Criminalization of Cyber-Espionage According to Jordanian Criminal Legislation

Barjes K. A. Alshawabkeh[(1)*] **Hassan Y. M. Magableh**[(2)]

(1) Assistant Professor of Criminal Law at the College of Law -Irbid National University, Irbid - Jordan.
(2) Associate Professor of Criminal Law at the College of Law -Irbid National University, Irbid - Jordan.

Received: 29/07/2024
Accepted: 01/09/2024
Published: 15/12/2024

* ***Corresponding Author:***
b.alshawabkeh@inu.edu.jo

DOI:https://doi.org/10.59759/law.v3i4.620

Abstract

This study addressed the criminalization of espionage in Jordanian criminal legislation due to its severity if carried out electronically, which makes the crime, in terms of its conduct, easier and its danger, in terms of the result, greater in undermining the state's security and safety internally and externally. The problem of the study lies in determining the extent to which traditional criminal texts can accommodate the crimes of technical espionage and its uniqueness in a legal model in light of the innovation that has occurred, which has changed its legal nature. Therefore, the study aimed to define the meaning of espionage and the extent to which it can be committed by electronic means, and to explain its pillars, elements, and the scope of its criminalization, as well as to evaluate the criminal policy adopted by the Jordanian legislator in combating espionage on the state's information and secrets to prevent access to them under the threat of punishment on the one hand, and to clarify the scope of penal aggravation in case of tampering with or assaulting this information on the other hand.

The researcher of this study followed the descriptive and analytical curriculum, by presenting the legal texts criminalized for technical espionage and analyzing its content. The study concluded a series of findings, the most important of which was the identification of the meaning of espionage and the control of its limits, the possibility of accommodating traditional texts of technical espionage offenses to the extent that it does not prejudice the principle of criminal legality on the one hand and the other hand, the protection of State secrets and documents. This requires the amendment of some of the existing legal texts and the enactment of new ones that seek to create a more effective penal legislative system in the face of technical espionage in all its forms.

Keywords: Electronic Espionage, Cybercrime, National Security, State Secrets, Protected Works.

تجريم التجسس التقنيّ في التشريع الجزائيّ الأردني

برجس خليل أحمد الشوابكة[١] حسن يوسف مصطفى مقابلة[٢]

(١) أستاذ مساعد، كلية القانون، جامعة اربد الاهلية، إربد – الأردن.

(٢) أستاذ المشارك، كلية القانون، جامعة إربد الأهلية، إربد – الأردن.

ملخص

تناولت هذه الدراسة تجريم التجسس في التشريع الجزائي الأردني نتيجة خطورته إذا تم بصورة إلكترونية، الأمر الذي يجعل الجرم من حيث سلوكه أسهل وخطره من حيث النتيجة أكبر في المساس بسلامة الدولة وأمنها على الصعيد الداخلي والخارجي، وتبرز إشكالية الدراسة في تحديد مدى استيعاب النصوص الجزائية التقليدية لجرائم التجسس التقني وتفرده بنموذج قانوني في ظلّ الاستحداث الذي طرأ عليه بصورة غيّر فيها من طبيعته القانونية، لذا هدفت الدراسة إلى تحديد مدلول التجسس ومدى قابلية ارتكابه بوسائل إلكترونية وبيان أركانه وعناصره ونطاق تجريمه وتقييم السياسة الجزائية التي انتهجها المشرع الأردني في مكافحة التجسس على معلومات الدولة وأسرارها؛ للحيلولة دون الاطلاع عليها تحت طائلة العقاب من ناحية وبيان نطاق التشديد العقابي في حال العبث بهذه المعلومات أو الاعتداء عليها من ناحية أخرى.

اتبع الباحث في هذه الدراسة المنهج الوصفي والمنهج التحليلي، من خلال عرض النصوص القانونية المجرمة للتجسس التقني، وتحليل مضمونها، وخلصت إلى مجموعة من النتائج وأهمها تحديد مدلول التجسس وضبط حدوده، وإمكانية استيعاب النصوص التقليدية لجرائم التجسس التقنية في الحد الذي لا يمس بمبدأ الشرعية الجزائية، بالإضافة إلى وجودِ تباينٍ في مقدار العقوبات التي يفرضها قانون الجرائم الإلكترونية من جهة، وقانون حماية أسرار الدولة ووثائقها من جهة أخرى؛ الأمر الذي يستدعي تعديل بعض النصوص القانونية الحالية وسن نصوص جديدة تسعى إلى خلق منظومة تشريعية جزائية أكثر فاعلية في مواجهة التجسس التقني بكافة أنماطه.

الكلمات الدالة: التجسس الإلكتروني، الجرائم الإلكترونية، الأمن الوطني، أسرار الدولة، المصنفات المحمية.

المقدمة:

شهدت الأردن في الآونة الأخيرة الانتشار العريض لاستخدام شبكة الإنترنت، وتوسع استخدام الحاسب الآلي لدى الأفراد والوحدات الحكومية على السواء، وكذلك في الوحدات الإدارية والعلمية والبحثية وازدادت في الوقت ذاته الأخطار التي يمكن أن تتعرض لها شبكات البيانات الحكومية في الوطن العربي خاصّة في الأردن، حيث توسعت في هذا القرن باستخدام شبكة الإنترنت نتيجة التحول الرقمي والأتمتة والبدء بتنفيذ مشروع الحكومة الإلكترونية، والانتقال إلى بيئة عمل متطورة (مكاتب بلا ورق).

فالشبكة المعلوماتية وجميع ما يرتبط بها من وسائل التقنية الحديثة تحتوي على معلومات مهمة، كالمواقع العسكرية أو أنظمة التسليح، أو غيرها من المعلومات التي لا يجوز الاطلاع عليها إلا لمن رخص له بذلك، وكما أن النظام المعلوماتي أو الموقع الإلكتروني الذي يحتوي على معلومات تمس الأمن القومي لا يجوز الدخول إليها دون تصريح أو بما يجاوز أو يخالف حدود التصريح.

أخرج المشرع الأردني جرائم التجسس من قانون العقوبات رقم ١٦ لسنة ١٩٦٠ وأدخلها بقانون خاص وهو قانون حماية أسرار الدولة ووثائقها رقم ٥٠ لسنة ١٩٧١، فقام بسن نصوص تواجه جريمة التجسس بصورتها التقليدية، وفي ظل التطور الرقمي والتكنولوجيا الحديثة وتنوع أساليب الإجرام وظهور الجرائم المستحدثة وعلى رأسها جريمة التجسس التقني، صدر قانون جرائم أنظمة المعلومات رقم ٣٠ لسنة ٢٠١٠ لأول مرة في المملكة الأردنية ثم استبدل بقانون الجرائم الإلكترونية رقم ٢٧ لسنة ٢٠١٥ والذي حلَّ محله مؤخراً قانون الجرائم الإلكترونية رقم ١٧ لسنة ٢٠٢٣.

ويكمن الخطر الأكبر في الضعف الأمني لمعظم الشبكات الحكومية في الوطن العربي، واعتماد الشبكات العربية بصورة أساسية على الشبكة العالمية، وغياب التواصل العربي في مجال الاتصال الإلكتروني ولا شك أن معظم خبراء الشبكات مطلعين على أدق تفاصيل الشبكة العالمية؛ وهي بذلك سهلة الاختراق نسبياً إذا لم تتوفر بعض الحلول الأمنية لهذه الشبكات، الأمر الذي استدعى إنشاء المركز الوطني للأمن السيبراني في الأردن بموجب قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩.

وقد جرمت المادة ٤ من قانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣ الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس المصلحة أو الأمن الوطني من خلال الدخول أو الوصول غير المشروع إلى الموقع الإلكتروني، أو الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات، أو أي جزء منها يعود للوزارات أو الدوائر الحكومية أو المؤسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة.

والبنى التحتية الحرجة مصطلح حديث على الساحة القانونية، ويعني مجموعة الأنظمة والشبكات الإلكترونية والأصول المادية وغير المادية أو الأصول السيبرانية والأنظمة وتقنية المعلومات التي يعد تشغيلها المستمر ضرورة لضمان أمن الدولة أو اقتصادها أو سلامة المجتمع (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤).

أهمية الدراسة:

تتبع أهمية هذه الدراسة، من أهمية البيانات والمعلومات السرية الماسة بالأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني؛ لذلك من الأهمية بمكان التطرق لموضوع التجسس التقني في التشريع الأردني، وبيان مدى استيعاب قانون حماية أسرار ووثائق الدولة التجسس بالصورة المستحدثة، ومناقشة عناصر تجريم التجسس في قانون الجرائم الإلكترونية، وتسليط الضوء على السياسة الجزائية الموضوعية في مواجهة هذه الجريمة، كما أن أساليب الإجرام الإلكتروني في ظل التحول الرقمي تؤكد على أهمية دراسة الموضوع وبيان الحلول التشريعية للحد من ارتكاب جرائم التجسس الإلكتروني على أسرار الدولة وبياناتها الأمنية.

إشكالية الدراسة:

تبرز إشكالية الدراسة في تحديد مدى استيعاب النصوص الجزائية التقليدية لجرائم التجسس التقني في ظل الصراع القائم بين قاعدة الإحالة الفنية في التجريم ومبدأ الشرعية الجنائية الأمر الذي قد يحول دون استغراق قانون حماية أسرار الدولة ووثائقها لتجريم التجسس إذا ارتكب بصورة إلكترونية، ومع إصدار قانون الجرائم الإلكترونية بصورته المستحدثة، تم بناء نموذج قانوني جديد لجريمة التجسس بصورة غيرت من طبيعته القانونية، وعليه انبثق عن هذا الإشكال تساؤلات عديدة ومنها:

١. ما المقصود بالتجسس التقني بالنظر إلى أركان وعناصر تجريمه؟
٢. ما طبيعة أفعال التجسس بالنظر إلى نموذجه القانوني؟
٣. ما مدى كفاية النصوص الواردة في قانون حماية أسرار الدولة ووثائقها لمواجهة الصور المستحدثة لجرائم التجسس؟
٤. ما مدى نجاح الخطة الجزائية التي رسمها المشرع الأردني في مواجهة التجسس التقني بكافة أنماطه؟

أهداف الدراسة:

تسعى دراسة تجريم التجسس التقني في التشريع الجزائي الأردني إلى تحقيق مجموعةٍ من الأهداف تعالج إشكالية الدراسة وتجيب على تساؤلاتها، ومن أبرزها:

١. بيان ماهية التجسس التقني وتحديد مدلول الأسرار والوثائق محل الجريمة.

٢. بيان طبيعة جرائم التجسس التقني وتحديد نوعها بالنظر إلى عنصر النتيجة في ركنها المادي.
٣. تصور مدى استغراق قانون حماية أسرار الدولة ووثائقها لجرائم التجسس المرتكبة بالوسائل الإلكترونية.
٤. تحديد مدى فاعلية السياسة الجزائية التي انتهجها المشرع الأردني في مواجهة التجسس التقني.

منهجية الدراسة:

إيفاء للغرض المقصود من الدراسة، وللإجابة عن تساؤلاتها، اتبع الباحث المنهج الوصفي والمنهج التحليلي، من خلال عرض النصوص القانونية المجرمة للتجسس التقني وبيان نموذجه وطبيعته القانونية، وتحليل مضمون هذه النصوص للوقوف على شروط تجريم التجسس وتحديد عناصره والسياسة الجزائية التي اتبعها المشرع الأردني في مواجهته، في ظل اختلاف مدلول التجسس ومحله بين قانون حماية أسرار الدولة ووثائقها وقانون الجرائم الإلكترونية.

تقسيم الدراسة:

للإجابة عن التساؤلات المطروحة، تم تقسيم الدراسة إلى أربعة مباحث على النحو التالي:

المبحث الأول: ماهية التجسس التقني.

المبحث الثاني: النموذج القانوني لجريمة التجسس التقني.

المبحث الثالث: مدى استيعاب قانون حماية أسرار ووثائق الدولة لجريمة التجسس التقني.

المبحث الرابع: الجزاءات القانونية المقررة لجرائم التجسس التقني.

المبحث الأول:
ماهية التجسس التقني

يعتبر التجسس التقني مصطلح مستحدث يطرح العديد من الإشكاليات المتعلقة بمفهومه؛ إذ يعدُّ من أكثر المصطلحات المعاصرة غموضاً بالنظر لصعوبة تحديد ماهية التجسس التقليدي أساساً، لذا لا بد من بحث مفهوم التجسس التقني، وتحديد طبيعته القانونية، فمن مرتكزات السياسة التجريمية في مواجهة التجسس التقني اعتباره من جرائم الخطر كجريمة شكلية لا تتطلب نتيجة، اذا تمت هذه الجرائم

عبر الدخول إلى الموقع الإلكتروني، وهذا استثناء على الأصل العام، ومن جانب آخر اعتبر المشرع الجزائي الأردني جرائم التجسس من الجرائم الماسة بأمن الدولة، وذلك لخصوصية هذا النوع من الجرائم وخطورة أثره على سلامة الدولة وأمنها ومصالحها.

المطلب الأول: مفهوم التجسس التقني

حاول فقهاء القانون الجنائي وضع مفهوم أو تعريف موحد للتجسس التقني، إلا أن التعريفات ظهرت متباينة وتعتمد على قانون الدولة الذي تمت دراسة أحكامه، لأنَّ السياسة التشريعية في تجريم التجسس تختلف من دولة لأخرى (المراغي، ١٩٩٨، ٩١). وعلى أي حال يقصد بالتجسس التقني استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني إلى أنظمة المعلومات الإلكترونية الخاصّة بالحكومة، والتنصت عليها بقصد الحصول على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها، وتشمل جميع أنواع المعلومات العسكرية والأمنية والسياسية والاقتصادية والعلمية والاجتماعية (سلامي، ٢٠١٩، ص٢٧).

أما عن المفهوم التشريعي للتجسس التقني، من المعروف بأن القانون لا يعرف الجريمة، وهذا الأمر من وظيفة الفقه والقضاء، إلا أنه يستفاد من الصياغة التشريعية للنص المجرم بأن التجسس التقني هو الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس المصلحة أو الأمن الوطني من خلال الدخول أو الوصول غير المشروع إلى الموقع الإلكتروني أو الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها يعود للوزارات أو الدوائر الحكومية أو المؤسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤).

أما عن التعريف القضائي للتجسس التقني، فلم نجد أي مبدأ أو اجتهاد أو حكم قضائي يعّرف التجسس التقني أو الإلكتروني إطلاقاً لغاية هذه اللحظة، ربما يعود ذلك لحداثة الجريمة نسبياً أو لقلة عدد مرات ارتكابها، الأمر الذي يحول دون مواجهة القضاء الجزائي لها كثيراً على أرض الواقع.

المطلب الثاني: الطبيعة القانونية لجريمة التجسس التقني

للحديث عن طبيعة أفعال التجسس التقني لا بد أولاً من التمييز بين نوعين من الجرائم؛ النوع الأول الجرائم المادية (جرائم الضرر) وهي الجرائم التي لا يكتمل نموذجها القانوني الا بتحقق النتيجة

الإجرامية، فهذه النتيجة تعتبر عنصراً أساسياً في النموذج القانوني للركن المادي؛ فالجريمة لا تقوم دونه (أبو العثم، ٢٠١٩، ص٣٩).

أما النوع الثاني من الجرائم يسمى بالجرائم الشكلية (جرائم الخطر) وهي الجرائم التي يكتمل شكلها القانوني بمجرد القيام بالسلوك الإجرامي دون الحاجة إلى وقوع نتيجة، فالمصلحة التي يحميها القانون تتعرض للخطر بمجرد ارتكاب السلوك المجرم (الصغير، ٢٠١١، ص١٥٣).

تبنى المشرع الأردني في المادة ٤/ج من قانون الجرائم الإلكترونية موقفه السابق الذي سلكه في قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥ حين اعتبار "الاطلاع" هدف وغاية وليس نتيجة متحققة، إذا ارتكب التجسس عبر موقع إلكتروني، حيث نصت المادة المذكورة على أنه: "يعاقب كل من دخل أو وصل قصدا إلى موقع إلكتروني يعود للوزارات ... بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني".

لعل أهم ما يميز جريمة التجسس التقني التي ترتكب عبر الموقع الإلكتروني أنها من جرائم الخطر الذي لم يشترط فيها المشرع تحقيق نتيجة، ذلك فإن الاطلاع على محتوى غير متاح للجمهور هو هدف وليس نتيجة، فيكفي أن تكون غاية الجاني من الدخول الاطلاع على البيانات أو المعلومات محل الجريمة حتى وإن لم يطلع الجاني عليها فعلاً.

تعدُّ جرائم التجسس من جرائم الخطر سواء ارتكبت بصورتها التقليدية خلافاً لأحكام قانون حماية أسرار ووثائق الدولة أم ارتكبت بصورتها المستحدثة خلافاً لأحكام قانون الجرائم الإلكترونية، إذا ارتكبت عبر الموقع الإلكتروني للمؤسسة الرسمية.

منح قانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣ جريمة التجسس التقني خصوصية معينة إذا استهدفت الموقع الإلكتروني، لأن المواقع الإلكترونية تحتوي كماً كبيراً من البيانات والمعلومات الحساسة والمتعلقة بأسرار الدولة وأمنها القومي (الجبرة، ٢٠٢١، ص٣٦٢)، فالموقع الإلكتروني هو في الأصل "حيز لإتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد" (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٢).

لذا يحدد مكان الدخول غير المشروع نوع جريمة التجسس فيما إذا كانت ضرر مشترط أم خطر مفترض، فإذا دخل المستخدم إلى الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها يشترط أن يطلع فعلاً على البيانات أو المعلومات محل الجريمة والتجسس التقني هنا

يعتبر جريمة ضرر، أما إذا دخل المستخدم إلى الموقع الإلكتروني فلا يشترط أن يطلع فعلاً على البيانات أو المعلومات محل الجريمة، ولكن شريطة أن يتوافر لديه قصد الاطلاع على خلاف ما هو عليه الحال بالنسبة للدخول إلى الشبكة المعلوماتية أو نظام المعلومات أو تقنية المعلومات كما أسلفناه من ذكر (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/ج).

وبالرغم من ذلك، فإذا دخل المستخدم إلى الموقع الإلكتروني، ولم يطلع فعلاً على البيانات أو المعلومات السرية التي يحوزها هذا الموقع، ولم يتوافر لديه قصد الاطلاع على هذه البيانات أو المعلومات، يكون أمام جريمة الدخول أو الوصول قصداً دون تصريح. وعليه فإن عدم قيام النموذج القانوني لجريمة التجسس التقني عبر الدخول إلى موقع إلكتروني لا تعني بالضرورة الحيلولة دون المسؤولية الجزائية (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٣).

ولم يشترط المشرع في قانون حماية أسرار ووثائق الدولة لقيام جريمة التجسس أن يستطيع الجاني الحصول على السر، فهذه الجريمة من جرائم الخطر المبكر التي ساوى فيها المشرع بين الفعل والشروع به بدليل قوله: "من دخل أو حاول الدخول إلى مكان محظور قصد الحصول على أسرار"، وإذا استطاع الجاني الحصول على الأسرار، ننتقل مباشرة إلى نصّ المادة ١٥ من قانون حماية أسرار ووثائق الدولة والتي نصّت على أنه: "من سرق أسرار أو أشياء أو وثائق أو معلومات كالتي ذكرت في المادة السابقة" (النوايسة، والعدوان، ٢٠١٩، ص٤٧١).

وبالنتيجة، تعتبر جرائم التجسس التقني المرتكبة عبر الموقع الإلكتروني (جرائم خطر)، كذلك الأمر بالنسبة لجريمة الدخول إلى مكان محظور قصد الحصول الأسرار خلافاً لأحكام المادة ١٤ من قانون حماية أسرار ووثائق الدول، وعلى النقيض من ذلك تعتبر جرائم التجسس التقني المرتكبة عبر الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها (جرائم ضرر).

أحسن المشرع الأردني في سياسته الجزائية القائمة على توسيع دائرة التجريم من خلال اعتبار بعض جرائم التجسس من جرائم الخطر (قانون حماية أسرار ووثائق الدولة، المادة ١٤ وقانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/ج) وذلك بصورة تخلق حماية جزائية احتياطية تواجه محاولة الاطلاع على البيانات والمعلومات السرية الخاصّة بأمن الدولة وسلامتها.

المطلب الثالث: اعتبار جرائم التجسس من الجرائم الماسة بأمن الدولة

كان قانون العقوبات الأردني رقم ١٩٦٠ ينصّ في المادة ١٢٤ منه على جريمة التجسس إلى حين

إلغائها بموجب المادة ١٧ من قانون حماية أسرار ووثائق الدولة رقم ٥٠ لسنة ١٩٧١، والنص عليها في المواد ١٤-١٦ من القانون الأخير بصورة تشير إلى خصوصية هذه الجريمة وخطورتها، كونها تمس الأسرار والأشياء والوثائق المحمية والمعلومات التي يجب أن تبقى سرية حرصاً على سلامة الدولة وأمنها.

منح المشرع الاختصاص القضائي في نظر جرائم التجسس لمحكمة أمن الدولة سنداً لأحكام المادة ٣/أ/٢ من قانون محكمة أمن الدولة حيث نصّت على أنه: "على الرغم مما ورد في أي قانون آخر تختص محكمة أمن الدولة بالنظر في الجرائم المبينة أدناه التي تقع خلافاً لأحكام القوانين التالية أو ما يطرأ عليها من تعديل يتعلق بهذه الجرائم أو ما يحل محلها من قوانين: جرائم التجسس الواقعة خلافاً لأحكام المواد (١٤) و(١٥) و(١٦) من قانون حماية أسرار ووثائق الدولة رقم (٥٠) لسنة ١٩٧١".

إلا أن قانون محكمة أمن الدولة لم يمنح الاختصاص لهذه المحكمة في النظر بجرائم التجسس المنصوص عليها في المادة ٤ من قانون الجرائم الإلكترونية؛ ولعل السبب في ذلك أن قانون جرائم أنظمة المعلومات صدر أول مرة في سنة ٢٠١٠ حين أن قانون محكمة أمن الدولة كان آخر تعديل قد طرأ عليه في سنة ٢٠١٤، الأمر الذي يحتمل معه منح الاختصاص بنظر جرائم التجسس التقني لمحكمة أمن الدولة عند أول تعديل سيطرأ على قانونها، وهذا ما لم يحصل في الاصدار الأخير لقانون الجرائم الإلكترونية لسنة ٢٠٢٣، الأمر الذي يدحض هذا الاحتمال.

فقد كان قانون جرائم أنظمة المعلومات السابق ينص على جريمة التجسس التقني، فلو أراد المشرع منح الاختصاص بنظرها لمحكمة أمن الدولة لفعل ذلك، حيث إن آخر تعديل لقانون محكمة أمن الدولة كان في سنة ٢٠١٤، في حين أن التجسس التقني كان منصوصاً عليه آن ذاك في قانون جرائم أنظمة المعلومات منذ سنة ٢٠١٠.

نرى بأن جرائم التجسس بنوعيه (التقني والتقليدي) تعتبر من الجرائم الماسة بأمن الدولة، كون محل الجريمة وموضوعها هي الأسرار والوثائق المحمية والمعلومات التي يجب أن لا تكون متاحة للجمهور، حرصاً على سلامة الدولة وأمنها وحفاظاً على مصالحها على الصعيد العسكري والاقتصادي والسياسي والدبلوماسي؛ حيث تقتضي خصوصية جرائم التجسس الماسة بأمن الدولة تحقيق حماية جزائية إجرائية أكبر لهذه الأسرار، فلا يكفي التجريم الموسّع والعقاب المشدد، ما لم تختص محكمة أمن الدولة بنظر هذه الجرائم.

المبحث الثاني:
النموذج القانوني لجريمة التجسس التقني

تتكون جريمة التجسس التقني التي نصّت عليها المادة ٤ من قانون الجرائم الإلكترونية من ثلاثة أركان رئيسية تتمثل بالركن المادي القائم على ثلاثة عناصر: سلوك ونتيجة وعلاقة سببية، وركن المحل الخاص بالمحتوى الإلكتروني المتمثل بالبيانات أو المعلومات التي تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، والركن المعنوي القائم على القصد الجنائي العام بعنصريه العلم والإرادة.

المطلب الأول: الركن المادي لجريمة التجسس التقني

لكل جريمة ركن مادي لا تقوم دونه، والركن المادي في جريمة التجسس التقني يتكون كأصل عام من ثلاثة عناصر: وهي الدخول غير المصرح به أو بما يخالف أو يجاوز التصريح إلى موقع إلكتروني أو الشبكة المعلوماتية أو نظام معلومات أو تقنية 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 (السلوك الجرمي)، والاطلاع على المحتوى الإلكتروني (النتيجة الجرمية) و(علاقة السببية) التي تربط النتيجة بالسلوك، ونوضح آتياً كل عنصر من هذه العناصر على حدةٍ:

الفرع الأول: السلوك الجرمي المتمثل بالولوج غير المشروع عبر وسائل التقنية

جرم المشرع الجزائي الأردني الدخول غير المشروع إلى المساكن أو الأماكن الخاصة أو ملحقاتها دون إذن صاحبها أو المنتفع بها، كما جرم المكوث في هذه الأماكن خلافاً لإرادة من له الحق في إقصائه عنها، (قانون العقوبات الأردني، المادة ١/٣٤٧). وهذا النوع من الدخول المجرم لا يثير أي إشكال، لأنه دخول مادي إلى أماكن في العالم الواقعي، بخلاف الولوج إلى العالم الافتراضي (الفضاء الإلكتروني) الذي لا يوجد فهم مشترك لمعناه؛ والسبب في ذلك أن الدخول أو الوصول الافتراضي مصطلح فني تقني (النوايسة والعدوان، ٢٠١٩، ص٤٧٣) الأمر الذي يستدعي بيان الدخول والوصول المقصود من جهة وانعدام التصريح أو تجاوز أو مخالفة التصريح من جهة أخرى، بالإضافة إلى استعراض وسائل التقنية المرتبطة بالسلوك المجرَّم.

أولاً: الدخول أو الوصول

سبق الحديث عن فكرة الدخول بصورته التقليدية (الدخول الواقعي) في المادة ١٤ من قانون حماية أسرار ووثائق الدولة؛ ففعل الدخول أو محاولة الدخول الواقعي يعني "كل نشاط يقوم به الجاني بهدف الوصول أو التواجد في المكان المحظور عليه دخوله"، والدخول هنا ينصرف معناه إلى الدخول المادي بانتقال الجاني جسدياً إلى داخل المكان المحظور عليه دخوله بغض النظر عن وسيلة الدخول وشرعيتها (الدروبي، ٢٠١٢، ص٧٥).

ولكن يثور التساؤل حول فكرة الدخول الافتراضي الواردة في المادة ٤ من قانون الجرائم الإلكترونية؟ جرمت المادة ٤ من قانون الجرائم الإلكترونية الدخول أو الوصول دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها للاطلاع على بيانات أو معلومات غير متاحة للجمهور.

في الحقيقة، لم يعرف قانون الجرائم الإلكترونية الدخول أو الوصول، وحسناً ما قام به، لأن تجريم الدخول أو الوصول غير المصرح به للنظام المعلوماتي يرتبط بأمور تقنية متغيرة ومتطورة، فتعريف مثل هذه المصطلحات قد يحد من التجريم لعجز التعريف عن مجاراة واستيعاب المستجدات التكنولوجية (النوايسة والعدوان، ٢٠١٩، ص٤٧٤).

عرفت المذكرة الإيضاحية لقانون جرائم أنظمة المعلومات الذي تم إلغاؤه بموجب قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥ الدخول غير المشروع على أنه: "التطفل أو القرصنة على موقع إلكتروني أو نظام معلومات، غير متاح للعموم الدخول إلى أي منها دون تصريح أو بما يخالف أو يجاوز التصريح".

ترك المشرع الأردني مسألة تعريف المصطلحات القانونية للفقه الجنائي حيث عرف الدخول بأنه: "كافة الأفعال التي تسمح بالولوج إلى نظام معلوماتي أو نظام معالجة آلية للبيانات باستخدام الحاسوب أو الإحاطة أو السيطرة على المعطيات التي تتكون منها هذه الأنظمة أو الخدمات التي تقدمها (بن يونس، ٢٠٠٤).

في الحقيقة أدرج الاستحداث الأخير لقانون الجرائم الإلكترونية الأردنية رقم (١٧) لسنة ٢٠٢٣ مصطلح جديد إلى جانب الدخول الذي اكتفى به قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥ سابقاً، وهو "الوصول" وهذا المصطلح جديد على الساحة القانونية على مستوى التشريع والفقه والقضاء.

وعودة إلى المدلول اللغوي لكلمة وصل نجد بأن: وصَلَ إلى يصِل، صِلْ، صِلَةً ووُصولاً، فهو واصل، والمفعول مَوْصول، وصَلَ الشَّخصُ إلى المكان/ أي بلَغه، انتهى إليه (موقع معجم المعاني، ٢٠٢٤).

للوهلة الأولى نرى بأن الدخول والوصول مصطلحان رديفان فكلاهما يعني الاختراق أو الولوج غير المشروع، ولكن عند قراءة نص المادة ٤/أ من قانون الجرائم الإلكترونية الأردنية رقم (١٧) لسنة ٢٠٢٣ الذي نصَّ على أنه: "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"، نلاحظ بأن المشرع قد تصور مجرد الوصول إلى أي جزء من الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات، فيكفي الوصول إلى جهاز الحاسوب إذا كان مثبتاً على سطح مكتبه برنامج يحتوي معلومات محمية تمس الأمن الوطني.

إذاً فالوصول هو مصطلح أشمل من الدخول، ذلك أن الدخول يعني بالضرورة الوصول، والعكس غير صحيح، وإذا ما تصورنا الأمر على أرض الواقع، فإن عدم دخول الجاني مسكن المجني عليه لا يعني بالضرورة عدم الوصول إليه، فقد يصل إليه ولكن لا يدخل.

والجدير بالذكر أن المشرع الجزائي الأردني لم يشترط وسيلة معينة في الدخول بدلالة المادة ٣/أ من قانون الجرائم الإلكترونية حيث نصّت 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"؛ لذا فقد يتم الدخول بشكل مباشر أو غير مباشر كما هو الحال في الدخول عن بعد عن طريق شبكات الاتصالات والتقنيات الحديثة.

ثانياً: انعدام التصريح أو تجاوز أو مخالفة التصريح

عرف المشرع الجزائي الأردني التصريح في قانون الجرائم الإلكترونية على أنه: "الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول أو الوصول إلى نظام المعلومات أو تقنية المعلومات أو الشبكة المعلوماتية أو استخدامها" (قانون الجرائم الإلكترونية، المادة ٢).

يعني عدم التصريح أي عدم وجود إذن للدخول إلى نظام المعلومات بشكل مطلق، فيصبح الدخول إليه ممنوعاً تحت طائلة العقاب سواء كان الدخول مباشر أو غير مباشر، وسواء كان الدخول كلياً أو جزئياً، وسواء كانت مدة الدخول قصيرة أم طويلة، إذا توافر القصد الجنائي العام بأن يكون هذا الدخول مقصوداً.

وتجدر الإشارة إلى أن تجاوز التصريح يعني بأن المستخدم مصرح له بالدخول أو الوصول ابتداءً، ولكنه يمكث على الموقع الإلكتروني الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها مدة زمنية أكثر من المدة المحددة له في تصريح الدخول مع علمه بذلك (محمود، ٢٠٢٠، ص١٧٧).

وتعني مخالفة التصريح بأن المستخدم مصرح له بالدخول أو الوصول ابتداءً ولكنه يدخل أو يصل إلى جزء من الموقع الإلكتروني الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها غير ذلك الجزء المصرح للمستخدم الدخول إليه، حيث يعتبر ذلك دخول غير مشروع.

فالدخول أو الوصول المجرم أصبح يستغرق الولوج دون تصريح أو بمخالفة التصريح أو بتجاوز التصريح (النعيمي، ٢٠٢١، ص٥٣)؛ وعلى ذلك أراد المشرع توفير حماية جزائية أكبر للأنظمة والشبكات الإلكترونية والبيانات والمعلومات المخزنة عليها، سيما وأن هذه البيانات أو المعلومات سرية تتعلق بأمن الدولة ومصالحها.

توسع المشرع الجزائي الأردني بتجريم أفعال الدخول التي ترتكب بوسائل إلكترونية، حيث تشمل: "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..".

أحسن المشرع الجزائي الأردني عند تجريمه للتجسس بشمول الدخول أو الوصول إلى الموقع الإلكتروني أو الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها حتى وان كان مصرح به، سعياً من المشرع في تحقيق حماية جزائية لأي بيانات أو معلومات تمس أمن الدولة، ذلك أن الدخول إلى الشبكة المعلوماتية قد يكون من قبل أشخاص مصرح لهم الدخول إليه دون أن يكون لهم صلاحيّة الاطلاع على هذه البيانات أو المعلومات غير المتاحة للجمهور.

ثالثاً: وسائل التقنية المرتبطة بالدخول المجرم

تتميز الجرائم الإلكترونية عن غيرها من الجرائم بأنها تتم عبر الفضاء الإلكتروني، وهذا ضابط التفرقة بين التجسس المجرم خلافاً لقانون حماية أسرار ووثائق الدولة والتجسس المجرم خلافاً لأحكام

قانون الجرائم الإلكترونية، ذلك أن التجسس بنوعه الأخير يركن الجاني في ارتكابه إلى الدخول إلى الشبكة المعلوماتية أو نظام المعلومات (Al-Shawabkeh, 2024, Criminalizing..).

لاكتمال البنيان القانوني لجريمة التجسس الإلكتروني لا بد أن يكون الدخول غير المشروع إلى الشبكة المعلوماتية أو نظام المعلومات أو تقنية المعلومات، أو الموقع الإلكتروني حيث نصّت المادة ٤/أ من قانون الجرائم الإلكترونية بمعرض تجريمها للتجسس التقني 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

ا يعود للوزارات.."، كما نصّت الفقرة ج من المادة ذاتها على أنه: "يعاقب كل من دخل قصداً إلى موقع إلكتروني يعود للوزارات..".

يلاحظ الباحث من خلال النصوص المذكورة بأن قانون الجرائم الإلكترونية اشترط في ارتكاب جريمة التجسس أن يكون الدخول إلى شبكة معلوماتية أو نظام معلومات أو تقنية معلومات أو موقع إلكتروني، الأمر الذي يقتضي التطرق إلى وسائل التقنية المرتبطة بالدخول المجرم على النحو الآتي:

١- الشبكة المعلوماتية

عرفت المادة ٢ من قانون الجرائم الإلكترونية الشبكة المعلوماتية بأنها: "ارتباط بين أكثر من نظام معلومات أو أي وسيلة من وسائل تقنية المعلومات لإتاحة البيانات والمعلومات والحصول عليها".

ويبدو أن المشرع الأردني أخذ هذا المفهوم من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٢ والتي صادقت عليها الأردن بموجب قانون التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم ١٩ لسنة ٢٠١٢، حيث عرفت المادة الثانية من هذه الاتفاقية الشبكة المعلوماتية بأنها: "ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها".

وعليه فإن الشبكة المعلوماتية إذاً عبارة عن أنظمة ووسائل تقنية مترابطة مع بعضها البعض تشكل شبكة معلوماتية متكاملة يتم من خلالها الوصول إلى البيانات والمعلومات، وهذه البيانات والمعلومات التي تتيحها الشبكة المعلوماتية قد تكون محل الولوج في جريمة التجسس التقني، إذا كانت بيانات أو معلومات سرية غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.

٢- تقنية المعلومات

عرفت المادة ٢ من قانون الجرائم الإلكترونية تقنية المعلومات بأنها: "جميع أشكال تسيير أنظمة المعلومات، التي تعتمد على الحواسيب أو الهواتف الخلوية أو البرمجيات أو أوامر برمجية أو أية

أجهزة إلكترونية أخرى، لتحويل أو تخزين أو حماية أو معالجة أو إرسال أو استرجاع أو إدارة أو تبادل للمعلومات أو البيانات وأي وسيلة أخرى تحقق الغاية ذاتها".

في حين عرفت المادة ٢ من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٢ تقنية المعلومات بأنها: "أية وسيلة مادية أو معنوية أو مجموعة وسائل مرتبطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة".

نلاحظ بأن التعريف الأخير أوضح من التعريف الأول رغم انهما يحملان المعنى ذاته، لذا ولما كان استخدام الوسائل الإلكترونية أساس للتجريم في التجسس التقني وعنصر من عناصره، لقد تصور المشرع ارتكاب هذه الجريمة بالولوج إلى تقنية 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، إذا كان الدخول أو الوصول غير المشروع منصباً على معلومات أو بيانات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.

٣- نظام المعلومات

عرفت المادة ٤ من قانون الجرائم الإلكترونية نظام المعلومات بأنه: "مجموعة البرامج أو التطبيقات او منصات التواصل الاجتماعي أو الأجهزة أو الأدوات المعدّة لإنشاء البيانات أو المعلومات إلكترونياً، أو المعدة لإرسال هذه البيانات أو المعلومات أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية".

ويمتاز نظام المعلومات بأنه مجموعة من الموارد والعناصر المرتبطة التي تتفاعل مع بعضها البعض داخل إطار معين وتعمل كوحدة واحدة نحو تحقيق هدف أو مجموعة من الأهداف، وفي كل دائرة أو مؤسسة عامة سواء كانت عسكرية أم مدنية يوجد نظام أو مجموعة أنظمة في ظل التحول الرقمي السريع الذي تشهده الدولة الأردنية.

ولما كان نظام المعلومات مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات، فقد اعتبر المشرع الجزائي الأردني هذا النظام أساساً لتجريم التجسس التقني ووسيلة من وسائله، فغالباً ما

يتم تخزين البيانات والمعلومات السرية غير المتاحة للجمهور على النظام الخاص لكل من الوزارات والدوائر والمؤسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة.

بالتالي، تقوم جريمة التجسس التقني بالولوج غير المشروع إلى نظام المعلومات للاطلاع على ما تحتويه أو تخزنه أو تعالجه أو تديره أو تعرضه أو ترسله من بيانات أو معلومات إذا كانت متاحة للجمهور وتمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.

٤- الموقع الإلكتروني

عرفت المادة ٢ من قانون الجرائم الإلكترونية الموقع الإلكتروني بأنه: "حيز لإتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد"، ويعرفها البعض بأنها ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على البيانات والمعلومات وتبادلها (محمود، ٢٠٢٠، ١٧٨).

إن المواقع الإلكترونية المحلية والدولية الرسمية والعامة في تزايد مستمر؛ فكل عنوان يتيح حيزه بيانات أو معلومات على الشبكة المعلوماتية يعتبر بالمدلول القانوني موقعاً إلكترونياً AlShawabkeh, (2024, 8).

يفرض نظام العمل الجديد بالمؤسسات الرسمية المدنية منها والعسكرية (مكاتب بلا ورق) استخدام موقع إلكتروني، وذلك لكثرة مزايا هذا النظام وندرة عيوبه، وعليه فقد ازداد استخدام المواقع الإلكترونية في مؤسسات العامة، مما حدا بالمشرع الأردني لتجريم التجسس إذا وقع بالولوج غير المشروع عبر الموقع الإلكتروني الخاص بالوزارات أو الدوائر والمؤسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة في حال الاطلاع على بيانات أو معلومات تحوزها هذه المواقع إذا كانت غير متاحة للجمهور وتمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامّة أو الاقتصاد الوطني.

والجدير بالذكر بأن المشرع الجزائي الأردني جعل الاطلاع على البيانات أو المعلومات السرية التي يحوزها الموقع الإلكتروني هدفاً وليس نتيجة، حيث اعتبر المشرع التجسس التقني في هذا الصدد جريمة خطر تهدد الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/ج).

الفرع الثاني: النتيجة الجرمية المتمثلة بالاطلاع على محتوى إلكتروني غير متاح للجمهور

لا يكفي الدخول غير المشروع إلى نظام أو تقنية أو شبكة المعلومات العائدة إلى الدولة لتقوم جريمة التجسس التقني ما لم يطلع الجاني على البيانات أو المعلومات غير المتاحة للجمهور (السرية) التي تمس الأمن الوطني، حيث قال المشرع: "..واطلع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.." (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/أ).

يتضح من خلال استخدام المشرع لـ (و) العطف في النص المطروح الذي جاء عقب الدخول غير المشروع إلى اعتبار اطلاع الجاني على البيانات أو المعلومات عنصر نتيجة إلى جانب عنصر النشاط المتمثل بالدخول، حيث لا يمكن أن يقوم الركن المادي لجريمة التجسس إلا بتحقق هذين العنصرين معاً.

والجدير بالذكر أن الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني تتمثل به النتيجة كعنصر من عناصر الركن المادي في جريمة التجسس التقني، بحيث لا يكتمل النموذج القانوني لجريمة التجسس التقني إلا بتحقق النتيجة الجرمية القائمة على الاطلاع على هذه البينات أو المعلومات المشار إليها.

في الحقيقة هذا توجه حديث للمشرع في قانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣، حيث إن قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥ لم يكن ينظر إلى الاطلاع سوى أكثر من هدف للجريمة، فلم يكن يشترط آنذاك حدوث الاطلاع على البيانات والمعلومات محل التجسس في التجريم.

ونذكّر بأن هناك استثناء على هذا الأصل العام، حيث إن جريمة التجسس التقني قد تقوم بدون تحقيق النتيجة المتمثلة بالاطلاع فعلاً على البيانات أو المعلومات غير المتاحة للجمهور إذا كان الولوج غير المشروع واقعاً على موقع إلكتروني حيث اعتبر المشرع التجسس في هذا الصدد من جرائم الخطر (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/ج).

الفرع الثالث: علاقة السببية

جريمة التجسس التقني شأنها شأن باقي الجرائم يحتاج الركن المادي فيها علاقة سببية تربط النتيجة بالسلوك، حيث يجب أن تكون النتيجة الجرمية المتمثلة بالاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني.

ويجب أن تكون النتيجة تحققت بسبب دخول الجاني أو وصوله 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.

والجدير بالذكر أن الاستثناء المشار إليه في عنصر النتيجة الجرمية سالفاً يسري أيضاً على العنصر الخاص بعلاقة السببية، إذا كان الولوج غير المشروع واقعاً على موقع إلكتروني، حيث إن جريمة التجسس التقني هنا قد تقوم دون تحقيق النتيجة المتمثلة بالاطلاع فعلاً على البيانات أو المعلومات غير المتاحة للجمهور، وإذا قام النموذج القانوني لجريمة التجسس التقني دون تحقق النتيجة فلا داعي لرابطة سببية ولا حاجة لها، حيث لا يوجد نتيجة حتى نربطها بالسلوك الجرمي المجرد.

جرم المشرع الجزائي الشروع في جريمة التجسس التقني رغم أنها جنحة، حيث يسأل جزائياً من يدخل إلى الشبكة المعلوماتية أو تقنية أو نظام المعلومات يعود لمؤسسة رسمية ومن ثم يحاول الاطلاع على معلومات غير مسموح للجمهور الاطلاع عليها لتعلقها بالأمن الوطني، أو العلاقات الخارجية للمملكة، أو السلامة العامة، أو الاقتصاد الوطني؛ لأن هذه الجرائم الجنحية ورد عليها استثناء بموجب نص خاص في قانون الجرائم الإلكترونية يعاقب على محاولة ارتكاب جرائم التجسس التقني مهما كان وصفها (قانون الجرائم الإلكترونية، المادة ٤/هـ).

يقوم النموذج القانوني لجريمة التجسس عبر الموقع الإلكتروني بمجرد الدخول إليه بقصد الاطلاع على ما يحوزه من معلومات دون الحاجة إلى تحقق هذا الاطلاع فعلاً، ولكن تظهر الإشكالية في حال محاولة (الدخول إلى الموقع الإلكتروني بقصد التجسس) مع عدم التمكن من هذا الدخول ابتداءً، حيث لا يكتمل النموذج القانوني لجريمة التجسس التقني على الفرض الأخير؛ مما يعيدنا إلى ضرورة قيام المشرع في تجريم محاولة الدخول غير المشروع إلى الموقع الإلكتروني بهدف التجسس، وحسناً ما فعله المشرع بذلك فيما استحدثه في قانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣، حيث جرمت المادة ٤/هـ منه محاولة ارتكاب أي من جرائم التجسس، بحيث يعتبر الشارع بالجريمة فاعلاً لها تماماً.

المطلب الثاني: محل جريمة التجسس التقني

يتمثل محل الجريمة في التجسس التقني في البيانات أو المعلومات غير المتاحة للجمهور والتي تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، ويخلق

محل الجريمة (البيانات والمعلومات السرية) في هذا الصدد معياراً لتمييز جريمة التجسس التقني عن جريمة الدخول المجرد المنصوص عليها في المادة ٣ من قانون الجرائم الإلكترونية، ذلك أن جريمة التجسس غير متصورة إلا بالدخول المقترن بالاطلاع على هذه البيانات أو المعلومات بموجب نص المادة ٤ من ذات القانون.

ولا بد من الإشارة إلى أن المحتوى غير المتاح للجمهور يقتضي أن يكون مؤمن بوسائل حماية إلكترونية ومحفوظ في موقع أو نظام أو شبكة معلومات حكومية، فكل ما يمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني هو اعتداء على أمن الدولة وسلامتها، الأمر الذي دفع الجهات المختصة إلى عدم إتاحة هذه المعلومات والبيانات للعامة (النوايسة والعدوان، ٢٠١٩، ص٤٧٦).

المطلب الثالث: الركن المعنوي المتمثل بالقصد العام

جريمة التجسس التقني يكفي فيها توافر القصد الجنائي العام القائم على عنصري العلم والإرادة، حيث يجب أن يعلم الجاني بأنه يريد الدخول بشكل غير مشروع 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 ويريد أيضاً الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني، كما يجب أن يعلم الجاني بذلك كله (أركان وعناصر جريمة التجسس التقني).

والجدير بالذكر بأن المشرع لا يتطلب سوى القصد العام لقيام النموذج القانوني لجريمة التجسس كأصل عام، وبالرغم من ذلك فقد جعل من التجسس التقني المقرون بقصد الاعتداء على البيانات أو المعلومات السرية ظرفاً مشدداً للعقوبة، فالجاني في هذه الحالة يقصد التجسس التقني على البيانات أو المعلومات السرية بصورة عامّة، ويقصد أيضاً الاعتداء على هذه البيانات أو المعلومات بصورة خاصّة، وصور الاعتداء المقصود هي: الإلغاء أو الإتلاف أو التدمير أو التعديل أو التغيير أو النقل أو النسخ أو النشر أو إعادة النشر أو خسارة السرية أو التشفير أو الحذف أو الإضافة أو الحجب أو الإفشاء أو الالتقاط (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/ب، د).

حيث قضت محكمة التمييز الأردنية بصفتها الجزائية بأن ما أقدم عليه مجموعة من المتهمين بتعطيل أجهزة الكاميرات على أحد أبراج المراقبة العسكرية لكي يتمكنوا من تنفيذ عمليات تهريب المخدرات من على الحدود الأردنية السورية يشكل كافة أركان وعناصر جريمة الدخول بدون تصريح إلى شبكة معلوماتية بقصد تعديل وتغيير بيانات ومعلومات غير متاحة للجمهور تمس الأمن الوطني (حكم تمييز جزاء، ٢٠٢٢/٤٠٩٦).

كما قضت محكمة التمييز بحكم آخر لها بأنه: ".. فنجد بأن هذا الجرم يتطلب لقيامة الأركان الآتية: الركن الأول (الركن المفترض): وهو وجود بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السلامة العامة أو الاقتصاد الوطني محفوظة في الشبكة المعلوماتية أو نظام معلومات محمي. الركن الثاني (الركن المادي): أن يكون الدخول إلى المعلومات الموجودة في شكل إلكتروني /الشبكة المعلوماتية أو نظام معلومات محمي بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها. الركن الثالث: أن يكون الدخول دون تصريح أو بما يخالف أو يجاوز التصريح. الركن الرابع (الركن المعنوي): هذه الجريمة من الجرائم المقصودة أي أن يكون الدخول بقصد إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو إفشائها" (حكم تمييز جزاء، ٢٠٢٢/٣٢٦٠).

المبحث الثالث:
مدى استيعاب قانون حماية أسرار ووثائق الدولة لجريمة التجسس التقني

قسّم المشرع الجزائي الأردني التجسس وفقاً لأحكام قانون حماية أسرار ووثائق الدولة إلى ثلاثة جرائم وهي: جريمة الدخول أو محاوله الدخول إلى مكان محظور (المطلب الأول) وجريمة الحصول على أسرار الدولة (المطلب الثاني) وجريمة إفشاء أسرار الدولة بواسطة الوظيفة أو بحكمها (المطلب الثالث) حيث تم التطرق آتياً إلى هذه الجرائم بشكل تفصيلي.

المطلب الأول: الدخول أو محاولة الدخول إلى أماكن محظورة بصورة تقنية

جرّم المشرع الجزائي الأردني الدخول أو حتى محاولة الدخول إلى أي مكان محظور دخوله بهدف الحصول على أسرار تتعلق بأمن الدولة أو سلامتها بشكل مباشر أو غير مباشر تحت طائلة العقاب؛ حيث نصّ قانون حماية أسرار ووثائق الدولة على أنه: "من دخل أو حاول الدخول

إلى مكان محظور قصد الحصول على أسرار أو أشياء أو وثائق محمية أو معلومات يجب أن تبقى سرية حرصاً على سلامة الدولة عوقب بالأشغال الشاقة المؤقتة" (قانون حماية أسرار ووثائق الدولة، ١٩٧١، المادة ١٤)

لمعرفة مدى إمكانية تجريم الدخول أو محاولة الدخول إلى أماكن محظورة بصورة تقنية لغاية التجسس لا بد من تحديد مدلول فعل الدخول أو محاولة الدخول والمكان المحظور (الفرع الأول) وبيان إمكانية تجريم الدخول أو محاولة الدخول إلى أماكن محظورة بصورة تقنية (الفرع الثاني).

الفرع الأول: مدلول فعل الدخول أو محاولة الدخول والمكان المحظور

فعل الدخول أو محاولة الدخول هو كل نشاط يقوم به الجاني بهدف الوصول أو التواجد في المكان المحظور عليه دخوله، والدخول هنا ينصرف معناه إلى الدخول المادي بانتقال الجاني جسدياً إلى داخل المكان المحظور عليه دخوله بغض النظر عن وسيلة الدخول وشرعيتها (الدروبي، ٢٠١٢، ص٧٥).

وقصد المشرع الجزائي الأردني بالمكان المحظور أي مكان تمنع السلطات المختصة عامة الناس الدخول إليه أو ارتياده أو ولوجه (الفاضل، ١٩٦٥، ص٣٥٨)، فلم يحدد المشرع في قانون حماية أسرار ووثائق الدولة الأماكن المحظورة بعينها كما أنه لم يقم بتعدادها أو ذكرها حصراً أو حتى مثالاً، وحسناً ما فعل المشرع بذلك حتى تستغرق المادة ١٤ من القانون المذكور كافة الأماكن التي يحظر دخولها بقصد التجسس، كما لو كانت هذه الأماكن افتراضية.

الفرع الثاني: تجريم الدخول أو محاولة الدخول إلى أماكن محظورة بصورة تقنية

ينطوي الدخول إلى الأماكن المحظورة المجرم في المادة ١٤ من قانون حماية أسرار ووثائق الدولة على سلوك مادي بحت، الأمر الذي يستبعد معه المشرع وقوع عملية الدخول بوسيلة تقنية إلى مكان محظور يتمثل بموقع إلكتروني محمي غير مصرح الدخول إليه؛ ذلك أن قانون حماية أسرار ووثائق الدولة لم يواكب التطور التقني والتقدم التكنولوجي الذي خلق أساليب جديدة للإجرام.

في الحقيقية جرمت المادة ٢٦ من قانون الجرائم الإلكترونية لسنة ٢٠٢٣ كل من ارتكب أي جريمة معاقب عليها بموجب أي تشريع نافذ باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني أو اشترك أو تدخل أو حرض على ارتكابها.

وبقراءة المادة ٢٦ من قانون الجرائم الإلكترونية مع المادة ١٤ من قانون أسرار وثائق الدولة،

يمكن القول: "كل من دخل أو حاول الدخول إلى مكان محظور، قصد الحصول على أسرار أو أشياء أو وثائق محمية أو معلومات يجب أن تبقى سرية حرصاً على سلامة الدولة باستخدام الشبكة المعلوماتية أو أي نظام معلومات أو موقع إلكتروني عوقب بالأشغال المؤقتة".

وعليه ومع عدم الإخلال بمبدأ الشرعية الجزائية الذي ينصّ على أنه لا جريمة ولا عقوبة إلا بنص (قانون العقوبات الأردني، المادة ٣) يمكن ارتكاب جريمة التجسس المنصوص عليها في المادة ١٤ من قانون حماية أسرار ووثائق الدولة بأي من الوسائل الإلكترونية استناداً إلى أحكام المادة ٢٦ من قانون الجرائم الإلكترونية (الشوابكة، ٢٠٢٠، ص١٤٧) خاصّة وأن نص المادة ١٤ من قانون حماية أسرار ووثائق الدولة جاء مطلقاً من كل قيد.

وما يبرر رأينا في هذا الشأن هو الغاية التي جرَّم النص أفعال التجسس من أجلها؛ وهي حماية أسرار الدولة ووثائقها الماسة بسلامتها؛ لذا من غير المعقول حماية الوثائق الورقية وإهمال حماية الوثائق الإلكترونية التي يمكن أن تكون أكثر سرية ومساساً بأمن الدولة وسلامتها، خصوصاً مع التحول الرقمي الذي تشهده مؤسسات الدولة الأردنية وأنظمة الأتمتة وصولاً إلى سياسة عمل لا ورقي، سيما وأن المادة ٢٦ من قانون الجرائم الإلكترونية خلقت شرعية لتطويع نصّ المادة ١٤ من قانون حماية أسرار ووثائق الدولة في تجريم التجسس التقني.

المطلب الثاني: سرقة الأسرار التي تتعلق بسلامة الدولة أو الحصول عليها بصورة تقنية

جرّم المشرع الجزائي الأردني سرقة أي أسرار تتعلق بأمن الدولة أو سلامتها أو الحصول عليها بشكل مباشر أو غير مباشر تحت طائلة العقاب؛ حيث نصّ قانون حماية أسرار ووثائق الدولة على أنه: "من سرق أسرار أو أشياء أو وثائق أو معلومات كالتي ذكرت في المادة السابقة أو استحصل عليها عوقب بالأشغال المؤقتة" (قانون حماية أسرار ووثائق الدولة، ١٩٧١، المادة ١٥).

لتصور جريمة سرقة الأسرار التي تتعلق بسلامة الدولة أو الحصول عليها بالوسائل الإلكترونية كصورة من صور التجسس؛ لا بد من تحديد مدلول السرقة والاستحصال (الفرع الأول) وتحديد مدلول الأسرار والأشياء والوثائق والمعلومات محل الجريمة (الفرع الثاني) وبيان مدى تجريم سرقة الأسرار التي تتعلق بسلامة الدولة أو الحصول عليها بصورة تقنية (الفرع الثالث).

الفرع الأول: مدلول السرقة والاستحصال

عرف الشرع الجزائي الأردني السرقة على أنها: "أخذ مال الغير المنقول دون رضاه، وتعني عبارة أخذ المال إزالة تصرف المالك فيه برفعه من مكانه ونقله وإذا كان متصلاً بغير منقول فبفصله عنه فصلاً تاماً ونقله، وتشمل لفظة مال القوى المحرزة" (قانون العقوبات، ١٩٦٠، المادة ٣٩٩).

يصعب تصور وقوع السرقة بمفهومها القانوني على أسرار الدولة إلا إذا تم سرقة السر أو الوثيقة بمكونها المادي كالبطاقة الذاكرة (Memory Card) أو القرص الصلب (Hard Disk) الذي يحتوي السر أو الوثيقة المحمية، وذلك باعتبار أنه أداه له قيمة مادية فحسب (نمور،٢٠٢١، ص٦٨).

أما الاستحصال فهو مفهوم أوسع وأشمل من السرقة ويعني "الوصول إلى السر والتمكن من حيازته بأي وسيلة وعلى أي وجه أو الالمام بمضمونه ومعناه من قبل شخص لا صفه له في الحصول عليه، أو احرازه معنوياً مثل الاطلاع على وثيقة سرية وحفظ معلوماتها بذاكرة العقل البشري" (الدروبي، ٢٠١٢، ص٩٢).

قضت محكمة التمييز بصفتها الجزائية بأن: "قيام المتهم بالاستحصال على معلومات سرية من درجة (سري للغاية) والتي لا يجوز افشاؤها؛ لأن ذلك يشكل خطراً على أمن وسلامة القوات المسلحة الأردنية وذلك لمنفعة دولة أجنبية يوفر أركان وعناصر جناية التجسس خلافاً لأحكام المادة (١٥/أ، ب) من قانون حماية أسرار ووثائق الدولة رقم ٥٠ لسنة ١٩٧١" (تمييز جزاء ١٩٩٦/٦٧٩).

الفرع الثاني: مدلول الأسرار والوثائق المحمية محل الجريمة

حددت المادة ١٤ من قانون حماية أسرار ووثائق لدولة محل جريمة التجسس وهو أسرار أو أشياء أو وثائق محمية او معلومات يجب ان تبقى سرية حرصاً على سلامة الدولة.

والشيء هو أي موجود مادي ملموس ثابت ومتحقق يصح تصوره والاخبار عنه، مثل أجهزة عسكرية سرية، والمعلومات هي أي معلومات سرية ذات طبيعة حربية أو سياسية أو دبلوماسية أو اقتصادية أو صناعية لا يعلم بها إلا أشخاص محددون في الدولة (نابلسي، ٢٠٢٠، ص٣٥، ٣٦).

والوثائق هي جميع أنواع الكتابات والمذكرات والتقارير والمخابرات والرسائل والخطط والرسوم وأي وثيقة مكتوبة مصنفة بدرجة السرية المحددة في قانون حماية أسرار ووثائق الدولة (الفاضل، ١٩٨٧، ص٣٦١).

عرف المشرع الجزائي الأردني الأسرار والوثائق المحمية بصورة عامّة على أنها: "أية معلومات

شفوية أو وثيقة مكتوبة أو مطبوعة أو مختزلة أو مطبوعة على ورق مشمع أو ناسخ أو أشرطة تسجيل أو الصور الشمسية والأفلام أو المخططات أو الرسوم أو الخرائط أو ما يشابهها والمصنفة وفق أحكام هذا القانون" (قانون حماية أسرار ووثائق الدولة، ١٩٧١، المادة ٢).

كما اصطلح عليها قانون ضمان حق الحصول على المعلومات بـ (الوثائق المصنفة) وعرفها بأنها: "أي معلومات شفوية أو وثائق مكتوبة أو مطبوعة أو مختزلة أو مخزنة إلكترونياً أو بأي طريقة أو مطبوعة على ورق مشمع أو ناسخ أو أشرطة تسجيل أو الصور الشمسية والأفلام أو المخططات أو الرسوم أو الخرائط أو ما يشابهها والمصنفة على أنها سرية أو وثائق محمية وفق أحكام التشريعات النافذة" (قانون ضمان حق الحصول على المعلومات، ٢٠٠٧، المادة ٢).

لم يتوسع قانون حماية أسرار الدولة بمدلول السر وقصره على المعلومات الشفوية أو الوثائق المحمية والمحفوظة بصورة تقليدية لا تعدو نسخ أشرطة التسجيل والصور الشمسية والأفلام، دون الإشارة إلى الأسرار المخزنة بصورة تقنية كما فعل قانون ضمان حق الحصول على المعلومات بمعرض تعريفه للوثائق المصنفة وتصور تخزينها بصورة إلكترونية.

الفرع الثالث: تجريم سرقة الأسرار التي تتعلق بسلامة الدولة أو الحصول عليها بصورة تقنية

نصّت المادة ١٥/أ من قانون حماية أسرار ووثائق الدولة على أنه: "من سرق أسرار أو أشياء أو وثائق أو معلومات كالتي ذكرت في المادة السابقة او استحصل عليها عوقب بالأشغال المؤقتة لمدة لا تقل عن عشر سنوات" والوثائق والمعلومات المذكورة في المادة ١٤ من هذا القانون هي: الأسرار والأشياء وأي وثائق محمية أو معلومات يجب أن تبقى سرية حرصاً على سلامة الدولة.

ورد مصطلح الاستحصال ومدلول السر بصورة واسعة على نحو يشمل صور الحصول على كافة الأسرار التي تشتمل عليها الوثائق المصنفة (المحمية)، ذلك أن أي سلوك يقوم به الجاني في سبيل الحصول على السر يجرم خلافاً لأحكام المادة ١٥ من قانون حماية أسرار ووثائق الدولة (لدادوه، ٢٠٢١، ص٧٦).

وإذا كان سلوك الجاني المتمثل في حصوله على السر متصور ارتكابه بوسيلة تقنية سواء كان السر محل التجسس محفوظ على شريط مادي أو بشكل إلكتروني، فلا مانع من استيعاب النص التقليدي لجرائم التجسس على الأسرار التي يحميها قانون حماية أسرار ووثائق الدولة إذا ما تمت بالوسائل الإلكترونية، وذلك لإطلاق ألفاظ النص دون شرط أو قيد، بالإضافة للإحالة الفنية في التجريم استناداً إلى أحكام المادة ٢٦ من قانون الجرائم الإلكترونية التي تصورت ارتكاب الأفعال المجرمة

بالنصوص الجزائية التقليدية إذا تمت بأساليب إلكترونية.

ولما كانت جريمة التجسس من جرائم القالب الحر (بهنام، ١٩٨٢، ٢١٢)، لا نرى ما يحول دون تجريم الحصول على الأسرار التي تتعلق بسلامة الدولة بصورة إلكترونية كصورة من صور التجسس التقني، سيما وأن مدلول الاستحصال أوسع من مدلول السرقة؛ فالوسيلة لم يقم لها المشرع وزناً في التجريم كأصل عام (alshawabkeh, 2024, criminalization.., p10)، مع إمكانية النظر للوسيلة المستخدمة في الجريمة المعلوماتية عند تقدير العقوبة وتغير وصفها الجرمي أحياناً.

المطلب الثالث: إبلاغ الأسرار المتعلقة بأمن الدولة أو إفشاؤها بصورة تقنية

جرّم المشرع الجزائي الأردني إبلاغ الأسرار المتعلقة بأمن الدولة وسلامتها أو إفشاءها بشكل مباشر أو غير مباشر تحت طائلة العقاب؛ حيث نص قانون حماية أسرار ووثائق الدولة على أنه: "من وصل إلى حيازته أو علمه أي سر من الأسرار أو المعلومات أو أية وثيقة محمية بحكم وظيفته أو كمسؤول أو بعد تخليته عن وظيفته أو مسؤوليته لأي سبب من الأسباب فابلغها أو أفشاها دون سبب مشروع عوقب بالأشغال.." (قانون حماية أسرار ووثائق الدولة، ١٩٧١، المادة ١٦).

لتصور جريمة إبلاغ الأسرار المتعلقة بأمن الدولة أو إفشائها بالوسائل الإلكترونية كصورة من صور التجسس؛ لا بد من تحديد مدلول تبليغ الأسرار (الفرع الأول)، ومدلول إفشاء الأسرار (الفرع الثاني)، وبيان مدى تجريم إبلاغ الأسرار المتعلقة بأمن الدولة أو إفشائها بصورة تقنية (الفرع الثالث).

الفرع الأول: مدلول تبليغ الأسرار

تبليغ الأسرار هو كل فعل من أفعال النقل أو الإخبار أو الايصال أو التسليم للسر من شخص قد يعلم به أو لا يعلم به لشخص معين بذاته، ويستهدف جرم الإفشاء شخصاً محدداً بذاته أو جهة بعينها، والجدير بالذكر أن الإبلاغ عن السر يتحقق بنشاط إيجابي فقط (الدروبي، ٢٠١٢، ص١١١-١١٢).

الفرع الثاني: مدلول إفشاء الأسرار

كل فعل من أفعال البوح أو الافصاح أو الاذاعة أو النشر للسر من شخص يعلمُ به سواء تم لجهة معينة أو لشخص معين أو لجهة أو شخص غير معين، وإفشاء السر يعني كشفه والبوح به، ولا يكون ذلك إلا من قبل شخص يعلم بالسر، فلا يتصور وقوع فعل الإفشاء من قبل من يجهل بالسر على

خلاف من يبلغ السر، حيث لا يشترط علم الأخير به (الشواربي، ٢٠٠٣، ص٨٧).

والجدير بالذكر أن الإفشاء يتحقق بسلوك إيجابي من حيث الأصل، إلا أنه قد يتحقق بسلوك سلبي أيضاً كما لو ترك المؤتمن على السر الوثيقة التي تحويه في مكان يسمح للآخرين الاطلاع على محتواه أو مضمونه (الصيفي، ١٩٧٢، ص١١٢-١١٣).

الفرع الثالث: تجريم إبلاغ الأسرار المتعلقة بأمن الدولة أو إفشائها بصورة تقنية

لم يحددّ المشرع الوسائل التي يتم من خلالها الإفشاء أو التبليغ، فقد تكون شفاهة بالكلام، أو كتابة، أو تصوير، أو بالرسم أو بالنشر في الصحف والمجلات أو على منصات التواصل الاجتماعي أو بالوسائل الإلكترونية أو الإنترنت أو من خلال الرسائل الإلكترونية أو الرسائل النصية، لذلك فلا عبره للوسيلة أو مدى الانتشار الذي تحققه هذه الوسيلة في تجريم إفشاء السر أو التبليغ عنه، وعليه يستوعب نص المادة ١٦ من قانون حماية أسرار ووثائق الدولة الصور المستحدثة لهذه الجريمة (الزعبي والناعسة، ٢٠٢٢، ص٢٨٤).

المبحث الرابع:
الجزاءات القانونية المقررة لجرائم التجسس التقني

من خصائص العقوبة في التشريع الجزائي الأردني التدرج بتحديد مقدارها وفقاً لجسامة الجريمة وخطورتها، وحديتها أي أن يكون لها حد أدنى وحد أعلى، حيث إن جرائم التجسس التقني عاقب عليها المشرع بصورة بسيطة (المطلب الأول) كما عاقب عليها المشرع بصورة مشددة في حال توافر ظروف معينة نص عليها القانون العقابي (المطلب الثاني) في حين أورد عقوبات تكميلية قررها على مرتكب جريمة التجسس لكونها جريمة إلكترونية (المطلب الثالث).

المطلب الأول: العقوبات الأصلية لجرائم التجسس التقني بصورتها العادية

ميز المشرع الجزائي الأردني في عقوبة التجسس التقني بصورتها البسيطة بين الدخول أو الوصول إلى الشبكة المعلوماتية أو تقنية أو نظام المعلومات أو أي جزء منها وبين الدخول أو الوصول إلى الموقع الإلكتروني.

ففي الحالة الأولى "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" (قانون الجرائم الإلكترونية، المادة ٤/أ).

أمَّا في الحالة الثانية، أي إذا كان الدخول أو الوصول في هذا الصدد إلى موقع إلكتروني، يعاقب الجاني بعقوبة الدخول إلى الشبكة المعلوماتية أو تقنية أو نظام المعلومات أو أي جزء منها مع اختلاف في الحد الأدنى لمدة الحبس، حيث تصبح أربعة أشهر (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/ج).

والجدير بالذكر إن المشرع الجزائي الأردني يعاقب على الشروع في جرائم التجسس التقني – سواء كانت جناية أم جنحة– بالعقوبة المقررة للجرائم ذاتها، بحيث يعتبر الشارع بالجريمة فاعلاً لها تماماً (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/هـ) وهذا توجه صائب للمشرع في ردع كل من تسول له نفسه محاولة ارتكاب هذه الجرائم.

من جانب آخر، أضاف قانون الجرائم الإلكترونية نصّاً يوفر سياسة عقابية رادعة لكل من تسول له نفسه الاشتراك أو التدخل أو التحريض على ارتكاب جريمة التجسس التقني، فعاقب الشركاء التبعيين والمحرضين على التجسس بالعقوبة ذاتها المحددة لمرتكبيها الأصليين (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٢٧).

كما عاقب المشرع الجزائي الأردني كل من دخل أو حاول الدخول إلى مكان محظور قصد الحصول على أسرار أو وثائق محمية أو معلومات سرية حرصاً على سلامة الدولة بالأشغال المؤقتة (قانون حماية أسرار ووثائق الدولة، المادة ١٤) والتي تتراوح ما بين ثلاث سنوات إلى عشرين سنة (قانون العقوبات، المادة ٢/٢٠).

وإذا تمت السرقة أو الاستحصال لهذه الأسرار يعاقب الجاني بالأشغال المؤقتة لمدة لا تقل عن عشر سنوات (قانون حماية أسرار ووثائق الدولة، المادة ١٥/أ) حيث يكون الحد الأعلى لهذه العقوبة الأشغال لمدة عشرين سنة (قانون العقوبات، المادة ٢/٢٠).

المطلب الثاني: العقوبات الأصلية لجرائم التجسس التقني بصورتها المشددة

شدد المشرع العقوبة عن جريمة التجسس التقني إذا كان الدخول المجرم إلى الشبكة المعلوماتية أو تقنية أو نظام المعلومات بقصد الاعتداء على البيانات أو المعلومات محل التجسس بالإلغاء أو الإتلاف أو التدمير أو التعديل أو التغيير أو النقل أو النسخ أو النشر أو إعادة النشر أو خسارة السرية أو التشفير أو الحذف أو الإضافة أو الحجب أو الإفشاء أو الالتقاط، لتصل إلى الأشغال المؤقتة وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على خمسة وعشرين ألف دينار (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/ب).

شدد المشرع عقوبة الجاني في هذا الصدد نظراً لجسامة أفعاله الجرمية وخطورتها، حيث تحول القصد الخاص للجاني من مجرد الاطلاع على أسرار الدولة إلى القيام بإحدى صور الاعتداء المذكورة، وإذا تحققت النتيجة من قصد الاعتداء، ووقع الاعتداء فعلاً بأي صورة من صوره، تشدد العقوبة مره أخرى وترتفع إلى الأشغال المؤقتة مدة لا تقل عن خمس سنوات والغرامة (٢٥٠٠٠) خمسة وعشرين ألف دينار.

وشدد المشرع بالعقوبة ذاتها، إذا كان الدخول المجرم في المادة ٤/ج من قانون الجرائم الإلكترونية إلى موقع إلكتروني بقصد إلغاء البيانات أو المعلومات غير المتاحة للجمهور أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو حذفها أو إضافتها أو حجبها أو تشفيرها (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٤/د).

ويلاحظ الباحث أن صور الاعتداء الأخيرة التي تقع على البيانات أو المعلومات محل التجسس من خلال الدخول إلى الموقع الإلكتروني لم تتضمن (النشر أو اعادة النشر أو خسارة السرية أو الالتقاط) المشار اليها في الدخول إلى الشبكة المعلوماتية أو تقنية أو نظام المعلومات.

لا بدَّ من الإشارة إلى إن المشرع أضاف نصّاً جديداً في قانون الجرائم الإلكترونية يضاعف العقوبة على جرائم التجسس التقني إذا ارتكبها الجاني باستغلال وظيفته أو عمله أو صلاحياته الممنوحة له، أو إذا كرر ارتكابها، أو إذا ارتكب الجاني جريمة التجسس التقني لمصلحة دولة أجنبية أو تنظيم غير مشروع (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٢٨).

ويعاقب المشرع الجزائي الأردني بالأشغال المؤقتة مدة لا تقل عن عشر سنوات كل من وصل إلى حيازته أو علمه أي سر من الأسرار أو المعلومات أو آية وثيقة محمية بحكم وظيفته أو كمسؤول أو بعد تخليته عن وظيفته او مسؤوليته لأي سبب من الأسباب فأبلغها أو أفشاها دون

سبب مشروع (قانون حماية أسرار ووثائق الدولة، المادة ١٦/أ) حيث يكون الحد الأعلى لهذه العقوبة الأشغال لمدة عشرين سنة (قانون العقوبات، المادة ٢/٢٠).

وشدد قانون حماية أسرار ووثائق الدولة العقاب على الجاني إذا كان مرتكباً إحدى جرائم التجسس المنصوص عليها في المواد ١٤ و١٥ و١٦ من هذا القانون لتصبح الأشغال المؤبدة إذا اقترفت الجناية لمنفعة دولة اجنبية، في حين ترتفع العقوبة إلى الإعدام إذا كانت الدولة الأجنبية عدوة.

أخذ المشرع الجزائي في جرائم التجسس بمبدأ التدرج في العقوبة بصورة ينسجم فيها مقدار العقاب مع حجم الضرر الواقع على الدولة جراء ارتكاب الجاني لإحدى جرائم التجسس، رغم أن مقدار العقوبات المنصوص عليها في قانون الجرائم الإلكترونية في مواجهة جريمة التجسس التقني أقل من مقدار العقوبات المنصوص عليها في قانون حماية أسرار ووثائق الدولة في مواجهة جريمة التجسس بصورته التقليدية، فالعقوبات الواردة في القانون الأول هي أولى بالتشديد نتيجة سهولة الجريمة التقنية من حيث السلوك وضخامة ضررها من حيث النتيجة، من جانب آخر لا يحول تطبيق العقوبات المنصوص عليها في قانون الجرائم الإلكترونية دون الحكم بأي عقوبة أشد ورد النص عليها في أي قانون آخر (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٣٠).

وأخيراً لا بدَّ من الإشارة إلى استثناء المشرع جرائم التجسس بصورتيه التقليدية والإلكترونية من العفو العام، لخطورة هذه الجريمة ومساسها بالصالح العام من خلال الإضرار بالأمن الوطني، حيث إنه: "لا يشمل الإعفاء المنصوص عليه في الفقرة (١) من المادة (٢) من هذا القانون الجرائم التالية سواء بالنسبة للفاعل الأصلي أو الشريك أو المتدخل أو المحرض كما لا يشمل الإعفاء الشروع في أي منها:- ٢٢. جرائم التجسس المنصوص عليها في المواد من (١٤) إلى (١٦) من قانون حماية أسرار ووثائق الدولة رقم (٥٠) لسنة ١٩٧١. ٣١. الجرائم المرتكبة خلافا لأحكام قانون الجرائم الإلكترونية رقم (٢٧) لسنة ٢٠١٥ ورقم (١٧) لسنة ٢٠٢٣ أو بدلالتيهما" (قانون العفو العام، ٢٠٢٤، المادة ٣).

المطلب الثالث: العقوبات التكميلية لجرائم التجسس التقني

لما كانت جريمة التجسس التقني من الجرائم الإلكترونية، نصَّ المشرع الجزائي الأردني على عقوبات إضافية (جزاءات تكميلية)، توقعها المحكمة على الجاني في حال إدانته بجريمة التجسس التقني

إلى جانب معاقبته بأي من العقوبات الأصلية السالف ذكرها.

ففي حال إدانة الجاني بجريمة التجسس التقني تقضي المحكمة من تلقاء نفسها بمصادرة الأجهزة أو البرامج أو الأدوات أو الوسائل أو المواد المستخدمة في ارتكاب أي من جرائم التجسس التقني، كما تقضي المحكمة بوقف أو تعطيل أو حجب عمل أي نظام معلومات أو موقع إلكتروني مستخدم في ارتكاب أي من جرائم التجسس التقني للمدة التي تقررها المحكمة، بالإضافة إلى حذف البيانات أو المعلومات السرية التي حازها الجاني أينما وجدت وذلك على نفقته، كما تقضي المحكمة بإغلاق المحل الذي استخدم لارتكاب أي من جرائم التجسس التقني لمدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٣١/ب).

ويجب على المحكمة أن تطبيق العقوبات التكميلية سالفة الذكر دون الإخلال بحقوق غير حسن النية، ذلك أن العقوبات أصلية كانت أم تكميلية تخضع لمبدأ الشخصية، فلا تتجاوز حدودها شخصية الجاني دون أن تمتد إلى غيره من الأشخاص سواء كان ذلك بصورة مباشرة أو غير مباشرة.

ولضمان تطبيق العقوبات التكميلية على مرتكبي جرائم التجسس التقني، عاقب المشرع الجزائي الأردني كل من يمتنع أو يعيق تنفيذ أي من القرارات القضائية المتعلقة بهذه العقوبات بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن (٣٠٠٠) ثلاثة آلاف دينار ولا تزيد على (٦٠٠٠) ستة آلاف دينار (قانون الجرائم الإلكترونية، ٢٠٢٣، المادة ٣١/ب).

الخاتمة:

بعد استعراض جرائم التجسس التقني في التشريع الأردني من خلال بيان مدلولها وطبيعتها ونموذجها القانوني ومدى استيعاب قانون حماية أسرار ووثائق الدولة لجريمة التجسس بصورتها المستحدثة وتأصيلها في قانون الجرائم الإلكترونية، وإبراز السياسة الجزائية في مواجهتها، توصلت الدراسة إلى مجموعةٍ من النتائج والتوصيات نجملها بالآتي:

أولاً: النتائج

١. لم يعرف قانون الجرائم الإلكترونية الدخول وحسناً ما قام به، لأن تجريم الدخول غير المصرح به للنظام المعلوماتي يرتبط بأمور تقنية متغيرة ومتطورة، فتعريف الدخول قد يحد من التجريم لعجز التعريف عن مجاراة واستيعاب المستجدات التكنولوجية.
٢. تضمن قانون الجرائم الإلكترونية في إصداره الأخير لسنة ٢٠٢٣ العقاب على الشروع في جرائم

التجسس الإلكترونية، حتى وإن كانت جنحاً، حيث منح القانون خصوصية في ذلك لجنح التجسس التقني، نظراً لخطورتها على الدولة.

٣. جرّم المشرع الأردني الشروع في جنح التجسس سواء كان تقنياً أم تقليدياً، لاعتبار التجسس من جرائم الخطر المبكر الذي ساوى فيه بين الفعل والشروع به، ولم يقف الأمر عند حد التجريم بل امتد إلى العقاب؛ حيث يعاقب على الشروع في التجسس بنوعيه بعقوبة الجريمة التامة.

٤. يمكن ارتكاب جريمة الدخول إلى الأماكن المحظورة خلافاً لأحكام نص المادة ١٤ من قانون حماية أسرار ووثائق الدولة بالوسائل الإلكترونية بتطبيق قاعدة الإحالة الفنية في التجريم استناداً إلى أحكام نص المادة ٢٦ من قانون الجرائم الإلكترونية خصوصاً وأن النص الأول جاء مطلقاً من كل قيد.

٥. إذا كان سلوك الجاني المتمثل في حصوله على السر متصور ارتكابه بوسيلة تقنية سواء كان السر محل التجسس محفوظ بشكل تقليدي أو ممغنط، فلا مانع من استيعاب النص التقليدي لجريمة التجسس التقني في ظل وجود المادة ٢٦ من قانون الجرائم الإلكترونية، التي تصورت ارتكاب الجرائم التقليدية بصورة تقنية، إذا ارتكبت باستخدام الوسائل الإلكترونية، على أن يعاقب عليها الجاني بعقوبتها الواردة في قانون حماية أسرار ووثائق الدولة.

٦. لم تتضمن المادة ٤/د بعض صور الاعتداء المشددة للعقوبة والتي تقع على البيانات أو المعلومات محل التجسس في حالة الدخول إلى الموقع الإلكتروني وهي: (النشر أو اعادة النشر أو خسارة السرية أو الالتقاط) رغم الإشارة إليها في حالة الدخول إلى الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها.

ثانياً: التوصيات

١. لم يدخل المشرع جرائم التجسس المنصوص عليها في المادة ٤ من قانون الجرائم الإلكترونية في اختصاص محكمة أمن الدولة بخلاف قانون حماية أسرار ووثائق الدولة؛ الأمر الذي ينادي بضرورة توحيد الاختصاص القضائي للنظر بجرائم التجسس بين هذين القانونين، ونظراً لأن التجسس بكافة صوره يشكل خطراً على الدولة وأجهزتها، ينبغي على المشرع منح اختصاص النظر بهذه الجرائم جميعها لمحكمة أمن الدولة.

٢. إدراج صور الاعتداء المشددة للعقوبة وهي: (النشر أو اعادة النشر أو خسارة السرية أو الالتقاط)

لتصور مساسها بالبيانات أو المعلومات محل التجسس في حالة الدخول إلى الموقع الإلكتروني، وذلك أسوةً بتشديد العقوبة عن هذه الاعتداءات في حالة الدخول إلى الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها.

٣. ضرورة توسع قانون حماية أسرار ووثائق الدولة بمدلول الأسرار والوثائق المحمية الذي لم يتجاوز حده السر المحفوظ على أشرطة التسجيل، وذلك ليشمل الأسرار والوثائق المحمية المخزنة بأي وسيلة تقنية، كما فعل قانون ضمان حق الحصول على المعلومات بمعرض تعريفه للوثائق المصنفة، الذي تصور تخزينها بجميع الوسائل الإلكترونية.

٤. ضرورة صياغة خطة عقابية موحدة للعقوبات المنصوص عليها في قانون الجرائم الإلكترونية وقانون حماية أسرار ووثائق الدولة، وتشديد العقوبات الواردة في القانون الأول على غرار القانون الأخير نتيجة خطورة الجرائم الإلكترونية وضخامة أثرها.

٥. ضرورة قيام المؤسسات الأمنية والجهات القانونية بما فيها وزارة العدل والمجلس القضائي ونقابة المحامين والمعهد القضائي ومعهد تدريب المحامين ووحدة الجرائم الإلكترونية والمركز الوطني للأمن السيبراني بتنظيم دورات وندوات وورش عمل ومحاضرات خاصّة بالجرائم الإلكترونية توضح مصطلحاتها الفنية وجوانبها التقنية لفهمها فهماً سليماً ومعرفة التعامل معها في سبيل مواجهة الجرائم الإلكترونية عامّةً، وجرائم التجسس التقني خاصّة.

قائمة المصادر والمراجع

أولاً: المراجع باللغة العربيّة

١) الكتب

- بهنام رمسيس، **القسم الخاص من قانون العقوبات**، منشأة المعارف، الإسكندرية- مصر، ١٩٨٢ الصفحات: ١-٦٣٧.
- الزعبي، جلال والمناعسة أسامة، **جرائم تقنية نظم المعلومات الإلكترونية**، ط٤، دار الثقافة، عمان، الأردن، ٢٠٢٢، الصفحات: ١-٣٤٤.
- الشواربي، عبد الحميد، **الجنايات والجنح المضرة بالمصلحة العامة في ضوء الفقه والقضاء**، بدون ط، منشأة المعارف، الإسكندرية- مصر، ٢٠٠٣، الصفحات: ١-١٠١٨.
- الصغير، جميل، **القانون الجنائي والتكنولوجيا الحديثة**، الكتاب الأول ط٢، دار النهضة العربية،

القاهرة–مصر،٢٠١١، الصفحات: ١–٢٠١.

- الصيفي، عبد الفتاح، **قانون العقوبات اللبناني**، جرائم الاعتداء على أمن الدولة وعلى الأموال، بدون ط، دار النهضة العربية، بيروت– لبنان، ١٩٧٢، الصفحات: ١–٥٧٣.
- الفاضل، محمد، **الجرائم الواقعة على أمن الدولة**، الجزء الأول، ط٢، مطبعة جامعة دمشق، دمشق– سوريا، ١٩٦٥، الصفحات: ١–٩٣٤.
- نمور، محمد سعيد، شرح قانون العقوبات القسم الخاص الجرائم الواقعة على الأموال، دار الثقافة للنشر والتوزيع، عمان– الأردن، ٢٠٢١، الصفحات: ١– ٣٧٦.

٢) الأبحاث والمقالات

- الجبرة، علي، أثر الجريمة الإلكترونية على سير المرافق العامة الإلكترونية في التشريع الأردني، **مجلة الزرقاء للبحوث والدراسات الإنسانية**، جامعه الزرقاء،٢١ (٢)، ٢٠٢١، الصفحات: ٣٤٦– ٣٦٦.
- الشوابكة، برجس، الجرائم الإلكترونية الشائعة على مواقع التواصل الاجتماعي، **مجلة دراسات**، جامعة عمار ثليجيي، العدد ٩١، ٢٠٢٠، الصفحات: ١٣٧– ١٥٢.
- محمود، عبد الله، جريمة الاختراق الواقعة على البيانات والمواقع الحكومية: دراسة مقارنة على التشريعات الأردنية والفلسطينية، **مجلة المنارة للدراسات القانونية والإدارية**، عدد خاص، ٢٠٢٠، الصفحات: ١٧٠–١٨٥.
- مساعدة، أنور، مدى كفاية القواعد الموضوعية في قانون الجرائم الإلكترونية الأردني رقم ٢٧ لسنة ٢٠١٥– دراسة مقارنة للتطور التشريعي على المستويين الوطني والدولي، **مجلة الشريعة والقانون**، جامعة الإمارات العربية المتحدة، ٣٢ (٧٤)، ٢٠١٨، الصفحات: ٤٥٥–٥١٢.
- النعيمي، أسامة، جريمة التجسس الإلكتروني في إطار مشروع قانون جرائم المعلوماتية العراقي لسنة ٢٠١١، **مجلة كلية القانون للعلوم القانونية والسياسية**، جامعة كركوك، ١٠ (٣٦)، ٢٠٢١، الصفحات: ٣١–٧٢.
- النوايسة، عبدالإله، والعدوان ممدوح، جرائم التجسس الإلكتروني في التشريع الأردني دراسة تحليلية، **مجلة دراسات لعلوم الشريعة والقانون**، الجامعة الأردنية، ٤٦(١)، ٢٠١٩، الصفحات: ٤٥٦– ٤٨٢.

٣) الرسائل العلميّة

- أبو العثم، رائد، **الأحكام العامة لجرائم أمن الدولة عبر الوسائل الإلكترونية في التشريع الأردني**، رسالة ماجستير جامعه الشرق الأوسط، عمّان، الأردن، ٢٠١٩.
- الدروبي، جمال، **جرائم التجسس في التشريع الأردني**، رسالة ماجستير، كلية الحقوق– جامعة جرش، الأردن، ٢٠١٢.
- سلامي، نادية، **آليات مكافحة التجسس الإلكتروني**، أطروحة دكتوراه، جامعة العربي التبسي، تبسة، ٢٠١٩.
- لدادوه، عماد، **مدى ملائمة قانون الجرائم الإلكترونية الأردني للأحكام العامة لقانون العقوبات**، رسالة ماجستير، جامعة الشرق الأوسط، عمّان، الأردن، ٢٠٢١.
- نابلسي، علاء الدين، **السياسة الجنائية في مواجهة جرائم التجسس** "**دراسة مقارنة**"، رسالة ماجستير، جامعة النجاح الوطنية، فلسطين، ٢٠٢٠.
- يونس، عمر محمد أبو بكر، **الجوانب الموضوعية والإجرائية لجرائم الإنترنت**، رسالة دكتوراه، جامعة عين شمس، القاهرة، مصر، ٢٠٠٤.

٤) التشريعات الوطنية والدولية

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة ٢٠١٢
- قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩.
- قانون التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم ١٩ لسنة ٢٠١٢
- قانون الجرائم الإلكترونية رقم ١٧ لسنة ٢٠٢٣
- قانون الجرائم الإلكترونية رقم ٢٧ لسنة ٢٠١٥.
- قانون العفو العام رقم (٥) لسنة ٢٠٢٤
- قانون العقوبات رقم ١٦ لسنة ١٩٦٠.
- قانون جرائم أنظمة المعلومات المؤقت لسنة ٢٠١١.
- قانون حماية أسرار ووثائق الدولة رقم ٥٠ لسنة ١٩٧١.
- قانون ضمان حق الحصول على المعلومات رقم ٤٧ لسنة ٢٠٠٧.

٥) الأحكام القضائية

- حكم رقم ٢٠٢٢/٣٢٦٠، محكمة التمييز بصفتها الجزائية، صادر بتاريخ ٢٠٢٢/١١/١٣، منشورات موقع قرارك.

- حكم رقم ٢٠٢٢/٤٠٩٦، محكمة التمييز بصفتها الجزائية، صادر بتاريخ ٢٠٢٢/٠٤/٢٠، منشورات موقع قرارك.
- حكم رقم ١٩٩٦/٦٧٩، محكمة التمييز بصفتها الجزائية، مبدأ عام، صادر بتاريخ ١٩٩٧/٠١/٠٥، منشورات موقع قرارك.

٦) **المواقع الإلكترونية:**

- موقع معجم المعاني، قاموس المعجم الوسيط، تاريخ الزيارة: ٢٠٢٤/٠٨/٢١، الرابط الإلكتروني: https://www.almaany.com/ar/dict/ar-ar/%D9%88%D8%B5%D9%84/

ثانياً: المراجع باللغة الإنجليزيّة

- Al-Shawabkeh, Barjes (2024). CRIMINALIZATION OF PERSONALITY ASSASSINATIONVIA ELECTRONIC MEANS, JOURNAL OF LAW AND SUSTAINABLE DEVELOPMENT, Miami| v.12, n. 1, pages: 01-20
- Al-Shawabkeh, Barjes (2024). Criminalizing Impersonation via Social Media Platforms, Pakistan Journal of Criminology, Pakistan Society of Criminology, Pakistan Society of Criminology, v. 16, n. 2, pages: 01-12.