The Legal Nature of the Crime of Electronic Hacking That Harms State Security a Comparative Study

Fatma Yaqub Yousif Alramsi
ALRamsi2@hotmail.com

Mohammed Shalal Al-Ani
dr_alani@sharjah.ac.ae

Accepted Date: 19/1/2025. **Publication Date: 1/4/2026.**

Abstract

Cyber-penetration is one of the most serious digital crimes threatening the stability and integrity of States' systems. For the purpose of espionage, sabotage or disruption of critical infrastructure, the research will show what the internal and external security of States is.

As for its legal nature, the cybercrime has two different natures, one of which is the material aspect, which is when the information is stored on an electronic supporter, and the latter is the moral aspect, which is when the information is in a state of transfer or is present in the memory of the information system. In order to clarify the concept of breach of diamonds by the security of States, and also for this crime to materialize, its main pillars must be found s intention to harm the security of the State.

Keywords: Cyber Espionage, Cybercrime, Information Security, Hack, Digital Crime, State security.

الطبيعة القانونية لجريمة الاختراق الإلكتروني الماس بأمن الدولة في القانون الإماراتي دراسة مقارنة

فاطمة يعقوب يوسف [*] ALRamsi2@hotmail.com

محمد شلال العاني [**] dr_alani@sharjah.ac.ae

تاريخ القبول: 2025/1/19. **تاريخ النشر: 2026/4/1.**

المستخلص

تعد جريمة الاختراق الإلكتروني الماسة بأمن الدولة من أخطر الجرائم الرقمية التي تهدد استقرار الدول وسلامة أنظمتها، بغرض التجسس أو التخريب أو تعطيل البنية التحتية الحيوية، لذا ينبغي علينا بيان ماهية أمن الدول الداخلي والخارجي، من أجل توضيح مفهوم الاختراق الماس بأمن الدول، أما بالنسبة لطبيعتها القانونية، فأن الجريمة الإلكترونية ذات طبيعتين مختلفتين أحداهما يتمثل في الجانب المادي والذي يتمثل في أن تكون المعلومات مخزنة على داعمة إلكترونية والأخير يتمثل في الجانب المعنوي وذلك عندما تكون المعلومات في حالة انتقال أو موجودة في ذاكرة النظام المعلوماتي، ومن أجل تتحقق هذه الجريمة لابد من توافر أركانها الرئيسية، وهي التي تتمثل في الركن المادي الذي يتمثل في الأفعال التي تؤدي للاختراق، والركن المعنوي الذي يتطلب نية الجاني للإضرار بأمن الدولة.

الكلمات المفتاحية: التجسس الإلكتروني، الجريمة السيبرانية، الأمن المعلوماتي، الاختراق، الجرائم الرقمية، أمن الدولة.

[*] طالب ماجستير
[**] أستاذ دكتور

المقدمة

Introduction

شهد العالم اليوم تطور كبير في المجالات التقنية الحديثة، وأصبحت الإنسانية تعيش في عصر الثورة المعلوماتية، التي أضحت تتقدم بشكل مستمر دون توقف، ولم يعد هناك أي مجال اجتماعي أو اقتصادي او ثقافي أو صناعي أو إداري إلا وتستخدم فيه التقنيات المعلوماتية، والتي تقوم بدور رئيسي في حفظ المعلومات ومعالجتها بسرعة هائلة.

وفي ظل هذا التطور المتسارع في استخدام تقنيات المعلومات والتحولات التكنولوجية المتعاظمة، وتزايد أعداد مستخدمي شبكة الإنترنت، ومواقع التواصل الاجتماعي، نشأت أنواع جديدة من الجرائم ما كانت ترتكب لولا وجود هذه الشبكة الإلكترونية، وهي التي تمثلت بالجرائم المعلوماتية بشكل عام وجريمة التجسس الإلكتروني بشكل خاص، وتزداد خطورة هذه الجرائم متى كان هذا الاختراق يمس بأمن الدولة الداخلي أو الخارجي، وعليه سنتناول في دراستنا الطبيعة القانونية لجريمة الاختراق الإلكتروني الماس بأمن الدولة في القانون الإماراتي ومقارنتها بالقوانين الأخرى وذلك على النحو التالي:

أولاً: التعريف بموضوع البحث

First: Defining the Research Topic

أن **اختراق الأنظمة الإلكترونية، جريمة خطيرة كما بينا، يمكن أن تلحق أضرار جسيمة وخطيرة بالدولة ومؤسساتها المهمة،** حيث يستطيع المخترق من خلالها الوصول بشكل غير قانوني إلى البيانات والمعلومات الحساسة، التى لا يمكن الوصول إليها والاطلاع عليها، ومن ثم استغلالها لأغراض غير مشروعة، مثل التنصت أو التخزين أو تغيير المحتوى او التخريب أو الحذف، مما يفضي ذلك إلى حصول خسائر كبيرة، مثل تدمير النظام أو سرقة الهوية أو انتحال الشخصية. وجميع هذه الأفعال يمكن أن تضر بمصالح الدول وأمنها وسلامتها[1].

ثانياً: أهمية البحث

- Second: The Importance of Research

تبرز أهمية هذه الدراسة في حداثة جريمة الاختراق الإلكتروني، وهي جريمة تهدد أمن الدول وسلامتها، وتتضح هذه الأهمية في النواحي الآتية :

أ- من الناحية العلمية:

تبرز الدراسة من الناحية العملية، مدى كفاية التشريع الوطني والتشريعات المقارنة في مواجهة جريمة الاختراق الالكتروني أو الحد منها وردع مرتكبيها.

ب- من الناحية العملية:

تحرص هذه الدراسة على رسم صورة شاملة لجريمة الاختراق الإلكتروني، وتسلط الضوء على الجهود التي بذلها المشرع الإماراتي والتشريعات المقارنة مثل التشريع المصري والأردني والسعودي إضافة إلى ذلك التشريع الإنجليزي، وتقدم خيارات ممكنة للتصدي لهذه الجريمة.

ثالثاً: إشكالية البحث

Third: The Research Problem

تتجلى مشكلة الدراسة في كون جريمة الاختراق الإلكتروني في دولة الإمارات العربية المتحدة، من الجرائم الجديدة والمستحدثة، حيث تستهدف هذه الجريمة البيانات أو المعلومات السرية المتعلقة بالدولة. ويعد الاختراق الإلكتروني من القضايا الحساسة والمعقدة والحديثة في نفس الوقت، مما يثير العديد من التحديات القانونية والقضائية، فعلى الصعيد القانوني، نحن مقيدون بمبدأ الشرعية الجزائية، الذي ينص على أنه لا جريمة ولا عقوبة إلا بنص قانوني، حيث نجد ان المشرع الإماراتي اضاف لقانون العقوبات الاتحادي رقم (3) لسنة 1987 بموجب المرسوم بقانون الاتحادي رقم 7 لسنة 2016 الفصل الثاني مكررا وعنوانه بأحكام عامة بشأن الجرائم الماسة بالأمن الخارجي والداخلي للدولة، وتتناول هذه الاحكام الجديدة التي تسري على جميع الجرائم الماسة بأمن الدولة الخارجي والداخلي الواردة في قانون العقوبات والقوانين الأخرى، كما نص المشرع الإماراتي على تعريف جريمة الاختراق في المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية وهي التي صاغها المادة (1) من خلال تعريف مفهوم الاختراق بأنه: (... الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة، أو البقاء بصورة غير مشروعة...)[2].

إلا أنه مع وجود نصوص قانونية إلا أنه يصعّب التعامل مع ظهور أشكال جديدة للاختراق الإلكتروني التي تتطور بالتوازي مع التقدم التكنولوجي في مجال الشبكة المعلوماتية، وهذا يستلزم تدخلًا مستمرًا من المشرع الوطني لتعديل القوانين.

أما على الصعيد القضائي، فإن هذه الجريمة تتجاوز الحدود الوطنية، مما يثير إشكالات بشأن الاختصاص القضائي.

رابعاً: منهجية البحث

Fourth: Research Methodology

وفي دراسة موضوع الطبيعية القانونية لجريمة الاختراق الإلكتروني الماس بأمن الدولة تم الاستعانة بالمناهج الآتية، لتناسبهما مع طبيعة الموضوع وهما:

- **المنهج الوصفي:** وذلك من خلال توصيف جريمة الاختراق الإلكتروني الماسة بأمن الدولة، وبيان مفهومها، واركانها.
- **المنهج التحليلي:** من خلال تحليل النصوص القانونية بجريمة الاختراق الإلكتروني الماس بأمن الدولة في التشريع الإماراتي والتشريعات المقارنة.
- **المنهج المقارن:** من خلال مقارنة التشريع الإماراتي، ومقارنتها بالتشريع المصري والسعودي والأردني والبريطاني.

خامساً: أهداف البحث

Fifth: Research Objectives

تهدف هذه الدراسة إلى إعطاء لمحة عن مفهوم جريمة الاختراق الإلكتروني الماسة بأمن الدولة، من خلال بيان مفهومها، وخصائص هذه الجرائم، وأنواعها، وأساس تجريمها، وتفصيل أركانها العامة والخاصة، وإبراز الوسيلة التي تحصل من خلالها الجريمة.

سادساً: تساؤلات البحث

Sixth: Research Questions

لقد تناولت الدراسة الاجابة على التساؤلات الاتية:

- ما هو المقصود بجريمة الاختراق الإلكتروني الماسة بأمن الدولة؟
- ما هي خصائص الاختراق الإلكتروني؟
- ماهي أركان جريمة الاختراق الإلكتروني الماسة بأمن الدولة؟
- ما هي وسائل الاختراق الإلكتروني؟
- ما هي طبيعة جريمة الاختراق الإلكتروني الماس بأمن الدولة؟
- ما مدى كفاية التجريم لهذه الأفعال؟
- ما هو أثر تلك الجريمة على أمن الدولة واستقرارها داخلياً وخارجياً؟

سابعاً: خطة البحث

Seventh: Research Plan

المقدمة

المبحث الاول: مفهوم جريمة الاختراق الإلكتروني الماس بأمن الدولة

المطلب الأول : مفهوم جرائم الاختراق الإلكتروني الماسة بأمن الدولة

المطلب الثاني: مفهوم أمن الدولة

المبحث الثاني: اركان جريمة الاختراق الإلكتروني الماس بأمن الدولة

المطلب الأول: الركن المادي

المطلب الثاني: الركن المعنوي

الخاتمة (النتائج والتوصيات)

المقدمة

Introduction

يعد حفظ أمن الدولة من أهم الأولويات لأي دولة، ولضمان تحقيقه أقرت له الدول العديد من الإجراءات و التدابير، وعملت على إحاطته بسياج منيع من قواعد الحماية وآليات التصدي، لكل ما من شأنه المساس بركيزة هذا الأمن وهي أسرار الدولة، لا سيما أسرار الدفاع الوطني، حيث أصبح اعتماد الدولة على توظيف تكنولوجيا الاتصال في حماية كل مظاهر نشاطها، فبعد أن كانت تتعامل مع أسرارها بطريقة تتوافق مع طبيعتها المادية، أصبحت تتعامل مع المعلومات بصورة رقمية، أما حفظ او تعديل أو نقل أو تخزين، حيث انعكست الصورة الجديدة والمستحدثة لأسرار الدولة على النشاط الإجرامي المستهدف، بعد أن كان تجسس تقليدي منصباً على أسرار تقليدية، يمارس في بيئة وفضاء اعتيادي وواقعي، أصبح تجسساً إلكترونياً منصباً على أسرار إلكترونية يمارس في بيئة وفضاء إلكتروني[3]، فعُد بذلك كأحد أسوء أوجه الاستخدام غير المشروع لهذا الفضاء الجديد على أمن الدولة، وحتم في المقابل على الدولة إعادة وضع آليات حماية تتوافق مع هذه المستجدات، لكن يبقى العائق المتمثل في تطور الانشطة المكونة للتجسس الإلكتروني الماسة بأمن الدولة، وهي نشاطات تقنية بالأساس، وارتباط هذه النشاط بأنشطة أخرى ناشئة عن نقل أغلب مظاهر نشاط الدولة من جهة أخرى، وعليه استوجب الأمر بداية وضع إطار تأصيلي للتجسس الإلكتروني.

وسنتناول الطبيعة القانونية لجريمة الاختراق الإلكتروني الماس بأمن الدولة في المبحثين الآتيين:

المبحث الاول: مفهوم جريمة الاختراق الإلكتروني الماس بأمن الدولة
Chapter One: The Concept of Cyber Hacking Crimes Affecting State Security

يُعد مصطلح التجسس الإلكتروني أحد صور التحول إلى العصر الرقمي، فأنه قد يصعب تحديد مدلوله، إذ يتم الخلط غالباً بين التجسس الذي قد يمس الأفراد، وبين التجسس الذي قد يمس الدولة، على الرغم من أن الأول قد يكون جزءً من الثاني، وعليه فأن عملية تحديد مفهوم التجسس الإلكتروني تمثل أهمية كبيرة، وعليه سنوضح في هذا المفهوم المطلبين الآتيين :-

المطلب الأول: مفهوم جريمة الاختراق الإلكتروني الماسة بأمن الدولة
Section One: The Concept of Cyber Hacking Crimes Affecting State Security

تنال جريمة الاختراق معلومات سرية غير متاحه للجمهور والتي تمس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني، لذا سنخصص دراستنا لتسليط الضوء على الاختراق الذي يمس بأمن الدولة، ولكن قبل التطرق لدراسة مفهوم جريمة الاختراق الإلكتروني الماسة بأمن الدولة، ينبغي علينا أن نوضح بعض المفاهيم الضرورية في هذه الدراسة، وهي مفهوم الجرائم المعلوماتية بداية، يتبعه مفهوم جريمة الاختراق الإلكتروني الماسة بأمن الدولة، باعتبارها جريمة تقنية ترتكب بوسائل فنية وتقنية، لذلك سنخصص هذا المطلب لبيان هذه الجريمة في الفرعين الآتيين:

الفرع الاول : ماهية الجرائم المعلوماتية
Subsection One: The Nature of Cybercrimes

لقد تبنت اغلب التشريعات العربية والغربية للسلوكيات الإجرامية الجديدة والمستحدثة والمتمثلة في الجرائم المعلوماتية، واستحدثت لها نصوص خاصة، ولقد حرص مجلس (الاتحاد الأوروبي) على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلى ذلك في اتفاقية بودابست الموقعة في 23 نوفمبر سنة 2001، المتعلقة بالجرائم المعلوماتية، إيماناً من الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على الاتفاقية، بالتغييرات العميقة التي حدثت بسبب الرقمية والعولمة المستمرة للشبكات المعلوماتية.

ولقد اختلفت تسمية الجرائم المعلوماتية واستخدمت لها عدة مصطلحات، فالبعض اطلق عليها جرائم الحاسب الآلي، والبعض الآخر أطلق عليها مفهوم الجرائم الإلكترونية وجرائم الحاسب الآلي، وهناك من يسميها بالجرائم المعلوماتية، ونرى من وجهة نظرنا

أنه من الأفضل تسميتها بالجرائم المعلوماتية، لأنها تشمل الحاسب الآلي، والأنترنت، وسائر التقنيات والمبتكرات الحديثة الراهنة والمستقبلية، حيث يتساوى ارتكابها من قبل الحاسب الآلي أو الهواتف الذكية، نظراً لارتباطها بالأنظمة المعلوماتية، ومن الممكن أن يكون في المستقبل نظام معلوماتي لمبتكر آخر غير الحاسب الآلي والهواتف الذكية.

لذا لا يوجد تعريف موحد على الصعيد الدولي للجريمة المعلوماتية بسبب الخلاف بشأن عناصر تكوينها، مما حمل اللجنة الأوروبية المعنية بمشاكل الجريمة المعلوماتية في المجلس الأوروبي على ترك الخيار لكل من الدولة المعنية، بوضع التعريف الخاص بها بما يتوافق مع نظامها وتقاليدها [4]، وعلى الرغم من المحاولات الجادة من التشريعات الداخلية، والجهود الدولية لتوفير حماية جزائية لتكنولوجيا المعلومات، إلا أنه حتى الآن ما زالت الطريق طويلة للوصول لحماية جزائية محكمة في هذه المجال – فضلا عن الصعوبات الإجرائية الخاصة بهذه الجرائم مقارنة بالجرائم التقليدية-، ومن الصعوبات التي تواجه تجريم صور الاعتداء على تكنولوجيا المعلومات، عدم الاتفاق على مفهوم محدد لما يدخل في الحماية، وما يُعد من تكنلوجيا المعلومات أو لازماً لها، وكذلك عدم الاتفاق على صور التجريم، فيوجد أزمة حقيقة في المصطلح الدال على الجرائم[5]، وانعكس ذلك على التسميات التي ظهرت لهذه الجرائم من الناحيتين التشريعية والفقهية، وعلى هذا الأساس سنعرض التعريف التشريعي والفقهي للجريمة المعلوماتية على النحو الاتي:

- **أولاً: التعريف التشريعي للجريمة المعلوماتية**

على الرغم من خلو بعض التشريعات من تعريف الجريمة المعلوماتية، إذ فضلت بعض التشريعات عدم وضع تعريف للجرائم المعلوماتية في تشريعاتها، تحسباً للتطور العلمي والتقني المستمر، واكتفت في قوانينها بتجريم أفعال الجريمة المعلوماتية بعد أن تصنفها تبعاً لأهدافها[6]، الا أنه من وجهة نظري كان من الأفضل وضع تعاريف للجريمة المعلوماتية وتحديد ملامحها، حتى وان كانت عرضة للتغيير والتعديل، نتيجة التطور المستمر، فلا يوجد هناك أي مانع من مواكبة هذا التطور، بتعديل القانون ليوائم تغييرات الثورة المعلوماتية.

ولم يتناول المشرع الاتحادي في دولة الإمارات العربية المتحدة أي تعريف محدد لمصطلح الجريمة المعلوماتية في المادة (1) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، إنما نص على صور الجريمة المعلوماتية وتعريفاتها، والمتمثلة بالاختراق والتسريب والاعتراض والهجمات الالكترونية، والتشفير وغيرها من الصور التي تعد صورة من صور الجريمة الإلكترونية، ونؤيده في ذلك، حيث أن المشرع الإماراتي وإن لم يكن قد وضع

تعريف محدد للجريمة الإلكترونية، إلا أنه قد أصاب في وضع تعاريف محددة لصورة هذه الجرائم المعلوماتية.

كما عرف نظام مكافحة الجرائم المعلوماتية السعودي لسنة 2017، في المادة الأولى منه الجريمة المعلوماتية بأنها:" أي فعل يرتكب متضمنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام"[7]، حيث أن المشرع السعودي حدد الضوابط والأفعال التي تدخل في عداد الجرائم المعلوماتية، وذلك عن طريق استخدام الحاسوب أو شبكة الإنترنت في ارتكاب الجريمة[8].

كذلك فعل المشرع المصري، إذ لم يتناول تعريف محدد للجريمة المعلوماتية في قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018، إنما اكتفى بعرض تعاريف صور هذه الجرائم كالاعتراض والاختراق وما في حكمها.

ومن ناحية أخرى، هناك تشريعات عرفت هذه الجريمة، كما هو الشأن بالنسبة للمشرع الجزائري في المادة (1/2) من القانون رقم (4/9) لسنة 2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وإذا عرفها بأنها: " كل الجرائم سواء المتعلقة بالمساس بالأنظمة أو غيرها من الجرائم الأخرى التي ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية، أو أي نوع آخر من نظم الاتصال الإلكتروني"[9].

أما المشرع القطري فقد عرف الجريمة الإلكترونية، في المادة (1) من قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014 بأنها: " أي فعل ينطوي على استخدام وسيلة تنقية المعلومات أو نظام معلومات أو الشبكة المعلوماتية، بطريقة غير مشروعة بما يخالف أحكام القانون".

ونرى أن المشرع القطري قد توسع في تعريف الجريمة الإلكترونية، حيث يشمل كل جريمة ترتكب بوسيلة إلكترونية، وبذلك يتضح لنا أن المشرع القطري قد تبنى المعيار الموسع للجريمة الإلكترونية.

أما بالنسبة للمشرع الأردني، فأنه لم يورد تعريف محدد للجريمة الإلكترونية في قانون الجرائم الإلكترونية رقم (27) لسنة 2015، إنما جرم الأفعال التي ترد على الأنظمة المعلوماتية والشبكات الإلكترونية، وكذلك استخدام الوسائل الإلكترونية في ارتكابها[10].

وقد عرفت منظمة التعاون الاقتصادي والتنمية (OECD) الخاص باستبيان الغش المعلومات عام 1982، والذي أوردته بلجيكا في تقريرها بأن الجريمة المعلوماتية هي: " كل فعل أو امتناع من شأنه الاعتداء على الاموال المادية والمعنوية، يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[11].

وترى الباحثة في ضوء التعريفات المقدمة، أن هذه الجريمة تقوم على اربعة عناصر أساسية تتمثل في فعل غير مشروع الذي يتم ارتكابه من خلال الوسائل الإلكترونية مع توافر القصد الجنائي بعنصرية العلم والارادة لدى مرتكب هذه الجريمة على اعتبار انها جريمة عمدية، وتحقق ضرر على مرتكب الجريمة.

- **ثانياً: التعريف الفقهي للجريمة المعلوماتية**

اختلف الفقهاء بشأن وضع تعريف موحد للجريمة المعلوماتية او الإلكترونية، حتى قيل إنَّ الجريمة المعلوماتية تقاوم التعريف، حيث أن عدم الاتفاق على تعريف الجريمة المعلوماتية يؤدي إلى تعذر تقدير حجم هذه الجرائم عالمياً للاختلاف في مفهومها، مما يصعب تحقيق التعاون الدولي لإيجاد الحلول اللازمة لمواجهتها[12].

فلقد عرفها البعض بأنها: "كل فعل غير مشروع، يكون فيه العلم بتكنولوجيا الحاسبات الآلية، بقدر كبير لازم لارتكابه من ناحية، لملاحقته وتحقيقه من ناحية اخرى"[13]، وهناك من يعرفها بأنها: "اي عمل يضر بالأشخاص أو الأموال، ويوجه ضده، أو يستخدم التقنية المتقدمة لنظم المعلومات" ويعرفها البعض الاخر بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، ويكون ناتجاً بطريقة مباشرة أو غير مباشرة، عن تدخل التقنية المعلوماتية "[14].

وهناك من عرفها ايضا بأنها: "هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلاً، وذلك باستخدام شبكات الأنترنت، من خلال غرف الدردشة، واختراق البريد الإلكتروني، ومختلف وسائل التواصل الاجتماعية، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول، تكون ضمن برنامج الاستهداف الحربي، أو الاقتصادي، أو الإضرار بسمعتها ، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب"[15].

كما عرفها الاخرون بأنها: "الفعل غير المشروع، الذي يتورط في ارتكابه الحاسب الآلي، وهو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية"[16].

وقد عرفها ايضا فقيهان آخرين[17] بأنها: "استخدام الحاسب كأداة لارتكاب الجريمة، هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به، لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية، سواء على جهاز الحاسب نفسه أو المعدلات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وانتهاك ماكينات الحساب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية، وتزيف المكونات المادية والمعنوية للحاسب"[18]، وعرفها البعض الآخر بأنها:" كل فعل أو امتناع عن فعل بشكل عمدي، مخالف لأحكام القانون، يرتكبه

شخص أو أكثر عبر جهاز إلكتروني، مما يسبب هذا الفعل أو الامتناع ضرراً للغير يستوجب إيقاع العقوبة على الفاعل وتعويض مادي عادل"[19].

وقد ذهب بعض الفقهاء إلى تعريف الجريمة المعلوماتية بالنظر إلى اعتبار الحاسب الآلي كوسيلة لارتكاب الجريمة، إذ عرفها بأنها: " أشكال السلوك غير المشروع الضار بالمجتمع الذي يرتكب باستخدام الحاسوب"[20]، وقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية بأنها: " الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً"[21].

وكتعريف شامل للجريمة المعلوماتية إلى جانب التعاريف السابقة، هناك من وضع تعريفاً شاملاً للجريمة الإلكترونية، يتمثل في تعريفها بأنها: " أي فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية أو نشاط غير مشروع موجه لنسخ أو تغيير أ حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه، أو أية جريمة يكون متطلباً لاختراقها توافر لدى فاعلها معرفة تقنية الحاسب"[22].

وبعد استقراء التعريفات الفقهية للجريمة المعلوماتية، نجد أن بعض التعريفات عولت على الوسيلة المستخدمة في ارتكاب الجريمة، وهي ضرورة ارتكاب الجريمة بواسطة الحاسوب، على الرغم من أن الوسيلة ليست من الأمور الجوهرية، فجميع الوسائل لدى المشرع سواء، فالأصل أن الوسيلة ليست عنصراً من عناصر التجريم إلا في الحالات التي يتطلبها المشرع لتحقيق البنيان القانوني للجريمة[23]، فضلا عن أنَّ من المنطق في الجريمة المعلوماتية يكون فيها الحاسوب محلاً للجريمة.

كما عولت التعريفات الأخرى على توافر المعرفة بتقنية المعلومات لدى مرتكب الجريمة المعلوماتية، ومن ثم يعتمدون على الجانب الشخصي لدى مرتكب الجريمة، حيث يتطلب توافر معرفة تقنية لدى مقترف جرائم الحاسوب، كمن يشترط المعرفة القانونية بالنصوص العقابية لقيام الجريمة[24].

إلا أنه يرى الباحث عدم دقة هذا المعيار؛ لأنه لا يستند على أساس علمي أو منطقي، فصحيح أن من خصائص المجرم المعلوماتي المعرفة التقنية، إلا أنها ليست شرطاً لازماً للجريمة المعلوماتية.

كما ترى الباحثة أن التعريف الشامل الحقيقي لمعنى للجريمة المعلوماتية: " هو كل فعل او امتناع من شأنه الاعتداء على الأحوال المادية والمعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، أو سلوك غير مشروع أو غير أخلاقي أو غير مصرح به بتعلق بالمعالجة الآلية للبيانات".

الفرع الثاني : مفهوم جريمة الاختراق الإلكتروني الماسة بأمن الدولة
Subsection Two: The Concept of Cyber Hacking Crimes Affecting State Security

1- الاختراق في اللغة:

أصل الاختراق في اللغة (خ ر ق) خَرَقت الثوب إذا شققته، وخَرَق الثوب فانْخرق وتخرَّق واخرورق. وخرقت الأرض إذا قطعتها حتى بلغت أقصاها [25].

يقال: فلان خَرَق: إذا قطع المفازة وبلغ أقصاها ومن ذلك قوله تعالى: ﴿ **إِنَّكَ لَنْ تَخْرِقَ الْأَرْضَ**﴾ خرق الأرض يخرقها قطعها حتى بلغ أقصاها وخرقت الأرض: أي جبتها[26].

2- التعريف التشريعي للاختراق الإلكتروني:

لقد عرف المشرع الاماراتي في المادة الاولى من قانون مكافحة الشائعات والجرائم الإلكترونية، الاختراق الالكتروني بأنه: (.. الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها..)

ومما سبق، ترى الباحثة أن تعريف المشرع الاتحادي جاء جامعاً؛ بحيث نص على صورة البقاء غير المشروع في النظام المعلوماتي، أو ما في حكمها، وبذلك يكون قد فتح المجال أمام أي تحديث مستقبلي قد يطرأ على الشبكة المعلوماتية.

كما تناولت المادة الأولى أيضا تعريف الهجمات الالكترونية، بأنها: (... كل استهداف متعمد ومخطط للأنظمة المعلوماتية أو البنية التحتية أو الشبكات الإلكترونية أو وسائل تقنية المعلومات يقلل من قدرات ووظائف أي منها، سواء كان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو الاختراق أو التسريب أو بغرض تعريض البيانات أو المعلومات للخطر أو تعطيل العمليات وما في حكمها..).

أما بالنسبة للمشرع الأردني، فأنه لم يحدد صراحة مفهوم الاختراق، وإنما اكتفى بالإشارة إلى الدخول غير المشروع إلى البيانات والمواقع، دون تحديد طبيعة هذه البيانات والمواقع، سواء كانت شخصية أو حكومية، حيث نجد أن المشرع الاردني قد جرم بعض الافعال التحضيرية التي تعد بحد ذاتها جريمة، ومن أمثلتها حيازة برامج الاختراق[27].

وقد نصت المادة (3/أ) من قانون الجرائم الإلكترونيَّة الاردني رقم (17) لسنة 2023م، على أنه: "يعاقب كل من دخل أو وصل قصداً إلى الشبكة المعلوماتية أو نظام المعلومات أو وسيلة تقنية المعلومات أو أي جزء منها 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 (300) ثلاثمائة دينار ولا تزيد على (600) ستمائة دينار أو بكلتا هاتين العقوبتين".

كما شدد القانون العقوبة فى المادة (3/أ) من القانون المذكور إذا كان الدخول او الوصول المنصوص عليه سابقاً كان بقصد الإلغاء أو حذف أو تدمير أو إفشاء أو نشر أو إعادة نشر أو اتلاف 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 المعلومات[28].

أما المشرع المصري، فقد عرف الاختراق فى المادة الأولي من قانون مكافحة جرائم تقنية المعلومات بأنه : "الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة، على نظام معلوماتي، أو حاسب آلي أو شبكة معلوماتية وما في حكمها".

ولم يضع المنظم السعودي، تعريف للاختراق بلفظه الصريح، وإنما أشار إليه بمعناه؛ حيث نص في الفقرة السابعة من المادة الأولى لنظام مكافحة جرائم المعلوماتية، على الدخول غير المشروع بأنه: " دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني ، أو نظام معلوماتي ، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها".[29]

اما المشرع البريطاني قد عرف فى المادة 1 من القانون إساءة استخدام الكمبيوتر لعام 1990 ان الشخص يعتبر مرتكب لجريمة الاختراق الالكتروني بأنه : " إذا ارتكاب اي شخص فعلا يؤدي إلى الدخول غير المصرح به إلى جهاز كمبيوتر أو نظام محوسب بنية أو بمعرفة أنه لا يملك الاذن القانون للقيام بذلك [30]"

3- التعريف الفقهي للاختراق الإلكتروني:

تعد جريمة الاختراق الإلكتروني من الجرائم الجديدة و المستحدثة، لذلك تعددت التعريفات الفقهية التي تناولتها، حيث من عرفها البعض بأنها: " الدخول إلى جهاز عضو في شبكة حاسب آلي، من قبل شخص غير مصرح له بالدخول إلى ذلك الجهاز أو تلك الشبكة، وذلك بغرض الاطلاع أو السرقة البيانات والمعلومات أو التخريب أو التعطيل أو زرع الفيروسات أو تدميرها "[31].

وهناك من عرف الاختراق الالكتروني بأنه: " مجموعة من الأعمال التي تؤدي إلى الإخلال بنظام وسرية الجهاز، ويقوم بالاختراق شخص أو أكثر، عن طريق شبكة الإنترنت، بإستخدام برامج متخصصة (سكانرز)، تعمل على فك الرموز والكلمات السرية، وكسر الحواجز الأمنية، عن طريق استكشاف نقاط الضعف في المواقع، التي

لا تحدَث أنظمتها بشكل دوري، ثم مهاجمتها واختراق نظامها الأمني"[32].
وعرف البعض الأخر الاختراق الإلكتروني بأنه: " القدرة على الوصول لأجهزة وبيانات الآخرين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة بهم، ويكون الهدف من ذلك إما الفضول أو تعمد تخريب المعلومات"[33].
ومن خلال استعراض التعريفات السابقة، يمكن تعريف الاختراق الإلكتروني الماس بأمن الدولة بأنه: " عملية غير مصرح بها لاختراق نظام أو شبكة معلوماتية، بهدف الوصول إلى المعلومات أو الموارد الرقمية، التي تمس بأمن الدولة، و يكون الغرض من الاختراق، هو سرقة البيانات أو العبث بها أو تعطيل النظام الخاص بالدولة والتأثير عليه بطريقة مباشرة أو غير مباشرة".
ويمكن تقسيم جريمة الاختراق الإلكترونية باعتبارها من الجرائم الماسة بأمن دولة إلى قسمين:
1 – جرائم ماسة بأمن الدولة الخارجي، مثل التجسس[34] والاتصال مع العدو لأغراض غير مشروعة.
2 – جرائم ماسة بأمن الدولة الداخلي، مثل جرائم إثارة الفتن، والجرائم التي تمس الوحدة الوطنية وتدعو إلى الخروج على الحاكم[35].

المطلب الثاني: مفهوم أمن الدولة

Section Two: The Concept of State Security

يتحقق مفهوم أمن الدولة القانوني من خلال تدخل المشرع في التجريم والعقاب، وذلك بهدف حماية عناصر أمن الدولة، والتي تتمثل في النظام الداخلي والخارجي للدولة، وحمايتها من التعرض للاعتداء أو المساس بها، مما يؤدي إلى الحفاظ على الأمن والاستقرار الذي تتمتع به الدولة[36].
وقد تباينت التشريعات في استخدامها لمصطلح أمن الدولة، فبعضها استخدم هذا المصطلح واطلق عليها الجرائم الماسة بأمن الدولة الخارجي والداخلي، مثل التشريع الإماراتي [37]،وذلك فى الفصلين الاول والثاني من الباب الاول من الكتاب الثاني لقانون الجرائم والعقوبات رقم (31) لسنة 2021 (المواد من 154- 234) حيث نجد أن المشرع الإماراتي قد تتناول هذه الاحكام الجديدة التي تسري على جميع الجرائم الماسة بأمن الدولة الخارجي والداخلي الواردة في قانون العقوبات والقوانين الأخرى [38].
أما المشرع المصري فقد استخدم مصطلح بيانات أو معلومات حكومية، بدلاً من لفظ مؤسسات الدولة[39]، وكان مبالغاً في المزج بين مفهوم كيان الدولة ككل ونظام الحكم فيها[40].

ويرى الباحث، أنه وان اختلفت المسميات بين التشريعات، فإنها في النهاية تفضي إلى المعنى نفسه، على الرغم من اختلاف المسميات.

وبناءً على ما تقدم، سنتناول مفهوم جرائم الأمن الداخلي للدولة من جهة ومن جهة جرائم الأمن الخارجي للدولة على النحو الآتي:

الفرع الأول: مفهوم جرائم الأمن الداخلي للدولة

Subsection One: The Concept of Internal State Security Crimes

سنتناول في هذا الفرع التعريف بمصطلح أمن الدولة الداخلي، تشريعاً وفقهاً على النحو التالي:

- **أولاً: التعريف التشريعي**

ركزت غالبية التشريعات المحلية والمقارنة على تحديد الجرائم الماسة بأمن الدولة الداخلي إذ أولتها عناية خاصة، حيث نجد أن المشرع الإماراتي لم يضع تعريف خاص لمصطلح أمن الدولة الداخلي، أنما اكتف فقط بتعداد الافعال التي تعد جرائم ماسة بأمن الدولة من جهة الداخل في المادة (181) إلى المادة (223) من قانون الجرائم والعقوبات الاتحادي رقم (31) لسنة 2021، والذي من خلاله يمكن استخلاص وتحديد الجرائم الماسة بأمن الدولة الداخلي.

ولما كانت الجرائم الواقعة على أمن الدولة الداخلي في التشريع الاماراتي تقع على نظامها السياسي الداخلي أو ضد الدولة بصفتها شخص من أشخاص القانون الداخلي، حيث تنطوي على اعتداء على النظام الداخلي للدولة [41].

وعلى غرار ذلك، أفرد المشرع المصري في قانون العقوبات المصري رقم 95 لسنة 2003 في الكتاب الثاني تحت عنوان: " الجنايات والجنح المضرة بالمصلحة العمومية وبيان عقوباتها"، وخصصه للجنايات والجنح المضرة بأمن الحكومة[42] من جهة الخارج[43]، في الباب الأول، وخصصه للجنايات والجنح المضرة بالحكومة من جهة الداخل في الباب الثاني[44].

اما المشرع الأردني فقد أدرج هذه الجرائم تحت عنوان " الجرائم الواقعة على أمن الدولة الداخلي"، وتناولها في المواد من (135) إلى (168) وقسمها إلى ستة أقسام:

القسم الأول، احتوى على الجنايات الواقعة على الدستور، أما **القسم الثاني،** فضم المواد (140) إلى (141) بعنوان اغتصاب سلطة سياسية أو مدنية أو قيادة عسكرية، اما **القسم الثالث،** فضم جرائم الفتنة في المواد (142) إلى المواد (146)، أما جرائم الإرهاب، فخصص لها المشرع الاردني الفصل الرابع في المواد (147) إلى المواد (149)[45].

اما المشرع الانجليزي لم يضع تعريفا محددا لجرائم أمن الدولة، وإنما حدد مفهوم الجرائم من خلال السوابق القضائية لهذه الجرائم، واشتملت على الافعال والاخطار الواقعة على أمن الدولة والملك وجرائم الخيانة والتجسس والفرار من الجيش الملكي والسرقة والاختلاس أو الإتلاف او تحريض الجنود والتمرد والعصيان، وقد صدرت تشريعات خاصة بالإرهاب، ومنها التشريع الذي صدر فى عام 1989، والتشريع الصادر فى عام 2000، والتى عرفت الإرهاب بأنه: " كل استخدام للعنف بغرض تحقيق أهداف سياسية أو إشاعة الخوف بين الشعوب أو قطاع معين". ويلاحظ على هذا التعريف انه لم يضع تعريفا محددا لأمن الدولة ، بل الافعال الارهابية[46].

- **ثانياً: التعريف الفقهي**

لقد اختلف تعريف مصطلح أمن الدولة الداخلي، حسب وجهة نظر كل فقيه، فقد تم تعريفها بأنها: " تلك الجرائم التي تنطوي على الاعتداء على النظام الداخلي للدولة أو المساس بالأمن والاستقرار داخل المجتمع"[47]، كما عرفها أخرون بأنها: "الجرائم التي تقع على نظامها السياسي الداخلي، إن كانت في حقيقتها موجهة إلى الحكام أنفسهم أو إلى نظامهم السياسي أو الاجتماعي، بقصد تغليب آخرين عليهم أو قلب نظام الحكم، وهذا ما تستهدفه جرائم تغيير دستور الدولة بغير الطرق القانونية، وإثارة العصيان المسلح، ضد السلطات القائمة شرعاً أو اغتصاب هذه السلطة، وإثارة الفتنة والاقتتال الطائفي والأعمال الإرهابية، المخلة بالأمن والنيل من الوحدة الوطنية أو من مكانة الدولة المالية"[48].

وعرف البعض الآخر جرائم أمن الدولة الداخلي بأنها: "الاجراءات الخاصة بتأمين الفرد داخل الدولة ضد الأخطار الماسة بالنفس والمال، ووضع التشريعات التي تحقق حمايته والحفاظ على مقدساته، من خلال أجهزة الأمن الداخلي، بمنع وقوع الجرائم وإنشاء الاجهزة القضائية لتوقيع العقاب على الخارجين عن القانون"[49].

وعرف الفقيه الفرنسي " جيغراد – Garraud جرائم الإخلال بالأمن الداخلي بأنها: " جرائم تقع على الحكومة، في حين أن جرائم الاعتداء على الأمن الخارجي تقع على الدولة أو الأمة بأسرها" .

من خلال التعاريف السابقة، يتبين لنا أن الجرائم التي تضر بأمن الدولة الداخلي تتعلق بالدولة في علاقاتها مع المحكومين، حيث يكون الهدف منها هو الإطاحة بالسلطة الحاكمة واستبدالها، بالإضافة إلى تحول النظام السياسي والاجتماعي إلى نظام آخر، بحيث يمكن أن تظهر هذه الجرائم على سبيل المثال كمحاولات لتغيير نظام الحكم وتعديل دستور الدولة وشكل حكومتها[50].

وتتضمن هذه الجرائم أيضًا تصنيفًا واسع، يشمل الجرائم التي تستهدف دستور الدولة، ونظام الحكم الخاص بها، وتشمل أيضًا التحريض على العصيان المسلح ضد سلطتها، وإشعال الفتنة والاقتتال الطائفي بين أفراد وفئات الشعب، وكذلك تنفيذ الأعمال الإرهابية داخل حدودها.

وبدون شك، تتطلب هذه الفئة من الجرائم اتخاذ إجراءات فعّالة للسيطرة عليها في مراحل التخطيط الأولية أو أثناء تنفيذها، بهدف التصدي لأي اعتداء على أمن الدولة الداخلي أو إثارة الفتن والتدخل في الأمان والاستقرار[51].

وعطفاً على ما سبق، ترى الباحثة أنه يمكن تعريف الجرائم الماسة أمن الدولة الداخلي بأنها: " هي الجرائم التي تهدف إلى الإخلال بالنظام العام وتعريض أمن الدولة للخطر، وذلك من خلال السعي إلى تغيير نظام الحكم، أو الإخلال بسلامة الدولة، أو الإضرار بمصالحها الحيوية، أو تهديد أمن المجتمع واستقراره".

الفرع الثاني: مفهوم جرائم الأمن الخارجي للدولة

Subsection Two: The Concept of External State Security Crimes

سنتناول في هذا الفرع التعريف بمصطلح أمن الدولة الخارجي، تشريعاً وفقهاً على النحو التالي:

- **أولاً: التعريف التشريعي**

لقد تناول المشرع الاماراتي الجرائم الواقعة على أمن الدولة الخارجي في قانون الجرائم والعقوبات الصادر بالمرسوم بقانون رقم (31) لسنة (2021)، حيث تناول هذه الجرائم في المواد (154) إلى المادة (181)، كما تناول نفس القانون أحكام خاصة بالجرائم الماسة بالأمن الخارجي والداخلي، في المواد من (224) إلى (237).

أما بالنسبة للمشرع الاردني، قد تناول هذه الجرائم فى الفصل الاول من الباب الأول من قانون العقوبات الأردني، الجرائم التي تقع على أمن الدولة الخارجي، فقد نصت المادة (114) من قانون العقوبات الأردني حيث نصت على انه: " يعاقب بالاشغال الشاقة المؤقتة خمس سنوات على الاقل كل اردني حاول باعمال أو خطب أو كتابات أو بغير ذلك أن يقتطع جزءا من الاراضي الاردنية ليضمها إلى دولة أجنبية أو أن يملكها حقا أو امتياز خاصا بالدولة الأردنية".

اما بالنسبة للمشرع المصري، فنجده نص في قانون العقوبات المصري رقم 95 لسنة 2003 في الكتاب الثاني تحت عنوان: " الجنايات والجنح المضرة بالمصلحة العمومية وبيان عقوباتها"، وخصصه للجنايات والجنح المضرة بأمن الحكومة52 من جهة الخارج53.

اما بالنسبة للمشرع الانجليزي فكما ذكرنا سابقا انه لم يضع تعريفا محددا لجرائم أمن الدولة، وإنما تحدد مفهوم الجرائم من خلال السوابق القضائية لهذه الجرائم، واشتملت على الافعال والاخطار الواقعة على أمن الدولة والملك وجرائم الخيانة والتجسس والفرار من الجيش الملكي والسرقة والاختلاس أو الإتلاف او تحريض الجنود والتمرد والعصيان، وقد صدرت تشريعات خاصة بالإرهاب، ومنها التشريع الذي صدر فى عام 1989، والتشريع الصادر فى عام 2000، والتى عرفت الإرهاب بأنه: " كل استخدام للعنف بغرض تحقيق أهداف سياسية أو إشاعة الخوف بين الشعوب أو قطاع معين"، ويلاحظ على هذا التعريف انه لم يضع تعريفا محددا لأمن الدولة ، بل الافعال الارهابية[54].

- **ثانيا: التعريف الفقهي**

أورد الفقهاء عدة تعاريف لجرائم أمن الدولة الخارجي، منها : "هي الجرائم التي تقع على الدولة في علاقاتها بالدول الأخرى، ويكون الهدف منها الاعتداء على استقلالها أو زعزعة كيانها في المحيط الدولي، أو الإساءة إلى علاقتها بالدول الأخرى، أو إعانة عدوها عليها، كانتهاك أسرار الدفاع القومي، والتخابر مع دولة أجنبية، والانضمام إلى قوات دولة معادية" [55].

وهناك من عرفها بأنها: " تلك الجرائم التي تقترف ضد كيان الدولة الخارجي، فتستهدف المساس بإستقلال الدولة أو الانتقاص من سيادتها أو تجزئه أراضيها، أو استقواء الغير عليها أو شل دفاعها، أو تعكير علاقتها الدولة، أو النيل من هيبتها الخارجية أو إضعاف الشعور القومي إزاءها فى زمن الحرب أو توقع نشوبها"[56].

وتؤيد الباحثة الرأي القائل، أن كلاً النوعين يقع على الدولة نفسها، أو بالأدق على "مصالحها " أو " حقوقها "، حيث نجد ان جرائم أمن الدولة الخارجي يقع على مصلحتها في صيانة استقلالها وسيادتها، وفى المحافظة على مكانتها واحترامها بين الدول، أما جرائم امن الدولة الداخلي فتقع على مصلحتها في حماية نظامها القانوني الأساسي وتنظيماته الحاكمة أو في تنفيذ قوانينها العادية[57].

وبرأينا يمكن تعريف الجرائم الماسة بأمن الدولة الخارجي بأنها: " هي الجرائم التي تضر بأمن الدولة من الخارج، وذلك من خلال الإضرار بمصالحها أو أهدافها أو سيادتها أو أمنها القومي"، ومن أمثلة هذه الجرائم: جرائم الخيانة والتجسس وجرائم الاتصال بالعدو والنيل من هيبة الدولة.

المبحث الثاني: اركان جريمة الاختراق الإلكتروني الماس بأمن الدولة
Chapter Two: The Elements of Cyber Hacking Crimes Affecting State Security

لقد بين المشرع الإماراتي من خلال المادة (1) من قانون مكافحة الشائعات والجرائم الإلكترونية، مفهوم جريمة الاختراق، حيث وضح مفهومها في الدخول بصورة غير مشروعة إلى الوعاء الإلكتروني محل الاختراق، أو البقاء فيه بصورة غير مشروعة، وهو ما يحصر أنماط السلوك الإجرامي في هذه الجريمة في فعلين رئيسين، هما الدخول والبقاء طالما وصم أحداهما بصفة عدم المشروعية[58]، وهي التي ترد على بيانات حساسة تمس بأمن الدولة وسيادتها.

ولم يكتف المشرع الاتحادي بالنص على السلوك الإجرامي في جريمة الاختراق المجرد، وإنما نظم حالات ارتباط الاختراق الإلكتروني بنتائج إجرامية قد تترب عليه، فتقع على الوعاء أو المحتوى المعلوماتيين، وتصيب أحداهما أو كلاهما بالضرر[59]، فضلاً عن ذلك تصدى المشرع الإماراتي لحالة تحقق الحصول على المعلومات والبيانات المخزنة في الوعاء المعلوماتي.

وبعد ما تم عرضه، يرى الباحث أن المشرع الإماراتي قد أحسن صنعاً في إصدار تشريع خاص، لشعوره بأهمية هذه الجرائم وخطورتها، ولم يول جهداً فى مواجهة ظاهرة التجسس الإلكتروني على اعتبارها جرائم عابرة للحدود الوطنية، التي شملت مخاطرها أمن الدولة ومؤسساتها العامة، وكان للوسائل التقنية الحديثة دور كبير في تسهيل ارتكابها، فكان لابد من أن يبقي المشرع يقظ دائماً، عن طريق سن القوانين المناسبة، للتصدي لهذه الأفعال التي تشكل اعتداء على سرية البيانات والمعلومات التي تمس بأمن الدولة.

كما سار المشرع الكويتي على نفس اتجاه المشرع الإماراتي، حيث رتب عدداً من النتائج الإجرامية المحتمل تحققها بناء على الاختراق الإلكتروني والتي نص عليها في القانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، وان اختلف مع المشرع الإماراتي في إيراد تعريف لفظ الاختراق، حيث انه عرف الاختراق في المادة الأولى تحت مسمى " الدخول غير المشروع " وهو الذي يقصد منه: " 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".

كما نص في الفقرة الثانية من المادة (2) من القانون المذكور على النتائج التي تؤدي إلى إضرار المحتوى المعلوماتي الخاص[60]، كما أشار إلى الاعتداء على المحتوى

المعلوماتي الحكومي، كنتيجة للاختراق الالكتروني، دون أن يتطرق إلى علاقة الاختراق الالكتروني في الاضرار بالوعاء المعلوماتي سواء كان وعاء تابعاً للأشخاص أو الحكومة[61].

في حين أن المشرع الأردني، لم يرد تعريفاً خاصاً للاختراق، كما فعل المشرع الإماراتي والمشرع الكويتي، ولكنه كان أكثر دقة عند إيراد النتائج الإجرامية في قانون الجرائم الإلكترونية رقم (17) لسنة 2023، وفرق فيما إذا كانت هذه المعلومات شخصية[62]، أو كانت تعود للوزارات أو الدوائر الحكومية، أو المؤسسات الرسمية العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم فيها[63].

وبالنسبة للقوانين الغربية فإن المشرع الانجليزي سلك نهجاً مختلفا اذا لم ينص في قانون إساءة استخدام الكمبيوتر الصادر عام 1990 والذي تم تعديله في عام 2022[64]، على أي نتائج إجرامية قد يسفر عنها الاختراق الإلكتروني، مكتفياً بالنص على الاختراق في صورته المجردة، أو إذا أدى الارتكاب أي سلوك مجرم في أي من القوانين الجنائية الإنجليزية، مفضلاً ترك تنظيم الأمر للجهود القضائية في مجال الجرائم الإلكترونية[65].

ومن خلال استعراضنا للقوانين المقارنة نجد أنه وأن كانت التشريعات قد عددت صور السلوك الإجرامي في جريمة الاختراق الإلكتروني، لم تغفل الإشارة إلى اختلاف صور القصد الجنائي في هذه الجرائم باختلاف أنماط هذا السلوك، إذ اكتفى المشرع بالنص على الركن المعنوي بالقصد الجنائي العام في بعض الأحيان، بينما نص على صور خاصة للقصد الجنائي في أحيانٍ أخرى، تبعاً لذلك سنتناول في هذا المبحث أركان جريمة الاختراق الإلكتروني الماسة بأمن الدولة، وهي التي تتمثل الركن المادي، والمعنوي، وذلك على النحو التالي:

المطلب الأول: الركن المادي

The First Requirement Is the Material Element

لم يتضمن قانون الجرائم والعقوبات الاتحادي، تعريفاً واضحاً للركن المادي، أو تحديداً كاملاً لعناصره، وإنما اقتصر على ذكر أحد عناصره وهو الفعل، فقد نصت المادة (32) من قانون الجرائم والعقوبات على أنه " يتكون الركن المادي للجريمة من نشاط إجرامي، بارتكاب فعل أو الامتناع عن فعل. متى كان هذا الارتكاب مجرماً قانونا" [66]، ووفقاً لهذا النص، يتجلى الركن المادي بتحقيق نشاط إجرامي، سواء أكان هذا النشاط إيجابياً أي بارتكاب فعل إيجابياً أم سلبياً، يتم بطريق الترك أو الامتناع عن القيام بفعل معين، ويمثل هذين النشاطين الايجابي والسلبي سلوكاً إجراميا يحقق الركن المادي للجريمة[67].

وقد عرف البعض الركن المادي بأنه: يتمثل في سلوك إجرامي معين، يشترطه القانون كمناط للعقاب على هذه الجريمة، على أن تتحقق نتيجة ضارة لهذا السلوك الإجرامي، وأن تكون هناك رابطة سببية بين السلوك الإجرامي والنتيجة الضارة "[68].

ومن المشكلات التي تثيرها جريمة الاختراق الإلكتروني الماسة بأمن الدولة، هي طبيعة الركن المادي، فهذه الجريمة تمثل سلوكاً غير مصرح به، ويتضح من هذا أن مفهوم أو مناط التجريم، ينصب على نظام معلوماتي يساء استخدامه، أو يتم اقتحامه على نحو غير مشروع، بما يكون لذلك الاستخدام أو الاقتحام، أثر مادي ملموس، يتجلى في صورة اختراق للمعلومات وتدمير للبيانات[69].

ويتمثل الركن المادي لهذه الجريمة في عملية الدخول للموقع أو الحساب الإلكتروني أو النظام أو الشبكة المعلوماتية، دون أن يكون الدخول حقاً بموجب القانون، سواء تمثل هذا الحق حق الملكية، أو حق الإدارة في ممارسة سلطتها، أو الدخول المشروع الذي يتبعه بقاء غير مشروع في أي من الأوعية الإلكترونية، وهو ما يعني تجريم فعل الولوج المجرد، طالما تم بطريق غير مشروع، سواء استهدف هذا الولوج تحقيق نتيجة إجرامية بعينها أو لم يستهدف، تحققت نتائج إجرامية عرضية أو لم تتحقق[70].

ويتحقق السلوك الإجرامي، بمجرد نجاح الجاني في الدخول لأحد الأوعية الإلكترونية التي يعتبر الدخول لها جريمة ماسة بأمن الدولة، وذلك دون أن يكون مرخصاً له بالدخول إليها قانوناً، أو اتفاقاً، فتقوم الجريمة في حق غير الحائزين لترخيص الدخول من الأصل، أو من الحائزين للترخيص، في حالة تجاوزهم للحدود المقررة لهم بموجب هذا الترخيص، وهو ما نص عليه المشرع الإماراتي بقانون مكافحة الشائعات والجرائم الإلكترونية، وهي التي صاغها المادة (1) من خلال تعريف مفهوم الاختراق بأنه: (... الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة، أو البقاء بصورة غير مشروعة...)[71].

ولقد حدد المشرع الاماراتي الركن المادي لجريمة الاختراق الإلكتروني المجرد بوجه عام، في الفقرة الأولى من المادة (2) وفي الفقرة الأولى من المادة (3) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، حيث تناولت المادة(2)، اختراق المواقع وغيرها من الاوعية الإلكترونية العائدة لأشخاص القانون الخاص ، حيث نصت على انه " يعاقب بالحبس والغرامة التي لا تقل عن (100,000) مائة ألف درهم ولا تزيد على (300,000) ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات" ، وفى الفقرة الثانية من المادة قام المشرع بتشديد العقوبة في حالة ادى ذلك الاختراق إلى إيقاف العمل أو تعطيل موقع إلكتروني

أو نظام معلوماتي إلكتروني ، حيث نصت الفقرة الثانية ،على انه ".. وتكون العقوبة الحبس مدة لا تقل عن (6) ستة أشهر والغرامة التي لا تقل عن (150,000) مائة وخمسون ألف درهم ولا تزيد على (500,000) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها".[72].

في حين تناولت المادة (3) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، الاختراق الإلكتروني الواقع على الجهات الحكومية، حيث نصت على انه".. يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (200.000) مائتي ألف درهم ولا تزيد على (500.000) خمسمائة ألف درهم ، كل من اخترق موقع إلكتروني أو نظام معلوماتي إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسة الدولة ..." [73]، وقد اتفقت المادتان على الاكتفاء بفعل الاختراق بمفهومه الوارد في المادة(1) كمناط للتجريم، حيث يقتصر فيه الركن المادي في جريمتي اختراق المواقع الإلكترونية الخاصة والحكومية، على مجرد الدخول غير المرخص به للموقع الإلكتروني، أو مخالفة شروط الترخيص الممنوح لدخولها، أو البقاء في أحد هذه المواقع بصورة لا تتفق مع مقتضيات القانون، وهو ما يعني أن هذه الجريمة تقع تامة بمجرد بلوغ الجاني الوعاء الإلكتروني الماس بأمن الدولة والنفاذ إليه، مهما كانت وسيلته في بلوغ هذا النفاذ طالما ترتب عليها تواجده فيها على نحو غير مشروع.

ويلاحظ من المادتين السابقتين، أن المشرع الإماراتي قد جرم فعل الاختراق [74]، واعتبر الاختراق الواقع على البيانات الحكومية ظرفا مشددا للعقاب، باعتباره جناية معاقب عليها، اما الاعتداء في المادة الثانية، فلقد ارتأى المشرع بأنها اقل ضرراً لذلك عدها جنحة.

وبناءً على ما سبق، فإن الركن المادي لجريمة الاختراق الإلكتروني، الواقعة على الجهات الحكومية أو الخاصة، يتمثل في السلوك الذي يقوم به الجاني، وهو الدخول غير المشروع إلى الموقع الإلكتروني أو مخالفة شروط الترخيص الممنوح لدخوله أو البقاء في أحد هذه المواقع بصورة لا تتفق مع مقتضيات القانون.

ويتحقق هذا الركن بمجرد بلوغ الجاني الوعاء الإلكتروني والنفاذ إليه، أيًا كانت وسيلته في بلوغ هذا النفاذ، طالما ترتب عليها تواجده بالموقع على نحو غير مشروع[75].

أما النتيجة الاجرامية في هذه الجريمة تتحقق بمجرد إحداث الخطر أو تدمير أو الإيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكترونية أو شبكة معلوماتية، أو إلغاء او حذف او تدمير أو إفشاء أو إتلاف او تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو انتهاك سريتها، ولا يشترط لقيام المسؤولية الجزائية عن هذه الجريمة، أن ينجح الجاني في بلوغ مرامه من جريمة الاختراق عن طريق الحصول على بيانات ومعلومات حساسة تتعلق بأمن الدولة، إنما يكفي لثبوت نيته في كون الاختراق قد تم تحقيقاً للغرض المنصوص عليه، إذ ان مناط التجريم في هذه الجريمة هو ارتكابها لتحقيق هدف معين، بغض النظر عن تحقيقه فعلياً من عدمه، حيث تستوي النتيجة الإجرامية في أثرها على التجريم الذي يستند فقط إلى الهدف من ارتكاب الجريمة، لان جرائم أمن الدولة من جرائم الخطر التى لا تتطلب تحقق النتيجة الإجرامية .

اما فيما يتعلق بعلاقة السببية بين السلوك والنتيجة الاجرامية في جريمة الاختراق الإلكتروني الماسة بأمن الدولة، فنجد ان هذا النوع من الجرائم فيه تتحقق علاقة السببية بين الفعل والنتيجة ، التي تؤدي إلى النتيجة الإجرامية، حيث يتمثل السبب في السلوك الذي ينبعث من الجاني حيث يعتبر سببا مباشرةً للنتيجة الإجرامية، مما يترتب عليه مسؤولية عن النتيجة الإجرامية[76]، ليس هذا السبب فحسب، وإنما لان هذه الجرائم ولا سيما الماسة بأمن الدولة لا تتطلب حصول النتيجة، ولأنها تعتبر من جرائم الخطر.

اما بالنسبة للمشرع الاردني، فنجد أن الركن المادي يتمثل في السلوك أو النشاط، الذي يؤدي إلى احداث النتيجة الإجرامية، مع ضرورة توافر العلاقة السببية بين الفعل والنتيجة، وعليه فقد نصت المادة (3/أ) من قانون الجرائم الإلكترونية الاردني رقم (17) لسنة 2023، على أنه: "كل من دخل عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".[77]

اما بالنسبة للمشرع المصري فيتحقق الركن المادي لجريمة الاختراق بناءا على سلوك مادي قوامه تصدي الجاني لأية معلومات أو بيانات أو كل ما هو متدوال عن طريق شبكة المعلومات أو أحد أجهزة الحاسب الآلي وما فى حكمها، حيث يتم الاختراق أو الاعتراض باستخدام وسائل فنية تمكن الجاني من خلالها بالتجسس المعلوماتي من خلال مشاهدة البيانات أو المعلومات او التصنت او التحكم ومراقبة ما هو متداول من خلال الولوج داخل النظام واستخدامه بشكل مباشر او غير مباشر.[78]

وهذا من ما نصت عليه المادة (20) من قانون جرائم تقنية المعلومات رقم 175 لسنة 2018 حيث نصت على انه: " يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا أو بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوك لها أو يخصها.

فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية تكون العقوبة السجن والغرامة التى لا تقل عن 100 ألف جنيه ولا تجاوز 500 ألف جنيه.

وفى جميع الأحوال، إذا ترتب على أى من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها أو إلغائها كليا أو جزئيا بأى وسيلة كانت، تكون العقوبة السجن والغرامة التى لا تقل عن مليون جنيه ولا تجاوز 5 ملايين جنيه".

اما بالنسبة للقانون الإنجليزي فقد نص على الركن المادي لجريمة الاختراق الالكتروني، في قانون إساءة استخدام الكمبيوتر الصادر عام 1990 والذ تم تعديله في عام 2022، حيث استخدم عنوان " الدخول غير المصرح به" كأسلوب لتحقيق النتيجة الإجرامية كمناط للتجريم، إذ نص هذا القانون بمعاقبة كل من ارتكب فعلا يمكن من خلاله الدخول إلى بيانات أو برامج مخزنة على أحد أجهزة الحاسب الآلي، دون اشتراط تحقق أي من الأضرار التي قد تترتب على هذا السلوك الإجرامي[79].

بناءً على ما سبق، يتضح لنا أن الركن المادي لجريمة الاختراق الإلكتروني، يتحقق فى القانون الإماراتي والاردني بمجرد قيام الجاني بممارسة فعل الاختراق، ولا يهم ما إذا كان الجاني قد حصل على الرقم السري واسم المستخدم وغيرها.

كما لا يشترط للعقاب على مجرد الاختراق بطريق مشروع أن يكون الموقع المخترق محمياً بأجهزة أمان، بل يكفي أن يكون الموقع مؤمنًا بكلمة مرور واحدة على الأقل، وذلك لأن اشتراط حماية الموقع بأجهزة أمان سيؤدي إلى قصر نطاق الحماية الجنائية على الأنظمة المحمية بأجهزة أمان فقط، وهذا ليس المقصود، بل يجب أن تكون القواعد الجنائية شاملة لكل الأحوال.[80]

المطلب الثاني: الركن المعنوي

The Second Requirement: The Moral Element

لا يكفي لتحديد المسؤولية الجنائية في جريمة الاختراق الإلكتروني الماسة بأمن الدولة، تحقق الركن المادي فحسب، وإنما لابد من توافر الركن المعنوي، والذي يمثل نية المخترق الداخلية، أن يكون الفعل أو الامتناع وليد إرادة حرة، أي صادر ممن يملك أهلية جنائية وهي ما تعرف بالإرادة[81]، ولما كانت جريمة الاختراق الالكتروني من الجرائم الماسة بأمن الدولة، فإن الجاني يسأل عن الجريمة سواء أكان ارتكبها عمداً أم خطأ ما لم يشترط القانون العمد صراحة، وهذا ما نصت عليه المادة (44) من قانون الجرائم والعقوبات الاتحادي، التى نصت على أنه: "يسأل الجاني عن الجريمة سواء ارتكابها عمدا أم خطا ما لم يشترط القانون العمد صراحة".

حيث يتكون الركن المعنوي من عنصرين هما: العمد والخطأ، ولقد عرفت المادة (39) من قانون الجرائم والعقوبات الاتحادي العمد بأنه هو: " اتجاه إرادة الجاني إلى ارتكاب فعل أو الامتناع عن فعل، متى كان هذا الارتكاب أو الامتناع مجرماً قانوناً وذلك بقصد إحداث نتيجة مباشرة أو أيه نتيجة أخرى مجرمة قانونا يكون الجاني قد توقعها، أما الخطأ يتوفر إذا وقعت النتيجة الإجرامية بسبب خطأ الفاعل، سواء أكان هذا الخطأ إهمالاً أم عدم انتباه أم عدم احتياط أو طيشا أو رعونة أو عدم مراعاة القوانين أو اللوائح أو الانظمة أو الأوامر".

ولم يشترط المشرع الإماراتي لقيام جريمة الاختراق الإلكتروني الماسة بأمن الدولة توافر قصد جرمي خاص، وهو ما يتبين من نص الفقرة الأولى في المادتين (2،3) من قانون مكافحة الشائعات والجرائم الإلكترونية[82]، حيث اكتفي بالقصد الجنائي العام المتمثل في العلم والإرادة، إذ يجب لقيام المسئولية الجزائية، أن يكون الجاني عالماً بأن ما يقوم به هو فعل يؤدي للنفاذ إلى وعاء إلكتروني لا يحق له الدخول إليه، أو انه يتواجد في هذا الوعاء دون وجه حق بعد دخوله، واتجاه إرادته إلى ارتكاب هذا الفعل، بشرط أن تكون إرادته مختاره وواعية، لا يشوبها أي من عيوب الإرادة التي حددها القانون[83].

وبناء على ذلك تعد جريمة الاختراق الإلكتروني الماسة بأمن الدولة، من الجرائم العمدية، والتي يجب أن يتوافر فيها العلم والارادة لارتكابها، لذلك سنوضح ذلك على النحو الاتي:

1- العلم:

يقصد بالعلم: " إدراك الجاني لجميع الظروف المادية المحيطة بالجريمة، والداخلة في التعريف القانوني لها، أي ينبغي تحقق علم الجاني بعناصر الفعل الإجرامي في لحظة سابقة على الإرادة، لأن العلم هو الذي يحدد اتجاه الإرادة وحدودها"[84].

ومن المهم في جريمة الاختراق الإلكتروني الماسة بأمن الدولة، أن يكون الجاني المخترق عالماً بمحل الجريمة، وهو موقع أو حساب إلكتروني أو شبكة أو نظام معلوماتي ماس بأمن الدولة، كما يجب أن يكون على علم عند قيامه بجريمته، بالضرر المترتب على اختراقه، كما يتوافر لدي الجاني المخترق العلم الكافي بوسيلة تنفيذ جريمته، إذ يتميز هذا العالم التقني الذي يخوض الجاني بأسرار بيانية يعلمها الجاني ويتقنها جيداً عن غيره[85]، كما يجب أن يكون عالماً بعلاقة السببية بين الأفعال التي يقدم عليها وبين تحقق النتيجة الإجرامية المتمثلة في الاختراق.

ويجب ايضاً ان يعلم الجاني المرتكب لجريمة الاختراق الإلكتروني الماسة بأمن الدولة، الظروف التي من شأنها تغيير وصف الجريمة، من اختراق المواقع إلى اختراق الشبكات المرتبطة بالإنترنت والتجول خلالها أو تغيير بعض المعلومات فيها، أو حذف شيء أو إضافته، فهذه الظروف من شأنها تغيير وصف الجريمة من جريمة اختراق للمواقع إلى جريمة أخرى، وايضاً من الظروف التي تغير من وصف الجريمة من جنحه إلى جناية، إذ يعد الاختراق الواقع على المواقع الحكومية من الجنايات[86]، التى شدد القانون العقار على مرتكبها.

كما يشمل هذا العلم الحدود المكانية والزمانية لارتكاب الجريمة، والتي تعد أحد العناصر الرئيسية في جريمة تجاوز حدود الترخيص بالدخول، وكذلك في أسلوب ارتكاب الجريمة والوسائل المستخدمة في ارتكابها، وصفته كموظف في حال ارتكاب الاختراق الإلكتروني عن طريق تجاوز حدود الترخيص والتي هي يشدد فيها المشرع العقاب على مرتكبها.

وهناك وقائع ثانوية لا يشترط القانون لتوافر القصد الجنائي في جريمة الاختراق الإلكتروني الماسة بأمن الدولة، أن يعلم الجاني بها، لأنها لا تؤثر على قيام الجريمة والمسؤولية عنها وهي تتمثل فيما يأتي :

1- عناصر الاهلية الجنائية .
2- الظروف المشددة للعقاب .
3- النتائج المتجاوزة قصد الجاني[87].

2- الارادة:

يقصد بالإرادة: " القوة النفسية التي تدفع الجاني إلى ارتكاب جريمته، على الرغم من إحاطته علماً بكافة الوقائع المتعلقة بالجريمة، ويلزم أن تكون إرادة الجاني واعية مدركة، وتتوافر لديه حرية الاختيار، فإذا كانت إرادته معيبه، إما لصغر السن أو الجنون أو السكر غير الاختياري أو وقوعه تحت إكراه مادي أو معنوي، فأن إرادته يشوبها عيب من عيوب الإرادة، تنتفي معها حرية الاختيار لديه، ومن ثم تنتفي عنه المسؤولية الجزائية "[88].

وقد نص المشرع الاتحادي على عنصر الارادة في جريمة الاختراق الإلكتروني، باتجاه إرادة الجاني لارتكاب كافة الخطوات المؤدية للجريمة، على الرغم من علمه بعناصرها ونتيجتها الاجرامية، حتى ولو تكن هذه الخطوات بطبيعتها تؤدي إلى تحقق هذه النتيجة، وهو ما يتصور حينما يقدم الفاعل على اتخاذ خطوات خاطئة من شأنها لا تؤدي إلى نجاح الاختراق، إلا أن الاختراق تم لسبب أو آخر.

وقد اكتفي المشرع الإماراتي بتحقق القصد الجنائي العام في الجريمة الواردة في الفقرة الثانية من المادتين (2،3) قانون مكافحة الشائعات والجرائم الإلكترونية، حيث عزف المشرع عن اشتراط تحقق اي من صور القصد الجنائي الخاص، وعلى هذا تقوم المسؤولية الجنائية عن الإضرار بالوعاء او المحتوى المعلوماتي كنتيجة الاختراق الإلكتروني دون اشتراط اي قصد جنائي خاص[89].

وعلى اتجاه معاكس للاتجاه السابق، تبنى المشرع الاتحادي اشتراط توافر القصد الجنائي الخاص في جريمة الاختراق الالكتروني بغرض الحصول على المعلومات والبيانات، بنص صريح في الفقرة الثالثة من المادة (2)[90]، والفقرة الثالثة من المادة (3)[91]، والتي نص فيها المشرع على "بغرض الحصول على البيانات أو المعلومات" وهي القصد الجنائي الخاص التي يلزم توافرها لقيام المسؤولية الجنائية عن الاختراق الإلكتروني المقترن بهدف الحصول على البيانات والمعلومات الذي يستوجب التشديد في العقاب.

وقد اتجه كلاً من المشرع الأردني والمشرع الكويتي، نفس اتجاه المشرع الإماراتي، حيث نص المشرع الأردني صراحة على أن جريمة الاختراق لا تقع إلى على سبيل العمد وهو واضح في نص الفقرة (أ) من المادة (3) من قانون الجرائم الإلكترونية رقم (17) لسنة 2023[92]، إلا انه خروجاً عن الأصل، اشترط المشرع الأردني وجود القصد الجنائي الخاص بخصوص جريمة الاختراق الإلكتروني الماس بأمن الدولة في نص المادة (4/ج) من القانون المذكور [93].

في حين أن المشرع الكويتي اشترط صراحة على وقوع جريمة الاختراق الإلكتروني

على سبيل العمد، من خلال تعريف الدخول غير المشروع الوارد في المادة (1) من القانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، والتي عرفها المشرع صراحةً بأنها: " النفاذ المتعمد غير المشروع .."[94].

وبرأينا فإن المشرع الكويتي قد أحسن صنعا في النص صراحة على أن الدخول غير المشروع، هو نفاذ متعمد لأنظمة تقنيات المعلومات وأجهزة الحاسب الآلي أو النظام أو الشبكة المعلوماتية أو المواقع الإلكتروني، بإيراد تعريف شامل ومفصل، قبل النص على العقوبة المترتبة عليها.

أما بالنسبة لتوافر القصد الخاص في جريمة الاختراق الإلكتروني الماس بأمن الدولة، فقد نص المشرع الكويتي عليها في نص الفقرة الأولى من المادة (3) من قانون مكافحة جرائم تقنية المعلومات[95]، والتي عاقبت على الاختراق الإلكتروني في حالة كان قصد الجاني من ورائها هو الحصول على البيانات أو المعلومات الحكومية، التي ينص القانون على سريتها.

في حين تبين من مسلك المشرع الإنجليزي في قانون إساءة استخدام الكمبيوتر الصادر عام 1990 والذي تم تعديله في عام 2022، في اشتراط تحقق صفة العمدية في جريمة الاختراق الإلكتروني وهو ما نص عليه في الفقرة الأولى من المادة (1)[96]، والتي نصت على علمه بالاختراق، وهو ما يعني وجوب علم المتهم أن ما يقوم به هو أحد خطوات الاختراق الإلكتروني، الأمر الذي يعني اشتراط المشرع الإنجليزي بدوره لصفة العمدية، كمناط لقيام جريمة الاختراق الإلكتروني، ولم تتضمن نصوص القانون أي شرط لضرورة توافر أي من صور القصد الجنائي الخاص في جريمة الاختراق الالكتروني، مما يعني انتهاجه النهج التشريعي المتمثل في الاكتفاء بالقصد الجنائي العام بعنصري العلم والإرادة على إتيان السلوك الإجرامي على الرغم من علم المتهم بعناصر الاختراق الإلكتروني.

أما المشرع المصري، فقد ارتأى أن جريمة الاختراق الإلكتروني، تقع عمداً بالولوج العمدي دون وجه حق أو المخالف لأحكام الترخيص وهو ما نص عليه في المادة الأولى من قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018[97].

وتجدر الإشارة إلى أن المشرع المصري قد أكتفى بتحقق القصد الجنائي العام، كمناط لقيام المسؤولية الجنائية، والذي اراه في هذا التوجه، رغبة المشرع المصري في اتساع نطاق التجريم، بحيث يكتفي المشرع بالقصد الجنائي العام دون الخاص، ويزيل تبعاً لذلك العراقيل التي قد تواجه نص التجريم، أو تقيد القضاء عند نظر الدعوى الجزائية، ويتزامن هذا السلوك عادة عندما يرى المشرع عند تقرير الحماية الجنائية لأحدى المصالح التي تكون على درجة عالية من الأهمية، فيرتبط إغفال النص فيها على

صور القصد الجنائي الخاص، رغبةً من المشرع في امتداد نص التجريم لينال أكبر قدر من السلوك الإجرامي.

ونخلص من ذلك إلى أن أغلب صور جريمة الاختراق الإلكتروني الماس بأمن الدولة، هي من جرائم القصد الجنائي العام، وهو الذي حرص من خلاله المشرع الإماراتي، والتشريعات القانونية المقارنة محل الدراسة على التأكيد عليه، بحيث يمكن القول بأن جريمة الاختراق الإلكتروني الماسة بأمن الدولة من جرائم القصد العام، حيث تفرض هذه الجريمة اتجاه إرادة الجاني لتحقيق نتيجة إجرامية معينه، وهي الحصول على المعلومات التي يحتويها الوعاء المعلوماتي محل الاختراق، ومن ثم تعتبر هذه الجرائم من جرائم الخطر اذا كان التركيز على الفعل ذاته كتهديد للنظام ، وتعتبر من جرائم الضرر اذا ترتب على الاختراق نتائج ملموسة ضارة .

الخاتمة

Conclusion

لقد تناولت هذه الدراسة الطبيعة القانونية لجريمة الاختراق الإلكتروني الماس بأمن الدولة، من خلال تسليط الضوء على مفهوم جريمة الاختراق الإلكتروني الماسة بأمن الدولة، وأركان جريمة الاختراق الإلكتروني الماسة بأمن الدولة، بالمقارنة مع تشريعات الدول الأخرى، وقد أسفرت الدراسة عن عدد من النتائج، وهي انعكاس لما توصلنا إليه، وعدد من التوصيات المتعلقة بالجوانب التي أثارها البحث وتتلخص فيما يأتي:

- **أولاً: الاستنتاجات**

1- لم يوجد تعريف جامع مانع لجريمة الاختراق الإلكتروني الماس بأمن الدولة على الصعيدين الفقهي والقانوني، وذلك نظراً لطبيعة هذه الجريمة المرتكبة.

2- تعد جريمة الاختراق الإلكتروني من الجرائم الجديدة والمستحدثة لذلك استخدمت لها عدة مصطلحات، فالبعض اطلق عليها جرائم الحاسب الآلي، والبعض الآخر أطلق عليها مفهوم الجرائم الإلكترونية وجرائم الحاسب الآلي، وهناك من يسميها بالجرائم المعلوماتية.

3-تتميز جريمة الاختراق الإلكتروني الماس بأمن الدولة بصعوبة الاثبات، نظراً للتغير المستمر في الوسائل المرتكب من خلالها الاختراق هذا من جهة، ومن جهة أخرى فإن المخترق قد يمتلك مهارات عالية، خاصة أن أغلب الأنظمة المعلوماتي قد تحتوي على ثغرات عند صناعتها.

3-أن المشرع الإماراتي وإن لم يكن قد وضع تعريف محدد للجريمة الإلكترونية، إلا أنه قد أصاب في وضع تعاريف محددة لصوره هذه الجرائم المعلوماتية.

4- تتحقق الجريمة بتوافر ركنيها المادي والمعنوي والذي يتمثل بنجاح الجاني في الدخول لأحد الأوعية الإلكترونية التي يعتبر الدخول لها جريمة ماسة بأمن الدولة، وذلك دون أن يكون مرخصاً له بالدخول إليها قانوناً، أو اتفاقاً ، لانها من جرائم الخطر.

- **ثانياً: المقترحات**

1- يجب الاتفاق على وضع مفهوم محدد للاختراق الالكتروني، وهذا يؤدي إلى حصر الحالات التي يمكن ان نطلق عليها اختراق الكتروني، وذلك عن طريق توحيد مسماها، وليس تحت عناوين مغايره، كمصطلح الدخول الغير مشروع، أو التجسس أو التصنت.

2- يتوجب تحديث قواعد القانون الدولي والقانون الدولي الإنساني فيما يتعلق بالاختراق الالكترونية.

3-إنشاء وكالة دولية عالمية متخصصة بمكافحة الاختراق الإلكتروني ومهاجمتها على غرار اليونيسيف واليونسكو، وتتولى بدورها تنسيق الجهود الدولية لمواجهات الهجمات السيبرانية التي تهدد أنظمة الدول الإلكترونية.

العمل على توفير الدعم للهياكل الوطنية التي تتكفل في عملية الرصد والتصدي للهجمات السيبرانية على أنظمة الدول الإلكترونية والمواقع الحكومية، لبناء استراتيجيات تنظيمية للمساعدة في منع الهجمات على المواقع الحكومية، نظراً لما تحويه على معلومات سرية تتعلق بأمن الدولة واقتصادها.

الهوامش
Endnote

[1] نرمين نبيل الأزرق، محددات المسئولية الجنائية لجرائم الاختراق والاعتراض والانتحال وآليات الضبط والردع في التشريعات العربية في العصر الرقمي " دراسة تحليلية مقارنة، مجلة البحوث الإعلامية، جامعة الازهر، العدد 56، الجزء 3، يناير 2021، ص 1044.

[2] انظر المادة (1) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية

[3] نادية سلامي، التجسس الإلكتروني كأثر للاستخدام غير المشروع للفضاء الإلكتروني على أمن الدولة الخارجي، مجلة دارسات لجامعة عمار ثليجي الأغواط، كلية الحقوق والعلوم السياسية، جامعة خنشلة، الجزائر، العدد 56، سنة 2017، ص 236.

[4] رامي متولي القاضي، مكافحة الجرائم المعلوماتية، في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية القاهرة، الطبعة الأولى، سنة 2011، ص25.

[5] عبدالإله محمد النوايسه، جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية لقانون الجرائم الإلكترونية، جامعة مؤتة، دار وائل للنشر والتوزيع، الطبعة الأولى، سنة 2017، ص34.

[6] هاني شاكر هاني، الاحكام العامة للأسرار البيانات المعلوماتية " دراسة مقارنة "، مركز الدراسات العربية ، القاهرة ، 2024، ص100.

[7] المادة (8/1) نظام مكافحة الجرائم المعلوماتية السعودي.

[8] عرفت المادة (3/1) من نظام مكافحة الجرائم المعلوماتية السعودي الشبكة المعلوماتية بأنها: " ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت) ."

[9] انظر المادة (1/2) من القانون رقم (4/9) لسنة 2009 المتعلقة بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال .

[10] المواد من (3-12) من قانون الجرائم الإلكترونية رقم (27) لسنة 2015.

[11] سفيان سوير، جرائم المعلوماتية، رسالة ماجستير، جامعة أبو بكر بلقايد تلمسان، الجزائر، سنة 2011، ص 15

[12] عبدالإله محمد النوايسه، جرائم تكنولوجيا المعلومات، مرجع سابق، ص41.

[13] حمزه بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير، جامعة باتنة، سنة 2011، ص 13.

[14] بكر يوسف بكر، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الاسكندرية، ط 1، سنة 2011، ص 89.

[15] سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث، مقال منشور بتاريخ 3-10-2015، على موقع https://www.alukah.net .

[16] MARWE VANDER, Computer Crimes And Other Grimes Against Information Technology In South Africa,"R.I.D.P",1993, p554.

[17] الفقيهان MICHEL & CREDO مشار إليه عند محمد الامين بن حريقة محمد الامين بن حريقة، وسائل وأساليب التحري في مجال مكافحة الجرائم الإلكترونية، رسالة ماجستير، جامعة عبد الحميد بن باديس مستغانم، الجزائر، سنة 2020، ص 10.

[18] محمد الامين بن حريقة، وسائل وأساليب التحري في مجال مكافحة الجرائم الإلكترونية، رسالة ماجستير، جامعة عبد الحميد بن باديس مستغانم، الجزائر، سنة 2020، ص 10.

[19] يوسف العفيفي، الجرائم الإلكترونية في التشريع الفلسطيني" دراسة تحليلية "، رسالة ماجستير، الجامعة الاسلامية بغزة، سنة 2013، ص 21.
[20] مدحت محمد عبدالعزيز إبراهيم، الجرائم المعلوماتية على النظام المعلوماتي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، سنة 2015، ص23.
[21] مشار إليه عند مدحت محمد عبدالعزيز إبراهيم، مرجع سابق ، ص23.
[22] رامي متولي القاضي، مكافحة الجرائم المعلوماتية، مرجع سابق، ص24.
[23] عبدالإله محمد النوايسه، جرائم تكنولوجيا المعلومات، مرجع سابق، ص43.
[24] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر العربي، الإسكندرية، الطبعة الثانية، سنة 2006، ص87.
[25] محمد بن مكرم بن منظور لسان العرب .. دار صادر ، بيروت. ط1. (73 / 10).
[26] محمد بن عبدالرزاق الحسينـي الملقب بمرتضى الزبيدي، تاج العروس من جواهر القاموس، دار الهداية، (219 / 25).
[27] محمود عبد الله ذيب عبد الله، جريمة الاختراق الواقعة على البيانات والمواقع الحكومية " دراسة مقارنة "، مجلة المنارة للدراسات القانونية والادارية، عدد خاص، سنة 2020، ص 157.
[28] المادة (3/ب) من قانون الجرائم الإلكترونيَّة الاردني رقم (17) لسنة 2023م.
[29] انظر المادة (7/1)من نظام مكافحة جرائم المعلوماتية السعودي والصادر من هيئة الاتصالات وتقنية المعلومات.
[30] انظر المادة (1) من قانون إساءة استخدام الكمبيوتر فى بريطانيا لعام 1990 https://www.legislation.gov.uk/ukpga/1990/18/section/1
[31] كريم أوراغ، الاختراق الإلكتروني في الفضاء السيبراني وأفضل الطرق للحماية منه، مجلة التطوير العلمي للدراسات والبحوث، العدد 4، سنة 2021، ص 32.
[32] عبد الله بن سعد القحطاني، أمن الإنترنت من الاختراق وأحصنة طروادة، مجلة أحوال المعرفة، مكتبة الملك عبدالعزيز، الرياض، سنة 2002م، ص 56.
[33] محمد القاسم وعبد الرحمن بن عبدالعزيز الحمدان، أساسيات أمن المعلومات، الرياض، سنة 2008، ص 146.
[34] التجسس الإلكتروني: هو التلصص وسرقة المعلومات من الافراد أو المؤسسات أو الدول او المنظمات، والتجسس على هذه المعلومات أياً كان نوعها، يأخذ ابعاداً جديدة، فتعددت اهدافها من معلومات اقتصادية إلى معلومات سياسية وعسكرية وشخصية، سامية بوشوشة، التجسس الإلكتروني وطرق مكافحته، مجلة العلوم الاجتماعية والإنسانية، المجلد رقم 16، العدد1، سنة 2023، ص52.
[35] عبد اللطيف بن صالح السويد، جريمة الاختراق الإلكتروني وعقوبتها " دراسة مقارنة "، رسالة ماجستير، جامعة الإمام محمد بن سعود الإسلامية، 1430 هـ، ص 46.
[36] أحمد فتحي سرور، قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، سنة 1992، ص 67.
[37] حيث تناول الكتاب الثاني الجرائم وعقوبتها في الباب الاول الجرائم الماسة بأمن الدولة ومصالحها من المادة 149 إلى 223 من قانون الجرائم والعقوبات لدولة الامارات العربية المتحدة وفقا لأحدث التعديلات بالمرسوم بقانون اتحادي رقم (31) لسنة 2021 .
[38] محمد شلال العاني و عبد الإله محمد سالم النوايسة ، الجرائم الماسة بأمن الدولة الخارجي والداخلي فى التشريع الإماراتي " وفقا لأخر التعديلات بموجب المرسوم بقانون رقم (7) لسنة 2016 ،بدون دار نشر ، 2018 ، ص 34
[39] نصت الفقرة الثانية من المادة (20) في القانون رقم (175) لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات والتي نصت على أنه: "... فإذا كان الدخول بقصد الاعتراض أو الحصول بدون

وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، والغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه".

[40] ابراهيم شاكر محمود الجبوري، جرائم الاعتداء على أمن الدولة من الداخل والخارج، المركز القومي للإصدارات القانونية، القاهرة، سنة 2011، ص 171.

[41] محمد شلال العاني و عبد الإله محمد سالم النوايسة ، الجرائم الماسة بأمن الدولة الخارجي والداخلي فى التشريع الإماراتي "، مرجع سابق ، ص 34.

[42] سمير عالية، الوجيز في شرح الجرائم الواقعة على أمن الدولة، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان، سنة 2008، ص 11.

[43] من المواد (77) إلى (85) من قانون العقوبات المصري رقم (95) لسنة 2003.

[44] من المواد (86) إلى (102) من قانون العقوبات المصري رقم (95) لسنة 2003.

[45] سفيان عرشوش، الجرائم الماسة بأمن الدولة الداخلي " دراسة مقارنة بين الشريعة والقانون "، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، سنة 2015-2016، ص 16.

[46] عبد الرزاق عبد الرحيم المازي ، الحماية الجنائية لأمن الدولة الدخلي من الإجرام المنظم فى التشريع العقابي الاماراتي " دراسة مقارنة ""،رسالة دكتوراه ، كلية شرطة دبي ، 2015 ، ص 45

[47] محمود سليمان موسي، الجرائم الواقعة على أمن الدولة " دراسة مقارنة في التشريعات العربية والقانونين الفرنسي والايطالي"، دار المطبوعات الجامعية، الاسكندرية، سنة 2009، ص 102.

[48] محمود عودة الجبور، الجرائم الواقعة على أمن الدولة وجرائم الارهاب في القانون الأردني والقوانين العربية، دار الثقافة للنشر والتوزيع، عمان، الطبعة الثانية، سنة 2010، ص 14.

[49] ابراهيم محمود اللبيدي، الحماية الجنائية لأمن الدولة، دار الكتب القانونية، مصر، سنة 2010، ص 39.

[50] عبد الرزاق عبد الرحيم المازمي، الحماية الجنائية لأمن الدولة الداخلي من الإجرام المنظم في التشريع العقابي الإماراتي، رسالة دكتوراه، كلية شرطة دبي، سنة 2015، ص 37.

[51] جمال سند السويدي، النظام الأمني في منطقة الخليج العربي " التحديات الداخلية والخارجية "، إصدارات مركز الامارات للدراسات والبحوث الاستراتيجية، الطبعة الاولى، سنة 2008، ص 37.

[52] سمير عالية، الوجيز في شرح الجرائم الواقعة على أمن الدولة، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان، سنة 2008، ص 11.

[53] من المواد (77) إلى (85) من قانون العقوبات المصري رقم (95) لسنة 2003.

[54] عبد الرزاق عبد الرحيم المازي ، الحماية الجنائية لأمن الدولة الدخلي من الإجرام المنظم فى التشريع العقابي الاماراتي " دراسة مقارنة ""،رسالة دكتوراه ، كلية شرطة دبي ، 2015 ، ص 45

[55] عبد المهيمن بكر سالم، جرائم أمن الدولة الخارجي " دراسة مقارنة في التشريع الكويتي والمقارن"، مطبوعات جامعة الكويت، سنة 1988، ص 2.

[56] سمير عالية ، الوجيز فى شرح الجرائم الواقعة على أمن الدولة " دراسة مقارنة "، المؤسسة الجامعية للدراسات والنشر والتوزيع ، بيروت ، 1999 ،ص 106

[57] بكر عبد المهيمن، الاحكام العامة في الجرائم الماسة بأمن الدولة الخارجي، مجلة العلوم القانونية والاقتصادية، المجلد رقم 7، العدد 1 ، سنة 1965، ص 3.

[58] نصت الفقرة الأولى من المادة (1) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية على أنه: "يعاقب بالحبس والغرامة التي لا تقل عن (100,000) مائة ألف درهم ولا تزيد على (300,000) ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات".

[59] نصت الفقرة الأولى من المادة (1) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية على أنه: " وتكون العقوبة الحبس مدة لا تقل عن (6) ستة أشهر والغرامة التي لا تقل عن (150.000) مائة وخمسون ألف درهم ولا تزيد على (500,000) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها".

[60] نصت الفقرة الثانية من المادة (2) من القانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات على أنه: " 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".

[61] نصت الفقرة الأولى من المادة (3) من القانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات على أنه: " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبتين كل من: 1- ارتكب دخولا غير مشروع الى 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. فإذا ترتب على ذلك الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها أو تعديلها، تكون العقوبة الحبس مدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن خمسة آلاف دينار ولا تجاوز عشرين ألف دينار أو بإحدى هاتين العقوبتين.ويسرى هذا الحكم على البيانات والمعلومات المتعلقة بحسابات عملاء المنشآت المصرفية".

62 نصت المادة (3/أ) من قانون الجرائم الإلكترونية رقم (17) لسنة 2023 على أنه: "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 (٣٠٠) ثلاثمائة دينار ولا تزيد على (٦٠٠) ستمائة دينار أو بكلتا هاتين العقوبتين".

[63] نصت المادة (4/أ) من قانون الجرائم الإلكترونية الاردني رقم (17) لسنة 2023 على أنه: " يعاقب كل من دخل أو وصل دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها يعود للوزارات أو الدوائر الحكومية أو المؤسسات الرسمية العامة أو المؤسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة واطلع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (٢٥٠٠) ألفين وخمسمائة دينار ولا تزيد على (٢٥٠٠٠) خمسة وعشرين ألف دينار".

[64] file:///C:/Users/Fatma/Desktop/%D8%A7%D9%84%D8%A7%D8%AE%D8%AA%D8%B1%D8%A7%D9%82/computer%20misuse.pdf

[65] إسلام هديب، الأمن السيبراني " الهجمات السيبرانية والجرائم السيبرانية "، دار مصر للنشر والتوزيع، الطبعة الاولى، سنة 2024، ص 104.

[66] نصت المادة (32) من قانون الجرائم والعقوبات لدولة الامارات العربية المتحدة من المرسوم بقانون اتحادي رقم (31) لسنة 2021 على أنه: " يتكون الركن المادي للجريمة من نشاط إجرامي بارتكاب فعل أو الامتناع عن فعل متى كان هذا الارتكاب أو الامتناع مجرماً قانوناً".

[67] محمد شلال العاني، أحكام القسم العام في قانون العقوبات الاتحادي الإماراتي، الافاق المشرقة ناشرون، سنة 2010، ص 169.
[68] رؤوف عبيد، مبادئ القسم العام في التشريع العقابي، دار الفكر الجامعي، مصر، سنة 1979، ص 188.
[69] عبد اللطيف بن صالح السويد، مرجع سابق، ص 125.
[70] وسيم الأحمد، مجموعة القوانين العربية المتعلقة بمكافحة جرائم تقنية المعلومات، الدار المنهجية للنشر والتوزيع، عمان، سنة 2020، ص166.
[71] انظر المادة (1) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.
[72] المادة (2) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.
[73] المادة (3)من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية. .
[74] لقد عرف المشرع الإماراتي في المادة (2) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية فعل الاختراق بأنه: " الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها".
[75] إسلام هديب ، مرجع سابق، ص 107.
[76] عبد اللطيف بن صالح السويد ، مرجع سابق ، ص 128.
[77] محمود عبد الله ذيب عبد الله، جريمة الاختراق الواقعة على البيانات والمواقع الحكومية " دراسة مقارنة "، مجلة المنارة للدراسات القانونية والادارية، عدد خاص، سنة 2020، ص 179.
[78] إسلام مصطفي جمعة مطصفي ، جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات فى القانون المصري ، رسالة دكتوراه ، المجلة القانونية ، المجلد 12 ، العدد 3 ، 2022 ، ص 734.
[79] اسلام هديب، مرجع سابق، ص 111.
[80] عبد الرحمن الدخيل، توصيف اختراق المواقع على الشبكة العالمية للمعلومات، مكتبة الرشد الرياض، سنة 2005، ص 64.
[81] تعرف الإرادة: "عبارة عن قوة نفسية من شأنها السيطرة، فهي كفيلة بخلق فكرة الجريمة، وبعد ذلك يأتي دور السيطرة في مرحلة التنفيذ، ففي مرحلة التفكير في الجريمة يكون لها دور نفسي يدخل في حيثيات الركن المعنوي، أما في دور التنفيذ تدخل في حيثيات الركن المادي بوصفها عنصراً فيه" للمزيد انظر: محروس نصار غايب، الجريمة المعلوماتية، مجلة التقني، المعهد التقني- محافظة الانبار، المجلد رقم 244، العدد 9، سنة 2011، ص 107-108.
82 استهل المشرع الاتحادي في المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية نص المادتين (2,3) بمصطلح " كل من اخترق "، حيث يستفاد من الصياغة التشريعية للمادتين على اشتراط العمد، وايضا نصت المادة 44 من قانون الجرائم والعقوبات على انه (يسأل الجاني عن الجريمة سواء ارتكبها عمدا أم خطأ ما لم يشترط القانون العمد صراحة).
[83] اسلام هديب، مرجع سابق، ص 113.
[84] محمد شلال العاني، مرجع سابق، ص 189 .
[85] عبد الرحمن الدخيل، مرجع سابق، ص 67.

[86] عبد اللطيف بن صالح السويد، مرجع سابق، ص 139.
[87] حسن ربيع محمد، شرح قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة (القسم العام) الجزء الأول، أكاديمية شرطة دبي، الطبعة الثانية، سنة 2004، ص 293.
[88] محمد الشناوي، استراتيجية مكافحة جرائم الاتجار في البشر، المركز القومي للإصدارات القانونية، القاهرة، سنة 2014، ص 93.
[89] إسلام هديب، مرجع سابق، ص 11.
[90] المادة (3/2) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية تنص على: " وتكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (200,000) مائتي ألف درهم ولا تزيد على (500,000) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع".
[91] المادة (3/3)) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية تنص على: "وتكون العقوبة السجن المؤقت مدة لا تقل عن (7) سنوات والغرامة التي لا تقل عن (250,000) مائتين وخمسين ألف درهم ولا تزيد على (1,500,000) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة".
92 نصت المادة (3/أ) من قانون الجرائم الإلكترونيَّة الاردني رقم (17) لسنة 2023م، على أنه: " يعاقب كل من دخل أو وصل قصداً إلى الشبكة المعلوماتية أو نظام المعلومات أو وسيلة تقنية المعلومات أو أي جزء منها 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 (300) ثلاثمائة دينار ولا تزيد على (600) ستمائة دينار أو بكلتا هاتين العقوبتين".

93 نصت المادة (4/ج) من قانون الجرائم الإلكترونيَّة الاردني رقم (17) لسنة 2023م، على أنه: " يعاقب كل من دخل أو وصل قصدا إلى موقع إلكتروني يعود للوزارات أو الدوائر الحكومية أو المؤسسات الرسمية العامة أو المؤسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة بهدف الاطلاع على بيانات | أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني بالحبس مدة لا تقل عن أربعة أشهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (٢٥٠٠) ألفين وخمسمائة دينار ولا تزيد على (٢٥٠٠٠) خمسة وعشرين ألف دينار".
[94] نص المشرع على تعريف الدخول غير المشروع في المادة (1) من القانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات على أنه: " الدخول غير المشروع النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح".
[95] نصت المادة (1/3) من القانون رقم (63) لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات الكويتي على أنه: " يعاقب بالحبس مدة لا تجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تجاوز 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".

[96] The Computer Misuse Act, Art 1-1: “He knows at the time when he causes the computer to perform the function that that is the case”.

[97] نص المشرع المصري على تعريف الاختراق في المادة (1) من قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018 على أنه: " الدخول غير المرخص به أو المخالف لأحكام الترخيص ، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها".

المصادر

References

Sources and References:

Firstly: - Linguistic References:

I. Mohamed bin Makram bin Manzur, *Lisan al-Arab*, Dar Sader, Beirut, 1st Edition, (73/10).
II. Mohamed bin Abdulrazzaq Al-Husseini, known as Murtadha Al-Zabidi, *Taj al-Arus Min Jawahir al-Qamus*, Dar Al-Hidaya, (219/25).

Secondly: - Arabic Reference:

III. Ibrahim Shakir Mahmoud Al-Jubouri, *Crimes Against National Security from Inside and Outside*, National Center for Legal Publications, Cairo, 2011, p. 171.
IV. Ibrahim Mahmoud Al-Lubaydi, *Criminal Protection of National Security*, Dar Al-Kutub Al-Qanuniya, Egypt, 2010.
V. Ahmed Khalifa Al-Malta, *Cyber Crimes*, Dar Al-Fikr Al-Arabi, Alexandria, 2nd Edition, 2006.
VI. Ahmed Fathi Surour, *Criminal Code: Special Part*, Dar Al-Nahda Al-Arabiya, Cairo, 1992.
VII. Islam Hadeeb, *Cybersecurity: Cyberattacks and Cybercrimes*, Dar Misr for Publishing and Distribution, 1st Edition, 2024.
VIII. Bakar Youssef Bakar, *Searching for Information in Modern Technology Tools*, Dar Al-Fikr Al-Jami'i, Alexandria, 1st Edition, 2011.
IX. Jamal Sand Al-Suwaidi, *The Security System in the Gulf Region: Internal and External Challenges*, Emirates Center for Strategic Studies and Research, 1st Edition, 2008.
X. Hassan Rabea Mohamed, *Explanation of the Federal Penal Code of the UAE (General Part) Part 1*, Dubai Police Academy, 2nd Edition, 2004.
XI. Rami Metwally Al-Qadi, *Combating Cyber Crimes in Comparative Legislation and in the Light of International*

Agreements and Treaties, Dar Al-Nahda Al-Arabiya, Cairo, 1st Edition, 2011.

XII. Raouf Obeid, *Principles of the General Part in Penal Legislation*, Dar Al-Fikr Al-Jami'i, Egypt, 1979.

XIII. Samir Alya, *Concise Explanation of Crimes Against National Security: A Comparative Study*, The University Foundation for Studies, Publishing, and Distribution, Beirut, 1999.

XIV. Samir Alya, *Concise Explanation of Crimes Against National Security*, The University Foundation for Studies, Publishing, and Distribution, Beirut, Lebanon, 2008.

XV. Abdulrahman Al-Dakheel, *Description of Hacking Websites on the World Wide Web*, Al-Rushd Library, Riyadh, 2005.

XVI. Abdul-Muhaymin Bakar Salem, *Crimes Against National Security Abroad: A Comparative Study in Kuwaiti and Comparative Legislation*, Kuwait University Publications, 1988.

XVII. Abdullah Muhammad Al-Nawaiseh, *Information Technology Crimes: Explanation of the Substantive Provisions of the Cybercrime Law*, Mutah University, Dar Wail for Publishing and Distribution, 1st Edition, 2017.

XVIII. Mohamed Al-Shanawi, *Strategy for Combating Human Trafficking Crimes*, National Center for Legal Publications, Cairo, 2014.

XIX. Mohamed Al-Qasim and Abdulrahman Bin Abdulaziz Al-Hamdan, *Essentials of Information Security*, Riyadh, 2008.

XX. Mohamed Shalal Al-Ani and Abdul-Ilah Muhammad Salem Al-Nawaiseh, *Crimes Affecting National Security Both Domestic and Foreign in UAE Legislation: According to the Latest Amendments by Decree-Law No. (7) of 2016*, No Publisher, 2018.

XXI. Mohamed Shalal Al-Ani, *Provisions of the General Part in the UAE Federal Penal Code*, Al-Afaq Al-Mushriqa Publishers, 2010.

XXII. Mahmoud Suleiman Mousa, *Crimes Against National Security: A Comparative Study in Arab Legislations and French and Italian Law*, Dar Al-Matboo'at Al-Jami'iya, Alexandria, 2009.

XXIII. Mahmoud Ouda Al-Jubour, *Crimes Against National Security and Terrorism Crimes in Jordanian Law and Arab Laws*, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2nd Edition, 2010.

XXIV. Midhat Mohamed Abdulaziz Ibrahim, *Cyber Crimes on Information Systems: A Comparative Study*, 1st Edition, Dar Al-Nahda Al-Arabiya, Cairo, 2015.

XXV. Hani Shakir Hani, *General Provisions of Informational Data Secrecy: A Comparative Study*, Center for Arab Studies, Cairo, 2024.

XXVI. Wassim Al-Ahmad, *Collection of Arab Laws Related to Combating Information Technology Crimes*, Al-Dar Al-Manhajiya for Publishing and Distribution, Amman, 2020.

Thirdly: - Foreign References:

XXVII. MARWE VANDER, *Computer Crimes and Other Crimes Against Information Technology in South Africa*, R.I.D.P, 1993.

XXVIII. The Computer Misuse Act, Art 1-1: "He knows at the time when he causes the computer to perform the function that that is the case."

Fourthly: - Academic Theses:

XXIX. Islam Mustafa Jumaa Mustafa, *Cybersecurity Breaches and Protection of Data and Information Use in Egyptian Law*, Doctoral Thesis, Legal Journal, Vol. 12, Issue 3, 2022.

XXX. Hamza Ben Aqoun, *Criminal Behavior of Cybercriminals*, Master's Thesis, Batna University, 2011.

XXXI. Sofiane Souir, *Cybercrimes*, Master's Thesis, Abou Bakr Belkaid Tlemcen University, Algeria, 2011.

XXXII. Sofiane Archouch, *Crimes Affecting Internal National Security: A Comparative Study Between Sharia and Law*,

Doctoral Thesis, Faculty of Law and Political Science, Mohamed Khider University of Biskra, 2015-2016.

XXXIII. Abdulrazzaq Abdulrahim Al-Mazmi, *Criminal Protection of Internal National Security from Organized Crime in UAE Penal Legislation*, Doctoral Thesis, Dubai Police Academy, 2015.

XXXIV. Abdul Latif Bin Saleh Al-Suwaid, *The Crime of Hacking and its Punishment: A Comparative Study*, Master's Thesis, Imam Muhammad Bin Saud Islamic University, 1430 AH.

XXXV. Mohamed Amin Ben Hariga, *Methods and Techniques of Investigation in Combating Cybercrime*, Master's Thesis, Abdelhamid Ben Badis University, Mostaganem, Algeria, 2020.

XXXVI. Youssef Al-Afifi, *Cybercrimes in Palestinian Legislation: An Analytical Study*, Master's Thesis, Islamic University of Gaza, 2013.

Fifthly: - Scientific Journals and Articles:

XXXVII. Bakar Abdul Muhaymin, *General Provisions on Crimes Affecting External National Security*, *Journal of Legal and Economic Sciences*, Vol. 7, Issue 1, 1965.

XXXVIII. Samia Bouchoucha, *Electronic Espionage and Methods of Combating It*, *Journal of Social and Human Sciences*, Vol. 16, Issue 1, 2023.

XXXIX. Samira Beitam, *Cybercrime and Emerging Criminal Technology*, Article published on 3-10-2015, on the website Alukah.net.

XL. Abdullah Bin Saad Al-Qahtani, *Internet Security from Hacking and Trojan Horses*, *Journal of Knowledge Affairs*, King Abdulaziz Library, Riyadh, 2002.

XLI. Karim Ouragh, *Electronic Hacking in Cyberspace and Best Methods of Protection Against It*, *Journal of Scientific Development in Studies and Research*, Issue 4, 2021.

XLII. Mahrous Nassar Ghaib, *Information Crime*, *Technician Magazine*, Technical Institute - Anbar Province, Vol. 244, Issue 9, 2011.

XLIII. Mahmoud Abdullah Dheeb Abdullah, *Hacking Crimes on Government Data and Websites: A Comparative Study*, *Al-Manara Journal for Legal and Administrative Studies*, Special Issue, 2020.

XLIV. Nadia Salami, *Electronic Espionage as a Consequence of the Illegal Use of Cyberspace on External National Security*, *Studies Journal of Ammar Thleiji University, Alghawat*, Faculty of Law and Political Science, Khenchela University, Algeria, Issue 56, 2017.

XLV. Nermin Nabil Al-Azraq, *Determinants of Criminal Responsibility for Hacking, Interception, and Impersonation Crimes and Mechanisms for Control and Deterrence in Arab Legislation in the Digital Age: A Comparative Analytical Study*, *Media Research Journal*, Al-Azhar University, Issue 56, Part 3, January 2021.

Sixthly: - Websites:

XLVI. See Article (1) of the Computer Misuse Act in the UK, 1990 here.

Seventhly: - Laws:

XLVII. *The Computer Misuse Act in the UK, 1990.*

XLVIII. *Saudi Cybercrime Control System*, issued by the Communications and Information Technology Commission, 1428 AH.

XLIX. *Federal Law No. (34) of 2021 on Combating Rumors and Cybercrimes.*

L. *Jordanian Cybercrime Law No. (17) of 2023.*

LI. *Criminal and Penal Code of the United Arab Emirates as per Federal Decree-Law No. (31) of 2021.*

LII. *Criminal and Penal Code of the United Arab Emirates according to the latest amendments by Federal Decree-Law No. (31) of 2021.*

LIII. *Egyptian Penal Code No. (95) of 2003.*

LIV. *Law No. (175) of 2018 on Combating Information Technology Crimes.*

LV. *Law No. (63) of 2015 on Combating Information Technology Crimes (Egypt).*
LVI. *Law No. (63) of 2015 on Combating Information Technology Crimes (Kuwait).*
LVII. *Federal Decree-Law No. (34) of 2021 on Combating Rumors and Cybercrimes.*
LVIII. *Combating Information Technology Crimes Law No. (175) of 2018.*