الحماية الجنائية للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني

"دراسة مقارنة بين التشريعين الفلسطيني والأردني"

د. محمد بدوسي

قسم علم الجريمة والقانون، كلية القانون، جامعة الاستقلال، فلسطين

Dr. Mohammad Badousi

Department of Criminology and Law, Faculty of Law, Al-Istiqlal University, Palestine

ma_badousi@pass.ps

Criminal Protection of State Security Secrets from Cyber Espionage

"A Comparative Study between Palestinian & Jordanian Legislation"

Abstract:

The current study aimed to shed light on the issue of criminal protection for state security secrets from cyber espionage in Palestinian legislation, in comparison with Jordanian legislation. To accomplish this objective, the researcher employed both the descriptive analytical method and the comparative method, by reviewing the legal rules regulating the provisions of this protection in both legislations. Through the study, we attempted to explore the concept of Cyber espionage, its scope, the importance of criminal protection of state security secrets, its types, & the penalties imposed. The major conclusion and recommendations of this study were that the Palestinian legislator didn't distinguish between ordinary government data and confidential information, which is prohibited for anyone other than authorized parties to access, and didn't allocate a specific penalty for such information in the event of an infringement. Among the recommendations is the need for the Palestinian legislator to amend Article (4), in line with the seriousness of Cyber espionage, by adding a special clause related to the infringement of confidential government information or data and establishing a specific penalty commensurate with the severity of the damage that may cause.

Keywords: Espionage, Cyber Espionage, State Secrets, Criminal Protection, Unauthorized Access

ملخص

هدفت الدراسة الحالية إلى تسليط الضوء على موضوع الحماية الجنائية للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني في التشريع الفلسطيني مقارنة مع التشريع الأردني، وللإحاطة الشاملة بمختلف جوانب الموضوع، تم تناول مفهوم التجسس الإلكتروني ومحله وأنواعه وخصوصية الحماية الجنائية للأسرار الخاصة بأمن الدولة، والمسؤولية الجنائية المترتبة على ارتكاب هذه الجريمة ، ولتحقيق الأهداف الموضوعة استخدم الباحث المنهج الوصفي التحليلي و المنهج المقارن، من خلال الرجوع للنصوص القانونية الناظمة لأحكام هذه الحماية وتحليلها في كلا التشريعين، وتوصلت الدراسة إلى مجموعة من النتائج والتوصيات؛ كان من أهمها أن المشرع الفلسطيني لم يميز بين المعلومات أو البيانات الحكومية العادية وتلك السرية منها، أو التي يحظر على غير الجهات المصرح لها الاطلاع عليها، ولم يقرر عقوبات خاصة في حال الاعتداء عليها، وقد أوصت الدارسة المشرع الفلسطيني بضرورة القيام بتعديل المادة رقم (4)، وذلك انسجاما مع خطورة التجسس الإلكتروني، وذلك من خلال إضافة بند خاص يتعلق بمحل الجريمة عندما يكون المعلومات أو البيانات الحكومية السرية، وإقرار عقوبات خاصة تتناسب وجسامة الضرر الذي قد ينجم عنها .

الكلمات المفتاحية: التجسس، التجسس الإلكتروني، أسرار الدولة، الحماية الجنائية، الدخول غير المصرح به

مقدمة

كان من آثار التقدم الذي حصل في مجال الاتصالات واستخدام الأجهزة الإلكترونية الحديثة، أن أصبح العالم قرية صغيرة مترابط بمجموعة من الشبكات الإلكترونية التي جعلت منه وحدة واحدة، فساهم ذلك في سهولة الوصول إلى المعلومة وانتقالها وتبادلها بين أفراد المجتمعات في أنحاء مختلفة من العالم.

وفي المقابل رافق هذا التطور العديد من الاختراقات التي استهدفت المعلومات بمختلف أنواعها، لاسيما منها المرفوعة على شبكة الإنترنت أو تلك المخزنة منها على أنظمة المعلومات، بالإضافة إلى ذلك ظهور وانتشار التجسس الإلكتروني كشكل من أشكال الاعتداء على المعلومات السرية الخاصة بأمن الدولة.

فالتجسس كما في مجلات الحياة الأخرى شهد تطورا وتحولاً جذرياً من ناحية أساليب ارتكابه، وذلك بسبب وقوعه بالفضاء الإلكتروني الذي جعل من جمع المعلومات أكثر قيمة وسهولة، وذلك نظراً للكم الهائل من المعلومات والبيانات المتاحة حالياً على الشبكات، كما أصبح الاختراق لأنظمة المعلومات مصدر قلق كبير لجميع الدول، بسب استهدافه مجموعة متنوعة من المعلومات الحساسة التي ترتبط بمصالح الدولة وأمنها القومي (Darien ,2017, p355). وأمام هذا الواقع والتحديات التي فرضها التطور في أساليب التجسس، وخطورته التي قد تزداد مستقبلا بالتزامن مع التقدم التقني، وما قد يلحقه من أضرار كبيرة على الدول التي أصبحت تعتمد بشكل كبير في تنظيم شؤونها على استخدام الحاسوب والإنترنت، كان لابد للمشرع الفلسطيني والأردني كغيرهم من المشرعين في أنحاء العالم، العمل على مواجهة هذا السلوك، ومواكبة وتنظيم هذا التطور، وإيجاد الحلول للإشكاليات التي قد يتسبب بها على الصعيد القانوني، وذلك من خلال البحث في مختلف جوانب هذا الموضوع، وصولا إلى تنظيم قانوني يضمن وضع حماية كافية للمعلومات والبيانات الخاصة بأمن الدولة.

أهمية البحث

تنبع أهمية هذا البحث من أهمية موضوعه، خاصة أن جريمة التجسس تعتبر واحدة من الجرائم التي تمس أمن الدولة الخارجي، وتزداد خطورة هذه الجريمة عندما ترتكب بوسائل حديثة تزيد من صعوبة اكتشافها وملاحقة مرتكبيها، فأصبحت أحد المخاطر التي تهدد استقرار الدولة ومصالحها، فأسرار الدولة مهما كان نوعها أصبحت محلا للاعتداء في هذه الجريمة، كما تكمن أهمية هذه الدراسة في البحث في أوجه القصور في القانون الفلسطيني في تنظيم أحكام التجسس الإلكتروني بالمقارنة مع التشريع الأردني، لاسيما تلك الأحكام الموضوعية المرتبطة بتوفير الحماية الجنائية للأسرار الخاصة بأمن الدولة في قانون الجرائم الإلكترونية، وكذلك محاولة تقديم بعض التوصيات لمعالجة هذا القصور والمساهمة في تطوير التشريع الجنائي في فلسطين.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

مشكلة البحث

كان لإصدار قانون الجرائم الإلكترونية دور هام في التصدي لظاهرة الإجرام الإلكتروني، حيث نظم المشرع الفلسطيني أحكام جزء كبير من الجرائم التي ترتكب باستخدام التقنيات الحديثة، ومنها الدخول غير المصرح به لأنظمة المعلومات والاعتداء على البيانات الحكومية، مع ذلك لم يكن هذا التنظيم كافيا للإحاطة بمختلف الآثار التي قد تنتج عن هذه الجريمة، فخلت أحكام هذا القانون من تنظيم مسألة وقوع هذه الجريمة على بيانات حكومية ذات طابع سري تتعلق بأمن الدولة، وعليه يمكن تحديد إشكالية البحث من خلال السؤال الرئيس الآتي: **ما مدى كفاية الحماية الجنائية للمعلومات والبيانات السرية الخاصة بأمن الدولة في ضوء أحكام قانون الجرائم الإلكترونية الفلسطيني والأردني؟ ويتفرع عن هذا السؤال عدد من الأسئلة:**

- ماهي خصوصية الحماية الجنائية للأسرار الخاصة بأمن الدولة؟
- ما المقصود بالتجسس الإلكتروني كجريمة من الجرائم الواقعة على أمن الدولة؟
- ماهي أنواع التجسس الإلكتروني؟
- ماهي أركان جريمة التجسس الإلكتروني؟
- ماهي العقوبات المقررة على جريمة التجسس الإلكتروني؟

أهداف البحث

- توضيح أهمية الحماية الجنائية للأسرار الخاصة بأمن الدولة.
- تحديد محل الحماية الجنائية في التجسس الإلكتروني.
- تحديد مفهوم التجسس الإلكتروني وأنواعه.
- التعرف على المسؤولية الجزائية المترتبة على جريمة التجسس الإلكتروني.

منهج البحث

لمعالجة الإشكالية المطروحة في هذه الدراسة، اعتمد الباحث المنهج الوصفي التحليلي، لوصف واقع جريمة التجسس الإلكتروني وتحليل النصوص القانونية الناظمة لأحكامها، خاصة الأحكام الموضوعية المتعلقة بالتجريم والعقاب، وكذلك الاطلاع على الآراء الفقهية حول الموضوع، وكما استخدم الباحث المنهج المقارن للتعرف على توجه المشرع الأردني في تنظيم أحكام هذه الجريمة في قانون الجرائم الإلكترونية، وذلك بهدف الاستفادة من هذه الأحكام في تطوير التشريع الفلسطيني في هذا الجانب.

خطة البحث: لمعالجة الإشكالية المطروحة في هذا البحث سيتم تقسيمه إلى مبحثين، وذلك على النحو الآتي:

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

المبحث الأول: ماهية الحماية الجنائية للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني

المبحث الثاني: المسؤولية الجزائية عن جريمة التجسس الإلكتروني

المبحث الأول: ماهية الحماية الجنائية للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني

تشكل الحماية الجنائية أحد أهم الأهداف التي تسعى الدولة من خلالها توفير الحماية للمصالح الجوهرية من الجريمة، فهي تتطلب من الدولة العمل على وضع سياسية جنائية تضمن فيها تحقيق هذا الهدف بوسائل مختلفة، والتي من بينها إصدار القوانين التي تعتبر الوسيلة الأولى في مواجهة الجريمة. وللتعرف إلى جوهر الحماية الجنائية التي قررها المشرع للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني، سنتناول هذا الموضوع في مطلبين. الأول: الحماية الجنائية للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني، والثاني: ماهية التجسس الإلكتروني.

المطلب الأول: الحماية الجنائية للأسرار الخاصة بأمن الدولة من التجسس الإلكتروني

للحماية الجنائية خصوصية تتمثل باقترانها بالجزاء الذي قد يفرض على من يخالف قواعد القوانين العقابية بفعل يشكل اعتداء على مصلحة ذات قيمة اجتماعية ،وعليه سنتناول موضوع هذه المطلب في فرعين: نتطرق في الأول منه إلى تعريف الحماية الجنائية وفي الثاني: نبحث في خصوصية الحماية الجنائية لأسرار الدولة من التجسس الإلكتروني.

الفرع الأول: تعريف الحماية الجنائية

تعرف الحماية الجنائية بأنها مجموعة من القواعد التي أقرها المشرع في إطار القانون الجنائي، بهدف حماية مصلحة ذات قيمة للفرد والمجتمع والدولة من أي اعتداء حال أو مستقبلي، ويفرض جزاء جنائي على من يخالف هذه القواعد. ورد في (عوشن، 2013، ص8).

فمفهوم هذه الحماية كوسيلة لحماية الحقوق المختلفة، تستند في أصلها إلى مبدأ الشرعية الجنائية بشقه الموضوعي، لا جريمة ولا عقوبة إلا بنص مكتوب صادر عن السلطة المختصة بالدولة، وذلك تطبيقا لأحكام القانون الدستوري الذي وضع مبدأ ثابتا» حدد فيه المشرع أساس وأدوات التجريم والعقاب (سرور، 2002، ص25)

وتتحقق أهداف هذه الحماية من خلال الجزاء الجنائي المتنوع الذي ينص عليه المشرع في القانون الجنائي، ويفرض على أي شخص ينتهك قواعد هذه الحماية سواء كان شخصا طبيعيا أو اعتباريا؛ وهذا الجزاء قد يأخذ أشكال متنوعة من العقوبات وكذلك التدابير الاحترازية (صالح، 2019، ص715).

وبناء على ما تقدم يتضح لنا، أن جوهر الحماية الجنائية يتمثل بمجموعة من الإجراءات والأدوات التي تتخذها الدولة في اطار سياستها الجنائية، وذلك بهدف الحفاظ على مختلف

العلاقات والمصالح والقيم الاجتماعية، وقمع الاعتداءات الإجرامية عليها، وذلك بالنص على تجريم الأفعال التي تشكل خطورة على الفرد والمجتمع والدولة في القانون الجنائي، وتحديد العقوبات والتدابير الاحترازية المناسبة التي قد تفرض على مرتكب الجريمة.

الفرع الثاني: خصوصية الحماية الجنائية لأسرار الدولة من التجسس الإلكتروني

يوجد العديد من وسائل الحماية التي تتخذها الدولة من أجل حماية الأسرار الخاصة بأمنها، منها استخدام الوسائل التقنية لحماية المعلومات السرية، وكذلك الحماية الجنائية التي تشكل وسيلة هامة في حال عدم نجاح التدابير التقنية لمنع الاعتداء على هذه الأسرار.

وتظهر أهمية هذه الحماية في مواجهة الجرائم الإلكترونية، من نواحي عدة منها ما يرتبط بتطور صناعة التكنولوجيا وتنوع استخدمها في المجتمع، وما صاحب ذلك من آثار سلبية تمثلت في استغلالها كوسائل لارتكاب الجريمة، الأمر الذي تسبب في أضرار كبيرة لمستخدميها، حيث تطلب ذلك من المشرع اللجوء إلى فرض الحماية اللازمة من هذه الجرائم، بالإضافة إلى ذلك تعتبر الحماية الجنائية أكثر فعالية من باقي أنواع الحماية القانونية، لما تحققه من ردع عام وخاص للمجرمين (باطلي،2015، ص 145-146).

فقواعد القانون الجنائي تقوم بدور أساسي في حماية الأسرار الخاصة بأمن الدولة وتظهر هذه الأهمية بشكل خاص عندما يتعلق الأمر بحماية أنظمة المعلومات التي تحتوي على أسرار الدولة من أي اعتداء خارجي، بالإضافة إلى ذلك تضمن هذه الحماية الجنائية توفير الحماية لمختلف أنواع المعلومات الأخرى .

ولضمان توفير الحماية للأسرار الخاصة بالدولة، قام المشرع بالنص على تجريم مجموعة من الأفعال التي تشكل اعتداء على أسرار الدولة، حيث يشكل الدخول إلى أماكن محظورة بقصد الحصول على أسرار الدولة أو سرقتها أو استحصالها أو إفشائها جرائم تمس بأمن الدولة الخارجي (المواد 124،125،126 من قانون العقوبات رقم 16 لسنة 1960 الأردني النافذ بالضفة الغربية)

ومن ناحية أخرى ومن أجل توفير الحماية الجنائية للمعلومات والبيانات الحكومية فقد جرم المشرع الفلسطيني في قانون الجرائم الإلكترونية الدخول غير المصرح به وما يرتبط به من أفعال قد تشكل خطورة على سلامة هذه البيانات والمعلومات وما قد ينتج عنه من أضرار قد تودي إلى إتلافها أو حذفها أو تعديلها أو إفشائها (المادة: 4 من القرار بقانون رقم 18 بشان الجرائم الإلكترونية)

وأما بالنسبة للمشرع الأردني فقد كان أكثر اهتماما بتوفير الحماية للأسرار الخاصة بأمن الدولة، وهذا ظهر من خلال قيامه بإصدار قانون خاص نظم بموجبه الأحكام الخاصة بالحفاظ على أسرار الدولة، حيث صنف ضمن هذا القانون المعلومات السرية وحدد درجة سريتها، وجرم الأفعال التي

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

تستهدف الأسرار الخاصة بأمن الدولة الأردنية (المواد 14،15،16 من قانون حماية أسرار وثائق الدولة لسنة 1971).

بالإضافة لذلك فرض المشرع حماية جنائية للأسرار الخاصة بالأمن الوطني، حيث جرم مختلف أشكال الاعتداء على البيانات والمعلومات التي تمس الأمن الوطني، بالإضافة إلى تشديده العقوبة في حال المساس بها بشكل يلحق ضرر بها «(المادة 4 قانون الجرائم الإلكترونية الأردني رقم لسنة 2023).

وحرصا على تعزيز الحماية للأسرار الخاصة بأمن الدولة من أي محاولة الاطلاع عليها، فقد اتبع المشرع الأردني سياسة جنائية تقوم على أساس التوسع في دائرة الأفعال المجرمة من خلال اعتبار العديد من جرائم التجسس الواردة في قانون الجرائم الإلكترونية وقانون حماية أسرار وثائق الدولة، من جرائم الخطر (الشوابكة ومقابلة، 2024، ص 28) وهي الجرائم التي تتم بمجرد ارتكاب الفعل المجرم المتمثل بتعريض مصلحة محمية للخطر.

وتجدر الإشارة هنا، إلى أن المشرع الأردني، وبعد إصداره قانون خاص لحماية أسرار ووثائق الدولة، استبعد جريمة التجسس على أمن الدولة وأحكامها وأخرجها من نطاق التجريم في قانون العقوبات؛ ليصبح مكان تنظيمها وعقوبتها ضمن إطار قانون حماية أسرار وثائق الدولة الأردنية، فهذه الجرائم منذ صدور هذا القانون لم تعد تصنف على أنها جرائم واقعة على أمن الدولة الخارجي (النوايسة، 2005، ص119)

وعليه يتضح لنا، أن المشرع الأردني كما المشرع الفلسطيني، خصص حماية جنائية لأسرار الدولة من التجسس في مواقع مختلفة في التشريع وذلك من خلال تجريم التجسس أو الحصول على المعلومات الخاصة بأمن الدولة، وهي الأسرار التي يحظر الإطلاع عليها أو إفشائها، لكن في المقابل تباينت أحكام هذه الحماية في كلا التشريعين من حيث تحديد المصلحة المقصود حمايتها، خاصة تلك المتعلقة بالبيانات والمعلومات محل التجسس الإلكتروني، وهي ذات طابع سري خاص بأمن الدولة، فالمشرع الأردني نص بصراحة على محل التجسس عندما يقع على معلومات سرية تخص الأمن الوطني.

المطلب الثاني: ماهية التجسس الإلكتروني

تعتبر جريمة التجسس بمختلف صورها المستحدث والتقليدي من الجرائم التي تمس أمن الدولة، فهي جريمة ظهرت ونشأت وتطورت مع تطور حياة الإنسان. وللتعرف إلى ماهية التجسس الإلكتروني سنقسم هذا المطلب إلى فرعين، في الأول: نبحث في مفهوم التجسس الإلكتروني وتمييزه عن التجسس التقليدي وأما الثاني: نخصصه لمحل الحماية الجنائية في التجسس الإلكتروني وأنواعه.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الفرع الأول: مفهوم التجسس الإلكتروني وتمييزه عن التجسس التقليدي

بادئ ذي بدء وقبل الخوض في التعريفات المختلفة التي وضعت للتجسس سواء بمفهومه التقليدي أو المستحدث، لابد لنا من الإشارة إلى أن المشرع على مستوى القوانين العقابية السارية في فلسطين وكذلك المشرع الأردني، لم يتطرق لتعريف جريمة التجسس سواء كان بمفهومه التقليدي أو الإلكتروني. وذلك انطلاقا من اعتياد المشرع على نهج عدم الخوض في وضع التعريفات للمصطلحات القانونية إلا إذا اقتضت الضرورة لذلك.

أولا: تعريف التجسس الإلكتروني

سعى الفقه الجنائي إلى محاولة وضع تعريف للتجسس، فظهر نتيجة لذلك العديد من الاجتهادات، لكنها تباينت من دولة لأخرى؛ بسب الأساس الذي انطلقت منه وهو سياسية التجريم والعقاب المتبعة في الدولة، وعليه وللوقوف على مفهوم التجسس الإلكتروني، لابد لنا في البداية من استعراض أهم التعريفات التي وضعت للتجسس بمفهومه العام ومن ثم التطرق إلى تعريف التجسس الإلكتروني.

المفهوم العام للتجسس (التجسس التقليدي)

أورد قاموس أكسفورد تعريفا للتجسس: بأنه عبارة عن فعل يتم من خلاله الحصول على المعلومات السرية الخاصة بأمن الدولة، سواء كانت المعلومات: عسكرية تجارية سياسية أو الصناعية، والاستيلاء عليها والإبلاغ عنها سراً (dictionary.cambridge,2025)

وعرف التجسس بأنه الاعتداء على أمن الدولة بفعل يتمثل في محاولة الحصول على معلومات سرية عن أمنها وقوتها وعتادها سواء حصل ذلك من أحد مواطنيها أو أجنبيا (اللبيدي، 2008، ص70).

كما عرف بعض الباحثين التجسس على أنه البحث والتحري عن أي نوع من المعلومات الخفية عن دولة معينة بهدف الاستيلاء عليها و إيصالها لدولة أجنبية، وذلك بهدف تحقيق مكاسب معينة أو بقصد الحاق الضرر بمصالح الدولة المستهدفة أو المجني عليها في جريمة التجسس ورد في (برهان، 2018،ص8).

فالتجسس بمفهومه العام عبارة عن عملية تهدف إلى الوصول إلى معلومات سرية بطرق مختلفة، وهو سلوك يتميز أحيانا بأنه الأكثر حدوثا في الواقع؛ للحصول على المعلومات السرية ، الذي يتميز بخطورته وعدم مشروعيته لأنه يتم دون علم أو موافقة من الجهة مالكة هذه المعلومات (Britannica, 2025).

وهكذا يتبين لنا أنه وبالرغم من تعدد واختلاف التعريفات التي وضعت للتجسس بمفهومه العام، أنها تتفق فيما بينها بالعناصر الأساسية التي تقوم عليها هذه الجريمة، والمتمثلة بتقصي المعلومات

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وجمعها بشكل سري، بهدف إيصالها إلى دولة اجنبيه، قد تكون هذه الدولة صديقة أو معادية، على اعتبار أن التجسس جريمة قد ترتكب من جهة معادية أو صديقة للدولة المجني عليها في وقت السلم أو الحرب، بالإضافة إلى اتفاق هذه التعريفات على تحديد أنواع المعلومات التي قد تكون محلا لهذه الجريمة.

تعريف التجسس الإلكتروني

بالرجوع إلى قانون الجرائم الإلكترونية الفلسطيني، نلاحظ أن المشرع في المادة الأولى من قانون الجرائم الإلكترونية قد استخدم مصطلح الاختراق ولم يضع تعريفا محددا للتجسس، لكنه بالرغم من ذلك تطرق إلى بعض المصطلحات المرتبطة به، كالدخول غير المصرح به والاختراق فعرف الأخير على أنه «الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية.

وبطبيعة الحال لا يختلف موقف المشرع الأردني في هذا التوجه، فلم يستخدم المشرع مصطلح التجسس الإلكتروني، ولكنه على غرار المشرع الفلسطيني استخدم في المواد(3،4) من قانون الجرائم الإلكترونية رقم 17 لسنة 2023 مصطلحات كالدخول غير المصرح به أو الوصول إلى أنظمة المعلومات أو الشبكات.

ويلاحظ أن المشرع على مستوى القوانين الخاصة بالجرائم الإلكترونية، لم يضع تعريفا للتجسس الإلكتروني،» إلا أنه يستفاد من الصياغة التشريعية للنص المجرم بأن التجسس التقني يتمثل بالاطلاع على معلومات وبيانات سرية تمس أمن الدولة ومصالحها العليا، وذلك من خلال الدخول غير المشروع إلى مواقع إلكترونية أو الشبكة المعلوماتية التي تعود للدولة أو مؤسساتها» (الشوابكة ومقابلة ،2024،ص278)

وفي هذا الإطار يرى البعض أنه وبالرغم من أن المشرع لم يستخدم مصطلح التجسس الإلكتروني بشكل صريح في قانون الجرائم الإلكترونية، ألا أنه يمكن تعريفه «بأن دخول الجاني إلى الشبكة المعلوماتية أو نظام المعلومات أو موقع إلكتروني للحصول على محتوى إلكتروني يمس الأمن الوطني أو العلاقات الخارجية للدولة أو السلامة العامة أو الاقتصاد الوطني» (النوايسة والعدوان، 2019، ص469)

فالتجسس الإلكتروني بمفهومه الخاص يقع من خلال القيام باستخدام وسائل تقنية الحديثة للاستيلاء بشكل غير مشروع إلى أنظمة معلومات خاصة بالدولة والاطلاع عليها بهدف الحصول على المعلومات الحساسة ذات العلاقة بكيانها السياسي وأسراها الأمنية والسياسية و الصناعية وغيرها من المعلومات الهامة. ورد في (العدوي، 2018، ص170).

ويرى بعض الباحثين أن مفهوم التجسس تغير من حيث الأهداف وطريقة الوصول لها، فبالإضافة

إلى الأسرار العسكرية والسياسية اصبح يستهدف الأسرار التجارية والاقتصادية والصناعية. وأما من ناحية طريقة ارتكابه، تم اللجوء إلى وسائل التكنولوجيا الحديثة مثل أجهزة التنصت والأجهزة الإلكترونية المتقدمة والأقمار الصناعية (Dayyani, 2016, p33)

وبناء على ما تقدم نستنتج، أن التجسس الإلكتروني في جوهره يعتبر وسيلة من وسائل الحصول على المعلومات ذات الطابع السري بشكل غير مشروع، و دون إذن مسبق من مالكها وهذه المعلومات قد تكون خاصة بالدولة أو الأشخاص أو المؤسسات الاقتصادية حيث يتصور ارتكاب هذا الجريمة من جهة معادية أو حليفة للدولة.

ثانيا: تمييز التجسس الإلكتروني عن التجسس التقليدي

أدى زيادة كم المعلومات والبيانات المخزنة على نظم المعلومات والمتاحة على شبكة الإنترنت، وسرعة الوصول لها، إلى جعل المعلومات التي يمكن الحصول عليها من خلال التجسس الإلكتروني اكثر من تلك التي يمكن الحصول عليها بأساليب التجسس التقليدي، هذا ما جعل التجسس الإلكتروني أكثر خطورة وأكثر أشكال التجسس انتشاراً وفعالية في العصر الحالي (Brown, 2016, P621).

فالتقدم التكنولوجي لاسيما في مجال الاتصالات وصناعة الحواسيب، ساهم في إيجاد ظروف مناسبة لارتكاب التجسس، فالتكنولوجيا الحديثة وفرت وسائل اكثر فاعلية للقيام باختراق أنظمة المعلومات, وبالتالي اصبح التجسس لا يقتصر على الأنواع التقليدية المتمثلة بالتجسس العسكري والأمني والصناعي، بل اصبح يشمل الجانب التقني والتجاري (المومني،2010، ص209).

ولعل أهم ما يميز التجسس الإلكتروني عن التقليدي هو استخدام تقنيات حديثة لتحقيق أهدافه، بالإضافة إلى تنوع الوسائل المستخدمة واتساعها لدرجة أنه يصعب تعددها أو حصرها، ويرجع ذلك التطور السريع للتكنولوجية الحديثة (سلامي، 2019، ص4-5)

وكما يختلف التجسس الإلكتروني عن التقليدي بدرجة معينة من الخطورة، ترتبط بخصائصه المتمثلة بعدم ترك أي دليل مادي بعد ارتكاب الجريمة، وهذا ما يصعب اكتشاف الجريمة أساسا، و سهولة إتلاف أدلتها و العثور على أي دليل يمكن إدانة الجاني، فمستخدمي هذا النوع من التجسس يمتلكون قدرات ومهارات في استخدام التقنيات الحديثة، بالإضافة إلى أن التجسس الإلكتروني يحدث في بيئة هادئة لا يحتاج إلى القوة. ورد في (أبو ذر شاكر، 2020ص44).

فالتجسس الإلكتروني كسلوك مجرم يتمثل في الحصول أو الإستيلاء على البيانات أو المعلومات عبر أنظمة الكمبيوتر والشبكة المعلوماتية، يختلف كذلك عن التجسس التقليدي، باستغلال الجاني البرامج الضارة وبرامج التجسس ونقاط الضعف في الشبكات وأنظمة الحاسوب لتحقيق أهدافه(Center for Development of Security Excellence, n.d.)

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وفي الواقع أدى استخدام الوسائل الرقمية في التجسس الإلكتروني للحصول بطريقة غير قانونية على معلومات سرية تخصص أمن الدولة، إلى جعل هذه النوع من التجسس يختلف عن التجسس التقليدي، من حيث طريقة الوصول للمعلومة؛ حيث يقع التجسس التقليدي من خلال التسلل المادي، على خلاف التجسس الإلكتروني يقع في بيئة رقمية، مما يجعل اكتشافه أكثر صعوبة وأسهل في التنفيذ من التجسس التقليدي (cyble, 2025).

وعلاوة على ذلك، يرى الباحث أن النطاق المكاني الذي يمتد خلاله التجسس الإلكتروني، سهل ارتكاب الجريمة ومكن الجاني من تنفيذها من أي مكان في العالم دون الحاجة إلى التنقل، على العكس من ذلك فالتجسس التقليدي يتطلب الإنتقال والدخول إلى مواقع معرفة على أنها محظورة، كما أن الإمتداد الإقليمي للتجسس الإلكتروني يجعل من الصعب على الدولة المستهدفة اكتشافه واتخاذ الإجراءات اللازمة لمنعه والتصدي له، كما أن خاصية العالمية لهذه الجريمة تصعب أيضًا إجراءات الملاحقة القانونية بسبب القيود القضائية والقوانين المتباينة.

وبناء على ما تقدم نستنتج أن التجسس الإلكتروني لا يختلف عن التجسس بمفهومه التقليدي إلا من حيث وسيلة ارتكابه، فكلاهما يقوم على وحدة الهدف والمحل وهو الحصول على معلومات ذات طابع سري عن الدولة، حيث يمكن أن تكون معلومات صناعية أو عسكريّة، كما أن التجسس بمفهومه التقليدي والمستحدث، جريمة تمس الأمن القومي للدولة وتنتهك قوانينها الخاصة بحماية أمنها الوطني، من خلال القيام بالإستيلاء على معلومات تتضمن أسرارا» خاصة بالدولة، وتسليمها إلى دولة أجنبيه سواء أكان بقصد الحصول على منفعة أم دون ذلك، مما يلحق ضرر بمصالح الدولة.

الفرع الثاني: محل الحماية الجنائية في التجسس الإلكتروني وأنواعه

لجريمة التجسس الإلكتروني طبيعة خاصة تميزها عن باقي جرائم الخيانة، من ناحية وقوعها على معلومات سرية تخص أمن الدولة الخارجي أو من حيث وسيلة ارتكابها، وكذلك تنوع المعلومات والبيانات التي يمكن أن تكون محلا لهذه الجريمة، وعليه وللتعرف إلى أنواع التجسس وطبيعة المصلحة المحمية في هذه الجريمة ستناول الموضوع على النحو الآتي:

أولا: محل الحماية الجنائية في جريمة التجسس الإلكترونية

يشكل محل الحماية الجنائية في الجرائم الواقعة على أمن الدولة الخارجي بشكل عام جميع المصالح التي يمكن أن تكون عرضة للأخطار الخارجية، و تهددها والتي قد تمس استقلال الدولة وجميع مصالحها الوطنية. ورد في (اللبيدي ،2008 ص67).

وفي هذا المقام تجدر الإشارة إلى وجود عدة تصنيفات للمعلومات المخزنة على أنظمة المعلومات والحواسيب، من ابرزها تصنيفها إلى معلومات متاحة وأخرى مقيدة، فالنوع الأول: يسمح لأي

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

شخص دون قيود الإطلاع عليها دون الحاجة إلى موافقة جهة معينة، أما النوع الثاني: فالوصول إليه يكون مقيد بشرط التصريح من الجهة المالكة للمعلومات والنظام (باطلي،2015،ص64).

فمحل الجريمة في التجسس الإلكتروني له خصوصية تتمثل في أن المحل المشمول بالحماية فيها، له خصوصية ترتبط بموضوع الجريمة الذي يقع عليه الاعتداء من حيث طبيعته الخاصة، المتمثلة بالمعلومات والبيانات المراد حمايتها وهي معلومات ذات طبيعة سرية تتعلق بأمن الدولة.

وبهذا الاتجاه عرف البعض الأسرار الخاصة بأمن الدولة أنها: عبارة عن المعلومات والبيانات أو أي شيء يرتبط بمصالح الدولة وغير مسموح لأي جهة غير مكلفة بحفظها من الاطلاع عليها أو إفشائها ما دامت مصنفة على أنها ذات طابع سري(النوايسة،2005،ص127). فهذه الأسرار تشمل مختلف أنواع المعلومات والوثائق والأشياء التي يجب أن تبقى سرية حفاظا على سلامة الدولة وكيانها ومصالحها، وهي تشمل كذلك الوثائق التي قد تحتوي على معلومات تصنف على أنها أسرار تخص أمن الدولة السياسي أو العسكري أو الاقتصادي أو العلمي والصناعي(عبيد، 2018،ص121)

وعليه لا يمكن أن تتحقق جريمة التجسس الإلكتروني، إلا إذا وقعت على محتوى الإلكتروني وباستخدام وسائل التكنولوجيا الحديثة، فطبيعة محل هذه الجريمة يجعلها تتميز عن التجسس التقليدي الذي يقع على أسرار وثائق مصنفة على أنها أسرار تخصص أمن الدولة، فمحل التجسس قد يكون على صورة بيانات أو معلومات تكون على شكل محتوى إلكتروني يمس الأمن الوطني. (النوايسة، والعدوان، 2019، ص 468 –670)

وعلاوة على ذلك يرى البعض عدم إمكانية حصر محل هذه الجريمة بالمعلومات الخاصة بالدولة ومؤسساتها، فالتجسس بالإضافة لذلك قد يقع على الأفراد وهو يشكل أهمية للجهة القائمة عليه وذلك نتيجة احتفاظ بعض الأفراد للأسرار الحساسة، فضلا عن وجود منظمات إرهابية قد تستهدف المعلومات الشخصية بهدف تجنيدهم للعمل في صفوفها (العدوي، 2018، ص 171)

فالمعلومات ذات الطابع السري بمختلف صورها، يمكن أن تأخذ شكل المحتوى الإلكتروني، وبصرف النظر عما إذا تم تقييد الوصول إليها لحمايتها باستخدام برامج خاصة، وبالتالي قد يكون المحتوى المحفوظ على أنظمة المعلومات هدفا للتجسس الإلكتروني على هذه المعلومات عن طريق اختراقها والإستيلاء عليها أو القيام بإفشائها بطرق غير مشروعة (أبو ذز شاكر، 2020،ص 44).

وأما فيما يتعلق بمحل جريمة التجسس في التشريع الفلسطيني، فقد حدد المشرع المصلحة محل الحماية في هذه الجريمة، حيث نص صراحة في الفقرة الثانية من المادة (4) من قانون الجرائم الإلكترونية على تجريم الاعتداء على المواقع الإلكترونية أو أنظمة المعلومات أو الشبكات

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الإلكترونية التي تحتوي على بيانات ومعلومات خاصة بالحكومة والمؤسسات التابعة لها. كما فرض المشرع الفلسطيني بموجب أحكام المادة (4/4) من قانون الجرائم الإلكترونية عقوبة مشددة اذا ترتب عليه أي ضرر نتيجة فعل من الأفعال المذكورة في الفقرة الثالثة من هذه المادة .

هذا وتجدر الإشارة هنا إلى أن المشرع الفلسطيني قدر عرف المقصود بالبيانات الحكومية لغايات تطبيق أحكام قانون الجرائم الإلكترونية:» بانها تلك البيانات التي تخص الدولة أو تلك التي تعود لإحدى هيئاتها والمؤسسات العامة أو الشركات التابعة لها» (المادة (1) من قانون الجرائم الإلكترونية)

ويتضح لنا من المواد المذكورة أعلاه، أن المشرع الفلسطيني نص على توفير الحماية للمعلومات والبيانات الحكومية المحفوظة على أنظمة المعلومات أو الشبكات إلالكترونية الخاصة بالحكومة ومؤسساتها، وحدد مفهوم هذه البيانات، لكنه مع ذلك لم يعمل على تصنيفها من حيث درجة سريتها، فالمشرع لم ينص على حماية خاصة عندما يكون محل الاعتداء في المادة (4) معلومات أو بيانات سرية خاصة بأمن الدولة.

وأما من ناحية المشرع الأردني فقد كان أكثر دقة من المشرع الفلسطيني من حيث تحديده محل جريمة التجسس الإلكتروني، وذلك عندما خصص مادة مستقلة نظم فيها أحكامها بشكل أكثر تفصيلا، فوفقا لأحكام هذه المادة تم تحديد أنواع مختلفة من العقوبات التي قد تفرض على كل من دخل أو وصل دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية، أو تقنية المعلومات أو أنظمة المعلومات التابعة للدولة ومؤسساتها، واطلع على بيانات أو معلومات تمس الأمن الوطني، كما شدد العقوبات إذا ترتب على الأفعال المذكورة في هذه المادة أي ضرر بها (المادة 4: من قانون الجرائم الإلكترونية لسنة 2023).

وبناء على ما تقدم يمكننا حصر نطاق محل الجريمة في التجسس الإلكتروني، الذي قد يكون هدفا لها، بأنه قد يشمل جميع المعلومات والبيانات المخزنة على أجهزة الحاسوب والأنظمة الخاصة بالدولة، والتي يمكن معالجاتها آليا وحفظها على مواقع خاصة على الإنترنت أو تسجيلها على أقراص مغناطيسية، ومصنفة على أنها سرية وتأخذ الطابع السري المرتبط بأمن الدولة.

ثانيا: أنواع التجسس الإلكتروني

في بداية ظهور التجسس بمفهومه التقليدي كسلوك مجرم، أقتصر على السعي للحصول على المعلومات العسكرية والسياسية، لكن هذا الأمر تغير بسب التطور العلمي الذي شهدته البشرية، فظهر أنواع أخرى مختلفة للتجسس الإلكتروني، شملت مختلف مجالات التطور الاقتصادي والصناعي والعلمي والعسكري، وعليه سنتناول في هذا الفرع أهم أنواع التجسس الإلكتروني على النحو التالي:

1. **التجسس العسكري:** يهدف إلى الحصول على المعلومات المرتبطة بالقطاع الأمني في الدولة، بما يتضمنه من خطط وصناعات عسكرية، وبشكل أساسي المعلومات السرية التي تخصص الجانب الأمني وهي معلومات سرية ذات قيمة استراتيجية (المومني،2010، ص.211).
2. **التجسس الاقتصادي:** يقع من خلال القيام بسرقة الأسرار التجارية أو معلومات خاصة بحقوق الملكية الفكرية أو الاستيلاء عليها دون إذن مالكها، والتصرف بها بأي شكل دون تصريح (National Counter Intelligence & Security،2018, p2) فالهدف من هذا النوع هو التعرف إلى قدرات وإمكانيات الدولة الاقتصادية، وموازنتها وديونها، وقدرتها على الاعتماد على هذه الموارد ، بالإضافة إلى ذلك التعرف إلى مرافقها الاقتصادية الحيوية ومواقعها، وتنبع أهمية هذا النوع من أهميته الاقتصاد في بناء القدرات العسكرية للدولة وأهميته في تطوير جميع مرافق الدولة. ورد في (صادق 2021، ص،18)
3. **التجسس الشخصي:** يهدف هذا النوع من التجسس على الأشخاص مراقبة حياتهم ومعلوماتهم الخاصة، لاسيما تلك الموجودة على مواقع الإنترنت (إبراهيم 2010، ص343).

مما تقدم يتبين لنا أن للتجسس الإلكتروني أنواع، وبمقدار هذا التنوع تتنوع أهدافه، بحيث تتسع لتشمل المعلومات الخاصة بأسرار الدولة بمختلف صورها المرتبطة بأمنها القومي بمفهومه الشامل، والمتمثلة بالأسرار الخاصة بالأمن السياسي والاقتصادي والعسكري والصناعي، وغيرها من هذه الأسرار ذات الطابع الحيوي بالنسبة للدولة، وكذلك يمتد ليشمل الاعتداء على الأسرار الخاصة بالأفراد والمؤسسات.

المبحث الثاني: المسؤولية الجنائية عن جريمة التجسس الإلكتروني

يكمن جوهر المسؤولية في القانون الجنائي بالبحث بمدى إمكانية تحميل الشخص مرتكب الجريمة نتيجة مخالفته لقواعد قانون العقوبات، وتطبق أحكامها من خلال العقوبات التي يمكن الحكم بها على كل من يرتكب فعل مجرم، فالعقوبة هي الأثر المترتب على المسؤولية الجنائية التي تقوم على تحقق عناصر الجريمة وأركانها جميعا، وعليه للبحث في هذ الموضوع سنتناوله في مطلبين في الأول: أركان جريمة التجسس الإلكتروني، وفي الثاني : نتناول الجزاء المقرر على التجسس الإلكتروني.

المطلب الأول: أركان جريمة التجسس الإلكتروني

تقتضي الملاحقة الجنائية لمرتكبي أي سلوك يعد جريمة، تحقق أركانها كما حددها المشرع، حيث تشكل هذه الأركان بمجملها البناء الأساسي لقيام المسؤولية الجنائية، فتوافرها يعتبر المقدمة الأساسية التي يترتب عليها توقيع الجزاء الجنائي على المتهم، وعليه سيتم البحث في هذا الموضوع

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

بشكل موجز بما يخدم موضوع البحث الرئيس، وذلك وفقا لما نص عليه المشرع في قانون الجرائم الإلكترونية، من خلال فرعين في الأول: نخصصه للركن المادي لجريمة التجسس الإلكتروني و أما الثاني: سنبحث فيه الركن المعنوي لجريمة التجسس الإلكتروني.

الفرع الأول: الركن المادي لجريمة التجسس الإلكتروني

يتكون الركن المادي للجريمة من مجموعة من العناصر، تشكل بمجملها المظهر الخارجي لها، وهو ركن أساسي يشترطه المشرع لاكتمال أركانها جميعا ، فهذا الركن يقوم على ثلاثة عناصر، هي الفعل النتيجة والرابطة السببية، ولا يختلف حال هذه العناصر في جريمة التجسس الإلكتروني؛ من حيث خضوعها للأحكام العامة في قانون العقوبات، فلابد لاكتمال هذه الجريمة تحقق جميع عناصر الركن المادي، وعليه ستناول هذه العناصر على النحو التالي:

1. **الفعل:** وهو عبارة عن المظهر الخارجي للنشاط المادي الذي يأتيه الجاني في سبيل تحقيق نتيجة إجرامية معينة معاقب عليها، وهو عنصر لابد من وجوده في كل جريمة وبالتالي يعتبر شرطا للعقاب (المجالي،2012، ص236)

وتكمن خصوصية هذا الفعل في أن التجسس الإلكتروني على المعلومات يتضمن أفعال وأنشطة متعدد يستخدمها الجاني لاختراق أنظمة الكمبيوتر، أو الشبكات للحصول على المعلومات الهامة التي قد تكون مخزنه على الأنظمة والشبكات أو تمر خلالها(Banks),2017,513p

فالسلوك المجرم في التجسس الإلكتروني يتمثل في فعل الدخول غير المشروع إلى أنظمة المعلومات، والمقصود بالدخول كل الأفعال التي تسمح للجاني بالولوج إلى النظام والوصول إلى المعلومات المحفوظة به، وهذا الفعل قد يتم بطريقة مباشرة أو غير مباشرة، ففي الحالة الأولى يدخل الفاعل كمستخدم دون أن يمتلك الحق أو التصريح بذلك ،وفي الحالة الثانية عندما يتم الدخول عن بعد من خلال الأنترنت . ورد في(الخن ،2018، ص31)

وأما في التشريع الفلسطيني فيتخذ هذا السلوك صورا متعددة، منها الدخول عمداً دون وجه حق بأي وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو تجاوز الدخول المصرح به أو الإستمرار في التواجد بها بعد العلم بانه لا يحق له التواجد في هذا الموقع(المادة 4 قانون الجرائم الإلكترونية الفلسطيني). وأما المشرع الأردني فقد حدد صور السلوك التي تقع به هذه الجريمة حيث أورد في المادة (4) من قانون الجرائم الإلكترونية صورا مختلفة يتحقق بها الركن المادي في هذه الجريمة، بحيث يشمل الدخول أو الوصول دون تصريح أو بما يخالف أو يجاوز التصريح.

2. **النتيجة:** تتحقق النتيجة الجرمية في جريمة التجسس الإلكتروني أو الدخول إلى غير المشروع بمجرد القيام بالسلوك؛ فبمجرد الدخول عمدا كافي لتجريم هذا السلوك، بغض النظر عن أحداثه أي أثر أو ضر أو أي نتيجة بمفهومها المادي.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

فالمشرع الفلسطيني لم يتطلب لاكتمال الركن المادي لهذه الجريمة بصورتها البسيطة أن يتمكن الجاني من الوصول إلى المعلومات المحفوظة على النظم المعلوماتية، واكتفى بمجرد النفاذ أو الولوج إلى هذه الأنظمة ,وهذا ما عبر عنه صراحة في المادة (4/1) «كل من دخل عمداً دون وجه حق بأية وسيلة موقعاً إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزءا منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس»..

وبطبيعة الحال لا يختلف هذا الحكم في التشريع الأردني، فقد اكتفى المشرع لمعاقبة الجاني أن يتمكن من الدخول أو الوصول دون تصريح أو بما يخالف أو يجاوز التصريح إلى الشبكة المعلوماتية ....(المادة: 4 /أ من قانون الجرائم الإلكترونية لسنة 2023) .

وعليه يتضح لنا أن التجسس الإلكتروني جريمة تعد من جرائم الخطر ،» فلم يشترط المشرع لقيامها تحقق نتيجة بمدلولها المادي، فمن الناحية القانونية مجرد القيام بالدخول عمدا أو الإطلاع على معلومات أو بيانات ذات طابع سري تخص أمن الدولة وغير متاح لأحد الإطلاع عليها دون تصريح مسبق، يعتبر هدف وليس نتيجة، ففي هذه الحالة يكفي أن يكون لدى الجاني غاية متمثلة بالدخول للإطلاع على محتوى سري يتعلق بأمن الدولة حتى ولو لم يتمكن فعلا من ذلك» (الشوابكة ومقابلة، 2024، ص279).

وأما من ناحية الشروع في جريمة الدخول غير المصرح به إلى أنظمة المعلومات أو الشبكات، يرى جانب من الفقه تصور وقوف هذه الجريمة عند مرحلة الشروع، ويتم ذلك في الحالات التي لا يتمكن بها الجاني من الدخول لهذه الأنظمة المعلوماتية لأسباب اضطراريه خارجة عن أرادته وتمنعه تحقيق أهدافه (الخن،2018،ص 33).

وفي هذا الإطار لا يختلف موقف المشرعين الأردني والفلسطيني بشأن تجريم الشروع في هذه الجريمة، فقد عاقب المشرع الفلسطيني بموجب أحكام المادة (69) من قانون الجرائم الإلكترونية على محاولة ارتكاب أي جريمة جناية أو جنحة منصوص عليها في هذا القانون، كما تبنى المشرع الأردني نفس التوجه الذي اتبعه المشرع الفلسطيني حيث عاقب على الشروع في ارتكاب هذه الجريمة عندما نص صراحة على ذلك في الفقرة (4/هـ) من قانون الجرائم الإلكترونية لسنة 2023)

3. **الرابطة السببية:** وهي العنصر الثالث من عناصر الركن المادي في الجريمة، حيث تكمن أهميتها في تحديد مقدار مسؤولية الجاني عن الجريمة المرتكبة، وتتفاوت أهميتها من جريمة لأخرى ، حيث تعتبر في جرائم الضرر من العناصر التي يجب أثباتها والتحقق من وجودها، وأما الجرائم ذات الخطر لا تعتبر فيها هذه الرابط ذات أهمية.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وفي جريمة التجسس كما سبق وتم الإشارة إلى أن التجسس في صورته البسيطة يكفي لتحقق النتيجة، مجرد القيام بالدخول بصورة غير مشروعة أو البقاء بشكل يتجاوز التصريح الممنوح ،ففي هذه الحالة لا تظهر للرابطة السببية أهمية لقيام الركن المادي في هذه الجريمة. وفي المقابل يجب إثبات هذه الرابطة والتحقق من قيامها بين السلوك والنتيجة وذلك إذا ترتب على هذا السلوك ضرر بسب الاعتداء على المعلومات والبيانات المخزنة على أنظمة المعلومات والشبكات، وهو يكون في حال اقتران الدخول بظرف من الظروف المشددة.

الفرع الثاني: الركن المعنوي في جريمة التجسس الإلكتروني

جريمة التجسس الإلكتروني المتمثلة بالدخول غير المشروع إلى أنظمة المعلومات والشبكات تعتبر من الجرائم المقصودة، حيث يتخذ ركنها المعنوي صورة القصد الجرمي العام الذي يتطلب توافر عنصري العلم والإرادة لدى الجاني وقت ارتكاب الجريمة.

وعليه يجب أن يكون الجاني عالما أن فعله يشكل خطورة على الأنظمة والمعلومات والبيانات المخزنة عليها، وأن سلوكه سوف يؤدي إلى الدخول إلى أجهزة الحاسوب أو الشبكات أو أنظمة المعلوماتية أو موقع الإلكترونية وكذلك يجب أن يكون عالما أنه لا يحق له الدخول و انتهاء التصريح للاستمرار والبقاء في هذه المواقع والأنظمة.

وأما فيما يتعلق بعنصر الإرادة، فيجب أن تتجه إلى فعل الدخول غير المصرح به، أو الاستمرار به بعد علمه بانتهاء التصريح، لذا اذا ثبت أن الفاعل كان يعتقد انه يجوز له الدخول إلى الشبكة أو الأنظمة المعلوماتية، فأن القصد الجنائي في هذه الحالة لا يتحقق في سلوكه .

كما أن هذا القصد أيضا لا يتوافر اذا وجد الشخص نفسه داخل نظام طريق الخطأ خلال قيامه بتصفح للأنترنت دون أن يكون مصرحا له بذلك، ولكن هذا الحكم يختلف إذا تعمد الشخص بالبقاء داخل الموقع الذي دخله عن طريق الخطأ اذا وجه أرادته إلى الاستمرار بالتواجد مع علمه بان لا يحق له ذلك ففي هذه الحالة يتوافر القصد الجرمي العام المطلوب لتحقق الجريمة (الخن،2018،ص33).

ويرى البعض أنه وبالرغم من أن المشرع اكتفى بالقصد العام لتحقق الركن المعنوي في هذه الجريمة ، ألا أنه ذهب في فرض عقوبات مشدد في حال تجاوز الدخول هذا القصد وترتب عليه نتائج معينة تتمثل بالحذف أو الإتلاف أو النسخ وغيرها من الأفعال التي تشكل خطورة على المحتوى السري الخاص بأمن الدولة (الشوابكة، ومقابلة 2024،ص291)

المطلب الثاني: العقوبات المقررة على جريمة التجسس الإلكتروني

وفقًا لإحكام قانون الجرائم الإلكترونية الفلسطيني، وكذلك الأردني يواجه مرتكب جريمة بالتجسس الإلكتروني عقوبات متنوعة، بالإضافة إلى الظروف التي تشدد بها العقوبة على مرتكبها وسنتناولها على النحو الآتي:

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الفرع الأول: عقوبة التجسس الإلكتروني بصورته البسيطة

فرض المشرع الفلسطيني عقوبة على جريمة الدخول غير المشروع إلى مواقع أو شبكة تحتوي على البيانات والمعلومات الحكومية، الحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو بكلتا العقوبتين (المادة 2/4 من قانون الجرائم الإلكترونية الفلسطيني)

وأما المشرع الأردني فقد حدد عقوبة الحبس مدة لا تقل عن ستة أشهر ولا تزيد على ثلاث سنوات، والغرامة لا تقل عن ألفين وخمسمائة دينار ولا تزيد على خمسة وعشرين ألف دينار وذلك عندما ترتكب هذه الجريمة بصورتها البسيطة كما حددتها الفقرة (أ/4) المتمثلة بالدخول أو الوصول دون تصريح أو بما يخالف أو يجاوز التصريح أو الاطلاع على البيانات الخاصة بالأمن الوطني وغيرها من البيانات غير المتاحة للجمهور.

كما فرض المشرع عقوبة الحبس مدة لا تقل عن 4 شهور ولا تزيد على 3 سنوات، والغرامة المالية وبغرامة لا تقل عن ألفين وخمسمائة دينار ولا تزيد على خمسة وعشرين ألف دينار وذلك في حال 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 تسهم 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.

ويلاحظ من خلال استعراض العقوبات التي فرضها المشرع الفلسطيني والأردني على هذه الجريمة بصورتها البسيطة، والتي تقع بأفعال كالدخول أو البقاء بشكل يجاوز التصريح الممنوح للشخص في هذه الأنظمة، أو مجرد الاطلاع علي المعلومات سرية غير المتاحة للجمهور، بانها عقوبة تضعها ضمن إطار جرائم الجنح، وهذا الوصف بحد ذاته يتناسب وخطورة هذه الأفعال، وذلك استنادا إلى مبدأ التناسب بين الجريمة والعقوبة، على اعتبار أن مجرد الدخول أو الإطلاع لا يشكل تلك الخطورة على هذه الأنظمة.

ولكن وفي المقابل وبالرغم من تشابه الوصف القانوني لهذه الجريمة في كلا التشريعين، ألا أن هناك تفاوت بينهما في مقدار عقوبة الغرامة المالية التي يمكن الحكم بها على مرتكبها ، فالمشرع الأردني كان اكثر تشددا في قيمة هذه الغرامة من المشرع الفلسطيني، وهذا بدوره يضمن تحقيق الردع ضد مرتكبي هذه الجرائم وتوفير الحماية اللازمة لأنظمة المعلومات والمواقع الإلكترونية.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الفرع الثاني: عقوبة التجسس الإلكترونية بصورتها المشدة

قد تقترن جريمة التجسس الإلكتروني بمجموعة من الظروف تؤثر على وصفها القانوني وتحوله إلى جناية، وتزيد من مقدار العقوبة المقررة لها بصورتها البسيطة، فبموجب أحكام الفقرة (4/4) من قانون الجرائم الإلكترونية شدد المشرع الفلسطيني العقوبة على جريمة الدخول غير المشروع إلى نظام معلوماتي بحيث تكون العقوبة السجن مدة لا تزيد عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد عن خمسة آلاف دينار أردني وذلك في حال ترتب على الدخول ضرر على النحو المذكور في الفقرة(3) من هذه المادة وكانت المعلومات المستهدفة تعود للحكومة.

كما حدد المشرع الأردني عقوبات مشددة على الدخول غير المشروع إلى أنظمة المعلومات والشبكات التي تحتوي معلومات خاصة بالأمن الوطني للدولة الأردنية، فبموجب أحكام (المادة4/ب)» إذا كان الدخول أو الوصول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسخها أو نشرها أو إعادة نشرها أو خسارة سريتها أو تشفيرها أو حذفها أو إضافتها أو حجبها أو إفشائها أو التقاطها فيعاقب الفاعل بالأشغال المؤقتة وبغرامة مالية لا تقل عن خمسة آلاف دينار ولا تزيد على خمس وعشرون الف دينار ، ويعاقب بالأشغال المؤقتة مدة لا تقل عن خمس سنوات والغرامة خمسة وعشرين ألف دينار إذا تمكن من تحقيق النتيجة»

كما شدد المشرع الأردني العقوبة المقرر لهذه الجريمة في حال أدت الأفعال المذكورة في الفقرة (ج) من هذه المادة (4) إلى الحاق الضرر بالمعلومات أو البيانات بأي صور من الصور من المذكورة بهذه الفقرة ، فجعل عقوبتها الأشغال المؤقتة غرامة مالية لا تقل عن (5000) ولا تزيد على (25000) دينار اردني.

ولتطبيق الظروف المشددة المقترنة بهذه الجريمة يرى جانب من الفقه أن القصد العام لا يكفي للقيام الركن المعنوي المطلوب للتشديد، و أنما يتطلب توافر القصد الخاص بالإضافة إلى القصد العام الذي يقوم على العلم والإرادة، فالقصد الخاص المطلوب في هذه الحالة هو توافر العلم لدى الجاني أنه يرتكب أحد الأفعال التي قد تسبب ضرر للمعلومات المحفوظة على أنظمة المعلومات، وأن تتجه أرادته إلى ارتكابها وتحقيق نتيجة معينة.(الخن ،2018،ص33).

ويلاحظ من خلال ذكر الظروف المشددة التي قد تقترن بها هذه الجريمة، أن المشرع الفلسطيني وكذلك المشرع الأردني، لم ينص على اعتبار التجسس الإلكتروني لصالح دولة اجنبيه معادية، أو في حالة حرب، وبالرغم من خطورته من ضمن الظروف المشدد للعقوبة على هذه الجريمة، الأمر الذي يتطلب من المشرع إجراء التعديل اللازم بما يتناسب مع خطورة هذا الفعل عندما يرتكب في ظروف تكون فيها الدولة في حالة عداء أو حرب مع دولة أخرى.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

وأما فيما يتعلق في العقوبات المقررة على الشروع في هذه الجريمة فقد عاقب المشرع الفلسطيني والأردني على محاولة ارتكابها، فمن ناحية المشرع الفلسطيني عاقب على الشروع في جميع الجنايات والجنح المنصوص عليها في قانون الجرائم الإلكترونية، حيث نص صراحة على ذلك في (المادة69: من قانون الجرائم الإلكترونية الفلسطيني). كما أن المشرع ذهب في الاتجاه نفسه وعاقب على الشروع في ارتكاب التجسس بالعقوبة المقررة للجريمة بصورتها التامة(المادة 4/هـ من قانون الجرائم الإلكترونية لسنة 2023).

وعليه وبعد استعراض السياسة العقابية للمشرع الفلسطيني والأردني في الجزاء المقرر للتجسس الإلكتروني، يلاحظ وجود توافق في السياسة المتبعة لاسيما في التمييز في العقوبات المقررة على هذه الجريمة والنص على الظروف المشددة التي تقترن بها هذه الجريمة، بالإضافة إلى العقاب على الشروع في ارتكاب هذه الجرائم بغض النظر عن نوعها جنحة أو جناية، وكذلك عدم النص على تشديد العقوبة على التجسس الذي يقع لصالح دولة معادية، ولكن المقابل يلاحظ وجود تباين في مقدار العقوبات السالبة للحرية والغرامات المالية المقررة سواء كانت الجريمة بصورتها البسيطة أو المشددة أو كانت في مرحلة الشروع ، فالمشرع الأردني ذهب باتجاه التدرج والتشدد في العقوبات على مرتكبي هذه الجريمة، لاسيما في حال وقوعها على معلومات وبيانات تمس الأمن الوطني للمملكة الأردنية، وهذه بدور يحقق الردع والحماية الجنائية المناسبة لأمن الدول من هذه الجريمة

وخلاصة القول في هذا الجانب يرى الباحث أن المشرع الأردني ذهب بالاتجاه الصحيح في سياسته الجنائية في تحديده للعقوبات التي قد تفرض على مرتكبي التجسس الإلكتروني، بالإضافة إلى نصه على الظروف المشددة التي تتناسب وهذه الجريمة، وذلك انطلاقا من خطورتها على الأمن الوطني وما قد تلحقه هذه الجريمة من أضرار على الدولة ومؤسساتها. أما من ناحية المشرع الفلسطيني ونظرا لعدم وضع المشرع أحكام خاصة تنظم وقوع هذه الجريمة على معلومات أو بيانات سرية تخص امن الدولة، فإن موضوع هذه الجريمة وما يقترن بها من ظروف قد تضاعف من خطورتها في ظل الواقع الفلسطيني يتطلب من المشرع التدخل لأجراء التعديلات المناسبة على النصوص ذات العلاقة في قانون الجرائم الإلكترونية التي يمكن من خلالها مواجهة هذه الجريمة وتطورها.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

الخاتمة

فرض التجسس الإلكتروني تحديًات كبيرة على الدول في ظل التطور التكنولوجي، حيث أثر على الأمن الوطني للدولة واستقرارها السياسي والاقتصادي. ومع استمرار هذا التطور مستقبلا قد تتطور أيضًا أساليب ارتكاب التجسس الإلكتروني ودوافعه وبالتالي تزداد خطورته. لذا فإن معالجة هذا التهديد يتطلب تنظيما قانونية يتناسب مع هذه الخطورة، بشكل يضمن القيام باتخاذ جميع الإجراءات القانونية اللازمة على الصعيد التشريعي؛ لتعزيز الحماية الجنائية للأسرار الخاصة بأمن الدولة، وذلك لمساندة الإجراءات الفنية الموضوعة لحماية إمن المعلومات.

النتائج والتوصيات

أولا: النتائج

- يشكل التجسس الإلكتروني في العصر الحالي واحدة من أخطر الجرائم التي تمس أمن الدولة الخارجي، لما ينتج عنه من أضرار كبيرة قد تلحق بمصالحها القومية.
- أن التجسس الإلكتروني لا يختلف عن التجسس بمفهومه التقليدي ألا من حيث وسيلة ارتكاب الجريمة وخطورته وتنوع أهدافه.
- يُتمثل التجسس الإلكتروني في القيام بالدخول إلى نظام معلوماتي خاص بالدولة من أجل الحصول على معلومات سرية تمس بأمنها.
- لمحل التجسس جريمة الإلكتروني خصوصية تتمثل في وقوعه على معلومات وبيانات سرية خاصة بأمن الدولة.
- لم يميز المشرع الفلسطيني في المادة (4) من قانون الجرائم الإلكترونية بين المعلومات الحكومية العادية وتلك المعلومات ذات الطابع السري المتعلق بأمن الدولة
- لم يخصص المشرع الفلسطيني كما فعل المشرع الأردني في قانون الجرائم الإلكترونية حماية خاصة للأسرار المرتبطة بأمن الدولة في قانون الجرائم الإلكترونية من التجسس
- لم ينص المشرع الفلسطيني والأردني على ظرف مشددة في حالة وقوع التجسس الإلكتروني على معلومات تخصص أمن الدولة لصالح دولة اجنبيه معادية أو في وقت الحرب.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

ثانيا: التوصيات

- نوصي المشرع الفلسطيني العمل على التمييز بين المعلومات الحكومية العادية والمعلومات السرية التي تخص أمن الدولة.
- ضرور قيام المشرع الفلسطيني على غرار المشرع الأردني وضع نص مستقل في قانون الجرائم الإلكترونية يبن فيه الإحكام الخاصة بالاعتداء على المعلومات والبيانات الحكومية السرية.
- نوصي المشرع الفلسطيني وكذلك الأردني بالنص على ظرف مشددة في حالة وقوع التجسس الإلكتروني على معلومات تخصص أمن الدولة لصالح دولة اجنبيه معادية أو في حالة وقوعه زمن الحرب.
- نوصي المشرع الفلسطيني العمل على تعديل الفقرة الثانية والرابعة من المادة (4) من قانون الجرائم الإلكترونية ونقترح التعديل الآتي: 2. إذا ارتكبت الأفعال المذكورة في الفقرة (1) من هذه المادة على المعلومات أو البيانات الحكومية أو المؤسسات التابعة لها أو اطلع على معلومات سرية تمس أمن الدولة ي يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.
- وأما بخصوص الفقرة الرابعة نقترح التعديل التالي – إذا وقع الفعل المذكور في الفقرة(3) من هذه المادة على معلومات سرية تخص أمن الدولة يعاقب الفاعل بالسجن مدة لا تقل عن خمس سنوات و لا تتجاوز عشر سنوات وبغرامة مالية لا تقل عن خمسة آلأف دينار اردني ولا تزيد عن عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً في الأراضي الفلسطينية.

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

قائمة المراجع

أولا: المراجع العربية

أبو ذر، شاكر (2020). جريمة التجسس الإلكتروني في التشريع الأردني، مجلة العلوم السياسية والقانون، 26(4).

إبراهيم، خالد (2010). فن التحقيق في الجرائم الإلكترونية، الإسكندرية: دار الفكر الجامعي

باطلي، غنية (2015). الجريمة الإلكترونية دراسة مقارنة، الجزائر: الدار الجزائرية للنشر والتوزيع.

برهان، رزق الله (2018). جريمة التجسس (أمن الدولة)، رسالة ماجستير، جامعة العربي التبسي ،كلية الحقوق والعلوم السياسية.

خن، طارق (2018). جرائم المعلوماتية، سوريا: منشورات الجامعة السورية الافتراضية

سلامي، نادية (2019). آليات مكافحة التجسس الإلكتروني، أطروحة مقدمة لنيل شهادة دكتوراه العموم في القانون الجنائي، جامعة العربي التبسي – تبسة، الجزائر.

سرور، احمد (2002). القانون الجنائي الدستوري، (ط2)، القاهرة: دار الشروق.

شوابكة برجس، ومقابلة حسن (2024). تجريم التجسس الإلكتروني في التشريع الجزائي الأردني، مجلة المنار، سلسلة العلوم السياسية والقانون، 3(4).

صادق، مدحت (2021). جريمة الاتصال غير المشروع بالجهات الأجنبية والعقوبات المقرر عليها في الشريعة الإسلامية والقانون الوضعي، جامعة المنصورة.

صالح، تامر (2019). الحماية الجنائية للمعلومات الرسمية، دراسة مقارنة، مجلة القانون والاقتصاد، ملحق خاص (92).

عدوي، علي (2018). مكافحة التجسس الإلكتروني في الشريعة الإسلامية مقارنا بالقانون الدولي، مجلة أصول الشريعة للأبحاث المتخصصة، 4(4).

عبيد، عماد (2018). قانون العقوبات الخاص(2)، سوريا: منشورات الجامعة السورية الافتراضية

عوشن، وليد (2013). الحماية الجنائية لإسرار الدولة في النظام السعودي، رسالة دكتوراه، جامعة نايف، الرياض.

قرار بقانون بشان الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات رقم (10) لسنة 2018 وتعديلاته.

قانون الجرائم الإلكترونية الأردني رقم (17) لسنة 2023 .

قانون حماية أسرار وثائق الدولة لسنة 1971.

قانون العقوبات الأردني رقم(16) لسنة 1960 النافذ في الضفة الغربية.

لبيدي، إبراهيم (2008). الحماية الجنائية لأمن الدولة، مصر: دار الكتب القانونية

مجالي، نظام (2012). شرح قانون العقوبات ،القسم العام، دراسة تحليلية في النظرية العامة والمسؤولية الجنائية، عمان: دار الثقافة للنشر والتوزيع

مومني، نهلا (2010). الجرائم المعلوماتية، عمان–الأردن: دار الثقافة للنشر والتوزيع

نوايسة عبد الإله، والعدوان ممدوح (2019). جرائم التجسس الإلكتروني في التشريع الأردني، دراسة تحليلية، مجلة دراسات علوم الشريعة والقانون، 46(1).

نوايسة، عبد الإله (2005). الجرائم الواقعة على أمن الدولة في التشريع الأردني، (ط1)، عمان: دار وائل للنشر والتوزيع

ثانياً: المراجع العربية باللغة الإنجليزية

Abu thar, S. (2020). The Crime of cyber Espionage in Jordanian Legislation, Journal of Political Science and Law, 26(4): Arab Democratic Center – Berlin.

Abaid, A. (2018). Special Penal Code (2), Syria: Publications of the Syrian Virtual University.

Adawi, A. (2018). Combating Electronic Espionage in Islamic Sharia Compared to International Law, Journal of Usul al-Sharia for Specialized Research, 4(4).

Batali, G. (2015). Cybercrime: A Comparative Study, Algeria: Algerian House for Publishing and Distribution.

Burhan, R. (2018). The Crime of Espionage (State Security), Master's Thesis, Arab Tebessi University, Faculty of Law and Political Science Decree-Law No. (10) of 2018 Concerning Cybercrimes, Communications and Information Technology Crimes and its Amendments.

Ibrahim, K. (2010). The Art of Investigating Cybercrimes, Alexandria: Dar Al-Fikr Al-Jami

Jordanian Cybercrime Law No. (17) Of 2023.

Jordanian Penal Code No. (16) Of 1960, applicable in the West Bank.

Khen, T. (2018). Cybercrimes, Syria: Publications of the Syrian Virtual Universit.

Labidi, I. (2008). Criminal Protection of State Security, Egypt: Dar Al-Kotob Al-Qanuniyah.

Majali, N. (2012). Explanation of the Penal Code, General Section, An Analytical Study of the General Theory and Criminal Liability, Amman: Dar Al-Thaqafa for Publishing and Distribution

Momani, N. (2010). Cybercrimes, Amman, Jordan: Dar Al-Thaqafa for Publishing and Distribution

Nawaisa, A., & Al-Adwan, M. (2019). Cyber Espionage Crimes in Jordanian Legislation: An Analytical Study, Journal of Sharia and Legal Studies, 46(1): Supplement (1)

https://journal.pass.ps « DOI: 10.36554/1796-010-999-001 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854

Nawaiseh, A. (2005). Crimes Against State Security in Jordanian Legislation, (1st ed.), Amman: Wael Publishing and Distribution House.

Oushan, W. (2013). Criminal Protection of State Secrets in the Saudi System, PhD Thesis, Riyadh: Naif- University Publication

Sadiq, M. (2021). The Crime of Illegal Communication with Foreign Entities and its Penalties in Islamic Sharia and Positive Law, Mansoura University: College of Graduate Studies

Salami, N. (2019). Mechanisms for Combating Electronic Espionage, a thesis submitted for a PhD in Criminal Law, Arab Tebessi University - Tebessa - Faculty of Law and Political Science

Saleh, T. (2019). Criminal Protection of Official Information: A Comparative Study, Journal of Law and Economics, Special Supplement (92).

Shawabka, B. & Muqabla, H. (2024). Criminalization of Electronic Espionage in Jordanian Criminal Legislation, Al-Manar Journal, Political Science and Law Series, 3(4):

Sorur, A. (2002). Constitutional Criminal Law, (2nd ed.), Cairo: Dar Al-Shorouk

State Document Secrets Protection Law of 1971

ثالثاً: قائمة المراجع باللغة الإنجليزية

Banks, C. W. (2017). Cyber Espionage & Electronic Surveillance: beyond the Media Coverage, Emory Law Journal, 66(3): 512-525.

Brown, G. (2016). Spying and Fighting in Cyberspace: What is which?, Journal of National Security Law & Policy , 8(3).

Darien, P. (2017) Rethinking Espionage in the Modern Era, Chicago Journal of International Law, 18 (1).

Dayyani, A. (2016). Electronic Data & Information Espionage: Civil or Criminal Liability, Journal of Law, Policy and Globalization, ISSN 2224-3240

Foreign Economic Espionage .(2018)National Counter Intelligence & Security Center - in Cyberspace

رابعا: المواقع الإلكترونية

Cambridge Dictionary (n.d). retrieved from: https://dictionary.cambridge.org/dictionary/english/espionage

Center for Development of Security Excellence (n.d.). Insider Threat, retrieved from: https://www.cdse.edu/Training/Insider-Threat/

- cyble (2025). What is Cyber Espionage?, retrieved from: https://cyble.com/knowledge-hub/what-is-cyber-espionage/

Britannica (2025). Cold War, retrieved from: https://www.britannica.com/event/Cold-War

https://journal.pass.ps « DOI: 10.36554/1796-010-999-002 « ISSN (Print): 2518-5756 « ISSN (Online): 2707-4854