جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

الدكتور

أشرف محمد نجيب السعيد الدرينى

دكتوراه في القانون الجنائي – جامعة المنصورة

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

ملخص:

تعد جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات أحد أبرز الجوانب السلبية التي أنتجتها الثورة المعلوماتية، والتي تشكل تهديد في مجال تقنيات المعلومات وقد تتمثل في جريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها، وفي جريمة الدخول غير المشروع، وفي جريمة تجاوز حدود الحق في الدخول، وكما في جريمة الاعتراض غير المشروع، وجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، وجريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة، وجريمة الاعتداء على تصميم موقع، وجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، وجريمة الاعتداء على سلامة الشبكة المعلوماتية، وجريمة استخدام البرامج والأجهزة والمعدات في ارتكاب جرائم تقنية المعلومات. ولذلك فقد تصدت لها العديد من التشريعات وهو ما سوف نتناوله في هذا البحث بتفصيل.

الكلمات المفتاحية:

تقنية المعلومات – البريد الإلكتروني – النظم المعلوماتي – الشبكة المعلوماتية

Summary:

The crimes of attacking the integrity of information networks, systems and technologies is one of the most prominent negative aspects produced by the information revolution, which constitutes a threat in the field of information technology and may be represented in the crime of unlawful use and fragmentation of communication services, the crime of illegal entry, and the crime of exceeding the limits of the right to entry, as in the crime of unlawful interception, the crime of assaulting the integrity of data, information and information systems, the crime of assaulting the information systems of the state, the crime of assaulting the integrity of the information network, and the crime of using software, hardware and equipment to commit information technology crime. Therefore, it has dealt with many legislations, which we will deal with in this search in detail.

Keywords:

Information Technology – E-Mail – Information Systems – Information Network.

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

مقدمة:

أصبح العالم عبارة عن قرية صغيرة بفضل التطور التكنولوجي والمعلوماتي، وقد تغني الأرقام عن كثير من الأقوال، وأحيانًا عن إيجاد مدخل عندما تتزاحم الأفكار فمنذُ ثلاث عقود مضت لم نكن نتصور أن الحاسب الآلي وملحقاته، يقتحم كافة المجالات بل وشتى مناحي الحياة دون استثناء، فالمصالح الحكومية الآن تعمل من خلال الحاسب الآلي، والشركات الخاصة والأفراد في حياتهم الخاصة، فأصبح التطور التقني في مجال تقنية المعلومات كالماء والهواء في حياة الإنسان الغني أو الفقير على حدًا سواء لا يستطيع أحد التخلف عن الرّكب مع التكنولوجيا، حتى يستطيع العيش مع المجتمع من حوله، فلم يعد هناك مجال للتعامل التقليدي مع المصالح أو الهيئة سواء العامة أو الخاصة الجميع يتسابق في التطور.

وهو ما حدا بالمشرع المصري التدخل بوضع قانون مكافحة تقنية المعلومات – على الرغم من التأخر الغير مبرر – بل أن المشرع المصري أخر من تدخل في هذا المجال بإصدار قانون رقم ١٧٥ في ٢٠١٨، ولكن لا يمكن انكار الجهد المبذول والمحمود من قبل المشرع المصري وصولا إلى قانون مكافحة جرائم تقنية المعلومات، وخروجه إلى النور والتطبيق والنفاذ، وما تضمنه من نصوص تجريميه وقيامه بالنص على معظم الجرائم التي قد تقع من مستخدمي تقنية المعلومات، فقد نص على الأحكام الموضوعية المتعلقة بالجرائم المعلوماتية، وعلى الجانب الآخر الأحكام الإجرائية، والتي تتعلق بالإجراءات الخاصة بالجرائم المعلوماتية، والتي كانت تمثل نقص تشريعي قبل صدور هذا القانون، لعدم استيعاب قانون الإجراءات وقانون العقوبات لبعض الجرائم المعلوماتية، والتي لا تندرج بنص عقابي أو إجرائي.

أهمية الموضوع:

أدى التطور السريع والمتلاحق لتقنية المعلومات إلى مضاعفة المخاطر والاعتداءات على الحريات الشخصية، وحرمة الحياة الخاصة، ونشر بعض العادات التي تمس المبادئ والقيم الأسرية، كما أنه يمكن من خلاله ارتكاب الجرائم التي تمس الأمن القومي، والتجسس عن بعد وسرقة المعلومات، والإرهاب والتحريض السياسي والتزوير والتزييف، مما يتطلب إعداد العدة لمواجهة سيل الجرائم الناتج من التقدم التقني، فكان من الضروري التدخل التشريعي لوقف تلك الجرائم فقررت بعض الدول عقد اتفاقيات تقرر تجريم بعض الأفعال التي تقع من خلال الوسائل الإلكترونية أو بواسطتها، كاتفاقية بودابست لعام ٢٠٠١، والقانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات، والذي تم إقراره من قبل وزراء العدل العرب في اجتماعهم المشترك في ٢٠٠٣/٥/٢٢، إلا أنه لم يُحدث تأثيرًا على أغلب التشريعات العربية.

وأما عن الوضع في القانون المصري، فقد أصدر المشرع العديد من القوانين، ومنها قانون الأحوال المدنية المصري رقم ١٤٣ لسنة ١٩٩٤، وقانون حماية الملكية الفكرية رقم ٨٢ لسنة ٢٠٠٢، وقانون تنظيم الاتصالات ١٠ لسنة ٢٠٠٣، وقانون التوقيع الإلكتروني ١٥ لسنة ٢٠٠٤، وقانون الطفل الصادر بالقانون رقم ١٢ لسنة ١٩٩٦ والمعدل في ٢٠٠٨، إلا أن هذه القوانين لم تفلح في مواجهة الجرائم المعلوماتية، فقرر المشرع التدخل بوضع القانون رقم ١٧٥ لسنة ٢٠١٨ لمكافحة جرائم تقنية المعلومات.

أسباب اختيار الموضوع:

مما لا مرية فيه أنه نتيجة للثورة المعلوماتية التي عرفها العالم برمته في الآونة الأخيرة تطور المجتمع في سائر المجالات، حيث أصبح التعامل مع التطور الناتج من ثورة المعلومات نتيجة حتمية ومقياس للتقدم، إلا أنه على الجانب الآخر من الثمار الإيجابية، توجد سلبيات وهي الجانب المظلم لتلك الثورة المعلوماتية لأن الإنسان يبقى حبيس نزواته ونواقصه وشهواته فأنتج الجرائم المعلوماتية، كظاهرة إجراميّة مُستجدَّة نِسبيًّا تقرع في جنباتها أجراس الخطر لتنبِّه مجتمعات العصر الرّاهن لحجم المخاطر، وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة.

والتي تختلف عن الجرائم التقليدية، في ركنها المادي سواء من حيث المكان أم الزمان، وما هو القانون واجب التطبيق على بعض الأفعال التي ترتكب في الخارج، كما أن السلوك الإجرامي في هذه الجرائم عبارة عن معلومات تتدفق عبرة الأجهزة الإلكترونية يصعب تحديده ماديًا أو الإمساك به، ومع تزايد هذه الجرائم أصبحت هناك حاجة مُلحة لمواجهة تلك الظاهرة الإجرامية، والتي تتمتع بطابع خاص.

منهجية البحث:

يتبع الباحث المنهج الوصفي التحليلي لتحليل النصوص القانونية، مع عرض وجهة نظر الباحث، كما يتبع المنهج المقارن، من خلال عقد مقارنات مع بعض التشريعات، كما يتبع المنهج التاريخي في مجال تقنية المعلومات.

نطاق البحث:

ويشمل نطاق البحث عن جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات على **نطاقين**: الأول **نطاق موضوعي**، ويتمثل في عرض الضمانات القانونية التي نص عليها المشرع في قانون مكافحة تقنية المعلومات، أما عن النطاق الثاني فهو **نطاق شخصي**، يتمثل في حماية مستخدم الخدمات المرتبطة بتقنية المعلومات، من كافة الجرائم التي قد ترتكب ضده.

مشكلة البحث:

ويجيب هذا البحث على مجموعة تساؤلات وهي:

- هل خرج المشرع المصري في هذا القانون على قواعد الاختصاص؟
- هل جريمة الدخول غير المشروع من الجرائم الشكلية أم من الجرائم التامة؟
- هل الركن المادي لجريمة التداخل يتكون من شقين؟
- هل جريمة الدخول غير المشروع يجوز فيها التصالح؟ وهل يختلف الأمر في حالة تجاوز حدود الحق في الدخول؟
- هل جريمة تجاوز حدود الحق في الدخول من الجرائم الشكلية؟
- هل يختلف الاعتراض عن الاختراق؟
- هل المشرع جرم استعمال أو حيازة أو أنتاج أجهزة لفك كلمة المرور تجنبًا للدخول الغير مصرح؟
- هل يختلف الأمر إذا تم الاعتداء على بريد إلكتروني خاص بآحاد الناس عن الاعتداء على بريد خاص بالأشخاص الاعتبارية الخاصة؟ وهل يختلف الأمر إذا كان الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة؟

خطة البحث:

- المبحث التمهيدي: ذاتية قانون مكافحة تقنية المعلومات

المطلب الأول: ماهية الجرائم المعلوماتية

المطلب الثاني: ذاتية قانون مكافحة تقنية المعلومات عن قانون العقوبات

- المبحث الأول: تجريم الدخول غير المشروع والانتفاع بدون وجه حق

المطلب الأول: تجريم الدخول غير المشروع وتجاوز حدود الحق والاعتراض

المطلب الثاني: الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها

- المبحث الثاني: جريمة الاعتداء على سلامة البيانات والبريد الإلكتروني وتصميم الموقع

المطلب الأول: الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية

المطلب الثاني: الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة وتصميم الموقع

- المبحث الثالث: جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة وسلامة الشبكة المعلوماتية واستخدام البرامج والأجهزة والمعدات في ارتكابها

المطلب الأول: الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

المطلب الثاني: الاعتداء على سلامة الشبكة المعلوماتية وتجريم استخدم البرامج والأجهزة في ارتكابها

الخاتمة (النتائج – التوصيات)

قائمة المراجع

المبحث التمهيدي

ذاتية قانون مكافحة تقنية المعلومات

تمهيد وتقسيم:

لقد أدى التطور التكنولوجي والمعلوماتي إلى ظهور جرائم جديدة على الساحة، والتي ترتكب بواسطة أنظمة وتقنيات المعلومات، فهي جرائم لها طابع خاص، سواء من حيث حجم الجريمة أو مقدار الخسائر الناجمة عنها، فالتطور التكنولوجي أنشأ بيئة خصبة للجريمة المعلوماتية بشكل كبير، ولم تقتصر على ارتكاب تلك الجرائم داخل الدولة الواحدة، بل ترتكب هذه الجرائم دون وجود حدود جغرافيا تحدها، ولذلك يتمتع قانون مكافحة تقنية المعلومات بذاتية خاصة عن قانون العقوبات، ليشمل تلك الجرائم المستحدثة وفقًا لهذا التطور التقني والمعلوماتي، وهو ما سوف نتناوله في السطور القادمة من توضيح ماهية الجرائم المعلوماتية لاختلافها عن الجرائم التقليدية، ثم نتبع ذلك بتناول ذاتية قانون مكافحة تقنية المعلومات من خلال مطلبين:

- المطلب الأول: ماهية الجرائم المعلوماتية
- المطلب الثاني: ذاتية قانون مكافحة تقنية المعلومات عن قانون العقوبات

المطلب الأول

ماهية الجرائم المعلوماتية

الجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين، انتقل بالجريمة من صورها التقليدية إلى أخرى إلكترونية

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

قد يصعب التعامل معها(١)، ففي بداية ظهور هذه الجرائم كانت هناك إشكالية تواجه المختصين في كيفية مكافحتها لأنها تتعلق بالبيانات والمعلومات، أي الكيان المنطقي للحاسب الآلي.

وهي بذلك تختلف عن الجريمة التقليدية وتكمن خطورة هذه الجرائم بداية في مرتكبيها الذين يتسمون بالذكاء لاختلاف الوسائل المستخدمة في الجرائم، فهم يمتلكون وسائل التدمير الناعمة كالفيروسات، ولا يستخدمون العنف مثل الجرائم التقليدية(٢)، ولذلك أطلق عليها البعض مسميات عديده منها الجرائم النظيفة، جريمة أصحاب الياقات البيضاء، الجرائم الناعمة، فالمجرم في هذه الجرائم يتسم ببعض الصفات الخاصة والتي تؤهله على ارتكاب الجريمة منها أنه خبيرًا في أنظمة المعالجة المعلوماتية الأمر الذي يصعب من إمكانية تعقبه، كما أن الأدلة في تلك الجرائم لها طبيعة خاصة من حيث إثباتها وتعقب مرتكبيها(٣)، كما أن الأدلة سهلة الإخفاء في فترة زمني قصيرة، كما أن ارتكاب تلك الجرائم لا يحتاج وجود المجرم المعلوماتي على مسرح الجريمة(٤).

---

١ - د. غنام محمد غنام، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، ١-٣ مايو ٢٠٠٣، المجلد الثاني، ص ٦٢٥ وما بعدها.

2- H. ALTERMAN et a. BLOCH – La Fraude Informatique, paris,Gaz, palais,(3) sep.1988,p531.

٣ - د. أشرف عبد القادر، الجرائم المعلوماتية، دار الثقافة عمان، ٢٠٠٨، ص ٨٦- د. أنور صدقي، المسئولية الجزائية عن الجرائم الاقتصادية، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٦، ص٣٩ – د. فتوح الشاذلي، د. عفيفي كامل عفيفي، جرائم الكمبيوتر، دراسة مقارنة، منشورات الحلبي، لبنان، ٢٠٠٣، ص٢٠.

4- MASCALA Corinne, "criminalité et contrat électronique", IN: Le contrat électronique, Travaux de L'association CAPITANT Henri, journées national, Paris,2000,p119.

ولذلك جرم العديد من المشرعين تلك الجرائم المستحدثة في مجال التجريم بناءً على تلك الثورة المعلوماتية التي انتجت العديد من الجرائم([1])، والتي تتطلب إصدار قوانين لتجريم الأفعال التي تعتبر جرائم وتبين الجزاء لها، وهو ما فعله المشرع المصري عندما اصدار قانون مكافحة تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ وأدخل صورًا من التجريم لم تكن موجودة من قبل، وهو ما فعله العديد من المشرعيّن على مستوى العالم، ومنها قانون البيانات السويدي عام ١٩٧٣، الذي عالج قضايا الدخول غير المشروع للبيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها، حيث يعتبر أول قانون للجرائم المعلوماتية.

وقانون مكافحة جرائم الحاسب الآلي والإنترنت الدنماركي ١٩٨٥، وقانون مكافحة التزوير والتزييف المعلوماتي البريطاني عام ١٩٨٦ والذي شمل تعريف أداة التزوير، وسائط التخزين الحاسوبية المتنوعة، أو أي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية أو الإلكترونية أو بأي طريقة أخرى، وقانون مكافحة التزوير المعلوماتي الألماني عام ١٩٨٦، والقانون الفرنسي الخاص بالتزوير المعلوماتي ١٩٨٨ والقانون الأمريكي الفيدرالي الصادر عام ١٩٨٤، والمشرع الكندي أولى الجريمة الإلكترونية أهمية أيضًا وجرم العديد من الصور لمكافحتها، والاتحاد الأوروبي الذي وضع اتفاقية حول جرائم الحاسب الآلي عام ٢٠٠٠.

ومفهوم الجريمة المعلوماتية لم يتفق الفقه الجنائي على إيراد تسمية موحدة له، فهناك من يطلق عليها تسمية الجرائم الإلكترونية، وهناك من يطلق عليها تسمية الجرائم

5-Marco Gercke, Regional and International Trends in Information Society Issues, in HIPCAR Working Group 1 (ST. Lucia: ITU, 2010), accessed through https://ccdcoe.org/publications/books/National Cyber Security Frame work Manual.pdf, on12.10.2020,p14

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

المعلوماتيةinformation crimes ، أو جرائم الغش المعلوماتي وصولًا إلى جرائم الإنترنت([1])

وينبغي توضيح أنّ المقصود في الغالب بالجرائم المعلوماتية هو جرائم الإنترنت حيث يتم استخدام الحاسب الآلي Computer-related crimes كأداة لتحقيق الكثير من الغايات غير القانونية مثل ارتكاب عمليات الاحتيال أو سرقة الملكية الفكرية أو انتهاك الخصوصية، وقد ازدادت معدلات حدوث الجرائم المعلوماتية لا سيما في السنوات الأخيرة([2])، وذلك للاعتماد على الحاسب الآلي وشبكة العنكبوتية في مؤسسات الحكومية ومؤسسات التجارة والصناعة والطب وغيرها([3])، ويتم معظم تلك الجرائم المعلوماتية من خلال أفراد أو مؤسسات غير حكومية أو منظمات إرهابية([4]).

وقد عرف الجرائم المعلوماتية مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها:" الجرائم التي تلعب فيها البيانات الحاسب الآلية والبرامج المعلوماتية دورًا رئيسيًا".([5]) إلا

6- DEBRAY Stéphane, Internet face aux substandes illicites: complice de la cybercriminalité ou outil de Prevention, DESS média électronique & Internet, Université de Paris, 2002 -2003,p8.

7- Manacorda (sc) la relegmenation du blanch cabitaux en droit interational du systems rev secri iminal zavril, 1999, p252.

8- David R. gohnson and David post, law Review, vol 48, May, 1996, p1379.

[4] - يشير القانون الفرنسي الخاص بالاتصالات السمعية والبصرية لسنة ١٩٨٢ إلى تعريف عام للمعلومة بأنها " رنينًا وصورًا للوثائق والبيانات أو الرسائل من أي نوع كان ".

[5] - وفي عام ٢٠٠٠ أقرّت وزارة العدل الأمريكية تصنيفًا لجرائم الحاسب الآلي، تضمن: السطو على بيانات الحاسب، والاتجار بكلمة السر، وحقوق الطبع (البرامج، الأفلام، التسجيل) وعمليات القرصنة، وسرقة الأسرار التجارية باستخدام الحاسب، وتزوير الماركات التجارية باستخدام الحاسب، وتزوير العملة باستخدام الحاسب، والصور الفاضحة واستغلال الأطفال، والاحتيال بواسطة شبكة الإنترنت، والإزعاج عن طريق شبكة الإنترنت. وصنف مكتب التحقيقات الفيدرالي الجرائم المعلوماتية في أبريل ٢٠٠٠ إلى سبع جرائم هي: اقتحامات شبكة الهواتف العامة أو الخاصة بواسطة الحاسب، واقتحامات شبكة الحاسب الرئيسية لأي جهة، واقتحامات السرية المؤرخة على بعض المواقع بالإنترنت أو الجهات، وانتهاكات سلامة الشبكة المعلوماتية، والتجسس الصناعي، وبرامج الحاسب المسروقة، والبرامج الأخرى عندما يكون الحاسب هو العامل الرئيسي في اقتراف هذه المخالفات.

أن المشرع الإنجليزي قد تبنى موقف مُغيّر في قانون إساءة استخدام الحاسب الآلي Computer Abuse عام ١٩٩٠ وهو عدم وضع تعريف محدد لجرائم تقنية المعلومات، وهو بذلك لم يحصر الأفعال التي تشكل الجرم في نطاق محدد، وضعًا في الاعتبار التطور التقني في المستقبل، وهو ما آخذ به المشرع المصري.

ولم يحدد تعريف للجرائم المعلوماتية في قانون مكافحة تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، تاركًا ذلك للفقه الجنائي(١)، وحتى لا يغلق الأمر على الوضع الحالي من الجرائم المعلوماتية، ولكن وضع في الاعتبار التقدم المذهل والدائم في تقنية المعلومات، وهو ما ذهب إليه المشرع الإمارات عند وضع القانون الاتحادي الصادر بالمرسوم بقانون ٥ لسنة ٢٠١٢ فلم يحدد تعريف الجرائم المعلومات بل ترك ذلك للفقه الجنائي، وقد تبنى المشرع الأردني هذا الفكر في عدم تحديد تعريف للجرائم المعلوماتية في التشريع رقم ٢٧ لسنة ٢٠١٥ بشأن قانون الجرائم الإلكترونية الأردني، كما أن المشرع البحريني هو الآخر لم يضع تعريف للجرائم المعلوماتية في القانون رقم ٦٠ لسنة ٢٠١٤، وكان هذا النهج محمود في عدم تحديد تعريف للجرائم المعلوماتية ويرجع ذلك إلى التطور التقنية الذي قد يؤدي إلى إفلات بعض المجرمين من العقاب(٢).

وعلى العكس من ذلك فقد تبنى العديد من المشرعيّن فكرة تحديد تعريف للجرائم المعلوماتية، ومنهما المشرع السوري في القانون رقم ١٧ لسنة ٢٠١٢ بأنها: " جريمة ترتكب باستخدام الاجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو

---

١ - راجع في ذلك: د. عبد الفتاح بيومي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار النهضة العربية، ٢٠٠٩، ص ٣٢- د. هدى قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، الطبعة الأولى، ١٩٩٢، ص٢٠.

٢- د. محمود رجب فتح الله، شرح قانون مكافحة جرائم تقنية المعلومات وفقا للقانون المصري الجديد، دار الجامعة الجديدة، مصر، الإسكندرية، الطبعة الأولى، ٢٠١٨، ص ٢٣.

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

الشبكة". كما عرفها المشرع السعودي في المرسوم الملكي رقم ١٧ لسنة ١٤٢٨ بأنها: " أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".

وقد تبنى نفس الاتجاه المشرع الكويتي، وعرف الجرائم المعلوماتية في القانون رقم ٦٣ لسنة ٢٠١٥ بأنها: " كل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون"، كما عرفت وزارة الداخلية الفرنسية الجرائم المعلوماتية بأنه:" الجرائم التي ترتكب بواسطة الإنترنت أو باستخدام أنظمة الكمبيوتر وانتهاكها للبرامج مثل الاحتيال وخيانة الأمانة"(١)، ويؤخذ على كل من عرف الجرائم المعلوماتية، أنه لم يضع في الاعتبار التقدم التقني والعلمي والتكنولوجي المتزايد بشكل يومي، مما قد يؤدي إلى إفلات الكثير من المجرمين تحت ذريعة عدم وجود نص عقابي للأفعال المستحدثة.

وهو ما تبنه المشرع المصري من عدم وضع تعريف حتى لا يكون مرتبط بمرحلة زمنية بعينها، فقد تستحدث التقنيات المعلوماتية بمرور الوقت. ويمكن تعرف الجرائم المعلوماتية بأنها: "هي كل سلوك إجرامي يحتاج إلى جهاز معلوماتي، متصل بوسيلة أو مجموعة وسائل، سلكيًا أو لا سلكيًا، ويشكل جريمة وفقًا لقانون مكافحة تقنية المعلومات".

---

13 - G. ROMAIN – la Delinqunace Informatique – Qu enest – on? (securite Informatique) guin 1998, n20,p2

المطلب الثاني

ذاتية قانون مكافحة تقنية المعلومات

لقد تمتع قانون مكافحة جرائم تقنية المعلومات بذاتية خاصة([1])، فقد تميز بالعديد من الأحكام والتي تعمل على الحد من الجرائم المعلوماتية، فحدد في المادة الأولى منه الكثير من التعريفات التي كانت تثير كثير من الجدل عند طرحها، وهذه إضافة تميز بها هذا القانون سالف الذكر فقانون العقوبات قلما يحدد تعريف، بل دائمًا ما ينقسم الفقه في تحدد تعريف بعض الجرائم، وهو ما فعله المشرع الإمارات في القانون الاتحاد المعدل في ٢٠١٢ حيث حدد الكثير من التعريفات الخاصة بتقنية المعلوماتية([2]).

كما حدد المشرع المصري في المادة الثانية التزامات وواجبات على مقدم الخدمة، وكانت أهمها حفظ وتخزين سجل النظام المعلوماتي أو أي وسيلة لتقنية المعلومات لمدة مائة وثمانين يومًا متصلة. وهو ما يساعد على إثبات الجرائم المعلوماتية من خلال الدليل الرقمي الموجود عند مقدم الخدمة، ويشتمل هذا الدليل على البيانات التي تمكن من التعرف على مستخدم الخدمة، وكافة البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه متى كان تحت السيطرة، وهو ما يمكن من خلاله تحديد المجرم.

كما أكد المشرع على مقدم الخدمة بالحفاظ على سرية البيانات التي تم حفظها أو تخزنيها، وهو ما نص على المشرع المصري في الدستور الحالي في المادة (٤٥) على

[1] - قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، والذي تم نشره في الجريدة الرسمية – العدد٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨

[2] - مرسوم بقانون ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

الحفاظ على سرية المراسلات الخاصة(١)، وهو أمر في غاية الخطورة، حيث أقر القانون عدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل البيانات الشخصية، أو أي بيانات أو معلومات متعلقة بالمواقع أو الحسابات الخاصة التي يدخل عليها هؤلاء المستخدمين(٢).

وعلى الرغم من أن المادة ٣١ من الدستور المصري الصادر عام ٢٠١٤ والمعدل في ٢٠١٩ نصت على" أمن الفضاء المعلوماتي جزءً أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون". إلا أنه حتى الآن لا يوجد بمصر تشريع عقابي متكامل خاص بالجرائم المعلوماتية.

كما نص أيضًا في المادة الثانية من قانون مكافحة تقنية المعلومات على عدم الإخلال بأحكام قانون حماية المستهلك، حيث الزم القانون مقدم الخدمة بمجموعة من الالتزامات للحفاظ على مستخدمي الخدمة، كما نص في ذات المادة على مراعاة حرمة الحياة الخاصة، وهي مصونة وفقًا للدستور المصري الحالي، وكما الزم مقدمو الخدمات والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومي ووفقًا لاحتياجاتها كافة الإمكانية الفنية التي تتيح لتلك الجهات ممارسة اختصاصاتها، كما الزم مقدم الخدمات والتابعون لهم بالحصول على بيانات المستخدمين، وحظر على غيرهم القيام بذلك. وهو ما يُحمد للمشرع المصري في تحديد الحقوق والواجبات على كل من مقدم الخدمة، ومستخدمي الخدمات في إطار تقنية المعلومات.

---

١ - الدستور الصادر في ٢٠١٤ والمعدل في ٢٠١٩ والذي تم نشره في الجريدة الرسمية في ٣ فبراير ٢٠١٤

٢ - أنظر قانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية، الجريدة الرسمية - العدد ٢٨ مكرر (هـ) - في ١٥ يوليه سنة ٢٠٢٠.

وإذ انتقلنا إلى المادة الثالثة، حيث خارج المشرع المصري على قواعد الاختصاص وفقًا لقانون العقوبات المصري([1])، على أن تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها في هذا القانون، متى كان هذا الفعل معاقبًا عليه في الدولة التي وقع فيها تحت أي وصف قانوني.

وهنا أيضًا نلاحظ أنه آخذ بمبدأ الشخصية في جانبه السلبي([2])، وهو عدم اشتراط جنسية في مرتكب الجرم المعلوماتي وقت ارتكاب الجريمة، وهو على خلاف الجانب الايجابي الذي يأخذ به المشرع المصري([3]) عند ارتكاب مصري في الخارج جريمة، ثم العودة إلى مصر بعد ارتكاب الجريمة ولا يعول على طريقة الرجوع سواء اختياري أم اجبارية، وتحقق شرط الازدواج في التجريم بين البلدين.

وهو ما لم يشترط في قانون مكافحة تقنية المعلومات، فالجاني غير مصري ولا يشترط أن يحمل الجنسية وقت ارتكاب الجرائم المعلوماتية حتى ينعقد الاختصاص للقضاء المصري في التطبيق من الناحية المكانية، فهنا قد توسع المشرع المصري في الاختصاص على خلاف قانون العقوبات الذي يأخذ بشكل أساسي بمبدأ الإقليمية – أن ترتكب الجريمة على الإقليم المصري من الحدود البرية أو البحرية أو الجوية، استثناءً

---

[1] - د. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠١٦، ص٦٩

[2] - راجع شرح مبدأ الشخصية/ د. عبد الرءوف مهدي، القواعد العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٢٠، ص٧٣ وما بعدها.

[3] - د. عبدالعظيم مرسي وزير، شرح قانون العقوبات، " القسم العام "، الجزء الأول، " النظرية العامة للجريمة"، دن، الطبعة التاسعة، ٢٠١١، ص٧٥.

مبدأ العينية وهو امتداد تطبيق قانون العقوبات على الجرائم الواقعة خارج الإقليم المصري([1])، وقد حددها المشرع على سبيل الحصر.

واستثناءً آخذ بمبدأ الشخصية الايجابية، وهي حالة ارتكاب المصري جريمة في الخارج ثم يعد إلى مصر، وقد اشترط القانون عدة شروط لكي ينطبق القانون المصري على الفعل، أولها كون الجاني وقت الجريمة يحمل الجنسية المصرية، والعودة إلى مصر، والازدواج في التجريم حتى لو اختلاف الوصف (جناية أو جنحة)، على خلاف قانون مكافحة تقنية المعلومات([2]) الذي لم يشترط وصف، إذًا قد تكون مخالفة وفقًا لقانون الدولة التي ارتكبت فيها الجريمة المعلوماتية، وفي مصر جنحة، هنا لا مانع من تطبيق القانون المصري، بخلاف قانون العقوبات الذي حدد الازدواج في التجريم بين الجنايات والجنح فقط([3])، وهو ما يعد توسع في الاختصاص في الجرائم المعلوماتية وفقًا لقانون مكافحة تقنية المعلومات المصري، وكما أفرد المشرع في تلك المادة عدة حالات على سبيل الحصر، وهي:

الحالة الأولى: " إذا ارتكبت الجريمة على متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي، وكانت مسجلة لدي جمهورية مصر العربية أو تحمل علمها ". فالمشرع استخدم لفظ أي وسيلة، ولم يستخدم لفظ محدد مثل سفينة بضائع أو ركاب أو طائرة حربية أو طائرة ركاب أو طائرة نفثة.

---

[1] - د. عبدالعظيم مرسي وزير، شرح قانون العقوبات، المرجع سابق، ص ١٠٠.

[2] - قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، والذي تم نشره في الجريدة الرسمية – العدد٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨

[3] - واستلزم المشرع الفرنسي شرطين: الأول، أن تكون الواقعة معاقبًا عليها في القانون الأجنبي (قانون محل التجريم) والقانون الفرنسي (قاعدة التجريم المزدوج)، الثاني: من اللازم أن يثبت ارتكاب الواقعة المعتبرة جناية أو جنحة بحكم نهائي يصدر من القضاء الأجنبي. نقض فرنسي ١٩٩٩/٢/١٠ بلتان رقم ١٥.

ونلاحظ عدم التحديد، واستخدام مصطلحات تحمل معنى التوسع في تطبيق القانون دون قصر الجرائم المعلوماتية على وسائل معينة، بل أي وسيلة يمكن ارتكاب الجريمة على متنها، كما عقد الاختصاص في حالة أن تكون الوسيلة مسجلة في مصر، إذًا أنه لم يكتفي بقانون العلم لعقد الاختصاص للقانون المصري في التطبيق بل توسع، في حالة التسجيل([1]) أو العلم، في الجرائم المعلوماتية التي ترتكب على متن أي وسيلة من وسائل النقل، وهو على خلاف قانون العقوبات، ووفقًا لقانون العلم([2])، كما ميز الوسائل الحربية أو تجارية([3]).

فإذا كانت السفينة حربية، وفقًا لقانون العقوبات خضعت الجريمة المرتكبة على ظهرها لقانون الدولة التي ترفع علمها نظرًا لأنها تمثل سيادة الدولة وتعد بمثابة قلعة عائمة([4]).

وقد نص المشرع الإمارات في المادة (١٧) من قانون العقوبات الاتحادي على أن:" تسري أحكام هذا القانون على الجرائم التي ترتكب على ظهر السفن الحربية التي تحمل علم الدولة أينما وجدت"، وهذا على خلاف إن كانت تجارية أو مدنية، فالقانون واجب التطبيق هو قانون العلم بحسب الأصل، إلا في حالات أوردها المشرع على سبيل الحصر في قانون العقوبات.

---

[1] - كما تنص المادة (١١/١١٣) من قانون العقوبات الفرنسي بأنه:" يكون قانون العقوبات الفرنسي قابلًا للتطبيق على الجنايات والجنح المرتكبة فوق أو ضد الطائرات غير المسجلة في فرنسا في الحالات الآتية: ١- إذا كان الجاني أو المجني عليه فرنسيًا، ٢- إذا هبطت الطائرة في فرنسا عقب وقوع الجناية أو الجنحة، ٣- إذا كانت الطائرة مؤجرة دون طاقم إلى شخص يتخذ المركز الرئيسي لأعماله أو محل إقامته الدائم في فرنسا"

[2] - راجع في ذلك/ د. عبد الرءوف مهدي، القواعد العامة لقانون العقوبات، مرجع سابق، ص ٦٤.

[3] - د. عبدالعظيم مرسي وزير، شرح قانون العقوبات، مرجع سابق، ص ٨١.

[4] - وقد تكلفت المادة (٣/١١٣) من قانون العقوبات الفرنسي الجديد بالنص على أنه: " يكون قانون العقوبات الفرنسي قابلًا للتطبيق على الجرائم المرتكبة فوق أو ضد سفن ترفع العلم الفرنسي في أي مكان وجدت، ويكون هذا القانون وحده دون غيره واجب التطبيق على الجرائم المرتكبة فوق أو ضد سفن تابعة للبحرية الفرنسية في أي مكان فيه".

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

وأما الوضع في الطائرات(١)، فإذا كانت حربية خضعت الجرائم التي ترتكب على متنها لقانون الدولة التي تحمل جنسيتها، أما الطائرات المدنية، فليس في شأنها عرف دولي مستقر غير ذلك الذي يجعل الاختصاص بالجرائم التي تقع على الطائرات لقانون الدولة المسجلة بها الطائرة(٢)، وهو ما لا يفعله قانون مكافحة تقنية المعلومات في تحديد أي وسيلة من الوسائل التي قد ترتكب عليها الجرائم المعلوماتية، وهو ما يعد توسع في الاختصاص وفقًا لقانون مكافحة تقنية المعلومات.

الحالة الثانية: " إذا كان المجني عليهم أو أحدهم مصريًا "، وهنا ينعقد الاختصاص بناءً على جنسية المجنى عليه وقت ارتكاب الجريمة، فإذا كان مصريًا واحدًا أو مجموعة من المصريين مجني عليهم، وهو مبدأ الشخصية في الشق السلبي له، قد عوّل على جنسية المجني عليه لانعقاد الاختصاص للقانون المصري، وهذه اضافة تخص الجرائم المعلوماتية في تقنية المعلومات على خلاف قانون العقوبات، في مبدأ الشخصية الايجابية حين اشترط أن يكون الجاني وقت ارتكاب الجريمة يحمل الجنسية المصرية، وليس المجني عليه.

الحالة الثالثة: " إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في جمهورية مصر العربية "، على الرغم إن هذه الإعمال تعد أعمال تحضرية إلا أن الجريمة قد وقعت في الخارج بالفعل، هنا ينعقد الاختصاص للقانون المصري، بناءً على تلك الأعمال التي تمت على الأراضي المصرية قبل تمام الجريمة في الخارج، بالإضافة إلى عدم اشتراط وصف تجريمي معين، وهذا على خلاف قانون العقوبات

---

١ - راجع / د. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، مرجع سابق، ص٧٢.

٢ - وهو ما نص عليه القانون الفرنسي الجديد في المادة (٤/١١٣) على أنه:" يكون القانون الفرنسي قابلًا للتطبيق على الجرائم التي ترتكب فوق أو ضد الطائرات المسجلة في فرنسا".

الذي لا يعاقب على الأعمال التحضيرية للجريمة، ولكن يعاقب على الاشتراك، وهو المعمول به في فرنسا أيضًا في قانون العقوبات(١).

الحالة الرابعة: " إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية ". وهنا المشرع يجعل الاختصاص للقانون المصري بناءً على وجود مصر ضمن الدول التي تمارس المنظمة أنشطة اجرامية فيها، وليس بناءً على وقوع جريمة على الإقليم المصري، أو جريمة في الخارج تمس أمن وسلامة مصر، ولكن عوّل المشرع في الجرائم المعلوماتية في هذه الحالة على وجود مصر داخل مجموعة الدول التي تمارس المنظمة الانشطة الاجرامية فيها، وهو أيضًا يختلف عن الوضع في قانون العقوبات الذي يشترط لقعد الاختصاص، أن يكون قد وقع بعض أفعال الاشتراك في مصر أو الجريمة في مصر(٢).

الحالة الخامسة: " إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها أو بأمنها أو بأي من مصالحها، في الداخل أو الخارج ". ويتبين من قراءة النص أن المشرع لم يعقد الاختصاص على المواطنين، بل عقد الاختصاص على المقيمين أيضًا في حالة وقوع ضرر عليهم، وسواء كان هذا الضرر في داخل مصر أو خارجها لأي منهما، بما يعني إذا وقع ضرر على أي من المواطنين أو المقيمين، عقد الاختصاص للقانون المصري دون تحديد سواء في الداخل أو الخارج، وهو ما يختلف عن قانون العقوبات في قواعد الاختصاص من حيث المكان، وهو مبدأ العالمية في شكل مقيد، وهو ما لم يأخذ به المشرع في قانون العقوبات(٣).

---

١ - حيث نصت المادة (٥/١١٣) من قانون العقوبات الفرنسي على أنه:" ينطبق على من يتهم بارتكابه فوق الأراضي الفرنسية لفعل الاشتراك في جناية أو جنحة وقعت بالخارج".

٢ - د. عبدالعظيم مرسي وزير، شرح قانون العقوبات، مرجع سابق، ص ٨٥ وما بعدها.

٣ - د. أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، مرجع سابق، ص ١٠١.

الحالة السادسة: "إذا وجُد مرتكب الجريمة في جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه ". بما يعني أن الجريمة لم تقع في مصر، ولم تلحق الضرر بأي من مواطنيها أو أحد المقيمين فيها، ولكن عوّل المشرع بعقد الاختصاص على تواجد مرتكب الجريمة في مصر بعد ارتكبها ولم يكن قد تم تسليمه إلى الدولة التي تختص بمحاكمته، وهو أيضًا مبدأ العالمية في شكل مقيد، فهو خروج على قواعد الاختصاص في قانون العقوبات، ويبرر هذا المبدأ رغبة الدولة في التعاون من أجل مكافحة نوع معين من الجرائم، وقد يقتصر تطبيقه على الجرائم التي تهم المجتمع الدولي، وهو موضوع الحديث في المادة التالية.

حيث نصت المادة الرابعة من قانون مكافحة تقنية المعلومات على أنه:" تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقًا لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات والمساعدة على التحقيق فيها، وتتبع مرتكبيها، على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن "، وهو تطبيق مبدأ العالمية بشكل مقيد، وهو ما لا يأخذ به المشرع في قانون العقوبات، وأن كانت تمليه اعتبارات التعاون بين الدول من أجل مكافحة الجريمة ومنع إفلات المجرمين من العقاب.

إلا أن تطبيقه يصطدم بالعديد من الصعوبات في الواقع العملي، ولذلك يقتصر تطبيق هذا المبدأ على نوع محدد من الجرائم، يوصف بأنه إجرام دولي تباشره عصابات من المجرمين ينتمون إلى دول متعددة ويمتد نشاطها الإجرامي إلى أكثر من دولة([1])، وقد

[1] - د. أحمد فتحي سرور، الوسيط في قانون العقوبات، الجزء الأول، القسم العام، دار النهضة العربية، ١٩٨١، ص ٢١٩.

أخذت بعض الدول بهذا المبدأ، فأجازت محاكمة المتهمين الذين يتواجدون على إقليم الدولة وفقًا للقانون المعمول به، ومنها المشرع الإمارات في قانون العقوبات الاتحادي لدولة الإمارات([1]) في المادة (٢١) وتنص على أنه: " يسري هذا القانون على كل من وجد في الدولة بعد أن ارتكب في الخارج بوصفه فاعلًا أو شريكًا في جريمة تخريب أو تعطيل وسائل الاتصال الدولية ". وهو ما لم يرد في قانون العقوبات المصري بالنص على الأخذ بمبدأ العالمية([2])، من ثم فإن هذا القانون لا يطبق على الأجانب الذين يرتكبون جرائم خارج إقليم الدولة. وهو المستجد في قانون مكافحة تقنية المعلومات في الجرائم المعلوماتية.

[1] - قانون اتحادي رقم ٣ لسنة ١٩٨٧، بشأن إصدار قانون العقوبات، الجريدة الرسمية العدد ١٨٢السنة السابعة عشرة بتاريخ ١٩٨٧/١٢/٢٠ وعمل به من تاريخ

[2] - د. عبد الرءوف مهدي، القواعد العامة لقانون العقوبات، مرجع سابق، ص ٧٧.

المبحث الأول

تجريم الدخول غير المشروع والانتفاع بدون وجه حق

تمهيد وتقسيم:

تعد جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، من الجرائم التي أنتجها التقدم التكنولوجي الحديث، فهي ليست جريمة تقليدي وفقًا للبنيان القانوني التقليدي، لكنها لها طبيعة خاصة، فقد ترتكب من خلال الدخول غير المشروع على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه، فهي إحدى جرائم الاعتداء على سلامة الشبكات، سواء كان الدخول عمدًا أو بخطأ غير عمدي وبقى في النظام بدون وجه حق، كما يعد اعتداء على سلامة شبكات وأنظمة المعلومات تجاوز حدود الحق في الدخول، وهي تختلف عن الصورة الأخيرة، هنا الدخول مشروع ولكن حدث اعتداء على سلامة الشبكات بتجاوز حدود هذا الحق من حيث الزمان أو مستوى الدخول. وكما نص المشرع على جريمة الاعتراض غير المشروع، وهي تختلف عن الاختراق؛ وهو ما سوف نوضحه بتفصيل.

كما ترتكب جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات من خلال الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها، فتلك الخدمات لها طبيعة خاصة من ثمة يصعب الإمساك بالسلوك الإجرامي المتمثل في تدفق المعلومات من خلال شبكات المعلومات، أو خدمة من خدمات قنوات البث المسموع أو المرئي مثل مباريات كرة القدم أو الأفلام. وسنوضح ذلك في السطور القادمة في مطلبين:

- المطلب الأول: تجريم الدخول غير المشروع وتجاوز حدود الحق في الدخول والاعتراض

- المطلب الثاني: الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها

المطلب الأول

تجريم الدخول غير المشروع وتجاوز حدود الحق في الدخول والاعتراض

أولًا: جريمة الدخول غير المشروع:

لم تكن التشريعات على مستوى العالم تعرف هذه الجريمة، ولم تكن هناك أي نصوص تشريعية تتعلق بالجرائم الإلكترونية أو الدخول غير المشروع، فكانت تطبق عليه النصوص التقليدية في قانون العقوبات، ولقد اختلفت التشريعات في تسمية هذه الجريمة والتي أسمها المشرع المصري بالدخول غير المشروع، وقد اتفق في هذه التسمية المشرع الكويتي([1])، والمشرع السعودي([2])، وهناك تشريعات أطلقت عليها الدخول دون تصريح كالمشرع الأردني([3])، والقانون الإنجليزي([4])، وأطلق عليها المشرع الأمريكي الدخول غير المصرح به، وهناك تشريعات أطلقت عليها جريمة الدخول إلى النظام المعلوماتي بطريق الغش كالمشرع الفرنسي([5])، كما أطلق عليها المشرع العماني الدخول بدون وجه حق([6]).

حيث تُعد جريمة الدخول عمدًا أو بدون على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه، أحد صور جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات

---

[1] - قانون رقم ٦٣ لسنة ٢٠١٥ في شأن مكافحة جرائم تقنية المعلومات الكويتي، الفصل الأول، تعريفات، المادة الأولى.
[2] - نظام مكافحة الجرائم المعلوماتية السعودي، المادة (٣).
[3] - قانون الجرائم الإلكترونية الأردني رقم ٢٧ لسنة ٢٠١٥، المادة (٣).
[4] - المادة (٢) من قانون إساءة استخدام الكمبيوتر الإنجليزي لسنة ١٩٩٠.
[5] - المادة (١/٣٢٣) من قانون العقوبات الفرنسي الجديد.
[6] - مرسوم سلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة تقنية المعلومات، المادة (٣).

المعلومات، وهي فرع على 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 كما جاء في مادة التعريفات بقانون مكافحة جرائم تقنية المعلومات.

كما اختلف الفقهاء في وصف الجريمة، فهناك جانب استخدم وصف الدخول إلى النظام المعلوماتي، وجانب آخر استخدم وصف الولوج، وكما ذهب جانب آخر إلى أطلق وصف انتهاك النظام المعلوماتي([1])، وقد اتفق جانب كبير على استخدم وصف الدخول غير المشروع وهو ما استخدمه المشرع المصري.

حيث يتمثل البنيان القانون لجريمة الدخول غير المشروع في شقين الأول: الركن المادي، وفي يجب أن يكون العدوان في هذه الجريمة على موقع أو حساب خاص أو نظام معلوماتي، ويختلف الأمر في بعض التشريعات التي تشترط تجرم الدخول غير المشروع عندم يكون النظام محمي، مثل المشرع الكويتي حين عرف الدخول غير المشروع:" 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"([2]). وبذلك يختلف عن موقف المشرع السعودي عندما عرف الدخول غير المشروع لم يشترط أن يكون الدخول على موقع أو حساب خاص أو نظام معلوماتي محمي من الدخول عليه، بقوله:" دخول شخص بطريقة متعمدة آلي حاسب آلي أو موقع إلكتروني أو نظام

[1] - د. عبد الله محمد الحضري، جريمة الدخول بدون وجه حق إلى المواقع الإلكترونية والنظم المعلوماتي العام في القانون القطري (دراسة تحليلية مقارنة)، رسالة دكتوراه، كلية القانون، جامعة قطر، ٢٠٢٠، ص٢.

[2] - قانون مكافحة تقنية المعلومات الكويتي، الفصل الأول، تعريفات، المادة الأولى.

معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"([1]). وهنا المشرع السعودي لم يشترط لقيام الجريمة أن يكون النظام محمي بحظر الدخول عليه مثل المشرع القطري والإماراتي والبحريني والسوداني والعماني والمصري.

وأما عن التشريعات الغربية لقد تباينت بشأن وجوب توفر الحماية، فمنها من اشترط الحماية للمواقع أو الأنظمة المعلوماتية حتى تكون تحت الحماية الجنائية، ومنها من شمل كافة المواقع والأنظمة المعلوماتية من دون اشتراط الحماية الأمنية، ومن هذه التشريعات قانون العقوبات السويدي، والسويسري، والألماني، والإيطالي، واشترط القانون الأمريكي الفدرالي أن يتم الدخول الغير مصرح به إلى حاسوب آلي محمي، ويقصد بالحماية أحد أجهزة المؤسسات المالية أو الحكومية الفدرالية، أو بالتجارة الأجنبية، وفي هذا الصدد لم يشترط المشرع الفرنسي أن يكون النظام المعلوماتي محمي بأحد صور الحماية، بل جعل التجريم يشمل المواقع المحمية والغير محمية([2])

وكما يشكل الركن المادي أيضًا الدخول عن طريق الخطأ غير العمدي إذا اقترن الدخول بالبقاء بالموقع الخاص أو النظام المحظور بدون وجه حق وقد عرف المشرع المصري الدخول غير المشروع من خلال المادة (١٤) من قانون مكافحة تقنية المعلومات بأنه:" كل من دخل عمدًا أو بخطأ غير عمدي وبقى بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه"، وقد فرق المشرع في هذه المادة بين الدخول عمدًا والدخول بخطأ غير عمدي وبقى في النظام بدون وجه حق.

---

[1] - نظام مكافحة جرائم المعلوماتية السعودي، المادة (١) فقرة (٧).

[2] - د. شيماء عبد الغني عطاالله، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق، ٢٠٠٥، ص ١١٨.

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

وأما الركن المعنوي يتطلب المشرع ركن خاص هو قصد العمد في الصورة الأولى، ولو لم يترتب على النشاط الإجرامي أية نتيجة إجرامية، فيكتفي بإثبات تعمد الجاني انتهاك حرمة الحساب الخاص أو النظام المحظور الدخول عليه، بينما لم يتطلب العمد حال الدخول بخطأ، ولكن تطلب إثبات أن الجاني ظل بالموقع الخاص أو المحظور عليه بعد أن دخل بخطأ، لذلك يكتفي بالقصد العام المتمثل في علم الجاني بالنص القانوني، وانصراف إرادته بالبقاء داخل الموقع أو النظام، ولو لم يترتب على ذلك البقاء أية نتيجة إجرامية([1]).

وأما عن العقوبة: يُعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من أتي الفعل المعاقب عليه بصورتيه، ويشدد المشرع العقاب في حالة إذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

كما نص المشرع في حالة العود: إذا ارتكبت الجريمة لحساب شخص معنوي فإن للمحكمة أن تقضي بإيقاف ترخيص مزاولة الشخص الاعتباري للنشاط مدة لا تزيد على سنة، ولها في حالة العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري.

---

[1] - د. خالد سليمان عبدالله الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، رسالة ماجستير، ٢٠١٩، ص٨١.

كما نص على المسئولية الجنائية للشخص الاعتباري، كل مسئول عن الإدارة الفعلية لأي شخص اعتباري، إذا تعرض الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي المخصص للكيان الذي يديره، لأي جريمة من الجرائم المنصوص عليها في هذا القانون، ولم يبلغ بذلك الجهات المختصة وقت علمه بالجريمة، وهو ما نص على المشرع في المادة (٣٥)، وفي الأحوال التي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون باسم ولحساب الشخص الاعتباري، يعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالحريمة أو سهل ارتكابها تحقيقًا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي، وهو ما نص عليه المشرع في المادة (٣٦) من القانون سالف الذكر.

كما يثور في هذا الصدد تساؤل هام هل جريمة الدخول غير المشروع جريمة شكلية أم يلزم لكي تتحقق أن تكون جريمة تامة؟ فالجريمة الشكلية هي التي تحدث بمجرد ارتكاب السلوك الإجرامي دون انتظار نتيجة، أما الجريمة التامة هي التي لا يكفى لقيامها السلوك الإجرامي بمفرده بل تحقق نتيجة معينة. فقد اعتبرت بعض التشريعات هذه الجريمة جريمة شكلية أي يكفى لقيامها مجرد الدخول إلى النظام المعلوماتي([1])

ويري أنصار هذا المذهب ضرورة تجريم الدخول المجرد حيث وأن لم توجب لدى الفاعل النية على ارتكاب أي جريمة لاحقة على الدخول أثناء دخوله غير المشروع، ألا أنه قد تتولد لديه هذه النية فيما بعد، وهو المعمول به في فرنسا، وفقًا لقانون العقوبات الفرنسي الجديد المادة (١/٣٢٣)، حيث عاقب على الدخول إلى النظام المعلوماتي بغير وجه حق بعقوبة السجن لمدة سنتين وغرامة مائتي فرنك فرنسي، فقد فرق بين حالتين: الأولى،

[1] - د. مدحت إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٥، ص ٧٦ وما بعدها.

وهو الدخول إلى النظام المعلوماتي بطريق الغش أما الثانية، هي الدخول والبقاء في النظام المعلوماتي([1]).

بينما اتجهت تشريعات أخرى إلى اعتبارها ذات نتيجة أي أنها لا تقع بمجرد الدخول بل بحدوث نتيجة، ويرى أنصار هذا المذهب عدم ضرورة تجريم الدخول المجرد في حال عدم وجود نية لدى الفاعل لارتكاب جريمة، فهو لا يعدو أن يكون استعراض للأفكار والقدرات لدى الفاعل على اختراق النظام أو مجرد فضول لديه، وهو ما آخذ به المشرع السعودي([2]).

وقد ذهب فرق ثالث إلى نظام مختلط بين هذا وذاك حيث اعتبر الجريمة شكلية، ولكن إذا ترتب على هذا الدخول ضرر غلظ العقوبة وهو ما آخذ به المشرع المصري في المادة (١٤) في الدخول غير المشروع، والباحث يؤيد هذا الاتجاه للمشرع المصري، بالآخذ بالمذهب المختلط والعقاب بصورة تدريجية، فيعاقب على الدخول العمدي أو دخل بخطأ غير عمدي وبقى في النظام، ثم يُغلظ العقاب إذا ترتب على ذلك إتلاف أو محو أو تغيير أو إعادة نشر البيانات.

كما يثور تساؤل آخر هل الركن المادي لجريمة التداخل يتشكل فقط بالدخول غير المشروع؟ نجد أن الركن المادي لجريمة التداخل يتكون من شقين: فهو من الجرائم المركبة التي يتكون ركنها المادي من أكثر من فعل، فجريمة التداخل في شقها المادي تتكون من الدخول بدون وجه حق، وهو ما نص عليه المشرع في المادة (١٤) من قانون مكافحة تقنية المعلومات، أما الشق الثاني فهو البقاء بدون وجه حق، فقد جرمت

---

49 - Nouveau Code pénal français, (323/1).

[2] - د. أسامة العبيدي، جريمة الدخول غير المشروع إلى النظام المعلوماتي (دراسة قانونية في ضوء القوانين المقارنة)، مجلة المعلومات، العدد١٤، جمعية المكتبات والمعلومات السعودية، ٢٠١٢، ص٣٠

المادة (١٥) من القانون سالف البيان فعل البقاء بدون وجه حق، وهو ما سنوضحه في السطور القادمة.

كما يثور تساؤل أيضًا وهو هل الشروع في هذه الجريمة معاقب عليه؟ وهل يجوز التصالح فيها؟ لقد نص المشرع في المادة (٤٠) من قانون مكافحة تقنية المعلومات على العقاب على الشروع في جميع الجنح الواردة في هذا القانون، وجريمة الدخول غير المشروع وفقًا لنوع العقاب هي جنحة، إذًا متصور الشروع فيها. وأما عن الشق الثاني من السؤال الخاص بالتصالح في هذه الجريمة فقد اجاز المشرع المصري التصالح في المادة (٤٢) من القانون سالف الذكر في جنح محددة على سبيل الحصر ومنها الدخول غير المشروع، ولكن وفقًا لهذه المادة لا ينتج التصالح أثره إلا باعتماده من الجهاز لأنها من ضمن الجنح المحددة التي لا تنتج أثرها في التصالح إلا بعد موافقة الجهاز القومي لتنظيم الاتصالات.

ثانيًا: جريمة تجاوز حدود الحق في الدخول

جريمة تجاوز حدود الحق في الدخول على موقع أو حساب خاص أو نظام معلوماتي، أحد صور جريمة الاعتداء على سلامة الشبكات وأنظمة وتقنيات المعلومات، والموقع كما عرفّه القانون مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة.

والشبكة هي مجموعة من الأجهزة أو نظم المعلومات مرتبطة معًا، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها. والحساب الخاص: هو مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له الحق دون غيره الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي. والنظام المعلوماتي: هو

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

مجموعة برامج وادوات معدة لغرض إدارة ومعالجة البيانات والمعلومات أو تقديم خدمة معلوماتية.

فقد نصت المادة (١٥) عن جريمة تجاوز حدود الحق في الدخول، " كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدمًا حقًا مخولًا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول"، فالأصل وفقًا لهذه المادة أن الدخول مشروع ومرخص له بدخول، ولكن قد حدث تجاوز في حدود الزمان، أي البقاء فترة أطول من المسموح بها، أو الدخول إلى مستوى آخر غير المسموح له الدخول عليه. وبالمثال يتضح المقال، أحد الموظفين له جهاز كمبيوتر يقوم بدخول عليه في مواعيد العمل، حيث يتيح له موقعه الوظيفي الدخول على منظومة وشبكة المعلومات في حدود صلاحياته الوظيفية فيتجاوز ذلك الحق، ويقوم بالاطلاع على أمور ليست من صميم عمله وصلاحياته على الشبكة. هنا الفعل يشكل جريمة وفقًا لقانون مكافحة تقنية المعلومات، جريمة تجاوز حدود الحق في الدخول.

حيث يتمثل البنيان القانوني لهذه الجريمة من شقين: الأول وهو الركن المادي المتمثل في تجاوز حدود الدخل من حيث الزمان أو المستوى المسموح به، فكما وضحنا من قبل أن الدخول مصرح به لكن السلوك الإجرامي يتمثل في تجاوز حدود الدخول المسموح به، والذي يترتب عليه قيام الركن المادي، وأما عن الشق الثاني الركن المعنوي: لا تتطلب هذه الجريمة ركن خاص فمجرد وقوع الفعل المادي يوجب العقوبة، ولو كانت على سبيل الخطأ، طالما تجاوز الحد المصرح له من قبل صاحب القرار.

وهنا يثور تساؤل هل جريمة تجاوز حدود الحق في الدخول جريمة شكلية أم جريمة تامة؟ لقد أكتفى المشرع المصري في المادة (١٥) سالفة البيان بأن الجريمة تتشكل بناءً على تجاوز حدود الحق في الدخول، دون حدوث نتيجة إجرامي بشكل معين، فالمشرع

جعل من السلوك الإجرامي سبب لقيام الجريمة، دون الوضع في الاعتبار بالقصد الجنائي في جانب الجاني إذًا جريمة تجاوز حدود الحق في الدخول جريمة شكلية وليست جريمة تامة.

كما عاقب المشرع على جريمة تجاوز حدود الحق في الدخول بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو إحدى هاتين العقوبتين. وأما عن جواز التصالح في هذه الجريمة فقد اجاز المشرع التصالح فيها وفقًا للمادة (٤٢)، ولكن التصالح ينتج أثره بمجرد إقراره من المجني عليه دون الرجوع إلى الجهاز حتى ينتج أثره على خلاف التصالح في الدخول غير المشروع، والذي لا ينتج التصالح أثره إلا بعد موافقة الجهاز. كما أن الشروع في هذه الجريمة غير متصور وفقًا لطبيعتها أنها جريمة شكلية، إذًا تتحقق الجريمة بمجرد التجاوز.

وقد قضت المحكمة الإدارية العليا بأنه:" وتبين وجود عمليات اختراق من الجهاز الذى يعمل عليه مما يشكل في حقه – وفي ضوء خطورة المعلومات المودعة بإدارة التداول وإدارة الإلزام بالهيئة العامة للرقابة المالية ومدي تأثيرها على عمل الشركات المصرية – خروجا جسيما على القواعد التي استنها المشرع في قانون مكافحة جرائم تقنية المعلومات وعدوانًا أثيمًا على الأنظمة المعلوماتية الخاصة بالدولة متجاوزًا حدود الحق المخول له من حيث الزمان أو مستوى الدخول مخترقا نظامًا معلوماتيًا يُدار لحساب الدولة ممثلا في أحد الأشخاص الاعتبارية العامة – الهيئة العامة للرقابة المالية – مما يستوجب مساءلته عنه تأديبيا مع أخذه بالشدة الرادعة، خاصة وأنه تبين تكرار الطاعن لذلك الفعل سابقًا حيال عمله بقسم الدعم الفني واستخدامه لبرامج تجسسيه من الجهاز الخاص به للحصول علي البيانات ومعلومات من أجهزة أخري ومجازاته عن ذلك الفعل

بالخفض لوظيفة من الدرجة الأدنى ونقله من إدارة الدعم الفني مما يكون معه جزاء الفصل من الخدمة هو الجزاء الأوفى"([1]).

وفي هذا الشأن توجد العديد من القضايا ومنها في القضاء الإنجليزي، في قيام أحد رجال الشرطة بالدخول إلى النظام الإلكتروني الخاص بالشرطة وأخذ معلومات لا تمت وظائفهم بصلة([2])، ورفضت المحاكم الأمريكية الدعوى المقامة من الولايات ضد أولسن، حيث تتلخص وقائع هذه القضية في كون أولسن ضابط شرطة قام بتجاوز التصريح الممنوح له وباستخدام ودخول النظام الإلكتروني الخاص بالسلطات لأغراض أخرى غير الاستخدامات المخصص له حيث قام بطباعة صور السيدات الآتي يقمن بالدراسة في الجامعة القريبة منه ودفع أولسن في أنه يملك التصريح بالدخول إلى النظام المعلوماتي في الأساس لذلك لا يمكن أتهامة بتجاوز التصريح، وذلك عن طريق طباعة صور رخص قيادتهم([3]). وتم الانتهاء بأن الدخول يعتبر مصرح به، وهو ما أتجه إليه النظام القضائي الإنجليزي بخصوص تجاوز حدود الدخول المصرح به.

ثالثًا: جريمة الاعتراض غير المشروع

تعد جريمة الاعتراض غير المشروع، صورة من صور الاعتداء على سلامة شبكات وأنظمة المعلومات، ومعنى الاعتراض: هو مشاهدة البيانات أو المعلومات أو الحصول

---

[1] – حكم المحكمة الإدارية العليا، بجلسة ٢٠٢٠/٨/٨.

[2] - د. نائلة عادل محمد فريد قوره، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية)، منشورات الحلبي، لبنان، ٢٠٠٥، ص٣٣٩.

53- Sami AL- Rawashdeh, legal Access to Information Systems in Qatari Criminal Law:
A Comparative Study, Kuwait Interational Law School Journal, Volume 6, Issue 1, Ser.No.21,March, 2018,p18

عليها، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق. وهو يختلف عن الاختراق حيث عرفه المشرع في المادة الأولى: هو 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، إذًا الاعتراض يختلف عن الاختراق.

حيث نص المشرع المصري على تجريم الاعتراض غير المشروع في المادة (١٦) "كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها". وتلك الجريمة هي إحدى صور التجريم الجديدة، وهي في غاية الأهمية بما كان حيث يشكل اعتراض البيانات أو المعلومات ضرر بالغ الخطورة.

وحيث يتكون البنيان القانون لهذه الجريمة من الركن المادي: ويتمثل في الاعتراض بدون وجه حق على أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها. والركن المعنوي: حيث تحتاج هذه الصورة من صور التعدي إلى قصد خاص، يتمثل في تحقيق النتيجة الإجرامية مثل التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام او تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة.

فيجب إثبات انصراف إرادة الجاني لارتكاب الفعل المادي، وإرادة تحقيق غرض غير مشروع. كما تتمثل العقوبة: في أن يعاقب الجاني بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه أو بإحدى هاتين العقوبتين.

وقد قضت المحكمة الإدارية العليا بمجلس الدولة سابق الإشارة إليه، " أن المشرع حظر على مقدمي الخدمة كل من الاعتراض والاختراق، فالاعتراض يشمل كل مشاهدة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق، والاختراق يشتمل على 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".

المطلب الثاني

الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها

تعد جريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنيتها أحد صور جرائم الاعتداء على سلامة شبكات وانظمة وتقنيات المعلومات، وهي نوع من 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 كما جاء في مادة التعريفات بقانون مكافحة جرائم تقنية المعلومات.

حيث نص في المادة (١٣) على أنه:" يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرة آلف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتي أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي"، وهو ما لم يكون مجرم قبل هذا القانون، مثل مباريات كرة القدم، والأفلام وغيرها من خدمات البث المسموع والمرئي.

وهو أمر في غاية الأهمية، حيث كان يتم الاعتداء دون وجود نص يجرم هذه الأفعال من ثم كان يكبد أصحاب تلك القنوات خسائر فادحة دون عقاب. وهو ما يحمد للمشرع المصري أن تبنى هذه الجريمة ووضع لها نص عقابي ليمثل ردع لكل من تسول له نفسه التعدي على حقوق الغير.

ويتشكل البنيان القانوني لهذه الجريمة من شقين الأول: الركن المادي، ويتمثل في الانتفاع بدون وجه حق عن طريق شبكة النظام المعلوماتي، أو إحدى وسائل تقنية المعلومات، بخدمة اتصالات أو خدمات قنوات البث المسموع والمرئي. ويعد تقديم خدمات الاتصالات، وتمرير المكالمات التليفونية الدولية بأية طريقة كانت والمنصوص عليها في المادة (٧٢/٣-٤) من القانون رقم (١٠) لسنة ٢٠٠٣ بشان الاتصالات من صور الانتفاع بدون وجه حق عن طريق شبكة النظام المعلوماتي([1]).

أما الشق الثاني: هو الركن المعنوي للجريمة لم يتطلب المشرع ركن خاص لهذه الجريمة كالعمد، لذلك يكتفى بالقصد العام المتمثل في علم الجاني بالنص القانوني، وانصراف إرادته لتنفيذ النشاط الإجرامي.

العقوبة: يُعاقب على هذه الصورة من صور الجريمة، بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين طبقًا لنص المادة (١٣)؛ ومن الجدير بالذكر أن الجريمة المنصوص عليها في المادة (٧٢ /٣- ٤) من قانون الاتصالات معاقب عليها بعقوبة الحبس مدة لا تقل عن ستة أشهر ولا تجاوز خمس سنوات وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين. وتقضى المحكمة من تلقاء

[1]- أنظر القانون رقم (١٠) لسنة ٢٠٠٣ بإصدار قانون تنظيم الاتصالات.

نفسها بإلزام المحكوم عليه بالتعويض المناسب في الحالة المنصوص عليها في البند (٤) من هذه المادة.

وقد احتاط المشرع لوجود عقوبتين مختلفتين لذات الفعل في أكثر من قانون فنص بالمادة (١٢) من قانون مكافحة جرائم تقنية المعلومات على: "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر، ويُفهم من ذلك أن العقوبة الأشد المنصوص عليها في قانون الاتصالات هي المُطبقة على صورتي تقديم خدمات الاتصالات وتمرير المكالمات، عن طريق الانترنت.

الظروف المشددة للعقاب: إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد، (المادة ٣٤).

العود: للمحكمة أن تقضي بإيقاف ترخيص مزاولة الشخص الاعتبار للنشاط مدة لا تزيد على سنة، ولها في حالة العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم في جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري، المادة (٣٦).

المسئولية الجنائية للشخص الاعتباري: يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن ثلاثين ألف جنية ولا تزيد عن مائة ألف جنية أو بإحدى هاتين العقوبتين، كل مسئول عن الإدارة الفعلية لأي شخص اعتباري، إذا تعرض الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتي المخصص للكيان الذى يديره، لأي جريمة من الجرائم المنصوص عليها في هذا القانون، ولم يبلغ بذلك الجهات

المختصة وقت علمه بالجريمة، المادة (٣٥)، في الأحوال التي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون، باسم ولحساب الشخص الاعتباري، يعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقًا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي، المادة (٣٦).

المبحث الثاني

جريمة الاعتداء على سلامة البيانات والبريد الإلكتروني وتصميم الموقع

تمهيد وتقسيم:

تعد جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، أحد الجرائم التي تمثل اعتداء على سلامة شبكات المعلومات وأنظمة وتقنيات المعلومات، فقد جرمها معظم المشرعين على مستوى العالم، لما تنطوي على خطورة من أتلف أو تعطيل أو إلغاء الارسال، وغيرها من وسائل الاعتداء. كما جرم المشرع الاعتداء على البريد الإلكتروني أو الموقع أو الحسابات الخاصة، والتي تمثل أيضًا اعتداء على سلامة شبكات المعلومات وأنظمة تقنيات المعلومات، سواء كان بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بآحاد الناس، أم بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، وقد شدد المشرع العقاب في الحالة الأخيرة.

كما جرم المشرع الاعتداء على تصميم موقع والذي يمثل اعتداء على شبكات وأنظمة وتقنيات المعلومات، لما ينطوي هذا الفعل على أتلف أو تعطيل أو أبطاء أو تشوّه أو أخفى أو غير تصاميم موقع سواء خاص بشركة أو مؤسسة أو منشأة، أم شخص طبيعي بغير حق. وهو ما سوف نتناوله بالشرح والتوضيح في السطور القادمة.

- المطلب الأول: الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية
- المطلب الثاني: الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة وتصميم الموقع

المطلب الأول

الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية

لم يكن يعرف القانون المصري تجريم مباشر لجريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية قبل صدور قانون مكافحة تقنية المعلومات، هذه الجريمة التي لا تقل أهمية عن العديد من الجرائم التي قد ترتكب للاعتداء على سلامة شبكات وأنظمة المعلومات، وما تمثله من تهديد على أتلف أو تعطيل أو تعديل مسار أو إلغاء البيانات والمعلومات، وما ينتج عن ذلك من أضرار، فقد تكون هذه المعلومات أو البيانات على موقع أو بريد الإلكتروني أو حساب خاص، فقد ينتج عن ذلك التعدي العديد من الاضرار التي تنجم عن الاعتداء على سلامة البيانات الخاصة بتلك الموقع أو الحساب الخاص.

وكما يتصور ذلك الاعتداء على موقع أو حساب أو نظام خاص بالدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها، أو يخصها، فقد ينتج عن الاعتداء على سلامة البيانات التي تخص الدول اضرار فادحة وبشكل خاص النواحي الحربية أو السياسي أو التي تمثل أمن القومي للبلاد، وهو ما دعا المشرع المصري في قانون مكافحة تقنية المعلومات إلى حماية البيانات والمعلومات والنظم المعلوماتية.

حيث نص في المادة (١٧) على: " كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا متعمدًا وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلقة على أي نظام معلوماتي وما في حكمه، أيا كانت الوسيلة التي استخدمت في الجريمة".

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

وبناءً عليه فإن تلك الجريمة يتشكل بنيانها القانوني من ركنيّن: ركن مادي، يتمثل الفعل المعاقب عليه في قيام الجاني بإتلاف أو تعطيل أو الإخلال بنظام المعلوماتي بدون وجه حق، وركن معنوي متمثل في القصد الجنائي، المكون من العلم والإرادة، العلم بالجريمة وإرادة ارتكابها، فهي جريمة عمدي وفقًا لنص المادة سالفة البيان، أن يكون الفاعل متعمدًا وبدون وجه حق، وبناءً عليه فإن تحقق النتيجة الإجرامية بخطأ وبدون عمد ينفي عن الفاعل القصد الجنائي، كما أن المشرع لم يُحدد وسيلة معينة ومحددة في ارتكاب السلوك الإجرامي المشكل للركن المادي فيها، فإذا تشكل الركن المادي يلزم للعقاب توافر القصد الجنائي.

ويثور في هذا الصدد تساؤل في غاية الأهمية بما كان وهو هل هناك عقاب على الشروع في تلك الجريمة؟ لقد عاقب المشرع المصري في قانون مكافحة تقنية المعلومات في المادة (٤٠) على الشروع في كافة الجنح المنصوص عليها في هذا القانون، وهو على خلاف قانون العقوبات الذي ينص على العقاب في الشروع بنص خاص([1]). ولما كانت جريمة الاعتداء على البيانات والمعلومات بحسب نوع العقاب جنحة إذا يتصور الشروع فيها.

كما يثور تساؤل آخر على نفس درجة الأهمية وهو هل يمكن التصالح في هذه الجريمة؟ لقد نص المشرع المصري في القانون سالف الذكر في المادة (٤٢)([2]) على جواز التصالح وقبل صيرورة الحكم باتًا، وحدد بعض المواد منها المادة (١٧)، ولكن لا ينتج إقرار المجني عليه بالصلح المنصوص عليه إلا باعتماد من الجهاز بالنسبة لبعض

---

[1] - فضلًا راجع د. أحمد شوقي عمر أبو خطوة، الأحكام العامة لقانون العقوبات، مرجع سابق، ص ٢٢٢.

[2] - للمزيد أنظر المواد (٤٠)، (٤٢) من قانون مكافحة تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

الجنح المنصوص عليها بالمواد (١٤،١٧،١٨،٢٣) من هذا القانون، إذًا يتبين حتى ينتج التصالح أثره يجب اعتماده من الجهاز (الجهاز القومي لتنظيم الاتصالات).

كما أن هذه الجريمة تشمل على تعطيل أجهزة الحاسب أو إتلافها عبر إرسال الفيروسات أو البرامج التي تحتوي على أنظمة هجومية تتسبب في إتلاف النظام المعلوماتي، ومن ثم يؤدي إلى تدمير المعلومات والبيانات وكل الأنشطة المرتبطة بهذا الحاسب([١])، ففي الولايات المتحدة الأمريكية قد أصدر مكتب التحقيقات الفيدرالي الأمريكي إنذارًا عامًا يحذر مستخدمي الإنترنت من مخاطر رسائل إلكترونية جديدة، تنطوي على خداع([٢])، يدفع المستخدمين إلى الكشف عن بيانات حساباتهم المالية الشخصية، ليتمكنوا لاحقًا من السطو على تلك الحسابات.

كما حذرت دائرة شكاوى جرائم الإنترنت التابعة للمكتب الفيدرالي، من ظهور مجموعة من الرسائل الإلكترونية التي تزعم أن الملتقى قد قام بعمليات شراء لبضائع عبر الشبكة، حيث يستدرج للكشف عن بيانات حساباته([٣]). إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة الأمريكية (FBI) نظرًا لتماثل دوافع المعتدين على نظم الحاسب الآلي مع مرتكبي العنف([٤]).

---

[١] - د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ط٢، ص ١٦٧.

[٢] - وقسمت وزارة العدل الأمريكية عام ٢٠٠٢ الدليل الرقمي إلى ثلاث مجموعات هي: السجلات المحفوظة في الحاسب الآلي؛ والسجلات التي يتم إنشاؤها بواسطة الحاسب الآلي ومخرجات برامجه التي لم يساهم الإنسان في إنشائها كسجلات الهاتف وفواتير أجهزة الحاسب الآلي؛ والنوع الثالث هو السجلات التي تم حفظ جزء منها بالإدخال والجزء الآخر تم إنشاؤه بواسطة الحاسب الآلي ومن أمثلة ذلك البيانات التي يتم إدخالها إلي الجهاز وتتم معالجتها من خلال برنامج خاص كإجراء العمليات الحسابية على تلك البيانات

[٣] - د. أحمد تمام، الحماية الجنائية للحاسب الآلي، دار النهضة العربية، ٢٠٠٩، ص٢٧٠ وما بعدها.

59 - Computer Hackers: Tomorrows Torrortsts, Dgnamics, News For And Aboutmembers Of the American Society For Industrial Security, Varyl Febrauary, 1990, p.7.

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

وفي الولايات المتحدة الأمريكية لا تثور مشكلة بهذا الخصوص، لأن القانون رقم (١٨) المتعلق بجرائم الحاسب الآلي يعالج هذه المسالة، وتطبيقًا لذلك فقد أدانت محكمة ولاية نيوجيرسي في الولايات المتحدة المتهم ديفيد سميث، حيث أسند إليه تهمة إنتاج فيروس ميليسا الذي اجتاح الولايات المتحدة عام ١٩٩٩ ميلاديًا وتسبب في عطل أكثر من مليون جهاز حاسب آلي، وخسارة مالية قدرت بحوالي ثمانين مليون دولار، وتم الحكم عليه وفقًا للفقرة (١٠٣٠/أ) البند الخامس من المرسوم رقم (١٨) الذي يعاقب على إتلاف البرامج والتسبب في الإضرار إلى أجهزة الحاسب الآلي المحمية والتي عرفها ذلك القانون بأنها أجهزة الحاسب الآلي العاملة لذى الحكومة أو لدى المؤسسات المالية والتجارية([1]).

وعن الوضع في فرنسا، نجد أن قانون العقوبات الفرنسي الجديد نظم هذه المسألة أيضًا، ونص في المادة (٢/٣٢٣) " كل من يدخل بطريق مخادعة لمعطيات داخل نظام المعالجة الآلية أو من يحذف أو يعدل بطريقة مخادعة معطيات موجودة في النظام، فإنه يعاقب بالسجن لمدة ثلاث سنوات وغرامة قيمتها ثلاثمائة ألف فرنك فرنسي".

وقد قضت المحكمة الإدارية العليا بأنه:" وحدد المشرع البيانات والمعلومات الإلكترونية بأنها كل ما يمكن إنشاؤه أو تخزينه، أو معالجته، أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات؛ كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات وما في حكمها، وأن البرنامج المعلوماتي عبارة عن مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق

[1] - د. محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، ط١، ص١٠٥.

نتيجة سواء كانت هذه الأوامر والتعليمات في شكلها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي"([1]).

المطلب الثاني

الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة وتصميم الموقع

أولًا: الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة:

لم يكون يعرف العالم هذه الجريمة حتى فترة قريبة من الزمان، حيث ظهر البريد الإلكتروني لأول مرة على يد العالم الأمريكي راي توملينسون Ray Tomlinson، حيث صمم على شبكة الإنترنت برنامج لكتابة الرسائل يسمى Send message، وذلك لتمكن العاملين على الشبكة من تبادل الرسائل فيما بينهم، ولم ينتظر طويلًا ليخترع برنامج جديد أطلق عليه تسمية Cypnte، الذي يسمح بنقل الملفات من جهاز كمبيوتر إلى آخر، ثم دمج فيما بعد البرنامجين في برنامج واحد هو البريد الإلكتروني، ويرجع وضع الرمز @ لأن الرسائل لم تكن تحمل اسم مرسلها فقد وضع توملنسون هذا الرمز بين اسم المرسل والموقع الذي ترسل منه الرسالة ليخرج في خريف ١٩٧١ أول عنوان بريد إلكتروني في التاريخ([2]).

وقد 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 أخد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها"، كما عرفه القانون الأمريكي لسنة ١٩٨٦

[1] - حكم المحكمة الإدارية العليا، بجلسة ٢٠٢٠/٨/٨.

[2] د. خالد ممدوح إبراهيم، أمن مراسلات البريد الإلكتروني، دار الجامعة الجديد، الإسكندرية، ٢٠٠٨، ص٥٣.

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

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 إلكترونيًا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه حيث يتم إرسالها عبر نظام خطوط تليفون إلى كمبيوتر المرسل إليه"(١).

كما توجد العديد من التعريفات الفقهية نعرض منها:" تلك المستندات التي يتم إرسالها واستلامها بواسطة نظام بريدي إلكتروني، وتتضمن ملحوظات مختصرة ذات طابع شكلي حقيقي، ويمكنه استصحاب مرفقات به، مثل نظام معالجة أو أية مستندات أخرى يتم إرسالها رفقة الرسالة ذاتها"، وكما عرف بأنه:" مكنة التبادل الإلكتروني غير المتزامن للرسائل بين أجهزة الحاسب الآلي"(٢). وقد عرف المشرع المصري البريد الإلكتروني: بأنه وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعي أو اعتباري، عبر شبكة معلوماتية أو غيرها من وسائل الربط الإلكترونية من خلال أجهزة الحاسب الآلي وما في حكمها.

كما عرف الحساب الخاص بأنه: مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي. وكما عرف الموقع بأنه: مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة.

---

63 - Florence Celen, Laurence Lomme, " Application de la Loi sur la Confiance dans l'économie Numérique au CNRS", Sécurité Informatique, N: 54, Septembre2005,p3.

٢- د. خالد ممدوح إبراهيم، أمن مراسلات البريد الإلكتروني، مرجع سابق، ص ٥٥.

وقد جرم المشرع المصري الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة، كأحد صور الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، حيث نص في المادة (١٨) على:" كل من أتلف أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بآحاد الناس". وهي من الجرائم المستحدثة التي نص عليها المشرع في القانون سالف الذكر، تجريم الاعتداء على البريد الإلكتروني الخاصة بآحاد الناس، وهي تمثل حماية للبريد الإلكتروني من التعدي عليه سواء، أتلف أو عطل أو أبطأ أو اخترق. وكما يشدد المشرع العقاب في حالة إذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة.

حيث يتكون البنيان القانون للجريمة من شقين: الأول ويتمثل في الركن المادي للجريمة، بنشاط الإجرامي في عدة صور منها إتلاف أو تعطيل أو التسبب في إبطاء أو مجرد اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بآحاد الناس. وأما عن الشق الثاني فيتكون من الركن المعنوي وهو القصد الجنائي، ولا يتطلب هذا النمط من التجريم ركنًا خاصًا فيكفي لإتيان الجاني النشاط المعاقب عليه، وعلمه بالنص العقابي، وهو علم مفترض بمجرد نشر القانون بالجريدة الرسمية.

كما أن العقوبة لها فلسفة خاصة حيث يتدرج العقاب مع اختلاف حالة المجني عليه فلو تم التعدي على آحاد الناس تكون العقوبة الحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين. فإذا وقعت الجريمة على بريدة إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين. ويرى الباحث ان عقوبتها

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

أخف من باقي صور الجريمة ربما لمحدودية آثار الجريمة كون المجني عليه فردًا، ويستنتج ذلك من تدرج العقوبة حال كان المجني عليه شخص معنوي.

ثانيًا: الاعتداء على تصميم موقع

ولقد جرم المشرع المصري الاعتداء على تصميم الموقع، كأحد صور الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، فجريمة الاعتداء على تصميم موقع أحد الجرائم المستحدثة التي أنتجتها التكنولوجي والتطور التقني في مجال المعلومات، فكان لزامًا على المشرع التدخل، حيث نص في المادة (١٩) على جريمة الاعتداء على تصميم موقع:" كل من أتلف أو عطل أو أبطأ أو شوَّه أو أخفى أو غيَّر تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق". وهي إحدى الجرائم المعلوماتية التي أنتجتها تقنية المعلومات.

حيث يتكون البنيان القانوني لهذه الجريمة من الركن المادي: بقيام الجاني بإتلاف أو تعطيل أو إبطاء أو تشوَّيه أو إخفاء أو تغييَّر تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعي بغير وجه حق، والركن المعنوي: ويتمثل في علم الجاني بالنص العقابي، وهو علم مفترض بمجرد نشر القانون، واتجاه إرادة الجاني نحو تحقق النتيجة الإجرامية، وأنه يقترف الفعل المعاقب عليه بغير وجه حق، كما أن العقوبة في هذه الجريمة عبارة عن الحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين.

وكما ذكرنا من قبل أن كافة الشروع في الجنح في هذا القانون معاقبًا عليها إذًا الشروع في الاعتداء على تصميم موقع معاقب عليه بنظر لنوع العقوبة وهي جنحة. كما يجوز التصالح فيها قبل صيرورة الحكم باتًا وفقًا لنص المادة (٤٢) من القانون سالف الذكر، حيث إنها من الجنح المنصوص عليه في جواز التصالح، ويكون التصالح منتج لأثره

دون موافقة الجهاز لأنها ليس من الجنح الواردة في القانون، والتي تتعلق في التصالح باعتماد الجهاز.

المبحث الثالث

جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة وسلامة الشبكة المعلوماتية واستخدام البرامج والأجهزة والمعدات في ارتكابها

تمهيد وتقسيم:

لقد جرم المشرع الاعتداء على الأنظمة الخاصة بالدولة، وهو ما نص عليه الكثير من التشريعات، وقد اتفق معهم المشرع المصري في ذلك حيث جعل الدخول في أنظمة الدولة أو إحدى الأشخاص الاعتبارية العامة بقصد الاعتراض أو الحصول على معلومات يشكل جناية وعقوبته السجن والغرامة، ويرجع ذلك إلى أن الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة يؤثر على الأمن القومي، كما جرم الاعتداء على سلامة الشبكة المعلوماتية، وهنا تكون الحماية الجنائية تقع على الشبكة المعلوماتي وليس الجهاز أو الأجهزة، فإذا كانت الشبكة تخص الدولة أو تديرها الدولة أو أحد الأشخاص الاعتباري العامة يصبح الفعل جناية كما هو الحال بالنسبة للشبكة العامة للإنترنت.

كما جرم المشرع استخدام البرامج والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات وبشكل خاص الإتجار في كلمة المرور (الباسورد)، وهي التي تمكن المجرم من الدخول إلى النظام المعلوماتي، ومن ثم تغيير كلمة المرور، ومنع صاحب الموقع أو الايميل من استخدامه، أو الدولة أو أي جهة من التعامل على موقعها، وهو ما يمثل اعتداء على البريد الخاص أو الحساب الخاصة، ويمثل اعتداء على الأنظمة المعلوماتية الخاصة بالدولة، وكما يمثل اعتداء على سلامة الشبكة المعلوماتية، بل ويمثل اعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، وسوف نتناول ذلك بالشرح

- المطلب الأول: الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة
- المطلب الثاني: الاعتداء على سلامة الشبكة المعلوماتية وتجريم استخدم البرامج والأجهزة والمعدات في ارتكابها

المطلب الأول

الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة

تعد جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة إحدى صور الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، فقد نصت المادة (٢٠) على جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، "كل من دخل عمدًا, أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفة أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها, أو يخصها".

ويتبين من ذلك مدى خطورة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة، فالمشرع عاقب كل من دخل عمدًا أي توافر في حقه الركن المادي متمثل في السلوك الإجرامي الدخول غير المشروع، والركن المعنوي بتوافر القصد الجنائي من خلال العلم والإرادة، كما عاقب من دخل بخطأ غير عمدي، أي انتفاء الركن المعنوي في حقه المتمثل في القصد الجنائي، ولكنه بقى في النظام بدون وجه حق، كما عاقب من تجاوز حدود الحق في البقاء، أي أن الدخول مصرح به، ولكن قد تجاوز حدود هذا التصريح سواء من ناحية الزمان أم مستوى الدخول.

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

كما عاقب من تمكن من خلال الدخول غير المشروع باختراق موقعًا أو بريدًا أو نظامًا يُدار بمعرفة الدولة، فكما وضحنا سابقًا في جريمة تجاوز حدود الحق في الدخول أنها جريمة شكلية، إذًا يعاقب المشرع على البقاء في النظام بمجرد السلوك دون الانتظار النتيجة الإجرامي، وبناءً عليه لا يعتد بتوافر القصد الجنائي من عدمه، على خلاف الجريمة العمدي التي يتطلب فيها المشرع النتيجة الإجرامية

كما أن الشروع في هذه الجريمة معاقب عليه وفقًا لنص المادة (٤٠) من هذا القانون، وأما عن جواز التصالح فبناءً على نص المادة (٤٢) من القانون سالف الذكر لا يجوز التصالح في هذه الجريمة حيث إنها ليست من الجرائم المدرجة في الجنح التي يجوز التصالح فيها. وهو ما يُحمد للمشرع المصري بعدم السماح بالتصالح في هذه الجريمة التي تمثل تهديد على الأمن القومي للبلاد من خلال الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.

وكما شدد المشرع العقاب في حالة الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، وجعل العقوبة السجن والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. فكما وضحنا من قبل أن الاعتراض يختلف عن الاختراق، فالمشرع غلظ العقاب على الاعتراض لما ينطوي على مخاطر بالغة الخطورة على الأمن القومي، فعاقب عليه بالسجن والغرامة، (جناية)، على خلاف الاختراق الذي عاقب عليه بالحبس سنتين والغرامة، (جنحة) واتفقا في أن كلًا منهما لا يجوز التصالح فيهما، وتجريم الشروع فيهما.

كما شدد العقاب أكثر في حالة إذا ترتب على هذا الدخول غير المشروع إتلاف تلك البيانات أو المعلومات أو ذلك الموقع ... تكون العقوبة السجن والغرامة لا تقل عن

مليون جنيه ولا تجاوز خمسة ملايين جنيه. لما ينطوي هذا الفعل على مخاطر لا يمكن تدركها

و**الباحث** يؤيد المشرع العقابي في هذه الفلسفة العقابي والتي تعمل على تحقيق الردع العام والخاص. كما أن **الباحث** يطالب بتغليظ العقاب في حالة الدخول العمدي أو تجاوز حدود الدخول لما ينطوي على أضرار كبيرة بالأمن القومي، فالدولة باتت بأكملها تتعامل من خلال شبكة المعلومات، فإذا تمكن المجرم من الوصول إلى المعلومات الهامة والحيوية، أو ذات الشأن العسكري أو السياسة، فقد يترتب على ذلك العديد من الأضرار والتي قد لا يمكن تدركها فيما بعد، فكان الأولى في هذه الجريمة أن يكون العقاب واحد وليس متدرج بحيث يكون العقاب السجن والغرامة التي لا تقل عن خمسة ملايين جنية.

وقد قضت المحكمة الإدارية العليا في حكمها سابق الإشارة إليه أنه:" يحظر الاعتراض أو الاختراق للبيانات والمعلومات الحكومية على شبكة الانترنت حماية للأمن القومي، وأن حماية أسرار الدولة للبيانات والمعلومات الإلكترونية وأجهزتها على الشبكة المعلوماتية أو نظام معلوماتي أو حاسب خاص من مسائل الأمن القومي، وأن الأمن القومي يتسع ولا يضيق ليشمل كل ما يتصل باستقلال واستقرار وأمن الوطن ووحدته وسلامة أراضيه، وأن الأمن المالي والاقتصادي للوطن جزء لا يتجزأ من أمنه القومي، وأن الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة جريمة لها عقوبات متعددة صارمة.

كما شددت أن التهمة ثابتة بالدليل الرقمي وليس الورقي والأدلة الرقمية السبيل لكشف مكافحة جرائم تقنية المعلومات، وأن الطاعن في الطعن الأول أثناء عمله بقسم الدعم الفني استخدم برامج تجسسيه من جهازه للحصول علي البيانات ومعلومات من أجهزة

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

أخري، وأن المرحلة التي تمر بها البلاد دقيقة والشائعات تستهدف النيل من اقتصادها القومي وزعزعة الاستقرار والبتر من الوظيفة لا يستلزم الضرر الفعلي، ويكفى الضرر المحتمل والتهديد المحتمل للأمن القومي وأن إفشاء الطاعن الثاني كلمة السر للأول خطأ جسيم مكنه من اختراق المعلومات السرية الخاصة بجهة عمله.

وقضت المحكمة في حيثيات حكمها، إن المشرع انتهج في قانون مكافحة جرائم تقنية المعلومات حماية لأسرار الدولة للبيانات والمعلومات الإلكترونية المتعلقة بالدولة أو أحد سلطاتها أو أجهزتها أو وحداتها أو الهيئات العامة أو الهيئات المستقلة أو الأجهزة الرقابية أو هيئاتها العامة الخدمية أو الاقتصادية، وغيرها من الأشخاص الاعتبارية العامة أو ما في حكمها المتاحة على الشبكة المعلوماتية أو أي نظام معلوماتي أو حاسب خاص بها. ونظرا لخطورة جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة رصد المشرع لها العديد من العقوبات الصارمة".

ولم يقتصر الاعتداء على القطاع المدني بل كان لها أكبر الأثر في تطوير أنظمة الحرب الحديثة، وأدت إلى ظهور ما يسمى بحرب المعلومات، حيث يستهدف هذا النوع من الإجرام الأهداف السياسية والعسكرية، وقد حدث ذلك من الإنجليزي (نيكولاس أندرسون) في اختراق موقع البحرية الأمريكية وتمكن من الوصول إلى معرفة كلمة المرور واستخدمت في الهجوم النووي، كما تمكن الألماني (هيس لأندر) في اختراق قاعدة بيانات شبكة البنتاجون واستطاع الحصول على ٢٩ وثيقة متعلقة بالأسلحة النووية([1]).

[1] - د. محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، ٢٠١٢، ص٣٥.

كما تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم، كما أنه قد يتمكن من اختراق الأجهزة الأمنية الحكومية، وكذلك أصبحت شبكة المعلومات مجالًا خصبًا لنشر أفكار العديد من الأفراد والمجموعات، ووسيلة لترويج لأخبار وأمور أخرى قد تحمل في طياتها مساسًا بأمن الدولة أو بنظام الحكم أو قدحًا في رموز دولية أو سياسية.

المطلب الثاني

الاعتداء على سلامة الشبكة المعلوماتية وتجريم استخدم البرامج والأجهزة والمعدات في ارتكابها

أولًا: الاعتداء على سلامة الشبكة المعلوماتية

يعد الاعتداء على سلامة الشبكة المعلوماتية، إحدى صور الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، وقد عرف المشرع شبكة المعلومات في المادة الأولى الخاصة بالتعريفات بأنه: مجموعة من الأجهزة أو نظم المعلومات تكون مرتبطة معًا ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية، والتطبيقات المستخدمة عليها.

وقد عاقب المشرع في المادة (٢١) على جريمة الاعتداء على سلامة الشبكة المعلوماتية، " كل من تسبب متعمدًا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها". وهنا تكون الحماية الجنائية تقع على الشبكة المعلوماتي وليس الجهاز أو الأجهزة، فإذا كانت الشبكة تخص الدولة أو تديرها الدولة أو أحد الأشخاص الاعتباري العامة يصبح الفعل جناية كما هو الحال بالنسبة للشبكة

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

العامة للإنترنت، وتكون العقوبة السجن المشدد، وبغرامة لا تقل عن خمسمائة ألف جنية ولا تجاوز مليون جنيه.

أما إذا تسبب في التعطيل أو إيقاف شبكة المعلومات يعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسون ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى العقوبتين، على فرض أن هذه الشبكة ليست خاصة بالدولة، على خلاف التشدد الذي نص عليه المشرع إذا كانت خاصة بالدولة كما وضحنا.

فيتكون البنيان القانوني لهذه الجريمة من شقين: أولهما الشق المادي للجريمة ويتمثل في كل فعل يؤدي إلى إيقاف شبكة المعلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها، إذا الركن المادي عبارة عن أي عمل يمثل اعتداء على سلامة الشبكة المعلوماتية، وأما عن الشق الثاني، فهو الركن المعنوي يتطلب المشرع ركن خاص هو قصد العمد، ولو لم يترتب على النشاط الإجرامي أية نتيجة إجرامية، فيكتفي بإثبات تعمد الجاني الاعتداء على سلامة الشبكة المعلوماتية.

كما أنه لا يجوز التصالح في هذه الجريمة، فهي لم ترد ضمن الجنح التي يجوز فيها التصالح في شقها الأول الذي يشكل جنحة، وفقًا لنص المادة (٤٢) من قانون مكافحة تقنية المعلومات، وهو ما نؤيده ونحمد المشرع على هذا الموقف المحمود من جانبه بعدم السماح بالتصالح في مثل هذه الجريمة، كما نؤيد موقفه من التشديد في حالة إذا كانت الشبكة المعتدي عليه تخص الدولة أو أحد الأشخاص الاعتبارية العامة، فكانت جناية وعقوبتها السجن المشدد والغرامة التي لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه.

كما أن البنيان القانون في الاعتداء على سلامة الشبكة المعلوماتية بالخطأ يختلف، حيث يتكون الركن المادي من إتيان السلوك المتمثل في تسبب بخطئه في الاعتداء على سلامة شبكة المعلومات، وأما عن الركن المعنوي، فالمشرع يفترض علم الجاني بنشر القانون في الجريدة الرسمية، فجعل هذا التعدي جريمة شكلية بمجرد السلوك، دون أن يذكر قصد خاص أن يكون عمدًا.

ثانيًا: البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات

لقد جرم المشرع البرامج والأجهزة والمعدات المستخدمة في ارتكاب جرائم تقنية المعلومات، والتي تمثل اعتداء على سلامة شبكة وأنظمة تقنيات المعلومات، حيث نص المشرع في المادة (٢٢) " كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأي صورة من صور التداول, أي أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أي بيانات مماثلة، بدون تصريح من الجهاز أو مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أي منها في ارتكاب أية جريمة من المنصوص عليها في هذا القانون أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء".

وقد جرم المشرع حيازة أو استيراد أو أنتاج أجهزة إذا كان بغرض استخدامها في الجرائم السابقة، ويقصد بذلك بصفة خاصة أجهزة فك كلمة المرور (الباسورد) والتي تمكن المتهم من الدخول بكلمة المرور وتغيير كلمة المرور، وبالتالي حرمان الدولة أو الأشخاص من استخدام اجهزتها.

وقد يرجع تجريم الاتجار في كلمة المرور درءًا للدخول غير المصرح له حيث لوحظ أن بعض المجرمين في المجال المعلوماتي يتوصلون إلى معرفة كلمات السر لشركات أو جهات وينشرون إعلانات على شبكة الإنترنت تفيد معرفتهم تلك الكلمات ويعرضون

٤- جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات

ببيعها أو يعرضون قدرتهم على معرفة تلك الكلمات للجهات التي ترغب فيها المتداخلون.

كما أن بعض المتداخلين يعرضون على بعضهم البعض إمكانية تبادل الكلمات التي بحوزتهم مع ما يحوزه الآخرين.

لذلك فإن بعض التشريعات تُعاقب على هذا الاتجار مثل القانون الفيدرالي الأمريكي الذي ينص على عقاب " كل شخص يقوم – بقصد الغش – بالإتجار في كلمة المرور واستطاع بذلك أو مكن الغير من الدخول في كمبيوتر".

وأما عن البنيان القانون لهذه الجريمة، فيتكون من الركن المادي: وهو عبارة عن أي صورة من الصور التي نص عليها المشرع من حيازة وإحراز، أما الركن المعنوي، فيتمثل في القصد الجنائي حيث يتطلب المشرع قصد خاص وهو أن يكون بدون تصريح، ويثبت أن السلوك كان بغرض استخدام أي منها في ارتكاب أو تسهيل ارتكاب أي جريمة من المنصوص عليها في هذا القانون.

وقد قضت المحكمة الإدارية العليا في حكمها سابق الإشارة إليه بأنه:" وعن المخالفة المنسوبة للطاعن في الطعن الثاني والتي تتمثل في أنه أعطى الطاعن الأول كلمة السر خاصة حاسبه الآلي، مما مكنه من استخدام هذا الحاسب واختراق المعلومات السرية الخاصة بجهة عمله بالمخالفة للتعليمات، فإنها ثابتة في حقة ثبوتا يقينيا على النحو الوارد بالتحقيقات والتي يتضح منها عدم استطاعة الطاعن في الطعن الأول القيام بهذه المخالفة الجسمية واختراق تلك الأجهزة من تلقاء نفسه دون كلمة السر الخاصة بالجهاز".

الخاتمة

أولًا: النتائج

- وفي نهاية بحثنا عن جرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، فقد تبين أنها تمثل تهديدًا في مجال تقنية المعلومات، وكان من الضروري تدخل المشرع بالقانون رقم ١٧٥ لسنة ٢٠١٨ للحد من تلك الجرائم التي قد عرضنا لها من قبل.
- كما أن المشرع انتهج فلسفة عقابية خاصة في العقاب على هذه الجرائم، حيث تدرج في العقوبة بحسب جسامة الضرر المترتب على الفعل، وشدد العقاب على الأفعال التي قد تؤثر على الأمن القومي.
- كما أن المشرع قد أباح التصالح في بعض هذه الجرائم بمجرد الإقرار من المجني عليه، وعلق البعض على اعتماد الجهاز.

ثانيًا: التوصيات

١- أن يكون هناك فرع في وزارة الداخلية يختص بهذا النوع من الجرائم بحيث يكون هناك دقة في مراحل جمع الاستدلالات من المتخصصين، لتميز هذه الجرائم المعلوماتية بالنواحي التكنولوجي، والذكاء المعلوماتي من مجرمين يتسمون بصفات عالية في الإجرام المعلوماتي، مما يتطلب من المشرع الحرص على الوصول إلى الأدلة من المتخصصين في هذا النوع من الجرائم حتى تستقيم الدلائل الكافة للوصول إلى الحكم العادل.

٢- أن يكون هناك محققين على درجة كافية من النواحي المعلوماتية، حتى يتمكن من الإلمام بالنواحي الفنية العامة، ولا نقصد أن يكون متخصص بدرجة عالية، بل مجرد

معرفة بعض القواعد التي تساعد في التحقيق، وهو ما يتطلب من المشرع العمل على وجود نيابة تختص بالجرائم المعلوماتية.

٣- إنشاء محاكم متخصصة في الجرائم المعلوماتية، وهو ما نُطالب المشرع بالعمل على تحقيقه من خلال إنشاء دوائر متخصصة في الشأن المعلوماتي، فكما أكدنا من خلال دراستنا أن الجرائم المعلوماتية تختلف عن الجرائم التقليدية، إذًا الجرائم المعلوماتية تتطلب محاكم غير التقليدية للوصول إلى عنوان الحقيقة، وهو ما قد لا يتحقق وفقًا للضوابط العادي في المحاكمات التقليدية، وذلك يرجع لما تتميز به الجريمة المعلوماتية من اختلاف نوع المجرم، واختلاف وسائل الاثبات واختلاف النتائج والأضرار التي تنتج من الجريمة المعلوماتية عن التقليدية.

٤- إنشاء قانون متكامل خاص بالجرائم المعلوماتية، بحيث يكون له فلسفة عقابية منفصلة عن غيره من القوانين، والتي قد نلجأ لتطبيقها لوجود نقص في الجانب التشريعي الخاص بالجرائم المعلوماتية. إذًا تدور التوصيات حول غاية، وهي فكرة وجود هيكل متكامل من الجوانب منذ لحظة وقوع الجريمة وحتى المحاكمة، لتحقيق الهدف الرئيسي من العدالة، بحيث تبدأ من مأمور ضبط قضائي متخصص، وتنتهي بمحكمة مختصة بالجرائم المعلوماتية يطبق فيها قانون متكامل بالجريمة المعلوماتية.

٥- كما يأمل الباحث على المستوى الدولي بتفعيل مبدأ العالمية في هذه الجرائم لما تتسم به من طابع عالمي، فقد يتم الإعداد للجريمة في دولة، والتنفيذ في مجموعة دول في آن واحد، فالجريمة المعلوماتية، لا يمكن ملاحقة مرتكبها إلا بمبدأ العالمية الكامل، وليس بشكل مقيد مثل ما فعل المشرع المصري. فهي لا تقل أهمية عن الاتجار في المخدرات ونشر المطبوعات المخلة بالآداب وتزييف العملة والإرهاب الدولي.

والله من وراء القصد وهو يهدي السبيل،،

المراجع:

أولًا المراجع باللغة العربية:-

المراجع العامة:

د. **أحمد شوقي عمر أبو خطوة**، شرح الأحكام العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠١٦.

د. **أحمد فتحي سرور**، الوسيط في قانون العقوبات، الجزء الأول، القسم العام، دار النهضة العربية، ١٩٨١.

د. **عبد الرءوف مهدي**، القواعد العامة لقانون العقوبات، دار النهضة العربية، القاهرة، ٢٠٢٠.

د. **عبد العظيم مرسي وزير**، شرح قانون العقوبات، " القسم العام "، الجزء الأول، " النظرية العامة للجريمة"، دن، الطبعة التاسعة، ٢٠١١.

المراجع المتخصصة:-

د. **أحمد تمام**، الحماية الجنائية للحاسب الآلي، دار النهضة العربية، ٢٠٠٩، ص٢٧٠.

د. **أحمد خليفة الملط**، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦.

د. **أشرف عبد القادر**، الجرائم المعلوماتية، دار الثقافة عمان، ٢٠٠٨.

د. **أنور صدقي**، المسئولية الجزائية عن الجرائم الاقتصادية، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٦.

د. **خالد ممدوح إبراهيم**، أمن مراسلات البريد الإلكتروني، دار الجامعة الجديد، الإسكندرية،٢٠٠٨.

د. **عبد الفتاح بيومي**، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، دار النهضة العربية، ٢٠٠٩.

د. **فتوح الشاذلي**، د. عفيفي كامل عفيفي، جرائم الكمبيوتر، دراسة مقارنة، منشورات الحلبي، لبنان، ٢٠٠٣.

د. **محمد أحمد عبابنة**، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥.

د. **محمد سيد سلطان**، قضايا قانونية في أمن المعلومات وحماية البيئة الإلكترونية، دار ناشري للنشر الإلكتروني، ٢٠١٢.

د. **محمود رجب فتح الله**، شرح قانون مكافحة جرائم تقنية المعلومات وفقا للقانون المصري الجديد، دار الجامعة الجديدة، مصر، الإسكندرية، الطبعة الأولى، ٢٠١٨.

د. **مدحت إبراهيم**، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٥.

د. **نائلة عادل محمد فريد قوره**، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية)، منشورات الحلبي، لبنان، ٢٠٠٥.

د. **هدى قشقوش**، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، الطبعة الأولى، ١٩٩٢.

الرسائل العلمية:

د. **خالد سليمان عبدالله الحمادي**، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، رسالة ماجستير، ٢٠١٩.

د. **شيماء عبد الغني عطاالله**، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق، ٢٠٠٥.

د. **عبد الله محمد الحضري**، جريمة الدخول بدون وجه حق إلى المواقع الإلكترونية والنظم المعلوماتي العام في القانون القطري (دراسة تحليلية مقارنة)، رسالة دكتوراه، كلية القانون، جامعة قطر، ٢٠٢٠.

المجلات والمؤتمرات:

د. **أسامة العبيدي**، جريمة الدخول غير المشروع إلى النظام المعلوماتي (دراسة قانونية في ضوء القوانين المقارنة)، مجلة المعلومات، العدد١٤، جمعية المكتبات والمعلومات السعودية، ٢٠١٢.

د. **غنام محمد غنام**، عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مؤتمر القانون والكمبيوتر والإنترنت، المنعقد بجامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، ١-٣ مايو ٢٠٠٣، المجلد الثاني.

ثانيًا المراجع باللغة الأجنبية:

أولًا اللغة الفرنسية:

1- H. ALTERMAN et a. BLOCH – La Fraude Informatique, paris,Gaz, palais,(3) sep.1988

2- MASCALA Corinne, "criminalité et contrat électronique", IN: Le contrat électronique, Travaux de L'association CAPITANT Henri, journées national, Paris,2000

3-DEBRAY Stéphane, Internet face aux substandes illicites: complice de la cybercriminalité ou outil de Prevention, DESS média électronique & Internet, Université de Paris, 2002 -2003

4- Manacorda (sc) la relegmenation du blanch cabitaux en droit interational du systems rev secri iminal zavril, 1999.

5-Florence Celen, Laurence Lomme, " Application de la Loi sur la Confiance dans l'économie Numérique au CNRS", .Sécurité Informatique, N: 54, Septembre,2005.

ثانيًا: اللغة الإنجليزية

1- Marco Gercke, Regional and International Trends in Information Society Issues, in HIPCAR Working Group 1 (ST. Lucia: ITU, 2010), accessed through https://ccdcoe.org/publications/books/National Cyber Security Frame work Manual.pdf,2020

2- David R. gohnson and David post, law Review, vol 48, May, 1996

3-G. ROMAIN – la Delinqunace Informatique – Qu enest – on? (securite Informatique) guin 1998, n20

4- Sami AL- Rawashdeh, legal Access to Information Systems in Qatari Criminal Law:

A Comparative Study, Kuwait Interational Law School Journal, Volume 6, Issue 1, Ser.No.21,March, 2018

5-Computer Hackers: Tomorrows Torrortsts, Dgnamics, News For And Aboutmembers Of the American Society For Industrial Security, Varyl Febrauary, 1990