International Journal of Law Research and Studies (IJLRS)
المجلة الدولية للبحوث والدراسات القانونية
Vol. (5), No. (9)
IJLRS
September 2026
الإصدار (5)، العدد (9)

التمييز بين جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعيّ، والجرائم الأخرى المرتبطة بها

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

ملخص البحث

تناولت هذه الدراسة جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي في النظام السعودي، وقُسِّمت هذه الدراسة إلى خمسة فصول؛ إذ سُلِّط الضوء على ماهية الجريمة، وأهمية تجريمها، وتُطُرِّق إلى أركان الجريمة، والعقوبات المترتبة على مرتكبيها. وقد استعان الباحث في هذه الدراسة بالمنهج الوصفيّ؛ لشرح مفهوم جريمة الدخول غير المشروع، وخطرها على المجتمع، وبالمنهج التحليلي؛ لاقتراح الأنظمة، والتشريعات الرادعة والزاجرة. تهدف هذه الدراسة إلى بيان مفهوم مدى خطورة الجريمة، وأثرها في المجتمع، وضرورة التعاون الدوليّ؛ لمكافحة الجرائم العنكبوتية، وقد خرجت هذه الدراسة بعدة نتائج، وتوصيات، من أهمّها: إذا كان المخترقون من داخل المملكة طُبِّق عليهم نظام مكافحة الجرائم المعلوماتية السعودي، أمّا اذا 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.

Distinguishing between the crime of unauthorized access to social media and other related crimes

Shihab Abdulrahman Hamed Al-Masoud
Master's Degree, 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 study 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 كلّه؛ لأنّ توفير الحماية والحرية للأفراد واجب على الدولة، ومن دون تلك الحماية؛ تتدهور الدولة، ويتضرّر الأفراد ويتفكك المجتمع، وتحدث الحروب الأهلية.

واعتبارًا لطبيعة الجريمة الإلكترونية العابرة للحدود، وإمكان ارتكابها من أيّ مكان في العالم؛ لإحداث نتائجها في مكان آخر، وسرعة إخفاء أدلّتها وسهولته؛ فهذا التداخل في دوائر الاختصاص المكانيّ لمباشرة الإجراءات القانونية، إضافة إلى تعقيدات التحقيق فيها، وضبط أدلّتها ومرتكبيها؛ كلّ ذلك يجعل دراستها ومواجهتها في المجتمع الخليجيّ، أو غيره من المجتمعات أمرًا، لا ينفصل عن التعرف تعرُّفًا عامًّا على ماهيتها، ومفهومها، وأسبابها، وتطوراتها، ودوافعها، وآثارها، والجهود الدولية، والإقليمية؛ لمواجهتها، والحدّ منها؛ فهي مشكلة عالميّة، تتأثر بها منطقة الخليج العربيّ بقدر معين مثل بقية أقاليم العالم، ودوله، وسوف نتناول ذلك بالقدر المناسب من التفصيل؛ فالجريمة الإلكترونية نوعان، الأول: الجرائم المُوجَّهة ضدّ جهاز الحاسب الآليّ، أو أنظمة تقنية المعلومات والاتصالات الأخرى؛ لإتلافها، أو تدميرها، أو تعطيلها، والنوع الآخر: الجرائم التي يكون فيها الحاسب الآلي وسيلة لارتكاب جرائم الاحتيال، وسرقة الهُويّات، وبطاقات الائتمان، والأرصدة المالية، والتزوير، والاختلاس، وسرقة حقوق الملكية الفكرية، والابتزاز، والسلوك الانحرافيّ، والاستغلال الجنسيّ للأطفال.

أهمية البحث

من الناحية العلمية تأتي أهمية الدراسة من حداثة النظم القانونية في صياغة تشريعات خاصة بمكافحة الجرائم المعلوماتية؛ لأن الجرائم المعلوماتية أصبحت في تزايد مستمر وبمختلف الأساليب والتقنيات، وذلك بسبب التطور المستمر في المجال التكنولوجي مما يوجب على الباحثين في هذا المجال على مواكبة ذلك التطور بمزيد من الأبحاث والدراسات، ومن هنا تكمن أهمية الدراسة في التعريف بجريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي. وأما من الناحية العملية فتكمن أهمية الدراسة في استعراض جهود المملكة العربية السعودية في مكافحة الجرائم المعلوماتية، وبيان خطورتها، وأيضًا بيان العقوبات التي فرضها المشرّع، وأخيرًا ظروف تشديد العقوبة، وبيان حالات الإعفاء من العقوبة.

مشكلة البحث

تكمن الإشكالية في جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي في أنها خطيرة للغاية، ويجب التصدي لها بشتّى أنواع 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، وهنا تظهر إشكالية البحث في الأسئلة التالية:

أولًا: ما مدى كفاية النصوص القانونية في الحد من جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟

ثانيًا: ما هو المقصود بجريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟

ثالثًا: ما هي أركان جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟

رابعًا: ما هي العقوبات المترتبة على الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟

أهداف البحث

أولًا: التعريف بجريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي.

ثانيًا: بيان مفهوم مدى خطورة جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي، وأثرها في المجتمع.

ثالثًا: مدى تطوّر جهود المملكة العربيَة السعوديَة في مكافحة جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي.

رابعًا: بيان أوجه التشابه والاختلاف بين جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي، والجرائم الأخرى المرتبطة بها.

خامسًا: توضيح العقوبات الأصليّة والتكميليّة لجريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي، والمنصوص عليها في نظام مكافحة الجرائم المعلوماتية السعوديّ.

منهج البحث

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

حدود الدراسة

من الناحية الموضوعية؛ تعتمد الدراسة على التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي، ومن الناحية المكانية؛ تتناول الدراسة جريمة الدخول غير المشروع إلى النظام المعلوماتي وفقًا لنصوص نظام مكافحة الجرائم المعلوماتيّة السعوديّ والتشريعات الدوليّة.

تساؤلات الدراسة

أولًا: ماذا تمّ في مجال مكافحة جريمة الدخول غير المشروع على المستوى المحليّ، والعربيّ، والدوليّ؟

ثانيًا: ماذا يُقصَد بالجرائم المعلوماتية، وجريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟

ثالثًا: ما هي أوجُه التشابه، والاختلاف بين جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟

رابعًا: ما هي أركان جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي الموجبة للعقوبة؛ المحل والمادّيّ والمعنويّ؟

خامسًا: ما هي العقوبات المقرَّرة لجريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي؟

صعوبات الدراسة

إنّ أبرز صعوبات الدراسة التي واجهها الباحث تتمثل في قلة المراجع، والدراسات، والبحوث المتعلقة جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعي على المستوى المحلّيّ، والدوليّ، وقد استند الباحث إلى المراجع المتاحة، واعتمد على المنهج التحليليّ لنصوص نظام مكافحة جرائم المعلوماتية السعوديّ، واستند الباحث -أيضًا- إلى المنهج المقارن؛ للتغلّب على تلك الصعوبات.

الدراسات السابقة

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

مشكلة الدراسة: تكمن مشكلة البحث 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 الثانية: شوران، جميلة سعيد مصباح، 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 صورته البسيطة، والمشدّدة، ومدى عدّ هذه الجريمة من جرائم السلوك، أو الضرر.

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

ثالثًا: مدى كفاية النّصّ القانونيّ المجرّم لفعل الدخول غير المشروع في تغطية كل ما يتصل بهذه الجريمة من أفعال.

الدراسة الثالثة: A Framework for Cyber Crime Investigation, Ayşe Okutan, Prof. Dr. Yalçın Çebi, 2019

مشكلة الدراسة: التطوّر التكنولوجي الجديد في العالم العولميّ ينتشر في جميع أنحاء العالم. ومع تطور التكنولوجيا، وزيادة التحكم في البيانات، وزيادة الاتصالات البيانية وتسارعها، ونتيجة لعدم كفاية تحليل المخاطر في هذا المجال؛ فإنّ هذا النوع من الجرائم قد برز في جميع أنحاء العالم، ويواجه كلّ يوم أنواعًا مختلفة من الجرائم، ولُحِظ أنّ الجريمة الأكثر انفتاحًا على التغيير والتطور هي الجرائم السيبرانية، بجانب الجرائم التي تؤثر في الأمن القوميّ، فقد وصلت إلى مستوى مهمّ للغاية، يمكن أن يؤذي شخصًا واحدًا، ومن أجل منع هذه الأضرار؛ أُدخِل النظام العقابيّ؛ إذ كان في جميع المجالات، وفي هذه الدراسة ستُفحَص العملية؛ حتى يُحكَمَ على النظام القضائي من حيث قابلية تطبيق تكنولوجيا المعلومات والاتصالات على الجريمة، وستُغطّى أنواع الجرائم السيبرانية، والمؤسسات التي ستكافح هذه العناصر الإجرامية، والأدوات البرمجية، والمادية المستخدمة في مرحلة تحديد هوية هذه المؤسسات بالتفصيل، وسيُفَصَّل الكشف عن مصادر البيانات الرقمية، وجمع الأدلّة من موقع الحادث، والحفاظ على السلامة، والبحث عن البيانات التي قد تُشكّل جريمة، وإعداد تحليل النتائج، واستعادة البيانات المحذوفة، أو المشفرة، أو التالفة، وإبلاغها، وفي هذه الدراسة ستُناقَش هذه الجرائم وفقًا لقوانين الجرائم السيبرانية في التشريع، ونتيجة لجميع هذه الخطوات؛ سيُتَّخذ القرار من خلال تفسير طريقة جعلها أكثر فائدة.

الدراسة الرابعة: 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

مشكلة الدراسة: تُبرز العديدُ من الدراسات البحثية النموَّ المتسارع لهجمات البرمجيات الخبيثة على مستوى العالم، ممّا يشكّل تهديدًا كبيرًا للمجتمع، ويُظهِر المجرمون الإلكترونيّون قسوة متزايدة، ولا يُظهِرون أيّ علامات على الشفقة تجاه الأفراد، أو المؤسسات، ومن الواضح أنّ المجرمين الإلكترونيّين لن يتردّدوا في استخدام أيّ وسيلة؛ للحصول على الدخول غير المصرّح به إلى المعلومات السّرّيّة؛ لمكافحة هجمات البرمجيّات الخبيثة كفاحًا فعّالًا، وتوجد حاجة إلى قوانين إلكترونية صارمة، ويُعاقب على استخدام البرمجيات الخبيثة في العديد من البلدان، ومع ذلك؛ لم تتناول الأدبيات القانونية ما إذا كانت هذه العقوبات تُحدث رادعًا، أو لا تحدث، وعالجت هذه المقالة البحثية هذه الفجوة، وفي هذه الدراسة؛ حُلِّلت فعالية القوانين الجنائية المتعلقة بجرائم البرمجيات الخبيثة في اختصاصات مختلفة باستخدام منهجيّة البحث العقديّ، وفُحِصت القوانين الإلكترونية في الولايات المتحدة الأمريكية، والمملكة المتحدة، وإثيوبيا، وباكستان، والصين؛ لتحديد ما إذا كانت العقوبات المفروضة على هذه الجرائم مناسبة بالنظر إلى شدة الأذى الناتج، وتوصلت الدراسة إلى أنّ عقوبات البرمجيات الخبيثة يجب أن تأخذ في الاعتبار إنشاء الشيفرات الخبيثة أو استخدامها، واستهداف الأفراد، أو المؤسسات، ودرجة العواقب دون النظر عمّا إذا كانت نية الإجرام موجودة، أو غير موجودة.

الدراسة الخامسة: A Vague Law in A Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act, 2013

مشكلة الدراسة: قانون مكافحة الاحتيال، والاعتداء على الحاسوب (CFAA) يجرم على نطاق واسع الوصول غير المصرّح إليه إلى أجهزة الحاسوب، والمعلومات الرقمية، ولكنْ إلى أيّ مدى يجب أن تمتدّ هذه المحظورات الفيدرالية إلى مجال البيانات المتنقلة؟ فمع استمرار الهواتف الذكية، وتطبيقات الهاتف المحمول في إعادة تعريف المشهد الرقمي؛ فقد أدّت محاولات تطبيق قانون مكافحة القرصنة الذي يبلغ عمره عقودًا في هذا المجال الجديد إلى خلق سابقةٍ مثيرة للقلق المحتمل.

كافح القُضاة والنقاد؛ لتفسير أحكام قانون مكافحة الاحتيال، والاعتداء على الحاسوب الغامضة والمبهمة، وتوجهوا إلى قانون العقود، وقانون الوكالة، وعلوم الحاسوب؛ للحصول على التوجيه، ويجادل هذا التعليق بأنّ التفسيرات القائمة على العقود، والوكالة تنطوي على مخاوف من الغموض الدستوري، وأنّ النهج القائم على الشفرة لا يعالج معالجة كافية سوء استخدام "الداخلية" للمعلومات، وفي سياق خصوصية بيانات تطبيقات الهاتف المحمول؛ فإنّ أوجُه القصور في التفسيرات الحالية

تستدعي نظرة أضيق؛ للوصول غير المصرح به، ومن خلال تقييد المسؤولية على مفاهيم القرصنة التقليدية، وسوء استخدام المعلومات الخطير فقط؛ يمكن أن يخدم قانون مكافحة الاحتيال والاعتداء على الحاسوب هدفه الأصلي والأساسي خدمة أفضل: كمعاقبة قراصنة الحاسوب الإجراميين، وأولئك الذين يسيئون استخدام حقوق الوصول الشرعية.

الدراسة السادسة: Ismaeel Alhadidi, Aman Nweiran, Ghofran Hilal, The influence of Cybercrime and legal awareness on the behavior of university of Jordan students ,2024

مشكلة الدراسة: توجد زيادة سريعة في استخدام الإنترنت، وتكنولوجيا المعلومات من الطلاب في الأوقات المعاصرة، ونتيجة لذلك؛ واجه المعلّمون التربويّون في جميع أنحاء العالم مشكلة كبيرة؛ بسبب المستوى غير المسبوق من الاعتماد، وإلى حدّ كبير على هذه التكنولوجيا، وإضافة إلى ذلك على غرار أي ظاهرة اجتماعية ناشئة مماثلة؛ أدّى هذا الاعتماد على التكنولوجيا إلى إنشاء طيف جديد من السلوكيات غير القانونية، والإجرامية، ويقدِّم هذا البحث تحليلًا شاملًا لأثر الجرائم الإلكترونية، والوعي القانوني على سلوك الأفراد الشباب في المجتمع مع دمج المنظورات النظرية، والتجريبية لمعالجة الموضوع قيد الدراسة، وأُجري تحقيق كمّيّ باستخدام استبانة، وُزِّعت على عينة عشوائية مكونة من 2000 طالب مسجل في جامعة الأردن بكونها موضوعًا لدراستنا، وتوضح نتائج دراستنا وجود ارتباط قويّ، وحاسم بين درجة الوعي القانونيّ للطلاب بالجرائم الإلكترونية، ومشاركتهم في الأنشطة الإلكترونية غير المشروعة، وعلاوة على ذلك؛ تشير النتائج إلى أنّ الجنس وعوامل أخرى متنوعة تؤثر في إقناع الطلاب بعدم المشاركة في هذه السلوكيّات الإجرامية، ولذا؛ فإنّ هذا يؤكد أهمية تنفيذ إستراتيجيات فعّالة؛ لتعزيز الوعي القانوني للطلاب بشأن الجرائم الإلكترونية؛ للحدّ من مشاركتهم فيها.

المبحث الأول: التمييز بين جريمة الدخول غير المشروع إلى وسائل التواصل الاجتماعيّ، والجرائم الأخرى المرتبطة بها

توجد العديد من الجرائم المرتبطة بجريمة الدخول غير المشروع، ومن الجرائم المرتبطة بجريمة الدخول غير المشروع: جريمة تجاوز حدود التصريح، وجريمة البقاء غير المصرح به، وجريمة الاعتراض غير القانوني، وجريمة تسهيل ارتكاب جريمة الدخول غير المشروع، وسوف نوضّح كلًّا منها على حدة في فرع مستقلّ.

المطلب الأول: جريمة تجاوز حدود التصريح:

نحن نعلم أنّ حالة عدم وجود التصريح لدى الشخص للدخول إلى النظام المعلوماتي -ابتداءً- إشكال بقدر ما تثيره حالة وجود هذا التصريح لدى الشخص؛ ففي الحالة الأولى نكون أمام جريمة الدخول غير المشروع إذا ما توافرت أركانها، أمّا في الحالة الثانية؛ فإنّ الشخص يكون مصرّحًا له بالدخول إلى النظام المعلوماتيّ في حدود معينة، إلا أنه يتجاوز تلك الحدود، فنكون – هنا- أمام جريمة تجاوز حدود التصريح، وذلك بكون هذا التصريح لا يمتدّ إلى البيانات الأخرى من النظام غير المصرَّح له بالدخول إليها، ونبين أنّ الفاعل في جريمة تجاوز حدود التصريح غالبًا ما يكون من الأشخاص العاملين لدى الجهة، أو المؤسسة التي دُخِل إلى النظام المعلوماتي فيها، إلا أنه يتجاوز التعليمات، والسلْطة المُخوّلة له من الجهة، أو المؤسسة، وذلك بالدخول إلى حدود أخرى غير مرخص له بالدخول إليها، فضلًا إلى أنّه من الصعب في كثير من الأحيان معرفة ما إذا كان العامل تجاوز حدود اختصاصه، والصلاحيات الممنوحة له أو لم يتجاوزها، وما إذا كان قد تجاوز حدود التصريح تجاوزًا متعمدًا، أو غير متعمدٍ، وبناءً على ذلك، وتفاديًا من الوقوع في الأخطاء الفادحة؛ ينبغي لكل جهة، أو مؤسسة أن تحدّد اختصاصات كل عامل وصلاحياته تحديدًا دقيقًا، ثمّ يُبحَث فيما إذا كان العامل قد تجاوز حدوده تجاوزًا متعمدًا، أو غير متعمدٍ، فإذا تجاوزها تجاوزًا متعمدًا؛ يُعدّ العامل مرتكبًا تجاوز حدود التصريح [1].

ومن التشريعات العربية التي تناولت جريمة تجاوز حدود التصريح: قانون الجرائم الإلكترونية الأردني في المادة الثالثة في الفقرة الأولى التي نصّت على أنه "يعاقب كل من دخل قصدًا إلى الشبكة المعلوماتية أو نظام معلومات بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح، بالحبس مدة لا تقل عن أسبوع ولا تزيد على ثلاثة أشهر أو بغرامة لا تقل عن (100) مائة دينار، ولا تزيد على (200) مائتي دينار، أو بكلتا هاتين العقوبتين"[2]. وكذلك قانون مكافحة جرائم تقنية المعلومات العماني في المادة الثالثة التي نصّت على أنه "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة

[1] الحمادي، خالد بن سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص29-30.
[2] قانون الجرائم الإلكترونية الأردني.

ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين كل من دخل عمدا ودون وجه حق موقعًا إلكترونيًا، أو نظامًا معلوماتيًا، أو وسائل تقنية المعلومات، أو جزءًا منها أو تجاوز الدخول المصرح به إليها، أو استمر فيها بعد علمه بذلك"[3]، وفي القانون القطري نجد أنه قد جرّم كلًّا من الدخول المجرد، وتجاوز حدود التصريح، والوجود داخل النظام بعد علم الشخص بذلك، وذلك في قانون مكافحة الجرائم الإلكترونية القطري؛ إذ نصّت المادّة الثالثة في الفقرة الأولى من النظام على أنه "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، دون وجه حق، بأي وسيلة، موقعًا إلكترونيًا، أو نظامًا معلوماتيًا، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك"[4]. وكلٌّ من المشرّع العمانيّ، والقطري كانا الأفضل في الصياغة إلى جانب أنهما قد شملا جميع الحالات على خلاف التشريع الأردنيّ؛ إذ إنّ المشرّع الأردني قد جرّم الدخول غير المشروع، وتجاوز حدود التصريح إلا أنه لم يجرّم البقاء غير المشروع الذي يكون في الأحوال التي يكون فيها الدخول مشروعًا، أي: مصرح به إلا أنّ التصريح ينتهي، ورغم ذلك يبقى الشخص داخل النظام، أو في الأحوال التي يكون فيها الدخول غير مشروع، ورغم ذلك لا تقوم الجريمة كالدخول عن طريق الخطأ [5].

المطلب الثاني: جريمة البقاء غير المصرَّح به:

يقصد بالبقاء غير المصرح به هو "التواجد داخل النظام المعلوماتي والبقاء فيه خلافًا لإرادة من له الحق في منح التصريح في التواجد في النظام"، ويكون ذلك إما في الأحوال التي يكون فيها الدخول مشروعًا: كوجود تصريح للدخول على سبيل المثال، أو لأن الدخول على جهاز حاسب آلي عن طريق الاختراق غير معاقب عليه؛ لانتفاء عنصر من عناصر التجريم، وتتحقق الصورة الأولى في وجود تصريح للدخول إلى النظام المعلوماتي لوقت معيّن إلا أنّ هذا الوقت ينتهي، ومع ذلك يظلّ هذا الشخص داخل النظام، وباقيًا فيه؛ فالبقاء في هذا الفرض يتحقق عند عدم قطع هذا الشخص بالاتصال بالنظام رغم إدراكه، وعلمه أنّ وجوده في النظام غير مشروع؛ بسبب انتهاء وقت التصريح، وصلاحيته؛ فالجريمة –هنا- تقوم من اللحظة التي كان يجب على الشخص أن يخرج فيها من النظام فورًا، ومع ذلك لا يخرج من النظام، وتتحقق الصورة الثانية لقيام جريمة البقاء غير المصرح به في الأحوال التي يكون فيها الدخول عن طريق الخطأ، أو عن طريق الصدفة، إلا أن الفاعل رغم اكتشافه ذلك يظلّ داخل النظام، ولا يخرج منه، فمعلومٌ أنّ جريمة البقاء غير مصرح به هي -أيضًا إلى جانب جريمة الدخول غير المشروع- تعدّ جريمة عمدية، ولا ترتكب بصورة الخطأ، ومن هنا؛ جاءت أهمّية تجريم جريمة البقاء غير المشروع لمواجهة هذين الفرضين، والبقاء في هذا الفرض يبدأ –أيضًا- من اللحظة التي يعلم فيها الشخص أنّ دخوله غير مشروع، ومع ذلك يبقى في النظام، ولا يضع حدًّا لوجوده داخل النظام[6]، ولقد نصّت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على هذه الجريمة؛ لأهمّيّتها، وذلك في المادة السادسة في الفقرة الأولى على أنه "الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به"[7]. ومن التشريعات التي جرّمت فعل البقاء غير المشروع: قانون مكافحة جرائم تقنية المعلومات العماني في المادة الثالثة التي نصّت على أنه "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين كل من دخل عمدًا ودون وجه حق موقعًا إلكترونيًا، أو نظامًا معلوماتيًا، أو وسائل تقنية المعلومات، أو جزءًا منها أو تجاوز الدخول المصرح به إليها، أو **استمر فيها بعد علمه بذلك**"[8]، وإذا نظرنا إلى المشرّع القطريّ نجد أنّه هو الآخر قد جرّم فعل البقاء غير المصرح به؛ عندما نصّت المادة الثالثة من قانون مكافحة الجرائم الإلكترونية القطري على أنه "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، دون وجه حق، بأي وسيلة، موقعًا إلكترونيًا، أو نظامًا معلوماتيًا، أو شبكة معلوماتية، أو وسيلة تقنية معلومات، أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك"[9]، ولعلّ ما يميز جريمة البقاء غير المصرح به عن جريمة الدخول غير المشروع هو أنّ الأولى جريمة مستمرة على خلاف الأمر لجريمة الدخول غير المشروع التي تعدّ من الجرائم

[3] قانون مكافحة جرائم تقنية المعلومات العماني
[4] قانون مكافحة الجرائم الإلكترونية القطري.
[5] الحمادي، خالد بن سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص32.
[6] الحمادي، خالد بن سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص33-34.
[7] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
[8] قانون مكافحة جرائم تقنية المعلومات العماني.
[9] قانون مكافحة الجرائم الإلكترونية القطري.

الوقتية؛ فالسلوك الإجراميّ في جريمة البقاء غير المصرح به يستمرّ مع ذلك الاعتداء على المصلحة القانونية، وذلك من اللحظة التي يعلم فيها الفاعل أنّ دخوله غير مصرح به، أو من اللحظة التي يعلم فيها أنّ التصريح قد انتهى، سواء أأدّى البقاء إلى نتيجة معينة، أم لم يؤدّ إلى نتيجة، أما جريمة الدخول غير المشروع؛ فهي تقوم من اللحظة التي يكون فيها الدخول غير مشروع، سواء أكان الدخول مجردًا، أم أدّى دخوله إلى نتائج معينة: كالحصول على البيانات، أو حذفها، أو تعديلها، أو إتلافها، أو تغييرها، وجريمة الدخول غير المشروع جريمة إيجابية على خلاف الأمر لجريمة البقاء غير المصرح به التي تعدّ من الجرائم السلبية؛ لأنّها ترتكب بسلوك سلبيّ، وقد قضت محكمة النقض الفرنسيّة أن استمرار الجاني في استخدام الرقم السري الذي يُسمح له بالدخول إلى قاعدة البيانات مدة، تفوق السنتين -وهذه المدة غير المسموح بها- يشكل جريمة البقاء غير المشروع المعاقب عليها؛ لأنّ هذا الرقم السري قد حُصِل عليه، ورُخِّص باستخدامه خلال مدة التجربة فقط، وهذه الأخيرة تجاوزها الجاني.

وعلى ذلك؛ عدم النص على جريمة البقاء غير المشروع: كجريمة مستقلة، أو مرتبطة بجريمة الدخول غير المشروع يعدّ أمرًا خطيرًا، ونقصًا تشريعيًّا، يجب أن يُسدّ؛ إذ قد يؤدي ذلك لإفلات الكثير من المجرمين من العقاب؛ لعدم إمكان سحب جريمة الدخول غير المشروع في الأحوال التي يكون فيها الدخول مشروعًا: كوجود تصريح إلّا أنّه انتهى، ورغم ذلك ظلّ الشخص داخل النظام، أو في تلك الأحوال التي يكون فيها الدخول عن طريق الخطأ، ورغم ذلك يظلّ الشخص داخل النظام رغم علمه بأنّ دخوله غير مشروع، ففي الفرضين الآخرين؛ لا يمكن معاقبة الفاعل على بقائه في النظام من خلال نصوص جريمة الدخول غير المشروع بتوافر تصريح؛ للدخول ابتداء من ناحية، ولعدم توافر العمد لدى الفاعل عند دخوله بالفرد الثاني من ناحية أخرى، ومن هنا؛ جاءت الأهمية للنص على جريمة البقاء لمعالجة هذين الفرضين، والجدير بالذكر أنّ القانون الأردنيّ لم يتناول جريمة البقاء غير المشروع، في حين أنه قد نصّ على كلٍّ من جريمة الدخول غير المشروع، وجريمة تجاوز حدود التصريح كما سبق أنْ بيّنّا [10].

المطلب الثالث: جريمة الاعتراض غير القانوني:

تقوم جريمة الاعتراض غير القانوني عن طريق التقاط الانبعاثات الكهرومغناطيسية الناتجة عن النظام المعلوماتي، وإعادة بناء هذه الانبعاثات بصورة بيانات، وذلك باستخدام وسائل فنية، ويرجع الهدف من وراء تجريم هذا الفعل لحماية الحقّ في نقل البيانات، والمعلومات؛ فالاعتراض غير القانونيّ يُعدّ انتهاكًا للحقّ في احترام الاتصالات، ومن هنا؛ تجدر الإشارة إلى أنّ الاعتراض غير القانونيّ يختلف عن الدخول غير المشروع؛ مما حدا بالتشريعات من النص على أنّ هذه الجريمة جريمة مستقلّة [11].

ومن التشريعات التي تناولت جريمة الاعتراض غير القانونيّ: نظام مكافحة جرائم المعلوماتية السعودي في المادة الثالثة في الفقرة الأولى التي نصت على أنه "يعاقب بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد عن خمسمائة ألف ريال أو بإحدى هاتين العقوبتين كل شخص يرتكب أي من الجرائم المعلوماتية الآتية: "التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطها أو اعتراضه"[12]، وقانون الجرائم الإلكترونية الليبيّ في المادة الثالثة عشر التي نصّت على أنه "يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 1,000 ألف دينار ولا تزيد على 5,000 خمسة آلاف دينار كل من اعترض نظامًا معلوماتيًا بقصد الحصول على بيانات رقمية أو للربط مع أنظمة إلكترونية أخرى"[13]، وقانون مكافحة جرائم تقنية المعلومات العمانيّ في المادة الثامنة التي نصّت على أنه "يعاقب بالسجن مدة، لا تقلّ عن شهر، ولا تزيد على سنة، وبغرامة، لا تقلّ عن خمسمائة ريال عماني، ولا تزيد على ألفي ريال عمانيّ، أو بإحدى هاتين العقوبتين، كل من اعترض عمدًا ودون وجه حق باستخدام وسائل تقنية المعلومات: كخط سير البيانات، أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية، أو وسائل تقنية المعلومات، أو قطع بثها، أو استقبالها، أو تنصت عليها" [14]. وقانون الجرائم الإلكترونية الأردنيّ؛ إذ نصّت المادة السابعة على أنه "يعاقب كل من قام قصدًا ودون وجه حق باعتراض خط سير البيانات أو التقاط محتواها أو أعاق أو حور أو شطب أو قام بتسجيل ذلك المحتوى سواء المرسل عن

10 الحمادي، خالد بن سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص35-36-37.
11 الحمادي، خالد بن سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص37.
12 نظام مكافحة جرائم المعلوماتية السعودي.
13 قانون الجرائم الإلكترونية الليبي.
14 قانون مكافحة جرائم تقنية المعلومات العماني.

طريق الشبكة المعلوماتية، أو تقنية المعلومات، أو نظام المعلومات، أو البيانات المتبادلة داخل النظام، أو الشبكة ذاتها بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن (1500) ألف وخمسمائة دينار ولا تزيد على (6000) ستة آلاف دينار"[15]، وفي المشرّع القطري نجد أنه –أيضًا- قد جرّم الاعتراض غير القانوني في المادة الرابعة من قانون مكافحة الجرائم الإلكترونية القطري التي نصّت على أنه "يعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كلُّ من التقط أو اعترض أو تنصت عمدًا، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور"[16].

والآن بعد أن استعرضنا بعض التشريعات التي نصّت على جريمة الاعتراض غير القانونيّ؛ سوف نُبيّن أوجُه التشابه والفوارق بين كلٍّ من جريمة الدخول غير المشروع، وجريمة الاعتراض غير القانوني، فكلتا الجريمتين تؤدّيان إلى نتيجة واحدة، وهي الوصول إلى مُعطيات غير مصرح للفاعل بالوصول إليها، وكلتا الجريمتين –أيضًا- تتطلبان عدم وجود تصريح من صاحب الحق، ولا يرتكبان بصورة الخطأ؛ إذ تعدّ كلتا الجريمتين من الجرائم العمدية، أما الفوارق؛ فإن الاعتراض غير القانوني لا يتطلب الدخول إلى النظام المعلوماتي؛ إنما هو تنصّت، وتلصّص، واعتراض على رسائل مرسلة بين جهازين عن طريق شبكة معلوماتية، وجريمة الدخول غير المشروع تفترض تشغيل النظام من الفاعل، وذلك على خلاف الأمر للاعتراض غير القانونيّ؛ إذ لا تتطلّب الجريمة تشغيل النظام من الفاعل؛ إذ يكون تشغيل النظام عن طريق شخص آخر، وجريمة الاعتراض غير القانوني لا يمكن معها تحديد المعلومات، والبيانات التي سوف يعترضها الفاعل ويلتقطها، على خلاف الأمر لجريمة الدخول غير المشروع التي يمكن معها تحديد ما يريده الفاعل من بيانات معلومات، وما يريد الفاعل –أيضًا- أن يفعله داخل النظام من إفشاء للمعلومات، وحذف المحتويات، ومن الممكن أن يستخدمها في الابتزاز، ومن الفوارق بين نتيجة الجريمتين -كذلك- أن جريمة الاعتراض غير القانوني تعدّ من الجرائم المادية؛ إذ لا بدّ من تحقّق نتيجة معينة، وهي التقاط الانبعاثات الكهرومغناطيسية، وهي مستمرّة متى ما استمرّ فعل الاعتراض، على خلاف الأمر لجريمة الدخول غير المشروع التي تعدّ من الجرائم الشكلية لدى أغلب التشريعات، وتعدّ –أيضًا- من الجرائم الوقتية.

ذلك أنّ جريمة الاعتراض غير القانوني في كلّ صورها لا تخرج العقوبة فيها عن إطار الجنح؛ إذ إنّ العقوبة فيها على الرغم من تباين التشريعات فيها إلّا أنّها لا تصل إلى مصافّ الجنايات، وذلك على خلاف الأمر لجريمة الدخول غير المشروع التي قد تصل العقوبة فيها في بعض التشريعات إلى مصافّ الجنايات؛ متى ما ترتبت على جريمة الدخول غير المشروع نتيجة معينة[17].

المطلب الرابع: تسهيل ارتكاب جريمة الدخول غير المشروع:

تجرّم بعض التشريعات الأفعال التي تسهّل ارتكاب الجرائم المعلوماتية حتى جريمة الدخول غير المشروع، على كون القيام ببعض الأفعال التي تساعد ارتكاب جريمة الدخول غير المشروع، وتسهلها؛ قد يستحيل تجريمها في إطار الاشتراك الجرميّ؛ لتخلّف شروط الاشتراك الجرميّ التبعيّ فيها على الرغم من خطورتها؛ ممّا جعل العديد من التشريعات أن تجرّم تسهيل ارتكاب جريمة الدخول غير المشروع بكونها جريمة مستقلة، أي: سلوك إجراميّ مستقلّ، ونبيّن أنّ الأفعال التي تجرّمها تلك التشريعات تساعد ارتكاب جريمة الدخول غير المشروع وتسهّلها، وجريمة تسهيل ارتكاب جريمة الدخول غير المشروع تقع حتى ولو لم تستخدم تلك الوسائل، والتسهيلات؛ لارتكاب الجريمة؛ فجريمة تسهيل ارتكاب جريمة الدخول غير المشروع هي جريمة مستقلة عن جريمة الدخول غير المشروع [18].

ومن التشريعات التي جرّمت تسهيل ارتكاب جريمة الدخول غير المشروع بكونها جريمة مستقلة: قانون الجرائم الإلكترونية الليبي في المادة الرابعة عشر؛ إذ نصّت على أنه "كل من قدم أو أنتج أو زرع أو أستورد أو أصدر أو روج أو حاز بقصد الاستخدام غير المشروع جهازًا أو برنامجًا معلوماتيًا أو أي بيانات معلوماتية معدة لإظهار كلمات السر أو رموز الدخول أو لكسر الحجب، يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن 1,000 ألف دينار ولا تزيد على 10,000 عشرة آلاف

[15] قانون الجرائم الإلكترونية الأردني.
[16] قانون مكافحة الجرائم الإلكترونية القطري.
[17] الحمادي، خالد سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص39-40.
[18] الحمادي، خالد بن سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص40-41.

دينار"[19]، وقانون مكافحة جرائم تقنية المعلومات العماني في المادة الحادية عشر التي نصّت على أنه "يعاقب بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على ثلاثة سنوات وبغرامة لا تقل عن ثلاثة آلاف ريال عماني ولا تزيد على خمسة عشر ألف ريال عماني أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في إنتاج، أو بيع، أو شراء، أو استيراد، أو توزيع، أو عرض، أو إتاحة برامج، أو أدوات، أو أجهزة مصممة، أو مكيفة لأغراض ارتكاب جرائم تقنية المعلومات، أو كلمات سر، أو رموز تستخدم لدخول نظام معلوماتي، أو حاز أدوات، أو برامج مما ذكر، وذلك بقصد استخدامها في ارتكاب جرائم تقنية المعلومات"[20]، وقانون جرائم تقنية المعلومات البحريني في المادة السادسة التي نصّت على أنه "يعاقب بالحبس مدة لا تزيد على سنة وبالغرامة التي لا تجاوز مئة ألف دينار أو بإحدى هاتين العقوبتين، من قام بقصد ارتكاب أي من الجرائم المنصوص عليها في المادة الثانية والثالثة والرابعة والخامسة من هذا القانون بإنتاج، أو استيراد، أو شراء، أو بيع، أو عرض للبيع، أو للاستخدام، أو توزيع، أو تداول، أو حياة، أو نشر، أو إتاحة:

أ- أداة -بما في ذلك أي برنامج -تم تصميمها أو تحويرها بصفة أساسية لغرض ارتكاب أي من الجرائم المشار إليها.

ب- كلمة مرور، أو شفرة دخول، أو أيّ رمز دخول، أو أية بيانات وسيلة تقنية المعلومات أخرى مماثلة، يمكن بواسطتها الدخول إلى نظام تقنية المعلومات أو أي جزء منه"[21].

وفي المشرّع القطري نجد أنه لم ينصّ على جريمة تسهيل ارتكاب جريمة الدخول غير المشروع، لا في قانون مكافحة الجرائم الإلكترونية القطريّ، ولا حتى في قانون العقوبات، وذلك عندما تناول جرائم الحاسب الآلي، ومع ذلك لا يعدّ ثغرة، يمكن من خلالها أن يلوذ الفاعل بالفرار، وعدم معاقبته، وذلك في الأحوال التي تُرتكَب فيها جريمة الدخول غير المشروع باستخدام تلك المساعدات والتسهيلات؛ إذ من الممكن معاقبة كلِّ من يقدّم المساعدة حسب نصّ المادة التاسعة والأربعون من قانون مكافحة جرائم الإلكترونية التي نصّت على أنه "يعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القانون، بذات العقوبات المقررة للفاعل الأصلي"[22]، ولذا؛ يكون الإسهام التبعيّ عقوبة الإسهام الأصلي نفسها، سواء إذا كان الشريك بالاتفاق، أم بالتحريض، أم بالمساعدة، إلا أنّ عدم وجود نصوص تشريعية، تجرّم تسهيل ارتكاب جريمة الدخول غير المشروع قد تجعل الشريك يفعل ما يريد من دون عقاب، وذلك في الأحوال التي يقدم فيها هذا الأخير المساعدة، والوسائل، والأدوات؛ لارتكاب جريمة الدخول غير المشروع، إلّا أنّ الجاني في جريمة الدخول غير المشروع يدخل دخولًا غير مشروع إلى النظام المعلوماتي باستخدام وسائل غير تلك التي قدّمها الشريك، ففي هذا الفرض لا يمكن معاقبة الشريك على ما قدّمه من مساعدة، وأدوات على الرغم من خطورة فعله، وفي الأحوال التي يقدّم فيها الشخص التسهيلات، والوسائل؛ للدخول غير المشروع إلّا أنّ الشخص المقدّمة إليه تلك التسهيلات، والوسائل يَعْدِل عن الدخول غير المشروع، ففي هذا الفرض –أيضًا- لا يمكن معاقبة من قدّم تلك التسهيلات، والوسائل.

ويرجع السبب من وراء عدم إمكان المعاقبة في الفرضين السابقين على كون الجريمة قد ارتُكِبت بوسائل أخرى غير تلك التي قدّمها الشريك في الفرض الأول، ولعدم ارتكاب جريمة الدخول غير المشروع في الفرض الثاني، وعلى ذلك؛ فإن الأمر يتطلب تدخل التشريعيّ، وذلك بالنص على جريمة تسهيل ارتكاب جريمة الدخول غير المشروع بكونها جريمة مستقلّة لمواجهة هذين الفرضين من ناحية، ولردع أي شخص يُنتِج برامج، أو يقدِّم تسهيلات ووسائل؛ لارتكاب جريمة الدخول غير المشروع؛ لما تنقضي عليها هذه الأخيرة من أخطار جسيمة، قد تصاحب خسائر مادية، ومعنوية، سواء أكان ذلك للأفراد، أم المؤسسات، أم الدولة [23].

النتائج

أولًا: أن المشرع السعودي لم ينص على جريمة البقاء غير المصرح به مثل بعض التشريعات.

ثانيًا: أن المشرع السعودي لم ينص على جريمة تجاوز حدود التصريح مثل بعض التشريعات.

---

19 قانون الجرائم الإلكترونية الليبي.
20 قانون مكافحة جرائم تقنية المعلومات العماني.
21 قانون جرائم تقنية المعلومات البحريني.
22 قانون مكافحة الجرائم الإلكترونية القطري.
23 الحمادي، خالد بن سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري، 2019م، ص43-44.

ثالثًا: أن المشرع السعودي لم ينص على جريمة تسهيل ارتكاب جريمة الدخول غير المشروع.

التوصيات

أولًا: أوصي بعمل نظام دوليّ صادر من الأمم المتحدة؛ لتبادل المخترقين بين الدول لمحاكمتهم.

ثانيًا: إنشاء محكمة دولية خاصة بالجرائم المعلوماتية.

ثالثًا: عمل معاهدة أو اتفاقية بين جميع الدول تخصص الجرائم الإلكترونية لتسليم المجرمين مثل اتفاقية بودابست.

رابعًا: نوصي المشرع السعودي بالنص على تجريم حالة تجاوز حدود التصريح.

خامسًا: نوصي المشرع السعودي بالنص على تجريم حالة البقاء غير المصرح به في النظام المعلوماتي.

سادسًا: نوصي المشرع السعودي بتجريم جريمة تسهيل ارتكاب جريمة الدخول غير المشروع.

سابعًا: نوصي المشرع السعودي بوضع حد لمن دخل إلى نظام معلوماتي ومعه تصريح بأن لا يزيد عن مدة معينة.

قائمة المراجع

- أحمد، عبد المجيد مراد داد محمد، المسؤولية الجزائية عن إساءة استخدام وسائل التواصل الاجتماعي،2019-2020م.
- إدريس، داود، أنيس، شيبان، جريمة الدخول إلى النظام المعلوماتي في القانون الجزائري، 2022-2023م.
- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
- الحمادي، خالد بن سليمان، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة، 2019م.
- الزوي، ماشاءالله عثمان، المسؤولية الجنائية للدخول أو البقاء غير المشروع في النظام
- الشعار، خالد بن علي بن نزال، التحقيق الجنائي في الجرائم الإلكترونية، 2022م.
- العابدين، جمال زين، جرائم اختراق النظم الإلكترونية بين التشريع المصري والمغربي، 2020م.
- الفلسطيني، 2024م.
- الفيتوري، عطية عبد السلام، جريمة الدخول غير المشروع إلى أجهزة الحاسب الآلي ومنظومات المعلومات الإلكترونية، 2017م.
- القاسمي، إبراهيم بن محمد، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية، 2018م.
- اللجنة العلمية معهد الكويت للدراسات القضائية والقانونية، 2018-2019م.
- المزمومي، محمد حميّيد، النظام الجزائي السعودي، 2019م.
- المعداوي، محمد أحمد، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، 2018م.
- المعلوماتي دراسة في القانون الليبي المقارن، 2023م.
- بطيحي، نسمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، 2019م.
- بن قربة، حفيظ، جريمة الدخول غير المصرح به إلى منظومة معلوماتية في التشريع الجزائري، 2017م.
- توكل، فادي، الشاهد، محمود فكري عبد الصادق، تنظيم القانوني لتجارة الفوركس، 2023م.

- جمعة، إسلام مصطفى، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، 2022م.
- رياض، خضران محمد، نظام تسليم المجرمين في القانون الدولي، 2013م.
- شوران، جميلة سعيد مصباح، جريمة الدخول غير المشروع وفقًا قانون الجرائم الإلكترونية الليبي رقم 5 لسنة 2022م، 2023م.
- عباوي، نجاة، الإختلافات التشريعية في تجريم الدخول غير المصرح به إلى أنظمة المعلومات، 2016م.
- عياش، راشد حسن حسين، جريمة اختراق النظم والشبكات المعلوماتية، 2019م.
- عياش، راشد حسن، جريمة الاختراق وتأثيرها على الشبكة الإلكترونية في ظل القانون
- عيمور، راضية، الجريمة الإلكترونية وآليّات مكافحتها في التشريع الجزائري، 2022م.
- فهمي، دينا عبد العزيز، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، 2019م.
- قانون الجرائم الإلكترونية الأردنيّ 2015.
- قانون الجرائم الإلكترونية الليبيّ 2022.
- قانون جرائم تقنية المعلومات البحرينيّ 2014.
- قانون مكافحة الجرائم الإلكترونية القطري2014.
- قانون مكافحة جرائم تقنية المعلومات العمانيّ 2011.
- كهينة، علواش، مخاطر الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي بين اختراق الخصوصية وآليات المواجهة، 2022م.
- مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، 2016م.
- نظام مكافحة جرائم المعلوماتية السعوديّ 1428هـ - 2007م.

References

- 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.