The Crime of Unauthorized Access to an Information System

Mustafa Mousa Alajarmeh, Nour Hshem Baj, Rakad Salem Khawaldeh

Ajarmehm@yahoo.com nbaj95@hotmail.com rakadalkhawaldeh@yahoo.com

Department of Law, Faculty of Law, Middle East University, Amman, Jordan

Corresponding Author: Dr. Mustafa Mousa Alajarmeh. Email: Ajarmehm@yahoo.com

Received: February 15, 2026 Accepted: May 7, 2026 Online Published: June 29, 2026

URL: https://journal.aut.edu.jo/index.php/aut

Abstract

The transition of individuals' lives to the digital world and the reliance of institutions and government departments on it through the digital infrastructure in terms of storing, processing and extracting information and data has become a given in our modern era, as countries through government departments and institutions regulate the progress of the public utility regularly and consistently through the digital world allocated to them. The aim of this research is to examine and scrutinize the legal provisions that criminalize the act of accessing an information system without authorization or legal permission, through the crime of unlawful access to an information system. This crime is directly related to unauthorized access by third parties to state-owned information systems, whether for the purpose of viewing the information contained therein, damaging or manipulating it, interfering with the system, or committing other acts that infringe upon the integrity of the information system. Mere access to an information system without authorization constitutes a criminal offense punishable by law. In this research, the study adopted the descriptive-analytical approach, establishing the legal texts addressing this crime as the cornerstone of the analysis, relying on Jordanian and Kuwaiti legislation within the framework of specialized penal laws concerning cybercrimes. The study initially shed light on the concept of crime by identifying the object of criminal protection and clarifying its meaning. Subsequently, the first section addressed the determination of the subject matter of the crime, while the second section examined the elements of the crime, its legal nature, and its constituent components. In conclusion, the researcher reached a number of findings, most notably that the crime of unlawful access to an information system is a formal offense for which the perpetrator is prosecuted upon its mere commission, regardless of the occurrence of harm. The study also presented several recommendations, the most important of which is the necessity of explicitly defining the object of infringement and criminal protection in this crime through clear legal provisions and definitions, in order to avoid ambiguity in the legal text and reduce reliance on interpretation and judicial construction.

Keywords: Official Information System, Unlawful Access, Authorization, Permission, Hacking

جريمة الدخول غير المشروع الى النظام المعلوماتي

مصطفى موسى العجارمة ، نور هاشم باج ، ركاد سالم فلاح خوالده
rakadalkhawaldeh@yahoo.com nbaj95@hotmail.com Ajarmehm@yahoo.com
قسم القانون، كلية الحقوق، جامعة الشرق الأوسط ، عمان، الأردن
الباحث المسؤول: د. مصطفى موسى العجارمة. البريد الالكتروني:Ajarmehm@yahoo.com

تاريخ الاستلام: 15 شباط 2026 تاريخ القبول: 7 أيار 2026 تاريخ النشر عبر الإنترنت: 29 حزيران 2026
الرابط الالكتروني: https://journal.aut.edu.jo/index.php/aut

الملخص

انتقال حياة الأفراد الى العالم الرقمي واعتماد المؤسسات والدوائر الحكومية عليه من خلال البنية التحتية الرقمية من ناحية تخزين المعلومات والبيانات ومعالجتها واستخراجها بات من المسلمات في عصرنا الحديث، حيث أن الدول من خلال الدوائر الحكومية والمؤسسات تقوم بضبط سير المرفق العام بانتظام واضطراد من خلال العالم الرقمي المخصص لها. ويهدف هذا البحث للتدقيق والتمحيص في النصوص القانونية التي جرمت فعل الدخول الى النظام المعلوماتي دون إذن أو صلاحية من خلال جريمة الدخول غير المشروع الى النظام المعلوماتي ، فهي جريمة تتعلق تعلقاً مباشراً بوصول الغير الى النظام المعلوماتي التابع للدولة إما بهدف الاطلاع على ما يحتويه من معلومات، أو بهدف اتلافها أو العبث بالنظام وغيرها من الأفعال التي تمس النظام المعلوماتي، على أن مجرد الدخول الى النظام المعلوماتي دون صلاحية تعد جريمة يعاقب عليها القانون. اعتمد البحث على المنهج الوصفي التحليلي، حيث جُعلت النصوص القانونية الناظمة لهذه الجريمة حجر الأساس للدراسة، وذلك بالاستناد إلى التشريعات الجزائية الأردنية والكويتية المتخصصة في مكافحة الجرائم الإلكترونية، وفي البداية تم تسليط الضوء على مفهوم الجريمة من خلال تحديد محل الحماية الجزائية وبيان مفهومها، حيث تم تحديد محل هذه الجريمة في المطلب الأول، بينما جرى التطرق في المطلب الثاني إلى أركان الجريمة وبيان طبيعتها وعناصرها. وفي ختام هذه الدراسة، تَمّ التوصّل إلى جملة من النتائج؛ تمثّلت أهمها في أن جريمة الدخول غير المشروع الى النظام المعلوماتي هي جريمة شكلية يُلاحق الجاني بها بمجرد وقوعها، وجملة من التوصيات وأهمها لابد من تحديد محل الاعتداء والحماية الجزائية في هذه الجريمة بصريح النص القانوني من خلال سردها وبيانها في التعريفات للابتعاد عن غموض النص والاعتماد على التفسير والتأويل.

الكلمات المفتاحية: النظام المعلوماتي ، الدخول غير المشروع، التصريح، الإذن، الاختراق.

أولاً: المقدمة:

أضحت الدول في العصر الحديث تتجه نحو الاعتماد الكلي على البيئة المعلوماتية في حفظ أعمالها ومعالجة بياناتها، تحقيقاً لسرعة إنجاز التعاملات اليومية للمواطنين بانتظام واضطراد. حيث تُعنى المؤسسات الحكومية بإنشاء بنوك معلوماتية شاملة تضم البيانات الشخصية للأفراد مع توفير امكانية معالجتها والتعديل عليها تماشياً مع ما يطرأ على الفرد من متغيرات قانونية أو واقعية في حياته الفنية والمدنية، ويهدف هذا التحول الرقمي إلى توفير الوقت والجهد على المواطنين عند استخراج وثائقهم الرسمية، فضلاً عن تعزيز قدرة الأنظمة المعلوماتية بالمؤسسات الحكومية على الاحتفاظ بتلك البيانات وحمايتها

حيث أن الدولة بممثليها أعطت الصلاحيات للموظفين العموميين الدخول الى النظام المعلوماتي والتعديل عليه واستخراج وثيقة معلوماتية عند طلب الأفراد، وهذه الصلاحيات منوطة فقط للموظف العام دون غيره استناداً الى علاقته الوظيفية والتبعية مع الدولة، حيث يتمكن الموظف من إتمام عمله من خلال الدخول الى النظام العام وانشاء بيانات خاصة للأفراد أو استحداثها او استخراجها وفقاً للمتطلبات، كما ولا ننسى اعتماد الشركات الخاصة اعتماداً كلياً على النظام المعلوماتي أيضاً في اجراء جميع التعاقدات وعمليات حفظ معلومات الأفراد والتعديل عليها طبقاً لطلباتهم ومعلوماتهم.

ونتيجة لذلك، أصبحت الأنظمة الرقمية التابعة للحكومات والمؤسسات والشركات الخاصة هدفاً رئيسياً للهجمات الإلكترونية والاختراقات غير المشروعة من قبل المجرمين من خلال إقدامهم على ارتكاب الجرائم الإلكترونية، وتعد جريمة الدخول غير المشروع للنظام المعلوماتي تحدياً أمنياً في العصر الرقمي الحديث، فهي تعبر عن تسلل المجرمين الى النظام المعلوماتي العائد الى الدولة وقواعد بياناتها الرقمية، وتكمن خطورتها في كون هذا الفعل يشكل اعتداءً على الكيان الرقمي، بالإضافة الى الاطلاع على ما تحتويه هذه القاعدة من معلومات مهمة تتعلق بالأفراد والدول، بالإضافة الى أن هذه الجريمة قد تكون الخطوة الأولى لدى الجاني لكي يقدم على ارتكاب الجريمة التالية له، من تلاعب أو إتلاف أو حذف أو بث فيروسات وغيرها من الجرائم المعلوماتية.

فهذه الجريمة تمثل خطراً كبيراً على الأمن القومي والسلامة العامة وسلامة الأفراد والمواطنين، ونظراً لحساسيتها، بمجرد قيام الجاني بالدخول الى النظام المعلوماتي يكون قد تحققت الجريمة ومستحق العقوبة في حقه، سواء أفضت الجريمة الى ارتكاب فعل مجرم آخر أم لا. ولخطورة الجريمة، فقد عملت التشريعات العربية المختلفة على تجريم هذه الحادثة من خلال النصوص العقابية التي عالجت الجرائم الإلكترونية، وذلك من خلال تجريمها بالدخول غير المشروع الى النظام المعلوماتي.

ثانياً: أهمية البحث:

تتجلى أهمية البحث في دراسة موقف القانون المقارن من جريمة الدخول غير المشروع لنظام معلوماتي، وذلك من خلال التطرق الى موقف المشرع الأردني والكويتي، وذلك لبيان التأصيل القانوني لهذه الجريمة من خلال بيان مفهوم هذه الجريمة ومحل الاعتداء، وتسليط الضوء على الركن المادي والمعنوي لها.

ثالثاً: إشكالية الدراسة:

أثارت القراءة التحليلية للنصوص التشريعية الناظمة لهذه الجريمة جملةً من التساؤلات والإشكاليات التي تسعى هذه الدراسة إلى الإجابة عنها، وتتمثل في:

1- هل عملت التشريعات المقارنة على تعريف جريمة الدخول غير المشروع بصريح العبارة من خلال القوانين الناظمة للجرائم الإلكترونية؟
2- هل حددت هذه التشريعات معالم وحدود محل الحماية الجزائية لهذه الجريمة؟
3- هل بينت التشريعات السلوك الجرمي آخذةً بعين الاعتبار الطبيعة الرقمية لهذه الجريمة؟
4- هل بينت التشريعات أثر بقاء الجاني في النظام المعلوماتي بعد دخوله وجرمتها؟
5- هل أوضحت التشريعات القصد الجرمي في هذه الجريمة؟

رابعاً: منهج البحث وخطته

وسعياً لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها، تم توظيف المنهج الوصفي التحليلي المقارن،حيث سيتم تحليل النصوص القانون التي عالجت جريمة الدخول غير المشروع لنظام معلوماتي وفق دراسة مقارنة بين القوانين الأردنية والكويتية، وقد تم تقسيم البحث على النحو التالي:

المطلب الأول: مفهوم جريمة الدخول غير المشروع لنظام معلوماتي.

الفرع الأول: تعريف جريمة الدخول غير المشروع لنظام معلوماتي

الفرع الثاني: محل الحماية الجزائية للجريمة.

المطلب الثاني: أركان جريمة الدخول غير المشروع.

الفرع الأول: الركن المادي لجريمة الدخول غير المشروع الى نظام معلوماتي

الفرع الثاني الركن المعنوي جريمة الدخول غير المشروع الى نظام معلوماتي

المطلب الأول: مفهوم جريمة الدخول غير المشروع

العالم المعلوماتي الجديد أصبح محلاً مستهدفاً من قبل المجرمين الذين يستهدفونه لدوافعهم المتعددة، على أثرها عملت الدول على تجريم الأفعال التي تشكل اعتداءً عليه والتي بنتيجتها يتأثر عمل المؤسسات والأفراد في المجتمع، فجريمة الدخول غير المشروع لنظام معلوماتي تتعلق تعلقاً مباشر بالوصول والاطلاع على نظام معلوماتي تابع للدولة أو لجهة حكومية أو رسمية أو غير رسمية دون صلاحية أو إذن، حيث أن الأصل العام أن الموظف العام أو المختص ذو الصلاحية منفرداً في الاطلاع على هذه المعلومات.

وعليه سنقوم بالتطرق الى مفهوم جريمة الدخول غير المشروع الى النظام المعلوماتي ، وبيان أهمية تجريم الفعل في هذا المطلب.

الفرع الأول: تعريف جريمة الدخول غير المشروع

لابد في بداية المطاف بيان مفهوم وتعريف جريمة الدخول غير المشروع، حيث أن هذه الجريمة تعد من الجرائم المستحدثة الإلكترونية التي تم تقنينها من خلال استحداث قوانين تعنى بالعالم المعلوماتي من خلال تسليط الضوء على موقف الفقهاء في تعريف جريمة الدخول غير المشروع، موقف المعاهدات والاتفاقيات الدولية من تعريف هذه الجريمة، وموقف القوانين المعنية.

تعد جريمة الدخول غير المشروع للنظام المعلوماتي من أهم الجرائم وأخطرها، اذ تمثل التسلل الى أنظمة المعلومات وما تحتوي من قاعدة بيانات والاطلاع على معلومات حساسة، سرية أو خاصة بالأفراد موجودة في البنية التحتية المعلوماتية للمؤسسات أو الجهات الحكومية، فينطوي على هذا الفعل المجرم، تهديداً لسلامة وسرية النظام المعلوماتي ، واعتداءً على المرفق المعلوماتي، كما يمكن أن تكون هذه الجريمة الخطوة الأولى للجاني لإقدامه على جريمة أخرى، كالعبث أو التعديل أو إتلاف البيانات الموجودة في النظام المعلوماتي، مما يؤثر سلبياً على سير عمل المرفق المعلوماتي وعلى المعطيات التي تنتج عن هذا النظام.

وأطلق عليها البعض بمسمى "الاختراق"، وهي عبارة عن اقتحام للأنظمة الخاصة بالأفراد أو المؤسسات خاصة كانت أم حكومية من خلال اللجوء الى البرامج المختصة في فك وسرقة كلمة السر وتصريح الدخول بقصد الاطلاع على المعلومات أو تخزينها أو سرقتها، حيث وإن تعددت المسميات فهي تشكل وجهان لعملة واحدة، وهي وحدة الفعل والنتيجة الجرمية.

وتتجلى أهمية الحماية وتجريم الدخول غير المشروع هي المحافظة على سرية المعلومات التي يحتويها النظام المعلوماتي، حيث أن البيانات بعد أن يتم تحويلها ومعالجتها تُترجم الى معلومات خاصة تتعلق بالأفراد، ولابد أن يتم حمايتها جزائياً من أي اعتداء وبغض النظر عن مدى جسامته، حيث أن البيانات والمعلومات أصبحت مكوناً في الشق المعنوي لجهاز الحاسوب والتي من خلاله تُباشر المؤسسات والشركات عملها فيما يتعلق بحياة الأفراد، نظراً لما يتمتع مع ميزة استيعاب الكم الهائل من المعلومات والوظائف المتعددة من تعديل ومعالجة من خلال جهاز الحاسوب، حيث وإن كنا سنعبر عنه فإن أجدر التعبيرات هي أنه يمثل مستودع رقمي لمعلومات الأفراد في العالم المعلوماتي.

وفي تعريف الجريمة، لابد لنا من أن نتطرق في البداية الى آراء الفقهاء القانونيين في تحديد مفهوم الجريمة، حيث عُرفت الجريمة على أنها الدخول الى النظام المعلوماتي من قبل فرد غير مختص ولا يملك صلاحية الدخول، ويستغل الفرصة للاطلاع على ملفات ومعلومات سرية دون وجه حق، وفي تعريف آخر هو عبارة عن النشاط الذي يقدم عليه الجاني بغرض الولوج الى النظام المعلوماتي كاملاً أو جزء منه دون وجود تصريح أو استيفاء شرط للدخول.

لابد لنا من أن نستعرض دور الجهود الدولية في مكافحة الجرائم الإلكترونية تحديداً جريمة الدخول غير المشروع للنظام المعلوماتي، كونها تعد جريمة لا تعرف الحدود، حيث عملت الاتفاقية العربية لمكافحة الجرائم المعلوماتية على تحديد مفهوم جريمة الدخول غير المشروع من خلال عرض معالم الجريمة في نص المادة السادسة (جريمة الدخول غير المشروع) في الفقرة الأولى والتي تنص على:" الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به."، وتجدر الإشارة الى الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست)، التي عالجت جريمة الدخول غير المشروع في المادة (2) تحت مسمى النفاذ غير المشروع، على أنها حددت أيضاً تعريف الجريمة ونصت على :" تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: النفاذ الكامل أو الجزئي إلى نظام كومبيوتر. يجوز لطرف أن يستلزم أن تُرتكب الجريمة عن طريق مخالفة التدابير الأمنية، بنِية الحصول على بيانات الكومبيوتر أو بأي نية غير صادقة أخرى، أو في ارتباط بنظام كومبيوتر متصل بنظام حاسوبي آخر."، وما نلاحظه من خلال التعريفات السابقة، أن الجهود الدولية ركزت على الولوج أو الاتصال بالنظام والنفاذ إليه بغض النظر عن صفة أو طبيعة هذا النظام، الأمر الذي يعول الى أنها تركت الدول لها حرية النصوص على العقوبة الملائمة وتحديد معالم الجريمة بدقة أكثر في التشريعات الوطنية الخاصة.

وبعد أن بينّا دور الجهود الدولية في مكافحة الجريمة، لابد أن نتطرق الى دور التشريعات الوطنية، حيث وبالرجوع الى قانون الجرائم الإلكترونية الأردنية، نجد أن المشرع الأردني لم ينص على تعريف لجريمة الدخول غير المشروع الى

النظام المعلوماتي وإنما بين المشرع أركان الجريمة، فقد نص المشرع الأردني على أنه:" أ- يعاقب كل من دخل أو وصل قصدا إلى الشبكة المعلوماتية أو نظام المعلومات أو وسيلة تقنية المعلومات أو أي جزء منها باي 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 (300) ثلاثمائة دينار ولا تزيد على (600) ستمائة دينار أو بكلتا هاتين العقوبتين".

وفي المقابل، اتخذ المشرّع الكويتي نهجاً مغايراً للتشريع الأردني؛ حيث عَمَدَ إلى وضع تعريف خاص بجريمة الدخول غير المشروع في المادة الأولى من القانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، إذ عرّفها بأنها" :**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.**'

أما على صعيد الجزاء الجنائي، فقد تمايزت السياسة العقابية بين التشريعين بحسب طبيعة الجرم المقترف؛ فبينما يعاقب المشرع الكويتي على النفاذ المجرد بعقوبات مخصصة لها في قانونه، نجد أن المشرع الأردني قد أفرد نصاً مشدداً في حال اقتران هذا الدخول بقصد تتبع البيانات الرسمية، وتحديداً من خلال نص المادة (3) من قانون الجرائم الإلكترونية الأردني والتي تقضي بـ" :**يُعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تتجاوز عشرة آلاف دينار، أو بإحدى هاتين العقوبتين، كل من: 1- ارتكب دخولاً غير مشروع إلى موقع أو نظام معلوماتي مباشرة أو عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية بحكم القانون**"

ومن خلال استعراض النصوص القانونية التي بين مفهوم الجريمة من خلال بيان وتحديد معالم أركانها، نجد أن المشرع الكويتي كان محموداً في النص على تعريف خاص لجريمة الدخول غير المشروع أو الاختراق، وذلك نظراً لطبيعة الجريمة المعلوماتية وطبيعة المحل التي تتطلب تحديد مفهومها كونها ذات طبيعة رقمية، وبتحديد مفهومها يمكن السلطات القضائية من تطبيق النص بعيداً عن اللبس والغموض في تفسير وتأويل النصوص العقابية، بالإضافة الى رسم حدود معالم الجريمة ضماناً لعدم إفلات الجاني من العقاب، وفي تقديرنا، وعلى الرغم من أن المشرع الأردني لم يتطرق الى التعريف الواضح للجريمة إلا أن الأمر يرجع الى الى تبني الأسلوب المرن في تطبيق النصوص القانونية، يعزى الأمر الى أن الجريمة تتعلق بالتطور التكنولوجي وبالتالي الجريمة تتطور بسرعة، ومن المتصور أن يصبح التعريف يطبق على الأفعال القديمة مقارنةً بالحديثة، إلا إننا نحبذ المشرع الأردني نظراً لحساسية وخصوصية محل

الجريمة أن يتطرق الى تعريف جريمة الدخول غير المشروع نظراً لطبيعة الجريمة التقنية ومنعاً من وقوع اللبس في تطبيق القانون أمام القضاء والمحاكم، حيث يكون القاضي أمام تطبيق واضح للنصوص القانونية من حيث المفهوم.

الفرع الثاني: محل الحماية الجزائية للجريمة

بادئ ذي بدء، لابد لنا من أن نتطرق ونلتفت إلى محل الحماية في هذه الجريمة، حيث وإن كان العالم الرقمي الذي يعبر فيه من خلال اللغة الخاصة في البرمجة والمعلوماتية، تماشياً مع موضوع هذا البحث، وفي ذات الوقت في بعض الحالات يحمل صفة استثنائية عن غيره حال كان يتبع لجهة حكومة أو مؤسسة رسمية، حيث تكمن أهمية البحث حول الصفة التي يحملها هذا النظام هي العقوبة المقررة في حال وقوع الجريمة وأثرها على المجتمع.

استجابةً للتطور المعلوماتي الرقمي، عملت الدول على تخزين معلومات الأفراد وفق المنظومة المعلوماتية توفيراً للوقت والجهد للدائرة أو المؤسسة الحكومية وللأفراد أيضاً، حيث أصبح الأفراد يستخرجون الوثائق والمستندات الإلكترونية التي تحمل معلوماتهم الشخصية من خلال الولوج الى موقع الإلكتروني الخاص بالمؤسسة، والذي من ناحية أخرى يحتفظ بهذه المعلومات والبيانات المتعلقة بهم، وعليه أصبح لكل مؤسسة مرجعية معلوماتية خاصة بها، تحمل معلومات الأفراد وتخزنها وتعالجها وفقاً للمطلوب والتي تُحتفظ في النظام المعلوماتي.

لابد لنا من وضع حجر الأساس في تعريف النظام المعلوماتي، فالنظام لغة عبارة عن الترتيب والاتساق، والعناصر المرتبطة وظيفياً، أما المعلومات فمفردها معلومة، وهي كلمة أصلها الاسم (مَعْلُومٌ) في صورة مفرد مذكر، وهو الأمر المعروف، جمعها معلومات، وهي الحقائق والأخبار التي تساعد على توضيح الأشياء.

أما من الناحية الجزائية، فقد عُرف النظام المعلوماتي على أنه "عبارة عن مجموعة من العناصر المتفاعلة معاً (المتساندة بنائياً والمتكاملة وظيفياً) لإنجاز هدف معين باستخدام الموارد بأنواعها، وهي مجموعة من العناصر والمكونات المترابطة معاً والتي تجمع الحقائق والبيانات وتعالجها وتخزنها وتقدم المعلومات المطلوبة والمناسبة والجيدة للاستفادة منها".

كما أنه عُرف على أنه النظام الذي يحتوي على مجموعة متناسقة ومتجانسة من الموارد يعمل على تجميع وتشغيل وإدارة البيانات بهدف توصيل وإنتاج معلومات مفيدة للمستخدمين من خلال شبكات القنوات، وعُرف على أنه "مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها التي تعمل على جمع البيانات والمعلومات، ومعالجتها وتخزينها وبثها وتوزيعها بغرض دعم صناعة القرارات والتنسيق وتأمين السيطرة على المنظمة، إضافةً الى تحليل المشكلات

وتأمين المنظور المطلوب للموضوعات المعقدة، ويشتمل نظام المعلومات على البيانات عن الأشخاص الأساسين والأماكن والنشاطات والأمور الأخرى التي تخص المنظمة والبيئة المحيطة بها".

ولا ننسى دور المعاهدات الدولية التي عنت بالتطرق الى تعريف النظام المعلوماتي في نطاق الجرائم الإلكترونية، كونها تعد جرائم مستحدثة وعابرة للقارات، حيث أن اتفاقية مجلس اوروبا المتعلقة بالجريمة الالكترونية/اتفاقية بودابست لسنة 2001 لم تتطرق بصورة مباشرة الى النصوص على مصطلح النظام المعلوماتي وإنما عرفت منظومة الكمبيوتر على أنها:" أي جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة، والتي يقوم واحد منها أو أكثر، وفقا لبرنامج، بالمعالجة الآلية للبيانات"، في حين ان الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 ذكرت وعرف النظام الملعوماتي على أنه: "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".

ولمواكبة القوانين للجرائم المستحدثة وتماشيها بصورة موازية والاتفاقيات الدولية، عرف المشرع الأردني انظمة المعلومات في قانون الجرائم الإلكترونية رقم (17) لسنة 2023 في المادة (2) على أنها:" مجموعة البرامج أو التطبيقات او منصات التواصل الاجتماعي أو الأجهزة أو الأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونيا، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية".

موقف المشرع الكويتي عرف النظام المعلوماتي بشكل وبصورة تفصيلية أكثر في قانون رقم (63) لسنة (2015) في شأن مكافحة جرائم تقنية المعلومات نص المادة (1)، حيث أنه في البداية تطرق الى تعريف النظام الإلكتروني المؤتمت وهو:" برنامج أو نظام الكتروني لحاسب آلي تم إعداده ليتصرف أو يستجيب لتصرف بشكل مستقل، كلياً أو جزئياً دون تدخل أو إشراف أي شخص طبيعي في الوقت الذي يتم فيه التصرف أو الاستجابة."، وبعدها في ذات المادة عرف نظام المعالجة الإلكترونية للبيانات على أنها:" نظام الكتروني لإنشاء أو إدخال أو استرجاع أو إرسال أو استلام أو استخراج أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونياً."، وبعدها عرف نظام الحاسب الآلي على أنه: " مجموعة برامج وأنظمة معلوماتية معدة لتحليل المعلومات والبيانات والأوامر وبرمجتها وإظهارها أو حفظها أو إرسالها أو استلامها، ويمكن أن تعمل بشكل مستقل أو بالاتصال مع أجهزة أو أنظمة معلوماتية أخرى.".

إن اتجاهات التشريعات في استخدامها ألفاظ تشريعية لبيان مدلول مكونات النظام المعلوماتي وفي موضوع البحث في محل الجريمة النظام المعلوماتي أمر في بالغ الأهمية لتحديده وفي تقدير الدراسة اتجاه تعريف المشرع الأردني والكويتي للنظام المعلوماتي، نلاحظ أن المشرع الاردني ارتكز على اساسين في تحديد تعريف النظام المعلوماتي، الركيزة الأولى الطابع التقني من حيث الأدوات التكنولوجية المحددة في كلا منهما، حيث تم ذكر البرامج، الأجهزة،

التطبيقات والمنصات، الركيزة الثانية الوسائل الإلكترونية المستخدمة في النظام من إنشاء وإرسال ومعالجة وعرض للبيانات.

أما موقف المشرع الكويتي في تعريفه للنظام المعلوماتي كان محموداً، حيث أنه ارتكز في تعريفه للنظام المعوماتي تبعاً لأنواعه، فنلاحظ أن المشرع الكويتي نظر وسّن في تعريفه للنظام المعلوماتي نظرة تقنية، حيث تطرق الى النظام المعلوماتي المؤتمت موضحاً أن هناك مجموعة من الأنظمة تعمل من تلقاء نفسها دون تدخل العنصر البشري تبعاً لبرمجيتها، وفي تعريفه لنظام المعالجة الإلكترونية للبيانات نلاحظ أنه وضع حجر الأساس القانوني في مفهوم النظام، حيث أن النظام الرقمي يتعامل مع البيانات إلكترونياً، كما أنه يغطي الدورة المعلوماتية للبيانات من حيث إنشائها الى معالجتها وتخزينها وإرسالها، وفي تعريف نظام الحاسب الآلي نلاحظ أن المشرع الكويتي بين قدرة النظام على العمل بشكل مستقل أو باتصاله مع خوادم أو أجهزة أخرى، كما أنه يشمل جميع أنواع الأنظمة سواء كانت الشخصية أم التابعة والمدارة من قبل مؤسسات أو شركات.

نتيجة لذلك، نلاحظ أن المشرع الكويتي في تعريفه القانوني للنظام المعلوماتي كان أدق من الناحية التفصيلية نظراً لطبيعة النظام المعلوماتي، حيث أن المشرع الكويتي راعى الجوانب الآلية والتقنية والوظيفية للنظام المعلوماتي والذي بناءً عليه يضبط جميع أنواع الجرائم التي تقع على النظام المعلوماتي وبالتالي صلاحية تطبيق القانون بصورة واضحة دون الحاجة الى تفسير أو تأويل، ونلاحظ أنه يعالج المفاهيم المعاصرة في العالم الرقمي وبالتالي يضع أساساً صلباً للقاضي للتعامل مع الجرائم المعاصرة للتطور الرقمي.

وعليه نحن نحبذ المشرع الأردني في تعديل تعريفه للنظام المعلوماتي ليتسع الى أنواع النظام وبصورة تتوافق مع طبيعة النظام المعلوماتي، حيث أن النظام المعلوماتي بالنتيجة هو عبارة عن محلاً رقمياً لجريمة، لابد من ان يتم تحديد تعريفه منعاً لوقوع القاضي في تطبيق النصوص القانونية في اللبس عند النظر في القضايا وتجسيداً للمسؤولية الجزائية عند تحديد وصف الجريمة في القرار، حيث على الرغم من أن القاضي بإمكانه الاستعانة بالخبير في الأمور المعلوماتية والتكنولوجية إلا أنه عند وجود نص واضح معرف لأركان الجريمة وتحديداً محل الحماية الجزائية فإن ذلك يتيح للقاضي السهولة في تطبيق القانون.

المطلب الثاني

أركان جريمة الدخول غير المشروع

بعد الوقوف على مفهوم جريمة الدخول غير المشروع لنظام المعلومات وتحديد محل الحماية الجزائية لها، تقتضي الدراسة المنهجية الانتقال إلى الخطوة التالية المتمثلة في بيان أركان الجريمة؛ إذ لا بد لقيامها من توافر مقوماتها

القانونية. وإذ تم استظهار الركن الشرعي لهذه الجريمة ضمنياً من خلال استعراض النصوص القانونية السابقة، فإن هذا المطلب سيتناول بالتفصيل والتحليل كلاً من الركن المادي والركن المعنوي المحدد لهذه الجريمة.

الفرع الأول: الركن المادي للجريمة

يعبر عن الركن المادي بشكل عام للجريمة عن ماديات الجريمة التي لها طبيعة مادية تلمسها الحواس، فلا جريمة دون ركن مادي لها، ونظراً للطبيعة المعلوماتية للجريمة فهي تتمثل بالنشاط الذي ينال الكيان المعنوي لجهاز الحاسوب، على سبيل المثال لا الحصر الاعتداء عليه تعطيلاً، أو اطلاعاً على معلومات أو بيانات من غير مخول، أو إضعاف برامجه والتأثير على أداء وظيفته، أو إتلاف أو العبث في المعلومات أو البيانات المخزنة فيه، أو الوصول إلى النظام المعلوماتي أو البرامج أو البيانات أو المعلومات، ولابد لنا من أن نبين النشاط الجرمي المكون من هذه الجريمة.

وفي نطاق موضوع الجريمة، تتألف هذه الجريمة من سلوك جرمي إيجابي يتمثل بالدخول الى النظام المعلوماتي من قبل فرد لا يملك صلاحية ذلك، وفي العالم المعلوماتي، يقصد به القيام بكافة الأعمال التي من شأنها الولوج الى النظام، وقد حاول الفقهاء بتحديد تعريف محدد للدخول كنشاط لجريمة الدخول غير المشروع من خلال اسباغها الى الوسيلة التقنية نظراً لطبيعتها، فقد عُرفت على أنه " إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول الى المعلومات والمعطيات المخزنة بداخله للاطلاع عليها أو لمجرد التسلية أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي.".

ومنهم من عرفها بأنها:" القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف.".

وما نلاحظه أن المشرع الأردني أخذ بعين الاعتبار الطبيعة التقنية للجريمة وبين في منطوق المادة (3) من قانون الجرائم الإلكترونية الأردني "كل من **دخل أو وصل**"، وبالمقارنة مع التشريع الكويتي في تعريفه لجريمة الدخول غير المصرح به في قانون استخدم مصطلح "**النفاذ المتعمد**"، حيث أن كلا التشريعين راعى الطبيعة الرقمية للجريمة، إلا أن التساؤل الذي يثور في هذا المقام هو هل يوجد فرق في الأفعال؟

ما هو بين وصريح أن المقصود بالدخول أو الوصول أو النفاذ كأفعال في الركن المادي للجريمة بالصورة والشكل المعنوي لها، أي أنها لا تنسحب الى الدخول الفعلي المادي للشخص، كدخول الشخص الى مكان ما بالمعنى المادي، وإنما دخوله من خلال الوسائط المعلوماتية والإلكترونية الى النظام، ولابد أن يسيطر الجاني على النظام المعلوماتي محل الجريمة، أي أن يمتلك القدرة على أن يقوم بعملية الولوج للنظام المعلوماتي، ونحن نقصد بالولوج دون تصريح،

أي أن الجاني يعلم أنه لا يملك التفويض أو الصلاحية بالدخول الى النظام المعلوماتي، وعليه فإن دخوله أو ولوجه دون وجه حق وغير مشروعاً، حيث أن صاحب النظام المعلوماتي ومن يملك صلاحية السيطرة عليه وحيازته حدد الأشخاص أو الموظفين الذين يملكون صلاحية الدخول الى النظام والاطلاع عليه أو حتى إدخال معلومات أو بيانات أو تعديلها أو حذفها.

تأسيساً على ما تقدم الجاني يعلم انه لا يملك صلاحية الدخول الى النظام وعلى الرغم من ذلك أقدم على ارتكاب الأفعال المادية التي من شأنها تحقق النتيجة الجريمة وهي الدخول أو الوصول أو النفاذ الى النظام المعلوماتي، مؤدى ذلك أن هذه الجريمة تعد من الجرائم الشكلية التي لا يشترط وقوع ضرر أو نتيجة معينة لتحققها، فهي تتحقق وتقوم بمجرد دخول الجاني الى النظام المعلوماتي.

ونحن نلاحظ أن كلا المشرعين استخدما مصطلحات التي تعبر عن ولوج الجاني الى النظام المعلوماتي، نلاحظ أن المشرع الأردني في متن المادة أن جريمة الدخول غير المشروع تعتمد على الدخول أو الوصول (دَخَلَ أو وَصَلَ) كنشاط جرمي للجريمة مؤسساً أركان الجريمة على اعتبار أنها جريمة معلوماتية تتطلب قيام الجاني بارتكاب فعل إيجابي، فالدخول المقصود به هو اختراق النظام أو الولوج له دون تصريح، ولا بد لنا من أن نميز بين المصطلحات المستخدمة لغاية استظهار السلوك الجرمي في هذه الجريمة، فالدخول عبارة عن الأفعال التي يقدم على ارتكابها الجاني والتي من خلالها يتم الولوج الى النظام المعلوماتي والإحاطة به، وبالتالي وبقراءة مدلول فعل "الدخول" نلاحظ أنه لا يُشترط أن يتم الاستقصاء أو الحصول على المعلومات أو البيانات الموجودة في النظام المعلوماتي، أي بمجرد قيام الجاني باختراق أنظمة الأمن والحماية الموجودة للأنظمة المعلوماتية يكون قد حقق فعل الدخول كالسلوك الجرمي، فالدخول هو المرحلة التي يتم استخدام اسم المستخدم وكلمة المرور كقفل للحساب وحال صحتهما يدخل الى النظام، فقد عرفها بعض الفقهاء تعريفاً واسعاً على أساس أنها عبارة عن تفاعل ناجح مع الكمبيوتر ليساير كافة التطورات التي تطرأ على التكنولوجيا.

ظهرت بعض الآراء الفقهية حول طبيعة مدلول فعل الدخول للنظام المعلوماتي، إن كان يستوجب التجريم بمجرد دخول الجاني الى النظام المعلوماتي، أم لابد أن يلحق الدخول نشاط ليُستفاد من الدخول الى النظام المعلوماتي.

في حقيقة الأمر كان هناك رأي من الفقهاء أيدوا أن مجرد دخول الجاني الى النظام المعلوماتي دون أن يُلحق بنشاط آخر يجرم وينطبق عليه جريمة الدخول غير المشروع الى النظام المعلوماتي كونه فعل في حد ذاته يعبر عن النية الجرمية للفرد بدخوله الى نظام هو غير مخول ولا يملك صلاحية الدخول إليه بالأساس، وفي حال أقدم على نشاط آخر بقصد العبث في مكونات النظام فيتم تطبيق مواد ونصوص القانون الخاصة بذلك، إلا أن رأي آخر من الفقهاء قضى بأنه لا يمكن تجريم الفرد فقط بمجرد الدخول الى النظام أي بمجرد اقترابه من أي جهاز آلي ودخوله

الى نظام معلوماتي دون تصريح وذلك لتوسع استخدام المدلول وتطبيق نصوص التجريم في هذه الواقعة، على أنه لابد أن يلحق فعل الدخول نشاط إيجابي آخر للجاني من شأنه التأثير سلباً وعبثاً بالنظام المعلوماتي.

وفي رأينا في موقف الفقهاء، أجد أن مجرد دخول الجاني الى النظام المعلوماتي دون حصول أي ضرر أو عبث فيه يعد جرماً يستوجب العقاب، حيث أن الجاني في هذه الحالة اتجهت إرادته الدخول الى النظام المعلوماتي وهو عالماً بأنه غير مخول ومصرح بالدخول اليه، كما أنه بمجرد دخوله، تمكن من الاطلاع على معلومات من شأنها أن تكون معلومات سرية وحساسة.

وفي مدلول فعل "الوصول" نستنتج أن الجاني استطاع أن يستطلع ويستعلم عما يحتويه النظام من بيانات أو معلومات من خلال ولوجه ودخوله الى النظام المعلوماتي، وبالتالي ما يمكن استنتاجه أن الوصول يشمل الدخول كنشاط جرمي.

أما النفاذ غير المشروع فهي لا تختلف في مفهومها عن الدخول والوصول، فهي تعبر عن قيام الجاني بالدخول الى موقع أو نظام معلوماتي من خلال اختراقه أو بتجاوز التصريح، فهو يستوعب الدخول الى النظام المعلوماتي والوصول الى أنظمة البيانات والمعلومات المحفوظة في النظام.

وعليه، الجاني في هذه الحالة يقوم من خلال اختراق مواقع النظام المعلوماتي الدخول اليه، وبمجرد دخوله تتحقق هذه الجريمة، أما في حال كان الشخص يتمتع بتخويل أو تصريح للدخول الى النظام المعلوماتي لا يعد فعلاً مجرماً طالما كان في حدود التصريح، وفي حال تجاوز هذا الشخص التصريح فإن الجريمة تتحقق.

والسؤال الذي يُدار في ذهننا هو هل يجب أن تتمع هذه الأنظمة المعلوماتي بأنظمة حماية من الاختراق، حيث أن الجاني في هذه الجريمة يلجئ الى عدة برامج واستخدام فيروسات حاسوبية من شأنها اختراق هذه الأنظمة لغاية الدخول اليها بالأساس، فإذا كانت هذه الأنظمة المعلوماتية لا تتمتع بأنظمة حماية، أو كان نظام الحماية غير قوي وفعال، هل تتحقق هذه الجريمة؟

الأصل أن الدخول غير المشروع يتحقق متى كان مخالفاً لإرادة صاحب النظام المعلوماتي أو من يقوم بإدارته، حيث أنه يقوم بوضع حدود وقيود من شأنها حماية النظام المعلوماتي من الإختراق واطلاع الجمهور على ما يحتويه النظام من بيانات ومعلومات حيث تفترض هذه الواقعة عدم صلاحية جميع الجمهور الدخول والاطلاع على ما يحتويه النظام المعلوماتي، وهذه الحماية التي يقوم مالك النظام بوضعها تعبر بصورة صريحة على عدم صلاحية الأشخاص أو الأفراد العاديين الدخول الى النظام إلا بوجود تصريح، فقد يتمثل إما باستخدام بصمة الفرد أو باستخدام كلمة سر أو بوضع نظام حماية خاص للنظام المعلوماتي، فعدم المشروعية مستمدة من عدم صلاحية الشخص بالدخول الى

النظام في هذه الحالة، حيث يقوم الجاني من خلال استخدام الفيروسات والوسائط المعلوماتية بالدخول الى النظام المعلوماتي دون تصريح.

أما في حال عدم وجود نظام حماية وتصريح، ومن خلال استقراء موقف المشرع الأردني والكويتي في نصوص مواد التجريم نلاحظ أن كلاهما اشترطا في متن المواد ارتكاب الجاني لفعل الدخول دون تفويض أو تصريح أو بتجاوزهما، مؤدى ذلك أنه في حال عدم اشتراط صاحب النظام وجود كلمة سر أو بصمة أو أي من الإدخالات أو الأفعال التي تبين صلاحية الشخص الدخول الى النظام يعد ضمناً أن النظام متاحاً للجمهور، وعليه فإنه يعبر ضمناً صاحب النظام بأن لأي فرد صلاحية وحق الدخول الى النظام المعلوماتي والاطلاع عليه.

والسؤال الذي يثار هنا هو إن لم يشترط صاحب النظام وجود تصريح معين للدخول إليه، إلا أنه قد يقوم بوضع أنظمة حماية تقوم مقام التصريح والتفويض، لا تسمح للجمهور الدخول الى النظام المعلوماتي، فهل في هذه الحالة قيام الجاني باختراق أنظمة الحماية والدخول الى النظام تحقق جريمة الدخول غير المشروع؟

في حقيقة الأمر، نص المشرع الكويتي على ذلك بصورة صريحة في متن المادة من خلال تقنين فعل اختراق وسائل وإجراءات الحماية الخاصة بالنظام، على عكس المشرع الأردني الذي لم يشترط وجود نظام حماية تقني مخترق، وإنما نص على عبارة "بأي وسيلة"، مؤداه شمول أي فعل يسمح للجاني بالدخول إلى النظام المعلوماتي (سواء تم عبر اختراق حماية أو استغلال جهاز مفتوح دون تصريح). وتأسيساً على ذلك، يُحبذ موقف المشرع الأردني نظراً للمرونة التشريعية التي تميزه؛ إذ من الصعب حصر السلوك الجرمي والوسائل التقنية المتطورة في الجرائم الإلكترونية، مما يدعو إلى التوصية بضرورة تعديل نص المشرع الكويتي ليتسع لجميع الأفعال والوسائط دون قصرها على اختراق التدابير الأمنية، توسيعاً لدائرة الحماية الجزائية ومنعاً لإفلات الجاني من العقاب".

الفرع الثاني: الركن المعنوي جريمة الدخول غير المشروع الى نظام معلوماتي

يتمثل الركن المعنوي بالأصول النفسية لدى الجاني والسيطرة عليها وترجمتها الى الواقع المادي الملموس الذي تدركه الحواس بإظهار النتيجة الجرمية، فالركن المعنوي يتمثل بعنصرين العلم والإرادة، فالعلم هو أن يكون الجاني على علم بأنه يقدم على ارتكاب جريمة وأن تتجه إرادته الى تحقيقها، ويعبر عنها بالقصد العام للجريمة، أما القصد الخاص فهو الذي يتطلبه المشرع في بعض الجرائم حال كانت الإرادة الآثمة صادرة عن دافع معين.

كما أن الجرائم في الركن المعنوي تتخذ صورة الخطأ، أي الجرائم غير المقصودة، وهي الاستثناء عن الأصل العام بأن تكون الجرائم مقصودة، ويقع الخطأ في خمول الإرادة عن توقع النتيجة أو إمكانية توقعها.

وتأسيساً على ما تقدم سنتطرق الى موقف المشرع الأردني والكويتي في القصد الجرمي في جريمة الدخول غير المشروع للنظام المعلوماتي وبيان إن كان يستوعب النص الخطأ في هذه الجريمة.

بين المشرع الأردني موقفه في القصد العام اتجاه جريمة الدخول غير المشروع للنظام المعلوماتي في بداية المادة (3)، حيث نص المشرع : (عاقب كل من دخل أو وصل **قصدا** إلى ..)، وأما عن موقف المشرع الكويتي فقد أشار في تعريفه الى الجريمة في بداية نص المادة (1) على أنها (النفاذ **المتعمد** غير المشروع...).

من خلال مدلول كلتا المادتين، تُعدّ جريمة الدخول غير المشروع من الجرائم المقصودة؛ حيث تطلّب المشرع تحقق القصد الجرمي بعنصريه: العلم والإرادة. أي علم الجاني بأن فعل الدخول يشكل سلوكاً جرمياً، وأن يحيط بكافة الوقائع التي يترتب عليها قيام الجريمة، وأن تتجه إرادته إلى تحقيق فعل الدخول، أي الولوج إلى النظام المعلوماتي كنتيجة جرمية. وعليه، في حال أثبت المتهم أن دخوله إلى النظام المعلوماتي كان على سبيل الخطأ، بحيث لم يعلم بأن فعله يشكل تعدياً، أو أن إرادته لم تتجه لإتيانها، انتفى القصد الجرمي وبالتالي انتفت الجريمة بحقه؛ تطبيقاً للقواعد العامة في القصد الجنائي التي تقضي بأن الغلط في الوقائع أمر جوهري ينفي القصد الجنائي. والأصل أن الفرد لا يُعاقب على الخطأ إلا في الجرائم غير المقصودة التي ينص عليها القانون حصراً، وهي استثناءات لا يجوز التوسع في تفسيرها أو القياس عليها.

أما عن موقف المشرعين عن القصد الخاص، فكما أشرنا سابقاً أن القصد الخاص مصدرها دافع معين، فلابد لنا من أن نفرق بين الدافع أو الباعث والقصد الجرمي، فالباعث يمثل القوة المحركة للإرادة أو الدافع النفسي لاشباع حاجة معينة، كالانتقام أو المحبة أو البغضاء وغيرها ذلك، وهي تختلف من جريمة لأخرى، فهي القوة النفسية التي تدفع الارادة لارتكاب الجريمة، وكقاعدة عامة، أن الباعث ليس له أثر قانوني في تحقق القصد الجنائي إلا في الأحوال التي ينص عليها المشرع.

نلاحظ أن موقف المشرع الأردني في جريمة الدخول غير المشروع قد شدد من العقوبة حال كان الهدف أو الغاية التي قصدها من دخوله إما لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو نشر أو إعادة نشر أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو خسارة سريتها أو تشفير أو إيقاف أو تعطيل، حيث نصت المادة (3/ب): " إذا كان الدخول أو الوصول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو نشر أو إعادة نشر أو إتلاف أو حجب أو تعديل أو تغيير أو نقل أو نسخ بيانات أو معلومات أو خسارة سريتها أو تشفير أو إيقاف أو تعطيل عمل الشبكة المعلوماتية أو نظام معلومات أو تقنية معلومات أو أي جزء منها فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة وبغرامة لا تقل عن (600) ستمائة

دينار ولا تزيد على (3000) ثلاثة آلاف دينار، وتكون العقوبة الحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وغرامة لا تقل عن(3000) ثلاثة آلاف دينار ولا تزيد على (15000) خمسة عشر ألف دينار إذا تمكن من تحقيق النتيجة".

كما أن المشرع الكويتي نص في المادة (2): "فإذا ترتب على هذا الدخول إلغاء أو حذف أو إتلاف أو تدمير أو إفشاء أو تغيير أو إعادة نشر بيانات أو معلومات ، فتكون العقوبة الحبس مدة لا تجاوز سنتين والغرامة التي لا تقل عن ألفي دينار ولا تجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبتين".

نلاحظ أن كلا المشرعين قد شددا العقوبة حال كان الدخول غير المشروع متى تحقق لدى الفاعل قصداً خاصاً يتمثل في نية ارتكاب جريمة أخرى لاحقة على جريمة الدخول غير المشروع.

نلاحظ النهج الذي سار عليه المشرع الأردني والكويتي في القصد الجنائي الخاص في هذه الجريمة وهي عدم ربطها بشكل أساسي مع القصد العام، أي أن الجريمة تتحق بمجرد دخول الشخص قصداً الى النظام المعلوماتي بصورة غير مشروعة، وفي حال تحقق القصد الخاص من خلال قيام الجاني بارتكاب أفعال جرمية أخرى كإتلاف البيانات أو إلغائها أو حذفها أو إفشاء الأسرار هذا من شأنه تشدد العقوبة، فالقصد الخاص هو ليس عنصراً ملازماً لقيام وتحقق جريمة الدخول غير المشروع في النظام المعلوماتي.

النتائج:

1- نلاحظ أن المشرع الكويتي عمل على وضع تعريف قانوني لجريمة الدخول غير المشروع في النظام المعلوماتي، الأمر الذي من شأنه يحقق وضوحاً تشريعياً أكبر ويساعد في حسن تطبيق النصوص القانونية.

2- المشرع الكويتي كان أكثر تفصيلاً ودقة في تعريف النظام المعلوماتي مقارنة بالمشرع الأردني الذي جاء تعريفه عاماً، الأمر الذي من شأنه يزيل اللبس والغموض في تحديد محل الحماية الجنائية.

3- راعت التشريعات العربية الرقمية والتقنية لجريمة الدخول غير المشروع من خلال تطبيق مصطلحات تقنية المعلومات في السلوك الجرمي مثل (الدخول، الوصول، النفاذ) وجعلها تتلاءم وطبيعة الجرائم المعلوماتية المستحدثة.

4- جريمة الدخول غير المشروع هي جريمة مقصودة يشترط فيها القصد الجنائي العام بعنصريه العلم والإرادة، ولا تقوم في حال كان الدخول قد تم بطريق الخطأ أو دون علم الجاني بعدم مشروعيته.

5- كلا المشرعين شددا العقوبة في حال اقترن القصد العام في جريمة الدخول غير المشروع بقصد خاص يتمثل في إتلاف البيانات أو تعديلها أو إفشائها أو العبث بها، وتكمن علة ذلك بما يعكس خطورة الجريمة وآثارها على أمن المعلومات.

التوصيات:

1- يحبذ البحث المشرع الأردني السير على هدي المشرع الكويتي بالنص صراحةً على تعريف قانوني لجريمة الدخول غير المشروع للنظام المعلوماتي لما في ذلك من دور في إزالة الغموض وضمان التطبيق السليم للنصوص القانونية.

2- توصي الدراسة بضرورة إعادة النظر في تعريف النظام المعلوماتي في التشريع الأردني ليشمل مختلف أنواعه وصوره التقنية الحديثة، بما يوائم مع التطور السريع في مجال تكنولوجيا المعلومات.

3- توصي هذه الدراسة المشرع الكويتي بالسير على هدي المشرع الأردني في قانون الجرائم الإلكترونية لعام 2023، وذلك من خلال توسيع الأساليب والوسائل التي يتحقق بها الدخول غير المشروع، وعدم رهن قيام الجريمة باختراق وسائل وإجراءات الحماية الفنية؛ تماشياً مع الطبيعة المتطورة والمتجددة لهذه الطائفة من الجرائم، وضماناً لشمول الحماية الجزائية للأنظمة كافة.

4- يوصي هذا العمل بضرورة تدريب الموظفين على قواعد أمن المعلومات، ورفع مستوى الوعي القانوني لديهم بحدود الصلاحيات الممنوحة لهم، للحد من الجرائم المرتبطة بتجاوز التفويض الوظيفي.

5- يوصي البحث بضرورة تحديث التشريعات الجزائية لمواكبة التطورات التقنية المستمرة وذلك من خلال عدم حصر الأفعال الجرمية بوسائل تقنية محددة قد تصبح متجاوزة مع مرور الزمن أو متطورة.

المراجع والمصادر:

- إبراهيم، خالد ممدوح .(2010) .*أمن الجريمة الإلكترونية* .الدار الجامعية.
- إبراهيم، مدحت محمد عبد العزيز .(2015) .*الجرائم المعلوماتية الواقعة على النظام المعلوماتي* .دار النهضة العربية.
- أبو النصر، مدحت محمد محمود. (1998). المعلومات: المفهوم والنظم والتدريب .*مجلة الإدارة*، 31(2)، 77-92. http://search.mandumah.com/Record/158300 .
- الجبور، محمد عودة .(2012) .*الوسيط في القانون العام – القسم العام* .دار وائل للطباعة والنشر.
- الحمادي، خالد .(2019) .*جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة* [رسالة ماجستير غير منشورة]. كلية القانون، جامعة قطر.

- حسني، أحمد حسني، وربيع، أحمد .(1998) .*نظم المعلومات المحاسبية: الإطار الفكري والنظم التطبيقية* . مكتبة الإشعاع الفنية.
- الخوالدة، محمد سليمان، وهياجنة، أحمد موسى محمد .(2012) .*جريمة الدخول غير المشروع إلى موقع إلكتروني أو نظام معلومات وفق التشريع الأردني: دراسة مقارنة*[رسالة ماجستير غير منشورة]. الجامعة الأردنية.
- الزوي، ما شاء الله عثمان. (2023). المسؤولية الجنائية للدخول أو البقاء غير المشروع في النظام المعلوماتي: دراسة في القانون الليبي المقارن .*المجلة العربية للدراسات الأمنية*، 39(1)، 45–60.
- عبد العزيز، رامي .(2005) .*الفيروسات وبرامج التجسس* .دار البراءة.
- القحطاني، منصور بن سعيد .(2008) .*مهددات الأمن المعلوماتي وسبل مواجهتها: دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض* .مركز البحوث والدراسات.
- قورة، نائلة عادل .(2005) .*جرائم الحاسب الآلي الاقتصادية: دراسة نظرية وتطبيقية* (ط. 1). منشورات الحلبي الحقوقية.
- المجالي، نظام .(2025) .*شرح قانون العقوبات: القسم العام* .دار الثقافة للنشر والتوزيع.
- معجم المعاني الجامع. (د. ت.) .*مادة (علم)* .موقع معجم المعاني الإلكتروني.
- مناصير، حسن فضيل خلف .(2016) .*جريمة الدخول غير المشروع إلى النظام المعلوماتي والتعدي على محتوياته: دراسة مقارنة*[رسالة ماجستير غير منشورة]. جامعة جرش.
- نصر، شريف. (2020). الجوانب الموضوعية لجرائم الدخول غير المشروع إلى الأنظمة المعلوماتية .*مجلة كلية الشريعة والقانون بجامعة طنطا*، (2)، 115–140.
- النوايسة، عبد الإله .(2017) .*جرائم تكنولوجيا المعلومات: شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية* (ط. 1). دار وائل للنشر والتوزيع.
- الهيتي، محمد حماد المهرج .(2006) .*جرائم الحاسوب* (ط. 1). دار المناهج للنشر والتوزيع.
- الهيتي، محمد حماد المهرج .(2016) .*بحوث جنائية متخصصة في الاعتداءات التي يتعرض لها الحاسب الآلي* (ط. 1). دار السنهوري.

ثانياً: الاتفاقيات الدولية والتشريعات:

- الأمانة العامة لمجلس وزراء الداخلية العرب .(2010) .*الاتفاقية العربية لمكافحة جرائم تقنية المعلومات*.
- مجلس أوروبا .(2001) .*الاتفاقية المتعلقة بالجريمة الإلكترونية (اتفاقية بودابست)*.
- *قانون الجرائم الإلكترونية الأردني رقم (17) لسنة 2023* .الجريدة الرسمية، الأردن.
- *قانون مكافحة جرائم تقنية المعلومات الكويتي رقم (63) لسنة 2015* .الكويت.