحتملة، في البيئة العربية، يمكن أن يكون كبيرا، باعتبار أن الجاهزية التقنية لمواجهتها ليست بالمستوى المطلوب، إن لم تكن غائبة تماما، وبالمقابل فقد أسست جرائم الأنترنت من أخطر الجرائم التي تقتدر في الدول المتقدمة، ومن هنا يطرح الإشكال الآتي: إلى أي مدى يمكن اعتبار جرائم الأنترنت خطرا على الأفراد وعن الأمن الوطني؟

تستدعي الإجابة على هذه الإشكالية التطرق إلى معالجة المحاور التالية:

- 1- المحور الأول : ماهية جرائم الأنترنت.
- 2- المحور الثاني : صور جرائم الأنترنت.
- 3- المحور الثالث : جرائم الأنترنت والأمن الوطني.

المحور الأول: ماهية جرائم الأنترنت

أحدث التطور الحاصل في تكنولوجيا الإعلام والإتصال وظهور الشبكة العالمية للأنترنت بكل ما حملته من تقدم وخدمات، أثارا إيجابية وغير نمط حياة المجتمعات، وساهم في التطور والرقى إلا إنه حمل - في الوقت نفسه - أثار سلبية على حياة الناس ومصالح الدول بأسرها، كل هذا تجلى في تطويع الأنترنت والوسائل الإلكترونية لتكون عالما من عوالم الجريمة، وهي الظاهرة التي طفت على السطح وحملت في عالم اليوم تسمية : جرائم الأنترنت أو الجرائم الإلكترونية.

1- مفهوم جرائم الأنترنت

أطلق على ظاهرة الجرائم المتعلقة بالكمبيوتر والأنترنت عدة مصطلحات دون أن يتم الاتفاق على مصطلح واحد للدلالة على هذا النوع من الجرائم الحديثة، وقد سائر هذا التباين التطور التقني، ونمو الظاهرة الجرمية بالموازاة، فبدأ بمصطلح جرائم الكمبيوتر، ثم جرائم التقنية العالية، إلى

دول مختلفة قد تتأثر بالجريمة الإلكترونية الواحدة في آن واحد، لأن السهولة في حركة المعلومات عبر أنظمة التقنية الحديثة قد جعل بالإمكان ارتكابها عن طريق حاسوب موجود في دولة معينة، بينما يتحقق الفعل الإجرامي في دولة أخرى، وذلك راجع إلى أن مجتمع المعلومات لا يعترف بالحدودية الجغرافية، فهو مجتمع متعدد عبر شبكات تخترق الزمان والمكان دون أن يخضع لحرس الحدود⁽⁹⁾، فقد يكون الجاني في بلد والمجني عليه في عدة دول، كالجرائم التي تمس الدين والأخلاق والأمن... الخ. وهنا نكون بصدد مشكلة الاختصاص القضائي والإجراءات القضائية⁽¹⁰⁾.

ج- جرائم صعبة الاكتشاف والإثبات:

مسألة الاكتشاف: تتميز جريمة الإنترنت بصعوبة اكتشافها، وإذا ما إكتشفت فإن ذلك يكون بمحض الصدفة، لأنها تعتبر من الجرائم المعلوماتية التي لا تحتاج إلى عنف...، وإنها عبارة عن أرقام وبيانات تتغير أو تمحى تماماً من السجلات المخزنة في ذاكرة الحسابات الآلية، فهذه الجرائم لا تترك أي أثر خارجي بصورة مرئية⁽¹¹⁾، هذا من جهة، وأن الجاني يمكنه ارتكاب هذه الجريمة من دول أخرى بإضافة إلى قدرته على دليل الإدانة في أقل من ثانية من أخرى وهذا يشكل عاملاً إضافياً في صعوبة إكتشاف هذا النوع من الجرائم.

مسألة الإثبات: إن اكتشاف جريمة الإنترنت كما سبق الإشارة إليه ليس بالسهل، وحتى في مجال اكتشاف وقوع هذه الجريمة والإبلاغ عنها، فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب وترجع صعوبة هذا إثبات إلى عدة أمور منها:

التطور في ارتكابها وسرعة إخفاءها: تتسم جرائم الإنترنت بأنها خفية ومستمرة في أغلبها، لأن الضحية لا يلاحظها، رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من جرمته بدقة، على سبيل المثال عند إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة وإتلافها والتجسس وسرقة المكالمات وغيرها من الجرائم⁽¹²⁾.

سرعة محو الأدلة المادية: لا تترك هذه الجرائم أثراً لها بعد ارتكابها علاوة على صعوبة الاحتفاظ الفني بأثارها إن

للتعاون الإقتصادي بأنها كل سلوك غير مشروع أو منافي للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات⁽⁷⁾، كما تتميز الإنترنت بخصوصية إمكانية وجودها في عدة أماكن في نفس الوقت، فتتعدى المجال أو المفهوم الإقليمي والجنسية إلى المساس بكافة أنحاء العلم، التي يمكن ربطها، لذلك تسمى بالشبكة الأم.

2- خصائص جرائم الانترنت

تعتبر الجرائم التي ترتكب من خلال شبكة الانترنت، جرائم ذات خصائص منفردة، لا تتوافر في الجرائم التقليدية سواء من حيث أسلوب وطرق ارتكابها أو الأشخاص للذين ارتكبوها، وتعدد الخصائص والمميزات، ومنها:

أ- الحاسب الآلي هو أداة ارتكاب الجريمة وعلى شبكة الانترنت:

- الحاسب الآلي هو أداة ارتكاب جرائم الانترنت: إن الحاسب الآلي هو دائماً أداة الجريمة في الجرائم التي تقع على شبكة الانترنت، وهي خاصية منفردة عن أي جريمة أخرى، لأن الحاسب الآلي هو الأداة الوحيدة التي تمكن الشخص من الدخول على شبكة الانترنت، وقيامه بتنفيذ جرمته أياً كان نوعها، وعليه فالحاسب الآلي هو الأداة الوحيدة لارتكاب أي جريمة على شبكة الانترنت.

- جرائم ترتكب عبر شبكة الانترنت: تعد شبكة الانترنت هي حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات الصناعية، وغيرها من الأهداف التي ما تكون غالباً الضحية لتلك الجرائم، وهو ما دعا معظم تلك الأهداف إلى اللجوء أي نظم الأمن الإلكترونية في محاولة منها لتحمي نفسها من تلك الجرائم أو على الأقل لتحد من خسائرها عند وقوعها ضحية لتلك الجرائم⁽⁸⁾.

ب- عالمية الجريمة (الجريمة العابرة للحدود):

لم يعد هناك، بعد ظهور شبكات المعلومات حدود مرئية أو ملموسة تقف أمام المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحواسيب وشبكتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أنه في أماكن متعددة وفي

بالأفراد تعتبر من المقومات الشخصية، لذلك تسعى جل التشريعات إلى حماية سلامة الأفراد من مختلف الانتهاكات التي قد يتعرضون لها، وخاصة إذا تعلق الأمر بالسمعة والشرف، ومن بين هذه الاعتداءات التي تقع على الأفراد:

أ- جريمة الالتقاط غير المشروع للبيانات: هي عبارة عن دخول غير مشروع إلى نظام معلوماتي معين، كالنظام الخاص بالبنوك، وتمكين المجرم من التقاط البيانات الشخصية للمتعاملين عبر قنوات الاتصال⁽¹⁵⁾، إما عن طريق التجسس، ويتمثل هذا الأسلوب في قيام قراصنة الانترنت باستخدام البرامج التي تتيح لهم الاطلاع على البيانات والمعلومات الخاصة بالمتعاملين على شبكة الأنترنت، كالمؤسسات والشركات التجارية، ومن ثمة استخدام هذه البيانات والمعلومات في ممارسة الأنشطة غير المشروعة.

يمكن للجبان، أيضاً، استخدام برمجيات تمكنه من التقاط كلمة السر، من خلال تجواله في جزء من شبكة الانترنت، أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة، وفي كل اتصال بالشبكة تجرى مراقبة وتتبع حركات الإتصال، حتى يطبع المستخدم كلمة السر أو أسمه⁽¹⁶⁾، فإن البرنامج (الشماس) يجمع هذه المعلومات وينسبها، إضافة إلى أن أنواع هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها معها، كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها.

ب- جرائم القذف والسب وتشويه سمعة الأشخاص: تعتبر جريمة السب والقذف والتعرض للحياة الشخصية للأفراد بغرض التشهير والخوض في أغراضهم من أكبر الجرائم التي تجرمها كافة القوانين، وفي جميع دول العالم، أي كانت الطريقة أو الوسيلة التي تتم بها الجريمة، من قذف وسب وتشهير بعبارات بذيئة تمس وتخدش شرف المجني عليه، سواء كانت الاتصال المباشر أو يكون مكتوباً، وذلك عبر المبادلات الإلكترونية⁽¹⁷⁾.

تعتبر شبكة الانترنت مسرحاً غير محدود فهي تتلقى كل ما يدرج عليها دون قيد أو رقابة، لذلك تشكل بعض حالات سوء إستخدامها الأبعاد التواصلية سلبية شاذة تؤدي البعض خاصة إذا تم التشهير بهم عبر إيراد المعلومات مغلوطة⁽¹⁸⁾، وعليه فإن جريمة القذف والسب والتشهير التي

وجدت، فليست هناك أموالاً أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظمها تم اكتشافها بالمصادفة، وبعد وقت طويل من ارتكابها، لأنها تعد من الجرائم المستحدثة التي لا تترك شهوداً يمكن إستجوابهم، ولا أدلة مادية يمكن حصرها، ومن هنا تتأتى صعوبة الكشف عن هذه الجريمة⁽¹³⁾.

نقص الخبرة لدى الأجهزة الأمنية والقضائية:

تحتاج جرائم الانترنت والجرائم الالكترونية إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها، حيث يتطلب تحقّقاً خاصاً بالكمبيوتر ونظم المعلومات، سواء لارتكابها أو التحقق فيها أو للاحقة المجرمين قضائياً، لذلك يجد مأموري الضبط القضائي أنفسهم غير قادرين على التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم، فضلاً عن صعوبة إجراء التحريات السرية، وتتبع مسار العمليات الالكترونية العابرة للحدود⁽¹⁴⁾، كما أن رجال الشرطة ومأموري الضبط القضائي قد لا يتعاملون بمهارة واحترافية مع الدليل الإلكتروني المستمد من جريمة الأنترنت، ولذلك وجب عقد دورات تدريبية مشتركة بين رجال القضاء والنيابة العامة ورجال الشرطة والخبراء الفنيين مجتمعين معاً، وذلك بغرض معرفة كل جهة بطبيعة عمل الجهة الأخرى، مما يحقق التعاون بين هذه الجهات، وصولاً إلى أنسب الطرق القانونية لمكافحة جرائم الانترنت والجرائم الالكترونية.

المحور الثاني: صور جرائم الأنترنت

عرفت جل الدول تطوراً في مجال تكنولوجيات الإتصالات مما أدى إلى تطوير مجالات الإتصال، حتى إنها أصبحت من أهم الوسائل التي قد يعتمد عليها الكثير من الأفراد في معاملاتهم، رغم ذلك فقد استغلها البعض واستعملها لارتكاب بعض الجرائم التي تمس الحياة الخاصة للأفراد، وهناك جرائم تقع في حق الأموال.

1- الجرائم الواقعة على الأفراد

أدى التطور الذي شهدته التكنولوجيا إلى ظهور شبكة الانترنت، والتي قد ساهمت بدورها في تطوير الحياة الخاصة من جهة، والمجتمع من جهة ثانية، إلا أنها أصبحت سلاحاً فتاكاً في يد المجرمين، بالإضافة إلى أن هذه المعلومات المتعلقة

الشبكة، وتشمل الملاحقة رسائل تخويف ومضايقة، وتتفق مع مثلها خارج الشبكة في الأهداف المجسدة في رغبة التحكم في الضحية، وتتميز عنها بسهولة إمكانية إخفاء هوية المجرم، علاوة على تعدد وسهولة وسائل الاتصال عبر شبكة الأنترنت، وهو الأمر الذي ساعد في تفشي هذه الجريمة⁽²⁵⁾.

2- الجرائم الواقعة على الأموال

تغير نمط الحياة، في عصر الازدهار الإلكتروني وتغيرت معه مظاهر الأشياء وأنماطها، والتي من بينها أنماط الجريمة والتي يحتفظ بعضها بإسماها التقليدي، مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة تلك الواقعة منها على الأموال، والتي أخذت أشكالاً حديثة تتماشى مع التطور التقني عبر تغيير تطوير الأساليب التي يحاول المجرمون بوساطتها الوصول إلى أهدافهم، التي من بينها :

أ- جرائم السطو على أرقام البطاقات الائتمانية : منذ أن بدأ استخدام البطاقات الائتمانية عبر شبكة الأنترنت حتى عمد اللصوص للتسلل إليها، فالبطاقات الائتمانية تعد نقودا إلكترونية⁽²⁶⁾ والاستيلاء عليها يعد استيلاء على مال الغير، حيث تتم عملية التحويل الإلكتروني غير المشروع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه، مما يسمح للجاني بالتوغل في النظام المعلومات وعادة ما يكون هؤلاء من العاملين على إدخال البيانات في دائرة الجهاز، أو من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات⁽²⁷⁾.

ب - الجرائم المنظمة: يطلق إصطلاح الجريمة المنظمة على الظاهرة الإجرامية التي تهدف إلى تحقيق الربح وأمام انتشارها وتشعب نشاطاتها لم تتوصل معظم التشريعات إلى تحديد تعريف لها إلا أن شبكة الأنترنت تعتبر الآن من أهم الوسائل التي ساعدت كثيرا أعضاء عصابات (المافيا) على تطوير وتحسين عملياتهم على مستوى العالم إذ أنها عملت على إلغاء حاجز الزمان والمكان من أمامهم، فأصبحت عملياتهم أكثر تطورا وأعظم تأثيرا على مستوى العالم، حتى أنها قد أقامت لها مواقع على شبكة الأنترنت خاصة بها لتفادي القوانين، كما أن القدرات والفرص التي تؤمنها شبكة

تتم باستخدام شبكة الأنترنت بواسطة مواقع يكون هدفها الإساءة والتشهير سواء لشخص معين، أو بدولة من الدول، أو بدين من الأديان، تقع تحت طائلة نفس النصوص القانونية التي تجرم تلك الأفعال متى تمت بالطرق التقليدية⁽¹⁹⁾.

ج- جريمة انتحال شخصية المتعامل الشرعي بالبيانات :

يعتبر هذا النوع من الجرائم الأكثر حداثة وذلك نظرا لسرعة انتشارها خاصة في الأوساط التجارية، التي يتم فيها استخدام هوية شخصية أخرى بطريقة غير شرعية، وهدف الجاني إما لاستفادته من مكانة تلك الهوية أي هوية الضحية، أو لإخفاء هوية شخصية المجرم لتسهيل ارتكاب جرائم أخرى، وبالرجوع إلى قانون العقوبات الجزائري في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات نصت "على أنه تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة... بيانات المحرر الإلكتروني الأصلي"⁽²⁰⁾.

وعليه تعبر هذه الجريمة عن قيام شخص باستخدام شخصية شخص آخر للإستفادة من سمعته مثلا أو ماله أو صلاحياته، هذا الانتقال يمكنه من القيام بذلك عن طريق المعلومات التي تتعلق بتلك الشخصية، كالاسم والعنوان ورقم الهوية مثلا، والتي يحصل عليها من الأنترنت، ويمكن إن تؤدي هذه الجريمة إلى استنزاف رصيد الضحية في البنك أو السحب من البطاقات الائتمانية ...، وكثيرا ما يقوم المجرم بتغيير العنوان البريدي للضحية إلى عنوانه كي يستقبل بنفسه الفواتير والمطالبات⁽²¹⁾، ويقع التزوير بهذه الطريقة بإدخال التوقيع أو الإمضاء أو البصمة بطريقة الماسح الضوئي على مستند معالج أو محفوظ داخل الحاسب الآلي⁽²²⁾ وتصبح الوثيقة وكأنها موقعة وممضاة من قبل صاحب التوقيع أو الإمضاء أو البصمة، ويكون الحصول عليهما عن طريق الغش على صاحبهما، ودون رضا هذا الأخير⁽²³⁾.

د- جريمة التهديد والملاحقة: يعتبر التهديد شكلا من أشكال زرع الخوف في النفس، وهنا يكون تهديد الغير من خلال البريد الإلكتروني واحد من أهم الاستخدامات غير المشروعة للأنترنت، حيث يقوم الفاعل بإرسال رسالة إلكترونية للمجني عليه تنطوي على عبارات تسبب خوفا أو ترويعا لمتلقيها⁽²⁴⁾، والتي تتم عبر شبكة الأنترنت باستخدام البريد الإلكتروني، أو وسائل الحوارات الآتية المختلفة على

المقومات والركائز الجوهرية الحساسة التي تعتمد عليها الدول في تأمين أمنها، والتي أصبحت عرضة للعديد من التحديات التي تفرضها عليها الجرائم الإلكترونية في عالم اليوم، وعلى الرغم من إختلاف ترتيبها لدى البعض، فإن من أهمها:

1- المتغير السياسي:

قد تلجأ بعض الأطراف السياسية سواء داخل الدولة أم خارجها بالتأثير على النشاط السياسي لنظام الدولة، وذلك بهدف إحداث اضطرابات سياسية واجتماعية، وتغييرات داخل المجتمع.

يجدر الإشارة هنا، أن الجمعية العامة للأمم المتحدة أدانت أعمال الإرهاب التي تقوم بها الأنظمة (الدول) في إنكار حق الشعوب في تقرير مصيرها، وبالتالي فإن العمل الإرهابي يمكن أن تقوم به الدول أيضا مثال على ذلك الدول الإستعمارية أو الأنظمة عنصرية أو الدكتاتورية، إلا أن الواقع يظهر أن الجريمة الفردية التي تحمل بطبيعتها أهدافا سياسية أو إيديولوجية، بعكس العمل الإرهابي الذي يعمل على إشاعة الرعب بين مجموعة كبرى بين الناس، أكثر تأثيراً على إستقرار الأمن الوطني والدولي، وهو ما جعل الأنترنت باعتبارها لا تعرف حدوداً جغرافية تحمل عبر ممارساتها تحديات متجددة بإستمرار لسياسات الدول، سواء بالنسبة لتشويه سمعة ممثلها، أو بإستخدام الأساليب المسمية في التعامل معها، بهدف السيطرة عليها.

2 - المتغير الإقتصادي:

تعد الجريمة الإلكترونية، التي قد يلجأ إليها الأفراد من أجل المساس بدولة معينة، من بين أهم الجوانب التي تعتمد إلى مساسها هو الجاني الإقتصادي، وذلك عبر إشاعة بنشر عدم الإستقرار بالنسبة للأوضاع الأمنية المتعلقة بالنشاطات الإقتصادية، وعدم المقدرة على الإصلاح والتنمية والتصدي لمظاهر الفساد وتكون بصورة مبالغ فيها وقد يكون بإقتحام مواقع الخاصة بالشركات الإستثمارية الأجنبية، وبالتالي يعطل العلاقات الإقتصادية مع الدول الأخرى.... وحتى بين القطاعات العامة والخاصة على المستوى الداخلي، ومن ثم التأثير على ثقة المجتمع

الانترنت طورت العديد من النشاطات التجارية المشروعة وغير المشروعة، من خلال زيادة سرعة وسهولة إجراء المعاملات، بل يظهر جانب مظلم من الانترنت لا يشمل فقط على الاحتيال والسرقة ونشر المواقع الإباحية وشبكات المنحرفين جنسيا ممن يستهدفون الأحداث، بل أيضا منظمات المتاجرة بالمخدرات والمنظمات الإجرامية التي تركز على إستغلال ما توفره الشبكات الالكترونية من تسهيلات وفرص، مما جعلها تركز على تعطيل الشبكات كما يفعل الآخرون⁽²⁸⁾.

3- جريمة غسيل الأموال: أعطت شبكة الانترنت عدة مميزات لمن يقومون بعمليات غسيل الأموال، منها السرعة الكبيرة وتخطي الحواجز الحدودية بين الدول، وتفادي القوانين التي قد تضعها البعض منها لإعاقة نشاطهم، وكذلك تشفير عملياتهم مما يعطيها قدراً أكبر من السرية⁽²⁹⁾، وأيضا كان إنتشار التجارة عبر شبكة الانترنت خير المعين لهؤلاء القائمين على عمليات غسيل الأموال والتجارة الالكترونية وانتشارها عبر أنحاء العالم أجمع مما ساعد كثيراً في عمليات غسيل الأموال نظرا لسهولة الاتفاق على الصفقات وإتمامها من خلاله، دون أن تكون في معظم الأحيان تحت رقابة قانونية صارمة، بل أنه في حالة وجود تلك الصفقات عبر الأنترنت وبطريقة تشفير معقدة لا يمكن حلها، وبالتالي لا يمكن من خلالها معرفة كيفية إتمام تلك الصفقات⁽³⁰⁾.

المحور الثالث: تأثير جرائم الانترنت على الأمن الوطني

مع تطور مفهوم الأمن الوطني، الذي يعني، في مفهومه العام، مقدرة الدولة على حماية مقومات وجودها عبر التصدي لأية تدخل أجنبي يؤثر على مسار تطورها، بالإضافة إلى مقدرتها على التمكن من إدارة متغيرات سياستها على المستوى الداخلي للمحافظة على التوازن الإجتماعي، وتماسك الوحدة الوطنية، وإرتباطه بالأمن الدولي فإن مسألة جرائم الانترنت التي تعدو ظاهرة متعددة للحدود أصبحت في الوقت الحاضر من أفضع التحديات التي تمس بالأمن الوطني للدول لاسيما فيما يتعلق بالجانب السياسي والإقتصادي والإجتماعي، والعسكري، بإعتبارها من

ومع التقدم التقني وتطور وسائل الإتصال الذي نعيشه نكاد نلمسه فقد تغيرت وتطورت تلك الأساليب التي يحاول الإرهابيون بها الوصول إلى أهدافهم مما جعل الإرهاب الإلكتروني هو السائد حاليا وأصبح إقتحام المواقع الخاصة بالدول والتأثير على أمنها عبر الدخول على الشبكات والعبث بمحتوياتها وتغييرها أو بإزالتها أو الإستيلاء عليها أو الدخول على شبكات الطاقة أو شبكات الإتصالات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائيا وهي الظاهرة التي تمارسها ليست فقط الجماعات أو الأفراد، وإنما حتى الدول^(*).

يحاول الفلسطينيون في المقابل معالجة تلك الآثار وتصحيح وإزالة العبث الواقع على موقعهم وأيضا يحاولون اقتحام بعض المواقع الصهيونية ووضع العلم الفلسطيني على الصفحة الرئيسة الخاصة بالاحتلال الصهيوني⁽³⁴⁾.

يعتبر التقارب بين عولة الشبكات الحاسوبية والقلق من أن الشبكات الإلكترونية والتي قد تستخدم لإرتكاب الجرام التي قد تمس بالدول والأفراد حيث تقوم بتخزين الأدلة وإتلافها عبر هذه الشبكات، وهو ما يظهره الواقع الحياتي للمجتمع الدولي - عموما - والذي يعاني من وجود فجوة عميقة بين هذا التطور الإلكتروني بما يعنيه من علم القيادة والتحكم في الأحياء والآلات، ودراسة آليات التواصل في كل منهما وهو ما يسعى بعلم السبرانية والعلاقة بينهما، ومجموعة التشريعات الوطنية والدولية، ذات العلاقة بموضوع مكافحة الجريمة المنظمة عموما، والجريمة الإلكترونية على وجه الخصوص، وهو ما أعطى فرصة لممارسة هذا النوع من الجرائم التي وظفت هذه الثقافة (السبرانية) ليس خدمة لتقدم البشرية، وإنما لإلحاق الأضرار البالغة بمقومات الدول والمساس بأمنها سواء أكانت متقدمة أم نامية، ومن ثم إحداث عدم التوازن بين أفراد المجتمع لصالح مجموعة معينة منه، وهو ما يعد من أفدح المظاهر التي تمس بحقوق الإنسان والحق الإنساني التي تعتبر المؤثر الرئيس لمفهوم الأمن الوطني ومكانته في الدول، لذلك نجد اتفاقية بودابست الصادرة في 2001 عن المجلس الأوروبي الذي اعتبرها كقانون عام لمكافحة جريمة الانترنت ضننا من المجلس أن هذه الاتفاقية ستوفر ما يلتزم لردع أي

بمؤسساته الاقتصادية، وإرهابه عبر تخويله من عدم كفاءتها في تلبية إحتياجاته الضرورة.

3- المتغير الاجتماعي (الثقافي) :

تعد ظاهرة الإرهاب من اخطر الظواهر التي تؤثر سلبا في البنية الاجتماعية للدول وقد تفاقمت خطورة هذه الظاهرة في عالمنا المعاصر خاصة بظهور شبكة الانترنت وتحول ظاهرة الإرهاب من ظاهرة عنف إلى ظاهرة تمس الجانب الثقافي للدول⁽³¹⁾، وهو ما جعل بعض الأفراد يلجؤون إلى طمس حقائق تاريخية أو نشر ما يسوء إلى الدين وثقافة تلك الدولة، بهدف زعزعة الإستقرار الاجتماعي فيها، أو زرع ثغرات ثقافة ما على حساب الآخر في المجمع الواحد، و بدوره يؤدي هذا الإخلال بالهيكل الاجتماعي وتكوينه لأنه يشيع جوا من التوتر والإضطراب بين المواطنين وفقدان الثقة فيما بينهم⁽³²⁾، وهو ما يؤدي ببعض هؤلاء الأفراد إلى القيام بأعمال إرهابية مضادة والهدف منها زعزعة أمن وإستقرار تلك الدولة وذلك عن طريق تحالف الفئات المهمشة معهم لتحقيق مآربهم، وعلى الرغم من اختلاف مصالحيهم وأهدافهم، إلا أن الغاية التي يسعيان لتحقيقها تظل واحدة⁽³³⁾.

وبما أن هذه المتغيرات لها أبعاد وإرتباطات بالأمن الوطني للدول فإن التصدي لها لا يمكن ان يتم بواسطة دولة منفردة، بل يتطلب تضافر الجهود الدولية لمحاربة هذه الظاهرة.

من أبرز المظاهر المستجدة التي تهدد الأمن الوطني عبر جرائم الانترنت ذلك التوظيف السليبي الذي تقوم به الجماعات الإرهابية على إختلاق توجهاتها وتصورتها، وهنا يمكن الحديث عن جرائم الإرهاب الإلكتروني الذي يبرز فيه إلى حيز الوجود الدور الذي يمكن أن يلعبه الإعلام الرسمي وغير الرسمي في مواجهة المواقع التي تروج للفكر المتطرف على شبكة الانترنت. من أجل إلحاق الأذى بالأمن الوطني عامة وبالسيادة الوطنية والأفراد خاصة ولتفعيل مبادئ الدفاع عن الأمن الوطني فإن الوضع الحالي يستدعي إعادة القراءة المستمرة لتأثيراتها السياسية وكيفية توظيفها من قبل الأفراد والمجتمع للدفاع عن المصلحة العامة.

الحاسب الآلي، كغسيل الأموال والاتجار بالسلاح وتمويل الجماعات الإرهابية والعنف.

- وضع نصوص دولية موحدة تكفل الحماية الجنائية للمعلومات على شبكة الانترنت.
- معالجة القصور في القوانين الوطنية والدولية في مجال جرائم الانترنت، إذ أنه ما تزال الكثير منها تخضع للنصوص التقليدية، وهو الشيء الذي يعد مساسا مباشرا بمبدأ الشرعية، الذي ينعكس سلبا في مجال المتابعة إذ أنه يؤدي إلى إفلات الكثير من الجناة من العقاب.

يتطلب تفعيل هذه الإقتراحات :

- ضرورة تكوين القضاة في مجال الجرائم المعلوماتية خاصة وأن القاضي الجزائي وفي غياب النصوص التجريبية ونظرا لمستلزمات مبدأ شرعية الجرائم والعقوبات وحظر القياس في المجال الجنائي يجد نفسه مقيدا تجاه هذا الشكل المستحدث من الإجرام.
- استحداث نصوص خاصة بالاعتداء على سير نظام المعالجة الآلية للمعطيات.
- ضرورة التعاون الدولي لمواجهة صور السلوك المنحرف في البيئة المعلوماتية وهذا ما أوجت به الاتفاقية الدولية للإجرام المعلوماتي المبرمة سنة 2001 وذلك بتشجيع الدول على إدراج الجرائم المعلوماتية في قوانينها العقابية.

بالمحصلة، فإن الوضع الدولي ما زال يتسم بوجود فجوة متفاقمة بين التطور الإلكتروني، وعملية توظيفه في عالم الجريمة الإلكترونية المنظمة وهو ما يدل على أن مواجهتها ستكون طويلة، وستتطلب مزيدا من التنسيق والعمل الميداني للحد من آثارها السلبية على أمن الأفراد والجماعات والدول، وهي تطلعات بقدر ما تتسم بالواقعية بقدر ما يعترض تطبيقها ضبابية القوانين، وتدني مستوى سياسات عدم الثقة المتفشى بين المؤسسات والدول في التعامل مع هذه الظاهرة.

الهوامش:

(1) مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دراسة مقارنة، الطبعة 1، دار النهضة العربية، 2001، ص 20.

عمل إرهابي ضد السرية وتوفير نظم الحاسوب و الشبكات والبيانات واتخاذ ما يكفي من الإجراءات و الصلاحيات لمكافحة هذه الجرائم⁽³⁵⁾.

تدفع الضرورة لحماية الأمن الوطني والحيلولة دون تعرضه لمظاهر الجريمة الإلكترونية، لتجسيد جديد لمفهوم الأمن الوطني، وإعادة ترتيب أولوياته باستمرار، بهدف ترسيخ مقوماته وتجديد مكوناتها، وصيانة، ورسم أبعاده، وتحديد آليات تنفيذه، وذلك في كنف خلق إمكانات وإعداد مهارات كفؤة وفعالة للتعامل مع هذا الوضع الذي يتسم بالسرعة الفائقة والإنتشار غير المحدود عبر قيام النظام برسم سياسات ووضع إستراتيجيات أمنية لتحقيق الجاهزية العالية لقوة الدولة للتعامل مع هذه الظاهرة للحد من توظيفها من قبل بعض السلطات والناقدین في التحكم في عملية التعبير، وفي وضع قيود أمام الحريات العامة، لا سيما وأن القوانين الحالية التي تسير هذه الظاهرة الإجرامية المتخطية للحدود ما تزال تتسم بالعمومية، وتفتقر إلى الآليات والوسائل القابلة للتطبيق من أجل وضع حد لتأثيرها على المصالح الوطنية للدول.

خاتمة:

شهد العالم تطورا تكنولوجيا في مجال الحاسبات الآلية وشبكات الانترنت أفرز نوعا جديدا من السلوك الإجرامي، والمتمثل في تلك الجرائم التي ترتكب عبر الانترنت، والتي يمكن أن نطلق عليها عدم مقدرة الإنسان في التحكم في العلم السبراني وهي ذات أبعاد مختلفة عن تلك الجرائم التقليدية، كما أن لها خصائص يمكن القول بأنها إنفردت بإرتكابها عبر الانترنت، وما ميزها بالخصوصية عن الجرائم الأخرى، وكان لها الدور الأكبر في إبراز هذا النشاط كظاهرة إجرامية مستحدثة.

في ظل خصوصية هذه الجرائم فإنه يصعب تحديد سلوك مرتكبها خاصة في ظل الطابع العالمي للجريمة المرتكبة عبر الانترنت مما يؤدي إلى إفلات الجناة من العقاب، ومن هنا يمكن إقتراح ما يلي :

- ضرورة تجريم الوقائع الإجرامية ذات الصبغة الدولية أو الوطنية كهريب متحصلات جرائم المخدرات باستعمال

الطبعة 1، دار السراطين للنشر والتوزيع، بيروت، 2004، ص312.

(18) سامي علي حامد عباد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي الإسكندرية، 2007، ص77.

(19) منير محمد الجنيبي وممدوح محمد الجنيبي، المرجع السابق، ص38.

(20) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، 2007، ص44.

(21) المادة 394 مكرر من قانون العقوبات الجزائري لسنة 2008 المعدل والمتمم.

(22) محمد خليفة، المرجع السابق، ص47.

(23) عبد الفتاح بيومي حجازي، الجريمة في عصر العولمة، الطبعة 1، دار الفكر الجامعي، 2007، ص126.

(24) خالد بن معيض العبيدي، الحماية الجنائية للتعاملات الالكترونية، 2009، ص52.

(25) إلياس سمير الهاجري، جرائم الانترنت، المملكة المغربية، 2006، ص58.

(26) هشام مفيد محمود، الآثار السلبية الناجمة عن تزوير البطاقات الائتمانية، الطبعة 1 أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2002، ص107.

(27) خالد ممدوح إبراهيم امن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2010، ص76.

(28) أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة 2، دار الفكر الجامعي، 2006، ص29.

(29) خالد ممدوح إبراهيم، المرجع السابق، ص130.

(30) منير محمد الجنيبي، المرجع السابق، ص100.

(31) رنا مولد سبع، ماهية الإرهاب وتأثيره على واقع حقوق الإنسان، دراسات دولية العدد 49 ص167.

(32) هبة الله خميس، الإرهاب الدولي، منشورات جامعة الإسكندرية، ط1، 2010، ص26.

(33) رنا مولود سبع، ماهية الإرهاب وتأثيره على واقع حقوق الإنسان، المرجع السابق، ص168.

(2) عبد الرحمن عبد اله السند، الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي شبكة المعلومات الانترنت، دار السراطين للنشر والتوزيع، الرياض، 2004، ص20.

(3) محمود نجيب حسني، شرح قانون العقوبات القسم العام، الطبعة 6، دار النهضة العربية القاهرة، 1989، ص40.

(4) محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، ص32.

(5) مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية، دار الكتب القانونية، مصر، 2005، ص56.

(6) مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة 1، مطابع الشرطة، القاهرة، 2009، ص112.

(7) عبد الله بد الكريم عد الله، جرائم المعلوماتية والانترنت، الطبعة 1، منشورات الحلبي الحقوقية، بيروت، 2007، ص15.

(8) منير محمد الجنيبي وممدوح محمد الجنيبي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، 2006، ص13.

(9) نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 1، دار الثقافة للنشر والتوزيع عمان، 2008، ص51 و50.

(10) RQVE-RQULIN Laurent, régales de conflits de juridictions et règles des conflits de lois appliquées aux cybers délit, mémoire de master 2 professionnel en droit de l'internet publique, université paris panthéon, Sorbonne, 2008, p.06.

(11) خالد ممدوح إبراهيم، امن لجريمة الالكترونية، الدار الجامعية، 2008، ص45.

(12) محمد عبيد الكعبي، المرجع السابق، ص32.

(13) خالد ممدوح إبراهيم، المرجع السابق، ص46، ص45.

(14) خالد ممدوح إبراهيم، المرجع نفسه، ص80، ص81.

(15) محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الطبعة 1، دار الثقافة للنشر والتوزيع الأردن، 2004، ص167، ص166.

(16) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دون طبعة، الدار الجامعة الجديدة، 2007، ص44.

(17) عبد الرحمن بن عبد الله السند، الأحكام الفقهية للتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات،

^(٤) مثال ذلك ما يمارسه الكيان الصهيوني لتشمل الإرهاب الإلكتروني على المواقع الفلسطينية على شبكة الانترنت تتعرض وبصفة مستمرة من الصهيوينيين إلى إقحام والعبث بمحتوياتها وإزالة ما عليها من معلومات وعرض صورة العلم الصهيوني على الصفحة الرئيسية بالموقع المفتوحة

⁽³⁴⁾ منير محمد الجنيهي، ممدوح محمد الجنيهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص111

⁽³⁵⁾ قانون إساءة الكمبيوتر البريطاني في 19 يوليو 1990 على الموقع

www.tootshamy.com