الحماية الجنائية للأنظمة المعلوماتية عن جريمة الدخول دون وجه حق: في القانون القطري والمقارن

الباحث: خالد فهد المحمدي
ماجستير في القانون العام - جامعة قطر

الملخص

تستعرض هذه الورقة البحثية إحدى صور الجريمة الإلكترونية، وهي جريمة الدخول دون وجه حق، وذلك من خلال البحث في مدى جدارة الأنظمة الالكترونية – غير المحمية- للحماية القانونية، ومدى شمول تلك الحماية عن الاعمال التحضيرية ومبدأ الشروع في ارتكاب الجريمة، وفي إطار ذلك نقارن ما بين القانون القطري والقوانين المقارنة.

وقد أصبح ارتكاب الجريمة الإلكترونية مفتاحاً لمختلف الجرائم المتنوعة، وهو النهج الجديد للجناة خاصة مع التطور الرقمي المستمر، ففي المطلب الأول نتناول مسألة الحماية الالكترونية للأنظمة المعلوماتية، ومدى اعتبارها شرطاً للحصول على الحماية القانونية.

ومما لا شك فيه أن الطبيعة الإلكترونية والمعنوية للجريمة الالكترونية تصعب إعمال مجموعة من المبادئ العامة في علم الاجرام والعقاب ولا سيما مرحلتي الاعمال التحضيرية والشروع وهو مجال البحث في المطلب الثاني.

وخلصت الدراسة في الختام إلى عدّة نتائج وتوصيات، التي تساهم في زيادة فعالية المواجهة الجنائية للجريمة الالكترونية وفهم ابعادها وتطوير النظم القانونية للتصدي لها.

Abstract

This paper studies one of type of cybercrimes, known as hacking. It goes through different aspects of the crime that all deals mainly with the criminal protection of the information systems, programs, and technology. Cybercrimes is proven to be the key/opening to different types of crimes, and it is favored by criminals. In the first chapter of this paper, we will look at the "System Protection Programs" and whether it is a must for the privilege of legal protection or not. Additionally, the paper will discuss fundamental ideas of all crimes, specifically the idea of "Attempted Crimes" and "Preparation Works of the Crime" and that in the second chapter. The study reaches a number of conclusions and remedies that mainly aim for increasing the criminal confrontation of cybercrimes and understanding the new aspects of that crime with regards to fundamental criminal law ideas.

المقدمة:

تدرجت الحماية الجنائية للأنظمة المعلوماتية أو الإلكترونية وتنوعت بين مختلف التشريعات القطرية، فنص عليها قانون العقوبات القطري رقم ١١ لسنة ٢٠٠٤ في الفصل الخامس بعنوان جرائم الحاسب الآلي ونظمها في المواد ٣٧٠ الى ٣٨٧، ولكن بالنسبة لجريمة الدخول دون وجه حق او الدخول غير المشروع كان يُنظر اليها من ناحية الدخول المادي الى الحاسب الالي وليس الدخول المعنوي او الذي يتم عن طريق شبكة الانترنت[1235]، ومع التطور السريع للشبكة المعلوماتية وللعالم الرقمي، ظهرت الحاجة الماسة لتجديد النصوص الواردة في قانون العقوبات، فصدر في عام٢٠١٤ القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، وتضمن قواعد واحكام حديثة تتماشى مع المفهوم المتطور للجريمة الالكترونية، وقد عاقب القانون على أفعال الدخول دون وجه حق الى النظام المعلوماتي، حيث نص في الفصل الأول: (جرائم التعدي على أنظمة وبرامج وشبكات المعلومات والمواقع الإلكترونية) من القانون [1236] على تجريم أفعال الدخول دون وجه حق، فقد نصت المادة 2 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." وكذلك نصت المادة 3 على: " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، 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.

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."

نتناول في هذا البحث موقف المشرع القطري وشقيقه الكويتي وغيره من القوانين المقارنة بشأن مدى اشتراط حماية النظام المعلوماتي لكي يصلح للحماية القانونية وذلك في المطلب الأول، ثم نستعرض مبدأي الشروع والاعمال التحضيرية في المطلب الثاني.

أولا: موضوع البحث

1235 الانترنت (Internet): هو شبكة عالمية تربط الملايين من أجهزة الحاسوب في العالم بأسره، وتعد نوع من أنواع الشبكات المعلوماتية، راجع: احمد يوسف الكواري، المرجع السابق، ص٢.

1236 القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية.

تُشكّل الجريمة الإلكترونية تحديًا صعبًا أمام نظم المكافحة والنظم العدلية الوطنية، ويتطلّب هذا الأمر بذل جهود مُضاعفة لمكافحتها ومواكبة تطورها السريع. إنّ هذا الأمر يضع حقيقة أمام الأطراف المعنيّة بهذه المسألة العديد من الإشكاليّات والتحدّيّات.

ثانيا: أهمية البحث

تأتي اهمية كتابة هذا البحث، والذي تناولنا به على وجه الخصوص جريمة الدخول غير المشروع لموقع الإلكتروني او نظام معلوماتي او شبكة معلوماتية، من طبيعة الجريمة الإلكترونية الخاصة، والتي تعد حديثة وتتقدم باستمرار، بوسائل ارتكابها وصورها، الأمر الذي يجب معه مواكبة هذه التطورات بتشريعات تنظمها وتحيط بها حفاظا على الحقوق، وبهدف تحقيق العدالة. ولدراستنا هذه اهمية خاصة، لاسيما وبأخذنا عين الاعتبار قلة الكتابات في ضوء القانون القطري، وندرة احكام محكمة التمييز، الأمر الذي يجعل المجال خصباً للأرآء الفقهية المختلفة، ومن خلفيات تشريعية وقانونية مختلفة.

ثالثاً: منهجية البحث

سوف نتبع في هذا البحث المنهج الوصفي التحليلي مع المقارنة بين القانون القطري وما ذهبت إليه القوانين المقارنة، وذلك عن طريق الاطلاع على نصوص القانون ذات العلاقة، وإدراج آراء الفقهاء في موضوع البحث، وأحكام المحاكم والسوابق القضائية مع التعليق عليها بالرأي كلما أمكن ذلك.

رابعاً: مُشكلات البحث:

تتحدّد إشكاليات دراستنا هذه، في الآتي: -

- ما مدى تمتع، الأنظمة الالكترونية غير المحمية بنظم الحماية المختلفة، بالحماية القانونية أو الجنائية؟
- ما هو موقف المشرع القطري بشأن توفير الحماية القانونية للأنظمة غير المحمية؟
- متى يعد الفعل في نطاق جريمة الدخول دون وجه حق، شروعاً أو عملاً تحضيرياً؟

المطلب الأول: مدى جدارة الأنظمة القانونية -غير المحمية - للحماية القانونية

إن الجريمة الالكترونية بطبيعتها التي لا تعترف بالحدود المادية والسياسية حتى تم تصنيفها من بين الجرائم العابرة للحدود، وجرائم مثل جريمة الدخول غير المشروع على المواقع الالكترونية عادة ما يترتب عليها جرائم أخرى تكون بمثابة المفتاح لها، كالاحتيال أو الاتلاف للمواقع الالكترونية أو السرقة أو غيرها من الجرائم[1237]. تكفل القوانين الحماية القانونية للأنظمة الالكترونية، وتنظم القواعد الأمنية المختلفة الإجراءات التي تحيط بتلك الأنظمة بحسب نظم الإدارة المتبعة، وتتدرج النظم الأمنية من كونها مجرد حفظ احتياطي للبيانات (Back-up) الى ان تصل الى الحماية المشفرة (Encryption).

1237د. راشد محمد المري، الجرائم الالكترونية: في ظل الفكر الجنائي المعاصر: دراسة مقارنة، دار النهضة العربية، جمهورية مصر العربية،٢٠١٨، ص٧٦.

والجدير بالذكر، هو أن القانون القطري لم ينص على اشتراط خضوع الأنظمة الالكترونية للحماية كشرط للحصول على الحماية القانونية، ولكنه نص على اشتراطات مشابهه في قانون حماية خصوصية البيانات الشخصية رقم ١٣ لسنة ٢٠١٦، حيث تنص المادة ١١ من القانون على عدة التزامات على المراقب ومنها وضع النظم التي تهدف لحماية البيانات الشخصية[1238]، ويأتي هذا النص مماثلا

لنص نظام حماية البيانات العامة الصادر عن المجلس الأوروبي GENERAL DATA PROTECTION REGULATIONفي المادة ٥ على ذات الالتزام على معالج البيانات[1239]، وتجدر الإشارة بالإيجاز الذي تحدده طبيعة هذه الدراسة، ان نصوص قانون حماية خصوصية

1238 انظر: المادة ١١ من قانون حماية خصوصية البيانات الشخصية رقم ١٣ لسنة ٢٠١٦:

"على المراقب اتخاذ الإجراءات التالية:

-1مراجعة إجراءات حماية الخصوصية قبل إدراج عمليات معالجة جديدة.

-2تحديد المعالجين المسؤولين عن حماية البيانات الشخصية.

-3تدريب المعالجين على حماية البيانات الشخصية.

-4وضع نظم داخلية لتلقي ودراسة الشكاوى، وطلبات الوصول للبيانات، وطلبات تصحيحها أو حذفها، وإتاحة ذلك للأفراد.

-5وضع نظم داخلية للإدارة الفعالة للبيانات الشخصية، والإبلاغ عن أي تجاوز للإجراءات التي تهدف إلى حمايتها.

-6استخدام الوسائل التكنولوجية المناسبة لتمكين الأفراد من ممارسة حقهم في الوصول إلى البيانات الشخصية ومراجعتها وتصحيحها بشكل مباشر.

-7إجراء عمليات تدقيق ومراجعة شاملة عن مدى الالتزام بحماية البيانات الشخصية.

-8التحقق من التزام المعالج بالتعليمات التي يوجهها إليه، واتخاذ الاحتياطات المناسبة لحماية البيانات الشخصية، ورصد ومتابعة ذلك بصفة مستمرة."

1239 انظر: المادة ٥ الفقرة السادسة من نظام حماية البيانات العامة الأوروبي

"Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a)processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');

(d)accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e)kept in a form which permits identification of data subjects for no h than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with r 89(1) subject to implementation of the appropriate technical and organizational

البيانات الشخصية القطرية جاء مشابهاً ومحتوياً على العديد من القواعد المشتركة مع نظيره الأوروبي، ولكن ما يساهم في فعالية القانون الأوروبي هو تطبيقه لدى الدول الأوروبية بإجماع، وهو ما لا يوجد له مثيل فيما بين الدول العربية الى يومنا الحالي.

وثار خلافاً بين الفقه الفرنسي، حول؛ مدى جدارة الأنظمة الإلكترونية غير المحمية بأنظمة الحماية الإلكترونية، للحماية القانونية ضد أفعال الدخول غير المشروع، وذهب رأي من الفقه الفرنسي الى القول، انه لا تقبل حماية الأنظمة الإلكترونية التي لم يضع أصحابها الحماية اللازمة لمنع دخول الغير اليها بشكل غير مصرح أو مشروع، واسس هذا الرأي قوله على القياس مع جريمة انتهاك حرمة المساكن، حيث لا تقوم الجريمة اذا كان الدخول الى المسكن مصحوباً بوسائل تشير الى عدم رضاء صاحب ذلك المنزل، فذهب انصار هذا الرأي أن النظام الإلكتروني، لكي يتمتع بالحماية القانونية، يجب ان يكون متمتعاً بنظم الحماية الإلكترونية، والسبب في ذلك يرجع الى؛ أن طبيعة شبكة المعلومات، تفرض بشكل لازم، ان يتم حماية الأنظمة الإلكترونية بما تحتويه من بيانات هامة، والأخذ بغير ذلك يجعل الوصول الى تلك الأنظمة سهلاً. ويشار هنا الى أن الفقه الفرنسي قد تناول المادة ١/٣٢٣ من قانون العقوبات الفرنسي، والتي لم تنص على شرط تمتع النظام بالحماية الإلكترونية كشرط لتجريم الدخول غير المشروع إليها-كما هو الحال في النص القانوني القطري- ولكن انتهى هذا الرأي الى أن التفسير القانوني الصحيح للمادة ٣٢٣-١ من قانون العقوبات الفرنسي، هو أنه ليتم تجريم الدخول غير المشروع يجب أن يتمتع النظام بنظم الحماية الإلكترونية[1240].

أما الرأي الثاني من الفقه الفرنسي، فقد ذهب الى القول، أنه يجب أن تشمل الحماية القانونية كافة الأنظمة الإلكترونية، المحمية منها وغير المحمية، واسس أنصار هذا الاتجاه رأيهم قياساً على جرائم السرقة، حيث تتمتع المنقولات بالحماية القانونية رغم عدم توافر الحماية الفعلية لها من قبل مالكها، وذهب أنصار هذا

الرأي الى استبعاد شرط النظم الأمنية أو نظم الحماية الإلكترونية كشرط لتجريم الدخول غير المشروع، ويؤكد رأيهم -وفق وجهة نظرهم- أن هذا الشرط قد تم ادراجه اثناء مناقشة القانون الخاص بالجرائم الالكترونية الفرنسي لعام ١٩٨٨ ولكن تم استبعاده، والقول بغير ذلك يؤدي الى عدم حماية شريحة كبيرة من النظم الإلكترونية وبالتالي يضيق من نطاق تطبيق القانون[1241].

ونرى من جانبنا، أن الرأي الأول هو الأرجح للتأييد، مع ملاحظاتنا وتحفظنا على الأفكار والأسانيد التي استندت اليها كلتا الآراء الفقهية السابقة، وذلك على النحو الآتي:

1 -اشتراط نظم الحماية الإلكترونية بأنواعها المختلفة، ودرجاتها المتفاوتة، من شأنه دفع أصحاب البرامج والشبكات الإلكترونية الى استخدام نظم الحماية الإلكترونية، وابتعادهم عن الإهمال في حماية اجهزتهم الإلكترونية أو شبكاتهم المعلوماتية.

---

measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f)processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."

1240د. نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية، الطبعة الأولى، منشورات الحلبي الحقوقية، جمهورية مصر العربية، ص٣٥٣.

1241د. نائلة قورة، المرجع السابق، ص٣٥٤.

2 - اشتراط نظم الحماية الإلكترونية كشرط لتجريم الدخول غير المشروع من شأنه -وبطبيعة الحال- أن يؤدي الى خفض اعداد جرائم الدخول غير المشروع لصعوبة ارتكابها، وقد يقف الأمر عند حد الشروع ارتكاب الجريمة، وهو اقل ضرراً بالتأكيد من الدخول الفعلي، وسنتناول مبدأي الشروع والأعمال التحضيرية في معرض لاحق في هذا البحث.

3 - رغم تأييدنا للشرط السابق، الا اننا نرى أنه يجب تجريم الدخول غير المشروع الى النظم الإلكترونية غير المحمية بنظم الحماية الإلكترونية، وذلك لتفادي الانتقادات السابق بيانها، والتي وجهت للرأي الأول، فضلاً عن عدم هدر الحماية القانونية للأشخاص. ونرى اعتبار الدخول غير المشروع للأنظمة الإلكترونية المحمية، ظرفاً مشدداً للجريمة، لما ترتب عليه من اعتداء فاق قوة المقاومة التي قام بها الجهاز وأنظمة الحماية الخاصة به، فضلاً عن تفادي الانتقادات التي وجهت للرأي الاخر.

ويجدر علينا أن نشير هنا أن رأينا هذا نراه في مجال التطبيق في قانون جرائم الكمبيوتر البرتغالي[1242].

4 - نرى أن الآراء الفقهية السابقة، قد أسست رأيها قياساً على الجرائم التقليدية، كالسرقة أو انتهاك حرمة المساكن، ونرى في ذلك عدم مراعاة للطبيعة الخاصة للجريمة الإلكترونية، والتي تأبى مثل تلك القياسات، وكان من الأجدر أن تؤسس تلك الآراء على أسس أقرب وذات طبيعة متصلة بالجريمة الإلكترونية، والتي سبق وأن بيّنا تمتعها بطبيعتها الخاصة بها.

الفرع الأول: موقف التشريعات المقارنة:

اختلفت التشريعات، كما اختلف الفقهاء، حول مسألة اشتراط وضع نظم الحماية الإلكترونية كشرط للحماية القانونية عن الدخول غير المشروع، فذهب بعض تلك التشريعات الى استبعاد هذا الشرط، ومنها المشرع الفرنسي وذلك في قانون العقوبات الفرنسي في المادة ١/٣٢٣ والمشرع الأسترالي، وذلك وفقاً للمادة ٧٦/فقرة ٢ و٤ من قانون العقوبات. وعلى خلاف من ذلك، هناك تشريعات أخرى تطلبت شرط توفير نظم الحماية الإلكترونية لتجريم أفعال الدخول غير المشروع كالمشرع الألماني وذلك في المادة ٢٠٢ من قانون العقوبات والمشرع اليوناني وذلك في المادة ٣٧٠ من قانون العقوبات[1243].

وعلى صعيد العالم العربي، فقد انفرد المشرع الكويتي بوضعه لشرط وجود أنظمة الحماية الإلكترونية كشرط لتجريم الدخول غير المشروع[1244]، وذلك في المادة ١ من قانون مكافحة جرائم تقنية المعلومات لسنة ٢٠١٥، وذلك على النحو الآتي:

"الدخول غير المشروع: النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح".

1242 انظر: المادة ٦ من قانون جرائم الكمبيوتر البرتغالي رقم ١٠٩ لسنة ٢٠٠٩، الذي نص على أن عقوبة جريمة الدخول غير المصرح به هي الحبس حتى سنة وتشدد الى الحبس لمدة ٣ سنوات إذا تم الدخول من خلال خرق النظم الأمنية.

1243 د. نائلة قوره، المرجع السابق، ص٣٥٦

1244 د. عبد الإله النوايسة، جرائم تكنولوجيا المعلومات، الطبعة الأولى، دار وائل للنشر والتوزيع، الأردن، عمان، ٢٠١٧، ص٢١٢.

أما على الصعيد الدولي، فهناك العديد من الاتفاقيات الدولية التي تناولت هذه المسألة، ومن ذلك، اتفاقية الجريمة الإلكترونية الخاصة بالمجلس الأوروبي، حيث نصت في موادها على ان أطراف الاتفاقية يمكنهم اشتراط أن تكون جريمة الدخول غير المشروع قد تمت من خلال تجاوز الأنظمة الأمنية "Security Measures" وذلك في المادة الثانية 1245.

الفرع الثاني: موقف المشرع القطري:

وبالنسبة لاشتراط أنظمة الحماية الإلكترونية كشرط لتجريم الدخول غير المشروع، فقد خلت المادة ٣ من قانون مكافحة الجرائم الإلكترونية من اية إشارة الى مثل هذا الاشتراط للتمتع بالحماية القانونية، ولم يذكر المشرع القطري في تعريفاته في المادة الأولى منه على هذا الشرط، كما هو الحال مع المشرع الكويتي.

ومع عدم وجود احكام محكمة التمييز في هذا الخصوص فلا يمكن الاخذ بمثل هذا الشرط ويجب التقيد بالنص، فالقاعدة المعروفة هي أن العام يبقى على عمومه مالم يرد نص يخصصه، وأن الخاص يقيد العام، وبالتالي مع عدم وجود أي حكم خاص بهذا الشأن، لا محل للحديث عن شرط وجود الأنظمة الأمنية الإلكترونية.

ويلاحظ أن أغلب التشريعات لا تلزم بمثل هذا الشرط لقيام جريمة الدخول غير المشروع، وهو الاتجاه التشريعي الذي يحظى تأييد الفقه1246 وسبق وقد أن بيّنا رأينا في هذه المسألة.

المطلب الثاني: الحماية عن الاعمال التحضيرية ومبدأ الشروع:

وفقاً لطبيعة الجريمة الإلكترونية الخاصة، فإن احكام الاعمال التحضيرية واحكام الشروع تأثرت بتلك الطبيعة الخاصة، اخذاً بعين الاعتبار أن الجرائم الإلكترونية، وتحديداً جريمة الدخول غير المشروع، تتطلب مجهوداً ذهنياً، فكيف يمكن تحديد فعل الجاني، إن كان يشكل شروعاً أم عملاً تحضيرياً؟ وهل يمكن العقاب على الشروع في الجنح المنصوص عليها في قانون مكافحة الجرائم الإلكترونية؟ ماذا عن الاعمال التحضيرية والعقاب عنها؟ نجيب على هذه التساؤلات في هذا المطلب وذلك على النحو الآتي:

الفرع الأول: الشروع في ارتكاب الجرائم الالكترونية:

اختلفت التشريعات فيما بينها حول احكام الشروع، وذلك نتيجة طبيعية ومنطقية للاختلافات التي بين تلك التشريعات في احكام جريمة الدخول غير المشروع على نحو ما سبق بيانه، من تلك التشريعات التي اعتبرت جريمة الدخول، جريمة مادية، وغيرها الذي اعتبرها جريمة شكلية، أي هناك من اشترط ان تترتب عليها نتيجة وهناك من اكتفى بالسلوك ذاته للقول بوجود الجريمة، وتعد النتيجة ظرفاً مشدداً.

1245 Council of Europe, Convention on Cybercrime, European Treaty Series – No.185, Article 2 – Illegals Access :Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

1246د. عبد الإله النوايسة، المرجع السابق، ص ٢١٢

ومن بين القوانين العربية، فإن القانون الكويتي والأردني مثلاً لم تتناول قوانينهم الخاصة بالجرائم الإلكترونية اية احكام بشأن الشروع، وبالتالي يحال الأمر الى القواعد العامة الواردة في قوانين الجزاءات او العقوبات[1247]. اما المشرع القطري، وكذلك المشرع السعودي والعماني، فقد نصوا على ان العقاب على الشروع يكون بما لا يجاوز نصف الحد الأقصى للعقوبة المنصوص عليها سواء في الجناية ام الجنحة[1248].

ولما كان الشروع هو جريمة ناقصة ولكن تخلفت بعض عناصرها، وهو يعرف قانوناً بأنه البدء في تنفيذ فعلاً ما بقصد ارتكاب جريمة ولكن خاب أثرها لسبب لا دخل لإرادة الجاني فيه[1249]، والإشكالية هنا، هي كيف يتم تحديد ما إذا كان الفعل يعد شروعاً أم مجرد عملاً تحضيرياً، وهل هناك عقاب على الأعمال التحضيرية؟

الفرع الثاني: الاعمال التحضيرية في مجال الجريمة الإلكترونية:

القاعدة العامة هي أن لا عقاب إلا على الجريمة التامة أو تلك التي تقف عند حد الشروع، أي أن الحد الأدنى للعقاب هو البدء في تنفيذ السلوك الإجرامي المكون للجريمة، ولا عقاب على الأعمال التحضيرية الا بنص خاص. إلا أن بعض التشريعات الأجنبية ذهبت الى تجريم الأعمال التحضيرية، وذلك بنصوص خاصة، ويذهب رأي من الفقه في أن المشرع الفرنسي اتخذ هذا النهج، حيث نص في المادة ٤/٣٢٣ على العقاب على الأعمال التحضيرية في حالة مساهمة أكثر من شخص في ارتكاب جرائم الاعتداء على النظم الإلكترونية[1250].

اما العمل التحضيري في مجال الجريمة الإلكترونية فهو قد يتمثل في الحصول على الرمز السري او المسح الرقمي للشبكة لبيان الثغرات للنظام المعلوماتي، فهو عملاً مادياً يسبق البدء في الركن المادي للجريمة، وهو - الركن المادي -في جريمة الدخول غير المشروع المتمثل في (فعل الدخول).

ولا نجد مثيلاً لهذا النص في قانون مكافحة الجرائم الإلكترونية القطري، والذي اكتفى بتجريم السلوك الى حد الشروع، ونعود الى القواعد العامة التي تأبى العقاب على العمل التحضيري، أما عن ما ذهب اليه المشرع الفرنسي، فنرى أنه لا يعد عقاباً على عملاً تحضيرياً بل هو عقاباً على اتفاقاً جنائياً، ونص المشرع القطري في قانون العقوبات على العقاب على الاتفاق الجنائي في المادة [1251]٤٦، حيث نص على" اذا اتفق شخصان أو اكثر على ارتكاب جناية أو جنحة، واتخذوا العدة لذلك على وجه لا يتوقع معه أن يعدلوا عما يتفقوا عليه، يعد كل منهم مسئولاً عن اتفاق جنائي، ولو لم تقع الجريمة موضوع الاتفاق....."

ويشترط لإعمال هذا النص أن يكون الأفراد قد اتفقوا على وجه لا عودة في اتفاقهم، أي أنهم بدأوا في تحضير اعمالاً مادية بموجب اتفاقهم، وفي مجال الجريمة الإلكترونية ومثال ذلك: في حال ما إذا اتفق شخصين أو أكثر على اختراق موقع إلكتروني وقد

1247 د. عبد الإله النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية: دراسة مقارنة، المجلة القانونية والقضائية: وزارة العدل، قطر،١٦ . ٢، ص٧٣.

1248انظر المادة ٥٠ من قانون مكافحة الجرائم الإلكترونية القطري، والمادة ١٠ من قانون مكافحة الجرائم المعلوماتية السعودي، والمادة ٣٠ من قانون مكافحة جرائم تقنية المعلومات العماني.

1249د. محمود نجيب حسني، شرح قانون العقوبات القسم العام: النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، الطبعة الثامنة، دار المطبوعات الجامعية، الإسكندرية، ١٧ . ٢، ص٣٨٧.

1250د. علي القهوجي الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، ١٠ . ٢، ص١١٧.

1251قانون العقوبات القطري الصادر بالقانون رقم 11 لسنة 2004.

قاموا بإنشاء حسابات ببيانات خاطئة، وذلك لغرض الاطلاع على سمات الشبكة الإلكترونية بشكل مشروع- وهو ما يسمى بالاستطلاع Reconnaissance -هنا نكون أمام اتفاق جنائي معاقب عليه وفقاً لنص المادة ٤٦ من قانون العقوبات القطري، أما عند قيامهم بتحميل الفيروسات أو برامج التجسس المختلفة1252باستخدام ذلك الحساب، فهنا يعد فعلهم سابقاً للركن المادي أو مؤدياً له، وبالتالي يعد شروعاً في الجريمة.

وعليه فإن خلاصة القول هي أن المشرع القطري لا يعاقب على العمل التحضيري، وإنما يعاقب على الاتفاق الجنائي بين شخصين فأكثر، إذا اقترن بعمل مادي، اما خلاف ذلك، فيقف العقاب عند حد الشروع.

كما نخلص الى أن الحد الفاصل بين العمل التحضيري والشروع، هو البدء في تنفيذ فعلاً يعد عنصراً من عناصر الركن المادي للجريمة الإلكترونية أو الذي يسبق الركن المادي مباشرة وسيؤدي لها فور تمامه، وهو كما أسلفنا البيان، يعد في جريمة الدخول غير المشروع أو التجاوز، فعل الدخول أو التجاوز للحدود المصرح بها، اما غير ذلك فهو يدخل في نطاق الاعمال التحضيرية التي لا ترقى لمرتبة الشروع، ولا عقاب عليها، ونهاية نشير هنا الى الأهمية التي قد برزت في فهم جوانب الجريمة الالكترونية وخصوصية القواعد العامة المتعلقة بالشروع والاعمال التحضيرية والاتفاق الجنائي عند اعمالها عليها، الامر الذي تبرز معه بشكل كبير أهمية وجود أعضاء متخصصين وملمين بجوانب واحكام الجريمة الالكترونية وعلى وجه الخصوص لدى النيابة العامة والمحاكم الجنائية.

الخاتمة

العالم التقني سريع التطور، ومعه مفهوم الجريمة الإلكترونية، لذي لن يبقى جامداً، بل سيتجدد ويتطور، وهنا يبرز دور رجال القانون والقوانين ذاتها، وسعيهم وراء مواكبة تلك التطورات. وقد استعرضنا في هذا البحث مدى اشتراط نظم الحماية الإلكترونية لتجريم فعل الدخول، وبعدها تناولنا مبدأي الشروع والاعمال التحضيرية، وفي نهاية هذا البحث توصلنا للنتائج والتوصيات الآتية:

أولاً: النتائج:

1. تُرك أمر تفسير قصد المشرع في جريمة الدخول غير المشروع للقضاء والفقه، حيث لم يورد المشرع تعريفاً لفعل الدخول غير المشروع.
2. جريمة الدخول غير المشروع هي جريمة عمدية، تقوم بالسلوك الإجرامي المجرد وهو يتمثل في فعل الدخول للنظام الإلكتروني، أو بقي فيه بعد علمه بدخوله دون وجه حق.
3. القانون القطري لم ينص على اشتراط خضوع الأنظمة الالكترونية للحماية كشرط للحصول على الحماية القانونية، وكشرط لتجريم فعل الدخول غير المشروع.
4. لا يوجد في قانون مكافحة الجرائم الإلكترونية القطري مايجرم الأعمل التحضيرية، واكتفى بتجريم السلوك الى حد الشروع، وبذلك نعود الى القواعد العامة التي تأبى العقاب على العمل التحضيري.

1252 تتنوع برامج التجسس والمراقبة المستخدمة من قبل الجناة، منها المشروعة والتي يتم إساءة استخدامها كبرنامج Nesus وغيرها من البرامج المخصصة للتجسس كبرنامج Pegasus، محاضرة بمعهد الدراسات الجنائية، النيابة العامة، بتاريخ ٢٠١٩/٣/٢٧م.

5. الحد الفاصل بين العمل التحضيري والشروع، هو البدء في تنفيذ فعلاً يعد عنصراً من عناصر الركن المادي للجريمة الإلكترونية أو الذي يسبق الركن المادي مباشرة وسيؤدي لها فور تمامه

ثانياً: التوصيات:

1 -على غرار النيابة العامة التي أنشأت نيابة الجرائم الإلكترونية، نوصي بضرورة انشاء دائرة بالمحاكم ذات قضاء متخصص في مجال الجريمة الإلكترونية نظراً للطبيعة الخاصة لهذه الجرائم وصعوبتها، التي تحتاج قضاة ورجال نيابة متخصصين بدورها.

2 -ننوه بضرورة تعديل الفصل الأول من الباب الثاني بقانون مكافحة الجرائم الإلكترونية لوضع ضوابط وإرشادات يستهدي بها القضاء لتفسير المقصود "بالدخول غير المشروع" بشكل واضح.

3 - نوصي المشرع بأن يتدخل بتعديل تشريعي لنص المواد الخاصة بالدخول غير المشروع، وذلك لإضافة "اختراق نظام الحماية الإلكتروني" كظرف من الظروف المشددة، نظراً للخطورة الإجرامية لدى الجاني، ومهارته التي مكنته لتجاوز الانظمة الأمنية الإلكترونية.

4 -المراجع والمصادر

أولاً: المراجع الورقية:

- د. راشد محمد المري، الجرائم الالكترونية: في ظل الفكر الجنائي المعاصر: دراسة مقارنة، دار النهضة العربية، جمهورية مصر العربية، م٢٠١٨

- د. عبد الإله النوايسة: جرائم تكنولوجيا المعلومات، الطبعة الأولى، دار وائل للنشر والتوزيع، الأردن، عمان، ٢٠١٧م

- د. عبد الإله النوايسة، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية: دراسة مقارنة، المجلة القانونية والقضائية: وزارة العدل، قطر،٢٠١٦، ص٧٣

- د. علي القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، ٢٠١٠

- د. محمود نجيب حسني، شرح قانون العقوبات القسم العام: النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي، الطبعة الثامنة، دار المطبوعات الجامعية، الإسكندرية، ٢٠١٧م

- د. نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية، الطبعة الأولى، منشورات الحلبي الحقوقية، جمهورية مصر العربية .

ثانياً: المواقع الإلكترونية:

• البوابة القانونية القطرية (موقع الميزان)

http://www.almeezan.qa

➢ دار المنظومة

/http://0-search.mandumah.com.mylibrary.qu.edu.qa

- المجلس الاعلى للقضاء

/http://www.sjc.gov.qa/Pages

- المنهل

http://0-platform.almanhal.com.mylibrary.qu.edu.qa

- شبكة قوانين الشرق

http://0-www.eastlaws.com.mylibrary.qu.edu.qa/

- مكتبة جامعة قطر:

http://library.qu.edu.qa/ar

ثالثاً: الاتفاقيات الدولية:

- Article 2 of Council of Europe, Convention on Cybercrime, European Treaty Series – No.185
- EUROPEAN GENEAL DATA PROTECTION REGULATION

رابعاً: محاضرات وندوات

- احمد يوسف الكواري، الجريمة الالكترونية في التشريع القطري، محاضرة في جامعة قطر ضمن مقرر الجرائم الالكترونية، الدكتور بشير سعد زغلول، ٢٠١٩م

- د. بشير سعد زغلول، محاضرة ضمن مقرر قانون مكافحة الجرائم الإلكترونية لبرنامج الماجستير بالقانون العام، جامعة قطر بتاريخ 2019/1/23م

- عدنان فكري، إدارة الأمن المعلوماتي بوزارة الداخلية، محاضرة في النيابة العامة القطرية، ضمن دورة معهد الدراسات الجنائية، ٢٠١٩م

- د. سامي حمدان الرواشدة، محاضرة بعنوان: Illegal Access to Information Systems in the Qatari Criminal Law: A Comparative Stud جامعة قطر

- وسيم حرب، كلمة خلال أعمال الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر19-20 نيسان/يونيو، 2007 المملكة المغربية

خامساً: القوانين:

- المادة ٣ من قانون مكافحة الجرائم الإلكترونية القطري رقم ١٤ لسنة ٢٠١٤
- المادة ١١ من قانون حماية خصوصية البيانات الشخصية القطري رقم ١٣ لسنة ٢٠١٦

- المادة ٦ من قانون جرائم الكمبيوتر البرتغالي رقم ١٠٩ لسنة ٢٠٠٩
- المادة ١٠ من قانون مكافحة الجرائم المعلوماتية السعودي
- المادة ٣٠ من قانون مكافحة جرائم تقنية المعلومات العماني

سادساً: أحكام المحاكم:

- محكمة التمييز القطرية-المواد الجنائية، جلسة 4 ديسمبر 2017، الطعن رقم 203 لسنة 2017