

الجريمة الإلكترونية : النقطة " المظلمة " بالنسبة للتكنولوجيا المعلوماتية

د. " رابحي أحسن "

أستاذ القانون العام بكلية الحقوق

— جامعة محمد بوفرة — بومرداس

المقدمة :

مذو وجود الإنسان على مهد الوجود وهو يواجه معضلات وتحديات كبيرة جدا، الأمر الذي جعل حياته أكثر مرونة وأكبر حركية، ومرد ذلك العقل البشري الذي نعتبره مرجع أي تحول وأي تغيير وأي تطور، حيث كان سببا أزليا في اكتشاف الظروف والوسائل والآليات التي من شأنها أن تجعل العنصر البشري أكثر إدراكا لخبايا النسيج الكوني وأسراره والعلاقات المتفاعلة داخله إلى درجة الاحتراف.

وقد استطاع أن يهيئ له حياة أكثر يسرا وازدهارا ورفاهية بين أحضان طبيعة جوفاء مهيئة بالتعقيدات والتحديات، وهذا الصراع الأبدي بين العقل البشري والطبيعة هو الذي نطلق عليه اليوم اصطلاح " الثورة المعرفية ".

ولعل من أبرز ما " أنجبت " هذه النهضة العلمية في منتصف القرن العشرين نذكر " الكمبيوتر "، هذا الجهاز — وبالرغم من صغر حجمه — قد تمكن من تهديم كل الحواجز والحدود المكانية والزمنية بين كل أجزاء العالم، لقد أحدث تغييرات عميقة و" صامتة " في كل المفاهيم التقليدية المرتبطة بمادة الاتصال، وهكذا أصبح لكل الشركات والمؤسسات والمرافق المختلفة وحتى الأفراد موقع معين في جوف هذا الجهاز الغريب، من خلال

شبكة تمتد إلى ما لا نهاية، توصف بالشبكة العنكبوتية، هذه الخيوط الممتدة يطلق عليها اسم شبكة الإنترنت.

هذه الثورة الصناعية وضعت العالم على عتبة جديدة، وعلى الخصوص في مجال العلوم والمعارف والمعلومات، حيث شكلت في السابق مشكلة كبيرة من حيث جمعها وحفظها وتصنيفها واسترجاعها، لكن اليوم -وبفضل هذا الجهاز- أصبحت هذه المعلومات في متناول اليد، حيث يمكن الحصول عليها في أي وقت، بأقل مجهود وبسرعة فائقة.

وحتى لا نفرط في تعداد فضائل هذه التكنولوجيا المتطورة إلى حد أعمى، فإنها قد نشأت -فعلا- كوسيلة فنية متميزة في مجال الاتصال وتبادل المعلومات، لكن هذه النعمة سرعان ما تحولت إلى "نقمة" حقيقية بدخولها عالم الإجرام، وذلك عندما "تسربت" لها بعض النوايا السيئة، لاستغلالها لتحقيق أغراض غير مشروعة بما يضر الآخرين، ولعل نمو وتطور وانتعاش وانتشار هذا السلوك "المتطفل"، هو الذي أدى في الأخير إلى انحصار هذه الثورة المعرفية تحت وطأة الجريمة الإلكترونية في مجال متعدد الأشكال. إن الخطر الذي يمكن أن تفرزه التكنولوجيا المعلوماتية قد يفوق كل تصور، ولعل تعدد مظاهر الإساءة في استعمال هذه التقنية، لدليل على انسياقها وتشعبها بشكل يصعب السيطرة عليه، وهذا يدل على أنه لا توجد أي نقطة تنتهي فيها الجريمة الإلكترونية، ومن ثم فإن المعلومات -كل المعلومات- التي يحتويها الحاسوب لا يمكنها -في النهاية- أن "تفلت من بصمة هذه الجريمة".

فقد يتم من خلال شبكة الإنترنت سرقة المستندات وتزويرها وتدمير مواقع المعلومات ونشر الإشاعات وتشويه سمعة الدول والأشخاص والشركات والمؤسسات، والاستيلاء على الإنتاج الفكري والعلمي للآخرين، بل ونشر الفتن والفسوق والفجور وغيرها من الجرائم الدنيئة.

ورغم كل هذه التجاوزات الخطيرة، إلا أن مرتكبيها ما زالوا -حتى اليوم- يتمتعون بقسط كبير من الأمان بعيدا عن تطبيق القانون، ومرجع ذلك أن التكنولوجيا المعلوماتية

قد ساهمت في تطور حياة البشر من الوجه الآخر، وهو الوجه الذي يهدم التطور ذاته، وذلك لأنها وضعت في متناول الجناة الدقة التي تنقصهم في ارتكاب الجرائم والتسلل من العقاب.

كل هذه المعطيات كونت في أذهاننا نقطة استفهام كبيرة مفادها: إذا كان ابتكار وتحديث التكنولوجيا المعلوماتية بالشكل الذي نعرفه اليوم، يستدعي "الإيمان" بقدرة الذاكرة الإلكترونية على تجاوز معضلة الاتصال وتبادل المعلومات، فهل أن الاستغلال السيئ لهذه التقنية من شأنه "تحسين" الجرائم التقليدية من العقاب بارتكابها عبر الإنترنت؟

هذا ما سوف نحاول الإحاطة به من خلال هذه الدراسة المتواضعة التي أعطيناها العنوان التالي:

"الجريمة الإلكترونية: النقطة المظلمة" بالنسبة للتكنولوجيا المعلوماتية".
ولدراسة هذا الموضوع، فقد اتبعنا الخطوات التالية، حيث تم تقسيم الفكرة الأساسية إلى مبحثين رئيسيين:

—تضمن المبحث الأول منها— "الكسوف" الطويل لظاهرة الجريمة الإلكترونية: من خلاله حاولنا توضيح الأبعاد التقنية والموضوعية للإنترنت، ابتداء من إبراز معالمه وكذا المفاهيم المرتبطة به ومراحل انتشاره وتطوره من جهة، علاوة على تحديد محاسنه ومزاياه التي سرعان ما تحولت إلى فضاء "فتي" لارتكاب صنف مستحدث من الجرائم يطلق عليها الجريمة الإلكترونية من جهة أخرى.

—أما المبحث الثاني منها— فقد تضمن "النضج البطيء" للجريمة الإلكترونية في اللغة القانونية:

من خلاله حاولنا توضيح الجهود الدولية الموجهة لمكافحة وقمع الجريمة الإلكترونية، قبل التعرّيج عن الأسباب التي حالت دون القضاء أو السيطرة على "تسرب" هذا الداء، لا سيما من خلال امتداد مساحات ارتكاب هذه الجريمة، وكذا صعوبة الكشف أو ضبط الجناة، وأخيرا معضلة التنازع المعيارى أو بالأحرى أزمة القانون الواجب التطبيق.

هذا ما حاولنا التوصل إليه في خاتمة هذه الدراسة، لتكون بمثابة حصيلة وثمره المبحثين المذكورين آنفاً.

المبحث الأول - "الكسوف الطويل" لظاهرة الجريمة الإلكترونية
حتى تكون دراستنا أكثر قوة وأكثر دقة وأكثر فاعلية في هذا المجال، نعتقد بضرورة بحث مدلول الإنترنت وطرق استعماله ومراحل تطوره وانتشاره من جهة، وكذا تحديد الأسباب والظروف التي من شأنها أن تجعل منه فضاء لارتكاب الجرائم.

المطلب الأول - تحديد الأبعاد التقنية والموضوعية للإنترنت
إن اصطلاح الإنترنت هو اختصار لكلمتين إنجليزيتين هما: الأولى International والثانية Network ويقصد به شبكة اتصالات دولية.

ولعل من أهم التعريفات التي قيلت في شأن الإنترنت ما يلي:
• أنها شبكة هائلة من أجهزة الكمبيوتر المتصلة فيما بينها بواسطة خطوط الاتصال العالمية، فهي تمثل شبكة الشبكات حيث تتكون من عدد كبير من شبكات الطلب المتزايدة في أنحاء كثيرة من العالم، فالإنترنت إذن هو مجموعة شبكات وأجهزة للحاسب الإلكتروني التي توجد في مختلف دول العالم، والتي تتصل ببعضها البعض، حيث تجمع بينها أنظمة الاتصالات الإلكترونية التي تستخدم لنقل البيانات، ويمكن لأي شخص لديه جهاز كمبيوتر، ولديه اشتراك لدى أحد مقدمي خدمة الإنترنت، وخط تليفوني، الدخول إلى شبكة الإنترنت.¹

• وقيل، الإنترنت عبارة عن استغلال متقدم للحاسب الآلي، مرتبط من خلال الاتصالات الدولية مع وجوب توافر تقنية خاصة، وهو يمثل شبكة ضخمة تتكون من عدد كبير من شبكات الحاسب الآلي المنتشرة عبر أنحاء العالم، والمرتبطة ببعضها البعض بواسطة خطوط الهاتف أو عن طريق الأقمار الصناعية، بحيث يمكن تبادل المعلومات بين المستخدمين عن طريق بروتوكول موحد يسمى "بروتوكول ترانسل الإنترنت".²

وفي هذا المجال نذكر بأن للإنترنت استخدامات عديدة أهمها:

1. البريد الإلكتروني، من خلاله تستطيع إرسال واستقبال الرسائل بسرعة مذهلة تقدر بالثواني.
 2. المحادثات الشخصية، يمكن من خلاله التحدث إلى طرف آخر أو أكثر، صوتاً وصورة وكتابة.
 3. خدمة نقل الملفات، تستطيع بواسطته نقل البيانات والمعلومات مهما كان حجمها.
 4. خدمة الأرشفة الإلكترونية، حيث تستطيع إنشاء وتثبيت ما تحتاجه من معلومات، والرجوع إليها في أي وقت بسرعة مذهلة.
 5. خدمة البحث في أي شيء تحتاجه من خلال شبكة الإنترنت العالمية، فبواسطتها يمكنك استخراج المعلومات والبرامج والمواقع والسلع ومواقع الترفيه، والإعلانات عن الوظائف وغيرها، وكل ما يحتاج إليه الإنسان.
 6. خدمة التسوق، فبواسطة شبكة الإنترنت تستطيع أن تنتقل من خلال قارات العالم لتستعرض المنتجات والسلع، وتتعرف على أوصافها وأثمانها وطرق نقلها ودفع ثمنها وغير ذلك.
 7. التحويل المالي الإلكتروني بين البنوك والشركات والمقاصة المالية بين البنوك، تماماً مثل استعمال البطاقات البنكية.³
- ومن الملاحظ أن الإنترنت قد نشأ في بادئ الأمر في الولايات المتحدة الأمريكية، إبان الحرب الباردة بينها وبين الاتحاد السوفيتي سابقاً، حيث عمدت وزارة الدفاع الأمريكية إلى إنشاء جهاز كمبيوتر عملاق يربط بين عدة أجهزة كمبيوتر لتسهيل عمليات تبادل الأبحاث والمعلومات، وأطلق على هذه الشبكة اسم "آربانت ARPANET"، وكان الدافع هو الخوف من أن الاعتماد على شبكة تدار مركزياً سيكون هدفاً سهلاً لهجوم مباغت قد يقضي عليها، لكن باستحداث شبكة آربانت أصبح بالإمكان إرسال تعليمات التصويب من خلال مركز التحكم إلى قواعد الصواريخ، ولو بعد تدمير جزء من الشبكات الدفاعية، وهذا ما جعلهم يطلقون عليه اسم "مشروع شبكة العمود الفقري".⁴

ثم تطور المشروع بعد ذلك إلى الاستعمال السلمي بجانب الاستعمال العسكري الذي بدأ العمل به بتاريخ 1969/1/2 بشبكة مركزية ربطت معظم الجامعات المركزية بشبكة آربانت، وأصبح يضم شبكة اتصالات بين أربعين جهاز كمبيوتر عملاق في هذه الجامعات. وفي عام 1983 انقسم المشروع إلى شبكتين، احتفظت الشبكة الأولى باسمها الأساسي آربانت وبالغرض العسكري الذي أنشأت من أجله، وهو خدمة المخابرات المركزية الأمريكية، أما الشبكة الثانية وهي شبكة الاستخدامات المدنية فقد سمح لمختلف الأفراد باستخدامها، ويعتبر عام 1983 التاريخ الحقيقي لميلاد شبكة الإنترنت Enter Net.

وفي عام 1986 توسعت شبكة الإنترنت لتشمل المئات من الجامعات والمعاهد، قبل أن تنتقل إلى التطبيقات التجارية التي كان عددها محدودا في مطلع عام 1993، لكنها سرعان ما اذتشرت بوتيرة سريعة جدا خلال العشرية اللاحقة.⁵

المطلب الثاني - الجريمة الإلكترونية: " الوجه المستتر " للإنترنت

الجريمة لغة مشتقة من فعل جرم على وزن ضرب، والتي تعني الذنب واكتساب الإثم،⁶ أما اصطلاحا فنقصد بها إتيان فعل محرم نهى عنه الشارع أو ترك فعل مأمور به، ولا يعدّ الفعل أو الترك جريمة إلا إذا تقرر عليه عقوبة محددة.⁷

وما يعنينا في هذا البحث هو مفهوم الجريمة الخاصة بشبكة الإنترنت العالمية، حيث يتم استخدامها في ارتكاب ما يعرف بجريمة الإنترنت أو الجريمة المعلوماتية أو الجريمة الإلكترونية أو جريمة الحاسب الآلي.

وفي هذا الشأن يمكننا أن نستعين بعدة تعريفات لتحديد أبعاد هذه الظاهرة، ولعل أهمها:

- كل أشكال السلوك غير المشروع أو الضار بالمجتمع، والذي يرتكب باستخدام الحاسوب، ومن ثم فإنه يمثل كل فعل إجرامي متعمد أيّا كانت صلته بشبكة المعلومات، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل.⁸

• هو سلوك احتيالي أو خداعي أو تخريبي أو تحريضي مرتبط باستخدام الكمبيوتر المتصل بشبكة الإنترنت، يهدف مرتكبه إلى تحقيق فائدة أو مصلحة مالية أو أي فعل ضار غير مشروع.⁹

• أما بالنسبة لخبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية فإن المقصود بالجريمة المعلوماتية كل سلوك غير مشروع أو منافع للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها أو تحويلها.¹⁰

وهكذا يجمع الفقهاء على أن الغش المعلوماتي يمكنه أن يشمل العديد من الأفعال غير المشروعة لاستغلال ما ينتجه الحاسب الآلي من معلومات بغرض ارتكاب الجريمة، سواء عن طريق إدخال بيانات أو ملفات مزورة، أو تدمير بيانات وبرامج مثبتة، أو سرقة الخدمات والأموال وسائر المنافع الأخرى من الحاسب الآلي، أو بث الإشاعات بحق الأفراد والمؤسسات والدول، أو التحريض على الفسق والفجور، وبث كل ما من شأنه الإخلال بالآداب العامة.

إن النمو المتزايد والانتشار المتسارع للجرائم الإلكترونية التي ترتكب من خلال شبكة الإنترنت هو الذي قاد رغبة الخبراء والمختصين إلى تحديد تصنيفاتها الداخلية على النحو التالي:

1. جرائم التحريف والتزوير :

وملخص هذه الجرائم الإعتداء على المعلومات المخزنة في ذاكرة الحاسب الآلي بسرقتها أو تحريفها أو التلاعب بها، وكذلك اعتراض المعلومات المرسلّة من خلال شبكة الإنترنت، ومن وسائل التخريب أيضا إرسال برامج تقوم بتدمير أنظمة المعلومات وتمتلك القدرة أحيانا على تعديل البرامج الأخرى، وهو ما يعرف اليوم بعمليات " القرصنة المعلوماتية".¹¹

2. جرائم الاختلاس والسرقة :

وصورة هذه الجرائم أن يستخدم الشخص الحاسب الآلي للدخول إلى شبكة الإنترنت والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية، وتحويل الأموال من

تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى، وذلك بإدخال بيانات غير حقيقية أو تعديل أو مسح البيانات الموجودة بقصد اختلاس الأموال أو نقلها أو إتلافها.¹²

3. الجرائم الجنسية والممارسات الإباحية:

يعيش العالم اليوم ثورة جنسية طاغية تجاوزت كل الحدود والتصورات، وهو أمر جعل هذه القضية تطرح على أنها من أشد الجرائم أثرا وخطرا على الكيان البشري برمته، وقد ذكر المفكر " جيمس رستون " في مجلة نيويورك تايمز بأن " خطر الطاقة الجنسية قد يكون في نهاية الأمر أكبر من خطر الطاقة الذرية " ¹³.

وهذا يدل على مدى خطورة المواقع والمحطات المتعلقة بممارسة الجنس على النظام الاجتماعي العالمي وأثره على ازدياد الإنحلال الخلقي لدى الشباب، وارتفاع معدل الجرائم المتعلقة بالجنس بشكل عام، وما يزيد من خطورة الوضع أن نعلم أن عدد الصفحات الإباحية في شبكة الإنترنت يقدر بنحو 3,2% من الحجم الكلي في الشبكة.¹⁴ ومن صور هذه الجرائم نذكر إنشاء مواقع الجنس على شبكة الإنترنت يكون الدخول إليها مجانا أو مقابل دفع مبلغ من المال، ويكفي أن نعلم أن بعض الصفحات الإباحية يزورها نحو 280 ألف زائر يوميا، وأن 20% من سكان الولايات المتحدة الأمريكية يزورون بصفة متكررة هذه المحطات، وقد بلغت مجموع مشتريات المواد المتعلقة بالجنس المعروضة في الإنترنت عام 1999 ما قيمته 18 مليار دولار أمريكي.¹⁵

إلى جانب المواقع الجنسية يتم توزيع الصور الفاضحة من خلال البريد الإلكتروني، علاوة على المواقع التي تشجع على الفسق والفجور والسياحة الجنسية وغيرها، وهنا نذكر بأن هذه الممارسات لا تتحقق معها جريمة الزنا، ولكن الذي يقع هو نشر الفساد وتحريف الشباب.

4. جرائم القذف والتشهير:

وصور هذه الجرائم هو اتخاذ شبكة الإنترنت للتشهير بالناس، وإفشاء أخبارهم والتعرض لحياتهم الخاصة بالدعاية الكاذبة، بل ويمكن أن يصل الأمر إلى التلصص على

مواقع بعض الأشخاص المهمين على شبكة الإنترنت والتسلل إليها، وأخذ ما فيها من صور خاصة وأخبار، والعمل على نشر كل هذه العناصر بشكل يسيء لأصحابها.¹⁶ ولم يقف الأمر عند هذا الحد، بل تعدى إلى الدول والشركات والمؤسسات ونشر البيانات والمعلومات التي تسيء لسمعتها، من خلال إبراز سلبياتها وأسرارها، أو نشر المعلومات الخاصة بتنظيمها الداخلي دون موافقتها، وقد يصل ذلك إلى حد الإبتزاز والقتل بشكل متهور وغير مسؤول.

المبحث الثاني - " النضج البطيء " للجريمة الإلكترونية في اللغة القانونية
لطالما جذبت الجريمة الإلكترونية محل اهتمام رجال القانون والمختصين من أجل إيجاد الحلول المناسبة لقمعها ومكافحتها، بيد أن خصوصياتها التي تنطوي على صور وظروف ارتكابها قد شكلت عائقا كبيرا أمام تقدم البحث، وذلك بدوره قد أثر سلبا على مردود ونجاعة الحلول المعتمدة لمواجهة هذه الظاهرة.

المطلب الأول - التكييف القانوني للجريمة الإلكترونية
في الواقع يوجد شبه فراغ قانوني بخصوص جريمة الإنترنت، وذلك راجع إلى حداثة هذه الآفة من جهة، وكذا تأخر المشرع في وضع القواعد والنظم الضرورية لتأطير استعمال التكنولوجيا المعلوماتية من جهة أخرى، ولعل الجهود الفقهاء
~ المتناثرة ~ قد لعبت دورا بارزا في إخراج النسيج ~ الإلكتروني إلى النور، وتحديد طرق التعامل معه مستقبلا.

مبدئيا فقد ثار التساؤل حول مسألتين رئيسيتين:

المسألة الأولى - تتعلق بتصنيف الجرائم الإلكترونية انطلاقا من تحديد طبيعة الأفعال المجرمة المنشأة لها :

في هذا الشأن ظهر بأن جزء كبيرا من الجرائم الإلكترونية مشابه تماما للجرائم التقليدية المنظمة بواسطة قانون العقوبات، مما يدعو إلى تمديد نفس الأسس والخصائص والقواعد المحيطة بالجرائم العادية على نظيرتها الإلكترونية.

• فبالنسبة لجريمة التحريف والتزوير على شبكة الإنترنت فإنه يتعين تنظيمها بذات الأسس التي تخضع لها في حال تحققها خارج النطاق المعلوماتي، ذلك أن البرامج والمعلومات المخزنة في جهاز الحاسوب تعتبر من الأموال، وهي قريبة إلى حد ما من بعض الحقوق التقليدية مثل حق الإبتكار أو الملكية الفكرية أو الإسم التجاري وغيرها. وهكذا فإن برامج الحاسب الآلي تعتبر من وسائل التعبير عن أفكار المؤلف، ومن ثم فإنها تندرج ضمن الأعمال الخاضعة لحماية قانون حقوق المؤلف، وهذا الاتجاه قد أضحى مستقرا في "ذهن" صنف راجح من الفقه.¹⁷

وكنتيجة لذلك، فإن من يدخل إلى شبكة الإنترنت ويعيث في البرامج المعروضة أو يحرفها أو ينسخها أو يدمرها، فإنه يكون قد اعتدى على مال غيره، ويقع تحت طائلة العقاب بوصفه معتديا على ملك غيره، مما يستوجب العقوبة التعزيرية والضمان على فعله.¹⁸

• أما بالنسبة لجريمة الإختلاس والسرقة على شبكة الإنترنت، فإنها تخضع لنفس قواعد وأحكام السرقة المنظمة بواسطة قانون العقوبات، لا سيما من حيث شروط وأركان تحققها، ولعل العنصر الجوهري في هذه الجريمة يتعلق بإخراج المال المسروق من حيازة صاحبه وإدخاله في حيازة الجاني، وهذا الوصف ينطبق على ذات الجريمة عند حدوثها داخل شبكة الإنترنت، حيث يقوم الجاني ببرمجة نظام الحاسب الآلي وأمره بتحويل مبلغ معين من رصيد شخص آخر، ثم يزود الحاسب الآلي بالرقم الذي يسمح بنقل هذا المال، وبعدها يتم تقييده في الرصيد الذي يسيطر عليه الجاني، وعلى رغم الطبيعة غير المادية لهذا النقل، إلا أن الدفع أو النقل قد تم فعلا، وهو ما يعادل التسليم المادي لهذا المال.¹⁹

أما العنصر الثاني في جريمة السرقة فيتعلق بالقصد الجنائي وهو محقق أيضا في مسألة الحال، حيث يكون للجاني العلم والنية والقصد بإخراج المال من حرزه من أجل الإستيلاء عليه وتملكه، وهذا يعني ارتكاب الجريمة بشكل متعمد.

وهكذا لا يوجد ما يميز عناصر الإختلاس والسرقة في المجالين العادي والمعلوماتي، باستثناء بعض الظروف المحيطة بنفس الجريمة في كلتا الحالتين.

المسألة الثانية- تتعلق بتحديد الاختصاص القضائي لنظر جرائم الإنترنت :

إذا كان الجاذب الشرعي للجرائم الإلكترونية قد أمكن معالجته على النحو السابق، فإن المشكل الذي لا زال عالقا -حتى اليوم- يتعلق بتحديد القانون الواجب التطبيق وكذا الجهة القضائية صاحبة الاختصاص في نظر الجريمة.

على هذا المستوى، لا يبتأبنا أي غموض أو إبهام في حال انتماء أطراف الجريمة لنفس البلد، حيث يطبق قانون هذا البلد، وتكون محكمته هي صاحبة الاختصاص، لكن الطبيعة العالمية للإنترنت هي التي عقدت أكثر المسألة بتحديد كل الحدود الإقليمية للدول، وهنا تطرح " معضلة " التنازع القانوني على أكثر من صعيد.

ولعل مرونة هذه النقطة هي التي جعلت الفقهاء يفترقون في عدة اتجاهات:

• الاتجاه الأول- يرى أن تكون المحكمة المختصة بنظر النزاع هي محكمة الإقليم الذي وقعت فيه الجريمة، حتى ولو كان المجرم يحمل جنسية دولة أخرى، ولكن الانتقاد الذي وجه لهذا الاتجاه أنه لا يقدم لنا جوابا مناسباً في حال ارتكاب الجريمة في أكثر من دولة.²⁰

• الاتجاه الثاني- جعل المحكمة المختصة هي محكمة محل إقامة المدعى عليه، وقد أخذت معظم التشريعات العربية بهذا الاتجاه، بيد أنه لم يسلم من النقد هو الآخر، لا سيما إذا كان هذا الفعل لا يعدّ جرماً في نظر الدولة محل ارتكابه، خاصة وأن صنفاً راجحاً من الدول لا زال بعيداً عن السيطرة على أفعال الاعتداء على حقوق الملكية الفكرية، أو الدعاية الكاذبة أو المضللة... الخ.²¹

• الاتجاه الثالث- يرى أن المحكمة المختصة هي محكمة جنسية مرتكب الجريمة، لكن رغم الجاذبية التي يتمتع بها هذا الاتجاه، إلا أنه صعب التجسيد من الناحية العملية، خاصة وأن الجناة المسؤولين عن الجرائم الإلكترونية هم على درجة عالية من العلم والمعرفة والذكاء، ومن ثم فإن تقفي آثارهم قد ظل أمراً مستعسراً.

في الأخير، نرى بأن هذا التساؤل " القديم-الجديد " لا زال يفرض نفسه حتى اليوم، ولعل الحل الأنجع نسبياً يقتضي إخضاع دعوى المسؤولية لقانون الدولة التي وقع فيها

الجرم الإلكتروني، بشرط تحقق الجانب الشرعي للجريمة - أي تجريم الفعل - في كلا القانونين أي قانون المدعى والمدعى عليه.

وهو الحل الذي تم تبنيه من قبل الدول الصناعية الكبرى في العالم، بالرغم مما أصابه من انشغاقات بسبب بعض الصعوبات التي لازالت تعترضه على مستوى التطبيق الفعلي.

المطلب الثاني - مكافحة " الداء الإلكتروني " في البرامج الرسمية
في هذا السياق، يمكننا أن نستأنس بعدة حالات عملية شهيرة تتعلق بجرائم الإنترنت ولعل أهمها:

• قضية مورس: ومفادها أن طالبا يبلغ من العمر 23 عاما يدعى Rober Morris تمكن من إطلاق فيروس عبر الإنترنت عرف باسم " دودة مورس " وكان ذلك بتاريخ فبراير 1988، حيث أدى إلى إصابة 6000 جهاز يرتبط معه حوالي 60.000 نظام عبر الإنترنت، من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية. وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي 100 مليون دولار، إضافة إلى مبالغ أكثر من ذلك لتغطية الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم على " مورس " بالسجن لمدة 3 أعوام و 10.000 دولار غرامة.²²

• قضية نادي الفوضى: حيث قامت جماعة منظمة - خلال عام 1997 - بإنشاء برنامج يتحكم بلغة Actif-X مصمم للعمل عبر الإنترنت، ويمكنه اختراق برنامج " كويكن Quiken " المحاسبي، وهكذا أصبح بإمكان هذه الجماعة سرقة الأموال من أرصدة مستخدمي برنامج " كويكن " في جميع أنحاء العالم.²³

• فيروس ميليسا: حيث قام شاب أمريكي من ولاية " نيوجرسي " من إطلاق فيروس خطير عبر الإنترنت عرف باسم فيروس Melissa، من أجل اختراق برامج الاتصالات العامة واستغلال الخدمات المتصلة بها.

وبعد فتح تحقيق طويل من قبل الشرطة الدولية، تم الكشف عن الجاني واعتقاله في شهر مارس 1999، وحينها حكم عليه بالسجن لمدة 40 عاما وبغرامة مالية قدرت بنحو 500.000 دولار.²⁴

• قضية الجحيم العالمي: مفادها أن جماعة منظمة أطلق عليها اسم "مجموعة الجحيم العالمي Global Hell"، تمكنت من إعداد برنامج معلوماتي دقيق يسمح باختراق المواقع الإلكترونية السرية لكل من البيت الأبيض والشرطة الفيدرالية الأمريكية والبنك؟ون الأمريكي ووزارة الداخلية الأمريكية، واعتبرت الواقعة بمثابة تهديدا خطيرا ومباشرا على البلاد. وبعد حملة تحقيق واسعة النطاق تم الكشف عن أفراد هذه المجموعة الذين يحملون الجنسية الأمريكية، أما عن ظروف المحاكمة فقد ظلت حيز "الظلام" حتى اليوم لارتباط الجريمة بأمن واستقرار الدولة.²⁵

وعلى صعيد آخر فقد كشفت دراسة بريطانية أن المملكة المتحدة وحدها تشهد جريمة إلكترونية جديدة كل عشر ثوان، حيث شهدت البلاد ارتكاب أكثر من ثلاثة ملايين جريمة إلكترونية خلال عام 2008.

وفي السياق نفسه أكدت شركة "جارليك Jarlick" المتخصصة في مجال التأمين الإلكتروني أن أكثر من 60% من الجرائم تستهدف الأفراد (انتحال الشخصية، الإحتيال، التحرش الجنسي... الخ).²⁶

ومن جهته حذر "ريموند جينيس Raymond Jennis" مدير التقنية في شركة "تريند مايكرو Truind Maicro" أن القرصنة على وشك إجراء نقلة نوعية تقنية كبرى هي الأولى من نوعها في التاريخ، حيث أن الفيروسات والتروجان وما يمكن إرساله عبر البريد الإلكتروني، أصبح شيئا من الماضي، وأن الموجة الجديدة من القرصنة ستأتي مباشرة عبر مواقع الإنترنت فيما يمكن أن يطلق عليه اسم تهديد المواقع Threats Web.²⁷

وفي محاولة للحد من الجرائم الإلكترونية استحدث "الاتحاد الدولي للاتصالات" دليلا إلكترونيا وصف بأنه "خريطة الطريق" فيما يتعلق بمعايير الأمن الخاصة بتكنولوجيا المعلومات والاتصالات، حيث يستطيع اكتشاف المعلومات والبيانات المتجددة

باستمرار، ثم يتم حفظها وإرسالها لكل المنظمات المعنية بالأمن المعلوماتي من أجل التحقيق والمتابعة.²⁸

وفي نفس السياق، وللحد من الخطر القادم عبر الشبكات، سارعت بعض الدول إلى تثبيت نظام أمن وقائي من الجرائم، حيث شكلت وزارة الداخلية المصرية "دوريات أمنية" من خلال الشبكة، ومهامها منع الجريمة الإلكترونية قبل وقوعها.

كما شكلت الحكومة البريطانية وحدة من قوات الشرطة من أجل مراقبة ومتابعة هذا الصنف من الجرائم، وبعد اقتناع تام بالخطر القادم ومداولات استمرت أربع سنوات قامت ثلاثون دولة أوروبية بتوقيع معاهدة لتوحيد الجهود في محاربة الظاهرة.²⁹

ونجد أن بعض القوانين قد نصت على عقوبة مرتكب هذه الجرائم، مثل القانون الفرنسي الصادر في 1988/1/5 في مادته 462 التي نصت:

"من يتعرض بإرادته بشكل مباشر أو غير مباشر فيدخل بعض المعلومات في النظام الآلي لمعالجة معلومات أخرى أو نقلها أو تعديلها أو حذفها، يعاقب بالسجن من ثلاثة أشهر إلى ثلاثة سنوات، وبغرامة مالية تتراوح بين ألفين وخمسة آلاف فرنك فرنسي أو بإحدى هاتين العقوبتين"، وقريب من هذا ما ذهب إليه القانون الأمريكي والقانون البريطاني.

وفي السعودية، فرضت، الحكومة عقوبات تصل إلى الحبس لمدة عام واحد وبغرامات مالية لا تزيد عن 500.000 ريال، لقمع جرائم القرصنة المرتبطة بالإنترنت، وكذا الجرائم الإلكترونية القريبة منها.

الخاتمة :

أخيراً، إن التكنولوجيا المعلوماتية قد انتهت إلى الخضوع لهيمنة الأساليب "السلطوية" المتطفلة، خاصة منها ذات المنظور الإجرامي، وهذا ما جعل هذه التكنولوجيا الجذابة تفقد تدريجياً دقتها الأصلية بسبب تسرب وانتعاش الداء الإلكتروني في إطار متعدد الأشكال. وفي نهاية تطورها، فإنه لا شيء أصبح يميز العالم المعلوماتي عن العالم الطبيعي الخارجي، ذلك أن نمو و تطور الجريمة الإلكترونية بالشكل الذي نعرفه اليوم، إنما دليل على الإنترنت لا يمكنه الإفلات من "بصمة" الشر، وأن تنظيمه الهيكلي الداخلي ما هو إلا تماثل لظروف الحياة التقليدية.

ولعل ارتكاب الجريمة في الحالة الأخيرة هو أكثر خطراً وأكبر ضرراً، لأن العلم في الأخير يكون قد منح الدقة التي كانت تنقص المجرمين في السابق، وهذا ما جعل الإعتداءات التي يرتكبوها اليوم بواسطة الإنترنت تتميز بالقوة والفاعلية أكثر من أي وقت مضى.

وعليه فقد بات من الضروري إعادة النظر في سياسة إدارة ومراقبة الإنترنت، والتوجه نحو إيجاد أنجع الوسائل من أجل تسييره وتأطيره وتنميته وتطويره وترشيده حتى تكون بمثابة انطلاقة جديدة لتثبيت مصداقية التكنولوجيا المعلوماتية، واكتساب ثقة المتعاملين مع الإنترنت، والقضاء على الممارسات السلبية، وسدّ ثغرات الجرائم عن طريق توسيع مجالات تدخل القوات الأمنية المتخصصة.

ولعل تعميم المجال المعلوماتي هو مؤشر آخر على ضرورة توحيد وتوطيد الجهود خارج الحدود الإقليمية للدول، بعد ثبوت أن الجريمة الإلكترونية قد أضحت تمثل مسؤولية الجميع.

إن تجسيد هذه المهمة النبيلة لا يمكنه أن يتأتى إلا عن طريق وضع إطار دائم للتشاور والحوار بين الأجهزة الدولية المختلفة المكلفة بالمراقبة المعلوماتية، مع التكفل الجاد بهذا الانشغال، ذلك أن التنسيق ما بين مختلف هياكل المراقبة الرقمية عن طريق التشاور والتعاون، هي عوامل ضرورية يجب أن تعطى لها الأولوية.

في النهاية، فإن التكنولوجيا المعلوماتية وبالرغم مما أصابها من انشغاقات موضوعية إلا أنها لازالت حتى اليوم تمثل " اللغة المفضلة " للاتصالات، في عالم يتميز بالسرعة المتزايدة والتعقيد المتنامي، ومن ثم فإن انتشار الجرائم في إطار هذا الفضاء لا يمكنه أن ينقص من شأنها أو يقلل من قيمتها، لأن مستقبل " النسيج المعرفي " لا يمكنه أن يكون له " وجه آخر غير الإنترنت.

المراجع:

أولاً- المؤلفات:

1. الممنوح إبراهيم خالد، "إبرام العقد الإلكتروني، دراسة مقارنة"، دار الفكر الجامعي، الإسكندرية، 2006.
2. المناعسة أحمد والزعبي جلال محمد، "جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة"، دار وائل للنشر، الطبعة الأولى، عمان، 2001.
3. العريان محمد العريان، "الجرائم المعلوماتية"، دار الجامعة الجديدة للنشر، الإسكندرية، 2006.
4. الربيعي محمود، المعجم الشامل لمصطلحات الحاسب الآلي، دار النهضة العربية، القاهرة، 2005.
5. الشوي محمد ساجي، "ثورة المعلومات وانعكاساتها على قانون العقوبات"، دار الفكر العربي، القاهرة، 2003.
6. جميل عبد الباقي، "الجرائم الناشئة عن استخدام الحاسب الآلي"، دار النهضة العربية، القاهرة، 2004.
7. جميل عبد الباقي، "الجوانب الإجرائية للجرائم المتعلقة بالإنترنت"، دار النهضة العربية، القاهرة، 2006.
8. طه أحمد سالم، "الجرائم الناشئة عن استخدام الحاسب الآلي"، دار النهضة العربية، القاهرة، 2001.
9. منصور حسين منصور، "جرائم الكمبيوتر والإنترنت"، دار الجامعة الجديدة، الإسكندرية، 2003.
10. قوره نائلة عادل، "جرائم الحاسب الآلي"، منشورات الحلبي الحقوقية، الطبعة الأولى، بيروت، 2005.
11. رشدي محمد السعيد، "الإنترنت والجوانب القانونية لنظم المعلومات"، دار الكتب للطباعة والنشر، الكويت، 2002.

ثانيا- الرسائل الجامعية :

أ. رسائل الدكتوراه :

12. القدومي عدير، " جرائم الكمبيوتر " رسالة دكتوراه في القانون، كلية الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة، 2004-2005.

ب. رسائل الماجستير :

13. عرب يونس، " جرائم الحاسوب " رسالة ماجستير، فرع القانون الجنائي، جامعة عمان، الأردن، 1998-1999.

ثالثا- المقالات :

14. أبو عيد عارف خليل، " جرائم الإنترنت، دراسة مقارنة "، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 5، العدد الثالث، الإمارات العربية المتحدة، أكتوبر 2008.

15. عبد الله حسين علي محمود، " الجوانب القانونية والأمنية للعمليات الإلكترونية "، مجلة أكاديمية شرطة دبي، العدد الأول، الإمارات العربية المتحدة، مارس 2003.

رابعا- الوثائق (الملتقيات والأيام الدراسية) :

16. الكركي كمال أحمد، " التحقيق في جرائم الحاسوب "، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، الإمارات العربية المتحدة، 2006.

17. أشرف توفيق شمس الدين، " الحماية الجنائية للمستند الإلكتروني "، مؤتمر الأعمال المصرفية الإلكترونية، كلية الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة، 2003.

الهوامش :

- 1 - راجع- إبراهيم خالد ممنوح، ~ إبرام العقد الإلكتروني، دراسة مقارنة ~، دار الفكر الجامعي، الإسكندرية، 2006، ص 13.
- 2 - راجع- أحمد المناعسة وجمال محمد الزعبي، ~ جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة ~، دار وائل للنشر، الطبعة الأولى، عمان، 2001، ص 60.
- 3 - راجع- رشدي محمد السعيد، ~ الإنترنت والجوانب القانونية لنظام المعلومات ~، دار الكتب للطباعة والنشر، الكويت، 2002، ص 11 وما بعدها.
- 4 - راجع- عارف خليل أبو عيد، ~ جرائم الإنترنت، دراسة مقارنة ~، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 5، العدد الثالث، الإمارات العربية المتحدة، أكتوبر 2008، ص 79.
- 5 - المرجع السابق، ص 80.
- 6 - راجع- الربيعي محمود، المعجم الشامل لمصطلحات الحاسب الآلي، دار النهضة العربية، القاهرة، 2005، ص 26.
- 7 - المرجع السابق، ص 26.
- 8 - راجع- قوره نائلة عادل، ~ جرائم الحاسب الآلي ~، منشورات الدابي الحقوقية، الطبعة الأولى، بيروت، 2005، ص 17.
- 9 - راجع- عارف خليل أبو عيد، المرجع السابق، ص 83.
- 10 - راجع- قوره نائلة عادل، المرجع السابق، ص 18.
- 11 - راجع- منصور حسين منصور، ~ جرائم الكمبيوتر والإنترنت ~، دار الجامعة الجديدة، الإسكندرية، 2003، ص 155.
- 12 - المرجع السابق، ص 156.
- 13 - راجع- رشدي محمد السعيد، المرجع السابق، ص 65.
- 14 - راجع- عبد الله حسين علي محمود، ~ الجوانب القانونية والأمنية للعمليات الإلكترونية ~، مجلة أكاديمية شرطة دبي، العدد الأول، الإمارات العربية المتحدة، مارس 2003، ص 592.
- 15 - في تفصيل هذه المسألة راجع- الشوي محمد ساجي، ~ ثورة المعلومات وانعكاساتها على قانون العقوبات ~، دار الفكر العربي، القاهرة، 2003، ص 122 وما بعدها.
- 16 - راجع- عارف خليل أبو عيد، المرجع السابق، ص 94.
- 17 - حول هذه المسألة، راجع- عرب يونس، ~ جرائم الحاسوب ~، رسالة ماجستير، فرع القانون الجنائي، جامعة عمان، الأردن، 1999-1998، ص 147.
- راجع كذلك- أحمد سالم طه، ~ الجرائم الناشئة عن استخدام الحاسب الآلي ~، دار النهضة العربية،

- القاهرة، 2001، ص 254. راجع أيضا- قوره نائلة عادل، المرجع السابق، ص 78.
- 18 - راجع- عارف خليل أبو عيد، المرجع السابق، ص 87.
- 19 - راجع- جميل عبد الباقي، " الجرائم الناشئة عن استخدام الحاسب الآلي "، دار النهضة العربية، القاهرة، 2004، ص 92 و 93.
- 20 - المرجع السابق، ص 113 و 114.
- 21 - راجع- شمس الدين أشرف توفيق، " الحماية الجنائية للمستند الإلكتروني "، مؤتمر الأعمال المصرفية الإلكترونية، كلية الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة، 2003، ص 485 وما بعدها.
- 22 - راجع- جميل عبد الباقي، " الجوانب الإجرائية للجرائم المتعلقة بالإنترنت "، دار النهضة العربية، القاهرة، 2006، ص 112.
- 23 - المرجع السابق، ص 115.
- 24 - راجع- القدومي كبير، " جرائم الكمبيوتر "، رسالة دكتوراه في القانون، كلية الشريعة والقانون، جامعة الإمارات، الإمارات العربية المتحدة، 2005-2004، ص 364 وما بعدها.
- 25 - المرجع السابق، ص 369 و 370.
- 26 - راجع- العريان محمد العريان، " الجرائم المعلوماتية "، دار الجامعة الجديدة للنشر، الإسكندرية، 2006، ص 111.
- 27 - المرجع السابق، ص 113.
- 28 - راجع- الشوي محمد ساجي، المرجع السابق، ص 183.
- 29 - في تفصيل هذه المسألة، راجع- الكركي كمال أحمد، " التحقيق في جرائم الحاسوب "، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، الإمارات العربية المتحدة، 2006، ص 46 وما بعدها.