جامعة قطر

كليّة القانون

جريمة الدخول بغير وجه حق إلى المواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطري
"دراسة تحليلية مقارنة"

إعداد

عبد الله محمد الحضري

قُدّمت هذه الرسالة استكمالا لمتطلّبات

كليّة القانون

للحصول على درجة الماجستير في

القانون العام

يناير 1440/2020

©٢٠٢٠ عبد الله محمد مسلم الحضري. جميع الحقوق محفوظة.

لجنة المناقشة

استُعرضت الرسالة المقدّمة من الطالب/ عبد الله محمد الحضري بتاريخ ديسمبر \ ٢٠١٩، وَوُفِقَ عليها كما هو آتٍ:

نحن أعضاء اللجنة المذكورة أدناه، وافقنا على قبول رسالة الطالب المذكور اسمه أعلاه .وحسب معلومات اللجنة فإن هذه الرسالة تتوافق مع متطلبات جامعة قطر، ونحن نوافق على أن تكون جزء من امتحان الطالب.

المشرف على الرسالة

الاسم الدكتور/ أحمد سمير حسنين

مناقش

الاسم الأستاذ الدكتور غنام محمد غنام

مناقش

الاسم الدكتور إياد هارون الدوري

المُلخَّص

عبدالله محمد الحضري، ماجستير في القانون العام

نوفمبر – ٢٠١٩.

العنوان: جريمة الدخول بغير وجه حق إلى المواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطري "دراسة مقارنة"

المشرف على الرسالة: الدكتور/ أحمد سمير حسنين

تقدم هذه الرسالة دراسة قانونية تحليلية مقارنة عن جريمة الدخول بغير وجه حق للمواقع الإلكترونية والنظم المعلوماتية العامة في القانون القطري والقانون المقارن، حيث أن المشرع القطري في قانون مكافحة الجرائم الكترونية القطري الصادر في سنة ٢٠١٤، قد خصص المادة الثانية من القانون بجريمة الدخول بغير وجه حق إذا وقعت على المواقع الإلكترونية أو الأنظمة المعلوماتية التابعة لأحد أجهزة الدولة أو مؤسساتها أو الشركات التابعة لها.

حيث تسلط هذه الدراسة الضوء على محل جريمة الدخول بغير وجه حق وفق المادة الثانية من قانون مكافحة الجرائم الإلكترونية القطري والقوانين المقارنة، حيث أفرد الباحث في هذه الدراسة مبحثاً تحدث فيه عن المحل في جريمة الدخول بغير وجه حق في القوانين المقارنة والقانون القطري، فتحدث في مطلبه الأول عن محل هذه الجريمة بالنسبة للقوانين المقارنة، وخص المطلب الثاني منه بالمحل وفق المادة الثانية من قانون مكافحة الجرائم الإلكترونية القطري. حيث عرف الباحث فيه جميع الجهات التي ذكرها المشرع في المادة الثانية، وبين أسباب حرص المشرع على تضمين هذه الجهات في نص المادة، بالإضافة إلى ذلك تطرق الباحث في هذه الدراسة الى أركان هذه الجريمة والعقوبات المقررة لها وفق القانون القطري والقوانين المقارنة، ومدى تصور الشروع في هذه الجريمة بالنسبة للقانون القطري والقوانين المقارنة.

ABSTRACT

Subject: THE CRIME OF UNAUTHORIZED ACCESS TO PUBLIC WEDSITES AND INFORMATION SYSTEM UNDER THE QATARI ANTI-CYBERCRIMES LAW "COMPARATIVE STUDY"

This thesis brings a legal comparative study on the unauthorized access to public websites and information systems in the Qatari Law and comparative laws, as the Qatari legislator in Cybercrime Prevention Law issued in 2014 stated in the second Article the crime of unlawful access to a website or information system that belongs to. State authority, body, entity or any affiliated corporation.

This study highlights the object/subject matter of the crime of unlawful access as per Article 2 of the Cybercrime Prevention Law and comparative legislations. The researcher focused on the object of unlawful access in comparative legislations and the Qatari Law. The researcher also defined all the entities which are stated by the legislator in the Qatari law, and demonstrated the reasons for the legislator to include these entities in the article. Furthermore, the researcher stated the elements that constitute the crime and the punishment stated in both the Qatari Law and comparative legislations. In addition to exploring the Qatari legislator and comparative legislators' interpretation of "attempting' the crime.

شكر وتقدير

الشكر أوله وآخره لله سبحانه وتعالى أن من علي بنعمة العلم وأرشدني للعمل به

ثم

أتقدم بالشكر والتقدير لكل من ساهم في أنجاز هذا العمل بالدعم المعنوي أو بتقديم النصح والتوجيه.

وارفع شكري وتقديري للدكتور أحمد سمير مشرف هذه الرسالة على كل ما قدمه لي من إرشاد وتوجيه خلال فترة عملي على هذه الرسالة.

كما أتقدم بجزيل الشكر والعرفان لمكتب شرق للمحاماة والاستشارات القانونية من السادة الشركاء الأستاذ/ راشد بن سعد آل سعد، والأستاذ/ حسن محمد المرزوقي، وسعادة المستشار/ عبدالرؤوف البقيعي، وكافة الزملاء والزميلات على كل ما تم تقديمه لي من دعم طوال فترة دراستي للماجستير.

الإهداء

الى والدتي الغالية التي لم تنساني يوما في دعائها ووالدي العزيز وكافة أفراد أسرتي.

الى كل طالب جعل العلم نبراساً يهتدي به.

الى زملائي باحثين القانون العام دفعة ٢٠١٧ / ٢٠١٨ .

أهدي هذا العمل المتواضع، وأرجو من المولى – عز وجل– أن يجعل هذا العلم مما ينتفع به.

فهرس المحتويات

الشكر والتقدير.....ج

الإهداء.....ح

فهرس المحتويات..... خ

المقدمة.....1

المبحث الأول: مفهوم جريمة الدخول بغير وجه حق.....8

المطلب الأول: تاريخ الجرائم الإلكترونية وصولاً إلى جريمة الدخول.....9

المطلب الثاني: تمييز جريمة الدخول عن غيرها من الجرائم التقليدية.....16

الفرع الأول: جريمة الدخول بغير وجه حق وجريمة السرقة التقليدية.....17

الفرع الثاني: جريمة الدخول بغير وجه حق إلى الواقع الافتراضي وجريمة انتهاك حرمة المساكن... 20

المبحث الثاني: المواقع الإلكترونية والنظم المعلوماتية العامة كمحل لجريمة الدخول بغير وجه حق.....24

المطلب الأول: المواقع الإلكترونية والنظم المعلوماتية العامة كمحل للجريمة في القوانين المقارنة.....24

الفرع الأول: موقف التشريعات الأجنبية.....25

الفرع الثاني: موقف التشريعات العربية.....28

الفرع الثالث: شرط الحماية الأمنية للمواقع والنظم المعلوماتية.....31

المطلب الثاني: المواقع الإلكترونية والنظم المعلوماتية العامة كمحل للجريمة في القانون القطري.....33
المبحث الثالث: الركن المادي لجريمة الدخول بغير وجه حق.....41
المطلب الأول: مقصود الدخول بغير وجه حق 42
المطلب الثاني: المقصود بعدم التصريح.....53
المطلب الثالث: الطبيعة القانونية للدخول.....58
المبحث الرابع: الركن المعنوي.....62
المطلب الأول: القصد الإجرامي العام.....62
المطلب الثاني: القصد الجنائي الخاص.....65
المبحث الخامس: العقوبات المقررة لجريمة الدخول بغير وجه حق..... 60
المطلب الأول: العقوبات الأصلية والظروف المشددة.....69
المطلب الثاني: العقاب على الشروع.....73
المطلب الثالث: الإعفاء من العقوبة.....75
الخاتمة.....76
قائمة المصادر والمراجع.....80
مراجع بالغة العربية.....80
مراجع باللغات الأجنبية.....84
مراجع شبكة الأنترنت.....84

المقدمة

تعتبر جريمة الدخول بغير وجه حق إلى المواقع الإلكترونية والنظم المعلوماتية، مدخل وباب يؤدي لارتكاب جميع الجرائم الإلكترونية فلا يتم ارتكاب أي جريمة إلكترونية، بحسب الأصل، إلا بعد الدخول إلي النظام المعلوماتي، ومنذ حدوث ثورة تكنلوجيا المعلومات في بداية القرن العشرين، تم الاعتماد بشكل كبير على الحواسب الآلية في جميع القطاعات، سواء القطاع العام أو القطاع الخاص، فأغلب دول العالم استحدثت نظام الحكومة الإلكترونية الذي يعتمد اعتمادا كلياً على الحاسب الآلي، وكذلك القطاع الخاص فجميع التعاملات البنكية أو التجارية أصبحت من خلال شبكة المعلومات، فأصبح من الملح فرض الحماية الجنائية على الحواسب الآلية، ومعاقبة المخترقين، وذلك للحفاظ على مصالح وأسرار الدول، وكذلك المحافظة على سرية المعاملات البنكية والتجارية، وعلى الصعيد الفردي اصبح الشخص العادي لا يستطع أن يستغني عن الحاسب الألي في حياته اليومية وتعاملاته الشخصية، فأصبح من اللازم حماية الخصوصية الفردية من الانتهاك.

وفي بداية ظهور هذه الجريمة لم تكن التشريعات في كافة الدول تجرم هذه الجريمة، حيث لم تكن هناك أي نصوص تشريعية تتعلق بالجرائم الإلكترونية او بشكل خاص جريمة الدخول بغير وجه حق، اتجه القضاء في بعض الدول الى محاولة تطبيق النصوص العقابية التقليدية على جريمة الدخول، فاتجهت هذه الأنظمة إلى محاولة إسقاط النصوص العقابية الخاصة بجريمة السرقة على هذه الجريمة او تطبيق النصوص العقابية المتعلقة بالدخول الى المساكن، مما أدى ذلك الى صدور احكام غير متناسقة أو معيبة، ومن الدول التي أخذت هذا المسلك بريطانيا.

حيث أتجه القضاء البريطاني قبل صدور القانون المتعلق بأساءه استخدام الحاسوب الالي في ١٩٩٠ بأسقاط النصوص العقابية التقليدية لجريمة السرقة وجريمة دخول ملك الغير على جريمة الدخول بغير وجه حق.

وبعد ذلك تتالت التشريعات العقابية في الدول الى اصدار قوانين خاصة بالجرائم الالكترونية، فصدر في الولايات المتحدة الأمريكية القانون الفدرالي لجرائم الحاسب الآلي لسنه ١٩٨٤، وكذلك صدر القانون البريطاني المتعلق بإساءة استخدام الحاسب الآلي سنة ١٩٩٠.

وتأخرت التشريعات العربية في اصدار تشريعات خاصة بالجرائم الالكتروني، حيث صدرت كافة التشريعات العربية في بداية القرن ٢١، حيث أن اول مشرع خليجي أصدر قانون لمكافحة الجرائم الالكترونية هو المشرع الاماراتي حيث أصدر قانون جرائم تقنية المعلومات الاماراتي سنة ٢٠١٢، وتبعه المشرع القطري والبحريني في عام ٢٠١٤، وبالنسبة للمشرع الكويتي فقد صدور قانون مكافحة جرائم تقنية المعلومات الكويتي لسنة ٢٠١٥، وأحدث التشريعات هو قانون جرائم تقنية المعلومات المصري الصادر في سنة ٢٠١٨.

و جريمة الدخول بغير وجه حق تحتوي على عدة عناصر يجب توافرها من محل وركن مادي وركن معنوي حتى يمكن اعتبارها جريمة تامة، فيجب أن يكون العدوان في هذه الجريمة على موقع الكتروني أو نظام معلوماتي وبغض النظر عن وجود حماية على هذا الموقع، حيث لم تشترط العديد من التشريعات أن يكون هذا النظام أو الموقع الالكتروني محمي بأحد أنظمة الأمن ومن الدول التي انتهجت هذا النهج هي قطر والامارات عمان والبحرين ومصر والسودان، ولكن اشترطت بعض التشريعات أن يكون هذا النظام محمي بأحد أنظمة الحماية حتى يمكن اعتبار الدخول مجرم ومن هذه التشريعات التشريع الكويتي.

وبالنسبة للركن المادي لهذه الجريمة يحتوي على ثلاثة عناصر، فالعنصر الأول هو فعل الدخول ذاته الى النظام المعلوماتي حيث تم تعريف الدخول على أنه" الدخول الى نظام معلومات أو الى

موقع إلكتروني من قبل شخص غير مخول له الدخول، فينتهز الفاعل هذه الفرصة للاطلاع علي ملفات أخرى سرية دون وجه حق" كما يجب أن يكون هذا الدخول من دون أي تصريح من الشخص المسؤول عن هذا النظام، أما بالنسبة لطبيعة هذه الجريمة فهل هي جريمة شكلية أم جريمة ذات نتيجة، فقد اعتبرت بعض التشريعات هذه الجريمة جريمة شكلية أي لا يشترط لوقوعها حدوث نتيجة اجرامية، بينما اتجهت تشريعات أخرى علي اعتبار هذه الجريمة ذات نتيجة أي انها لا تقع الا اذا ترتب على الدخول حدوث نتيجة، وهناك جانب اخر من التشريعات الذي أخذ بمنهج مختلط حيث اعتبر الجريمة شكلية ولكنه غلظ العقوبة في حال حدوث أي ضرر جراء ذلك الدخول.

اما بالنسبة للركن المعنوي في هذه الجريمة فأن الأمر يختلف على حسب اتجاه التشريعات في طبيعة هذه الجريمة، فهناك تشريعات اعتبرتها جريمة شكلية أي لا يتطلب لتمامها وجود أي نتيجة إجرامية، وتشريعات اعتبرتها جريمة ذات نتيجة بحيث لا تعتبر جريمة تمامة الا اذا ترتب على الدخول نتيجة معينة أو ضرر جراء ذلك الدخول

أهمية البحث:

في ظل التطور السريع لتكنولوجيا المعلومات وظهور أجهزة الحاسب الآلي، ظهرت ظواهر سلبية مرتبطة بأجهزة الحاسب الآلي مثل الجرائم الإلكترونية، وهذا يرجع الى الاستخدام السيئ لهذه التكنلوجيا، فأصبح من الصعب تكيف النصوص العقابية التقليدية على مثل هذه الجرائم، فظهرت الحاجة الى سن تشريعات جديدة ومتنوعة، تجرم صور الاعتداء على تكنلوجيا المعلومات، او استعمالها في ارتكاب هذه الجرائم.

كما ان اغلبية التشريعات نصت على تجريم جريمة الدخول الغير المصرح به للأنظمة المعلوماتية، يرجع ذلك لخطورة هذه الجريمة، وتكمن أهميتها في أن جريمة الدخول من الجرائم التي لا يقابلها

جريمة من الجرائم التقليدية، فهي تعتبر من الجرائم الفريدة من نوعها، فغالبية الجرائم الالكترونية الأخرى يوجد ما يقابلها من الجرائم التقليدية ما عادا جريمة الدخول.

مشكلة البحث:

يثير البحث في جريمة الدخول بغير وجه حق عدة إشكاليات سيقوم الباحث في بيانها وهي على النحو التالي:

- ما هو محل جريمة الدخول بغير وجه حق بالنسبة للمادة الثانية من قانون مكافحة جريمة الدخول بغير وجه حق للمواقع الالكترونية العامة؟
- ماهي الجهات التي تضمنتها نص المادة الثانية في قانون مكافحة الجرائم الإلكترونية؟
- السبب الذي دعا المشرع القطري الي تخصيص نص خاص بالجرائم الواقعة على المواقع الإلكترونية والأنظمة المعلوماتية الخاصة بالدولة.
- هل جريمة بغير وجه حق جريمة ذات نتيجة ام هي جريمة شكلية؟
- هل يتصور الشروع في جريمة الدخول بغير وجه حق في القانون القطري؟
- القصد الجنائي في جريمة الدخول هل هو قصد جنائي خاص أم يكفي فيها القصد الجنائي العام.

منهجية البحث

سوف يتبع الباحث في هذا الدراسة المنهج الاستقرائي التحليلي المقارن للوصول الى إجابات علي التساؤلات المطروحة في هذه الدراسة، وذلك من خلال تحليل النصوص القانونية الوطنية، ومقارنتها بالتشريعات العربية والأجنبية مع الاستعانة بآراء الفقهاء والسوابق القضائية.

الدراسات السابقة

الدراسة الأولى:

الدراسة الاولى / نائلة قورة

جرائم الحاسب الالي الاقتصادية، اصدار منشورات الحلبي، سنه ٢٠٠٤.

انقسمت هذه الدراسة الى قسمين، القسم الأول انطوى على باب تمهيدي تم تعريف الجرائم المعلوماتية وخصائصها، والقسم الثاني من هذه الدراسة تحدثت الباحثة عن الجرائم المرتبطة بالحواسب الالية، والتي تضمنت الحديث عن جريمة الدخول بغير وجه حق، ابتدائاً من المحل في هذه الجريمة واركانها المادي والمعنوي منهيه فيها باتجاهات التشريعات المقارنة فيما يتعلق بهذه الجريمة، حيث تحدثت الباحثة عن جريمة الدخول بغير وجه حق بشكلاً عامً عن بداية هذه الجريمة ومواقف التشريعات تجاهها.

وتختلف دراسة الدكتورة نائلة قورة عن دراستنا في أن الأولى قد تكلمت وبشكل عام عن جريمة الدخول بغير وجه حق، ولكن دراستنا جاءت متعمقة في الشق المتعلق في المواقع الالكترونية العامة وبيان كافة الأجهزة والمؤسسات التي ذكرها المشرع القطري في المادة الثانية من قانون مكافحة الجرائم الكترونية، معا بينا كافة الاتجاهات التشريعية المتعلقة بهذه المسألة.

الدراسة الثانية رسالة ماجستير/ محمد سليمان الخوالدة

جريمة الدخول غير المشروع الى موقع الكتروني أو نظام معلوماتي وفق التشريع الأردني: دراسة مقارنة، رسالة ماجستير، ٢٠١٢.

انقسمت هذه الدراسة فصل تمهيدي وثلاث فصول، تحدث فيها الباحث في الفصل التمهيدي هن ماهية الأنظمة المعلوماتية والجرائم الالكترونية مع بيان خصائص الجريمة المعلوماتية، وحدث الباحث في الفصول الثلاث التالية على الفصل التمهيدي عن جريمة الدخول غير المشروع الى

المواقع الالكترونية والأنظمة المعلوماتية في ضوء القانون الأردني، حيث تحدث الباحث عن ماهية الجريمة وماهية الدخول غير المشروع وموقف التشريعات المقارنة اتجاهه.

وتختلف الدراسة السابقة عن دراستنا في أن دراستنا جاءت متعمقة متعلقة بالمواقع الإلكترونية العامة، وبيان كافة الأجهزة والمؤسسات التي ذكرها المشرع القطري في المادة الثانية من قانون مكافحة الجرائم الكترونية، معا بينا كافة الاتجاهات التشريعية المتعلقة بهذه المسألة.

خطة البحث:

المبحث الأول: مفهوم جريمة الدخول بغير وجه حق.

المطلب الأول: تاريخ الجرائم الالكترونية وصولاً الى جريمة الدخول.

المطلب الثاني: تمييز جريمة الدخول عن غيرها من الجرائم التقليدية.

الفرع الأول: جريمة الدخول بغير وجه حق وجريمة السرقة التقليدية.

الفرع الثاني جريمة الدخول بغير وجه حق الي الواقع الافتراضي وجريمة انتهاك حرمة المساكن وملك الغير.

المبحث الثاني: المواقع الإلكترونية والنظم المعلوماتية العامة كمحل لجريمة الدخول بغير وجه حق

المطلب الأول: المواقع الإلكترونية والنظم المعلوماتية العامة كمحل للجريمة في القوانين المقارنة.

الفرع الأول: موقف التشريعات الأجنبية.

الفرع الثاني: موقف التشريعات العربية

الفرع الثالث: شرط الحماية الأمنية للمواقع والنظم المعلوماتية.

المطلب الثاني: المواقع الإلكترونية والنظم المعلوماتية العامة كمحل لجريمة في القانون القطري.

المبحث الثالث: الركن المادي لجريمة الدخول بغير وجه حق.

المطلب الأول: مقصود الدخول بغير وجه حق.

المطلب الثاني: المقصود بعدم التصريح

المطلب الثالث: طبيعة الدخول.

المبحث الرابع: الركن المعنوي.

المطلب الأول: القصد الجنائي العام.

المطلب الثاني: القصد الجنائي الخاص.

المبحث الخامس: العقوبات المقررة لجريمة الدخول بغير وجه حق.

المطلب الأول: العقوبات الأصلية والظروف المشددة.

المطلب الثاني: العقاب على الشروع.

المطلب الثالث: الإعفاء من العقوبة.

المبحث الأول

مفهوم جريمة الدخول بغير وجه حق

إن جرائم الحاسب الآلي هي جرائم حديثة النشأة ظهرت بعد ظهور الحواسب الالية والأنظمة الالكترونية، وذلك لتعلقها بتكنولوجيا المعلومات مما أدى ذلك الى جعل هذه الجرائم صعبة الفهم وغامضة[1]، كل هذا يأتي نتيجة ثورة تكنلوجيا المعلومات والتقدم العلمي الذي شهده العالم خلال العقدين الماضيين، من استغلال العالم للتطور التقني لوسائل التكنولوجيا الحديثة والحواسب الآلية، فكانت الاستفادة من التطور التكنلوجيا للحواسب الآلية للأفراد في حياتهم الشخصية، وللحكومات ايضاً حيث اتجهت اغلبية الحكومات في العالم الي انشاء ما يسمى بالحكومات الإلكترونية "e-Government" ، وأصبحت تقدم العديد من خدماتها الكترونية وبأقل تكلفة مما ذي سبق[2]، وعلى ضوء ما سبق فكان التطور السريع لتكنلوجيا المعلومات والحواسب الآلية دافعاً لظهور العديد من الجرائم المرتبطة بالحواسيب الآلية ومنها جريمة الدخول من غير وجه حق الى النظام المعلوماتي والذي سنناقش تاريخ الجرائم الإلكترونية وصولاً الى جريمة الدخول في المطلب الأول، وتمييزها عن الجرائم التقليدية في المطلب الثاني.

---

[1] - بوريدي مختاره، ماهية الجرائم الإلكترونية، اعمال الملتقى الوطني : آليات مكافحة الجريمة الإلكترونية، الجزائر ، ٢٩ مارس،٢٠١٧، ص٩.

[2] – اكرم المشهداني، "الجرائم الالكترونية"، مجلة الأكاديمية العربية للعلوم المالية والمصرفية، المجلد ٢٣، العدد ١، ٢٠١٥، ص٢٣.

المطلب الأول

تاريخ الجرائم الالكترونية وصولاً الى جريمة الدخول

لقد تم تصميم أول جهاز حاسب ألي في عام ١٩٣٩ من قبل العالمين (أتاناسوف وبيري) وسمي هذا الجهاز (ABC) حيث كان يعمل هذا الجهاز على مبدأ الأنابيب المفرغة، ومع بداية الحرب العالمية الثانية تزايدت المجهودات الى انشاء حواسب الية للأغراض العسكرية فتم إنشاء أول جهاز حاسوب آلي في عام ١٩٤٣ وسمى حاسوب (كولوسس) والذي كان الهدف منه فك شفرات رسائل الألمان من قبل دول الحلفاء، وحتى لا يكون الحاسوب متخصص لفك الشفرات عمل فريق متخصص في جامعة بنسلفانيا في الولايات المتحدة الامريكية على تصميم أجهزة للقيام بعمليات حسابية، وتم عمل أول حاسوب ومكمل الكتروني في عام ١٩٤٦، وقد شهدت الخمسينيات من القرن الماضي أول انتاج تجاري للحواسيب الالية بعيداً عن الاستخدامات العسكرية[3].

وفي نهاية العقد السادس من القرن الماضي كانت الحرب الباردة بين الاتحاد السوفيتي والولايات المتحدة الامريكية فكانت الأخيرة تبحث عن افضل الوسائل لحماية اتصالاتها من الاعتداءات الخارجية فتوجهت الجهود الامريكية الي انشاء رابط بين الحواسيب الالية معاً، وتنفيذا لذلك فقد ظهر بما يسمي "ARRANET" وهي نماذج لربط الحواسب الالية مع بعضها البعض وكانت

[3] - مصطفى عرب ،"جرائم الحاسوب: دراسة مقارنة"،، رسالة ماجستير، ا لجامعة الأردنية، عمان– الأردن،١٩٩٤ ، ص ١١.

آنذاك على نطاق ضيق ،وبما يعرف حالياً (شبكة الانترنت)، وفي بداية الثمانينات اتخذ الانترنت صفحات تجارية بعد أن كانت مقتصرة على الاتصالات التشغيلية والغايات العسكرية البحتة[4].

ومنذ ظهور شبكة الانترنت ظهرت العديد من الجرائم المتصلة بجهاز الحاسب الالي ولقد تعرضت العديد من الحواسب الالية والأنظمة المعلوماتية وبشكلً خاص التي تكون مرتبطة بشبكات المعلومات او كما يسميها البعض "الشبكة العنكبوتية"[5]، الى الاختراق بواسطة بعض الأشخاص الذين ليس لديهم الحق في الدخول الى الحاسب الآلي، حيث كان يتم الدخول الى النظم المعلوماتية أو أجهزة الحاسب الآلي عن طريق برامج خبيثة يتم دمجها في البيانات وأجهزة الحاسب الآلي حتى يتم الحصول على الشفرات الأصلية ليتم من خلالها الدخول الى البرنامج، مثل ما تم في اختراق وكالة ناسا في الولايات المتحدة الأمريكية[6].

واعمالاً بالإعلان العالمي لحقوق الانسان والصادر في باريس ١٠ديسمبر لسنة ١٩٤٨ م والذي تنص المادة ١١ الفقرة الثانية منه على "**لا يُدان أيُّ شخص بجريمة بسبب أيِّ عمل أو امتناع عن عمل لم يكن في حينه يشكِّل جُرمًا بمقتضى القانون الوطني أو الدولي، كما لا تُوقَع عليه أيَّةُ عقوبة أشدَّ من تلك التي كانت ساريةً في الوقت الذي ارتُكب فيه الفعل الجُرمي**" والتي اقرتها

---

[4] – أسامة ألمناعسة– جلال الزعبي، جرائم تقنية المعلومات الالكترونية، الطبعة الثانية، دار الثقافة للنشر، عمان– الأردن، ٢٠١٧، ص ٣٤،٣٥.

[5] تعرف الشبكة العنكبوتية بأنها نظام يعمل على ترابط المستندات ببعضها البعض أو مجموعة من النصوص التي تعمل فوق الانترنت، كما أن البعض قد يخلط ما بين مصطلح الأنترنت والشبكة العنكبوتية، فالأخيرة هي احد الطرق التي تتيح للمستخدم الاتصال بالأنترنت ومشاركة المعلومات والبيانات

[6] – نائلة قورة، جرائم الحاسب الآلي الاقتصادية : دراسة نظرية وتطبيقية، الطبعة الأولي، منشورات الحلبي، مصر، ٢٠٠٤، ص ٣١٥.

معظم الدول في تشريعاتها الداخلية والتي تتضمن في ثناياها مبدأ شرعية الجرائم والعقوبات والتي تعني أن القاضي الجنائي لا يملك إقرار أي جريمة ولا عقوبة جديدة من تلقاء نفسه وانما لتحقق ذلك ينبغي أن يكون هناك تشريع قائم أو صدور تشريع جديد يقضي بتجريم الفعل المراد توقيع العقوبة عليه[7].

كما أنه وبموجب المادة سالفة البيان يحظر ملاحقة أي شخص عن فعل كان قد ارتكبه قبل صدور التشريع القاضي بتجريم الفعل المرتكب أو عن الأفعال التي تشكل جرائم بعد الغاء القوانين المجرمة له، فالتشريعات تعد المصدر الرئيسي لتجريم الأفعال وعقابها فلا مكان لاجتهاد القاضي الجنائي إكمال التشريع الناقص أو استبدال النصوص الجزائية المقررة في القانون الجزائي بنصوص أخرى، فلا يجوز للقاضي تطبيقاً لهذا المبدأ الاجتهاد والتوسع في النصوص الجزائية وانما يجب عليه تطبيق النص الجزائي والالتزام بما تقتضيه القاعدة القانونية المجرمة للفعل، وكان السبب الرئيسي في إقرار هذا المبدأ في معظم التشريعات الداخلية للدول هو اعمالاً بالضمانات الأساسية لحقوق الانسان والتي حرصت معظم التشريعات على تضمينها في نصوصها حماية للأفراد من بطش السلطة التنفيذية، فلا يستطيع الانسان أن يشعر بالأمان اذا كان جاهلاً للتصرفات المباحه والغير مباحه وعقوبتها[8].

---

[7] – الإعلان العالمي لحقوق الأنسان، ١٠ ديسمبر، لسنه ١٩٤٨، باريس، المادة ١١، الرجاء النظر https://www.un.org/ar/universal-declaration-human-rights/index.html.

[8] – حنان المضحكي، الجرائم المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، ٢٠١٤، ص ٥٥.

- ففي المملكة المتحدة كان القضاء قبل صدور قانون ١٩٩٠ والمتعلق بأساءه استخدام الحاسوب الالي بتجريم جرائم الحاسب الآلي كان يطبق القوانين التقليدية في محاولة منه لقياس الجرائم التقليدية علي الجرائم المستحدثة بسبب ظهور ثورة تقنيات المعلومات والحواسب الالية، فكان يطبق القوانين التقليدية على الجرائم الالكترونية بطريقة تم وصفها بأنها عشوائية وغير دقيقة .[9]

ومن أبرز التشريعات التي استخدمها القضاء البريطاني لصبها على الجرائم الالكترونية هو قانون السرقة لعام ١٩٦٨، حيث اعتبر هذا القانون أن الاستيلاء على المعلومات والبيانات المخزنة في اجهزت الحاسب الالي تخرج عن نطاق السرقة الموضح في قانون ١٩٦٨ حيث أن نطاق القانون سالف البيان لا يتعدى المحيط الخارجي لأجهزت الحاسب الالي فقط، ومن هذا المنطلق تزايدت الحاجة في المملكة المتحدة لإصدار قوانين تتناسب مع تزايد الجرائم الواقعة علي الحاسب الالي، حيث استطرد القضاء الإنجليزي في أحاكمه مسبباً عدم اعتبار سرقة البرامج أو البيانات المخزنة في الحاسب الالي لا يمكن أن يطبق عليها نصوص قانون ١٩٦٨ حيث اعتبرها القضاء الإنجليزي أشياء معنوية ليس لها كيان مادي حتى يمكن اعتبار الحصول عليها بمثابة السرقة الواقعة على الاشياء التي لها كيان مادي ملموس[10].

يرى الباحث أن القضاء الإنجليزي قام بتطبيق النصوص التقليدية على جريمة الدخول بغير وجه حق في محاوله منه لقياس الجرائم التقليدية على جرائم الدخول، حيث قام بتطبيق نصوص جريمة

[9] – سامي الرواشدة وأحمد هياجنة، "مكافحة الجرائم المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجا"، المجلة الأردنية في القانون والعلوم السياسية، المجلد ١، العدد٣، ٢٠٠٩، ص ١٢٢،١٢٣.

[10] – سامي الرواشدة وأحمد هياجنة، المرجع نفسه.

السرقة والاحتيال وغيرها من النصوص التقليدية الأخرى على جريمة الدخول بغير وجه حق وذلك قبل صدور تشريعات تجرم الجرائم الالكترونية بشكل عام وجريمة الدخول بشكل خاص، مما أدى ذلك الى صدور احكام غير متناسقة او غير منطقية في هذه القضايا، فكان على القضاء الإنجليزي ومن باب أولى التقيد بمبدأ شرعية الجريمة والعقوبة ، لان ذلك أدى الى الاجتهاد الموسع من قبل القضاء الإنجليزي في النصوص الجزائية والذي يعد بذاته مخالفه صريحة لهذا المبدأ.

وفي الولايات المتحدة الأمريكية كان الظهور الأول لحادثة اختراق الحواسب الآلية من دون أن يكون لديهم حق الدخول حيث تم إطلاق اسم "Hackers" عليهم نسبته إلى الأشخاص الذين كان يعترضون البرامج الاذاعية فيما ما مضى[11].

وكان أول تشريع صدر يتعلق بجريمة الدخول بغير وجه حق كان عن طريق مقترح في الولايات المتحدة الأمريكية على المستوي الفدرالي، بإضافة نص في قانون الفدرالي لجرائم الحاسب الآلي لسنه ١٩٨٤ عن طريق تضمين نص يجرم "الاستخدام غير المصرح به لنظم المعلوماتية"، ولكن لم يؤخذ بهذا المقترح، ولكن في عام ١٩٩٦ صدر تعديل على القانون الفدرالي لجرائم الحاسب الآلي لسنه ١٩٨٤ وتضمن المادة ١٠٣٠ من ذات القانون الفقرة الرابعة على تجريم أفعال الاستخدام الغير مصرح به متى كانت نية الفاعل متجهه الى الحصول علي شيء ذو قيمة ومنها الخدمات التي يقدمها الحاسب الألي متي تجاوزت قيمتها خمس ألاف دولار امريكي[12].

[11] – نائلة قورة، مرجع سابق، ص ٣١٥.

[12] – USC 1030: Fraud and related activity in connection with computers Text contains those laws in effect on November 2, 2019

وفي كندا فقد اضُيف في عام ١٩٨٥ نص يجرم أفعال الاستخدام غير مصرح به، وكذلك القانون الألماني في نفس العام جرم أفعال الاستخدام الغير مصرح به في النظم المعلوماتية او شبكات الانترنت[13].

وبالنسبة للدول العربية فقد تأخرت في اصدار تشريعات خاصة بالجرائم الالكترونية، فكانت المحاكم العربية تعتمد على النصوص العامة الواردة في قانون العقوبات الوطني فيما يتعلق بجريمة الدخول، وقد صدر مؤخراً قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنه ٢٠١٨ والذي تنص المادة ١٤ منه على تجريم الدخول بغير وجه حق الى المواقع الالكترونية[14].

- واما بالنسبة للقانون القطري فقد تضمن قانون العقوبات القطري والذي تنص المادة ٣٧١ منه على أنه "**يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، وبالغرامة التي تزيد عن عشرة الالف ريال او بإحدى هاتين العقوبتين، كل من تواصل بطريق التحايل الي نظام المعالجة الالية للبيانات المحفوظة في جهاز الحاسب الالي او ضبط داخله او في أي جزء منه بدون وجه حق**"[15]

[13] – عمار عباس الحسيني، جرائم الحاسوب والانترنت: الجرائم المعلوماتية، الطبعة الأولى، منشورات زين الحقوقية، بيروت –لبنان، ٢٠١٧، ص ٢٠٥

[14] – قانون مكافحة جرائم تقنية المعلومات المصري، رقم ١٧٥ ،لسنه ٢٠١٨، المادة ١٤.

[15] – قانون العقوبات القطري، رقم ١١، لسنة ٢٠٠٤، المادة ٣٧١.

كما نص قانون ٣٤ لسنة ٢٠٠٦ بشأن اصدار قانون الاتصالات والتي تنص المادة ٦٦ \ ٢ على أنه "**الدخول إلى مرفق أو شبكة للاتصالات أو نظام مرتبط بها عن طريق اختراق الإجراءات الأمنيّة، بقصد الحصول على بيانات أو خدمة اتصالات**[16]."

وهذه كانت محاوله من المشرع القطري قبل صدور قانون خاص بشأن الجرائم الالكترونية في تجريم فعل الدخول الى القنوات وشبكات الاتصال بقصد الحصول على بيانات وخدمات الاتصال بغير حق، فقد نص المشرع القطري على تجريم الدخول الى شبكة الاتصالات بغير حق بقصد تجريم فعل الدخول غير مشروع في ظل غياب قانون خاص أو مواد تجرم فعل الدخول.

وكانت المواد سالفة البيان تطبق على جريمة الدخول بغير وجه حق الى حين صدور قانون مكافحة الجرائم الالكترونية القطري رقم ١٤ لسنة ٢٠١٤ والذي خصص المشرع فيه المواد ٢ و٣ لجريمة الدخول بغير وجه حق، حيث أن المشرع قد فصل جريمة الدخول في المادة الثانية والثالثة مجرماً في المادة الثانية الدخول الى المواقع الالكترونية التابعة للدولة ومؤسساتها المختلفة بغير وجه حق، فضلاً عن تجريمه للدخول بغير وجه حق للمواقع الإلكترونية الخاصة في المادة الثالثة منه.

بعد الاستعراض التاريخي السابق لجريمة الدخول بغير وجه حق سيواصل الباحث دراسته لهذه الجريمة من خلال استعراض الجرائم التقليدية بالنظر الى النصوص التقليدية ومحاولة مقارنتها معا جريمة الدخول بغير وجه حق في المطلب الثاني من المبحث الأول في هذه الدراسة، وذلك للوصول الي مواضع الاختلاف والتوافق بين الجرائم التقليدية وجريمة الدخول بغير وجه حق.

[16] – قانون الاتصالات القطري، رقم ٣٦، لسنة ٢٠٠٦، المادة ٦٦.

المطلب الثاني

تمييز جريمة الدخول مع غيرها من الجرائم التقليدية

ذهب اتجاه في الفقه إلي إمكانية تطويع النصوص العقابية التقليدية مثل جريمة السرقة وخيانة الأمانة ودخول ملك الغير على جريمة الدخول بغير وجه حق، ألا أن هذه المحاولة لم تكتب لها النجاح لما فيها من تشويه المبادئ المستقر عليها والتي تقوم عليها هذه الجرائم حيث أن النصوص التقليدية لا تؤمن الحماية الكافية للمال المعلوماتي والذي يختلف بطبيعته عن المال التقليدي والقول بغير ذلك يؤدي الى ثغرة في نظام حماية الأموال المعلوماتية[17].

فقد تتشابه جريمة الدخول بغير وجه حق الى النظم المعلوماتية مع بعض الجرائم التقليدية مثل جريمة السرقة وجريمة دخول ملك الغير، حيث حاول القضاء الإنجليزي كما اسلف الباحث سابقاً تطبيقها على الجرائم التي تقع على الحاسب الالي ولكن أدى ذلك الى نتائج مأساوية، وسيشرع الباحث في هذا المطلب بدراسة جريمة الدخول عن طريق مقارنتها بالجرائم التقليدية بحيث سيقسم هذا المطلب الي فرعين الفرع الأول: مقارنة جريمة الدخول بجريمة السرقة، والفرع الثاني جريمة الدخول الى الواقع الافتراضي وجريمة دخول ملك الغير في الواقع.

[17] - عبدالفتاح حجازي، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦، ص٣٣٢

الفرع الأول: جريمة الدخول بغير وجه حق وجريمة السرقة التقليدية:

عرفت المادة ٣٣٤ من قانون العقوبات القطري السارق بأنه " **يعد سارق كل من اختلس مالا منقولا مملوكا للغير بنية تملكه**"[18]، يتضح للباحث من خلال النظر في النص السابق أن جريمة السرقة يلزم لتوفرها شرطين الأول: اختلاس المال المنقول، الثاني: عدم رضاء حائز الشيء.

أولاً: اختلاس المال المنقول يتحقق هذا الفعل عن طريق قيام الجاني بأي حركة عضوية من شأنها أن تسلب حيازة الشيء مادياً ومعنوياً من حائزة لحيازته، بحيث يشترط في الحيازة أخراج المال المملوك للغير من حيازة المالك الي حيازة السارق فلا يكون للأول أي علاقة مادية أو معنوي بالشيء [19]

ثانياً: عدم رضاء الحائز: فلا تتم جريمة السرقة بشكل عام عندما يتم اختلاس المال المنقول المملوك للغير، أي بمجرد انتقال الحيازة من مالك الشيء الى السارق، وانما يشترط أن يكون هناك انعدام رضا من المالك عن انتقال الحيازة، ويعد عدم الرضاء عنصر جوهرياً من عناصر جريمة السرقة ويعرف على أنه "عدم توفر الإرادة المدركة الحرة لدى حائز الشيء على التخلي عن حيازته له"[20].

وبالرجوع الى ما سبق يتضح للباحث أن جريمة السرقة يجب أن تقع على شيء مادي ملموس في العالم الواقعي مملوك للغير بحيث يتم سلب حيازة الشيء من مالكه ومن دون رضاه، فاذا تحقق

---

[18] – قانون العقوبات القطري، مرجع سابق، المادة ٣٣٤.

[19] – طارق سرور، قانون العقوبات القسم الخاص : جرائم الاعتداء على الأشخاص والأموال، الطبعة الأولى، لا يوجد دار نشر، كلية القاهرة، مصر، ٢٠٠٤، ص٦١٨ و ٦١٩.

[20] – طارق سرور، مرجع سابق، ص ٦٢٢.

ذلك تعد اركان جريمة السرقة متوافرة حيث أن المعلومات والبيانات المخزنة على الحاسب الألي لا تعتبر من قبيل المنقولات المادية ولا يمكن أضفاء هذه الصفة على المعلومات الا اذا كانت المعلومات من قبيل الأشياء، كما أن المعلومات تختلف عن الأشياء على اعتبار أن هذه المعلومات مخزنة على الوسط المادي الذي يحتوي تلك البيانات وذلك على الرغم من تخزينها على اشرطة أو أقراص مدمجة[21]، وهذا الاتجاه قد عارضه البعض بحيث اعتبر الدخول الى العالم الافتراضي والحصول على البيانات والمعلومات جريمة سرقة ، وعبروا عن ذلك بقولهم أن البيانات والمعلومات المتواجدة في العالم الافتراضي قد تكون ذات قيمة مادية بحيث يمكن أن تطبق عليها النصوص العقابية التقليدية وسموها جريمة السرقة الالكتروني فكانت حججهم كالتالي:

1. بالنسبة الى المال محل السرقة اتجه البعض الي القول بأن البيانات بطبيعتها لا تعتبر كيان مادي له قيمة مالية ولكن قد يتم وضع هذه المعلومات في كيان مادي مستقل عن طريق وضع المعلومات في دعامات وهذه الدعامات قد تكون قابلة للسرقة عندما يتم وضعها في هذه الدعامات مثل الشرائط والاسطوانات فهذه الدعامات بطبيعتها مادية، فالمعلومات والبيانات التي تم نسخها لمرة واحده وتم إعادة نسخها بطريقة غير مشروعة يمكن اعتبار عنصر الاختلاس متوافر وتعتبر سرقة، كما أن البيانات والمعلومات تعد في الأصل من قبيل الأموال المعنوية التي يمكن أن تكون محلاً لجريمة السرقة، حيث وأن الفاعل في حقيقة الأمر يهدف من الحصول عليها الوصول الى شيء أخر أو توظيفها للحصول على مقابل مادي من ورائها.[22]

[21] – عمار عباس حسين، مرجع سابق، ص ١١٤.

[22] – عمار عباس حسين، مرجع سابق، ص ١٢٠ و١٢١.

2. أن يكون محل السرقة منقول اعتبروا أن الأصل في البيانات والمعلومات لا يمكن اعتبارها اموالاً ولكن يمكن أن يتم اعتبارها أموالا بالنظر الى الجانب الاقتصادي منها فاذا كانت هذه البيانات لها قيمة اقتصادية يمكن اسباغ صفة المال عليها، حيث أن المعلومات والبيانات الموجودة في الحاسب الألي تنتقل عبر كابلات وموصلات للطاقة وتقوم الأجهزة والاقسام المادية في الحاسب الالي الى ترجمتها لتكون بصورة معلومة للبشر، وبالتالي فأن المكونات المعنوية اذا رجعنا الى طبيعتها فهي تكون عبارة عن طاقة تنتقل من حيز الى أخر وهذه الطاقة ذات قيمة اقتصادية.[23]

3. أن يكون محل السرقة مملوكاً للغير فالبيانات الشائعة والمتاحة للعامة لا يمكن اعتبار الحصول عليها سرقة، وذلك لأنها متاحة للجميع، أما في حال كون هذه البيانات والمعلومات خاصة لأحد الأشخاص فأن الاستيلاء عليها يعد سرقة وتطبق عليها نصوص جريمة السرقة، وذلك لتوفر شرط ملكية الغير في جريمة السرقة. [24]

4. واتجه البعض الى أن النصوص الواردة في القوانين العقابية جاءت عامة أي أنها لم تشترط أن يكون السلوك المكون للنشاط للركن المادي في جريمة السرقة أن ينصب بحد ذاته الى محل مادي بحت، وبذلك يطبق النص العقابي على كافة المحال سواء كانت مادية أو معنوية.[25]

---

[23] – حنان المضحكي، مرجع سابق، ١٥٩.

[24] – نجوى نجم الدين، "جريمة السرقة عبر الوسائل الإلكترونية: دراسة مقارنة"، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد ٦، العدد٢١ ، ٢٠١٧، ص ٥١٩ الى ٥٢٢.

[25] – عمار عباس حسين، مرجع سابق ، ص ١٢١.

على ضوء ما سبق يرجح الباحث الاتجاه المعارض لتطبيق النصوص العقابية التقليدية وذلك أن النصوص العقابية لجريمة السرقة لا محل لتطبيقها على جريمة الدخول بغير وجه حق، وذلك لأن المعلومات والبيانات المخزنة على الحاسب الالي لا تعتبر من الأموال المادية الملموسة، كما أن النصوص العقابية المتعلقة بجرائم الأموال لا تحمي سوى المنقولات المادية مثل الحاسب نفسه او الاقراص المدمجة أو وحدة المعالجة المركزية حيث تطبق على هذه الجرائم النصوص العقابية التقليدية او بالأخص نصوص جريمة السرقة، ولكن بالنسبة الى البيانات والمعطيات المخزنة داخل الحاسب الالي نفسه هذه تحتاج الى نصوص عقابية خاصه بها مثلما فعل اغلب المشرعين في العالم، وأفردوا لتلك الجرائم نصوص خاص تحتويها وتعاقب على مخالفتها، ومن ناحية أخرى البيانات والمعلومات المخزنة داخل الحاسب الآلي نفسه لا يمكن اختلاسها كون أن الاختلاس كما تم تعريفة سابقاً بأنه سلب حيازة الشيء مادياً أو معنوياً من حائزة أما في هذه الحالة وأن تم نسخ البيانات آلا أنه تبقى نسخة منها لدى مالك الحاسب آلي أو الموقع الالكتروني محل الجريمة، وبذلك ينتفى شرط الاختلاس مما يترتب معه عدم أمكانية تطبيق النصوص التقليدية على هذه الجريمة.

الفرع الثاني: جريمة الدخول بغير وجه حق الى الواقع الافتراضي وجريمة انتهاك حرمة المسكن وملك الغير

تنص المادة ٣٢٣ من قانون العقوبات القطري على أنه "**يُعاقب بالحبس مدة لا تجاوز سنة، وبالغرامة التي لا تزيد على خمسة آلاف ريال، أو بإحدى هاتين العقوبتين، كل من دخل مكاناً مسكوناً أو معداً للسكنى أو أحد ملحقاته، أو محلاً معداً لحفظ المال، وكان ذلك بدون رضا حائزه وفي غير الأحوال التي يُرخص فيها القانون ذلك .**

وتكون العقوبة الحبس مدة لا تجاوز خمس سنوات، إذا كان القصد من الدخول الاعتداء على الحيازة بالقوة، أو بقصد ارتكاب جريمة.

وتكون العقوبة الحبس مدة لا تجاوز عشر سنوات، إذا وقعت الجريمة ليلاً بواسطة كسر أو تسور أو تسلق، أو كان الجاني حاملاً سلاحاً، أو ارتكبت من شخصين فأكثر، أو من شخص انتحل صفة عامة كاذبة، أو ادعى قيامه بخدمة عامة[26]"

بعد استعراض النص السابق يرى الباحث أن هذه الجريمة قد تتشابه مع جريمة الدخول بغير وجه حق وهي دخول المساكن من غير اذن ولكنها مختلفة تماماً عنها.

فالدخول الى المساكن من غير أذن محرم و تستمد المساكن حرمتها من الحق في الحياة الخاصة والتي اقرتها جميع الدساتير والتشريعات في العالم، وتعتبر المساكن من أهم أساليب ممارسة الحياة الخاصة، فيجد الشخص راحته وحريته في مسكنه كما اعتبر البعض المساكن بأنها المقر الرئيسي للحياة الخاصة وجوهرها، فقد حرمة التشريعات الاطلاع على اسرار الأشخاص او فشائها ،من هذه الغاية أتت حرمة المساكن والتي حي جوهر حرمة الحياه الخاصة ومضمونها، والمسكن هو أي مكان يتخذه الأنسان مقر لنفسه فيستوي أن يكون منزلاً أو شقة أو حجرة صغيرة طالما اتخذها الشخص مقراً له، كما اعتبر البعض أن حجر الفنادق تدخل ضمن المساكن ولها حرمتها ولا يجوز دخولها الا وفق الأوضاع التي حددها القانون [27] .

[26] – قانون العقوبات القطري، مرجع سابق، المادة ٣٢٣.

[27] – طارق سرور، مرجع سابق، ص ٤٨٥ و٤٨٦.

- وقد عرفت محكمة النقض المصرية المسكن بأنه "كل مكان يتخذه الشخص مأوي لنفسه على وجه التوقيت أو الدوام بحيث يكون حرماً آمنا لا يباح لغيره دخوله إلا بأذنه "وكذلك محكمة النقض الفرنسية عرفت المسكن بأنه المكان الذي يحق للشخص قانوناً آن يشغله للأنشطة الأسرية ويحتاج إليه الانسان لممارسة أنشطة تعد من صميم الحياة الخاصة [28].

كما اكدت وثيقة حقوق الأنسان علي حرمة المساكن وهذا ما نصت عليه في المادة الثانية عشر منه بأنه "**لا يجوز تعريضُ أحد لتدخُّل تعسُّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حقٌّ في أن يحميه القانونُ من مثل ذلك التدخُّل أو تلك الحملات**[29]"

وعلى ضوء ما سبق يري الباحث ومن خلال النظر في التعريفات السابقة أن المساكن كما تم بيانها في السابق تتمتع بحرمتها وهذا ما اكدت على كافة التشريعات من خلال تضمينها في قوانينها، أي أنه لا يجوز لأي شخص الدخول الى مسكن مملوك للغير من دون الحصول على أذن مالكة بما في ذلك رجالات السلطة العامة، حيث لا يجوز لمأمور الضبط الدخول الى المساكن وتفتيشها ألا بأذن مالكة، الا في الحالات المحددة وعلي سبيل الاستثناء في قوانين الإجراءات ، هذه الجريمة قد تتشابه مع جريمة الدخول إلى الواقع الافتراضي ولكن هل يصح تطبيق النصوص السابقة عليها ؟

---

[28] – محمد عبدالقادر، "التعويض عن الضرر على الاعتداء على حق الأنسان في حرمة مسكنه في ضوء الوثيقة الخضراء الكبرى لحقوق الانسان في عصر الجماهير وبعض النظم المعاصرة"، جامعة بنغازي – كلية الحقوق، لا يوجد رقم للمجلد، العدد ١٧، ٢٠٠٨، ص١٣٩.

[29] – الإعلان العالمي لحقوق الأنسان، مرجع سابق، المادة ١٢.

- للإجابة عن هذا التساؤل يتعين النظر الى مفهوم الدخول نفسه، الدخول هو مصطلح غير جديد كما رأينا سابقاً حيث أن معظم التشريعات تجرم الدخول الي المساكن ولا يوجد أي اختلاف في مفهوم الدخول في الواقع الحقيقي للمساكن، لكن الغموض وصعوبة مفهوم الدخول الى الواقع الافتراضي مفهوم يصعب تحديده كونه مرتبط بالمسائل التقنية، واتجه البعض الى المقارنة والتقريب بين جريمة الدخول في الواقع الحقيقي مع جريمة الدخول الافتراضي للنظام المعلوماتي[30].

يرى الغالب من الفقه أن جريمة الدخول بغير وجه حق تختلف تماما عن جريمة الدخول الى المساكن من حيث الغاية والمحل والسبب ويؤيد الباحث هذا الاتجاه، حيث أن الدخول الى المساكن قد يكون الهدف منه سرقة منقولات في المسكن نفسه، أي أشياء مادية ملموسه، على خلاف الوضع في جريمة الدخول الي العالم الافتراضي والذي يكون فيها الدخول أخطر من الدخول الى المساكن وتكون من الحصول على معلومات وبيانات قد تكون سرية بطبيعتها وقد تهدد الأمن القومي للدولة نفسها، كما أن البيانات والمعطيات لا تكون مادية ملموسة، و محل جريمة الدخول للمساكن هو المنزل المراد دخوله أما في جريمة الدخول بغير وجه حق هو الحاسب الآلي نفسه أو الشبكة المعلوماتية، لذلك لا يمكن تطبيق نصوص جريمة الدخول إلى المساكن وملك الغير على جريمة الدخول بغير وجه حق إلي النظام المعلوماتي، وكما أسلف الباحث سابقاً يترتب على تطبيق النصوص التقليدية على جريمة الدخول بغير وجه حق نتائج خطيرة متمثلة في صدور احكام متناقضة وغير متناسقة من القضاء مما قد يسبب في كثير من الأحيان افلات الجناة من العقاب.

---

[30] – عبد الإله النوايسة، جرائم تكنلوجيا المعلومات: شرح الأحكام الموضوعية لقانون الجرائم الإلكترونية، الطبعة الأولى، دار وائل للنشر والتوزيع، سنه٢٠١٧ ، ص ٣٢و٣٣.

المبحث الثاني

المواقع الإلكترونية والنظم المعلوماتية العامة كمحل لجريمة الدخول في القانون القطري والقانون المقارن

لقد تباينت التشريعات في تحديد المحل في جريمة الدخول بغير وجه حق، فأدى ذلك التباين إلى اختلاف التشريعات في تحديد وبشكل واضح المحل في هذه الجريمة فمنها من اعتبر المواقع الإلكترونية وحدها محل في هذه الجريمة ومنها من اعتبر النظام المعلوماتي، كما أن هناك تشريعات أخرجت المواقع الإلكترونية الغير محمية من نطاق هذه الجريمة، لذلك سيقوم الباحث في هذا المبحث بدراسة محل الجريمة في مطلبين، المطلب الأول المواقع الإلكترونية كمحل لجريمة الدخول بغير وجه حق في القوانين المقارنة، والمطلب الثاني المواقع الإلكترونية كمحل لجريمة الدخول في القانون القطري.

المطلب الأول

المواقع الإلكترونية والنظم المعلوماتية كمحل لجريمة الدخول بغير وجه حق في القوانين المقارنة

لقد تباينت التشريعات في العالم حول تحديد محل جريمة الدخول بغير وجه فمن التشريعات اعتبر النظام المعلوماتي والمواقع الإلكتروني محل لهذه الجريمة، ومنها من اعتبر الحاسب الآلي وحده محل لهذه الجريمة ومنها من جمع بينهما.

كما أن هناك تشريعات اشترطت أن يكون النظام محيمي بوسائل حماية أمنية حتى تشمله الحماية الجنائية، لذلك سيقوم الباحث بدراسات موقف التشريعات الأجنبية في الفرع الأول، وموقف

التشريعات العربية في الفرع الثاني، والفرع الثالث سيتناول شرط الحماية الأمنية للمواقع الإلكترونية والنظم المعلوماتية

الفرع الأول موقف التشريعات الأجنبية:

لقد اختلفت التشريعات الأجنبية في تحديد محل جريمة الدخول بغير وجه فمن التشريعات اعتبر الحاسب الالي محلاً لجريمة الدخول، وهناك تشريعات أعتبرت النظام المعلوماتي والشبكات المعلوماتية محل لهذه الجريمة.

أولاً التشريعات التي اعتبرت الحاسب الالي محل لجريمة الدخول:

- في الولايات المتحدة الأمريكية تجرم المادة ١٠٣٠ (أ) من القانون الفيدرالي الخاص بأساءه استخدام الحاسب الآلي للحصول على معلومات عن طريق الدخول الغير مصرح به الى الحاسب الآلي، وكذألك جرمت المادة ١٠٣٠ (أ) (٣) من القانون ذاته الدخول المجرد الى الحواسب الآلية التابعة للحكومة الأمريكية، او تلك التي يؤدي الدخول إليها المساس بمتعلقات الحكومة الأمريكية وبياناتها، وعرفت المادة السابقة المقصود بالحاسب الآلي، ويقصد به أي جهاز إلكتروني أو كيمائي كهربائي أو جهاز سريع المعالجة المعلومات يقوم بأجراء عمليات منطقية وحسابية،. بحيث قصد المشرع الأمريكي في تعريفه للحاسب الالي النظام المعلوماتي من خلال ذكرة لكيفية عمل الحاسب الالي من حيث معالجة المعلومات. [31]

في القانون الإنجليزي فالمادة الأولى من قانون إساءة استخدام الحاسب الآلي، تجرم فعل الدخول الغير مصرح به الى نظام الحاسب الآلي الذي يحتوي على المعلومات[32]، وأثار نص

[31] –USC 1030: Fraud and related activity in connection with computersText contains those laws in effect on November 2, 2019

[32] - قانون إساءة استخدام الحاسب الآلي البريطاني ، الرجاء النظر:

المادة السابقة جدلا كبير، وذلك لأن المادة لم تحدد المقصود بالحاسب الألي، ولم تتطلب أن يتم الدخول الى أنظمة المعلومات أو الشبكة المعلوماتية، بل تطلبت أن يتم الدخول الى المعلومات المخزنة في الجهاز الحاسب الآلي نفسه[33].

وأول تطبيق لنص المادة السالف ذكرها تم في عام ١٩٩٠، عندما قام أحد الأشخاص بزيارة زميلة السابق في أحد المتاجر، فقام المتهم بإدخال تعليمات الى جهاز الحاسب الآلي يتم بمقتضاها عمل خصم ٧٠ ٪ من قيمة السلع المعروضة، فتم تقديم المتهم الى المحكمة بتهمة الدخول الغير مصرح به إلى جهاز الحاسب الآلي، ألا أن محكمة أول درجة قامت بتبرئة المتهم من هذه التهمة، أستنادً الى أن نص المادة السابقة تتطلب الدخول إلى الحاسب الآلي عن طريق حاسب ألي أخرى، أي أن محل الجريمة وفق نص المادة الأولى ينصب على المعلومات المخزنة داخل الحاسب الآلي الذي يتم الدخول إليه وليس الحاسب الآلي المستخدم في عملية الدخول الغير مصرح به، ولكن محكمة الاستئناف ألغت حكم المحكمة المتقدم، وجاء في حكمها أنه لا يجب تحميل عبارات النص أكثر مما تتحمل [34].

وبالنسبة للقانون البلجيكي فقد جعل المحل في جريمة الدخول نظام الحاسب الالي[35]، وجعل القانون اليوناني محل جريمة الدخول البيانات المخزنة على الحاسب الآلي[36]، وكذلك أخذ ذات

---

https://www.legislation.gov.uk/ukpga/1990/18/section/1. 9/11/2019.

[33] – نائلة قورة، مرجع سابق، ص ٣٢٦.

[34] – نائلة قورة، المرجع نفسة.

[35] - قانون العقوبات البلجيكي، الرجاء النظر:

9/11/2019 https://www.cybercrimelaw.net/Belgium.html.

[36] قانون الجرائم الالكترونية اليوناني، الرجاء النظر:

9/11/2019. https://www.cybercrimelaw.net/Grecce.html.-

الاتجاه القانون النيوزلندي حين جعل الحاسب الآلي والمعالج محلاً لجريمة الدخول بغير وجه حق [37].

ثانياً: التشريعات التي اعتبرت النظم والشبكات المعلوماتية محلاً للجريمة:

- بالرجوع التشريعات الأجنبية نجد أن المشرع الفرنسي في المادة ١-٣٢٣ من قانون العقوبات قد جرم فعل الدخول أو البقاء غير المشروع داخل نظم المعالجة الآلية للمعلومات[38]، فالمادة السابقة تجرم الدخول إلى النظام أو إلى أي جزء منه كشرط لقيام هذه الجريمة، أي أن الجريمة لا تقوم ألا بالدخول الى عنصر من عناصر النظام المعلوماتي الذي يحتوي على معلومات متى كان بمعزل عن نظام المعالجة الآلية للمعلومات[39].
- وفي الدنمارك قد جرم قانون العقوبات الدخول الغير مصرح به إلى المعلومات من البرامج التي يتم تخصيصها للاستعمال داخل نظام المعالجة الآلية للمعلومات، ويشمل نص التجريم شبكات المعلومات، وفي أستراليا قانون العقوبات اعتبر محل جريمة الدخول بغير وجه حق أنظمة الحاسب الالي شريطة ان يتم الدخول اليها بواسطة شبكات المعلومات[40]

---

[37] – قانون الجرائم النيوزلندي، الرجاء النظر:

9/11/2019.http://www.legislation.govt.nz/act/public/1961/0043/latest/DLM330422.html

[38] - French criminal code, o*rdinance no. 2000-916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January 2002, (Act no. 2004-575 of 21 June 2004 article 45 I Official Journal of 22 June 2004.*

[39] دينا فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي، الطبعة الأولى ، دار النهضة العربية و دار النهضة العلمية الإمارات، ٢٠١٨، ص ٧٢و ٧٣.

[40] قانون العقوبات الأسترالي، الرجاء النظر:

https://www.coe.int/en/web/octopus/country-legislative-profile/--/asset_publisher/LA6eR74aAohY/content/denma-1?_101_INSTANCE_LA6eR74aAohY_viewMode=view#article2.9/11/2019

- كما جعل القانون الإيطالي المحل في جريمة الدخول هو نظام الحاسب الالي أو نظام الاتصالات والمقصود بنظام الاتصالات الشبكات المعلوماتية، وبالنسبة لدولة بيرو فأن محل جريمة الدخول بغير وجه حق هو انظام الحاسب الالي أو شبكة الانترنت[41].

الفرع الثاني: موقف التشريعات العربية

بالنسبة للتشريعات العربية فقد نص المشرع الأردني على تجريم جريمة الدخول بغير وجه حق، حيث جرمت المادة الثالثة من قانون الجرائم الإلكترونية الأردني جريمة الدخول الغير مشروع على انه" يعاقب كل من دخل قصداً إلى الشبكة الخصوصية أو نظام معلومات بأي وسيلة"، أي أن القانون الأردني نص على أن المحل في جريمة الدخول الغير مصرح به يجب أن يكون الشبكة المعلوماتي أو نظام معلوماتي 42.

وعلى ضوء ذلك فأن الباحث يرى أن تجريم الدخول الغير مصرح به في التشريع الأردني منوط بأن يتم الدخول إلى موقع إلكتروني أو نظام معلومات، ويفهم من ذلك ان المشرع الأردني وسع من مفهوم الحماية، في جريمة الدخول الغير مصرح به، فلم يقصر الحماية الجنائية على المواقع المحمية بوسائل حماية أمن المعلومات، بل جعلها عامه بحيث تشمل جميع المواقع الإلكترونية.

واتفق المشرع المصري مع المشرع الأردني حيث نصت المادة ١٤ من قانون مكافحة جرائم تقنية المعلومات المصري على أن "يعاقب بالحبس مدة لا تقل عن سنه وبغرامة لا تقل عن خمسين ألف جنيه أو بأحد هاتين العقوبتين، كل من دخل عمداً أو دخل بخطأ غير عمدي وبقى بدون وجه

---

[41] – قانون الجرائم الالكترونية الإيطالي، الرجاء النظر:
https://www.cybercrimelaw.net/Italy.html.9/11/2019

[42] – عبد الإله النوايسة، المرجع السابق ٢٠٧.

حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه"[43]، حيث أن المشرع المصري واعتبر أن النظم المعلوماتية والمواقع الالكترونية هي أحدى محال جريمة الدخول بغير وجه حق.

وسار على هذا النهج المشرع السوداني حين نص في المادة الرابعة من قانون جرائم المعلوماتية لسنه ٢٠٠٧ على محل الجريمة وأعتبر النظام المعلوماتي والمواقع الالكترونية محالاً لهذه الجريمة[44]، ونصت المادة ١٥ من قانون تنظيم التواصل على الشبكة ومكافحة الجرائم المعلوماتية السوري على محل جريمة الدخول الغير مشروع واعتبرت النظم المعلوماتية والمواقع الالكترونية محلاً للجريمة[45].

وبالنسبة للتشريعات الخليجية فقد نص المشرع العماني في المادة الثالثة من قانون مكافحة جرائم تقنية المعلومات على أنه "يعاقب بالسجن فترة لا تقل عن شهر ولا تزيد عن سته أشهر وبالغرامة التي لا تقل عن مائة ريال عماني ولا تزيد عن خمسمائة ريال عماني أو بأحد هاتين العقوبتين، كل من دخل عمداً ومن دون وجه حق موقعاً الكترونياً أو نظماً معلوماتياً أو وسائل تقنية المعلومات أو جزء منها أو تجاوز الدخول المصرح به اليها او استمر فيها بعد علمه بذلك"[46]

ونصت المادة الثانية من قانون جرائم تقنية المعلومات الاماراتي على المحل في جريمة الدخول بغير وجه حق واعتبرت ايضاً المواقع الالكترونية والنظم المعلوماتية محل لهذه الجريمة[47]، واعتبر المشرع الكويتي ايضاً النظام المعلوماتي أو الموقع الكتروني محلاً لجريمة الدخول بغير وجه

---

[43] قانون مكافحة جرائم تقنية المعلومات المصري، مرجع سابق، المادة ١٤.

[44] – قانون جرائم المعلوماتية السوداني، القانون رقم ١٣، الصادر في سنه ٢٠٠٧، المادة الرابعة.

[45] – قانون تنظيم التواصل على الشبكة ومكافحة الجرائم المعلوماتية السوري، ١٧، لسنه ٢٠١٢، المادة ١٥.

[46] – قانون مكافحة تقنية المعلومات العماني، الصادر بمرسوم سلطاني رقم ١٢، سنه ٢٠١٢، المادة الثالثة.

[47] – قانون جرائم تقنية المعلومات الاماراتي، مرسوم اتحادي رقم ٥، لسنه ٢٠١٢، المادة الثانية.

حق،[48] واما بالنسبة للتشريعات الخليجية التي اختلفت فهو التشريع السعودي الذي اعتبر الموقع الالكتروني وحده محل للجريمة[49]، والمشرع البحريني الذي اعتبر النظام المعلوماتي محل للجريمة من دون المواقع الالكترونية ولم ينص عليها صراحة[50].

- بعد استعراض التشريعات الأجنبية والعربية المقارنة، عن محل جريمة الدخول بغير وجه حق ، نجد ان هناك دول توسعت في محل الجريمة، كما ان هناك دول أخرى ضيقت من مفهوم جريمة الدخول، وهذا ينعكس بالضرورة على النص التجريم ، وذلك لان محل الجريمة يكون على مدى الوسائل او الأجهزة التقنية التي ضمنها المشرع نص التجريم، أي وأن قام المشرع بتحديد محل جريمة الدخول الغير مصرح به ألا أن الولوج الغير مصرح به إلى جهاز الحاسب الآلي يحتاج الى رأي اهل الخبرة في مجل تقنية المعلومات وذلك بسبب التطور الدوري والمستمر في هذا المجال فمن المكن يؤدي التطور الى ظهور أشياء جديدة في المستقبل يتم اعتبارها محل لهذه الجريمة، ويرى الباحث أن أغلبية التشريعات العربية اتفقت على أن محل جريمة الدخول بغير وجه حق هو النظام المعلوماتي والمواقع الالكترونية، ما عاد التشريع البحريني والسعودي حيث أفرد كلاً من المشرعين محلاً للجريمة، فاعتبر المشرع البحريني

---

[48] – قانون مكافحة الجرائم المعلوماتية الكويتي، رقم ٦٣، لسنة ٢٠١٥، المادة الثانية.

[49] الرجاء النظر الى القانون السعودي :

https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf، ٢٠١٩\١٠\١٧.

[50] –قانون جرائم تقنية المعلومات البحريني، رقم ٦٠، لسنة، ٢٠١٤، المادة الثانية.

النظام المعلوماتي وحده محلاً للجريمة، بينما اعتبر المنظم السعودي المواقع الإلكترونية محلاً للجريمة. [51]

الفرع الثالث: شرط الحماية الأمنية للمواقع والنظم المعلوماتية

لقد تباينت التشريعات وانقسمت الآراء الفقهية حول اشتراط الحماية الأمنية للمواقع الالكترونية حتى يمكن اضفاء الحماية الجنائية عليها، فذهب أتجاه الى عدم أضفى الحماية الجنائية على المواقع الالكترونية غير محمية بحماية أمنية، وذهب اتجاه أخر الى ضرورة حماية كافة المواقع جنائياً سواء كانت محمية بحماية أمنية أم غير محمية.

فقد ذهب جانب من فقهاء القانون الى اعتبار المواقع والأنظمة المعلوماتية المحمية بوسائل أمنية أجدر بأن تكون تحت الحماية الجنائية، وقاس هذا الجانب من الفقه المواقع والنظم المعلوماتية المحمية بجريمة انتهاك حرمة المنازل فلا يشترط في الأخيرة أن يتم فقط الدخول بغير رضاء صاحب المسكن، بل يجب أن يصحب هذا الدخول نشاط أخر حتى تقع هذه الجريمة مثل التهديد أو الاحتيال، واستند أنصار هذا الاتجاه أنه وبالنظر الى طبيعة الأنظمة المعلوماتية والحواسب الالية وما تحتويه على معلومات قد تكون مهمة وحساسة في بعض الأحيان تقتضي من المسؤولين عن الأنظمة المعلوماتية وضع برامج لحمايتها، واستندوا ايضاً أنه في حال وجود أنظمة أمنية لحماية هذه المواقع أو الأنظمة المعلوماتية وحاول أحد الأشخاص الدخول بغير وجه حق ففي هذه

---

[51] لقد نصت المادة من نظام مكافحة الجرائم المعلوماتية السعودي على أنه" يعاقب بالسجن مدة لا تزيد عن سنه وبالغرامة التي لا تزيد عن خمسمائة ألف ريال أو بأحد هاتين العقوبتين كل شخص يرتكب أيا من الجرائم المعلوماتية التالية:
٣- الدخول غير المشروع الى موقع الكتروني، أو الدخول الى موقع الكتروني لتغير تصاميم هذا الموقع او اتلافه أو تعديله أو شغل عنوانه"
ونصت المادة الثانية من قانون جرائم تقنية المعلومات البحريني على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز ثلاثين ألف دينار أو بإحدى هاتين العقوبتين، من قام دون مسوغ قانوني بالدخول إلى نظام تقنية المعلومات أو جزء منه."

الحالة يتوفر دليل قاطع على نية هذا الفاعل من الدخول، وبالتالي يسهل التحقق من توافر القصد الجنائي من خلال الأثر الذي تسبب به الفاعل اثناء محاولته للدخول الى النظام[52].

أما **الاتجاه الثاني** فلا يرى ضرورة من وجود أنظمة حماية على المواقع أو النظم المعلوماتية وقاس هذا الاتجاه على جريمة السرقة حيث أن الحماية الجنائية للمال متوافرة سواء كان صاحب هذا المال وفر الحماية لماله أم لا، كما ذهب أصحاب هذا الاتجاه الى أن وجود شرط الحماية على المواقع والأنظمة المعلوماتية يضيق من نطاق الحماية الجنائية لجريمة الدخول بغير وجه حق ويقصر الحماية على المواقع المحمية من دون الأخرى مما يؤدي الى افلات الكثير من الجناة من طائلة العقاب، كما أنه لا يشترط النظر إلى الحماية كشرط لتجريم الدخول بل يمكن اعتباره مجرد قرينة على الدخول.[53]

ولقد تباينت التشريعات بشأن وجوب توفر الحماية الأمنية فمنها من اشترط الحماية الأمنية 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 ان يتم الدخول الغير مصرح به الى حاسوب آلي محمي، ويقصد بالحماية هنا احد أجهزة المؤسسات المالية أو الحكومية الفدرالية، أو بالتجارة الأجنبية، ولم يشترط المشرع الفرنسي أن يكون النظام المعلوماتي محمي بأحد وسائل الحماية مثل الحائط الناري، أو كلمة مستخدم وكلمة سر، بل جعل التجريم يشمل المواقع المحمية والغير محمية[54]

---

[52] – نائلة قورة، مرجع سابق، ٣٥٤ و ٣٥٥.

[53] – سامي الرواشدة واحمد الهياجنة، مرجع سابق ١٣٤.

[54] – شيماء عبدالغني، " الحماية الجنائية للتعاملات الإلكترونية"، رسالة دكتوراه، جامعة المنصورة – كلية الحقوق– ٢٠٠٧، ص ١١٨

وعلى صعيد الدول العربية لم تشترط الدول العربية مثل هذا الشرط سوى التشريع الكويتي الذي اشترط أن يتم الاختراق الى أحد الأنظمة المعلوماتية المحمية بأحد وسائل حماية أمن المعلومات، بينما لم تتطلب أغلبية التشريعات أن يكون النظام المعلوماتي محمي بأحد وسائل الحماية [55].

ويؤيد الباحث التشريعات التي لم تتطلب أن يكون النظام المعلوماتي محمي بأحد وسائل حماية أمن المعلومات، وذلك لان الحماية الجنائية في هذه الحالة تشمل الأنظمة المعلوماتية المحمية، والأنظمة الغير محمية، مما يؤدي الى تضيق الخناق أمام مرتكبي هذه الجرائم.

المطلب الثاني

الموقع الإلكتروني والنظم المعلوماتية العامة كمحل لجريمة الدخول في القانون القطري

لقد اتفقت أغلب التشريعات التي سبق الإشارة اليها في هذه الدراسة إلى اعتبار المواقع الإلكترونية والنظم المعلوماتية محل جريمة الدخول بغير وجه حق، وانتهج المشرع القطري ذات النهج وجرم في المادة الثانية من قانون مكافحة الجرائم القطري جريمة الدخول بغير وجه حق واعتبر المواقع الإلكترونية والنظم المعلوماتية محلاً لهذه الجريمة ولكنه خصص المادة سابقة الذكر للمواقع الإلكترونية والنظم المعلوماتية التابعة لأحد أجهزة الدولة أو مؤسساتها آو هيئاتها أو الجهات أو الشركات التابعة لها، وأفرد المشرع القطري المادة الثالثة من ذات القانون للمواقع الإلكترونية والنظم المعلوماتية العامة حيث شملت الحماية الجنائية في القانون القطري المواقع الإلكترونية العامة

[55] – عبد الإله النوايسة، المرجع نفسه .

والخاصة، وعلى ضوء ما سبق سيواصل الباحث دراسته في هذا المطلب لمحل جريمة الدخول بغير وجه حق كما هو وارد في المادة الثانية من قانون مكافحة الجرائم الإلكترونية القطري.

لقد نص المشرع القطري في المادة الثانية من قانون مكافحة الجرائم الإلكترونية رقم 14 لسنة 2014 على "**يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها.**

وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحقة.".

وبذلك شمل نص المادة الثانية من قانون مكافحة الجرائم الإلكترونية على المواقع الإلكترونية والأنظمة المعلوماتية واعتبرهما محل للجريمة، وسنبين كلاً منهم كالتالي:

أولاً: المواقع الإلكترونية:

لم يغفل المشرع القطري عن تعريف الموقع الإلكتروني فقد عرفته المادة الأولى من القانون، بأنه "مكان إتاحة أو معالجة البيانات أو المعلومات الإلكترونية على الشبكة المعلوماتية من خلال عنوان محدد.[56]

وقد عرفه الفقه بأنه "هو مكان أتاحة المعلومات على شبكة الانترنت من خلال عنوان محدد" وايضاً تم تعريف ماهية المواقع الالكترونية بأنها "نظام معلومات نشط يعمل على الأنترنت له طابع اتصال عالمي متفاعل يخترق الحدود بأسلوب الربط الصوري"[57]،

وتعتبر المواقع الالكترونية من أهم طرق التواصل استخداماً في ظل ثورة تكنلوجيا المعلومات، وقد تزايد استخدمها في الآونة الأخيرة بحيث بلغ عدد المواقع بناء على الإحصائيات التي أعلنت عنها شركة نيتكرافت لمراقبة الإنترنت إلى ١٠٠ مليون موقع الكتروني في عام ٢٠٠٦[58].

كما أن جميع المواقع الإلكترونية التي يتم أنشائها تحتوي على ما يسمى بالعناوين الخاصة أو ما يطلق عليها بالدومين، حيث أن الفائدة المترتبة على العنوان أو الدومين يمكن المتصفح من الوصول إلى الموقع الالكتروني ذاته، والمواقع الالكترونية تنقسم الى قسمين مواقع الأنترنت العامة أو الدولية وموقع الوطنية أو المحلية، فالمواقع العامة أو الدولية هي المواقع التي لا تنتمي الى

---

[56]– قانون مكافحة الجرائم الالكترونية القطري، ١٤، لسنة ٢٠١٤ ، المادة الأولى.

[57] – محمد سليمان الخوالدة، جريمة الدخول غير المشروع الى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني: دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية "كلية الدراسات العليا"، الأردن ، ٢٠١٢، ص ٨.

[58] – محمد سليمان الخوالدة، المرجع نفسه، ص٨.

دولة معينة بحيث يكون محتواها موجه الى جميع الأشخاص في العالم ممن يملكون القدرة على الوصول الى الشبكة المعلوماتية، أما بالنسبة الى المواقع المحلية فهي التي تتبع في غالب الأوقات الى مؤسسات الدولة المختلفة وتحمل في نهايتها رمز يرمز لذات الدولة فعلى سبيل المثال موقع وزارة التعليم العالي في قطر http://www.edu.gov.qa يحتوي في نهاية على اختصار لأسم دولة قطر Qatar، حيث أن الهدف من أنشاء هذه المواقع هو خدمة من هم على أرض قطر.[59]

ثانياً: نظام المعلومات

لقد عرف قانون مكافحة الجرائم الالكترونية القطري النظم المعلوماتية بأنها" مجموعة برامج وأجهزة، تستخدم لإنشاء أو استخراج المعلومات، أو إرسالها، أو استلامها، أو عرضها، أو معالجتها، أو تخزينه"[60].

وعرف الفقه نظام المعلومات بأنه "هو نظام يتكون من أشخاص وسجلات البيانات وعمليات يدوية وغير يدوية ويقوم هذا النظام بمعالجة البيانات والمعلومات في أي منظومة" أو هو مجموعة من العناصر المتدخلة التي تعمل مع بعضها البعض لجمع ومعالجة وتخزين وتوزيع المعلومات المتوفرة عن موضوع ما يشكل منهجي لدعم اتخاذ القرار ولدعم التنظيم والتحكيم والتحليل في والمنظمة وبناء تصور حالي ومستقبلي واضح"[61]

ويمكن تعريف نظم المعلومات "بأنها جملة أنظمة مترابطة تتكون من البيانات والسجلات ومجموعة أشخاص تربطهم علاقة وظيفية أو اجتماعية حيث تم من خلالهم العديد من العمليات اليدوية والغير يدوية، إذ تعالج النظم كل البيانات والمعلومات الخاصة بمنظمة ما أو حالة ما، فهي

---

[59] –محمد سلمان خوالدة، مرجع سابق، ص ٩ وما بعدها.

[60] - قانون مكافحة الجرائم الالكترونية القطري، مرجع سابق، المادة الأولى.

[61] –محمد سليمان خوالدة، مرجع سابق١٦.

العناصر المتداخلة فيما بينها كما أنها تعمل بنسق معين بهدف معالجة المعلومات، حيث تستند عملية المعالجة إلى التحكم المنظم بها، كما إن الأنظمة المتعددة للمعلومات والتي تستخدم بهدف معالجة المعلومات ككل تعمل من خلال مجموعة عمليات منظمة بغية الاستفادة القصوى من البيانات من خلال تنظيمها وإدارتها بالطرق المُثلى[62]."

وقد اشترطت المادة سابقة الذكر أن يكون الدخول منصب على أحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها:

ويقصد بأحد أجهزة الدولة الوزارات والمرافق العامة التي تديرها الدولة وتكون تابعة لها تبعية كلية، والمرافق العامة هي التي تهدف الى تحقيق المصلحة العامة وخدمة الأفراد في المجتمع، حيث تم تعريفها بأنها "الجهاز الإداري أو الهيئة التي تقوم بتقديم خدمات عامة، بغرض اشباع حاجات الجمهور" وقد عرفها الفقيه هوريو بأنها "منظمة عامة تتمتع بالسلطات والاختصاصات التي تكفل لها القيام بخدمات تقدمها للجمهور بشكل منتظم، أو هو نشاط إداري يتولاه شخص معنوي عام لإشباع حاجة جماعية[63]"

وقد تم تعريف المؤسسة العمومية في قانون الهيئات والمؤسسات العامة بأنها " **المؤسسة العامة شخص اعتباري عام يقوم على إدارة مرفق عام اقتصادي أو يهدف إلى استغلال مورد من موارد الثروة الطبيعية أو المشاركة في التنمية الاقتصادية، وتدار على أسس تجارية"[64]**

---

[62] – الرجاء النظر الى مقالة تتحدث عن نظم المعلومات في الموقع الالكتروني أدناه :
https://weziwezi.com/أنواع-نظم-المعلومات ، تاريخ الزيارة ٢٠١٩/٩/٣٠.

[63] –الرجاء النظر :
https://elawpedia.com/view/67/تعريف-المرفق-العام-والعناصر-المميزة-له تاريخ الزيارة ٢٠١٩/١٠/١٩.

[64] – قانون الهيئات والمؤسسات العامة، رقم ٢٦، لسنه٢٠٠٤، المادة ٥

وتم تعريفها في الفقه " بأنها هو مرفق عام يُمنح الشخصية المعنوية عن طريق تطبيق فكرة اللامركزية الإدارية، حيث أن المؤسسة هي شخصية معنوية تمنح المرفق العام تنظيماً إداريا يتمتع بقدر من الاستقلالية نتيجة منحة شخصية المعنوية 65، وقد عرف القانون ذاته الهيئة بأنها " **الهيئة العامة شخص اعتباري عام يقوم على إدارة مرفق عام غير اقتصادي أو يهدف إلى تقديم خدمة عامة**"[66].

وعرفت المادة الثانية من قانون المؤسسات الخاصة ذات النفع العام المؤسسة الخاصة بأنها "**منشأة يؤسسها شخص أو أكثر من الأشخاص الطبيعيين أو المعنويين، لتحقيق غرض أو أكثر من أغراض النفع العام.**

ويكون للمؤسسة شخصية معنوية وذمة مالية مستقلة"[67].

كما يقصد بالشركات التابعة للدولة هي الشركات التي تساهم فيها الدولة أو أحد مؤسساتها أو هيئاتها بنسبة ٥١٪ من راس المال حيث نصت المادة ٢٠٧ من قانون الشركات القطري على أنه" **للحكومة وغيرها من الهيئات والمؤسسات العامة، والشركات التي تساهم فيها الدولة بنسبة لا تقل عن (51%) أو بنسبة تقل عن ذلك بشرط موافقة مجلس الوزراء ، تأسيس شركة مساهمة خاصة أو أكثر بمفردها أو بالاشتراك مع مؤسس آخر أو أكثر، وطنياً أو أجنبياً، وسواء كان شخصاً طبيعياً أم معنوياً عاماً أو خاصاً، ولا تخضع هذه الشركات لأحكام هذا القانون، إلا بالقدر**

---

[65] – بوزيد غلابي، مفهوم المؤسسة العمومية، ،رسالة ماجستير، جامعة العربي بومهدي أبو البوقي، الجزائر، ٢٠١١، ص١٥، الرجاء النظر –http://bib.univ

oeb.dz:8080/jspui/bitstream/123456789/213/1/مفهوم%20المؤسسة%20العمومية.pdf ، تاريخ الزيارة ٢٠١٩\٩\٣٠.

[66] – قانون الهيئات والمؤسسات العامة، مرجع سابق، المادة ١.

[67] –قانون المؤسسات الخاصة ذات النفع العام، رقم ٢١، لسنة ٢٠٠٦.

الذي لا يتعارض مع الأوضاع والاتفاقيات التي عقدت في ظلها أو عند تأسيسها، والأحكام المنصوص عليها في عقد تأسيسها ونظامها الأساسي."[68]

وبالرجوع إلى النصوص القانونية سالفة البيان يرى الباحث أن المشرع القطري وفي سبيل حماية أمن المعلومات والبيانات في النظم المعلوماتية التابعة للدولة أفرد المادة الثانية من قانون مكافحة الجرائم الإلكترونية لتجريم الدخول بغير وجه حق إلى المواقع الإلكترونية أو النظم المعلوماتية التي تتبع لأحد أجهزة الدولة أو مؤسساتها أو الشركات التابعة لها، وذلك لعدة أسباب، الأول لما في هذه المواقع أو الأنظمة المعلوماتية من حرمه لبياناتها ومعلوماتها، كون أن المواقع الإلكترونية التابعة لأحد أجهزة الدولة هو أحد الطرق الرسمية للتواصل مع المجتمع في الدولة ذاتها، عن طريق عرض الخدمات التي توفرها أجهزة ومؤسسات الدولة أو كطريق للتواصل مع الجمهور في الدولة، هذا بالنسبة للمواقع الإلكترونية المتاحة لكافة الأفراد.

والسبب الثاني من وجه نظر الباحث متعلق بحساسية المعلومات أو ما قد تسببه هذه المعلومات في حال استخدامها بشكل خاطئ، هذا بالنسبة إلى المواقع الحكومية الخاصة والتي لا يمكن للجميع الاطلاع والولوج إليها من دون أي تصريح مسبق من المسؤول عن النظام، وذلك مثل ما سببه اختراق وكالات الأنباء القطرية "قنا" في يونيو الماضي الذي قام فيه المخترق بنشر انباء كاذبة عن سمو أمير قطر، والذي أدى في نهايته الى حصار جوي وبحري وبري على قطر، وأدى الى قطع الأرحام بين الأسر المشتركة بسبب منع دول الحصار الموطنين القطرين من دخول أراضيهم، وكذلك منع مواطنيهم من دخول الأراضي القطرية.[69]

---

[68]– قانون الشركات القطري، رقم ١١، لسنة ٢٠١٥، المادة ٢٠٧.

[69] الرجاء النظر:

https://www.aljazeera.net/knowledgegate/newscoverage/2017/6/11/مقاطعة–قطر–وحصارها–آثار–ونتائج، تاريخ الزيارة ٢٠١٩/١٠/١٩.

ذلك فضلاٍ عن ما قد يسببه الدخول بغير وجه حق من أضرار وأخطار على أمن الدولة في حال تمكن أحد الأشخاص من الدخول الى المواقع ونظم المعلومات التي تحتوي على معلومات تخص الأمن القومي للدولة وتسريبها الى دول معادية أو غيرها من الاستخدامات التي تضر أمن الدولة، ومن أجل كل ما سبق أفرد المشرع القطري نص المادة الثانية لحماية أجهزة الدولة ومؤسساتها وحماية أمنها الالكتروني، كما قد يتسبب الدخول في الى هذه المواقع أو الأنظمة في تعطيل استخدام النظام أو الموقع مما يكبد الدولة خسائر مادية، أو قد يتمكن الفاعل من الحصول على مزايا أو أموال كما لو يقوم بالدخول الى موقع وزارة الداخلية وإلغاء كافة المخالفات المروية الخاصة به أو لغيره نظير تلقي نصف ثمنها من أشخاص أخرين أو غيرها من مخاطر جريمة الدخول غير المشروع.

وتظهر أهمية البيانات والمعلومات المحفوظة على المواقع الإلكترونية أو النظم المعلوماتية التابعة للدولة من تشديد المشرع العقاب اذا تسبب الاختراق الوصول الى المعلومات تخص أمن الدولة الوطني أو الاقتصادي أو البيانات والمعلومات السرية بطبيعتها أو تسبب الدخول بإتلاف أو نقل البيانات او الإضرار بالمستخدمين او المستفيدين أو الحصول على مزايا أو أموال من الدخول.

المبحث الثالث

الركن المادي لجريمة الدخول بغير وجه حق

يمثل الدخول الغير مصرح به النشاط الإجرامي في هذه الجريمة، ولقد جرمت كافة التشريعات فعل الدخول بغير وجه حق للنظام المعلوماتي، وقد نص القانون القطري على جريمة الدخول في المادة الثانية والثالثة من قانون مكافحة الجرائم الالكترونية حيث نص في المادة الثانية على أنه " **يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، كل من تمكن عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات، بغير وجه حق، من الدخول إلى موقع إلكتروني أو نظام معلوماتي لأحد أجهزة الدولة أو مؤسساتها أو هيئاتها أو الجهات أو الشركات التابعة لها**[70]."، ومن خلال النص السابق يتبين لنا عناصر الركن المادي لهذه الجريمة، فقد ذكر المشرع كل من تمكن من خلال الشبكة المعلوماتية **الدخول** الى موقع الكتروني أو نظام معلوماتي، وبهذا يتضح لنا أن اول عناصر الركن المادي في هذه الجريمة وهو عنصر الدخول الى النظام المعلوماتي أو الموقع الالكتروني، كما اشترط المشرع أن يكون الدخول الى النظام المعلوماتي أو الموقع الإلكتروني **بغير وجه حق**، أي أن يكون الدخول من دون أي تصريح بحيث يمكن اعتبار العنصر الثاني متوفر في هذه الجريمة، ومن ناحية أخرى هل جريمة الدخول من الجرائم الشكلية أو الجرائم التي يستلزم لتحققها أن يترتب على الدخول ضرر في النظام أو المعلومات والبيانات المحفوظة على النظام، وبناء على ذلك سيقوم الباحث في بيان مفهوم الدخول الى النظام المعلوماتي في مطلب، والمقصود بعدم التصريح في مطلب، وطبيعة جريمة الدخول في مطلب أخر.

[70] – قانون مكافحة الجرائم الإلكترونية القطري، مرجع سابق، المادة الثانية.

المطلب الأول

مقصود الدخول بغير وجه حق

لقد شبه الكثير من الفقهاء الدخول بغير وجه الى العالم الافتراضي بفكرة الدخول في ذاكرة الإنسان، حيث يعتبر هذا الجانب من الفقه أن التعريف المعنوي والواقعي للدخول يشمل جميع أنواع الاعتداء سواء كان الاعتداء مباشر أو غير مباشر، حيث أن جريمة الدخول بغير وجه حق تنطوي اساساً على سلوك يرتكبه مرتكب الدخول باستخدام تقنيات المعلومات، ويشمل معنى الدخول هنا جميع الأفعال التي تنطوي على فعل الدخول والتي تسمح بالولوج الى النظام المعلوماتي أو جهاز الحاسب الآلي.[71]

كما أن هناك العديد من المحاولات لتعريف الدخول الغير مصرح به للنظام المعلوماتي، والتقريب بين الدخول الافتراضي للنظام المعلوماتي، والدخول الواقعي، حيث يرى الفقيه (Orin Kerry) أنه ينبغي التشبيه بين الدخول الواقعي والدخول الافتراضي إلى النظام المعلوماتي، فعلى سبيل المثال لو أن أحد المستخدمين لديه جهاز حاسب موصول بشبكة الأنترنت محمي باسم مستخدم و بكلمة مرور، فعند محاولة أحد الأشخاص الدخول سيطلب منه إدخال أسم مستخدم وكلمة مرور صالحين لإتمام عملية الدخول، في هذه الحالة يمكن القول أن شاشة الكمبيوتر التي طلبت اسم مستخدم وكلمة مرور تشبه القفل الموجود على وجهة الباب، وإدخال اسم مستخدم وكلمة المرور يشبه

[71] – رشدى علي، الحماية الجنائية للمعلومات على شبكة الإنترنت، دراسة مقدمة لنيل درجة الدكتور في الحقوق، جامعة القاهرة، كلية الحقوق، قسم القانون الجنائي، سنه ٢٠٠٩، ٣١١و٣١٢.

استخدام المفتاح لفتح الباب، ويكون بالتالي المستخدم الذي يدخل اسم مستخدم وكلمة مرور صحيحين قد دخل للنظام[72].

وقد عرف البعض الدخول الغير مشروع بأنه "الدخول الى نظام معلومات أو الى موقع إلكتروني من قبل شخص غير مخول له الدخول، فينتهز الفاعل هذه الفرصة للاطلاع على ملفات أخرى سرية دون وجه حق"[73]، كما تم تعريفه ايضاً بأنه "قيام أحد الأشخاص باختراق النظام المعلوماتي أو الشبكة المعلوماتية أو الموقع الإلكتروني، أو الولوج له دون تصريح أو بما يجاوز أو يخالف التصريح"[74]

ولا يتفق الباحث مع التعاريف السابق ذكرها كونها لم تشتمل على البيانات والمعلومات المخزنة في الموقع الالكتروني أو النظام المعلوماتي حيث أن التعريف الأمثل من وجهة نظرنا هو "الوصول الى النظام المعلوماتي أو الشبكة المعلوماتية أو المعلومات والبيانات المخزنة داخل الحاسب الالي، من قبل شخص لا يملك الحق وغير مخول له بالوصول اليها "

ويلاحظ أن أغلب التشريعات لم تتطرق الى معنى الدخول أو تعريفه لذلك اتجهت المحاكم في الولايات المتحدة الأمريكية الى محاولة تعريف الدخول في عام ١٩٦٦ في قضية الولايات المتحدة ضد ALLEN، حيث تتلخص وقائع القضية في أن ALLEN قام باستخدام حسابه الشخصي للاتصال بالشبكة "dial up" وتلاعب بها بشكل يسمح له بأجراء التحويلات الاتصالية البعيدة

---

[72] – عبد الإله نوايسة، مرجع سابق، ص ٣٣و٤٣.

[73] – محمد سليمان الخوالدة، مرجع سابق، ص ٤٢.

[74] حسن المناصير، مرجع سابق ،ص٤٢.

وبالمجان، وعندما ظهر له على شاشة جهازه كلمة المرور واسم المستخدم قام ALLEN بتخمينها وتمكن من الولوج الى النظام مع محو الدليل على نشاطه، وعلى اثر ذلك تم ادانة ALLEN بجريمة الدخول لانتهاكه تشريع جرائم الحاسب الالي بولاية تكساس، ولكن ALLEN دفع بعدم وجود دليل على دخوله، واستندت المحكمة على التعريف الموسع للتشريع والذي ينص على أن الدخول هو "الاقتراب أو إصدار أمر أو الاتصال ب ..... أو تخزين بينات في ..... أو استرداد بيانات من ..... أو أية شيء أخر يؤدي الى استخدام مصادر الحاسوب"، بيد أن المحكمة قالت بأن التعريف التشريعي لهذه الجريمة تعريف موسع ولا يمكن الأخذ به لأن قد يؤدي الى الغموض التشريعي، وفسرت المحكمة بقولها بأن قاموس webster يعرف الدخول access "كحرية أو قابلية للحصول أو الاستخدام" وأدى هذه التعريف الى القول بأنه لا يوجد دليل على دخول ALLEN ، فحتى المرحلة التي تسبق دخول ALLEN فلن نستطيع القول بأن لديه القابلية لاستخدام حاسبات شركة الاتصال.[75]

- و عرفت بعض التشريعات الدخول، مثل القانون الإنجليزي الذي عرف الدخول على أنه الدخول الى البيانات والبرامج الموجودة في جهاز الكمبيوتر، وذلك بجعله ينفذ أي وظيفة، ويمحو أو يغير في البيانات والبرامج، بنسخ أو بنقل البيانات أو البرامج من مكان حفظها إلى وسيلة تخزين، أو استخدام البيانات والبرامج أو جعلها كمخرجات من الكمبيوتر المحفوظة فيه سواء بجعلها معروضة أو بزي أسلوب آخر[76].

[75] – رشدي علي، المرجع السابق، ص ٣١٢.

[76] – عبدالإله نوايسة، مرجع سابق، ص٣١.

- ومن التشريعات العربية التي عرفت الدخول غير مصرح به نظام مكافحة الجرائم المعلوماتية السعودي الذي عرف الدخول بأنه" دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"[77] ، كما عرفت المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الكويتي لسنة ٢٠١٥ الدخول غير مشروع بأنه " النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو النظام المعلوماتي 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" [78]. ومن التشريعات التي لم تعرف الدخول التشريع القطري والمصري والسوداني، والإماراتي والبحريني.

كما يشمل الدخول الى النظام المعلوماتي كافة الأفعال والتصرفات التي تمكن المخترق من الولوج الى النظام المعلوماتي، وبموجبها يتمكن المخترق من احكام سيطرته على كافة المعطيات التي يتكون منها النظام المعلوماتي[79].

---

[77] – الرجاء النظر:
https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf، ٢٠١٩\١٠\١٧

[78] – قانون مكافحة جرائم تقنية المعلومات الكويتي، مرجع سابق، المادة الأولى.

[79] – مهند وليد أسماعيل، ، التنظيم القانوني لجريمة الدخول الغير مصرح به الى نظام الحاسب الآلي: دراسة مقارنة، مجلة العلوم الشرعية– جامعة القصيم، المجلد ١١، العدد، ١، ٢٠١٧، ص ٥٤١.

- **ويثور التساؤل هل تعتبر جريمة الدخول من الجرائم الشكلية أو جرائم التي تتطلب تحقق نتيجة معينة حتى تعتبر جريمة تامة ؟** فاذا تم اعتبارها جريمة شكلية فأن جريمة الدخول تتحقق بالدخول المجرد والذي

تم تعريفة بأنه هو "التواجد داخل النظام دون أحداث أدنى ضرر لصاحبة، سواء الاطلاع على المعلومات المختزنة به دون غرض محدد"، فقد أثار هذا الموضوع جدلاً فقهيا كبيرا من حيث التجريم وانقسمت الآراء الى رأيين:

الأول كان يرى عدم ضرورة تجريم الدخول المجرد في حال عدم وجود أدنى نية لدي الفاعل لارتكاب جريمة لاحقة على الدخول، فهو لا يعدو أن يكون استعراض للأفكار الذهنية والقدرات الذاتية لدى الفاعل على الاختراق وقد يكون في كثير من الأحوال مجرد فضول لدى الفاعل لذلك لا يشكل هذا الدخول أي تهديداً يستوجب إضفاء صفة التجريم و العقوبة عليه.

أما الرأي الثاني يرى اصاحبه ضرورة تجريم الدخول المجرد حيث وأن لم توجب لدى الفاعل النية على ارتكاب أي جريمة لاحقة على الدخول اثناء دخوله بغير وجه حق، ألا آنه قد تتوفر هذه النية لديه لاحقاً، حيث أن النشاط الإجرامي لهذه الجريمة هو فعل الدخول بحد ذاته، فهي جريمة شكلية لا تتطلب قيام الفاعل بأي نشاط أخرى ماعد فعل الدخول. حيث أن الباعث لتجريم جريمة الدخول هو الحفاظ على سلامة وأمن المعلومات المخزنة داخل النظام المعلوماتي أو الوقع الالكتروني وحمايته من العبث والتزوير والتزليف، لذلك يعد الدخول المجرد بحد ذاته عدوان على هذه المعلومات والبيانات.[80]

[80] – مدحت أبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي . دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٥، ص ٧٦و ٧٨و٧٩.

ويؤيد الباحث الرأي الثاني وذلك لأن اغلب التشريعات المقارنة تجرم الدخول المجرد واعتبرت جريمة الدخول جريمة شكلية يستحق مرتكبها العقاب، وسوف نفصل في المباحث الاحقه طبيعة جريمة الدخول بغير وجه حق واتجاه التشريع الوطني والمقارن في تصنيفها.

- **كما أن الدخول إلى المواقع أو النظم المعلوماتية ممكن تصوره في عدة فروض كالتالي :**

الفرض الأول –يكون من خلال دخول المستخدم الى النظام من دون أن يكون مسموح له بالدخول، على الرغم من عمل المستخدم في نفس الجهة المالكة للحاسب الآلي (كأن يكون المستخدم موظفاً في نفس المؤسسة ولكن في قسم أخر) وفي قضية US V. Morris وهي قضية في الولايات المتحدة الأمريكية ضد Morris والتي اشتهرت بقضية دودة الأنترنت، حيث تتمثل الوقائع في أن طالب في جامعة كورنيل قام بتصميم برنامج حاسب آلي لكشف كافة الثغرات في الأنظمة الالكترونية تسمى بالدودة وتم اطلاقها وانتشرت هذه الدودة وأعادت طبع نفسها الى حين لم يتم الاستطاعة التحكم بها، و تم أدانة Morris من قبل هيئة المحلفين بموجب المادة ١٠٣٠ من القانون الفدرالي الذي كان يحظر الخول العمدي لأجهزة الجهات الفدرالية في حال تسبب ذلك الدخول بضرر ما، حيث أسس Morris دفاعه على أن كان له الحق بالدخول الى بعض من تلك الأجهزة منها جامعة هارفرد كورنيل، بحيث ميز الدفاع بين نوعين من الدخول وهو الدخول الغير مصرح به والدخول بناء على تجاوز الحق في الدخول، كما استند Morris الي تقرير مجلس الشيوخ الأمريكي الذي اقترح التمييز ما بين المصطلحين الدخول بدون تصريح وتجاوز التصريح، حيث يعتبر الدخول بدون تصريح كما عبر عنه مجلس الشيوخ في التقرير سالف الذكر الى أنه الدخول الذي يتم من قبل الذين لا يملكون الحق في الدخول اساساً، بينما تجاوز التصريح يكون

من الأشخاص الذين يكون مصرح لهم الدخول وقد اسماهم بالمطلعين مثل الموظفين في إحدى الجهات الذين يدخلون الى حاسوب جهة العمل، كما أستند Morris إلى الأقتراح الوارد في التقرير بأنه "في الحالات التي يحظر فيها الكونجرس الدخول إلى الحواسيب بدون تصريح ولكن لم يحظر تجاوز التصريح في الدخول فأنه يعد العدة لحظر أفعال الدخلاء وليس المطلعين"، لكن الدائر الثانية رفضت الدفوع التي تقدم بها Morris على الرغم من أتفاقها مع التشريعات.[81]

الفرض الثاني –يقوم أحد الأشخاص من الخارج بالدخول الى النظام وهنا نميز بين حالتين الدخول المباشر والدخول الغير مباشر:

الحالة الأولى:

كأن يقوم الشخص (المخترق) بالتوجه الى أماكن تواجد أجهزة الحاسب الآلي ويقوم بالدخول إليها وأستعمالها ويعد هذا الدخول هو الدخول المباشر.

- وقد أكدت محكمة التمييز القطرية على أن لا عبرة في الجهاز الذي تم الدخول منه سواء كان الجهاز المستخدم جهاز الجاني نفسه أو جهاز المجني عليه، ونصت على" **لما كان ذلك، وكانت المادة (371) سالفة البيان مع صراحة نصها ووضوح عباراتها تدل بجلاء على أن المشرع قد أثم التوصل بالتحايل إلى نظام المعالجة الآلية للبيانات المحفوظة بالحاسب الآلي ولم يحدد طريقة الدخول على الحاسب الآلي سواء كانت من جهاز المجني عليه نفسه أو من أي جهاز آخر، فإن ما تقول به الطاعنة من أنه يلزم للتجريم أن يكون الدخول إلى نظام المعالجة الآلية للبيانات المحفوظة في الحاسب أن يكون من خلال جهاز الحاسب الخاص بالمجني عليه فقط إنما هو تخصيص للنص بغير مخصص، هذا فضلاً عن أنه**

[81] –رشدي علي، مرجع سابق، ص٣١٧و٣١٨.

يترتب عليه عدم تأثيم الدخول إلى نظام المعالجة الآلية للبيانات المحفوظة إذا كان عن طريق جهاز آخر خلاف جهاز المجني عليه وهو ما لم يقره الشارع بتلك المادة" [82].

يستنتج من الحكم السابق أن محكمة التمييز لم ترد تخصيص النص الذى ورد بشأن الدخول الغير مصرح به، حيث أن نص المادة٣٧١ من قانون العقوبات القطري لم تحدد نوع الجهاز الذي يتم استخدامه للدخول الغير مصرح به، حيث أن النص جاء عام غير مخصص لجهاز المجني عليه ، بالإضافة الى أن تخصيص نص المادة السابقة يؤدي الى عدم تجريم الدخول اذ تم عن طريق جهاز أخر غير جهاز المجني عليه، ويلاحظ الباحث أن حكم محكمة التميز قد صدر استنادً على قانون العقوبات، وذلك لأن قانون الجرائم الإلكترونية القطري لم يصدر الا في سنة ٢٠١٤، ولو تم تطبيق القانون الجديد لصدر الحكم على نفس النهج وذلك لان المادة ٢ والمادة ٣ جاء عامة لكافة سوائل الدخول ولم يحدد الوسيلة المستخدمة سواء كان الدخول من جهاز الجاني أو من جهاز المجني عليه

الحالة الثانية:

أما بالنسبة للدخول الغير مباشر هذه الحالة تتطلب دخول الشخص (المخترق) الى النظام المعلوماتي عن بعد، سواء كان دخوله عن طريق عمل توصليه بين الأجهزة، أو عن طريق الشبكة المعلوماتية (شبكة الأنترنت)، وبغض النظر عن حالة النظام سواء كان محمياً بكلمة مرور آم لا [83].

[82] – حكم محكمة التميز القطرية، الأحكام الجنائية، الطعن رقم٢٢٩، لسنة ٢٠٠٩.

[83] – شيماء عبدالغني، مرجع سابق ، ص ١١٤و١١٥.

- **ويعتبر من أشهر البرامج الخبيثة التي تمكن الفاعل من ارتكاب الجريمة برنامج حصن طروادة، الفيروسات، القنابل المعلوماتية، حيث يمكن من خلال هذا البرامج اتلاف او الحذف او الإضافة.**

1 – برنامج حصن طروادة:

تقوم هذه الفكرة على أرسال ملف صغير يسمى بحصان طروادة، وسبب تسميته بذلك لأنه يشبه حصان طروادة الخشبي الشهير في الأسطورة حيث أن شكل الملف الخارجي طبيعي ولكن محتواه خبيث يقوم باختراق البيانات والمعلومات في الجهاز فور دخوله الى الحاسب الآلي[84]، حيث يعتبر حصن طروادة من أخبث وأخطر البرامج الالكترونية التي يتم استخدامها في الدخول الى المواقع الالكترونية، وسبب ذلك يعود الى الخصائص العديدة التي يحتوي عليه البرنامج مما يمكن ذلك المخترق إلى الدخول وبسهولة إلى الموقع الإلكتروني مع عدم ترك أي دليل على دخوله، ففي بداية الأمر كان يتم استخدام حصن طروادة في استخدامات مفيدة مثل مراقبة اعمال الموظفين والأطفال في غياب المسؤولين والوالدين، وتم تطويرها مع مرور الزمن حتى أصبحت من أفضل البرامج للمخترقين.[85]

2 – الفيروسات

مما لا شك فيه بأن البرامج الفيروسية تعتبر من أشد وأخطر البرامج ضد الحاسب الآلي، وهي برامج يكون الهدف منها أحداث أكبر ضرر ممكن، ولا يكون ذلك ألا بعد عملية الدخول إلى الموقع الإلكتروني أو الحاسب الآلي، حيث تتميز البرامج الفيروسية بقدرتها على ربط نفسها بالبرامج

---

[84] – حسين الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت "دراسة مقارنة"، رسالة دكتوراه، جامعة عين شمس، القاهرة ٢٠٠٩، ص ٢٦٦.

[85] – حسين المناصير، مرجع سابق، ص ٤٤.

الأخرى وإعادة انشاء نفسها، فضلاً عن قدرتها عن الانتشار والانتقال من نظام إلى أخر، وهناك أنوع متعددة من الفيروسات منها من يصيب النظام المعلوماتي وينتشر بصورة بطيئة، وهناك نوع يصيب النظام وينتشر بسرعة كبيرة ويمتاز بتدمير كامل المكون المعلوماتي ومن أبز الأمثلة على ذلك فيروس مايكل انجلو الذي ظهر في ١٩٩٢/٣/٢٦.[86]

3 – برنامج القنبلة المعلوماتية.

هو برنامج يتم تثبيته في النظام المعلوماتي نفسه على أن يعمل هذا البرنامج في وقت محدد يتم فيه تدمير أو تعطيل أو محو البيانات داخل مكون النظام المعلوماتي، وتنقسم القنبلة المعلوماتية إلى نوعين النوع الأول **القنبلة الزمنية** وهي تعمل بوقت محدد وفي يوم معين وساعه معينه. أما بالنسبة إلى **القنبلة المنطقية** فهي تهدف إلى تنفيذ عمل غير مشروع من خلال مسحها للنظام المعلوماتي، حيث لا تقوم هذه القنبلة باتخاذ أي سلوك عدائي ضد النظام فتكون في بداية الأمر ساكنه ولهذه يصعب اكتشافها بسهولة، ولا تتفعل هذه القنبلة إلا بعد أن يتم أحد الشروط المنطقية في النظام قبل البدء بأي عمل تخريبي، ويشبه عملها التخريبي الانفجار مما يصعب الأمر على صاحب النظام في تدارك الأمر.[87]

كما أنه لا يشترط لوقوع جريمة الدخول بغير وجه حق ان يتم باستخدام وسيلة معينة فكل الوسائل سواء، هذا ما عبر عنه المشرع القطري في نص المادة الثالثة من قانون الجرائم الإلكترونية" كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً". وكذلك جرم المشرع الأردني في

---

[86] – محمد الخوالدة، مرجع سابق، ص ٧٣.

[87] – حسين المناصير، مرجع سابق، ص ٤٥.

قانون الجرائم الإلكترونية والتي نصت على " كل من دخل قصداً إلى موقع إلكتروني أو نظام معلوماتي بأي وسيلة"، ويستنتج الباحث مما سبق بأن كلا المشرعين لم يعتد بوسيلة معينة للدخول بل ترك الأمر مفتوح، أي ان الدخول الغير مصرح به يعتبر جريمة وبغض النظر عن الوسيلة المستخدمة في الدخول، وكذلك لا عبرة في الجهاز المستخدم بالدخول سواء كان جهاز الجاني أو جهاز المجني عليه.

المطلب الثاني

المقصود بعدم التصريح

إن المفهوم التقليدي لعدم التصريح يفترض أن الشخص ليس لديه الحق ان يكون متواجد في المكان الذي وجد فيه، هذا المفهوم بالنسبة للدخول الغير مصرح به في العالم الواقعي، ومن الصعب جداً تطبيقه في العالم الافتراضي، حيث يعتبر عنصر الرضاء غير متوفر في حال تعليق صاحب النظام الدخول إلى النظام مقابل اشتراك مالي يدفع أو بتوافر شروط معينه لدخوله، حيث تعتبر الجريمة تامة بمجرد دخول الفاعل الى النظام من دون دفع الاشتراك المالي أو من دون توافر الشروط المعروضة من قبل صاحب النظام.[88]

حيث يعتبر الدخول إلى جهاز الحاسب الآلي غير مصرح به في حالتين ؛ الحالة الأولى تكون اذا افترضنا وجد مسؤول عن جهاز الحاسب الألي، وقام الفاعل بالدخول إلى هذا الجهاز من دون تصريح من المسؤول عن جهاز الحاسب الآلي، أما الحالة الثانية تفترض تجاوز الفاعل التصريح الممنوح له بدخوله الى بيانات أو معلومات لا يشملها التصريح الممنوح له، وعلى أي حال فأن لا تثور مشكلة حول تجريم الحالة الأولى، ولكن تكمن المشكلة في الحالة الثانية، حينما يتجاوز العامل في المؤسسة حدود التصريح الممنوح له بدخوله الى النظام في غير الحالات المصرح له فيها، حيث أن التجريم في هذه الحالة يخاطب الأشخاص العاملين في الجهات العامة، وذلك لأن

[88] شيماء عبد الغني، مرجع سابق، ص ١٠٢.

الأشخاص العاملين في الجهة اذا قاموا باستخدام النظام بعد ساعات العمل أو في استخدامات اخرى يعتبر هذا محل لجرمة الدخول بغير وجه حق .[89]

و تطلبت بعض التشريعات التي جريمة الدخول غير مصرح في المؤسسات في حال كان هناك تعليمات واضحة وصريحة من قبل المؤسسة تحدد الشخص الذي له الحق بالدخول، مثلما ما نص عليه المشرع اليوناني في قانون العقوبات أذا كان الشخص الذي قام بالدخول إلى النظام هو مالك أساس لحق الدخول فلا يمكن العقاب على فعل الدخول في هذه الحالة إلا في حال كانت المؤسسة قد منعت وبشكل صريح إستناداً لقواعدها الداخلية أو بموجب قرار مكتوب وصادر من مالك الحق ، حيث ثارت العديد من التساؤلات الفقهية حول أن كان يجب لدخول النظام تصريح من فمن هو مالك الحق بمنح هذا التصريح وهل يمكن أن يكون هناك أكثر من شخص [90]. لقد اطلق الفقه الفرنسي تعريف لصاحب السلطة بالدخول النظام "بأنه كل شخص طبيعي أو معنوي، أو كل سلطة عامة، أو كل مؤسسة أو جهاز أو محتواه، وكيفية تنظيمه، والهدف منه". أما بالنسبة الى تعدد المسؤولين عن النظام فأنه يجوز أن يكون هناك أكثر من مسؤول فلا يوجد أي مانع بأن يكون هناك أكثر من شخص مسؤول عن النظام وله جميع سلطات التصرف من منح تصريح أو سحبه الى أخره .[91]

كما أن هناك استخدام أخر للنظام أثير بشأنه التساؤل فهل يمكن اعتباره تحت طائلة الدخول بغير تصريح أو تجاوز التصريح عندما يتم استخدام النظام لأسباب أخرى غير التي منح التصريح

---

[89] – شيماء عبد الغني، المرجع نفسه، ص ١٢٤.

[90] – نائلة قورة، مرجع سابق، ص ٣٣٥

[91] – نائلة قورة، مرجع سابق، ص٣٣٤.

بشأنها، لقد ثارت العديد من الأحكام القضائية في القضاء الإنجليزي فيما يتعلق بهذه المسألة حيث تنص أحد وقائع القضايا وهي قضية

- DPP V. Bingel في قيام أحد أفراد رجال الشرطة بالدخول الى النظام الإلكتروني الخاص بالشرطة وأخذ معلومات لا تمت وظائفهم بصلة .[92]ورفضت المحاكم الأمريكية الدعوى المقامة من الولايات ضد اولسن، حيث تتلخص وقائع هذا القضية في كون اولسن ضابط شرطة قام بتجاوز التصريح الممنوح له وباستخدام ودخول النظام الإلكتروني الخاص بالسلطات لأغراض أخرى غير الاستخدامات المخصص له حيث قام بطباعة صور السيدات الاتي يقمن بالدراسة في الجامعة القريبة منه ودفع ولسن في أنه يملك التصريح بالدخول الى النظام المعلوماتي في الأساس لذلك لا يمكن أتهامة بتجاوز التصريح، وذلك عن طريق طباعة صور رخص قيادتهم. وتم الانتهاء بأن الدخول يعتبر مصرحً به، هذا ما أتجه اليه النظام القضائي الإنجليزي بخصوص هذه المسألة. [90]

وهذا على غرار العديد من التشريعات التي نصت صراحتاً على تجريم الدخول الغير مصرح به من العامل بالمؤسسة التي يتبعها النظام المعلوماتي، وهذا ما نص عليه المشرع الأردني في المادة الثامنة من قانون الجرائم الإلكتروني حينما نص على " تضاعف العقوبة بحق كل من قام بارتكاب أي من الجرائم الواردة في المواد ٣ الى ٦ من هذا القانون أثناء تأديته وظيفته أو عمله أو باستغلال

---

[92] – نائلة قورة، المرجع نفسه، ص ٣٣٩

[90] –Sami AL–Rawashdeh, Illegal Access to Information Systems in Qatari Criminal Law: A Comparative Study, Kuwait International Law School Journal – Volume 6 – Issue 1 – Ser. No. 21 – Jumada Al–Akhirah 1439 – Rajab 1439 – March 2018,p 18

أي منها" [93]، وقد جرم المشرع القطري في المادة الثالثة كذلك على تجاوز التصريح حين نص على انه" **كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك**"[94]

- والمقصود بالتصريح في قانون الجرائم الإلكترونية الأردني للدخول للنظام المعلوماتي هو " الأذن الذي يمنح من صاحب العلاقة الى شخص أو أكثر أو للجمهور للدخول أو استخدام النظام المعلوماتي أو الشبكة المعلوماتية، أو موقع إلكتروني، بقصد الاطلاع أو إلغاء أو حذف أو إضافة أو تغير أو إعادة نشر بيانات أو معلومات أو حجب الوصول إليها أو إيقاف عمل الأجهزة أو تغيير موقع إلكتروني أو إلغائه أو تعديل محتوياته"[95]

بينما لم يعرف المشرع القطري التصريح بالدخول وهذا ما يؤخذ على القانون القطري في سكوته عن تعريف التصريح بالدخول، فكان من باب أولى أن يقوم المشرع القطري بتعريفه، على الرغم من قيام المشرع بتعريف العديد من المصطلحات في المادة الأولى من قانون الجرائم الإلكترونية، على غرار التشريعات الأخرى.

ويؤيد الباحث الاتجاه الذي ذهب له المشرع القطري والمشرع الأردني في تجريم أو استغلال تجاوز التصريح الممنوح، ولكن المشرع القطري لم يورد الجزء الأخير الوارد في نص المادة الثالثة في

---

[93] – قانون الجرائم الالكترونية قانون الجرائم الالكترونية الأردني، رقم ٢٧، لسنة ٢٠١٥، المادة ٣و٦.

[94] – قانون مكافحة الجرائم الإلكترونية القطري، مرجع سابق.

[95] – قانون الجرائم الالكترونية قانون الجرائم الالكترونية الأردني، المرجع السابق، المادة الثانية.

المادة الثانية والخاصة بالدخول بغير وجه حق الى الأنظمة والمواقع الإلكترونية، في حين كان من باب أولى للمشرع ان يعتبره كذلك. حيث أنه من المتصور أن يقوم أحد الأشخاص الذين لهم الحق في استخدام النظام بتجاوز أو استغلال هذه التصريح لأفعال لا تمت المصلحة العامة بصلة مثلما حدث في قضية الولايات ضد أولسن.

- ولقد ثار جدل فقهي حول اعتبار عدم التصريح بالدخول ينصرف الي الحالات التي يكون فيها الدخول الى أجهزة الحاسب الآلي مشروطاً، مثل الأماكن التي تقدم الخدمات بمقابل نقدي في حال عدم قيام المنتفع من الخدمة بدفع المقابل النقدي للخدمة، فاذا تمكن الشخص من الدخول الى النظام المعلوماتي من دون دفع الثمن فأن دخوله يعد غير مصرح به، بينما ذهب جانب اخر من الفقه الى عدم اعتبار هذا النوع من الدخول يتعلق بجريمة الدخول الغير مصرح به الى النظام المعلوماتي، وذلك لان الهدف من تجريم الدخول الغير مصرح به هو حماية المعلومات والبيانات الموجودة في جهاز الحاسب الآلي، وهذا لا يتحقق في هذه الحالة حيث ان عدم تسديد الثمن هو شرط تنظيمي للدخول الى الحاسب الآلي والذي يعد مصرح به من قبل أي شخص يسدد الثمن المطلوب مقابل الدخول ، أي ان المعلومات والبيانات الموجدة في هذا الجهاز لا تتمتع بالسرية، وذلك لأنها متاحه لكل من يسدد ثمن استعمال هذا الجهاز، حيث ان الذي يشكل المصلحة من تجريم جريمة الدخول هو حماية المعلومات والبيانات السرية[96]. ولا خلاف حول الدخول الى شبكة المعلومات في الأماكن العامة التي تقدم خدمات الأنترنت، مثل الجامعات والمطارات والمطاعم، وذلك لان بمجرد قيام هذه الأماكن بتوفير خدمات الأنترنت لمرتاديها يعتبر تصريح ضمني بالدخول[97].

[96] – عبد الإله نوايسة، مرجع سابق، ص٣٩.

[97] – عبد الإله نوايسه، المرجع ذاته.

المطلب الثالث

طبيعة القانونية للدخول

اختلفت المناهج التشريعية في تجريم الدخول الغير مصرح به الى النظام المعلوماتي، وأدى ذلك الى اختلاف طبيعة الجريمة، فجريمة الدخول الغير مصرح به تعد جريمة شكلية في بعض التشريعات، وذات نتيجة في تشريعات أخرى، كما أن هناك بعض التشريعات التي تجرم مجرد القيام بفعل الدخول كسلوك مجرد، حتى ولو لم يترتب علية نتيجة إجرامية.

من حيث الأصل أن جريمة الدخول هي من الجرائم الشكلية وليست من جرائم ذات النتيجة، وما يدلا على ذلك أتجاه أغلبية التشريعات وأولهم التشريع الفرنسي إلى اعتبارها جريمة شكلية لا يشترط لتحققها وقوع أي ضرر، وأنما شددت العقوبة في حال تحقق الضرر من وراء الدخول بغير وجه حق.[98]

حيث يرى جانب من الفقه أنه ليس من الضروري أن يتمكن الفاعل من الوصول الى المعلومات أو البيانات المخزنة على المواقع والأنظمة المعلوماتية وهو ليس شرطاِ لتحقق النشاط الاجرامي في هذه الجريمة، بل أن النشاط الإجرامي في هذه الجريمة هو فعل الدخول ذاته وليس الحصول على المعلومات والبيانات، كما أن وإن كانت الغاية الرئيسية من تجريم الدخول بغير وجه حق الحفاظ على المعلومات والبيانات من الوصول إليها، ألا أن الدخول بحد ذاته هو تهديداً لهذا الحق[99]

[98] – شيماء عبدالغني، مرجع سابق، ص ٩٧.

[99] – نائلة قورة، مرجع سابق، ص ٣٤٣.

فالتشريعات التي جرمت الدخول وتطلبت نتيجة إجرامية تترتب على الدخول القانون الفيدرالي لجرائم الحاسب الالي في الولايات المتحدة الأمريكية، حيث تطلب لقيام الجريمة أن يتم الحصول على البيانات كأثر مباشر لفعل الدخول الغير مصرح به[100]، كما يتطلب القانون النرويجي الوصول الى البيانات والبرامج لوقوع جريمة الدخول[101]، وأشترط القانون العقوبات الدنماركي لوقوع جريمة الدخول الغير مصرح به الوصول الى المعلومات والبيانات الموجودة في نظام معالجة البيانات [102] .

واخذ المنظم السعودي المنهج ذاته حيث أعتبر جريمة الدخول بغير وجه حق جريمة ذات نتيجة حيث لا تتحقق الجريمة لدى المنظم السعودي ألا اذا ترتب على دخول الموقع الالكتروني تغيراً لتصميمة أو إزالة المعلومات التي يحتويها او تم الدخول بهدف التهديد أو الابتزاز، بحيث ربط المنظم السعودي تحقق الجريمة بالضرر المترتب من ذلك الدخول.[103]

بينما هناك العديد من التشريعات التي اعتبرت جريمة الدخول الغير مصرح به جريمة شكلية، أي ان الجريم تقوم ولو لم يصل الفاعل الى البيانات والمعلومات المخزنة على النظام المعلوماتي، وتسمى في هذه الحالة جريمة دخول مجرد، ومن هذه التشريعات الفرنسي والذي نص في المادة ٣٢٣١١ من قانون العقوبات الجديد على عقوبة الدخول الى النظام المعلوماتي بغير وجه حق

---

[100] - USC 1030: Fraud and related activity in connection with computers Text contains those laws in effect on November 2, 2019

[101] -قانون الجرائم الالكترونية النرويجي، الرجاء النظر:
9/11/2019 https://www.cybercrimelaw.net/Norway.html.

[102]قانون العقوبات الدنماركي، تاريخ الزيارة، ٢٠١٩/١١/٩ الرجاء النظر:
- https://www.coe.int/en/web/octopus/country-legislative-profile/-/asset_publisher/LA6eR74aAohY/content/denma-1?_101_INSTANCE_LA6eR74aAohY_viewMode=view#article2

[103] الرجاء النظر القانون السعودي:
https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf. ٢٠١٩/١٠/١٠.

بعقوبة السجن لمدة سنتين وغرامة مائتي فرنك فرنسي حيث فرق القانون سالف الذكر بين حالتين الحالة الأولى وهو الدخول الى النظام المعلوماتي بطريق الغش أما الجريمة الثانية فهي الدخول والبقاء في النظام المعلوماتي، وقد لقت صياغة المشرع الفرنسي (بطريق الغش) انتقاد من جانب الفقه [104]، وذلك لأن العبارة السابقة قد توحي بأنه يجب للعقاب على هذا الفعل أن يكون النظام المعلوماتي محمي تقنياً حتى يمكن تطبيق هذا النص، مؤدى هذا الانتقاد أن النظام المعلوماتي أو الموقع الالكتروني الغير مشمول بنظام حماية لا يمكن أن تشمله حماية النص سالف الذكر لان الدخول اليه لا يتصور أن يكون بطريقة الغش، مما يؤدي ذلك الى اعتبار الاتصال مشروع.[105]، كما أن هناك بعض التشريعات العربية التي جعلت جريمة الدخول جريمة شكلية مع تغليظ العقوبة في حال وصول المخترق الى البيانات او المعلومات، ومن هذه التشريعات القانون الإماراتي، وقانون مكافحة الجرائم الإلكترونية القطري[106].

و هناك بعض التشريعات التي تجرم فعل الدخول المجرد، وتشدد العقوبة، في حال كان يهدف الجاني الى تحقيق نتيجة معينة، وبناء عليه تتحقق الجريمة اذا قام الجاني بالدخول ولو لم يحقق الهدف من دخوله بالحصول على بيانات او معلومات معينة، من هذه التشريعات قانون الجرائم الإلكترونية الأردني[107]، وكذلك القانون السوداني الذي جرم الدخول الغير مصرح به للنظام

---

[104] - French criminal code, o*rdinance no. 2000-916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January 2002, (Act no. 2004-575 of 21 June 2004 article 45 I Official Journal of 22 June 2004*

[105] – أسامة العبيدي، جريمة الدخول غير المشروع الى النظام المعلوماتي: دراسة قانونية في ضوء القوانين المقارنة، مجلة الدراسات المعلومات، العدد ١٤، جمعية المكتبات والمعلومات السعودية، ص ٣٠، ٢٠١٢.

[106] – عبدالآله النوايسة، المرجع نفسة.

[107] – قانون الجرائم الالكترونية قانون الجرائم الالكترونية الأردني، مرجع سابق، المادة ٣.

المعلوماتي، ولكنه نص على أن الدخول يجب أن يكون الهدف منه الحصول على بيانات ومعطيات تمس الأمن القومي أو الاقتصاد الوطني، أو بغرض الحذف أو الإلغاء أو تدمير البيانات أو المعلومات التي تتعلق بذلك [108]، وسار على هذا النهج ايضاً المشرع المصري في قانون جرائم تقنية المعلومات حيث عاقب على الدخول المجرد الى المواقع والنظم المعلوماتية، ولكنه شدد في حال حدوث اتلاف أو محو أو تغير أو نسخ أو إعادة نشر للبيانات او المعلومات الموجودة على الموقع الإلكتروني أو النظام المعلوماتي[109]

يرى الباحث أن التشريعات التي تجرم فعل الدخول المجرد مع تشديد العقوبة إذا كان الغرض من الدخول تحقيق هدف ما او الحصول على معلومات معينة، هو المنهج الصحيح السليم الذي أحسن فيه المشرع الأردني والسوداني، وذلك لان في هذه الحالة الجمع بين التشريعات التي تعتبر الجريمة مادية، وكذلك ما بين التشريعات التي تعتبها شكلية، وهذا يساعد في ردع الدخول والحد من هذه الجريمة سواء كان الدخول مجرد، أو كان هناك غرضا أو هدف معين من وراء هذا الدخول، وهاذا ما نص عليه المشرع القطري في قانون مكافحة الجرائم الإلكترونية في المادي الثانية الفقرة الثانية والمادة الثالثة الفقرة الثانية، فقد اخذ المشرع القطري بنفس ما اخذ به المشرع الأردني والسوداني، حيث جرم الدخول المجرد وضاعف العقوبة في حال ترتب على الدخول المساس بالمعلومات الأمن الداخلي او القومي ،او في حال ترتب على الدخول اتلاف او تعديل البيانات او محوها او تغيرها.

[108] – قانون جرائم المعلوماتية السوداني، مرجع سابق، المادة الرابعة.

[109] –قانون جرائم تقنية المعلومات المصري، مرجع سابق، المادة ١٤.

المبحث الرابع

الركن المعنوي

تعتبر جريمة الدخول بغير وجه حق الى النظام المعلوماتي من الجرائم العمدية، أي أن الأصل فيها أن تكون عمدية، والاستثناء عليها التجريم بطريق الخطاء، وقد اكدت على ذلك العديد من التشريعات، سواء تشريعات عربية ام كانت تشريعات اجنبية، وسيقوم الباحث بتقسيم هذا المبحث الى مطلبين لبيان وتفصيل الركن المعنوي، فالمطلب الأول سيكون عن: القصد الإجرامي العام، والمطلب الثاني، القصد الإجرامي الخاص.

المطلب الأول

القصد الإجرامي العام

يعتبر الركن المعنوي في جريمة الدخول بغير وجه حق الى النظام المعلوماتي من أهم الأركان التي يجب أن تتوفر حتى تقوم الجريمة، ولذلك لا يمكن تجريم الأفعال الا بتحققه، فالركن المعنوي في هذه الجريمة يتخذ صورة القصد الجنائي، على اعتبار أن جريمة الدخول بغير وجه حق من الجرائم العمدية، التي تتطلب توفر القصد الاجرامي فيها[110].

جريمة الدخول هي جريمة عمدية لا تختلف عن باقي الجرائم العمدية، فلابد من توافر عنصرين حتى يتوفر القصد الإجرامي العام وهما العلم والإرادة، فلا بد أن يعلم الجاني بأن دخوله الى النظام المعلوماتي غير مشروع، وكذلك يجب أن تتجه إرادة الجاني الى هذا الدخول، كما يتطلب في

[110] – شيماء عبد الغني، مرجع سابق، ص١٢٦.

القصد الإجرامي العام أن يكون الجاني عالماً بالواقعة القانونية ومكونتها، فحتى يتوافر القصد الجنائي للجريمة المرتكبة يجب أن يحيط الجاني علماً بعناصر الركن المادي للجريمة[111]، فيجب أن يكون عالماً بأنه فعله ينصب على نظام معلوماتي بما يتضمنه من معلومات وبيانات محل الحق الذي يحميه القانون، وعلى كل حال يجب أن يقترن العلم مع الإرادة، فاذا انتفي العلم أنتفا القصد الإجرامي[112]، فالإرادة هي النشاط النفسي الذي يهدف الى تحقيق الغرض الذي دخل من أجله الفاعل إلى النظام، فيجب أن تتجه أرادة الفاعل الى أحداث الأثر الإجرامي الذي من أجله دخل الى النظام المعلوماتي[113].

كما أن الجريمة تعتبر تامة في الدخول، وذلك بغض النظر عن الباعث سواء كان الباعث أو السبب في دخول الفاعل الى النظام لاختباره على سبيل المثال واكتشاف الثغرات الأمنية فيه أو كان دخول لأي سبب أخر، فقد قضى في أحد القضايا بإدانة مهندس تقني لدخول نظام معلوماتي لأحد البنوك من خلال الثغرات الأمنية الموجودة في النظام، وذلك بغض النظر عن السبب الرئيس الذي دخل من أجله هذا المهندس وهو أثبات جدارته للبنك من أجل الفوز والالتحاق بالتدريب لدى البنك.[114]

و يجب أن يتوقع الجاني في جريمة الدخول النتيجة الإجرامية التي سوف تترتب على الفعل، والنتيجة الإجرامية في هذه الجريمة هي الدخول الغير مصرح به الى النظام المعلوماتي، فيتعين على الجاني أنه يقوم بالدخول الى نظام معلوماتي غير مخول له بالدخول إليه، ولكن أذا توقع الجاني الدخول الى نظام معين ولكنه دخل الى نظام أخر فأن القصد الجنائي يعتبر متوفر في

---

[111] – أشرف شمس الدين، شرح قانون العقوبات القطري القسم العام: النظرية العامة للجريمة والعقوبة، الطبعة الأولى، جامعة قطر، ٢٠١٠، ص٢٨٢.

[112] – أسامة العبيدي، مرجع سابق، ص١٧.

[113] – أشرف شمس الدين، مرجع سابق، ص ٣١٤.

[114] – شيماء عبدالغني، مرجع سابق، ص ١٢٦.

هذه الحالة لتحقق النتيجة، حيث أن تحقق النتيجة في موضوع معينة يعتبر من عناصر النتيجة الإجرامية[115] ، ولكن لا يشترط أن يتوقع الجاني حدوث الضرر الذي سوف يلحق بالنظام المعلوماتي محل الدخول كأثر مباشر لدخوله، كما لا تشترط بعض التشريعات أن ينصرف قصد الجاني الى ما يترتب على الدخول من أفعال، كأتلاف البيانات أو تغيرها أو نقلها 116 ، بينما هناك بعض التشريعات التي تتطلب قصدا جنائيا خاصاً في هذه الجريمة وسيقوم الباحث في بيانها في الفرع الثاني من هذا المطلب.

[115] – نائلة قورة، مرجع سابق، ص٣٦٦.

116 – أسامة العبيدي، المرجع نفسه.

المطلب الثاني

القصد الإجرامي الخاص

وقد تطلبت بعض التشريعات في جريمة الدخول الغير مصرح به الى النظام المعلوماتي قصداً خاصاً الى جانب القصد العام، ويترتب على توفر القصد الإجرامي الخاص تشديد العقوبة في كثير من الأحيان، ففي الدنمارك تشدد العقوبة أذا ارتكبت الجريمة بنية معرفة المعلومات تتعلق بأسرار إحدى الشركات التجارية[117]، وكذلك في استراليا تشدد عقوبة جريمة الدخول الغير مصرح به الى النظام المعلوماتي متى ارتكب الجريمة بهدف الأضرار بالغير[118] ، أما في البرتغال فالقانون البرتغالي يتطلب قصداً جنائيا خاصاً حيث عاقب القانون البرتغالي الصادر في المادة السادسة من القانون رقم ٢٠٩\١٠٩ منه بشأن الجرائم المعلوماتية في حال كان الهدف من الدخول الحصول على فائدة أو ربح غير مشروع كما شدد القانون البرتغالي العقوبة في حال كانت الفائدة أو الربح مرتفعتين[119]، وفي المملكة المتحدة تطلب القانون توافر قصداً جنائياً خاصاً متى ارتكبت جريمة الدخول بقصد ارتكاب جريمة أخرى لاحقة على الدخول الغير مشروع[120].

117القانون الدنماركي، الرجاء النظر:

- https://www.coe.int/en/web/octopus/country-legislative-profile/-/asset_publisher/LA6eR74aAohY/content/denma-1?_101_INSTANCE_LA6eR74aAohY_viewMode=view#article2. 9/11/2019

[118] سمير علي، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراة، كلية الحقوق- جامعة القاهرة، ٢٠١٣،ص ١٠٩.

[119] قانون الجرائم المعلوماتية البرتغالي، الر جاء النظر:

https://www.anacom.pt/render.jsp?contentId=985560-. 9/11/2019

[120] قانون أساة استخدام الحاسب الآلي البريطاني، الرجاء النظر:

https://www.legislation.gov.uk/ukpga/1990/18/section/2.9/11/2019

أما بالنسبة الى التشريعات العربية فيما يتعلق بالقصد الجنائي الخاص، نجد أن أغلبها قد جرم الدخول الذي يقصد منه الجاني غاية معينة مثل القانون الإماراتي**121**، وكذلك القانون السوداني تطلب قصداً إجرامياً خاصاً حيث نصت المادة الرابعة منه على "**كل من يدخل موقعاً أو نظاماً معلوماتياً من دون أن يكون مصرحاً له :**

أ- بالاطلاع عليه أو نسخه يعاقب بالسجن مدة لا تجاوز سنتين أو بالغرامة أو بالعقوبتين معًا

ب-إلغاء بيانات أو معلومات ملكًا للغير أو حذفها أو تدميرها أو إفشائها أو إتلافها أو تغييرها أو إعادة نشرها أو تغيير تصاميم الموقع أو إلغائه أو شغل عنوانه ، يعاقب بالسجن مدة لا تجاوز أربع سنوات أو بالغرامة أو بالعقوبتين معًا "

- ولقد جرم القانون العماني الدخول متطلباً قصداً اجرامياً خاصاً، أذا كان الهدف من الدخول الحصول على معلومات أو بيانات الحكومية الإلكترونية السرية بطبيعتها وكذلك الدخول عمداً الى المواقع الإلكترونية، بقصد تعدله أو تغير تصميمه أو إلغائه أو إتلافه"[122]

وسار المشرع السعودي على خطى المشرع السوداني حيث تطلب في جريمة الدخول قصداً اجرامياً خاصاً حيث نصت المادة الثالثة البند الثالث منه على أن" **يعاقب بالسجن مدة لا تزيد عن سنه وبالغرامة التي لا تزيد عن خمسمائة ألف ريال، أو بأحد هاتين العقوبتين كل شخص يرتكب أحد الجرائم المعلوماتية التالية:**

[121] – عبد الإله النوايسة، مرجع سابق، ص ٥١.

[122] – قانون مكافحة تقنية المعلومات العماني، الصادر بمرسوم سلطاني رقم ١٢، سنه ٢٠١٢، المادة الثالثة.

3 - الدخول غير المشروع الى موقع إلكترونيا و الدخول الى الموقع الكتروني لتغير تصاميم هذا الموقع أو أتلافه أو تعديله أو شغل عنوانه"[123]

حيث يتضح من النص السابق أن جريمة الدخول بغير وجه حق لا تتحقق مكتملة الأركان الا اذا كان الهدف من الدخول تغير تصميم الموقع أو تعديله أو أتلافه.

ولم يرد أي نص في القانون القطري حول القصد الإجرامي الخاص، ويعني ذلك ان المشرع القطري تطلب توافر القصد العام أي تتحقق الجريمة بمجرد الدخول من دون أن يكون هناك أي هدف من وراء هذا الدخول، ولكن غلظ العقوبة في حال ترتب على الدخول الحصول على بيانات او اتلافها او تعديله وذلك في نص المادة الثالثة الفقرة الثانية حينما نص على انه "وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول إلغاء أو حذف أو إضافة أو إفشاء أو إتلاف أو تغيير أو نقل أو التقاط أو نسخ أو نشر أو إعادة نشر بيانات أو معلومات إلكترونية مخزنه في النظام المعلوماتي، أو إلحاق ضرر بالمستخدمين أو المستفيدين، أو تدمير أو إيقاف أو تعطيل الموقع الإلكتروني أو النظام المعلوماتي أو الشبكة المعلوماتية، أو تغيير الموقع الإلكتروني أو إلغائه أو تعديل محتوياته أو تصميماته أو طريقة استخدامه أو انتحال شخصية ماله أو القائم على إدارته"[124]

---

[123] الرجاء النظر
https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Documents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf، ٢٠١٩/٩/٢٢.

[124] – قانون مكافحة الجرائم الإلكترونية القطري، مرجع سابق.

ويتضح من النص السابق ان المشرع القطري لم يتطلب قصداً اجرامياً خاص في جريمة الدخول بغير وجه حق، وانما اكتفى بمضاعفة العقوبة في حال ترتب على الدخول المساس بالبيانات او المعلومات داخل جهاز الحاسب الآلي.

حيث أخذ القانون القطري بما أخذت به الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث نصت المادة السادسة منها على جريمة الدخول، وفي البند الثاني من ذات المادة شددت العقوبة في حال ترتب على الدخول المساس بالمعلومات بأي طريقة كانت سواء بالحذف او الإضافة او التعديل أو غيرها[125].

[125] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، القاهرة، المادة السادسة، ٢٠١٠\١٢\٢١.

المبحث الخامس

العقوبات المقررة لجريمة الدخول بغير وجه حق

سنتناول في هذا المبحث في عدت مطالب، سيتحدث الباحث في المطلب الأول عن العقوبة الأصلية والظروف المشددة، وفي المطلب الثاني العقاب على الشروع، وفي المطلب الثالث عن الإعفاء من العقوبة.

المطلب الأول

العقوبة الأصلية والظروف المشددة

فرضت جميع التشريعات التي جرمة جريمة الدخول بغير وجه حق عقوبات أو جزاءات أصلية توقع على مرتكب جريمة الدخول، ويقصد بالعقوبة الأصلية الجزاء الذي يقرره القانون للجريمة المرتكبة، كما أنه لا توجد أي جريمة لم يحدد لها المشرع عقوبة ، سواء كانت العقوبة سالبة للحرية أو الغرامة المالية ، وقد ميزت التشريعات المقارنة في تكيف الجريمة، فاذا كانت الجريمة بصورتها البسيطة مثل الدخول المجرد أو الجريمة بصورتها المشددة تأخذ وصف الجنحة، أما اذا كان الهدف في بعض الحالات من الدخول الحصول على معلومات تخص أمن الدولة تأخذا الجريمة وصف الجناية [126].

وقد شددت التشريعات العقوبة في حال ترتب علي الدخول ضرر مثل المشرع الفرنسي في المادة ١-٣٢٣ من قانون العقوبات الفرنسي في حال ترتب على الدخول إلغاء أو حذف بينات النظام أو

[126] – عبدالإله النوايسة، المرجع نفسه، ص ٦٧.

الأخلال بسير النظام فالعقوبة الأصلية هي سنتان حبس والغرامة التي لا تزيد عن ٣٠ ألف يورو وشدد العقوبة في حال ترتب على الدخول أي من الأفعال السابق ذكرها فقرر عقوبة الحبس لمدة ثلاث سنوات وبالغرامة التي لا تزيد عن ٤٥ ألف يورو،[127]

وفي ذات الإطار اتجه القانون العماني والقطري أتجاه القانون الفرنسي حيث نصت المادة الثالثة من قانون مكافحة تقنية المعلومات حيث عاقب على الجريمة بالسجن مدة لا تقل عن شهر ولا تزيد على سته أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بأحد هاتين العقوبتين ، وشدد العقوبة الى في حال ترتب على الدخول ي ضرر و كانت المعلومات شخصية بحيث تزيد العقوبة آلي سته أشهر ولا تتزيد عن ثلاث سنوات وغرامة ألف ريال عماني.[128]

أما بالنسبة لقانون مكافحة الجرائم الإلكترونية القطري فقد غلظ العقوبة في حالتين تم ذكرهما في المادة الثانية والثالثة من ذات القانون فقد نص المشرع في الفقرة ٢ من المادة الثانية على" وتُضاعف العقوبة المنصوص عليها في الفقرة السابقة، إذا ترتب على الدخول الحصول على بيانات أو معلومات إلكترونية، أو الحصول على بيانات أو معلومات تمس الأمن الداخلي أو الخارجي للدولة أو اقتصادها الوطني أو أية بيانات حكومية سرية بطبيعتها أو بمقتضى تعليمات صادرة بذلك، أو

---

[127] –French criminal code, o*rdinance no. 2000-916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January 2002, (Act no. 2004-575 of 21 June 2004 article 45 I Official Journal of 22 June 2004) Article no 323-1.*

[128] – قانون مكافحة تقنية المعلومات العماني، مرجع سابق، المادة الثالثة.

إلغاء تلك البيانات والمعلومات الإلكترونية أو إتلافها أو تدميرها أو نشرها، أو إلحاق الضرر بالمستفيدين أو المستخدمين، أو الحصول على أموال أو خدمات أو مزايا غير مستحق"[129].

نستنتج من النصوص السابقة بأن المشرع القطري في قانون مكافحة الجرائم الإلكترونية ضاعف العقوبة الاصلية في حال تم الحصول على معلومات تخص أمن الدولة أو أمنها الاقتصادي، أو ترتب على هذا الدخول الضرر، إي أن المشرع القطري جرم الدخول المجرد الى النظام المعلوماتي، وشدد العقوبة في حال حدوث نتيجة إجرامية مثل الحصول على البيانات أو اتلافها أو تغيرها.

كما أن هناك تشريعات أخرى شددت العقوبة في حال ارتكب الجريمة موظف عام مسؤول عن النظام المعلوماتي، مثل القانون الأردني والقانون السوادني حيث نص الأخير في المادة الخامسة منه على أنه " كل موظف عام، يدخل بدون تفويض موقع أو نظام معلومات خاص بالجهة التي يعمل بها أو يسهل ذلك للغير ، يعاقب بالسجن مدة لاتتجاوز خمس سنوات أو بالغرامة أو بالعقوبتين معًا ."[130]

ونص المشرع الأردني في الجرائم الإلكترونية على جريمة الدخول في المادة ٣ /أ وعاقب عليها بالسجن مدة لا تقل أسبوع ولا تزيد عن ثلاث أشهر وبالغرامة التي لا تزيد عن ٢٠٠دينار ،وفي الفقرة ب شدد العقوبة اذا ترتب على الدخول ضرر وأوصل العقوبة الى بالسجن مدة لا تقل عن ثلاث أشهر ولا تزيد عن سنه وبغرامة لا تزيد عن ١٠٠٠ دينار، وضاعف العقوبة في المادة الثامنة من ذات القانون اذا تم ارتكابه من شخص اثناء تأدية وظيفته أو بسببها. [131]

---

[129] – قانون مكافحة الجرائم الإلكترونية القطري، مرجع سابق، المادة الثانية.

[130] – قانون جرائم المعلوماتية السوداني، مرجع سابق، المادة ٥.

[131] – قانون الجرائم الالكترونية الأردني، مرجع سابق، المادة ٣.

وبالنسبة للمشرع القطري ضاعف في المادة ٥١ من قانون مكافحة الجرائم الالكترونية العقوبة في حال تم ارتكاب او تسهيل ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون من قبل موظف عام الموظف العام أي من الجرائم المنصوص عليها في هذا القانون بالضعف للعقوبة المقررة للجريمة المرتكبة.

المطلب الثاني

العقاب على الشروع

اختلفت التشريعات في العقاب على الشروع في الدخول الغير مصرح به للنظام المعلوماتي، حيث لم تسر جميع التشريعات على منهج واحد خاص في العقاب على الشروع، فلم ينص المشرع الأسترالي على الشروع في قانون الجرائم الإلكترونية لسنة ٢٠٠١، كما عاقب المشرع الفرنسي والمشرع البلجيكي على الشروع في جريمة الدخول الغير مصرح به بنفس العقوبة الجريمة التامة، ولم يذكر أي نص في القانون النرويجي والألماني على نصوص بشأن الشروع في جريمة الدخول الغير مصرح به، أما بالنسبة للتشريعات العربية نجد أن هناك بعض المشرعين مثل المشرع الإماراتي والكويتي والأردني لم ينص على الشروع ، وبذلك يتم تطبيق القواعد العامة بالنسبة للشروع فيما يتعلق بجريمة الدخول الغير مشروع، وبالنسبة للقانون السعودي والعماني والسوداني ،يكون العقاب على الشروع فيها بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة للجريمة التامة [132]،

وبالنسبة للشروع في جريمة الدخول بغير وجه حق في القانون القطري، فهل يتصور الشروع في هذه الجريمة أم لا؟

من حيث الأصل أن الشروع يقع في الجرائم ذات النتيجة ولا يتصور في الجرائم الشكلية، وذهب جانب من الفقه الى ان الشروع غير متصور في جريمة الدخول بغير وجه حق كونها من الجرائم الشكلية التي لا تتطلب تحقق نتيجة معينة [133]، ولكن ومن وجهة نظر الباحث أن الشروع يتصور في جريمة الدخول بغير وجه حق، حيث تم تعريف الشروع في القانون القطري بأنه " الشروع هو

---

[132] – عبد الإله نوايسة، مرجع سابق، ص ٧٣.

[133] – محمد علي سويلم، مكافحة الجرائم الالكترونية– دراسة مقارنة، دار المطبوعات الجامعية، الطبعة الأولى، القاهرة، ٢٠١٩، ص١٠٧.

البدء في تنفيذ فعل بقصد ارتكاب جناية أو جنحة، إذا أوقف أو خاب أثره لسبب لا دخل لإرادة الفاعل فيه"[134]. ومن خلال النظر الى النص السابق يتضح أن الشروع يقوم علي أساس البدء في تنفيذ الجريمة، والفاعل في جريمة الدخول بغير وجه حق عندما يقوم بمحاولة الدخول الى النظام المعلوماتي يعتبر شرع في ارتكاب هذه الجريمة، كما أنه وبالنظر الى التطور التكنلوجي في هذا العصر، جميع المواقع او الأنظمة المعلوماتية الخاصة بالدولة أو أحد مؤسساتها تحتوي علي نظام مراقبة فعال ومتطور بحيث يمكن اكتشاف محاولات الدخول بسهولة، فاذا تم اكتشاف الفاعل قبل دخوله أي اثناء محاولته للدخول على النظام المعلوماتي يجب أن يتم محاسبته على الشروع في الدخول، فليس من المقبول أن لا تتم محاسبته على أساس أن المشرع القطري اعتبر جريمة الدخول بغير وجه حق من الجرائم الشكلية، كما لا تعتبر محاولة الدخول الى الموقع أو النظام من الأعمال التحضيرية الغير معاقب عليها كون أن تلك الاعمال تعني عدم البدء في ارتكاب الجريمة ولكن جمع أو التخطيط للجريمة، فعلى سبيل المثال لا يمكن معاقبة شخص قام بشراء جهاز حاسب الي متقدم لاستخدامه بارتكاب جريمة الدخول كون ان عملية الشراء او جمع البرامج التي تساعده على ارتكاب جريمة الدخول تعتبر من الأعمال التحضيرية السابقة على التنفيذ، كما أن المشرع القطري وفي المادة ٥٤ من قانون مكافحة الجرائم الإلكترونية عاقب علي الشروع في الجرائم الالكترونية، مما يدل معه تصور المشرع للشروع في كافة الجرائم الإلكترونية.

[134] – قانون العقوبات القطري، مرجع سابق، المادة ٢٨ .

المطلب الثالث

الإعفاء من العقوبة

لقد نصت بعض التشريعات على الإعفاء من العقاب على جريمة الدخول الغير مصرح به، في حال قيام الجاني بالتبليغ قبل وقوع النتيجة الإجرامية أو وقوع الضرر، وفي حال وقوع الجريمة يستفيد من الإعفاء اذا كان من شأن البلاغ ضبط باقي الجناة في حال تعددهم، وهذا ما فعله المشرع السعودي، ولقد نص على ذلك المشرع القطري في المادة ٥٤ من قانون مكافحة الجرائم الإلكترونية حيث نصت على" **يعفى من العقوبات المنصوص عليها في هذا القانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأية معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر.**

ويجوز للمحكمة أن تقضى بوقف تنفيذ العقوبة، إذا حصل الإبلاغ بعد علم السلطات المختصة، وأدى إلى ضبط باقي الجناة" [135].

يستنتج من النص السابق أن المشرع القطري أعفا الجاني من العقاب في حال إبلاغه عن الجريمة قبل وقوعها أو وقوع الضر، وفي حال وقوع الجريمة وقام الجاني بالإبلاغ عن الجريمة وأدى بلاغه الى ضبط باقي الجناة في حال تعددهم، يجوز للمحكمة الحكم بوقف تنفيذ العقوبة، ويرى الباحث أن الغاية وراء اتجاه اغلبية التشريعات للإعفاء من العقاب على جريمة يؤدي الى إعطاء فرصة للجاني للرجوع عن هذا الفعل.

[135] - قانون مكافحة الجرائم الإلكترونية القطري، مرجع سابق.

الخاتمة

أن جريمة الدخول من الجرائم الخطيرة والمؤثرة على المجتمع، وذلك لما في هذه الجريمة من مساوئ على الصعيد الشخصي للفرد وعلى الدولة، حيث أن العدوان على البيانات والمعلومات المحفوظة على مواقع الدولة وأنظمتها المعلوماتية يمثل عدواناً على الدولة بحد ذاته، لذلك اتجه المشرع القطري الى تخصيص نص المادة الثانية من قانون مكافحة الجرائم الإلكترونية القطرية للمواقع والأنظمة المعلوماتية الخاصة بالدولة أو أحد أجهزتها، وتطرق الباحث في هذا الدراسة الى جريمة الدخول بغير وجه حق للأنظمة والمواقع الالكترونية الخاصة بالدولة وافرد مبحث خاصاً لدراستها، كما تطرق الباحث الى الركن المادي لهذه الجريمة والى عناصره الثلاث والمتمثلة في الدخول، وعدم التصريح ، طبيعة الجريمة، كما تطرق الى الركن المعنوي لهذه الجريمة والمتمثل في القصد الجنائي العام والخاص والى العقوبات المقررة ايضاً، وفي نهاية هذه الدراسة توصل الباحث بعد دراسة جريمة الدخول بغير وجه حق الى والمواقع الالكترونية، في القانون القطري وفي ضوء التشريعات المقارنة، الى العديد من **النتائج** وهي كالتالي:

1. إن الجرائم المعلوماتية عامة وجريمة الدخول خاصة لهم مخاطر وأضرار خطيرة، فقد تسبب هذه الجرائم خسائر مادية كبيرة تطال المؤسسات العامة والخاصة، وكذلك الخصوصية الفردية.
2. اتجهت كافة التشريعات العربية والمقارنة الى تجريم جريمة الدخول بغير وجه حق، وذلك من خلال أفراد نصوص خاصة بها في تشريعاتها الخاصة بالجرائم الالكترونية.
3. عدم القدرة على تطبيق نصوص القوانين العقابية التقليدية على مثل هذه الجرائم، لكونها جريمة تقنية تتطلب خبرات تقنية محددة على عكس الجرائم التقليدية، ولما في جريمة

الدخول بغير وجه حق من اختلاف عن الجرائم التقليدية بحيث تتطلب نصوص خاصة لتجريمها

4. لقد تباينت التشريعات في الدول حول كيفية مواجهة هذه الجريمة، فبعض الدول جرمت الدخول المجرد، وبعض الدول تطلبت توافر شروط موضوعية أو شكلية لتجريم هذه الجريمة.
5. اتجهت بعض التشريعات الى اعتبار جريمة الدخول من جرائم الشكلية التي تتم بمجرد الدخول، ولا يتطلب فيها حصول أي نتيجة إجرامية لقيامها، فتعتبر جريمة تامة بمجرد الدخول، اتجهت تشريعات الى اعتبارها من الجرائم ذات نتيجة، وهناك تشريعات اعتبرتها شكلية مع تغليظ العقوبة في حال ترتب ضرر مثل المشرع القطري.
6. هناك تشريعات اشترطت ان يكون النظام المعلوماتي او الموقع الالكتروني محمي بأحد وسائل الحماية الأمنية حتى يتم يخضع للحماية الجنائية مثل المشرع الكويتي، واتجهت تشريعات أخرى الى فرض الحماية على كافة المواقع الالكترونية والأنظمة المعلوماتية بغض النظر عن الحماية الأمنية مثل المشرع القطري.
7. أحسن المشرع القطري في تخصيص نص خاص يتعلق بجريمة الدخول الى المواقع الإلكترونية والأنظمة المعلوماتية التابعة للدولة، مما يدل ذلك على خطورة هذه الجريمة إذا وقعت على الأنظمة والمواقع التابعة للدولة
8. جريمة الدخول بغير وجه حق من الجرائم التي يتصور فيها الشروع في القانون القطري

التوصيات

1. يجب علي التشريعات التي اشترطت تحقق نتيجة إجرامية في جريمة الدخول الى تجريم الدخول المجرد الى النظام المعلوماتي، من دون اشتراط تحقق الضرر نتيجة الدخول، وذلك للحد من جرائم الدخول بغير وجه حق.
2. نتمنى من المشرع القطري أن يعرف الهيئات والمؤسسات العامة والأجهزة والشركات التابعة لها في باب التعريفات في قانون مكافحة الجرائم الالكترونية.
3. نتمنى من المشرع القطري النص على الدخول بغير وجه حق الى المواقع الالكترونية المحمية بحماية أمنية مع تشديد العقوبة على مرتكبها.
4. النص صرحتاً على الشروع في جريمة الدخول بغير وجه حق، كون ان المادة ٥٤ الواردة في قانون مكافحة الجرائم الالكترونية جاءت عامة لكافة الجرائم الالكترونية، مما قد يؤدي ذلك الى لبس بشأن الشروع في جريمة الدخول.
5. تشديد العقوبة الواردة في نص المادة الثانية في حال الدخول المجرد الى المواقع والأنظمة المعلوماتية التابعة للدولة، وعدم مساوة الدخول الي المواقع العامة مع المواقع الخاصة.
6. النص على تجاوز التصريح واستغلاله في المادة الثانية من قانون مكافحة الجرائم الالكترونية القطري والمتعلقة بالجهات والأجهزة الحكومية، حيث أن المشرع القطري نص على تجاوز التصريح أو استغلاله في المادة الثالثة دون المادة الثانية ، حيث كان من باب أولى على المشرع أن ينص عليها في المادة الثانية.
7. ضرورة تكوين لجان تحقيق خاصة بالجرائم المعلوماتية، تكون لديها جميع الخبرات التقنية والفنية، وتدريب منسوبيها على طريقة التعامل مع هذا النوع من الجرائم.

8. يجب نشر الوعي والثقافة القانونية لدى مستخدمي الشبكة المعلوماتية حتى لا يضحو ضحية لأعمال الاختراق، ولكي لا تتعرض بيانتهم ومعلوماتهم للسرقة.

قائمة المصادر والمراجع

المراجع باللغة العربية:

1. أسامة العبيدي، جريمة الدخول غير المشروع الى النظام المعلوماتي: دراسة قانونية في ضوء القوانين المقارنة، مجلة الدراسات المعلومات، العدد ١٤، جمعية المكتبات والمعلومات السعودية، ٢٠١٢.
2. أسامة ألمناعسة وجلال الزعبي، جرائم تقنية المعلومات الالكترونية، الطبعة الثانية، دار الثقافة للنشر، عمان– الأردن، ٢٠١٧.
3. أشرف شمس الدين، شرح قانون العقوبات القطري القسم العام: النظرية العامة للجريمة والعقوبة، الطبعة الأولى، جامعة قطر، ٢٠١٠.
4. اكرم المشهداني، "الجرائم الالكترونية"، مجلة الأكاديمية العربية للعلوم المالية والمصرفية، المجلد ٢٣، العدد ١، ٢٠١٥.
5. بوريدي مختاره، ماهية الجرائم الإلكترونية اعمال الملتقى الوطني: آليات مكافحة الجريمة الإلكترونية، الجزائر ، ٢٩ مارس،٢٠١٧.
6. حسن المناصير، جريمة الدخول غير المشروع الى النظام المعلوماتي والتعدي على محتوياته: دراسة مقارنة، رسالة ماجستير ، جامعة جرش، الأردن.
7. حسين الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت "دراسة مقارنة"، رسالة دكتوراه، جامعة عين شمس، القاهرة ٢٠٠٩.
8. حنان المضحكي، الجرائم المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، ٢٠١٤.

9. دينا فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي، الطبعة الأولى ، دار النهضة العربية و دار النهضة العلمية الإمارات، ٢٠١٨.

10. رشدى علي، الحماية الجنائية للمعلومات على شبكة الإنترنت، دراسة مقدمة لنيل درجة الدكتور في الحقوق، جامعة القاهرة، كلية الحقوق، قسم القانون الجنائي، سنه ٢٠٠٩.

11. سامي الرواشدة– أحمد هياجنة، "مكافحة الجرائم المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجا"، المجلة الأردنية في القانون والعلوم السياسية، المجلد ١، العدد٣، ٢٠٠٩.

12. سمير علي، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه، كلية الحقوق– جامعة القاهرة، ٢٠١٣.

13. شيماء عبدالغني، " الحماية الجنائية للتعاملات الإلكترونية"، رسالة ماجستير، جامعة المنصورة – كلية الحقوق–، ٢٠٠٧.

14. طارق سرور، قانون العقوبات القسم الخاص : جرائم الاعتداء على الأشخاص والأموال، الطبعة الأولى، لا يوجد دار نشر، كلية القاهرة، مصر، ٢٠٠٤.

15. عبد الإله النوايسة، جرائم تكنلوجيا المعلومات: شرح الأحكام الموضوعية لقانون الجرائم الإلكترونية، الطبعة الأولى، دار وائل للنشر والتوزيع، سنه٢٠١٧.

16. عبدالفتاح حجازي، جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، ٢٠٠٦.

17. عمار عباس الحسيني، جرائم الحاسوب والانترنت : الجرائم المعلوماتية، الطبعة الأولى، منشورات زين الحقوقية، بيروت –لبنان، ٢٠١٧.

18. محمد سليمان الخوالدة، جريمة الدخول غير المشروع الى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني: دراسة مقارنة، رسالة ماجستير، الجامعة الأردنية "كلية الدراسات العليا"، الأردن ، ٢٠١٢.

19. محمد عبدالقادر، "التعويض عن الضرر على الاعتداء على حق الأنسان في حرمة مسكنه في ضوء الوثيقة الخضراء الكبرى لحقوق الانسان في عصر الجماهير وبعض النظم المعاصرة"، جامعة بنغازي – كلية الحقوق، لا يوجد رقم للمجلد، العدد ١٧، ٢٠٠٨.

20. محمد علي سويلم، مكافحة الجرائم الالكترونية– دراسة مقارنة، دار المطبوعات الجامعية، الطبعة الأولى، القاهرة، ٢٠١٩.

21. مدحت أبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي . دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠١٥.

22. مصطفى عرب، "جرائم الحاسوب: دراسة مقارنة"، رسالة ماجستير، ا لجامعة الأردنية، عمان– الأردن،١٩٩٤.

23. مهند وليد أسماعيل، التنظيم القانوني لجريمة الدخول الغير مصرح به الى نظام الحاسب الآلي: دراسة مقارنة، مجلة العلوم الشرعية– جامعة القصيم، المجلد ١١، العدد، ١، ٢٠١٧.

24. نائلة قورة، جرائم الحاسب الآلي الاقتصادية : دراسة نظرية وتطبيقية، الطبعة الأولي، منشورات الحلبي، مصر، ٢٠٠٤.

25. نجوى نجم الدين، "جريمة السرقة عبر الوسائل الإلكترونية: دراسة مقارنة"، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد ٦، العدد٢١ ، ٢٠١٧.

التشريعات:

1 – قانون مكافحة الجرائم الالكترونية القطري، رقم ١٤، لسنة ٢٠١٥

2 – قانون العقوبات القطري، رقم ١١، لسنة ٢٠٠٤.

3 – قانون الاتصالات القطري، رقم ٣٦، لسنة ٢٠٠٦.

4 – قانون جرائم تقنية المعلومات البحريني، رقم ٦٠، لسنة، ٢٠١٤.

5 – قانون الهيئات والمؤسسات العامة القطري، رقم ٢٦، لسنه٢٠٠٤.

6 – قانون المؤسسات الخاصة ذات النفع العام القطري، رقم ٢١، لسنة ٢٠٠٦

7 – قانون الشركات القطري، رقم ١١، لسنة ٢٠١٥.

8 – قانون مكافحة جرائم تقنية المعلومات المصري، رقم ١٧٥، لسنه ٢٠١٨.

9 – قانون جرائم المعلوماتية السوداني، القانون رقم ١٣، الصادر في سنه ٢٠٠٧.

10 – قانون تنظيم التواصل على الشبكة ومكافحة الجرائم المعلوماتية السوري، رقم ١٧، لسنه ٢٠١٢.

11 – قانون مكافحة تقنية المعلومات العماني، الصادر بمرسوم سلطاني رقم ١٢، سنه ٢٠١٢.

12 – قانون جرائم تقنية المعلومات الاماراتي، مرسوم اتحادي رقم ٥، لسنه ٢٠١٢.

13 – قانون مكافحة الجرائم المعلوماتية الكويتي، رقم ٦٣، لسنة ٢٠١٥.

14 – قانون الجرائم الالكترونية قانون الجرائم الالكترونية الأردني، رقم ٢٧، لسنة ٢٠١٥.

معاهدات واتفاقيات دولية:

1. الإعلان العالمي لحقوق الأنسان، الصادر في باريس، سنه ١٩٤٨، المادة ١٢

2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، القاهرة، ، ٢١\١٢\٢٠١٠.

احكام قضائية

1. حكم محكمة التميز القطرية، الأحكام الجنائية، الطعن رقم٢٢٩، لسنة ٢٠٠٩.

المراجع باللغات الأجنبية:

1. French criminal code, ordinance no. 2000-916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January 2002, (Act no. 2004-575 of 21 June 2004 article 45 I Official Journal of 22 June 2004.
2. -Sami AL-Rawashdeh, Illegal Access to Information Systems in Qatari Criminal Law: A Comparative Study, Kuwait International Law School Journal - Volume 6 - Issue 1 - Ser. No. 21 - Jumada Al-Akhirah 1439 - Rajab 1439 - March 2018

مراجع شبكة الإنترنت:

1. Ihttps://www.un.org/ar/universal -declaration-human-rights/index.html
2. https://weziwezi.com أنواع-نظم-المعلومات/

3. http://bib.univoeb.dz:8080/jspui/bitstream/123456789/213/1مفهوم/
.العمومية20%المؤسسة20%pdf.
4. https://www.citc.gov.sa/ar/RulesandSystems/CITCSystem/Docum
ents/LA_004_%20A_%20Anti-Cyber%20Crime%20Law.pdf ،
٢٠١٩\١٠\١٧
5. https://elawpedia.com/view/67/تعريف-المرفق-العام-والعناصر-المميزة-له
6. https://www.aljazeera.net/knowledgegate/newscoverage/2017/6/1
1.مقاطعة-قطر-وحصارها-آثار-ونتائج/
7. https://www.legislation.gov.uk/ukpga/1990/18/section/2
8. https://www.anacom.pt/render.jsp?contentId=985560
9. https://www.coe.int/en/web/octopus/country-legislative-profile/-
/asset_publisher/LA6eR74aAohY/content/denma-
1?_101_INSTANCE_LA6eR74aAohY_viewMode=view#article2
10. https://www.cybercrimelaw.net/Belgium.html
11. https://www.cybercrimelaw.net/Grecce.html
12. http://www.legislation.govt.nz/act/public/1961/0043/latest/D
LM330422.html.
13. https://www.cybercrimelaw.net/Italy.html.
14. https://www.cybercrimelaw.net/Norway.html
15. https://www.anacom.pt/render.jsp?contentId=985560

16. https://www.legislation.gov.uk/ukpga/1990/18/section/2