



المحاضرة التاسعة

المواجهة الجنائية والتشريعية للجرائم السيبرانية

تمهيد وتقسيم:

إن الجريمة السيبرانية تطرح إشكالاً فيما يتعلق بالغاية من التجريم، والسؤال المطروح في هذا الصدد هل أن الحماية الجنائية تستهدف المحتوى وهو النظام المعلوماتي أم المحتوى وهو المعلومة المعالجة عن طريق النظام ؟

الراجح أن الغاية من التجريم هي حماية النظام المعلوماتي في حد ذاته ومنتجاته لأن هذا الأخير يتضمن إضافة إلى المعلومات والبرامج بكافة أنواعها وبالتالي المحتوى إضافة إلى أن حماية النظام المعلوماتي لا تطرح إشكالاً، بينما حماية المعلومة يثير إشكالات باعتبار أن المعلومة شئ معنوي يثير جدلاً فيما يتعلق بقابليتها للتملك من عدمها.

ولقد أدي ظهور الجرائم السيبرانية إلى خلق تحديات كثيرة في مواجهة النظام القانوني القائم في العديد من الدول وخاصة في مواجهة قانون العقوبات الأمر الذي دعا الفقه والقضاء إلى البحث فيما إذا كانت النصوص القائمة كافية لمواجهة هذه الجرائم بشتي أنواعها أم أن الأمر يستدعي استحداث قوانين أو نصوص خاصة قادرة على احتوائها ومراعاة طبيعتها وخصوصيتها؟

ولما كان للجرائم السيبرانية خصائص تتميز بها أدي ذلك إلى صعوبة التعامل مع النشاطات الإجرامية المستحدثة وتكييفها على أساس النصوص الجنائية التقليدية مع قد يشكك ذلك من مساس بمبدأ الشرعية الجنائية والتفسير الضيق للنص الجنائي، فكان لا بد من إتخاذ الخطوات التشريعية الضرورية لمكافحتها وذلك بمن نصوص قانونية لتجريم الأنشطة الإجرامية السيبرانية المستحدثة.

ولذلك سوف نقسم المحاضرة على محورين علي النحو التالي:

المحور الأول : المواجهة الجنائية للجرائم السيبرانية:

المحور الثاني: المواجهة التشريعية للجرائم السيبرانية:

• عناصر المحاضرة:

المحور الأول: المواجهة الجنائية للجرائم السيبرانية:

المحور الثاني: المواجهة التشريعية للجرائم السيبرانية:

أولاً: جرائم الإعتداء علي أنظمة المعلومات:

1. جريمة الدخول غير المشروع إلي نظام المعالجة الإلكترونية:
2. جريمة البقاء غير المشروع داخل النظام المعلوماتي:
3. جريمة تجاوز حدود الحق في الدخول إلي نظام المعالجة الإلكترونية :

ثانياً : الجرائم المرتكبة بواسطة أنظمة المعلومات:

1. جريمة الاعتراض غير المشروع :
2. جريمة الاعتداء على تصميم موقع :
3. جريمة الإعتداء علي بطاقات الدفع الإلكتروني:
4. جرائم الإعتداء علي البريد الإلكتروني أو المواقع أو الحسابات الخاصة:
5. جرائم إصطناع البريد والمواقع والحسابات الإلكترونية الزائفة:

ثالثاً : جرائم الإعتداء علي حرمة الحياة الخاصة (الخصوصية المعلوماتية) سوف يخصص لها بالشرح
مقرر مستقل الترم القادم بمشيئة الله تعالى.

المحور الأول

المواجهة الجنائية للجرائم السيبرانية

والتساؤل المطروح الآن هو هل قواعد القانون الجنائي تشكل مجموعة مستقلة تكفي نفسها بنفسها أم أن هذه القواعد لها طبيعة جزائية بحتة، فيعتمد وجودها علي وجود قواعد من طبيعة أخرى؟ أي هل يتمتع قانون العقوبات بالذاتية والاستقلال؟ وهل يتسم القانون الجنائي بذاتيه خاصه تفرد به بخصائص معينة؟

في البداية يقصد بالذاتية الاستقلال عن الغير، والواقع أن مشكلة ذاتية قانون العقوبات تخص استقلاله القاعدي. وانقسم علماء القانون في الإجابة علي هذا السؤال:

فذهب فريق من العلماء وهو الإتجاه المنكر إلي الذاتية ويذهب هذا الإتجاه إلي أن القوانين العقابية ليست طائفة خاصة من القوانين، بقدر ما هي جزاء علي مخالفة أحكام القوانين الأخرى، وبناء علي ذلك يعتبر قانون العقوبات قانوناً جزائياً وتابعا للقوانين الأخرى التي يزودها بعقوبات عندما تكون الجزاءات المنصوص عليها في هذه القوانين – أو عندما تبدو – غير كافية، أي أن القانون الجنائي هو حارس القوانين الأخرى.

بينما ذهب فريق آخر وهو الإتجاه المؤيد إلي الذاتية ويذهب أنصاره إلي استقلال قانون العقوبات في أفكاره وقواعده عن فروع القانون الأخرى، ولم يعد جزائياً بصفة مطلقة، فلم يقتصر غرضه علي العقاب فحسب إنما يمتد إلي الوقاية والإصلاح، كما أن هذا الاستقلال يجد تفسيره وتبريره في غايته وهي حماية المصالح الأساسية للمجتمع.

لا أحد ينكر الآن ذاتية القانون العقوبات، وبحيث تجعله قانوناً مستقلاً، له انظمته وفنياته التي تميزه عن غيره من فروع القوانين الأخرى، وتبدو هذه الذاتية واضحة سواء في قواعده الموضوعية أم قواعده الإجرائية.

فإذا كانت الدولة مصدراً **للحقوق الشخصية** فهي من ناحية أخرى تمارس السلطة التشريعية، ويمكنها - بمقتضى هذه السلطة - أن تعدل بالتضييق أو التوسع من نطاق هذه الحقوق، وعلى الأخص عندما ينجم عنها تعسف أو إضرار بالمصلحة العامة. ويتم ذلك بالقيام بوظيفة ذات طابع مزدوج الأولى وظيفة إنشائية، والثانية الوظيفة الجنائية.

فمن المعروف في العصر الحديث أن كل قانون له ذاتيته الخاصة ونطاقه، كما أن لكل قانون وسائله الخاصة التي تكفل احترامه، غير أن ذلك لا يمنع أن يستعير قانون ما بوسائل قانون آخر ليكفل هذا الاحترام. ومن هنا نجد أن القانون الجنائي يمثل القانون السوبر أو الأقوي بالنسبة لكل القوانين الأخرى؛ فهو الملجأ الأخير الذي تحتمي به سائر القوانين؛ عندما تفشل - أو تكاد - الوسائل التي رسمتها هذه القوانين لحماية ما تقرره من قواعد قانونية.

المحور الثاني

المواجهة التشريعية للجرائم السيبرانية

تمهيد وتقسيم:

تولد عن ثورة الاتصالات وتكنولوجيا المعلومات العديد من التطبيقات ، التي أثرت لدرجة كبيرة علي أوجه النشاط الاقتصادي والاجتماعي، كان من بينها التجارة الإلكترونية، والحكومة الإلكترونية، والتعليم من بعد، والعمل من بعد ... الخ.

وهكذا أصبح النظام الدولي للمعلومات يعتمد علي نمط جديد للتطور والسيطرة والسلطة علي المعرفة العلمية المتقدمة والاستخدام الأمثل للمعلومات المتدفقة بوتيرة سريعة. ويتصف هذا النمط بسيطرة المعلومات والمعرفة علي مختلف مجالات الحياة وبروز دور صناعة المعلومات باعتبارها الركيزة الأساسية في بناء الاقتصاديات الوطنية. فمطلوب من المشرع مواكبة التطورات والمستجدات لسد هذه الثغرات القانونية.

يصنف الفقهاء والدارسون جرائم السيبرانية ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، فبعضهم يقسمها إلى جرائم ترتكب على نظم المعلوماتية وأخرى ترتكب بواسطته، وهناك من الفقه يقسمها بحسب أسلوب ارتكاب الجريمة، ومنهم من ذهب لتقسيمها حسب الباعث من ارتكاب الجريمة، والجانب الأخير منهم من يرى تقسيمها بناء على محل الجريمة .

وفي هذه المحاضرة سنتعرف علي أهم صور الجرائم السيبرانية وذلك من خلال عرضها علي النحو التالي :

أولاً: جرائم الإعتداء علي أنظمة المعلومات:

1. جريمة الدخول غير المشروع إلي نظام المعالجة الإلكترونية:

2. جريمة البقاء غير المشروع داخل النظام المعلوماتي:

3. جريمة تجاوز حدود الحق في الدخول إلى نظام المعالجة الإلكترونية :

ثانيا : الجرائم المرتكبة بواسطة أنظمة المعلومات:

1. جريمة الاعتراض غير المشروع :
2. جريمة الاعتداء على تصميم موقع :
3. جريمة الإعتداء علي بطاقات الدفع الإلكتروني:
4. جرائم الإعتداء علي البريد الإلكتروني والمواقع أو الحسابات الخاصة:
5. جرائم إصطناع البريد والمواقع والحسابات الإلكترونية الزائفة:

ويمكن تقسيم صور الجرائم الواقعة علي الشبكات وأنظمة تقنية المعلومات إلي الأشكال التالية:

1. جريمة الدخول غير المشروع إلي نظام المعالجة الإلكترونية:

مع الإنتشار الكبير في استخدام أجهزة الكمبيوتر وشبكة الإنترنت ازدادت الجرائم التي ترتكب باستخدام هذه التقنية، ومن هذه الجرائم جريمة الدخول غير المشروع إلى أنظمة المعالجة الإلكترونية للبيانات.

وجريمة الدخول إلى أنظمة المعالجة الإلكترونية للبيانات هي جريمة تمس بأنظمة المعالجة أي المعلومات والبيانات الموجودة داخل جهاز الكمبيوتر ، وتكون هذه المعلومات غالباً محمية بشفرة أو برنامج كمبيوتر حيث أن المجرم يقوم بالدخول إليها وذلك دون الحصول على تصريح من صاحب النظام، ويمكن لهذه الجريمة أن تقوم بصفة مستقلة، أي قيام جريمة الدخول منفصلة عن جريمة البقاء، كما يمكن أيضا قيامها بصفة مرتبطة.

ويعتبر الدخول غير المشروع بمثابة الجريمة السيبرانية الرئيسية التي تنطوي على تهديد هذا وتعد على أمن النظم أي السرية والسلامة والإتاحة للنظم والبيانات والمعلومات، ولذلك تم تجريم الفعل في كافة التشريعات الخاصة بجرائم السيبرانية في مختلف بلدان العالم نظرا لما يتميز به الفعل الجرمي من طابع فريد بالنسبة لأجهزة الكمبيوتر وشبكة الإنترنت.

أ. ماهية جريمة الدخول غير المشروع :

لقد تعرضت الكثير من الأنظمة المعلوماتية الى الاختراق بواسطة أشخاص غير مصرح لهم بالدخول إليها، وقد أطلق على هؤلاء الذين يدخلون الى أنظمة الكمبيوتر بدون تصريح بالقراصنة أو الهكر Hacker. وأطلقت كلمة قراصنة Hackers أساسا على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدون الأنظمة المعلوماتية المختلفة ويحاولون اقتحامها وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة، ولكن نجاحهم في الاختراق يعتبر نجاحا لقدارتهم ومهاراتهم، إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان لفترض لا يجب أن يكونوا فيه.

وتتعدد المسميات في هذا الشأن فقد أستخدم كل من اتفاقية بودابست عام ٢٠٠١ في المادة الثانية، والتوجيه الأوروبي رقم ٤٠ لسنة ٢٠١٣ الصادر عن البرلمان الأوروبي، مصطلح الدخول غير المشروع، وتبعهما في ذلك المشرع المصري، بينما استخدمت غالبية التشريعات الوطنية المقارنة مصطلح الدخول غير المصرح به ومنها المشرع الأمريكي والإنجليزي والفرنسي.

ويقصد بمصطلح الدخول: ينصرف معني مصطلح " الدخول " في إطار المعلوماتية بصفة عامة ليشمل كافة الأفعال التي تسمح بالولوج إلى نظام المعالجة الإلكترونية للبيانات، ويقصد بذلك أن توجه هجمات إلى معلومات وبيانات الكمبيوتر أو خدماته أو برامجه، بقصد المساس بالسرية أو المساس بالسلامة والمحتوى ، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها.

ب. مفهوم جريمة الدخول غير المشروع في بعض التشريعات العربية:

- المشرع المصري:

إن المشرع المصري حين أراد تعريف فعل الدخول غير المشروع لم يستخدم هذا التعبير وإنما استخدم لفظ اختراق والذي عرفه بأنه " : الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة، إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية، وما في حكمها " .

وهجمات الاختراق penetration attacks هي تلك الهجمات التي يتم من خلالها الدخول غير المشروع إلى الأنظمة المعلوماتية وتخطي نظام التأمين الخاص بها، وفي حالات الاختراق الكامل يتمكن المهاجم من السيطرة الكاملة على جهاز الكمبيوتر ، وتغيير البيانات أو تبديلها، أو زرع برامج خبيثة داخل الجهاز.

وحسنا فعل المشرع المصري - ونحن نؤيده مع جانب من الفقهاء - حين أختار مصطلح الاختراق للدلالة على الدخول غير المشروع في نظام المعالجة الإلكترونية للبيانات، فهو يدل على تغلب الجاني على وسائل الحماية التقنية الموضوعة للنظام، كما يدل من ناحية أخرى على عدم مشروعية الدخول لنظام محمي.

- المشرع الإماراتي:

أما المشرع الإماراتي فقد أصدر القانون رقم ٣٤ لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية - والذي دخل حيز التنفيذ بتاريخ ٢٢/١/٢٠٢٢ وأستخدم لفظ الاختراق مثل المشرع المصري والذي عرفه في المادة الأولى من القانون بأنه الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها.

- المشرع السعودي:

أما المشرع السعودي فقد استخدم مصطلح الدخول غير المشروع، حيث عرف النظام السعودي في القانون رقم ١٧ لسنة ٢٠٠٧ الدخول غير المشروع بأنه " دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها".

- المشرع الكويتي:

إستخدم المشرع الكويتي مثل المشرع السعودي تعبير الدخول غير المشروع، كما عرف المشرع الكويتي في القانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الدخول غير المشروع بأنه النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح".

ويستفاد من نص المادة ١٤ من القانون المصري، والمادة ٢ من القانون الإماراتي، والمادة رقم ١/٧ من النظام السعودي والمادة ٢ من القانون الكويتي فيما يتعلق بجريمة الدخول غير المشروع المسائل الآتية:

1. أن الدخول غير المشروع قد يكون من قبل شخص، سواء كان شخصاً طبيعياً أو عن طريق جهاز روبوت آلي Robot مزود بخاصية الذكاء الاصطناعي أو أي تقنية أخرى.
2. إن الجريمة تقع سواء كان الدخول عمدي أو غير عمدي عن طريق الخطأ، وذلك بالنسبة للقانون المصري والإماراتي، أما بالنسبة للنظام السعودي فيلاحظ أنه قد اشترط في الدخول المعاقب عليه أن يتم بطريقة عمدية، أي اشترط توافر ركن العمد، ومفاد ذلك أن جريمة الدخول غير المشروع - طبقاً للنظام السعودي - لا تقع إذا تمكن شخص ما من الدخول بطريقة غير عمدية.
3. أن يكون الدخول غير المشروع، طبقاً للقانون المصري، يكون إلى أحد أمور ثلاثة هي: موقع إلكتروني، أو حساب خاص أو نظام معلوماتي، أما بالنسبة للقانون الإماراتي فقد حدد أمور أربعة هي: موقع الكتروني أو نظام معلومات الكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات وفيما يخص القانون السعودي فقد حدد أمور أربعة هي: حاسب آلي أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية.
- ويلاحظ مما سبق أن المشرع الإماراتي أضاف في النص عبارة " أو وسيلة تقنية معلومات " وذلك تحسباً لما قد يظهر في المستقبل من أجهزة أو شبكات إلكترونية أخرى قد تكون محل لهذه الجريمة.
4. أن تكون الأجهزة والأنظمة المعلوماتية والشبكات صالحة للدخول فيها والتعامل معها، فإن كان أي منهم به عطل يمنع الشخص من الدخول إليه، فإن الدخول في هذه الحالة يكون مستحيلاً.
5. لا يشترط تحقق أي ضرر لتوافر هذه الجريمة، فمجرد الدخول المجرد ولو لم ينتج عنه أي ضرر تتحقق جريمة الدخول إلى نظام المعالجة الإلكترونية.
- ويستفاد من ذلك أن الجريمة تقع بمجرد فعل الدخول إلى النظام بغض النظر عن أية نتيجة أخرى، فلا يشترط لقيامها التقاط المتدخل للمعلومات التي يحتويها النظام أو استعمال تلك المعلومات، بل إن الجريمة تقوم حتى ولو لم تكن لدى الجاني القدرة الفنية لتنفيذ العمليات على النظام.
6. لا يشترط لوقوع الجريمة أن يكون الوصول إلى نظام المعالجة الإلكترونية أو جهاز الكمبيوتر بالكامل، وبالتالي فإن الجريمة تقع ولو وصل الجاني إلى أي جزء من النظام، طالما كان الدخول غير مشروع.

(ج) مفهوم جريمة الدخول غير المشروع في القانون المقارن:

تتناول في هذا الصدد القانون الأمريكي والقانون الإنجليزي، وذلك على نحو تالي:

- القانون الإنجليزي:

بخصوص القانون الإنجليزي لسنة ١٩٩٠ في شأن إساءة استخدام الكمبيوتر، فقد نص على ثلاثة مستويات من جريمة الدخول غير المشروع، المستوى الأول : هو الوصول غير المصرح به إلى جهاز كمبيوتر ، والمستوى الثاني: هو الوصول إلى جهاز كمبيوتر دون إذن من أجل سرقة البيانات أو المشاركة في جريمة أخرى ، مثل استخدام هذه البيانات لارتكاب عمليات احتيال، والمستوى الثالث: يكون في حالة إذا قام الجاني بتعديل محتوى جهاز كمبيوتر ، أو قام بتوفير الأدوات حتى يتمكن الآخرون من القيام بذلك، كما في حالة توزيع برامج ضارة بقصد تدمير محتويات الكمبيوتر أو تغييرها، وقد تصل العقوبة إلى السجن مدي الحياة في حالة إلحاق ضرر بشخص ما أو تعريض الأمن القومي للخطر .

وفي عام ٢٠١٥ تم تعديل قانون إساءة استخدام الكمبيوتر لسنة ١٩٩٠ ، وذلك بإضافة جريمة جديدة إلي الجرائم الثلاثة السابقة وهي إذا نتج عن الفعل غير المشروع أضراراً جسيمة، ومن أمثلة ذلك الأضرار الجسيمة الناتجة عن الهجوم على أنظمة المعلومات الأساسية التي تتحكم في إمدادات الطاقة أو الاتصالات أو الأغذية أو توزيع الوقود، باعتبار أن هذا النوع من الهجوم قد يقع بشكل عام تحت عنوان الحرب الإلكترونية أو الإرهاب الإلكتروني cyber terrorism.

- القانون الأمريكي:

عدل القانون الأمريكي في شأن جرائم الاحتيال وإساءة استخدام الكمبيوتر، عدة مرات منذ عام ١٩٨٦، كان آخرها في عام ٢٠٠٨ ، ووسع السلوك الذي يحظره القانون، وزادت العقوبات. ويجرم قانون الاحتيال وإساءة استخدام الكمبيوتر بعد تعديله عام ٢٠٠٨ في المادة ١٠٣٠ في شكله الحالي تسعة أنواع من الأفعال الإجرامية وهي:

1. الحصول على معلومات متعلقة بالأمن القومي.
2. الوصول غير المصرح به إلى جهاز كمبيوتر والحصول على معلومات من سجل مالي لمؤسسة مالية أو مصدر بطاقة ائتمان، أو معلومات من أي إدارة أو وكالة بالولايات المتحدة، أو معلومات من أي كمبيوتر محمي ويؤثر على التجارة بين الولايات أو التجارة الخارجية حتى لو كان موجوداً خارج الولايات المتحدة.
3. استخدام الكمبيوتر لأغراض الاحتيال أو السرقة.

4. التعدي على جهاز كمبيوتر حكومي.
5. الإتلاف العمدي للبيانات عن طريق ارسال شفرة أو فيروس كمبيوتر.
6. الدخول غير المصرح به بطريقة عمدية وإتلاف بيانات لجهاز كمبيوتر محمي بطريقة الخطأ.
7. الدخول غير المصرح به بطريقة عمدية، والتسبب بإهمال في إحداث ضرر وخسارة لجهاز كمبيوتر محمي.
8. الاتجار في كلمات المرور الخاصة بأجهزة الكمبيوتر التي تستخدمها الولايات المتحدة.
9. الابتزاز عن طريق أجهزة الكمبيوتر.

2. جريمة البقاء غير المشروع داخل النظام المعلوماتي:

تعتبر جريمة البقاء من الجرائم المستحدثة، وهي جريمة ذات طابع دولي في الغالب، أي يمكن أن تقع في نطاق إقليم الدولة الواحدة أو خارجه، وهي من الجرائم التي تستهدف مرتكبيها للاعتداء على سرية الحياة الخاصة، سواء تمس شخص طبيعي أو معنوي.

ونتناول في هذا المجال الأساس القانوني لتجريم فعل البقاء غير المشروع وتعريف جريمة البقاء غير المشروع داخل النظام، وأختلافها عن جريمة الدخول غير المشروع، وذلك علي نحو ما يلي:

أ. الأساس القانوني لتجريم فعل البقاء غير المشروع:

الواقع أن مبدأ المشروعية في قانون العقوبات يتطلب تجريم البقاء غير المشروع داخل أنظمة المعالجة الآلية للمعطيات صراحة، سواء كانت جريمة الدخول غير المشروع تتم بمجرد الدخول إلى النظام، أو تشترط الوصول إلى ما يحتوي عليه من بيانات وبرامج لما يشكله فعل البقاء من تهديد لنظام المعلوماتية بمختلف محتوياته شأنه في ذلك شأن الدخول غير المصرح به.

ب. تعريف فعل البقاء غير المشروع :

يعرف البعض فعل البقاء غير المشروع داخل النظام بأنه " التواجد داخل نظام المعالجة الآلية للبيانات ضد إرادة من له الحق في السيطرة على هذا النظام " ..

ويُعد البقاء غير المشروع جريمة شكلية ذات سلوك مجرد أي أنها تقع وتكتمل بمجرد الانتهاء من فعل البقاء غير المشروع في النظام، دون أن يطلب المشرع أية نتيجة إجرامية، ويمكن أن يكون نشاط فعل البقاء سلبياً أو إيجابياً.

3. جريمة تجاوز حدود الحق في الدخول إلى نظام المعالجة الإلكترونية :

نتناول في هذا المبحث الأساس القانوني لتجريم تجاوز حدود الحق في الدخول ومفهوم هذه الجريمة على نحو ما يلي:

أ. الأساس القانوني لتجريم تجاوز حدود الحق في الدخول:

وتجريم فعل تجاوز حدود الحق في الدخول يهدف أساساً إلى حماية نظام المعالجة الإلكترونية بصورة مباشرة إلا أنه يحقق بصورة غير مباشرة حماية البيانات والمعلومات بحد ذاتها.

ب. تعريف جريمة تجاوز حدود الحق في الدخول:

ذهب جانب من الفقه بتعريف هذه الجريمة بأنها " هي الجريمة التي تقع من شخص حاصل على تصريح دخول ومخول له الحق في الدخول في موقع إلكتروني أو حساب خاص أو نظام معلوماتي، ولم يلتزم بالحدود المرسومة له، فتجاوز حدود هذا الحق، سواء من حيث الفترة الزمنية أو مستوي الدخول".

ويتحقق التجاوز أيضاً في الدخول حينما يرد الدخول على محل غير محله كأن يلج الجاني الحساب الخاص حال أنه مصرح له قانوناً بولوج الموقع فقط، أو يدخل في الموقع لضبط أدلة جريمة غير الجريمة المصرح له بالدخول من أجلها هو ما مسماه القانون تجاوز مستوي الدخول.

ويلزم أن يرد فعل التجاوز على محل بعينه وهو إما موقع أو حساب خاص أو نظام معلوماتي، ومن ثم لا تتحقق النتيجة إن أنصب التجاوز على بيانات ومعلومات الكترونية.

وهي جريمة عمدية، أي يتطلب توافر ركن العمد في ارتكابها، فلا تقع بالإهمال ولو كان جسيماً.

ونظراً لصعوبة معرفة متى يتم التجاوز في الصلاحية في الدخول فقد تطلبت بعض التشريعات الوطنية أن يكون هناك تعليمات واضحة وصريحة داخل المؤسسة تحدد بدقة من له الحق في الدخول إلى

النظام، وبالتالي لا يمكن تجريم فعل الدخول ما لم يكن هذا الدخول ممنوعاً صراحةً بموجب القواعد واللوائح الداخلية للمؤسسة، أو بموجب قرار مكتوب من الحائز الشرعي النظام أو من ينوب عنه .

وعلي سبيل المثال ، فإن مأمور الضبط القضائي إذا تجاوز حدود الأذن القضائي الصادر له وذلك في حالة إذا كان الأذن صادر له لمدة ٤٨ ساعة فقط وتجاوز هذه الفترة الزمنية، أو حالة إذا كان الأذن القضائي صادر بتفتيش البريد الإلكتروني للمتهم فقط دون باقي الملفات وقام بتفتيش ملفات أخرى، أو تم إلغاء الأذن القضائي من جهات التحقيق المختصة وأستمر مأمور الضبط القضائي في التفتيش والمعاينة رغم علمه بالإلغاء، فإنه يكون مرتكب جريمة تجاوز حدود الحق في الدخول.

وجدير بالذكر أن العقوبة الجنائية في التشريعات المقارنة لن تطل الفاعل الأصلي فقط، بل أن المدير الفعلي الشخص الاعتباري - إذا ثبت علمه بالجريمة أو سهل ارتكابها - يعاقب بذات عقوبة الفاعل الأصلي، وذلك بالإضافة إلى عقوبات تبعية تتمثل في العزل من الوظيفة.

ثانيا : الجرائم المرتكبة بواسطة الشبكات وأنظمة تقنية المعلومات:

ونتيجة التطور في تقنيات الكمبيوتر الحديثة وشبكات البيانات فإن الكثير من اموال البنوك أصبحت لا يتم الاحتفاظ بها في خزائن البنوك، بل أصبحت الأموال موجودة في الفضاء الإلكتروني، وكذلك فإن التطور المتزايد والمتسارع في تقنية المعلومات وبرامج الاتصال امتد إلى الحياة الخاصة، مما أدى إلى ظهور وبرزو الإساءة الإلكترونية المتمثلة في جرائم الإعتداء علي البريد الإلكتروني أوالمواقع أو الحسابات الخاصة وكذلك اصطناع بريد إلكتروني أو حساب خاص أو موقع ويب غير حقيقي، كما أن التطور في تقنية المعلومات أدى إلي ظهور جريمة الإعتراض غير المشروع، وجريمة الإعتداء علي تصميم موقع.

ومن هذا المنطلق سوف نقسم الجرائم المرتكبة بواسطة الشبكات وأنظمة تقنية المعلومات على النحو التالي:

1. جريمة الاعتراض غير المشروع :
2. جريمة الاعتداء على تصميم موقع :
3. جريمة الإعتداء علي بطاقات الإتمان:
4. جرائم الإعتداء علي البريد الإلكتروني أوالمواقع أو الحسابات الخاصة:
5. جرائم إصطناع البريد والمواقع والحسابات الإلكترونية الزائفة:

1. جريمة الاعتراض غير المشروع :

يقصد بهذه الجريمة كل فعل ينطوي على اعتراض يتم بدون وجه حق لأي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها. وقد جاء النص على هذه الجريمة في المادة السادسة عشر من القانون المصري ، كما تناولتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والسعودي ، هذا وقد حرص كل من المشرع الكويتي ، والإماراتي على إتباع ذات النهج بتجريم كل فعل ينطوي على اعتراض غير المشروع ومتعمد للبيانات والمعلومات المتداولة بوسائل التقنية المعلوماتية، أو الاعتراض غير المشروع والمتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات .

هذا وقد ضاعف كل من التشريع الكويتي ، والإماراتي من حد العقوبة في حالة إذا ما أفشى الشخص ما تحصل عليه من معلومات عن طريق هذا الاعتراض .

2. جريمة الاعتداء على تصميم موقع :

تعد هذه الجريمة من أحدث الجرائم التي رصدتها بعض التشريعات الحديثة، وقننت لها نصوصاً عقابية وتجرىميته مستقلة، وكان من بين هذه التشريعات التشريع المصري الذي تناول هذه الجريمة في المادة التاسعة عشر منه، وأسهب في ذكر الأفعال التي تعتبر انتهاكاً أو اعتداءً على تصميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق.

وكذلك كل من التشريعين الكويتي، والسعودي بتجريم هذه الأفعال والسلوكيات المتعلقة بالاعتداء على تصميم موقع سواء أكان مملوكاً ملكية خاصة لشخص طبيعي أو شركة أو مؤسسة أو منشأة.

3. جريمة الإعتداء علي بطاقات الدفع الإلكترونية:

في ظل التطور التكنولوجي الذي نعيشه اليوم والذي مس جميع القطاعات، ومنها قطاع البنوك الذي طور وسائل الدفع واعتمد الالكترونية منها كبديلة عن الوسائل التقليدية، حيث ظهرت بطاقة الدفع الإلكتروني من بين أهم تلك الوسائل الحديثة التي أصبحت تستخدم في شتى المعاملات المصرفية والتجارية، وقد عرفت هذه الآلية انتشاراً واسعاً نظراً لما تتميز به من سهولة حملها واستعمالها مما وفر الكثير من الجهد والوقت على المتعاملين بها.

فقد شهد العصر الحديث ثورة رقمية طالت جميع مناحي الحياة، ولم تكن المعاملات المالية في منأى عن ذلك حيث أفرزت هذه التغيرات نوعاً جديداً من التعاملات يعرف بالتعاملات الإلكترونية، إذ تمت مختلف عمليات السحب أو الوفاء بطريقة إلكترونية عن طريق بطاقة الدفع الإلكتروني، وبقدر ما سهلت هذه التطورات إجراء مختلف المعاملات المالية إلا أنها لم تمنع من ظهور اعتداءات عديدة جرت الاستخدام غير الشرعي لهذه البطاقة الإلكترونية.

إلا أن استعمال هذه البطاقات على الشبكة يثير مشاكل كبيرة على عكس الدفع العادي الذي يتم مباشرة بين البائع والمشتري في دقائق معدودة، فالتعامل بهذه البطاقات في ساحة الانترنت يكون عبر فضاء مفتوح لأن من يقوم بالدفع ببطاقته هو حقيقة الواقع يتعامل مع مئات الآلاف ممن يحاولون اصطيد بيانات هذه البطاقة وارقامها ليقوموا باستعمالها في مشترياتهم.

ومن هنا كان ظهور أحد أهم وأخطر صور الأنشطة الإجرامية المستحدثة التي تقع على البطاقات الائتمانية الا وهو السطو على الارقام والبيانات الخاصة بتلك البطاقات واستخدامها فيما بعد استخداما غير مشروع من قبل الغير.

وللحد من ذلك قام العلماء باختراع بطاقة ائتمان جديدة لا تعمل الا من خلال كلمة بصوت صاحبها، تعد أولى المحاولات من قبل العلماء بهدف مكافحة سرقة ارقام البطاقات الائتمانية خاصة تلك التي يتم تداولها عبر شبكة الانترنت، ولمزيد من الامان وحتى لا يعتمد المجرم إلى تسجيل تلك البصمة ليستخدمها فيما بعد فإنها تتغير بعد كل مرة تستخدم فيها البطاقة بتتابع معين لا يعلمه إلا الكمبيوتر.

جريمة الاعتداء على بطاقات الدفع الإلكتروني من الجرائم العمدية، التي تقوم على توافر القصد الجنائي، والقصد المطلوب هنا هو القصد العام بعنصرية العلم والارادة، فالجاني وهو يقوم بعملية السطو على بيانات البطاقات الائتمانية لابد وأن يكون عالماً بأن هذه البيانات مملوكة للغير ولا يجوز الاستيلاء عليها، أو علمه بأنه يستخدم تلك البيانات بصورة غير مشروعة من أجل الحصول على أموال الغير أو الخدمات التي تتيحها تلك البطاقة.

4. جرائم الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة:

أ. تعريف البريد الإلكتروني والمواقع والحسابات الخاصة:

✓ تعريف البريد الإلكتروني:

قد عرف القانون الفرنسي المتعلق بالثقة في الاقتصاد الرقمي الرسالة الإلكترونية على أنها: "كل رسالة سواء كانت نصية أو مرفق بها صور أو أصوات، ويتم إرسالها عبر شبكة اتصالات عامة، وتخزن عند أحد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها".

كما عرفه القانون الأمريكي لسنة ١٩٨٦ المتعلق بخصوصية الاتصالات الإلكترونية، على أنه: "وسيلة يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تليفونية عامة أو خاصة، وغالبًا ما يتم كتابة الرسالة على جهاز كمبيوتر ثم يتم إرسالها إلكترونياً إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه حيث يتم إرسالها عبر نظام خطوط تليفون إلى كمبيوتر المرسل إليه".

✓ تعريف الموقع:

ونلاحظ أنه جاء تعريف الموقع في المادة الأولى من القانون المصري رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات بأنه "مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة".

بينما عرف المشرع الإماراتي في القانون رقم ٣٤ لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية **الموقع الإلكتروني** بأنه "مكان أو مجال افتراضي على الشبكة المعلوماتية يعتمد على برامج ذكية تمكن مستخدميه من إتاحة أو تبادل أو نشر أي محتوى سواء كان نصي أو صوتي أو مرئي أو بيانات ويشمل مواقع وشبكات ومنصات التواصل الاجتماعي والصفحات والحسابات الشخصية والمدونات والخدمات الإلكترونية وما في حكمها".

✓ تعريف الحساب الخاص:

إن الحساب الخاص هو الذي يتم إنشائه في مواقع التواصل الاجتماعي ويحتوي على بيانات صاحبه وصورته ويستطيع التواصل من خلاله مع أصدقائه ونشر ما يريد من أخبار ومعلومات.

ج. المواجهة التشريعية لجرائم الإعتداء علي البريد والمواقع والحسابات الإلكترونية الخاصة:

نلاحظ في الآونة الأخيرة كثرة الانتهاكات والاعتداءات الموجهة لوسائل التواصل الاجتماعي بما فيها البريد الإلكتروني ، والمواقع والحسابات الخاصة الشخصية، وتعرضها لمحاولات التعدي عن طريق سرقتها أو اختراقها، وكشف سريتها، وسرقة محتواها، وقد يصل الأمر نتيجة هذه الانتهاكات إلى ابتزاز مالكيها وتهديدهم، مما دعي إلى ضرورة التدخل التشريعي لحماية هذه الوسائل التقنية ومواقع للتواصل الاجتماعي من مثل هذه الاعتداءات وفرض عقوبات رادعة.

نص المشرع المصري والإماراتي بالنص على تجريم أفعال التعدي على البريد الإلكتروني، والمواقع والحسابات الخاصة والشخصية.

5. جرائم اصطناع البريد والمواقع والحسابات الإلكترونية الزائفة:

يمكن أن تتخذ هجمات الاصطناع عدة أشكال، منها هجمات اصطناع البريد الإلكتروني الشائعة، وهجمات اصطناع مواقع الإنترنت، وهجمات انتحال هوية المتصل من خلال اصطناع صاب خاص الكتروني والذي غالبًا ما يُستخدم لارتكاب عمليات احتيال.

أنضم إلي رأي الفقه القائل بأن المشرع المصري قد أصرف وتزايد في النص على هذه الجريمة، حيث كان من المتعين إدراجها ضمن الجريمة الواردة في نص المادة ١٨ من القانون والمتعلقة بالاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة، بحيث يضاف إلي فعل الاعتداء المجرم فعل الاصطناع، دون الحاجة للنص عليها استقلالاً والوقوع في هذا التزايد والاسترسال غير المبرر.

ولم نري في تشريعات الدول المقارنة صدي لمثل هذه الحماية التشريعية، حيث لم يتناول أيًا من هذه التشريعات المقارنة النص على مثل هذه الأفعال التي تمثل جريمة من جرائم الاعتداء التقني، كما لم يرد بنصوصها أية إشارة تفيد الاتجاه نحو تجريم فعل الاصطناع التقني لمواقع أو حسابات خاصة أو بريد إلكتروني أسوة بما جاء بنصوص قانون التقنية المصري، ولكن ذلك لا يمنع أن نستعرض هذه الجرائم :

✓ جريمة إصطناع البريد:

وجدير بالذكر أن الجاني أو الشخص مصطنع البريد الإلكتروني يعرفه البعض بأنه " الشخص الذي يغير أو يصطنع عنوان بريد إلكتروني، ويتظاهر بأنه ينشأ رسالة من عنوان مصدر مختلف عن العنوان الذي لديه فعلاً".

اصطناع البريد الإلكتروني هو آلية يستخدمها الجاني لكي يبدو البريد الإلكتروني وكأنه مرسل من المستخدم الحقيقي ولكن في الواقع مرسل من الشخص المصطنع. وتتم طريقة اصطناع البريد الإلكتروني - في الغالب - عن طريق اصطناع عنوان بريد إلكتروني مشابه لعنوان البريد الإلكتروني الأصلي للضحية فيعتقد مستلم الرسالة أنها جاءت له من مصدرها الأصلي.

وعادة ما يُضمن الجاني البريد الإلكتروني المصطنع علامة تجارية مألوفة، مثل الشعار والألوان والخط، وغير ذلك من وسائل الخداع، حتى توحى للضحية أن البريد الإلكتروني المصطنع هو بريد الكتروني حقيقي وربما يكون مرسلاً من صديق أو زميل عمل أو فرد من العائلة أو شبكة أو جامعة أو مؤسسة مالية يتعامل معها، وعلى سبيل المثال، فإن موقع ياهو للبريد الإلكتروني هو Yahoo.com ، ويمكن للمجرم السبيري أن يقوم باصطناع موقع وهمي مشابه مثل Yahoo.net وبنفس شعار والوان الموقع الأصلي مما قد يؤدي إلى وقوع المستلم في الخداع والتعامل مع الموقع الوهمي على أساس أنه الموقع الأصلي.

ويمكن القيام بذلك، على سبيل المثال، عن طريق تغيير اسم الدومين Domain لأحد الجامعات أو البنوك فيقوم الشخص المصطنع باستبدالها بكلمة مشابهة وأرسالها إلى الشخص الضحية الذي يعتقد أنها قادمة من الجامعة التابع له أو البنك الذي يتعامل معه فيقوم بكتابة البيانات الشخصية الخاصة به من اسم أو رقم قومي أو رقم الحساب البنكي أو رقم بطاقة الائتمان، ثم يقوم بإرسال الرسالة إلى الجهة المعنية التي يعتقد أنه يتعامل معها، ولكن في حقيقة الأمر فإن الرسالة سوف تصل إلى الجاني وبها البيانات الشخصية للضحية والتي عن طريقها يستطيع الحصول على أموال الضحية أو يستخدمها للأضرار به أو لأغراض غير مشروعة، وفي هذه الحالة يكون الجاني قد اصطنع بريد إلكتروني ونسبه زوراً إلى شخص اعتباره هو الجامعة أو البنك.

ونؤيد جانب من الفقه أن اصطناع عنوان البريد الإلكتروني في الفضاء الإلكتروني " يعتبر جريمة تزوير، قياساً على أن التلاعب والتحريف في المراسلات والمستندات الورقية يشكل جريمة تزوير، بحسبان أن البريد الإلكتروني هو المكافئ الإلكتروني للبريد الورقي ".

✓ جريمة إصطناع مواقع الإنترنت:

والمقصود باصطناع موقع الويب : هو إنشاء نسخة طبق الأصل من موقع موثوق به بقصد تضليل زوار الموقع الوهمي، وغالباً ما يُستخدم في ذلك الشعارات والخطوط والألوان والوظائف المشروعة لجعل الموقع الوهمي يبدو واقعياً ومشابه للموقع الحقيقي.

أي أن اصطناع الموقع الإلكتروني هو عملية خداع تمويه اتصال أو هوية حيث تجعل المستخدم يبدو كأنه مرتبط بمصدر موثوق ومعتمد. وقد يستهدف قراصنة الإنترنت في الاصطناع العديد من العناصر التقنية لشبكة الانترنت.

اصطناع مواقع الويب - أو مواقع الإنترنت - هو شكل من أشكال الجرائم السيبرانية حيث يقوم الجاني - المصطنع - بإنشاء موقع ويب يشبه إلى حد كبير موقع الويب واسم النطاق لشعار أو علامة تجارية موثوق بها، ثم يقوم الجاني بخداع موظفي العلامة التجارية وعملائها وأطراف أخرى بوسائل متنوعة تدفعهم إلى التعامل مع الموقع المصطنع بغرض الكشف عن المعلومات والبيانات الشخصية الخاصة بهم .

✓ جريمة إصطناع الحساب الشخصي الإلكتروني:

وقد بات اصطناع الحسابات الخاصة على مواقع الإنترنت بصفة عامة، ومواقع التواصل الاجتماعي للأشخاص - سواء الطبيعية أو الاعتبارية - بصفة خاصة ظاهرة شائعة يلجأ إليها قراصنة الإنترنت لتحقيق مآرب غير مشروعة أهمها الابتزاز أو إيذاء أصحاب الحسابات ببث أمور تؤدي إلى ازدراء الناس لهم واحتقارهم، ولم تنجوا الحسابات أي كان نوعها من الاصطناع سواء انستغرام أو توتر أو فيس بوك.

وإزاء انتشار جريمة اصطناع الحسابات الخاصة على مواقع الإنترنت حرص المشرع في المصري على تجريم إنشاء حساب شخصي إلكتروني وهمي ومزور على الإنترنت ونسبته زورا إلى شخص طبيعي أو اعتباري.

ولعل أشهر الحسابات الخاصة هي صفحات التواصل الاجتماعي على شبكات التواصل الاجتماعي وهي مجموعة من المواقع على شبكة الانترنت ينشئها أفراد أو منظمات تتيح التواصل غير المباشر بين الأصدقاء.

إن جريمة اصطناع الحساب الخاص تعد من جرائم الخطر أو الضرر، إذ تعد من جرائم الخطر متى تحققت في صورة اصطناع الحساب ونسبه زوراً إليه شخص طبيعي أو اعتباري ولو لم يلحق صاحب الحساب أي ضرر، وبغض النظر عن الباعث على الاصطناع، إذ الجريمة تتحقق بمجرد فعل الاصطناع ولا ترتفع بباعث ونية الجاني من الاصطناع، ولكن إن أعقب سلوك الاصطناع استخدام الجاني الحساب الخاص المصطنع في أمر يسيئ إلى من نسب إليه أضحت من جرائم الحدث الضار.

والواقع والحقيقة يؤكدان إن كان للشخص الحق في إنشاء حساب خاص أو بريد إلكتروني عبر الإنترنت أو موقع يثبت من خلاله أفكاره ويعرض أخطاره ومنتجاته وآراءه، فإنه قد يتعرض هذا الحق للخطر إذا إنشأه غيره دون رضاه ونسبه زوراً إليه، وقد يتحول الخطر إلى ضرر مادي إستخدام المجرم السيبراني الحساب في أمور تسيء إلى الشخص المصطنع الحساب باسمه لاسيما أن كان شخصاً اعتبارياً عاماً.

المراجع

• الكتب:

1. د. أحمد حسام طه تمام، الجرائم الناشئة عن إستخدام الحاسب الآلي، (الحماية الجنائية للحاسب الآلي)، دراسة مقارنة، دار النهضة العربية، سنة 2000.
2. د. أحمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، دار النهضة العربية، 2005.
3. د. أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها، دراسة تحليلية تأصلية مقارنة، الطبعة الأولى، سنة 2017 .
4. د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دراسة متعمقة في القانون المعلوماتي، دار الفكر الجامعي، الطبعة الأولى، 2006.

• الرسائل:

5. د. أحمد طلعت عبد الحكيم عبد الحكيم عبد الرحمن، السياسة الجنائية في مواجهة جرائم تقنية المعلومات في ضوء القانون المصري رقم 175 لسنة 2018، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2022.
6. د. محمد خالد إبراهيم، الجوانب الموضوعية لجرائم تقنية المعلومات، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، سنة 2023.
7. د. محمد صلاح محمد، الجرائم الإلكترونية وتحدياتها، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة.

• المواقع الإلكترونية:

8. د. حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، دراسة تحليلية مقارنة، منشور علي موقع:

<https://jdl.journals.ekb.eg>

تم بحمد الله

الإنهاء من شرح المحاضرة التاسعة

مع تمنياتي بالتوفيق د. أسماء رويحي