International Journal of Law Research and Studies (IJLRS)
Vol. (4), No. (2)
IJLRS
February 2025
المجلة الدولية للبحوث والدراسات القانونية
الإصدار (4)، العدد (2)

أركان الجريمة الإلكترونية

شهاب بن عبدالرحمن بن حامد المسعود
قسم القانون العام، كلية الحقوق، جامعة الملك عبدالعزيز، المملكة العربية السعودية
Sheehab84@gmail.com

المستخلص

تناولت هذه الدراسة جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي، وقُسِّمت هذه الدراسة إلى خمسة فصول؛ إذ سُلِّط الضوء على ماهية الجريمة، وأهمية تجريمها، وتُطُرِّق إلى أركان الجريمة، والعقوبات المترتبة على مرتكبيها. لقد تم اتباع المنهج الوصفي في هذه الدراسة لشرح مفهوم جريمة الدخول غير المشروع، وخطرها على المجتمع، واتباع المنهج التحليلي لاقتراح الأنظمة، والتشريعات الرادعة والزاجرة.

تهدف هذه الرسالة إلى بيان مفهوم مدى خطورة الجريمة، وأثرها في المجتمع، وضرورة التعاون الدوليّ؛ لمكافحة الجرائم المعلوماتية، وقد خرجت هذه الدراسة بعدة نتائج، وتوصيات، من أهمّها: إذا كان المخترقون من داخل المملكة طُبِّق عليهم نظام مكافحة الجرائم المعلوماتية السعودي، أمّا إذا كان المخترقون من خارج المملكة العربية السعودية؛ فإنّني أوصي بعمل نظام دولي صادر من الأمم المتحدة لتبادل المخترقين بين الدول؛ لمحاكمتهم، أو إنشاء محكمة دولية خاصة بالجرائم المعلوماتية، وسيكون من نتائجها أنّ جميع المخترقين سينالون جزاءهم أينما كانوا.

الكلمات المفتاحية: شبكة الإنترنت، الاختراق، النصب والاحتيال، وسائل التواصل الاجتماعي، الجريمة المعلوماتية، المحكمة الدولية، السعودي.

Elements of Electronic Crime

Shehab bin Abdulrahman bin Hamed Al-Masoud
Department of Public Law, Faculty of Law, King Abdulaziz University, Kingdom of Saudi Arabia
Sheehab84@gmail.com

Abstract

This study examines the crime of unauthorized access to social media platforms. The study is divided into five chapters, shedding light on the nature of this crime, the importance of criminalizing it, and delving into the elements of the crime and the corresponding penalties for perpetrators. A descriptive approach was adopted in this study to explain the concept of unauthorized access and its danger to society,

while an analytical approach was used to propose systems and deterrent legislation>

This thesis aims to clarify the extent of the crime's danger and its impact on society, as well as the necessity of international cooperation to combat cybercrimes. This study has yielded several results and recommendations, most notably: if the perpetrators are from within the Kingdom, the Saudi Cybercrime Law will be applied. However, if the perpetrators are from outside the Kingdom of Saudi Arabia, I recommend the establishment of an international system issued by the United Nations for the extradition of perpetrators to be trialed, or the establishment of an international court specifically for cybercrimes. As a result, all perpetrators will face justice wherever they may be.

Keywords: Internet Network, Penetration, Fraud and Cheat, Social Media, Cyber Crime, International Court, Saudi.

مقدمة

إنّ تمتّع الإنسان بحقه وحريته أمرٌ، أقرّتْه الشريعة الإسلامية، وجميع الأنظمة الوضعية؛ لأنّها تعدّ دعامة أساسيّة، ومهمة من دعامات النظام الجنائي لأنّ توفير الحماية والحرية للأفراد واجب على الدولة، ومن دون تلك الحماية؛ تتدهور الدولة، ويتضرّر الأفراد ويتفكك المجتمع، وتحدث الحروب الأهلية.

مشكلة البحث

تكمن الإشكالية في جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي في أنها خطيرة للغاية، ويجب التصدي لها بشتّى الطرائق، سواء من الحكومة، أو الأفراد، كأن يرسل المخترق رسائل نصية، فيها روابط احتيالية، تؤدي إلى سرقة المعلومات الخاصة، أو الدخول على الحسابات البنكية، أو الدخول على نظام (أبشر)، أو نظام (ناجز) وغيرها من التطبيقات الخدمية السعودية، وهنا تظهر إشكالية البحث في الأسئلة التالية:

- ما المقصود بجريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟
- ما أركان جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟
- ما العقوبات المترتبة على الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟

أهداف البحث

يهدف البحث إلى بيان مفهوم مدى خطورة جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي، وأثرها على المجتمع، ولهذا؛ كان الهدف من البحث هو توعية المجتمع وحمايته من الاختراق، وما ينتج عنه من آثار سلبية.

أهمية البحث

تكمن أهمية البحث في حماية الأفراد، والمجتمع من الاختراق المؤدّي للابتزاز، وسرقة المعلومات، والأموال ويساعد البحث على التوعية من الاختراق، وحماية المجتمع منها؛ لأنّها تُشكّل خطرًا على المجتمع، والعالم أجمع، ومن خلال البحث؛ سوف نتطرق إلى مدى خطورة الاختراق، وطرائق الحماية منه، وأساليبه.

منهجية البحث

تم استخدم المنهج الوصفي؛ لشرح مفهوم جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي، وخطرها على المجتمع، واستخدام المنهج التحليليّ؛ لاقتراح الأنظمة، والتشريعات الرادعة للمخترقين.

الدراسات السابقة

الدراسة الأولى: إبراهيم القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية.

مشكلة الدراسة: تكمن مشكلة البحث المنشور في عام 2018م في معرفة مدى الحماية الجنائية التي يوفّرها المرسوم الاتحادي بقانون رقم (5) لسنة 2012م في شأن مكافحة جرائم تقنية المعلومات للنظام المعلوماتي الإماراتي، وحماية محتويات النظام المعلوماتي من البيانات، والمعلومات، ولا سيما المعلومات، والبيانات الحكومية، والمعلومات، والبيانات السّرّيّة الخاصة بالمنشآت المالية، والتجارية، والاقتصادية، وذلك من خلال تقييم النصوص القانونية الواردة في شأن هذه الجرائم، والعقوبات، والتدابير المقررة لهذه الجرائم، وما تشتمل عليه من عنصر الردع، وتشديد العقوبة، والتدرج في تشديدها.

الدراسة الثانية: مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، مسابقة الأمير نايف بن عبد العزيز للبحوث الأمنية، الجريمة الإلكترونية في المجتمع الخليجي، وطريقة مواجهتها، 2015م.

مشكلة الدراسة: تكمن مشكلة الدراسة في تفاقُم الجريمة الإلكترونية، وتعدُّد أنواعها، وازدياد حجم خسائرها، وأضرارها؛ إذ أصبحت مهددًا حقيقيًا لأمن المعلومات في المجالات العامة كافة، والحيوية في

القطاع العامّ، والخاصّ، والأفراد، بل مصدر خطورة على الأمن القوميّ، وعلى السّلْم، والأمن الدوليَّيْن؛ بسبب استخدام الإنترنت في النشاطات الإرهابية.

الدراسة الثالثة: أ. جميلة سعيد مصباح شوران، جريمة الدخول غير المشروع وفقًا لقانون الجرائم الإلكترونية الليبي رقم 5 سنة 2022م.

مشكلة الدراسة: إنّ أبرز ما يمكن أن يُثار في هذه الدراسة من تساؤلات يتمثّل في بيان ما يلي:

أولًا: الغاية من تجريم الفعل في كل صوره ومدى عدّ هذه الجريمة من الجرائم السلوك، أو الضرر.

ثانيًا: الأنظمة التي شملها النصّ بالحماية، وهل هي خاصة مملوكة للأفراد، أو عامة مملوكة للدولة؟

ثالثًا: مدى كفاية النّصّ القانونيّ المجرّم للدخول غير المشروع في تغطية كل ما يتصل بهذه الجريمة.

المبحث الأول: محلّ الجريمة

إنّ جريمة الدخول غير المشروع إلى النظام المعلوماتي جريمة ذات طبيعة خاصة، حدّد لها المشرّع شرطًا مفترضًا، أو محلًّا لا بد من توافره، وهو النظام المعلوماتيّ، سواء أكان موقعًا، أو شبكة معلوماتية، أو أيّ وسيلة من تقنية المعلومات.

الشرط المفترض في هذه الجريمة ليس من الأركان العامة، ولكنّه ضروري لقيام الجريمة، وهو بمنزلة الركن الخاصّ، ولا بدّ من توافره؛ حتى يتحقّق قيام الجريمة[1]. ويقصد بالشرط المفترض، أو محل الجريمة: الحقّ أو المصلحة التي يحميها القانون التي تكون هدفًا للجريمة.

وقد عرّف المشرّع السعوديّ ركن المحلّ أنه (حاسب آليّ، أو موقع إلكترونيّ، أو نظام معلوماتيّ، أو شبكة حاسبات آلية)[2].

عرّف الفقهُ المصريُّ الشرطَ المفترضَ أنه (العنصر الذي يفترض قيامه وقت مباشرة الفاعل لنشاطه).

أما الفقهُ الإيطاليُّ؛ فقد عرّف الشرط المفترض أنه: (عنصر، أو ظرف إيجابيّ، أو سلبيّ، يسبق بالضرورة، وجود الجريمة، أو الواقعة، أو أنّه عنصر، أو مركز يسبق في وجوده قيام الجريمة -منطقيًّا وقانونيًّا- ويُعدّ بمنزلة الوسط الضروري لتوافر السلوك غير المشروع)[3].

[1] إبراهيم بن محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، 2018م، ص9.
[2] نظام مكافحة جرائم المعلوماتية السعودي، 1428هـ.
[3] إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، 2018م، ص10.

المبحث الثاني: الركن المادّيّ

لا يعدّ السلوك الإنسانيّ سلوكًا غير مشروعٍ، أو جريمة بالمعنى القانونيّ، إلا إذا توافرت فيها العناصر اللازمة؛ لتحقق الجريمة، وهي أركان الجريمة.

ويتكوّن الركن المادّيّ من ثلاثة عناصر، وهي: النشاط، والعلاقة السببية، والنتيجة.

الركن المادّيّ للجريمة هو مظهرها الخارجي المتمثّل بنشاط الجاني الإيجابيّ، أو امتناعه عن النشاط أي: (الموقف السلبيّ)، وقيام علاقة سببية بين النشاط الإجراميّ، والنتيجة[4].

وقد عرّف المشرّع السعودي الدخول غير المشروع في الفقرة السابعة من المادة الأولى من نظام مكافحة الجرائم المعلوماتية لسنة 1428هـ أنه (دخول شخص بطريقة متعمده إلى حاسب آليّ، أو موقع إلكترونيّ، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها[5].

ويقوم الركن المادي لهذه الجريمة على تحقّق فعليّ، وهو السلوك، أي: دخول الجاني، أو بقاؤه غير المشروع داخل النظام الإلكتروني، وليس من الضروري أن يكون الدخول إلى النظام الإلكتروني كاملًا؛ حتى يقوم الركن المادي، بل يكفي أن يكون الدخول جزئيًّا[6].

ولعلّ أهم مثال على ذلك: هو النشاط الإيجابي في جريمة إتلاف المستندات الإلكترونية؛ فالفعل، أو النشاط الإيجابيّ من الجاني المتمثّل في بثّ فيروسات: كحصان طروادة، أو من خلال برامج ضغط، تأتي عن طريق قيامه ببثّ هذه الفيروسات عن طريق جهاز الحاسب الآلي من خلال شبكة الإنترنت، وهو ما يمثّل أهمية النشاط التقني بكونه فعلًا إيجابيًّا في الجرائم الإلكترونية.

والنشاط، أو السلوك المادي في جرائم الإنترنت يتطلب وجود بيئة رقمية، واتصال بالإنترنت، ويتطلب – أيضًا- معرفة بداية هذا النشاط، والشروع فيه، ونتيجته، فمثلًا: يجهِّز مرتكب الجريمة الحاسب الآليّ؛ لكي يحقّق له حدوث الجريمة. فالجرائم الإلكترونية ليست مثل أيّ جريمة، تستلزم وجود أعمال تحضيرية؛ إذ إنّه يصعب الفصل بين العمل التحضيريّ، والبدء في التنفيذ حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية إلا أنّ الأمر في مجال تكنولوجيا المعلومات يختلف بعض الشيء، فشراء برامج اختراق، ومعدّات فكّ الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال، أو صور وفيديوهات إباحية للنساء، أو حتى بعض الفيروسات التي لم تُطلق على الشبكة الإلكترونية، فكل هذه الأفعال تمثّل جريمة بحد ذاتها[7].

---

[4] المرجع السابق رقم 1.
[5] نظام مكافحة جرائم المعلوماتية السعودي، 1428هـ.
[6] أ. نسمة بطيحي، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، 2019م، ص77-78.
[7] اللجنة العلمية معهد الكويت للدراسات القضائية والقانونية، 2018-2019م، ص15-16.

صور السلوك الإجراميّ لهذه الجريمة:

أولًا: الدخول إلى النظام المعلوماتيّ دون تصريح:

وللدخول معنيان، أحدهما: مادّيّ: كالدخول مثلا إلى محل أو غرفة، والآخر معنويّ، وهو المقصود هنا، ويعني ذلك النشاط الذهني الذي يقوم به الجاني؛ لغرض الوصول إلى النظام ويشَبه الفقه الدخول إلى النظام المعلوماتي بالدخول إلى ذاكرة الإنسان، ويوجد من يعرّف الدخول على أساس البعد المكانيّ، والزمانيّ له، فمن حيث المكان؛ يُقصَد بالدخول إلى النظام فعل التسلل داخله، ومن حيث الزمان؛ يقصد به تجاوز حدود الترخيص ووقته بالدخول إلى النظام المعلوماتيّ، أي: أنّ أيّ وسيلة تقنية تستعمل وتستخدم لغرض الدخول إلى النظام تتحقق بها الجريمة، فقد يُدخَل –مثلًا- باستخدام الجاني لكلمة السر الحقيقية المملوكة للضحية بعد الحصول عليها بطريقة غير مشروعة، أو باستخدام برامج أو شفرات خاصة، ويستوي أن يتم الدخول إلى النظام المعلوماتي بطريقة مباشرة، أو غير مباشرة، فقد يعمد الجاني إلى الدخول مباشرة إلى جهاز الحاسب الآلي للضحية، ومن الممكن أن يدخل إليه بطريقة غير مباشرة من خلال جهاز آخر متصل مع جهاز الضحية بوساطة شبكة الإنترنت، وقد ذهب القضاء إلى تأييد ذلك؛ فقد جاء في قرار محكمة استئناف باريس الصادر في 5 أبريل 1994م من أن الدخول يشمل جميع أشكال الاختراق غير القانونية لنظام المعالجة الآلية للمعطيات التي يستعملها الجاني على الحاسب الآلي ولو على نظام آخر، يتصل به عن بُعد[8].

ثانيًا: تجاوز حدود التصريح:

تثير حالة وجود التصريح إشكالًا؛ لأنه في هذه الحالة يكون المجرم لديه تصريح، أو إذن سابق بالدخول إلى النظام المعلوماتي في حدود معينة، ولكنه يتجاوز هذه الحدود[9]، وهذا الإذن، أو التصريح قد يكون محدّدًا من حيث المدة، والزمان، أو حتى نطاق المعلومات المسموح له بالاطلاع عليها، فإذا تجاوز المجرم هذا التصريح من حيث المدة، أو الزمان المحدّد له بأن دخل في غير المواعيد المحددة في التصريح، أو تجاوز المدّة المحددة للدخول في التصريح، أو تجاوز نطاق المعلومات المصرح له بها يكون في هذه الحالة مرتكبًا للجريمة[10].

أ- تجاوز حدود الدخول من الزمن: قد يحدث أن يكون الجاني قد تحصل على الموافقة بالدخول، إلا أنّه تجاوز حدود هذا الدخول من حيث الزمان، ويذهب بعضنا إلى أنّ تجاوز حدود الدخول يتحقق عن طريق التجاوز من حيث الموضوع، لا من حيث الزمن.

[8] أ. نسمة بطيحي، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، 2019م، ص78.
[9] داود إدريس وشيبان أنيس، جريمة الدخول إلى النظام المعلوماتي في القانون الجزائري، 2022-2023م، ص41.
[10] إبراهيم بن محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، 2018م، ص29-30.

ونرى أنّه يتحقّق تجاوز حدود الدخول من حيث الزمن: كأن يكون قد سُمِح له بالدخول مرة واحدة فقط، إلّا أنّه أعاد الدخول أكثر من مرة؛ إذ إنّه تمكّن من الدخول، والاطلاع على رسائل، أو معلومات، وصلت في الوقت نفسه إلى النظام، ويتحقّق ذلك –أيضًا- في الحالة التي يسمح بها للشخص بالدخول مدّة معينة، إلّا أنّه يتجاوز هذه المدة بما يخالف الإذن[11].

ب- تجاوز حدود الدخول من حيث الموضوع: قد يسمح صاحب السلطة على النظام لأحد الأشخاص بالدخول إلى جزء معيّن؛ للاطلاع على ما يحتويه من ملفّات دون غيره، إلا أنّه يتجاوز حدود هذا الإذن، ويدخل على ملفات أخرى بالمخالفة لحدود الإذن الممنوح له، ولا شكّ في أنّ الدخول في الحالات السابقة -وإن كان قد تمّ بموافقة صاحب السلطة أو إذنه على النظام- فإنّه يبقى دخولًا غير مشروع؛ لأنه خالف حدود الإذن، أو الموافقة، وتتحقق من خلالها علّة تجريم المشرِّع للدخول غير المشروع للنظام المعلوماتيّ[12].

ثالثًا: البقاء بصورة غير مشروعة في النظام المعلوماتيّ:

تبرز أهمية تجريم البقاء داخل النظام المعلوماتي بصورة غير مشروعة في الفرض الذي لا يدخل فيه الدخول في حدّ ذاته في دائرة التجريم: كأنْ يقع الدخول –مثلًا- بطريق الصدفة، أو الخطأ، ويستغلّ الجاني الفرصة بعد ذلك، ويبقى داخل النظام المعلوماتيّ دون أن يكون له أيّ حق في ذلك، وفي هذا الإطار نصّ الفصل 3-607 في فقرته الثانية (2) من مجموعة القانون الجنائي المغربيّ على أنه (ويعاقب بـ... من بقي في نظام للمعالجة الآلية للمعطيات أو في جزء منه؛ كان قد دخله عن طريق الخطأ وهو غير مخوّل له حقّ دخوله)، أو مثلًا: أن يبقى الجاني داخل النظام المعلوماتي خارج الوقت المسموح به من مالك النظام، أو لغرض غير الغرض المخصص له لذلك، ومن ثَمَّ؛ لا بد من الردع، والعقاب لمثل هذه التجاوزات، وقد قضت محكمة النقض الفرنسية بأن استمرار الجاني في استخدام الرقم السري الذي يسمح له بالدخول إلى قاعدة البيانات مدّة تفوق السنتين، وهذه المدة غير المسموح بها يشكّل جريمة البقاء غير المشروع المعاقب عليها؛ لأنّ هذا الرقم السري قد حُصِل عليه، ورُخِّص باستخدامه خلال مدة التجربة فقط، وهذه الأخيرة التي تجاوزها الجاني[13].

[11] ما شاءالله عثمان الزوي، المسؤولية الجنائية للدخول أو البقاء غير المشروع في النظام المعلوماتي دراسة في القانون الليبي المقارن، 2023م، ص145.

[12] ماشاءالله عثمان الزوي، المسؤولية الجنائية للدخول أو البقاء غير المشروع في النظام المعلوماتي دراسة في القانون الليبي المقارن، 2023م، ص145.

[13] أ. نسمة بطيحي، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، 2019م، ص79.

المبحث الثالث: الركن المعنويّ

من المتّفق عليه أنّ جريمة الدخول غير المشروع هي جريمة عمديّة، وهذا ما أكّدتْه العديد من التشريعات[14] مثل المشرِّع الأردنيّ، والمشرّع العمانيّ، والمشرّع القطريّ الذين استخدموا عبارة "كلّ من دخل عمدًا"[15]، أي: أنّه يتعيّن أن تتجه إرادة الجاني إلى الدخول إلى النظام مع علمه أنّ ذلك يحظره القانون، ولا يمكن لدخوله إلى النظام أن يكون دخولًا عرضيًّا، وقد أكّدت محكمة استئناف باريس ذلك؛ حينما نفت مسؤولية الجاني على فعل الدخول إلى النظام الذي تم عن طريق الخطأ[16] وللركن المعنويّ صورتان، هما القصد الجنائيّ، والخطأ غير العمدي، فيعرّف القصد الجنائي على أنّه علم الجاني بالعناصر المكونة للجريمة، واتجاه إرادته إلى إحداث هذه العناصر، أو إلى قبولها[17].

ويتكون الركن المعنويّ من عنصرين، هما: العلم، والإرادة.

العلم: هو العلم بالنشاط، والنتيجة اتجاه إرادة الجاني إلى تحقيق النشاط، والنتيجة.

الإرادة: هي إرادة الجاني إلى ارتكاب فعل، أو الامتناع عن فعل متى كان هذا الفعل مجرمًا قانونًا[18].

ويقصد بالركن المعنويّ: هو نيّة الجاني عند ارتكابه للجريمة.

قد يكون القصد الجنائيّ عامّا، أو خاصًا، وعليه؛ فالقصد الجنائيّ العام يتوافر في جميع الجرائم الإلكترونية دون استثناء، ولكن توجد بعض الجرائم الإلكترونية يتوافر بها القصد الجنائيّ الخاصّ، مثل: جريمة تشويه السمعة عبر الإنترنت[19].

وبتطبيق هذه المبادئ العامة على الجرائم الإلكترونية؛ ينبغي أوّلًا أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية تدخل في تكوين هذه الجريمة، فلكي يتوافر القصد الجنائيّ؛ يجب أن يحيط علم الجاني بعناصر الركن المادّي للجريمة.

ولعلّ أوّل هذه العناصر هو موضوع الحق المعتدى عليه، وعلى سبيل المثال: يتعيّن توافر علم الجاني أنّ فعله ينصبّ على مستند إلكترونيّ محميّ جنائيًّا بما يتضمّنه من معلومات، وبيانات بكونه محلّ الحق الذي يحميه المشرّع، فإذا ظنّ الفاعل بناء على أسباب معقولة أنه يجري على سبيل المثال بعض العمليات الحسابية عن طريق الحاسب الآلي دون أن يتّجه علمه إلى أنه يدخل إلى نظام الحاسب الآلي بما يحتوي عليه من مستندات إلكترونية؛ فإنّ قصد الدخول لا يتوافر لديه، والحقيقة أن هذا الفرض على الرغم من أهميته القانونية إلا أنه يفتقر إلى هذه الأهمية من الناحية العملية، ونادرًا ما يدخل الفاعل إلى نظام

---

[14] أ. نسمة بطيحي، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، 2019م، ص80.
[15] خالد بن سليمان الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص79-80.
[16] أ. نسمة بطيحي، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، 2019م، ص80.
[17] خالد بن علي بن نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، 2022م.
[18] د. محمد حميد المزمومي، النظام الجزائي السعودي، 2019م.
[19] راضية عيمور، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، 2022م، ص96.

الحاسب الآليّ، وهو على غير علم بذلك، ويرجع ذلك للخبرة التي يتمتّع بها المجرم المعلوماتيّ في أغلب الأحوال التي تحوّل دون إمكان التسليم بهذا الفرض، وعلى الرغم من ذلك؛ فإنّه إذا ثبت انتفاء هذا العلم انتفى القصد الجنائي[20].

المناقشة

تتحدث الدراسة عن الجرائم المعلوماتية وعن المخترقين وكيفية الاختراقات وسهولة دخولهم إلى الأجهزة الحاسوبية وسرقة البيانات والمعلومات والهدف منها، وتم الاطلاع على دراسات أخرى تناولت مثل هذا النوع من الجرائم، ووجد أن هناك ثغرة يقوم المخترق باستغلالها وهي عدم وجود اتفاقيات بين الدول التي من شأنها القبض عليهم، ولما كانت اتفاقية بودابست تشمل ثلاثين دولة فقط فإن المخترقين يعملون من غير الدول الثلاثين وبالتالي لابد من الاتحاد بين جميع دول العالم ووضع اتفاقية تعالج إشكالية دولية وهي الجريمة الإلكترونية وتجاوزها للحدود الدولية بما يساعد الدول على مكافحة هذه الجريمة وتعقب مرتكبيها والقبض عليهم وتقديمهم للعدالة. لذا كان الهدف من هذه البحث اقتراح الحلول المناسبة للقضاء على قضية الاختراقات الدولية للشبكة العنكبوتية.

النتائج والتوصيات

أوصي بتطوير اتفاقية يودابست التي وقعت عليها ثلاثون دولة لمقاومة الجرائم المعلوماتية والاتصالات لعام 2001م وذلك بعمل نظام دولي يشمل جميع الدول صادر من الأمم المتحدة لتبادل المخترقين بين الدول لمحاكمتهم أو إنشاء محكمة دولية خاصة بالجرائم المعلوماتية لمحاكمة مخترقي الانترنت حتى ينالوا جزائهم أينما كانوا.

قائمة المراجع

المصادر الدينية:

- القرآن الكريم

الكتب:

- د. محمد حميد المزمومي، النظام الجزائي السعودي، 2019م.

الرسائل الجامعية:

- إبراهيم بن محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، 2018م.

[20] اللجنة العلمية، معهد الكويت للدراسات القضائية والقانونية، 2018-2019م، ص 16-17.

- خضران محمد رياض، نظام تسليم المجرمين في القانون الدولي، 2013م.
- خالد بن سليمان الحمادي، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م.
- عبد المجيد مراد داد محمد أحمد، المسؤولية الجزائية عن إساءة استخدام وسائل التواصل الاجتماعي،2019-2020م.
- راشد حسن حسين عياش، جريمة اختراق النظم والشبكات المعلوماتية، 2019م.
- داود إدريس وشيبان أنيس، جريمة الدخول إلى النظام المعلوماتي في القانون الجزائري، 2022-2023م.

المقالات:

- د. إسلام مصطفى جمعة، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، 2022م.
- د. علواش كهينة، مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي بين اختراق الخصوصية وآليات المواجهة، 2022م.
- د. فادي توكل، د. محمود فكري عبد الصادق الشاهد، تنظيم القانوني لتجارة الفوركس، 2023م.
- د. دينا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، 2019م.
- د. محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، 2018م.
- أ. جميلة سعيد مصباح شوران، جريمة الدخول غير المشروع وفقًا قانون الجرائم الإلكترونية الليبي رقم 5 لسنة 2022م، 2023م.
- أ. نسمة بطيحي، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، 2019م.
- خالد بن علي بن نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، 2022م.
- اللجنة العلمية معهد الكويت للدراسات القضائية والقانونية، 2018-2019م.
- مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، 2016م.
- راضية عيمور، الجريمة الإلكترونية وآليّات مكافحتها في التشريع الجزائري، 2022م.
- ما شاء الله عثمان الزوي، المسؤولية الجنائية للدخول أو البقاء غير المشروع في النظام
- المعلوماتي دراسة في القانون الليبي المقارن، 2023م.

- راشد حسن عياش، جريمة الاختراق وتأثيرها على الشبكة الإلكترونية في ظل القانون الفلسطيني، 2024م.
- جمال زين العابدين، جرائم اختراق النظم الإلكترونية بين التشريع المصري والمغربي، 2020م.

الأنظمة:

- نظام مكافحة جرائم المعلوماتية السعوديّ 1428هـ - 2007م.
- قانون الجرائم الإلكترونية الليبيّ 2022.
- قانون الجرائم الإلكترونية الأردنيّ 2015.
- قانون مكافحة جرائم تقنية المعلومات العمانيّ 2011.
- قانون جرائم تقنية المعلومات البحرينيّ 2014.
- قانون مكافحة الجرائم الإلكترونية القطري2014.

الاتفاقيات:

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

المصادر الأجنبية:

- Nadia Khadam, Nasreen Anjum, Abu Alam, Qublai Ali Mirza, Muhammad Assam, Emad A.A. Ismail, Mohamed R. Abonazel, How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan, 2023
- A Framework for Cyber Crime Investigation, Ayşe Okutan, Prof. Dr. Yalçın Çebi, 2019
- Ismaeel Alhadidi, Aman Nweiran, Ghofran Hilal, The influence of Cybercrime and legal awareness on the behavior of university of Jordan students ,2024
- A VAGUE LAW IN A SMARTPHONE WORLD: LIMITING THE SCOPE OF UNAUTHORIZED ACCESS UNDER THE COMPUTER FRAUD AND ABUSE ACT, 2013
- CYBERCRIME'S SCOPE: INTERPRETING "ACCESS" AND "AUTHORIZATION" IN COMPUTER MISUSE STATUTES, 2003.
- Cyber-trespass and ‘Unauthorized Access’ as Legal Mechanisms of Access Control: Lessons from the US Experience, 2007.
- Illegal Access to Information Systems in the Qatari Criminal Law: A Comparative Study, 2018.