



المحاضرة السابعة

الطبيعة القانونية للجريمة السيرانية وأركانها

● عناصر المحاضرة:

المحور الأول: الطبيعة القانونية للجريمة السيرانية:

المحور الثاني: أركان الجريمة السيرانية:

الركن الأول: الركن المادي في الجريمة السيرانية:

أ. السلوك المادي في الجريمة السيرانية:

1. عناصر السلوك المادي:

2. صور الركن المادي:

ب. النتيجة الإجرامية في الجريمة السيرانية:

ج. علاقة السببية في الجريمة السيرانية:

الركن الثاني: الركن المعنوي في الجريمة السيرانية:

الركن الثالث: الركن الشرعي في الجريمة السيرانية :

الركن الرابع : (الركن المفترض) :

المحور الأول

الطبيعة القانونية للجريمة السيبرانية

انقسم الفقه إلى اتجاهين لتحديد الطبيعة القانونية للجريمة السيبرانية:

الأول: يرى أنه وفقا للقواعد العامة **أن الأشياء المادية وحدها هي التي تقبل الحيازة والاستحواذ،** وأن الشيء موضوع السرقة يجب أن يكون ماديا أي له كيان مادي ملموس حتي يمكن أنتقاله وحيازته عن طريق الإختلاس المكون للركن المادي في جريمة السرقة.

ولما كانت المعلومة لها طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ، إلا في ضوء حقوق الملكية الفكرية، لذلك تستبعد المعلومات ومجرد الأفكار من مجال السرقة، ما لم تكن مسجلة على اسطوانة أو شريط ، فإذا ما تم سرقة إحدى هاتين الدعامتين الخارجية، فلا تثار مشكلة قانونية في تكيف الواقعة على أنها سرقة مال معلوماتي ذو طبيعة مادية، وإنما المشكلة تثار عندما نكون أمام سرقة مال معلوماتي غير مادي.

والإتجاه الثاني يرى أن المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة الإستحواذ مستقلة عن دعامتها المادية ، على سند من القول أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال .

وهناك من يرى إنه يجب أن نفرق **بأن هناك مالا معلوماتيا مادي فقط** ولا يمكن أن يخرج عن هذه الطبيعة وهي الآت و أدوات الحاسب الآلي مثل وحدة العرض البصري ووحدة الإدخال ، وأن هناك من **المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية** وهي المال المادي كالشريط الممغنط أو الأسطوانة الممغنطة أو الذاكرة أو السلك التي تنتقل منها الإشارات من على بعد ، كما هو الحال في جرائم التجسس عن بعد ، إذن من المنطق القول إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة والبرامج لقيمتها المادية وهي ثمن الشريط أو ثمن الأسطوانة، وإنما يسرق ما هو مسجل عليهما من معلومات وبرامج .

ويرى أصحاب هذا الرأي أنه **يجب الإعتماد بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي البرامج والمعلومات،** وإنها لا يمكن أن تكون شيئا ماديا محسوسا، ولكن لهما كيان مادي قابل للإنتقال والاستحواذ عليه بتشغيل الجهاز ورؤيتهما على الشاشة مترجما إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي، وانتقال المعلومات يتم عن طريق انتقال نبضات ورموز تمثل شفرات يمكن حلها إلى معلومات معينة لها أصل صادرة عنه يمكن سرقتها، وبالتالي لها كيان مادي يمكن الاستحواذ عليه (البرامج والمعلومات)، واستطرد أصحاب هذا الإتجاه في القول بأنه **طالما أن**

موضوع الحيازة غير مادي فإن واقعة الحيازة تكون من نفس الطبيعة أي غير مادية، وبالتالي يمكن حيازة المعلومات بواسطة الإلتقاط الذهني عن طريق البصر .

يُستخلص من ذلك أن المعلومة بوصفها قيمة، فهي تندرج تحت القيم المستحدثة، وتصبح بذلك قيمة معلوماتية، وتندرج تحت الملكية التي تُعد لها قيمة قانونية، والاستيلاء عليها يستوجب العقاب، ويؤيد جانب من الفقه وبحق - الاتجاه الثاني القائل بأن المعلومات عبارة عن مجموعة من القيم المستحدثة استناداً إلى الحجج المنطقية التي ساقها أنصاره، فضلاً عن أن التطور الحديث يقتضي توفير حماية قانونية للمعلومات؛ دعماً للتطور العلمي والتقدم التكنولوجي، وقد أدى التطور الحديث للمعلوماتية إلى إضفاء قيمة اقتصادية للمعلومة، تتمثل في قيمتها التجارية المباشرة التي جعلتها سلعة تُباع وتشتري مثل بنوك المعلومات التي تتضمن تحليلاً للسوق، وكذا المعلومات التي يتم تبادلها بين الشركات التي تأخذ شكل خدمة مالية.

ويرى أحد الفقهاء أن: (كل عمل إنساني مفيد ينتج فائدة اقتصادية يجب أن يتم تكييفه بأنه مال ، فالمعلومات تُعد مالا لأنها ذات قيمة اقتصادية، حيث تمثل مصدرا حقيقياً لتحقيق عائد مادي لصاحبها) .

المحور الثاني

أركان الجريمة السيبرانية

لكي يمكن القول بوجود جريمة ما فإن المشرع يتطلب كأصل عام وجود ثلاثة أركان أساسية وهي الركن المادي والركن المعنوي وركن المشروعية، وبغير هذه الأركان لا يمكن القول بوجود جريمة، وهذا هو الحال بالنسبة للجريمة السيبرانية.

ويتمثل الركن المادي في النشاط أو السلوك الذي يرتكبه الجاني وله مظاهر خارجية، أما الركن المعنوي فيتمثل في اتجاه الإرادة والنية لارتكاب هذا السلوك الإجرامي ويكمن في نفس الجاني، أما الركن الثالث وهو الركن الشرعي فيقصد به وجود نص قانوني يحدد الجريمة والجزاء الجنائي في حالة ارتكابها، فلا جريمة ولا عقوبة إلا بنص .

ونظراً للطبيعة الخاصة للجريمة السيبرانية فإنه يمكن القول إن هناك ركن رابع مفترض وهو أن تتم الجريمة السيبرانية أثناء المعالجة الإلكترونية للبيانات، وسوف نتناول هذه الأركان بالتفصيل علي النحو التالي:

أولاً: الركن المادي في الجريمة السيبرانية:

يتطلب مبدأ تحديد الفعل غير المشروع وإعطائه صفة الجريمة، تحديد الركن المادي فيه، فلا جريمة دون ركن مادي الذي يتمثل في المسلك الذي يقوم به الجاني من أجل تحقيق غاية ما ويحدد له القانون الجزاء اللازم، وهو يتباين بتباين الجرائم المرتكبة من قبل الجاني شريطة أن يكون له مظهر خارجي ملموس وبناء على ذلك يقصد بالركن المادي:

كل سلوك إجرامي بارتكاب فعل جرمه القانون أو الامتناع عن فعل يأمر به القانون، فلا بد إذن من فعل أو امتناع يمكن إثباته إذ لا عبء بما يدور في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لآخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة السيبرانية تحت تكييف واحد فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة السيبرانية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماماً لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى الجرائم الواقعة عن طريق جهاز الحاسوب، وهذا لا يسبب إشكالاً إذا يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعاً من السلوك يتطلب التمييز بينها وبين سابقتها التقليدية وهذا ما يدعو للتدخل التشريعي.

السلوك المعلوماتي التقليدي:

إن الكثير من أنواع السلوك والتي يمكن معها الحصول على المعلومات بواسطة الحاسب الآلي ليس من الصعب خضوعها لنصوص قانون العقوبات كالتهديد والفعل الفاضح والسرقة والقذف والسب وغيرها إلا أن هناك أنماطاً من السلوك جاءت نتيجة وسائل متقدمة تكنولوجيا لا يمكن أن ينطق عليها أيًا من نصوص قانون العقوبات بل إن تطبيق النصوص القانونية عليها يثير استنكار الفقه لأن ذلك يعد خروجاً على مبدأ الشرعية الذي يتعين على القضاء أن يلتزم به هذا من جانب، ومن جانب آخر لا يمكن التعويل على التفسير الواسع للنصوص لأن من شأنه أن يوسع من دائرة التجريم وهذا الواقع يفرض تدخلاً تشريعياً نظراً لغياب النصوص التي تحكم الوقائع المعروضة وعدم انطباق النصوص التقليدية على هذه الوقائع.

مثلاً اختراق الشبكات وأجهزة الحاسب الآلي التابعة للغير سواء أكان شخصاً طبيعياً أم معنوياً بصفته يمثل تطفلاً غير مشروع أو خرق للسرية أو للحياة الخاصة للأفراد أو الاطلاع على المعلومات بصورة غير مشروعة ومن هذه الجرائم أيضاً بث الأفكار غير المشروعة عبر شبكات الإنترنت سواء أكانت دينية أو سياسية أو أخلاقية، وكذلك استعمال البريد الإلكتروني للاعتداء على حقوق الملكية الفكرية وكذلك تعطيل شبكات الإنترنت والدخول لأجهزة الحاسب الآلي وتعطيلها بطريق الفيروسات التي قد تسبب التدمير الكلي أو الجزئي للمعلومات أو تحريف المعطيات المخزنة على أجهزة الحاسب الآلي التابعة للدولة بشكل كامل أو جزئي.

الركن المادي لازم الوجود على الشكل والهيئة التي يتطلبها المشرع، سواء من حيث اجتماع عناصره الثلاثة من نشاط أو سلوك مادي ونتيجة إجرامية وعلاقة سببية، وأحياناً قد يكتفي المشرع بعنصر وحيد وهو النشاط أو السلوك المادي فقط، وفي هذه الحالة تتوافر الجريمة دون حاجة للبحث في النتيجة المتحققة أو علاقة السببية. وسوف نتناول بشيء من التفصيل السلوك والنتيجة وعلاقة السببية بينهما في خصوص الجرائم السيرانية على النحو التالي:

أ. السلوك المادي في الجريمة السيرانية:

إن السلوك المادي في الجريمة السيرانية له عناصر وصور تقتضي أن نتناولها علي نحو التالي:

1. عناصر السلوك المادي:

أن السلوك المادي في الجريمة السيرانية يتطلب وجود بيئة رقمية Digital environment تتمثل في وجود أمرين أساسيين:

الأمر الأول: وجود جهاز تقني كالكومبيوتر أو الموبايل أو الكومبيوتر اللوحي Tablet أو ما يُستحدث من أجهزة إلكترونية أخرى - والاتصال الإنترنت للجرائم المرتبطة بالإنترنت، وبدون هذه الأجهزة لا يمكن مباشرة السلوك الإجرامي.

الأمر الثاني: معرفة كيفية استخدام هذه التقنية، مثل كيفية تحميل جهاز الكومبيوتر ببرامج مخلة اختراق أو تجسس، أو القيام بإنشاء صفحات ويب Web Page تحمل في طياتها مواد وصور بالآداب العامة وتحميلها على الجهاز المضيف Hosting Server ، أو إعداد برامج فيروسات تمهيداً لبثها في أجهزة الغير.

وبالنسبة للأمر الأول : فإنه مما لا شك فيه أن حيازة هذه الأجهزة التقنية كالكومبيوتر والموبايل أو غيرها من الأجهزة الإلكترونية الحديثة مشروعة بحسب الأصل وهي تختلف عن حيازة سلاح ناري مرخص ، ففي حالة السلاح المرخص فإن الأصل هو عدم مشروعية حيازة السلاح، إلا أن المشرع لاعتبارات خاصة يقررها يسمح بمشروعية حمل السلاح بعد اتباع إجراءات خاصة، ومثل هذا الأمر لا ينطبق على الكومبيوتر أو الموبايل أو شبكة الإنترنت أو الخادم Server أو المضيف Host أو غير ذلك، فهذه كلها أجهزة مباح استخدامها أصلاً، لكونها أجهزة ذات قيمة علمية تشير إلى عوامل التطور التكنولوجي في المجتمع.

ولا شك أن حياة جهاز تقني كالحاسوب أو الموبايل أو الكمبيوتر اللوحي يجعل الجريمة السيبرانية ذات طابع موحد بالضرورة فهي تباشر من خلال هذه الأجهزة التقنية، ولعل هذا هو ما دفع المشرع في بعض القوانين المقارنة مثل القانون الأمريكي والقانون الفرنسي إلى استخدام عبارات في القانون مثل عبارة " جرائم ترتكب عبر الكمبيوتر " أو عبارة " إذا ارتكبت الجريمة باستخدام الكمبيوتر"، أو عبارة " باستخدام المعالجة الآلية للبيانات ".

- مدى اعتبار شراء كمبيوتر أو حياة برامج كمبيوتر من قبيل الأعمال التحضيرية للجريمة:

قد يثور التساؤل حول عما إذا كان شراء جهاز كمبيوتر أو تليفون محمول والاشتراك في الإنترنت أو شراء وحياة برامج تستخدم في القرصنة يعتبر من قبيل الأعمال التحضيرية أو شروع في ارتكاب الجريمة.

وفي الواقع أن معرفة الفارق بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم السيبرانية أمر صعب للغاية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء فشراء برامج اختراق ومعدات لفك الشفرات وكلمات المرور وحياة صور ودعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها.

فشراء جهاز كمبيوتر أمر مشروع وغير مجرم، بينما حياة أو شراء برامج اختراق أو فيروسات مثل برامج الفدية الضارة أو أدوات فك الشفرات وكلمات المرور، تمثل جريمة في حد ذاتها، إذا كانت بدون تصريح من الجهات المختصة وبنية ارتكاب جريمة أو استخدام في ارتكاب جريمة.

وبالنسبة للأمر الثاني: فإنه نظراً لخصوصية الجريمة السيبرانية من أن السلوك المادي في تلك الجريمة يبدأ من الكمبيوتر أو من الإنترنت، وذلك حسب الأحوال، وهذا يعني أن المجرم الذي يرتكب هذا النوع من الجرائم يجب أن يتمتع بالقدر الكافي من المعرفة التكنولوجية اللازمة في كيفية التعامل من الكمبيوتر والإنترنت لارتكاب الجريمة السيبرانية.

فمثلاً يقوم مرتكب الجريمة بتجهيز الحاسوب لكي يحقق له حدوث الجريمة فيقوم بتحميل الحاسوب ببرامج اختراق أو أن يقوم بإعداد هذه البرامج بنفسه وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها أشياء أو صور مخلة بالآداب العامة وتحميلها على الجهاز المضيف كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها.

ولذلك فإننا نتفق مع الرأي القائل بأنه في حالة اتهام شخص ما بارتكاب جريمة سيبرانية ودفع هذا الشخص أمام المحكمة المختصة بعدم وجود قدرات تقنية وفنية لديه لكونه يجهل التعامل بالكمبيوتر،

فهذا الدفع يعتبر من الدفع الموضوعية الجوهرية التي تلتزم محكمة الموضوع بالرد عليه تفصيلاً وعدم الالتفات عنه وإلا عاب حكمها القصور في التسبب والإخلال بحق الدفاع بما يسمح بقبول نقضه.

خلاصة ما تقدم: إن الركن المادي يبني على العلاقة التقنية بين مرتكب الجريمة السيبرانية وبين الأجهزة التقنية الحديثة مثل الكمبيوتر أو الموبايل أو غيرها من الأجهزة التكنولوجية، **ومثل هذه العلاقة يجب أن تؤخذ في الاعتبار** عند بناء الركن المادي في الجرائم السيبرانية.

2. صور السلوك المادي:

يتخذ السلوك المادي في الجرائم السيبرانية صورتين : الأولى وهي السلوك **الإيجابي** والذي يتطلب مجهود بدني يتمثل في العالم الخارجي من حركات عضوية يأتيها الجاني بهدف الاعتداء على المصلحة التي يحميها المشرع.

ومثال ذلك في الجريمة السيبرانية اختراق مواقع غير مصرح للجاني بالوصول إليها بهدف الاطلاع على ما بها من بيانات أو نسخها أو إتلافها، وكذلك نشر الفيروسات على أجهزة كمبيوتر الضحية بهدف تعطيل جهاز الكمبيوتر أو قطع خدمة الإنترنت عنه، أو سرقة الأموال الموجودة في بطاقة الائتمان أو غير ذلك من الجرائم المختلفة.

أما الصورة الثانية وهي **السلوك السلبي**، والذي يتمثل في الامتناع عن إتيان أمر أو فعل كان من الواجب إتيانه، إذ من الممكن ارتكاب جريمة بالامتناع عن عمل معين كان من الواجب مباشرته، ومثال ذلك في الجريمة السيبرانية امتناع الموظف المختص عن تفعيل برامج الحماية ضد الفيروسات.

ب. النتيجة الإجرامية في الجريمة السيبرانية:

النتيجة الإجرامية هي العنصر الثاني من عناصر الركن المادي للجريمة، وهي عبارة عن الضرر الذي نتج عن السلوك الإجرامي سواء كان فعلاً أم تركاً، وبمعني آخر هو يمثل **الاعتداء على المصلحة التي يحميها القانون**.

والضرر في الجريمة السيبرانية قد يكون **ضراً مادياً**، مثال ذلك إتلاف أو تدمير أو تحريف البيانات والمعلومات المخزنة على الكمبيوتر، أو قطع خدمة الاتصال بشبكة الإنترنت، مما قد يترتب خسائر مادية فادحة، أما **الضرر المعنوي** فيمكن حدوثه في حالة المساس بحرمات الحياة الخاصة من خلال التجسس الإلكتروني أو عن طريق اختراق الأجهزة والحصول على صور وبيانات شخصية.

وتثير مسألة النتيجة الإجرامية في جرائم السيرانية مشاكل عدة فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا باختراق جهاز خادم أحد البنوك في مصر وهذا الخادم موجود في السعودية، فكيف يمكن معرفة وقت حدوث الجريمة، هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم الذي يوجد في السعودية ويثور أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن، حيث إن هناك بعد دولي في هذا الباع.

كما قد تثار مشكلة أخرى في هذا الصدد من ناحية تحديد القانون واجب التطبيق على هذا الفعل، حيث أن هناك بعداً دولياً في هذا الشأن، باعتبار أن الجريمة في هذه الحالة عابرة للحدود.

فإذا كانت الجريمة السيرانية التي تحدث باستخدام الإنترنت تحدث في العالم الافتراضي أو الفضاء الإلكتروني (Cyber Space) وكذا علاقة السببية ، فإن النتيجة الإجرامية لها كيان منفصل، لكونها تحدث بشكل انقسامى ما بين حدوثها في العالم الحقيقي جزئياً أو كلياً، ولذلك نجد القضاء الأمريكي في قضية " توماس " أقر مبدأ قضائي مفاده اختصاص ولاية كاليفورنيا لمجرد تحقق النتيجة في هذه الولاية، وذلك بغض النظر عما إذا كانت قوانين ولاية كاليفورنيا تجرم مثل هذه الأفعال أم لا تجرمها .

ج. علاقة السببية في الجريمة السيرانية:

علاقة السببية هي العلاقة بين السلوك الإجرامي والنتيجة الإجرامية الضارة، بمعنى أن السلوك الإجرامي هو السبب في إحداث النتيجة الإجرامية، ولولا هذا السلوك ما كانت لتحدث النتيجة الإجرامية، وتبرز الأهمية القانونية لعلاقة السببية من حيث أنها من العناصر الأساسية المكونة للركن المادي للجريمة، فإذا أسندت النتيجة الإجرامية إلى السلوك قامت المسئولية الجنائية، أما إذا انقطعت رابطة السببية بينهما انتفت المسئولية الجنائية.

ومثال تحقق النتيجة الإجرامية في الجرائم السيرانية إتلاف البيانات والمعلومات بسبب نشر الفيروسات أو اختراق الأجهزة هو الأثر والنتيجة المترتبة على تلك الجرائم، وكذلك الدخول على موقع أو نظام معلوماتي أو بريد إلكتروني والاطلاع على ما به من رسائل إلكترونية ومعلومات يعتبر تعدي على الحق في الخصوصية وتعتبر علاقة السببية قائمة بمجرد ثبوت الضرر في مجرد الاطلاع.

الركن الثاني: الركن المعنوي في الجريمة السيرانية:

الركن المعنوي للجريمة هو الوجه الباطني أو النفسى للسلوك المادي الذي لا يتعدى انتساب السلوك الإجرامي إلى نفسية صاحبه، فهو الرابطة النفسية بين الفعل والفاعل، والركن المعنوي يأخذ أشكالاً عدة

من قصد جنائي عمدي وخطأ غير عمدي وتجاوز القصد وكذلك قد يتخذ صورة القصد الاحتمالي حسبما يتطلب المشرع في كل جريمة.

وأشكال الركن المعنوي في الجريمة التقليدية تنطبق كذلك على الجريمة السيبرانية، فالفاعل عندما يرتكب جريمة من هذه الجرائم يجب أن تتوافر العلاقة النفسية بين الفعل والفاعل في صورة العلم بكل عناصر السلوك المادي وإرادة متجهة نحو هذه العناصر.

ويلاحظ مما سبق أن بعض الأفعال في الجرائم السيبرانية قد تسبب أضرار مادية وخسائر مالية كبيرة لدى الجهة المجني عليها، ولذلك فإن انتقاء القصد الجنائي وركن العمد وأن كان يعفي الجاني من المساءلة الجنائية أو يخفف عنه العقوبة، إلا أن ذلك لا يمنع الجهة المتضررة من الرجوع عليه بالتعويض المدني على أساس قواعد المسؤولية المدنية إذا توافرت شروطها. نخلص من ذلك أن تحديد القصد الجنائي على قدر كبير من الأهمية في تحديد نوع الجريمة والجزاء المترتب عليها.

الركن الثالث: الركن الشرعي في الجريمة السيبرانية :

يقصد بركن الشرعية - أو ركن التجريم - أن القانون هو المصدر الحصري والوحيد لتحديد الأفعال والسلوكيات التي تعتبر جرائم والعقوبات المقررة لها، فالركن الشرعي هو السند القانوني التجريم الفعل وذلك تطبيقاً لمبدأ " لا جريمة ولا عقوبة إلا بنص " .

وقد نص على هذا المبدأ ضمن الإعلان العالمي لحقوق الإنسان الصادر عن منظمة الأمم المتحدة سنة ١٩٤٨ في المادة الحادية عشرة منه، وقد تضمنته أغلب الدساتير ضمن نصوصها، فإذا أغفل المشرع وضع نص يجرم واقعة ضاره بالمجتمع أو تهدد مصالحه القانونية فلا يمكن وصف هذه الواقعة بعدم المشروعية طالما لا يوجد نص سابق بتجريمها وبتحديد العقاب المترتب على ارتكابها، وإعمالاً لذلك فإنه من لا يجوز للقاضي الجنائي القياس أو التوسع في تفسير النص بغية شمول هذا الفعل بالتجريم والعقاب.

ولعل هذا المبدأ هو ما دفع غالبية مشرعو العالم إلى وضع قوانين مستقلة تبين ماهية الجرائم السيبرانية وتضع القواعد العقابية لمرتكبيها، باعتبار أن القوانين الجزائية التقليدية جاءت خلوا من بيان مفهوم هذه النوعية من الجرائم الحديثة التي رافقت الثورة التكنولوجية والتطور العلمي في مجال تكنولوجيا الاتصالات والمعلومات، ولذلك وضعت العديد من الدول قوانين أو تشريعات خاصة، أو العمل على جبهة قوانينها الداخلية لجهة تعديلها من أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم.

وبغرض مواجهة الجرائم السيبرانية نجد العديد من الدول العربية والأجنبية والمنظمات الدولية والقارية قد سارعت بإصدار التشريعات المجرمة لهذه الجرائم، نستعرض أهمها على النحو التالي:

1. بالنسبة للقوانين العربية:

القانون المصري رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، وقانون دولة الامارات العربية المتحدة رقم ٣٤ لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية، ونظام المملكة العربية السعودية رقم ١٧ لسنة ١٤٢٨هـ الموافق سنة ٢٠٠٧م بشأن مكافحة نظم الجرائم المعلوماتية، والقانون الأردني رقم ٢٧ لسنة ٢٠١٥ بشأن قانون الجرائم الالكترونية، وقانون مملكة البحرين رقم ٦٠ لسنة ٢٠١٤ بشأن جرائم تقنية المعلومات، والقانون الكويتي رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات، والقانون السوري رقم ١٧ لسنة ٢٠١٢، وقانون قطر رقم ١٤ لسنة ٢٠١٤ بشأن مكافحة الجرائم الإلكترونية، وقانون سلطنة عمان رقم ١٢ لسنة ٢٠٠١ بشأن قانون مكافحة جرائم تقنية المعلومات.

2. بالنسبة للقوانين الأجنبية:

وعلي سبيل المثال أصدرت السويد قانون البيانات سنة 1973 ، كما من المشرع الألماني قانون مكافحة التزوير المعلوماتي سنة ١٩٨٦، كما أصدر المشرع الإنجليزي قانون إساءة استخدام الكمبيوتر عام ١٩٩٠ والقانون الأمريكي رقم ١٢١٣ لسنة ١٩٨٦ الخاص بجرائم الكمبيوتر ، وقانون الهند بشأن تكنولوجيا المعلومات العام 2000.

كما قام المشرع الفرنسي بإصدار قانون " الجرائم في مواد المعلوماتية " عام ١٩٨٦، والذي تم تعديله بقانون " الاعتداءات علي نظم المعالجة الآلية للمعلومات عام ١٩٩٤ وقانون دولة صربيا الخاص بمكافحه جرائم التكنولوجيا الفائقة لسنة ٢٠١٠.

٣- بالنسبة للاتفاقيات الدولية:

وفيما يتعلق بالمعاهدات والاتفاقيات على الصعيد الدولي والإقليمي، فقد صدرت اتفاقية الجرائم الإلكترونية عن المجلس الأوروبي والمعروفة باسم اتفاقية بودابست لسنة ٢٠٠١، والقانون النموذجي لدول الكمنولث بشأن الكمبيوتر والجرائم المتصلة به لسنة ٢٠١٧ ومشروع اتفاقية الاتحاد الافريقي بشأن إنشاء اطار قانوني موثوق لأمن الفضاء الإلكتروني في أفريقيا لسنة 2011، كما صدر عن جامعة الدول العربية كل من قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها لسنة ٢٠٠٣،

والقانون العربي الإسترشادي للإثبات بالتقنيات الحديثة لسنة ٢٠٠٨، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٠.

الركن الرابع: (الركن المفترض):

وقوع الجريمة السيبرانية أثناء المعالجة الآلية يجعل لبيانات الجريمة السيبرانية تحتاج إلى ركن مفترض شأنها في ذلك شأن بعض الجرائم التقليدية، فإذا كان الركن المفترض في جريمة الرشوة وجود موظف عام، وفي جريمة الإجهاض وجود عنصر الحمل ومن دون توافر هذا العنصر لا يمكن إسناد تهمة الإجهاض للمشكو في حقه، فإن الركن المفترض في الجريمة السيبرانية هو وجود كمبيوتر وإنترنت إذا كانت الجريمة تتطلب الاتصال بالإنترنت ونظام معالجة إلكتروني للبيانات.

المراجع

• الكتب:

1. د. أحمد خليفة الملط ، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي / الأسكندرية، سنة 2005.
2. د. أحمد حسام طه تمام، الجرائم الناشئة عن إستخدام الحاسب الآلي، الحماية الجنائية للحاسب الآلي، دراسة مقارنة، دار النهضة العربية، 2000م.
3. د. محمد سامي الشوا : [ثورة المعلومات وإنعكاستها علي قانون العقوبات] - دار النهضة العربية - الطبعة الأولى - سنة 1994م.
4. د. محمد علي العريان : [الجرائم المعلوماتية] - الدار الجامعية الجديدة للنشر الإلكتروني - الطبعة الأولى - سنة 2004م.

• الرسائل:

5. د. حمام عبد اللطيف عبد الشافي حنفى معوض، الحماية الجنائية للبرامج والبيانات المعالجة إلكترونياً، دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، 2017م.
6. د. محمد خالد ممدوح إبراهيم، الجوانب الموضوعية لجرائم تقنية المعلومات، دراسة مقارنة، رسالة دكتوراة، كلية الحقوق، جامعة القاهرة، 2023م.
7. محمد صلاح محمد عبد المنعم، الجرائم الإلكترونية وتحدياتها - دراسة مقارنة - رسالة دكتوراة - كلية الحقوق- جامعة المنصورة.

8. د. محمد عبيد الكعبي، (الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الإنترنت) ، رسالة ماجستير، كلية الحقوق، جامعة القاهرة، سنة 2004م.
9. د. منى فتحي أحمد عبد الكريم : (الجريمة عبر الشبكة الدولية للمعلومات صورها ومشاكل إثباتها) – رسالة دكتوراة – كلية الحقوق – جامعة القاهرة – 2008 .
10. د. نائلة عادل محمد فريد قورة : [جرائم الحاسب الإقتصادية] – رسالة دكتوراة – جامعة القاهرة – 2003م.

• الدوريات والمؤتمرات:

11. د. مخلص إبراهيم الزغبى، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم السيبرانية، المجلة العربية للنشر العلمي، العدد سبعة وثلاثون، تاريخ الإصدار 2 – تشرين الثاني – 2021 م.
12. د. محمد علي سالم، د. حسون عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل للعلوم الإنسانية، المجلد 14، العدد 2، سنة 2007م.

تم بحمد الله
الإنهاء من شرح المحاضرة السابعة
مع تمنياتي بالتوفيق د. أسماء رويحي