

الجريمة السيبرانية بين المفاهيم والنصوص التشريعية الجزائر أنموذجاً

الدكتور: نبيل دريس

كلية الحقوق والعلوم السياسية- جامعة البليدة 2.

ABSTRACT:

الملخص باللغة العربية:

The use of electronic means has become inevitable at all levels and in all public and private circles, to achieve these means of ease and speed of doing business and dealing with information, especially after the international télécommunications network appearance, known online as the, so it had to be addressed by the law and puts appropriate rules to take advantage of this scientific-induced, in order to preserve the Financial, personal, and intellectual property rights arising from the technological développement in the cyber-mail from any possible attack,

ان استخدام الوسائل الالكترونية والانترنت أصبح أمراً لا مفر منه على جميع الأصعدة وفي جميع الدوائر العامة والخاصة، لما تحقّقه هذه الوسائل من يسر وسرعة في أداء الأعمال والتعامل مع المعلومات، خاصة بعد ظهور شبكة الاتصالات الدولية المعروفة اختصاراً باسم الإنترنت، لذا كان لزاماً أن يتصدّى القانون ويضع القواعد الملزمة للاستفادة من هذا المستحدث العلمي، حتى تُحفظ الحقوق المالية والشخصية والفكرية المترتبة عن التطور التكنولوجي السيبراني الالكتروني من أي اعتداء محتمل، ولا تتحقّق الحماية القانونية للنظم السيبرانية إلا من خلال قواعد قانونية تجرّم كلّ فعل يهدف إلى الاعتداء ضد هذه النظم، أو يهدف إلى استخدامها كوسيلة لارتكاب إحدى الجرائم التقليدية، وهذا يتطلب تدخل القضاء لتوسيع نطاق النص الجنائي ليستوعب هذا النوع من الجرائم.

مقدمة:

شهد العالم ثورة كبيرة في مجال تكنولوجيا الحسابات الآلية ومعالجة البيانات الإلكترونية، وكانت هذه الثورة المعلوماتية وراء ما يُطلق عليه مصطلح صناعة المعلومات، حيث ظهرت منافذ استثمارية جديدة تمثّلت في مؤسسات وشركات

ومشروعات فردية، منها ما يهتم بتصنيع الحسابات، ومنها ما هو موجّه لإعداد البرامج لمعالجة المعلومات آلياً، وأخرى لتسويق هذه أو تلك أو التّعامل فيها بصفة عامّة، وأخرى تتولّى إعداد الإطارات الفنيّة المختصّة في تشغيلها، وغيرها من الاختصاصات.

ولقد صاحب هذه الثّورة تطوّرات وتغيّرات أصابت كلّ جوانب الحياة، ومست كلّ فئات المجتمع، ولم يكن القانون بمنأى عن ذلك؛ فالتّفاعل الأبدي بين القانون والواقع يعكس تطوّر كافّة العوامل الاقتصادية والاجتماعية والعلمية، من خلال مواجهة مستجدّاته أو عبر تطويع نظريّاته ومفاهيمه ومبادئه وأفكاره القائمة، والمرونة في تطبيقها.

ولا تتحقّق الحماية القانونية للنّظم السيبرانية وللموضوعات الناشئة عنها إلّا من خلال قواعد قانونية تجرّم كلّ فعل يهدف إلى الاعتداء ضد هذه النّظم، أو يهدف إلى استخدامها كوسيلة لارتكاب إحدى الجرائم التّقليدية، وهذا يتطلّب تدخّل القضاء لتوسيع نطاق النّص الجنائي ليستوعب هذا النوع من الجرائم، وقد يتطلّب تدخّل التشريع لسنّ قواعد قانونية خاصّة بها، وهذا ما حدث في أغلب دول العالم، ومنها الجزائر.

وحيث أنّ موضوع الجريمة السيبرانية يُعتبر من المواضيع المستجدة، ومن أهمّ الدّراسات والتّقارير حول الموضوع نذكر أبحاث مكتب تقييم التّقنية في الولايات المتّحدة الأمريكيّة، وتقارير معهد ستانفورد الدّولي للأبحاث، وكذلك القواعد الإرشادية للحماية الجنائية للبيانات الشّخصية التي قدّمتها منظّمة التّعاون الاقتصادي والتنمية OECD.

أما على المستوى العربي، فإنّ الاهتمام بهذا الموضوع يكاد يكون منعدماً، وهذا راجع إلى قلة ارتكاب مثل هذا النوع من الجرائم بسبب انحصار استخدام الوسائل الالكترونية والانترنت في الحياة، ومع ذلك فقد ظهرت بعض الدراسات في الموضوع، إلا أنّ هذه الدراسات لم تضيف الجديد للمكتبة القانونية، فهي إمّا نقل كامل عن المراجع الاجنبية، وموضوع الجريمة السيبرانية بشكل موضوعي يعتمد على وضع الآراء الفقهية والتجسيدات التشريعية للاستفادة منها، وذلك عن طريق تحليل جميع الآراء ووضع مقارنات والبحث عن نقاط الاتفاق والاختلاف. ومما سبق من أهداف، نطرح الإشكالية التالية:

- إلى أي مدى يمكن اعتبار الحماية القانونية من الجرائم السيبرانية من خلال النصوص الجنائية التقليدية كافية وملائمة، وهل يستوجب الأمر وضع نصوص خاصة لهذا النوع من الجرائم ؟ وما مدى إحاطة التشريع الجنائي المقارن بهذه الجريمة من خلال نصوص خاصة ؟ وما هو موقف المشرع الجزائري من الجريمة السيبرانية ؟

المحور الأول: الإطار المفاهيمي، نظم الحماية القانونية من الجرائم السيبرانية.

يُعدّ جهاز الكمبيوتر أو الحاسب¹، من أهمّ الابتكارات التي توصل إليها مهندسو ومصمّمو الأجهزة الإلكترونية لما يميّز به من قدرة فائقة على معالجة البيانات وتخزينها واسترجاعها بسرعة، ولا يقوم الكمبيوتر بمهامه إلاّ بعد تغذيته ببرامج رقمية وتجهيزه إذا تطلّب الأمر بالوسائط الصّورية التي تجعله أكثر فعالية وملاءمة

¹ نعتبر المصطلحات التالية بنفس الدلالة، وهي: الكمبيوتر، الحاسب، الحاسب الآلي، الحاسب الإلكتروني، الحاسوب، الناظم الآلي والمنظم الآلي.

لمتطلبات العصر، بما في ذلك مجال الاتصالات الرقمية؛ كل ذلك يشكل نظاماً متكاملًا يسمّى بالنظام المعلوماتي.

ولهذا ليس غريباً أن نرى الحاسبات الآلية قد غزت مجالات كثيرة في المجتمع، وأصبحت الاستعانة بها واستخدامها ضرورة لا غنى عنها على مستوى أجهزة الدولة وإداراتها، أو على مستوى المشروعات العامة والخاصة، أو على مستوى الأفراد العاديين. كما أضحت استخدامها أمراً لا مفر منه حالياً في الدول الأوروبية وفي الدول المتقدمة عموماً، وفي دول العالم الثالث سيأتي يوم قريب تكون فيه الحاجة إليها ملحة¹.

وبفضل هذه الثورة المعلوماتية وانتشار وسائل الاتصال عن بعد، أصبح العالم قرية كونية صغيرة تسبح في فضاء إلكتروني تتقلّص فيه المسافات، فانفتحت كافة المجتمعات الإنسانية عبر شبكة الإنترنت التي أزاحت الحواجز التقليدية بين الدول، وأصبح بإمكان شعوب العالم التّحاور في أيّ وقت ومن أيّ مكان عبر تلك الشبكة العجيبة دون أيّ حائل².

إنّ التّقدم العلمي والتّكنولوجي في العصر الحديث يفتح آفاقاً ضخمة أمام تقدّم البشرية وتحقيق مستوى أفضل من الحياة، إلّا أنّه يحمل في نفس الوقت بين طياته مخاطر ضخمة تهدّد قيم و حقوق وأمن الأفراد والجماعات، وبدأت الحاجة ماسةً لمواجهة تلك المخاطر والتّغييرات، ولعلّ أوّل التّطلّعات في هذا المجال كان نحو القانون، الذي يُعدّ من أقدس مهامه وضع الصّيغ الملائمة للاستفادة من التّقدّم

¹ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، صفحة غير مرقّمة.

² نجوى أبو هيبه، التّوقيع الإلكتروني، دار النّهضة العربية، القاهرة، 2002، ص: 4.

العلمي دون المساس بالقيم والحقوق والحريات الأساسية للأفراد. ومن هنا كانت أهمية وجود الضوابط القانونية التي يعمل في إطارها التطور التكنولوجي، ودون هذه الضوابط يصبح التّقدّم العلمي يشكل خطراً على المجتمع، وعلى حقوق وأمن المواطنين¹، وعلى ذلك، فقد ظهرت علاقات تربط منظومة الحماية القانونية من الجرائم السيبرانية بالمنظومة القانونية من خلال ما يسمى بقانون المعلوماتية، هذا الأخير يعمل على حماية النّظم المعلوماتية من الإعتداء، ويضع الإطار الصحيح لتداولها، كما يعمل على تحقيق هذه الحماية من خلال نصوص خاصة أو من خلال إعمال النّصوص التقليدية، وعليه ولكي تتّضح هذه العلاقة، نتعرض لمفهوم النّظام المعلوماتي، وقانون المعلوماتية وتحديد نطاقه.

الفرع الأول: مفهوم النّظام السيبراني.

تتجسّد فكرة السيبرانية من خلال نظام يتفاعل فيه الحاسب الآلي مع المعلومات عن طريق تفاعل الكيان المادي المكوّن للحاسب الآلي مع الكيان المنطقي، والذي يتمثّل في مجموعة البرامج والأوامر التي تخرج الكيان المادي من حالة الجمود إلى حالة الفعّالية والأداء المفيد. هذا النّظام يسمّى بالنّظام المعلوماتي.

1. تعريف النّظام السيبراني

نعني بالنّظام المعلوماتي كلّ مكوّنات الحاسب الآلي المادية **HardWare** والمعنوية **SoftWare**، وشبكات الاتّصال الخاصّة به **NetWorks**، أو هي مجموع عناصر مادية وغير مادية يمكن باجتماعها العمل الفوري مع المعلومة².

¹ محمّد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2003، ص: 8.

² رشا مصطفى أبو الغيط، الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، 2003، ص: 5.

فالحاسب الآلي منظور إليه من خلال مكوناته المادية المحسوسة لا يعدو أن يكون كتلة حديدية غير قادرة على القيام بشيء في حد ذاتها ومن تلقاء نفسها، ولكنها معدة لكي تنفذ ما يقدمه لها الإنسان من تعليمات، فالجهاز لا يبحث ولا يقارن ولا يحسب إلا لأن الإنسان قد أعدّه وأمدّه بالمعلومات (أي العنصر غير المادي أو الكيان المنطقي) التي تمكنه من تقديم النتائج وإجراء العمليات التي هيأه الإنسان لإعدادها، وهكذا فإنّ الكيان المادي لا يعدو أن يكون مجرد العناصر المادية للحاسب الآلي والتي يمكن لمسها وإدراك وجودها¹.

2. عناصر النظام السيبراني:

ذكرنا فيما سبق أنّ النظام المعلوماتي يقوم على عنصرين، أحدهما مادي والآخر معنوي، هذا بيانها:

أ- العنصر المادي HardWare :

يتمثل أساساً في جهاز الحاسب الآلي بالإضافة إلى مجموعة من ملحقاته والوسائط التي توصل به لكي يتلقّى من خلالها المعطيات والمعلومات، أو لكي يخرج من خلالها النتائج بعد المعالجة. فالحاسب الآلي هو جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعليمات المعطاة له بسرعات كبيرة، تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة، وبدرجة عالية الدقة، وله القدرة على التعامل مع كمّ هائل من المعلومات، وكذلك تخزينها واسترجاعها عند الحاجة إليها². أو هو عبارة عن آلة يمكن برمجتها لتقبل بيانات (مدخلات) وتجري

¹ محمد محمد شتّا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001، ص: 50.

² هلالى عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1999، ص: 16.

تشغيلاً عليها لتحوّلها إلى معلومات مفيدة (مخرجات)، وتخزينها للاحتفاظ بها لاستخدامها في المستقبل¹، ويتكوّن من الوحدات التالية:

- **وحدات الإدخال:** تقبل بيانات أو أوامر في صورة يستطيع الحاسب أن يستخدمها بها، وذلك بإدخالها إلى وحدة التشغيل المركزية وبتوجيه من وحدة التحكم والمراقبة.

- **وحدات الإخراج:** تظهر البيانات التي أجري عليها التشغيل (المعلومات) في صور مفهومة للمتلقّي، سواءً كان إنساناً أو وسيطاً متّصلاً بالحاسب، وتشمل الشاشة والطابعة والرّاسم وسّماعات الإخراج الصّوتي... إلخ.

- **وحدة المعالجة المركزية:** وبها دوائر إلكترونية تعالج بيانات المدخلات لتحوّلها إلى معلومات، وتسمّى أيضاً وحدة التشغيل المركزية. وهكذا فإنّ وحدة التشغيل تتكوّن من وحدة الحساب والمنطق، وهي تقوم بجميع العمليات الحسابية كالجمع والطّرح والقسمة، وتقوم بالمقارنات المنطقية مثل (أكبر من) أو (أصغر من) أو (تساوي) وغير ذلك². وأثناء إجراء العمليّات الحسابية والمنطقية تحتاج وحدة الحساب والمنطق لتخزين بعض البيانات بصورة مؤقتة إلى مسجّلات كذاكرة خاصّة بها، حيث تتراكم وتتجمّع بيانات العمليّات الوسيطة³، وتتكوّن أيضاً وحدة المعالجة المركزية من ذاكرة للقراءة فقط مخزّن فيها برنامج التشغيل الابتدائي للحاسوب؛ هذا البرنامج مهمّته التّعرف على عناصر الجهاز وتحميل نظام التشغيل ليتولّى المهمة، وتتكوّن أيضاً من ذاكرة للقراءة والكتابة RAM تخزّن فيها

¹ كابرون، الحاسبات والاتّصالات والإنترنت، ترجمة: سرور علي إبراهيم سرور، دار المريح للنشر، الرياض، 2003، ص: 82.

² محمّد محمّد شتّا، المرجع السابق، ص: 51.

³ هلاّلي عبد الله أحمد، المرجع السابق، ص: 22.

المعلومات مؤقتاً إلى حين تخزينها على دعامات أو إخراجها عن طريق وحدات الإخراج. بالإضافة إلى ذلك تشمل وحدة المعالجة المركزية وحدة التحكم والمراقبة التي تقوم بالتنسيق بين وحدات الحاسب الأخرى، وضبط كافة التعليمات التي تتم داخل وحدة المعالجة المركزية بإرسال إشارات إلى كل الوحدات المعنية بالأمر¹.

- **وحدات التخزين:** وهي تحتفظ بالبيانات والبرامج بصفة دائمة، وهي أنواع كثيرة منها الأشرطة المغنطة، والاسطوانات المغنطة، والاسطوانات المرنة، والقرص الصلب، وتعتبر الاسطوانات الضوئية أو ما يسمى بأقراص الليزر **CD.ROM** ذات السعة التخزينية الهائلة أكثر وسائل التخزين تطوراً وفعالية، وتنقسم أجهزة الكمبيوتر بحسب طريقة أدائها إلى كمبيوتر رقمي، وفيه تخزن البيانات في ذاكرته على شكل أرقام²

ب- **العنصر المعنوي software:**

وهو ما يعرف بالكيان المنطقي للنظام المعلوماتي، والذي يشمل جميع العناصر غير المادية اللازمة لتشغيل الكيان المادي، وعرفه المنشور الفرنسي الصادر في 22 نوفمبر 1981 بأنه مجموع البرامج والأساليب والقواعد، وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات.

إذاً يختلف الكيان المنطقي عن البرنامج، فالكيان المنطقي مصطلح أعم وأشمل من البرنامج، حيث يضم بالإضافة إلى البرنامج وصف البرنامج والمستندات الملحقة بالبرنامج. وهكذا فإن البرنامج في مفهومه الواسع يضم إلى جانب التعليمات والأوامر

¹ هلالى عبد الله أحمد، نفس المرجع، ص: 23.

² محمد أمين الزومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004،

ص: 14.

(المفهوم الضيق) التّعليمات الموجهة إلى العميل، مثل بيانات استعمال البرنامج وكيفية المعالجة الإلكترونية للمعلومات.

الفرع الثاني: تعريف ونطاق قانون السيبرانية.

أدى التّطوّر الكبير في نظم الفضاء السيبراني إلى ظهور مجالات أوسع لاستخدام هذه التّقنية، وذلك لما تتميز به الحاسبات من سرعة في تنفيذ العمليّات والأوامر، ومن إمكانية تخزين كمّيات هائلة من البيانات واسترجاعها بكفاءة، بالإضافة إلى إجراء الاتّصالات.

وعلى إثر ذلك، ظهرت علاقات قانونية تنظّم كيفية التّعامل والتّعاطي مع هذا المستحدث المعلوماتي، وحمايته من الاعتداءات والاستعمال غير المشروع، ووضع قواعد كفيلة بنقل تكنولوجيا المعلومات على الوجه الصّحيح.

ومن ثمّ، كان لزاماً إيجاد منظومة قانونية تتصدّى لجميع الموضوعات الناشئة عن هذه العلاقات، وذلك بتطويع النّصوص التّقليدية واستحداث تشريعات جديدة خاصّة بنظم المعلوماتية، لتشكّل بذلك ما يسمّى بقانون المعلوماتية.

1. تعريف قانون السيبرانية:

السيبرانية فكرة واسعة ولها قوانينها الصّابطة، ويمكن تعريف قانون السيبرانية بأنّه: "مجموع القواعد والأحكام الواردة في شتّى فروع القانون، والتي يمكن تطبيقها على مسألة معلوماتية بحسب نوع المشكلة المثارة، والتي قد تخضع لأحكام قانونية متعدّدة"¹. وتشير فكرة المعلوماتية قلّقاُ بالغاُ إذا استخدمت أنظمة المعلومات في انتهاك حقوق الأفراد وحرّياتهم العامّة، كما أنّ ظهور فكرة المعلوماتية قد أدّى إلى

¹ أحمد خالد العجلوني، التّعاقد عن طريق الإنترنت، الدّار العلمية الدّولية للنشر، عمّان، 2002،

ابتداع عقود جديدة هي عقود المعلوماتية، تعتبر المعلومات محلاً لها. وقد تشعبت موضوعات قانون المعلوماتية ومست جميع المجالات الإنسانية وكافة فروع القانون.

2. نطاق قانون السيبرانية

يشمل قانون المعلوماتية القوانين التقليدية كالقانون المدني والجنائي والتجاري، ويشمل قوانين حماية الملكية الفكرية والقوانين الخاصة والاتفاقيات الدولية، وذلك فيما يتعلق بموضوع نظم المعلوماتية. وتظهر أهمية القانون المدني باعتباره مصدراً لقانون المعلوماتية في المقاربة القانونية للتعاقد [الإلكتروني] عن طريق الإنترنت مع النظرية العامة للعقد، حيث يُثار التساؤل عن مدى قانونية ومشروعية هذا النوع من التعاقد، كما يثار التساؤل عن مدى تطابق هذا التعاقد مع وسائل التعبير عن الإرادة¹.

المحور الثاني: الجريمة السيبرانية في الفكر القانوني.

الجريمة هي فعل غير مشروع صادر عن إرادة جنائية، ويقرّر القانون لهذا الفعل عقوبة أو تدبيراً أمنياً، وكان من نتائج التطور التكنولوجي في الوقت الراهن وجود ثمة علاقة ارتباط قوية بين القانون والجريمة.

الفرع الأول: ماهية الجريمة السيبرانية.

الجريمة السيبرانية جريمة مستحدثة، يعتمد مرتكبها على وسائل تقنية، ويكون ذا دراية كافية باستخدام النظم المعلوماتية، لذا فإن الإحاطة بمفهومها الدقيق لا يزال محل خلاف فقهي، وعليه نذكر بعض المفاهيم حول الجريمة السيبرانية وكذا موضوعاتها.

¹ محمد حسين منصور، المرجع السابق، ص: 18.

1. مفهوم الجريمة السيبرانية

الجريمة السيبرانية هي فعل أو امتناع عمدي ينشأ عن الإستخدام غير المشروع لتقنية المعلومات، يهدف إلى الاعتداء على الأموال المادية أو المعنوية [أو الاعتداء على خصوصية للأفراد]، أو هي عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به، من جهة أخرى هي الجريمة التي يكون النظام المعلوماتي فيها وسيلة لارتكاب جريمة تقليدية، إما ضدّ الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضدّ الأشخاص كجريمة السب أو القذف عبر الإنترنت.

أما في الجزائر فقد عالج الأمر: 97-10 المتعلق بحماية حق المؤلف والحقوق المجاورة الملغى بالأمر 03-05 مسألة التعدي على المصنّفات المعلوماتية إذ أدرج هذه الأخيرة بموجب المادة 4/أ ضمن المصنّفات المحمية قانوناً، ثم صدر القانون 04-15 المؤرخ في: 10-11-2004 المعدّل والمتمّم لقانون العقوبات¹، أدرج فيه المشرّع قسماً كاملاً متعلّقاً بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما صدر قانوناً² يتضمنّ القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها، نصّ على أحكام إجرائية تتعلّق بكيفيات التحقيق في هذه الجرائم، وأدرج عقوبات تسلّط على كل من يعرقل حسن سير التحقيقات القضائية في هذا المجال.

¹ القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 مؤرخة في 10 نوفمبر 2004.

² القانون رقم: 09-04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها، الجريدة الرسمية عدد 47، مؤرخة في 16 غشت 2009.

2. أسباب ارتكاب الجريمة السيبرانية:

إنَّ أسباب انتشار الإجرام المعلوماتي تتأثّر بلا شكّ بالثّورة المعلوماتية، وإذا كانت الأنماط المختلفة للمجرمين المعلوماتيين تكشف لنا عن اشتراك هؤلاء عند ارتكابهم الجريمة المعلوماتية في غرض واحد؛ هو مجرّد الهواية واللّهُو في بداية الأمر، وذلك نتيجة انبهارهم بالثّورة المعلوماتية والحاسبات الآلية، فمن ناحية أخرى قد يكون رغبة هؤلاء المجرمين في تحقيق الثّراء السّريع يمثّل أيضاً أحد أسباب انتشار الإجرام السيبراني، وأخيراً قد تكون الأسباب الشّخصية بالمجرمين هي أحد أسباب ذلك¹. وعليه يمكن تلخيص أسباب انتشار الجريمة المعلوماتية فيما يلي:

أ- **الولع بجمع المعلومات:** هناك من يقوم بارتكاب جرائم الكمبيوتر بغية الحصول على الجديد من المعلومات، فيرى قرصنة الكمبيوتر أنّ الحصول على المعلومة يجب ألا يكون عليه أيّ قيد؛ فالقرصان يكرّس كلّ جهده في تعلّم كيفية اختراق المواقع المحمية، وغالباً ما يكون القرصنة مجموعات الهدف منها التّعاون وتبادل المعلومات وتقاسم البرامج والأخبار.

ب- **تحقيق مكاسب مالية:** قد تدفع حاجة البعض إلى تحقيق الثّراء السّريع عن طريق إتاحة الاطّلاع على معلومات معيّنة أساسية ذات أهمية خاصّة لمن يطلبها.

ت- **الدّوافع الشّخصية:** يتأثّر الإنسان في بعض الأحيان ببعض المؤثّرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توافر هذه المؤثّرات، فإنّ الأمر يؤوّل في النّهاية إلى ارتكابه لجريمة معلوماتية، هذا

¹ محمّد أمين الرّومي، المرجع السابق، ص: 24.

وتتعدّد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك، سواء كان ذلك بدافع اللّهُو أو الانتقام.

3. موضوع الجريمة السيبرانية:

إنّ المعيار في تحديد ما إذا كان الاعتداء يستهدف الشقّ المعنوي من النظام المعلوماتي من خلال استهداف شقّه الماديّ يتعلّق بالبحث في اتّجاه القصد الجنائي، فإنّ كان القصد هو الاعتداء على المكوّنات الماديّة، فهنا الجريمة هي جريمة الإعتداء على ملك الغير أو غيرها من الجرائم التّقليدية، أمّا إذا كان القصد هو الإعتداء على البرامج والمعلومات، فالجريمة من غير شكّ من الجرائم المعلوماتية.

الفرع الثّاني: وقوع الجريمة باستخدام النظام المعلوماتي.

في هذه الحالة، الجريمة لا تقع على جهاز الكمبيوتر ذاته أو على ما يحتويه من معلومات وبرامج، ولكن تقع باستخدام الكمبيوتر كأداة لتنفيذ الجريمة، ومن أمثلة هذه الجرائم، التّجسس والتّصنّت والتّزوير في عمليات سحب جوائز المسابقات وتحويل الأموال من حساب إلى آخر، وهناك الجرائم التي تُرتكب على شبكة الإنترنت أو بواسطتها، وهي دائماً في ازدياد نتيجة التّطوّر التّكنولوجي المتواصل. وجرائم الإنترنت إمّا أن يكون محلّ الإعتداء فيها هو المال، وإمّا أن يكون محلّ الإعتداء فيها هو الأشخاص، وقد يكون محلّ الاعتداء فيها هو الحقوق الذّهنية، كالاعتداء على حقوق المؤلّف، ومن أمثلة جرائم الإنترنت جريمة السّب والقذف، وجريمة النّصب عن طريق الإعلان عن بيع سلع وهمية والاستيلاء على أموال العملاء، وكذلك جريمة انتحال شخصية الغير وإبرام صفقات تجارية باسمه.

وللتغلب على هذه الجريمة بدأت كثير من الشركات في المعاملات التجارية الهامة على شبكة الإنترنت -للتأكد من هوية المتعامل معها- اشتراط أن يوقع المتعامل معها إلكترونياً على العقد.

1. إثبات الجريمة السيبرانية:

لا شك أنه كلما تقدّم الإنسان في فهم تقنية العمل في الحاسبات الآلية كلما استطاع أن يرتكب جريمته دون أن يخلف أي آثار يمكن الإعتداء إليه من خلالها، ولهذا تعتبر هذه الجريمة من أهمّ الجرائم التي تحتاج إلى حماية جنائية كافية.

2. القصور في القوانين الجنائية ومشكل الاختصاص:

الجرائم السيبرانية تثير صعوبات جمة أمام تطبيق النصوص التقليدية الجنائية المنصوص عليها في القوانين القائمة، وهذه الصعوبات ترجع في الغالب إلى أنّ هذه النصوص قد وضعت أساساً لحماية الأشياء المادية في مواجهة صور الإعتداء المألوفة والتقليدية، وبمعنى آخر فإنّ مثل هذه النصوص قد يتعذر معها أو يستحيل معها أن تقع تحت طائلة العقاب في حالة الاعتداء على المكونات غير المادية لأنظمة المعلوماتية¹.

وكذلك قد لا تتمتع البرامج والمعلومات المعالجة بحماية جنائية من خلال قانون حق المؤلف بسبب تخلف أحد شروط هذه الحماية، وبصفة خاصة شرط الابتكار، مما يتطلب ضرورة توافر حماية جنائية إضافية.

¹ في المواد 16، 37، 40 من قانون الإجراءات الجزائية، وسن أيضاً بموجب القانون رقم 04-09 السابق الذكر.

ونظراً لهذه الخصوصية فقد وسّع المشرّع الجزائري¹ في مجال اختصاص جهة التحريات الأولية والنيابة والتحقيق إذا تعلّق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

3. ضبط مكونات النظم السيبرانية:

الضبط هو التّحقّط على الأشياء وحجزها ووضعها في أختام، فيجيز القانون لقاضي التحقيق أن يقوم بذلك إذا كانت هذه الأشياء والوثائق تتفع في إظهار الحقيقة، أو تلك التي يضرّ إفشاؤها بسرّ التحقيق، والضبط عادة ما يكون مقترناً بالتّفتيش الذي يهدف إلى نفس النتيجة.

والضبط الذي يقع نتيجة تفتيش قد يرد على منقولات تقليدية كما قد يرد على مكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، وهي من المنقولات أيضاً، ولذا نرى تسميتها بالمنقولات المعلوماتية تمييزاً لها عن سابقتها. ولأنّه بالإضافة إلى إمكانية نقلها من مكان لآخر، فإنّه أيضاً يمكن نقل البيانات المعالجة إلكترونياً أو المعلومات من حاسب معيّن إلى حاسبات أخرى عن طريق شبكات الاتصال².

الفرع الثاني: مدى قابلية المكونات المادية والمعنوية في النظام المعلوماتي للضبط.

لا يثير ضبط المكونات المادية للحاسب الآلي مشاكل في الفقه المقارن، في إمكانية ضبط الوحدات المعلوماتية، أمّا بالنسبة لمكونات الحاسب المعنوية فالمسألة ليست بالأمر السهل، بل إنّها أكثر تعقيداً وتركيباً، لأنّها تثير مشكلة لامادية بيانات الحاسب الآلي، فإذا كان التفتيش يتمّ لمكونات الحاسب المادية، فهل الشّيء الذي يتمّ

¹ المادتان 65 مكرر 9 و 6 مكرر 10 من قانون الإجراءات الجزائية.

² القسم 94 من ق.إ.ج الألماني.

ضبطه هو هذا الشيء المادي، أم أنه يتضمّن كذلك البيانات غير المادية، وما هو السند القانوني في ذلك؟

هناك رأي ينظر إلى الواقع العملي الذي يؤكّد أنّ الضبط لا يُتصوّر إلاّ إذا اتخذت بيانات الحاسب الآلي شكلا ماديا، ففي ألمانيا فإنّ الأدلة المضبوطة يجب أن تكون أشياء ملموسة، وبالتالي لا تشكّل البيانات أشياء يمكن ضبطها، لكن إذا تمّ طبع هذه البيانات.

1. مدى قابلية الرسائل الإلكترونية للضبط:

يقصد بالبريد الإلكتروني E-Mail الرسائل الإلكترونية التي تبعث عن طريق استخدام شبكات الحاسب كديل عن الوسائل التقليدية، حيث يخصص لكل شخص صندوق بريد إلكتروني تسجّل فيه جميع المراسلات الواردة أو الصادرة أو المستغنى عنها في سلّة المهملات، ويمكن الاطلاع على محتوى الصندوق أو الإرسال من أي مكان في العالم باستخدام خطوط التليفون أو الموجات اللاسلكية أو الأقمار الصناعية¹.

ومن المسائل الهامة المتعلقة بالبريد الإلكتروني كيفية المحافظة على سرّيته، وفي هذا الخصوص عجّلت نظم البريد الإلكتروني بابتكار برامج تشفير خاصة بحيث لا يمكن الاطلاع على أية رسالة إلاّ ممن يعرف تلك الشفرة. ولكي يتمّ ضبط الرسائل الإلكترونية، على المحقّق اختيار صندوق البريد الخاص بالمتهم محلّ التفتيش، وذلك بعد إعطاء شفرة الدخول، ومن ثمّ يمكنه الاطلاع على جميع الرسائل المحفوظة وتخزينها على دعامات خارجية أو طباعتها على الورق لتكون بذلك أدلة

¹ يشار محمود دودين، الإطار القانوني للعقد المبرم عبر شبكة الإنترنت وفقاً لقانون المعاملات الالكترونية وبالتأصيل مع النظرية العامة للعقد في القانون المدني، دار الثقافة للنشر والتوزيع، الأردن، 2006، ص: 26.

تستخدم في مواجهة المتّهم مع ضرورة أن يحزّر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضراً عن كل عملية اعتراض وتسجيل المراسلات، وكذا عن عمليات وضع الترتيبات التقنية، وعمليات الإلتقاط والتثبيت والتسجيل الصوتي أو السّمي البصري، ويصف أو ينسخ المراسلات والصّور والمحادثات المسجّلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف.

وأضاف أحكاماً جديدة¹ تنظّم مباشرة إجراءات الحجز فعندما تكتشف السلطة التي تباشر التّفتيش في منظومة معلوماتية معطيات مخزّنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنّه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة الوضع في أحرار وفقاً للقواعد المقرّرة في قانون الإجراءات الجزائية².

وإذا كان التّعديل الأخير لقانون العقوبات الجزائري لم ينص صراحة على مسألة تزوير المحرّرات الإلكترونية، إلّا أنّه يمكن تطبيق نصّ المادّة 394 مكرّر 1 التي تجرّم فعل الإدخال بطريق الغش لمعطيات في نظام المعالجة الآلية، أو الإزالة أو التّعديل بطريق الغش للمعطيات التي يتضمّنّها، ومنها المحرّرات الإلكترونية.

الخاتمة:

من خلال موضوع مفهوم الجرائم السيبرانية، والتي كنت قد مهّدت لها بإبراز العلاقة التي تربط المنظومة القانونية بالنّظم المعلوماتية، حيث ظهرت ضوابط

¹ المواد 6، 7، 8، 9 من القانون 09-04 السالف الذكر.

² الأمر رقم: 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بمقتضى القانون رقم: 17-07، المؤرخ في 27 مارس 2017، المنشور بالجريدة الرسمية عدد 20، مؤرخة في 29 مارس 2017.

قانونية يعمل في إطارها التطور في مجال تكنولوجيا المعلومات، وبخاصة بعد أن أصبح استخدام الوسائل المعلوماتية ضرورة لا غنى عنها على مستوى أجهزة الدولة وإداراتها، أو على مستوى المشروعات العامة والخاصة، أو على مستوى الأفراد العاديين.

وتطّرت بعد ذلك لمفهوم الجريمة السيبرانية، حيث خلصت إلى أن الجريمة السيبرانية مستحدثة، مرتبطة أساساً بوجود نظام معلوماتي، وتُرتكب من مجرم متميّز ذي دراية كافية بطريقة عمل هذا النظام واستغلاله في القيام بأعمال غير مشروعة، يكون الغرض منها غالباً إما الحصول على معلومات أو برامج، وإما تحقيق مكاسب مادية، وإما لدوافع شخصية.

إنّ الاعتداء على المكونات المادية للنظام المعلوماتي لا تثير أيّ أشكال، إذ لا يوجد أدنى شك في خضوع الفعل إلى قانون العقوبات على اعتباره يشكّل جريمة تقليدية ضدّ الأموال، كالسرقة أو الإتلاف أو الحريق، لكن يصعب الأمر في حالة وقوع الاعتداء على العنصر المعنوي في النظام المعلوماتي كالبرامج والمعلومات المخزنة، ذلك أنّ جرائم الأموال يُشترط لتحقيق وقوعها أن يكون محلّ الاعتداء شيئاً مادياً منقولاً، ومع ذلك فقد اتفق أغلب الفقه على أنّ النص الجنائي الخاص بجرائم الأموال يستوعب الكيان المعنوي للنظام المعلوماتي لعموميته.

هناك جرائم ترتكب باستخدام النظام المعلوماتي وخاصة تلك التي تنفذ على شبكة الإنترنت أو بواسطتها، وهي دائماً في ازدياد نتيجة التطور التكنولوجي المتواصل، وهذه الجرائم إما أن يكون محلّها المال، وإما أن يكون محلّها الأشخاص، وإما أن يكون محلّها الحقوق الذهنية كحق المؤلف.

ونظراً لخصوصية الجريمة السيبرانية، فقد وسَّع المشرِّع الجزائري في مجال اختصاص جهة التحريات الأولية والنيابة والتحقيق إذا تعلَّق الأمر بالجرائم الماسَّة بأنظمة المعالجة الآلية للمعطيات، ونظراً لهذه الخصوصية فإنَّ اكتشاف وقوع الجريمة السيبرانية وإثباتها يُعتبر من الصَّعوبة بما كان، لأنَّها لا تترك أثراً خارجياً كالذي تتركه الجرائم التقليديَّة، ممَّا يتيح لبعض الجناة الإفلات من توقيع الجزاء، وترجع الصَّعوبة أيضاً في توقيع الجزاء لوجود مبادئ تحكم القانون الجنائي منها مبدأ إقليمية القانون الجنائي، عينيته وشخصيته وعالميته.

أمَّا بالنسبة لضبط الأشياء المعلوماتية، فإنَّ ضبط المكونات المادية كالحاسب والأقراص لا يثير أيَّ إشكال في الفقه المقارن، أمَّا بالنسبة لمكونات الحاسب المعنوية فالمسألة تعدَّدت فيها الآراء، ومن بين هذه الآراء الرأْي الذي ينظر إلى الواقع العملي والذي يؤكِّد أنَّ الضَّبط لا يتصوَّر إلَّا إذا اتخذت بيانات الحاسب الآلي شكلاً مادياً، كأنَّ تُنسخ على دعامات أو يُطبع محتواها، وهذا الرأْي سائد في ألمانيا ورومانيا والولايات المتَّحدة والمملكة المتَّحدة.

كخلاصة لما سبق يمكن القول أنَّه يمكن إخضاع بعض الجرائم السيبرانية للنصوص الجنائية التقليديَّة، وهذا في غياب نصوص خاصَّة بها؛ فجريمة سرقة البرامج والبيانات المعالجة آلياً وجريمة التَّحويل الإلكتروني غير المشروع للأموال وجريمة الإتلاف المعلوماتي، وجريمة تزوير محرَّرات التَّجارة الإلكترونيَّة والتَّوقيع الإلكتروني وغيرها، تخضع كلُّها لنصوص جرائم الأموال في قانون العقوبات، وجريمة القذف والسَّب عبر الإنترنت تخضع هي الأخرى لنصوص جرائم الأشخاص في قانون العقوبات.

قائمة المراجع:

أولاً. الكتب:

- علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر، الإسكندرية، 1997.
- بشار محمود دودين، الإطار القانوني للعقد المبرم عبر شبكة الأنترنت وفقاً لقانون المعاملات الالكترونية وبالتأصيل مع النظرية العامة للعقد في القانون المدني، دار الثقافة للنشر والتوزيع، الأردن، 2006.
- نجوى أبو هيبة، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2002.
- محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2003.
- رشا مصطفى أبو الغيط، الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية 2003.
- محمد محمد شتّا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001.
- هلاي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، القاهرة، دار النهضة، 1999.
- كابرون، الحاسبات والاتصالات والإنترنت، ترجمة: سرور علي إبراهيم سرور، دار المريخ للنشر، الرياض، 2003.
- محمد أمين الزومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2004.

- أحمد خالد العجلوني، التعاقد عن طريق الإنترنت، الدار العلمية الدولية للنشر، عمان، 2002.

ثانياً. النصوص القانونية:

- القانون رقم 04-15 مؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66-156، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، الجريدة الرسمية عدد 71 مؤرخة في 10 نوفمبر 2004.
- القانون رقم: 09-04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية عدد 47، مؤرخة في 16 غشت 2009.
- الأمر رقم: 66-155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، المعدل والمتمم بمقتضى القانون رقم: 17-07، المؤرخ في 27 مارس 2017، المنشور بالجريدة الرسمية عدد 20، مؤرخة في 29 مارس 2017.