Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss
AJSS

Criminal Liability for Eavesdropping via the Internet and Computers in the Saudi Law

المسؤولية الجنائية عن التنصت عبر الشبكة المعلوماتية وأجهزة الحاسب الآلي في النظام السعودي

متعب سعد دليبح المطيري
جامعة نايف العربية للعلوم الأمنيَّة، الرياض، المملكة العربية السعودية

Mutaib Saad Dulaibh Al-Mutairi
Naif Arab University for Security Sciences, Riyadh, Kingdom of Saudi Arabia

Received 25 Jul. 2025; accepted 9 Oct. 2025; available online 9 Dec. 2025

Abstract

The study aims to examine the legal basis of criminal liability arising from the offense of eavesdropping through the internet or a computer device under the Saudi Anti-Cybercrime Law. This research adopts an analytical approach to the relevant statutory provisions by identifying the constitutive elements of this offense, determining its possible forms of commission, and explaining its legal consequences.

The findings indicate that eavesdropping represents one of the most serious violations of digital privacy and is based on three essential pillars: the statutory provision criminalizing the act, the conduct consisting of eavesdropping, interception, or acquisition without legal authorization, and the criminal intent reflected in the offender's awareness of the illegality of such conduct. The study further concludes that the offense may occur by way of attempt or participation, and that the prescribed penalties include imprisonment and fines, with aggravated penalties in cases involving public officials or organized collective action. The study recommends reviewing the upper limits of penalties to reflect the varying degrees of gravity asso-

Keywords: *security studies, criminal responsibility, eavesdropping, information network, computer device, cybercrimes*

المستخلص

تهدف هذه الدراسة إلى بيان الأساس القانوني للمسؤولية الجنائية الناشئة عن جريمة التنصت عبر الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي في ظل أحكام نظام مكافحة الجرائم المعلوماتية السعودي. وقد اعتمدت الدراسة على المنهج التحليلي للنصوص النظامية ذات الصلة، من خلال الكشف عن الأركان المكوّنة لهذه الجريمة، وتحديد صور ارتكابها وآثارها النظامية. وتوصلت النتائج إلى أن جريمة التنصت تُعدُّ من أبرز صور الاعتداء على الخصوصية الرقمية، وتقوم على ثلاثة أركان رئيسة: النص النظامي المجرّم للفعل، والسلوك المتمثل في التنصت أو الاعتراض، أو الالتقاط دون مسوغ مشروع، والقصد الجنائي القائم على إدراك الجاني لعدم مشروعية فعله. كما ثبت أن الجريمة قد تتحقق بطريق الشروع أو المساهمة الجنائية، وأن العقوبات المقررة لها تتنوع بين السجن والغرامة، وتُشدد في حال ارتكابها من موظف عام، أو ضمن إطار جماعي منظم. وأوصت الدراسة بمراجعة سقف العقوبات بما يتناسب مع خطورة صور الجريمة المختلفة، وتفعيل

الكلمات المفتاحية: الدراسات الأمنية، المسؤولية الجنائية، التنصت، الجرائم المعلوماتية، الشبكة المعلوماتية، أجهزة الحاسب الآلي

* Corresponding Author: *Mutaib Saad Dulaibh Al-Mutairi*
Email: 202300086@student.nauss.edu.sa

doi: 10.26735/QRXF7901

Production and hosting by NAUSS

1319-1241© 2025. AJSS. This is an open access article, distributed under the terms of the Creative Commons, Attribution-NonCommercial License.

الوسائل التقنية الوقائية للحد من وقوعها، وتوسيع نطاق التوعية النظامية لحماية الخصوصية المعلوماتية وتعزيز الثقة في البيئة الرقمية.

ciated with the different forms of the offense, adopting preventive technical measures to mitigate its occurrence, and expanding legal awareness initiatives to protect informational privacy and reinforce trust in the digital environment.

1. المقدمة

شهد العالم في العقود الأخيرة تطورًا تقنيًا متسارعًا رافقه توسع كبير في استخدام الحاسب الآلي والشبكات المعلوماتية؛ مما أسفر عن ظهور أنماط مستحدثة من السلوك الإجرامي، تمس القيم الاجتماعية والأمنية، وتؤثر في استقرار المجتمعات. وقد برزت الجرائم المعلوماتية بوصفها من أبرز التحديات المعاصرة التي تواجه الدول في سعيها لحماية الأفراد وضمان بيئة رقمية آمنة.

وتأتي جريمة التنصت عبر الشبكة المعلوماتية أو أجهزة الحاسب الآلي في مقدمة هذه الجرائم؛ لما تنطوي عليه من مساس مباشر بالحياة الخاصة وحق الأفراد في السرية وصون المعلومات. وتتضاعف خطورة هذه الجريمة في ظل ما أتاحته التقنيات الحديثة من وسائل خفية ومتطورة، تسهّل ارتكابها، بما ينعكس سلبًا على الثقة في التعاملات الإلكترونية والأمن المجتمعي.

وانطلاقًا من خطورة هذا الفعل، أفرد المنظم السعودي نصوصًا خاصة لتجريم التنصت الإلكتروني ضمن نظام مكافحة الجرائم المعلوماتية، تأكيدًا لوعي الدولة بتداعياته على الأمن العام والثقة في البنية التقنية.

وفي هذا الإطار، يتناول هذا البحث المسؤولية الجنائية الناشئة عن جريمة التنصت عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي، من خلال تحليل أركانها وعناصرها والعقوبات المقررة لها، استنادًا إلى النصوص النظامية والأسس الفقهية والقانونية ذات الصلة، بغية بيان أبعادها النظرية وتطبيقاتها العملية.

أهمية الدراسة

تبرز أهمية هذه الدراسة في ضوء التطورات المتسارعة في المجال الرقمي، وما رافقها من ظهور جرائم تهدد خصوصية الأفراد وأمنهم المعلوماتي، وفي مقدمتها جريمة التنصت غير المشروع عبر الشبكة المعلوماتية، أو أجهزة الحاسب الآلي. وتتجلى هذه الأهمية من جانب نظري في توضيح الإطار المفاهيمي والقانوني لهذه الجريمة وبيان أبعادها الجنائية، ومن جانب عملي في إبراز دور المنظم السعودي في حماية الحقوق الأساسية وصون الحياة الخاصة من خلال النصوص النظامية ذات الصلة.

مشكلة الدراسة

تتمثل مشكلة هذه الدراسة في تحديد الطبيعة القانونية للمسؤولية الجنائية الناشئة عن جريمة التنصت عبر الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي وَفق نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية، وما يثيره ذلك من إشكالات تتعلق بحدود التجريم والعقاب، ومدى كفاية النصوص النظامية القائمة في مواجهة هذا النمط المستحدث من الجرائم.

أسئلة الدراسة

1. ما المقصود بجريمة التنصت وفقًا لنظام الجرائم المعلوماتية؟
2. ما أركان جريمة التنصت وفقًا لنظام الجرائم المعلوماتية؟
3. ما الأوصاف التي تلحق بجريمة التنصت عن طريق الشبكة المعلوماتية؟
4. ما العقوبة المقررة لجريمة التنصت وفقًا لنظام مكافحة الجرائم المعلوماتية؟

الدراسات السابقة

- **الدراسة الأولى:** دراسة هانيا فقيه، وعنوانها «حماية الحق في الخصوصية المعلوماتية» دراسة تحليلية لواقع الحماية وتحديات العصر، مجلة الدراسات القانونية والاقتصادية، 2018.

وهدفت الدراسة إلى تحليل الإطار القانوني لحماية الخصوصية المعلوماتية في التشريع اللبناني، مع التركيز على أبرز التحديات التقنية والقانونية التي تواجه سبل مكافحة الانتهاكات الرقمية. واعتمدت على المنهج التحليلي في دراسة النصوص التشريعية ذات الصلة، إلى جانب تتبع الجهود الدولية في هذا المجال.

وتوصلت الباحثة إلى أن جوهر الإشكال لا يكمن في أفعال المعتدين على الخصوصية، وإنما في قصور التشريعات التقليدية التي وُضعت قبل انتشار الإنترنت؛ مما جعل بعض الممارسات الحديثة خارج نطاق التجريم لغياب النصوص النظامية الكافية. وأوصت الدراسة بتحديث المنظومة التشريعية بما يواكب التطورات الرقمية، وإدراج مقرر دراسي حول أخلاقيات استخدام الإنترنت ضمن المناهج التعليمية، وتعزيز التعاون الدولي بين الجهات المعنية بحماية الخصوصية المعلوماتية.

وتتقاطع هذه الدراسة مع الدراسة الحاليَّة في اهتمامهما بالجرائم المعلوماتية من زاوية الاعتداء على الحياة الخاصة، غير أن دراستي تنفرد بمعالجة جريمة التنصت تحديدًا في إطار نظام مكافحة الجرائم المعلوماتيَّة السعودي دون التوسع في تشريعات مقارنة أخرى.

- **الدراسة الثانية:** دراسة سعد حسنين بعنوان «أحكام المسؤولية الجنائية عن الجرائم المعلوماتية: دراسة مقارنة». مجلة الدراسات القانونية والاقتصادية، 2023.

تُعدُّ هذه الدراسة دراسة تحليلية مقارنة جمعت بين التشريع الجنائي المصري والتشريعات الجنائية الدولية، وهدفت إلى تطوير المنظومة القانونية المصرية بما يضمن مواجهة فعَّالة للجرائم المعلوماتية المستحدثة.

وقد انتهت الدراسة إلى أن التشريع المصري لم يُحط بعد بالمسؤولية الجنائية عن أفعال المتطفلين عبر شبكة الإنترنت، وأن صور المساهمة الجنائية الواردة في قانون مكافحة جرائم تقنية المعلومات ما تزال قاصرة عن ضبط الأشكال المتنوعة للسلوك الإجرامي الإلكتروني؛ مما يتيح لبعض الجناة فرصة الإفلات من العقاب. كما خلصت إلى أن العقوبات المقررة لا ترقى إلى مستوى الردع المطلوب. ومن ثمَّ أوصت الدراسة بضرورة تدخل المشرّع المصري لوضع أوصاف قانونية دقيقة للأفعال التي يرتكبها المتدخلون عبر الإنترنت، وتوسيع نطاق التجريم في صور المساهمة الجنائية، مع الاسترشاد بالتجارب التشريعية المقارنة، ولا سيما في فرنسا والإمارات العربية المتحدة والمملكة العربية السعودية.

وتتشابه هذه الدراسة مع الدراسة الحاليَّة في اهتمامهما بالمسؤولية الجنائية عن الجرائم المعلوماتية، غير أن دراستي تنفرد بمعالجة الموضوع في إطار النظام السعودي حصرًا، دون التوسع في المقارنات التشريعية، فضلًا عن أنها تركز على جريمة التنصت عبر الشبكة المعلوماتية باعتبارها إحدى صور الجرائم المتعددة.

منهج الدراسة

اعتمدت هذه الدراسة على المنهج التحليلي؛ وذلك من خلال تفسير نصوص نظام مكافحة الجرائم المعلوماتية وبيان دلالاتها النظامية، مع تحليل الأحكام المتعلقة بجريمة التنصت عبر الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، بهدف تحديد الأساس القانوني لهذه الجريمة وتوضيح نطاق المسؤولية الجنائية المترتبة عليها.

2. المبحث الأول: ماهية جريمة التنصت عن طريق الشبكة المعلوماتية وأركانها

لبيان المسؤولية الجنائية الناشئة عن جريمة التنصت عبر الشبكة المعلوماتية أو أجهزة الحاسب الآلي، يلزم أولًا تحديد مفهوم الجريمة وبيان صور الخصوصية التي يمسّها فعل التنصت غير المشروع، ثم الانتقال إلى دراسة أركانها وفق القواعد العامة للجريمة، من خلال توضيح كل من الركن المادي والمعنوي. وسيتم تناول ذلك في المطلبين الآتيين.

2. 1. المطلب الأول: مفهوم جريمة التنصت وتمييزها عن غيرها

يُعَدُّ التنصت عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي من أبرز صور الاعتداء على حرمة الحياة الخاصة؛ لما يمثله من كشفٍ غير مشروع لما يتبادله الأفراد من معلومات دون علمهم أو إذنهم. وقد حرص المنظّم السعودي على تجريم هذا السلوك بموجب نظام مكافحة الجرائم المعلوماتية، إدراكًا لما ينطوي عليه من تهديد للخصوصية والأمن المعلوماتي، غير أن تحديد مفهوم هذه الجريمة يقتضي أولًا بيان دلالتها النظامية والفنية (كفرعٍ أول)، ثم تمييزها عن الأفعال القريبة منها، مثل: التجسس أو التسجيل غير المصرح به، أو التقاط الصور، منعًا للخلط وضمانًا لحسن تطبيق النصوص النظامية (كفرعٍ ثانٍ).

2. 1. 1. الفرع الأول: تعريف جريمة التنصت في ضوء نظام مكافحة الجرائم المعلوماتية

من الجدير بالذكر أنه على الرغم من النص في المادة الثالثة من نظام مكافحة الجرائم المعلوماتية على أنه: «يعاقب بالسجن مدة لا تزيد على سنة، وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًّا من الجرائم المعلوماتية الآتية: التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه» (هيئة الخبراء بمجلس الوزراء، 2007).

إلا أنه لم يرد تعريف لمفهوم التنصت ضمن المفاهيم التي أشار إليها المنظم السعودي في المادة الأولى من النظام، ومع ذلك فقد قام جانب من الفقه بتعريف التنصت أو التجسس على خصوصيات الناس وانتهاك الخصوصية بأنه «أي عمل يقوم به شخص أو مجموعة من الأشخاص للحصول على معلومات أو بيانات شخصية عن شخص آخر دون موافقته أو علمه» (العجاجي، 2021)، ومن خلال هذا التعريف، يتبيَّن أن جريمة التنصت لا تقتصر على وسيلة محددة، بل يمكن أن تقع عبر صور وأساليب تقنية متنوعة أهمها:

- **التجسس الإلكتروني:** استخدام برامج التجسس أو الهندسة الاجتماعية للحصول على معلومات حول شخص ما عبر الإنترنت (الشهري، 2012).
- **التجسس المادي:** مراقبة شخص ما أو مكان ما دون الموافقة (العجاجي، 2021).

ومن ثم يمكن تعريف مفهوم التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية بأنه «القيام بالتلصص أو معرفة البيانات الخاصة

بالشخص عن طريق الإنترنت، أو باستخدام الحاسب الآلي دون مبرر لذلك، ودون موافقه شخصية ممن تم معرفة بياناته»، ومن الجدير بالذكر إن للإنسان الحق في الحفاظ على تفاصيل حياته الخاصة، وكذلك له الحق في حماية جميع المعلومات التي تتعلق بهُويته، وخصوصياته، ومسكنه، ومراسلاته، واتصالاته، وأسراره، وأنه لا يمكن إحداث أي خرق أو أي تدخل في هذا الحق، إلا بصورة مشروعة، أي في الحالات التي يقرها ويسمح بها النظام (فقيه، 2018).

أما أنواع هذه الخصوصية فيمكن تقسيمها الى أربعة:

أ. **خصوصية جسدية:** وهي التي تتعلق بالحماية الجسدية للأفراد تجاه أية إجراءات ماسة بالنواحي المادية لأجسامهم كفحص المخدرات أو الجينات مثلًا.

ب. **خصوصية الاتصالات والمراسلات:** وهي التي تتعلق بحق الأفراد في الحفاظ على سرية اتصالاتهم، ومراسلاتهم، وبريدهم الإلكتروني وغيرها من الاتصالات.

ج. **خصوصية مكانية:** وهي التي تتعلق بحرمة المسكن، والقواعد الإجرائية المنظمة للتفتيش الحاصل في الأماكن الخاصة والعامة.

د. **خصوصية معلوماتية:** وهي التي تتمثل بالقواعد المنظمة لجميع إدارات البيانات الخاصة الموجودة على الأجهزة الإلكترونية، أو على شبكة الإنترنت (فقيه، 2018).

ولما كان مبدأ الشرعية يقتضي الوقوف عند المفاهيم التي نصَّ عليها المنظم السعودي في نظام مكافحة الجرائم المعلوماتية، فقد وردت في المادة الأولى التعريفات الآتية:

1. **النظام المعلوماتي:** مجموعة برامج وأدوات معدَّة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية (هيئة الخبراء بمجلس الوزراء، 2007).
2. **الشبكة المعلوماتية:** ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل: الشبكات الخاصة والعامة والشبكة العالمية (الإنترنت) (هيئة الخبراء بمجلس الوزراء،2007).
3. **البيانات:** المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها (هيئة الخبراء بمجلس الوزراء،2007).
4. **برامج الحاسب الآلي:** مجموعة من الأوامر، والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة (هيئة الخبراء بمجلس الوزراء،2007).
5. **الحاسب الآلي:** أي جهاز إلكتروني ثابت أو منقول سلكي أو لا سلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له (هيئة الخبراء بمجلس الوزراء، 2007).
6. **الموقع الإلكتروني:** مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد (هيئة الخبراء بمجلس الوزراء، 2007).

2. 1. 2. الفرع الثاني: التمييز بين جريمة التنصت وغيره من المفاهيم المشابهة

تقتضي دراسة جريمة التنصت التمييز بينها وبين بعض المفاهيم المتقاربة التي قد يلتبس مدلولها في الفقه أو في التطبيق العملي، مثل: التجسس، أو التسجيل غير المصرح به، أو المراقبة الإلكترونية، أو التقاط الصور. ويُعدُّ هذا التمييز ضرورةً لفهم الخصائص التي تنفرد بها جريمة التنصت، ولتحديد نطاقها القانوني على نحو دقيق. وفيما يلي عرض لأبرز تلك الفوارق:

1. التجسس

يُعدُّ التجسس مفهومًا قريبًا من التنصت، ويُعرّف بأنه «جمع معلومات سرية عن الأشخاص أو المؤسسات لأغراض غير مشروعة» بينما يُعدّ التجسس أوسع نطاقًا من التنصت؛ حيث يمكن أن يشمل تجميع المعلومات بطرق لا تقتصر على الاستماع أو الاطلاع المباشر على المراسلات (نباش وبولقرون، 2022)، ومن ثم فإن الفرق الأساسي بين التنصت والتجسس يكمن في النطاق؛ إذ يركز التنصت بشكل أكبر على الاستماع أو التسجيل المباشر للمحادثات دون إذن، بينما يشمل التجسس وسائل متنوعة لجمع المعلومات السرية، كالتقاط الصور أو جمع المستندات.

2. التسجيل غير المصرح به

يتضمن التسجيل غير المصرح به تسجيل المحادثات أو المكالمات الهاتفية، أو أي نوع من أنواع الاتصالات دون علم الطرف الآخر، ويُعدُّ هذا السلوك مشابهًا للتنصت، إلا أنه يركز على جمع المعلومات بشكل غير مباشر دون الحاجة إلى الاستماع الفوري (فايق، 2025)، ومن هذه الزاوية يمكن القول بأن الفرق بين التنصت والتسجيل غير المصرح به يكمن في الآلية المستخدمة؛ حيث يتم التنصت عن طريق الاستماع المباشر، بينما يتضمن التسجيل غير المصرح به توثيق المحادثة بشكل دائم دون إذن.

3. المراقبة الإلكترونية، أو التقاط الصور

تشمل المراقبة الإلكترونية استخدام الأجهزة الإلكترونية لمتابعة تحركات أو سلوكيات الأفراد، وتختلف المراقبة عن التنصت في أن الأخيرة تتعلق بالمحادثات، أو الاتصالات مباشرة، بينما قد تتضمن المراقبة متابعة موقع الشخص أو نشاطه على الإنترنت (حسين، 2022)، وهذا يعني أن المراقبة تتباين عن التنصت في أنها لا تركز على المحادثات الخاصة بالضرورة، بل تتسع لتشمل أنشطة الأفراد الأخرى، وتستخدم غالبًا في سياقات أمنية محددة، هذا من ناحية، ومن ناحية أخرى فإن التنصت جريمة سمعية في حين أن المراقبة أو التقاط الصور جريمة مرئية أو مشاهدة.

2. 2. المطلب الثاني: أركان جريمة التنصت

تقوم المسؤولية الجنائية في أصلها على قدرة الشخص على الإدراك والتمييز، باعتبارهما من المقومات الجوهرية التي تُحدّد أهلية الفرد لتحمّل تبعات تصرفاته غير المشروعة. أما في نطاق جريمة التنصت، فإن هذه المسؤولية لا تقوم إلا بتوافر أركان الجريمة كما حددها النظام، شأنها شأن سائر الجرائم الأخرى. وتمثل هذه الأركان الأساس القانوني الذي يُبنى عليه التجريم والعقاب، بحيث يؤدي تخلف أيٍّ منها إلى انتفاء المسؤولية الجنائية.

وتتمثل هذه الأركان في الركن الشرعي الذي يتجسد في النص النظامي المجرّم للفعل، والركن المادي الذي يشمل السلوك الإيجابي أو الامتناع المكوّن للجريمة، والركن المعنوي الذي يقوم على القصد الجنائي لدى الجاني. وبناءً على ذلك، سيتم تناول الركنين الشرعي والمادي معًا في الفرع الأول، بينما يُخصَّص الفرع الثاني لمعالجة الركن المعنوي.

2. 2. 1. الفرع الأول: الركنان الشرعي والمادي لجريمة التنصت باعتبارها جريمة معلوماتية

الركن الشرعي

استنادًا إلى مبدأ شرعية الجرائم والعقوبات القاضي بأنه «لا جريمة ولا عقوبة إلا بنص»، يتبين أن النظام الأساسي للحكم في المملكة العربية السعودية قد كرَّس هذا المبدأ بصورة صريحة؛ حيث نصَّ في المادة (38) على أن: «العقوبة شخصية، ولا جريمة ولا عقوبة إلا بناءً على نص شرعي أو نص نظامي، ولا عقاب إلا على الأعمال اللاحقة للعمل بالنص النظامي» (هيئة الخبراء بمجلس الوزراء، 1992).

وانطلاقًا من هذا الأساس، فإن الركن الشرعي في جريمة التنصت عبر الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي يتمثل في وجود نص نظامي يُسبغ على الفعل الصفة غير المشروعة، ويحدد العقوبة المقررة له عند ارتكابه. ويُعدُّ ذلك تطبيقًا مباشرًا لمبدأ الشرعية.

إذ لا تقوم المسؤولية الجنائية في هذا النوع من الجرائم إلا إذا نص النظام صراحةً على تجريم الفعل، سواء من خلال التنصت، أو الالتقاط، أو الاعتراض دون مسوغ مشروع، بحيث يُستمد عدم المشروعية من نص شرعي أو نظامي قائم.

الركن المادي

يقوم الركن المادي لجريمة التنصت عبر الشبكة المعلوماتية، أو من خلال أحد أجهزة الحاسب الآلي - وفقًا لأحكام نظام مكافحة الجرائم المعلوماتية - على ثلاثة عناصر مترابطة تمثل الأساس الذي يقوم عليه التجريم، وهي:

أولها، الفعل الإجرامي المتمثل في التنصت، أو الاعتراض، أو الالتقاط غير المشروع لما يُرسل من بيانات عبر الوسائط الإلكترونية.

وثانيها: النتيجة الجرمية، وهي الأثر الذي يترتب على هذا السلوك، والمتمثل في انتهاك سرية المعلومات وخصوصية الاتصالات.

أما **ثالثها:** فهو العلاقة السببية التي تقتضي وجود صلة مباشرة بين الفعل المرتكب والنتيجة الضارة المترتبة عليه، ويُشترط لقيام هذا الركن أن تتوافر العناصر الثلاثة بشكل مترابط، بحيث لا يمكن مساءلة الفاعل جزائيًّا إلا إذا ثبت أن الفعل الإجرامي كان هو السبب المباشر في تحقق النتيجة المحظورة نظامًا.

1. السلوك أو الفعل الإجرامي

يقوم الركن المادي لجريمة التنصت على نشاط إجرامي يصدر عن الجاني، إيجابيًّا أو امتناعًا، يمس سرية الاتصالات والمراسلات عبر الوسائط الرقمية. وقد نصت المادة الثالثة من نظام مكافحة الجرائم المعلوماتية على أن من صور هذا النشاط: «التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه» (هيئة الخبراء بمجلس الوزراء، 2007).

وبالرجوع إلى النص يتضح أن الفعل يأخذ ثلاث صور رئيسة:

أ. **الاستماع المباشر:** ويقصد به متابعة محتوى الاتصالات أو المحادثات أثناء انتقالها عبر الشبكة، وهو ما يُعدُّ أخطر صور التنصت لكونه يتيح للجاني الاطلاع الفوري على أسرار المجني عليه.

ب. **الاطلاع أو الالتقاط:** ويتمثل في الحصول على ما يُرسل أو يُخزن من بيانات أو رسائل عبر الشبكة المعلوماتية بعد

انتقالها، سواء بالولوج غير المشروع إلى النظام أو عبر برامج مخصَّصة لاعتراض البيانات.

ج. **الاعتراض:** ويعني التدخل في مسار البيانات، أو الرسائل أثناء انتقالها بين طرفين، بما يتيح للجاني إيقافها أو تعديلها أو الاستفادة منها، وهو ما يشكل اعتداءً مزدوجًا على الحق في سرية المراسلات وسلامة تبادلها.

ومن ثمّ، يتضح أن المنظم السعودي أحاط بالفعل الإجرامي في جريمة التنصت بإطار واسع يشمل مختلف صور المساس بالاتصالات، سواء عبر السمع المباشر أو الحصول غير المشروع أو اعتراض البيانات في مسارها، بما يكفل سدَّ جميع الذرائع التقنية التي قد تُستغل لارتكاب هذه الجريمة.

2. النتيجة الإجرامية

تتحقق النتيجة الإجرامية في جريمة التنصت عندما يترتب على السلوك المجرَّم نظامًا أثر ضار مباشر يمس حقوق المجني عليه، أو مصالحه المشروعة. وقد نصَّت المادة الثالثة من نظام مكافحة الجرائم المعلوماتية صراحة على أن التنصت أو التقاط أو اعتراض ما يُرسل عبر الشبكة المعلوماتية أو أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - يُعد فعلًا محظورًا يرتب مسؤولية جنائية على مرتكبه (هيئة الخبراء بمجلس الوزراء، 2007).

وتظهر النتيجة بوضوح عندما يؤدي التنصت إلى انتهاك سرية الاتصالات أو الاطلاع غير المشروع على بيانات ذات طابع شخصي أو مهني، وهو ما يمثل اعتداءً صريحًا على الحق في الخصوصية، وإخلالًا بالحماية النظامية التي أوجبها المنظم. ومن ثمَّ فإن اكتمال هذه النتيجة هو الذي يربط بين الفعل المادي والجزاء الجنائي، ويُظهر خطورة السلوك الإجرامي في البيئة الرقمية.

3. الرابطة السببية بين الفعل والنتيجة الجرمية

تُعدُّ علاقة السببية عنصرًا جوهريًّا في تكوين الركن المادي للجريمة؛ إذ لا يكفي لقيام المسؤولية الجنائية مجرد ارتكاب الفعل المجرَّم، بل يلزم أن يترتب عليه أثر ضار مباشر، يمس بالمصلحة التي يحميها النظام. وفي نطاق جريمة التنصت، نصت المادة الثالثة من نظام مكافحة الجرائم المعلوماتية على تجريم التنصت أو التقاط أو اعتراض ما يُرسل عبر الشبكة المعلوماتية أو أجهزة الحاسب الآلي - دون مسوغ نظامي - باعتبارها أفعالًا تؤدي إلى انتهاك سرية الاتصالات وخصوصية الأفراد (هيئة الخبراء بمجلس الوزراء، 2007).

وتثور أهمية الرابطة السببية هنا عند وجود عوامل متداخلة، كأن يكون الضرر قد تحقق بسبب خلل تقني مستقل عن فعل الجاني، أو نتيجة تسريب البيانات من طرف ثالث، أو بسبب إهمال المجني عليه في حماية بياناته. ففي هذه الحالات، يتعين التحقق مما إذا كان فعل الجاني هو السبب المباشر والحاسم في تحقق النتيجة أم أن تدخل عامل آخر قد قطع رابطة السببية.

وبناءً على ذلك، فإن توافر الصلة المباشرة بين فعل التنصت والنتيجة المترتبة عليه شرط لازم لقيام الركن المادي للجريمة، أما إذا ثبت أن النتيجة قد تحققت لأسباب أخرى منفصلة عن فعل الجاني، فإن المسؤولية الجنائية تنتفي لغياب أحد الأركان الأساسية للجريمة.

2. 2. 2. الفرع الثاني: الركن المعنوي لجريمة التنصت باعتبارها جريمة معلوماتية

يُعَدُّ الركن المعنوي من الأركان الجوهرية في جريمة التنصت عبر الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي؛ إذ لا يكفي مجرد تحقق الفعل المادي ما لم يقترن بإرادة آثمة تعكس قصد الجاني ووعيه بعدم مشروعية سلوكه. ويتكون هذا الركن من عنصر أساسي هو النية الجرمية لدى الفاعل، كما لا يكفي لقيام الجريمة المعلوماتية مجرد تحقق الفعل المادي من جانب الفاعل، بل يتعين - كشرط لازم للمساءلة الجنائية - توافر القصد الجنائي باعتباره أحد الأركان الجوهرية للجريمة العمدية. ويتحقق هذا القصد متى كان الجاني عالماً بطبيعة فعله ومدركًا لكونه سلوكًا محظورًا نظامًا، فضلًا عن تمتعه بالأهلية القانونية الكاملة التي تخوله تحمل التبعات المترتبة على فعله.

وعلى ذلك، فإذا دخل شخص إلى شبكة معلوماتية بغرض مشروع، ثم ارتكب - نتيجة جهله بالضوابط النظامية - فعلًا ترتب عليه إضرار بالغير دون أن تتوافر لديه نية ارتكاب السلوك المحظور، فإن مسؤوليته تكون في نطاق الخطأ غير العمدي، بحيث يلتزم بالتعويض المدني عن الضرر دون أن تُطبّق عليه العقوبات المقررة للجرائم المعلوماتية العمدية. ومن ثم، فإن انتفاء القصد الجنائي يؤدي إلى سقوط الوصف الإجرامي عن الفعل، وانتفاء المسؤولية الجنائية في نطاق نظام مكافحة الجرائم المعلوماتية (الدعدي، 2024).

ومن ثم يمكن القول بأن القصد الجنائي هو اتجاه نية الفاعل إلى ارتكاب الجريمة، وهو أحد الأركان الأساسية التي يجب توافرها لاعتبار الفعل جريمة، هذا ومن الجدير بالإشارة أن القصد الجنائي ينقسم الي قسمين على النحو التالي:

أ. **القصد العام**، يتحقق متى ثبت أن الجاني كان عالماً بطبيعة السلوك الذي يباشره، وبأنه يُشكّل فعلًا مجرَّمًا نظامًا، وأن إرادته اتجهت إلى ارتكاب هذا السلوك بكامل حريته واختياره، ولا يُفترض هذا العلم ابتداءً، بل يُستخلص من ظروف الواقعة وملابساتها، كما يُشترط لصحة الإرادة أن تكون خالية من أي مؤثر يُعدم الحرية أو يُضعف الإدراك، مثل: الإكراه أو التدليس أو الغش (المنشاوي، 2025).

ب. **القصد الخاص**: لا يقتصر على نية تحقيق منفعة مالية، وإن كان ذلك أحد الدوافع المحتملة، بل يكفي أن يتجه قصد الجاني إلى الحصول على المعلومات، أو الاطلاع عليها أو استغلالها لأي غاية غير مشروعة؛ سواء كانت مالية أو شخصية أو انتقامية أو تجسسية، ومن ثم، فإن معيار القصد الخاص يتحقق متى كان الهدف من فعل التنصت هو تحقيق فائدة غير مشروعة، أو إلحاق ضرر بالغير، بصرف النظر عن طبيعة تلك الفائدة أو شكلها (إدريس، 2020).

ويرى الباحث أن جريمة التنصت عبر الشبكة المعلوماتية لا تستلزم قصدًا خاصًا كنية التكسّب أو الإضرار بذاته، وإنما يكفي لتحقق المسؤولية الجنائية توافر القصد العام، المتمثل في علم الجاني بطبيعة الفعل الذي يقدم عليه، وأنه غير مشروع وفقًا للنظام، مع اتجاه إرادته الحرة إلى ارتكابه دون خطأ أو إكراه يفقده حرية الاختيار. فلا يُشترط أن يسعى الجاني لتحقيق منفعة معينة، وإنما يكفي أن يكون سلوكه قد صدر عن إدراك ووعي وإرادة نحو القيام بفعل التنصت المحظور نظامًا.

3. المبحث الثاني: الصور التي ترتبط بجريمة التنصت والعقوبة المقررة لها

يتناول هذا المبحث دراسة العقوبات المقررة لجريمة التنصت عبر الشبكة المعلوماتية، وما يرتبط بها من أوصاف قانونية؛ إذ قد يكون مرتكب الجريمة فاعلًا أصيلًا، وقد تتعدد الأفعال لنكون أمام صورة من صور المساهمة الجنائية. كما نصَّ المنظم السعودي على حالات تشديد للعقوبة في إطار مكافحة الجرائم المعلوماتية، وهي تنطبق على جريمة التنصت محل الدراسة، فضلًا عن بعض حالات الإعفاء من العقوبة التي تستوجب التحليل. وفيما يلي بيان ذلك.

3. 1. المطلب الأول: الأوصاف التي ترتبط بجريمة التنصت

قد تلحق بجريمة التنصت عبر الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أوصاف قانونية نصَّ عليها نظام مكافحة الجرائم المعلوماتية تجعلها أكثر خطورة، وتستوجب أحكامًا أشد. ويظهر ذلك من خلال حالتين أساسيتين:

- **المساهمة الجنائية**: وقد نصَّت عليها المادة التاسعة التي رتبت مسؤولية كل من حرّض أو ساعد أو اتفق على ارتكاب الجريمة، بحيث يُساءل كل شريك بحسب دوره في التنفيذ.
- **حالات التشديد**: وقد نصَّت عليها المادة الثامنة التي اعتبرت ارتكاب الجريمة في ظروف معينة - مثل صدورها عن موظف عام أو اقترانها بالمساس بالأمن الوطني - سببًا لتشديد العقوبة.

وعلى هذا الأساس، نقسم هذا المطلب إلى فرعين: يتناول الأول أحكام المساهمة الجنائية في جريمة التنصت، بينما يتناول الثاني حالات تشديد العقوبة المنصوص عليها في النظام.

3. 1. 1. الفرع الأول: المساهمة الجنائية في جريمة التنصت

الأصل في جريمة التنصت أن تكون جريمة فردية، لكن من الوارد أن تكون قد تمت وفق صورة من صور المساهمة الجنائية، كما تمت الإشارة في المادة التاسعة الى صورة المساهمة في الجريمة المعلوماتية، سواء بالتحريض أو الاتفاق أو المساعدة (هيئة الخبراء بمجلس الوزراء، 2007).

ويقصد بالمساهمة الجنائية في الفقه الجنائي وقوع الجريمة من عدة أشخاص شرط أن تجمعهم رابطة معنوية هي التعاون في السلوك الإجرامي لإحداث النتيجة في الجريمة العمدية، وإرادة التعاون في السلوك في الجريمة غير العمدية (محمود، 1970).

وقد نصَّ المنظم السعودي في نظام مكافحة الجرائم المعلوماتية على قاعدة عامة تتعلق بالشروع في الجريمة، حيث جاء في المادة العاشرة أنه: «يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة» (هيئة الخبراء بمجلس الوزراء، 2007).

وقد تتخذ المساهمة الجنائية عدة صور، كما يأتي:

1. **التحريض**: هو خلق فكرة الجريمة لدى الغير، ويُعرف أيضًا بأنه دفع الغير إلى ارتكاب الجريمة (أحمد، 2022).
2. **الاتفاق**: هو تلاقي إرادتين أو أكثر، ويتحقق الاشتراك بمجرد اتفاق شخص مع آخر، أو مع آخرين على ارتكاب الجريمة، ما دامت قد وقعت نتيجة الاتفاق، فلا يمنع توافره استقلال أحد المتفقين بوضع تفاصيلها ورسم الخطط اللازمة لتحقيقها، ثم قيامه بتنفيذها، ولهذا يبدو الفرق بين التحريض والاتفاق واضحًا، ففي التحريض تطغى إرادة المحرض على الفاعل،

فتدفعه إلى ارتكاب الجريمة، بينما في الاتفاق تكون إرادات المتفقين في مستوى واحد.

3. **المساعدة**: هي تقديم العون إلى الفاعل فيرتكب الجريمة بناءً عليه، وتتحقق المساعدة بتدخل الشريك مع الفاعل تدخلًا مقصودًا يتجاوب صداه مع فعله، ويتحقق فيه معنى تسهيل ارتكاب الجريمة، ويتمثل العون في تقديم الوسائل المادية المعينة على ارتكاب الجريمة، كتقديم السلاح للقاتل والمداد للمزور، وقد يتمثل العون في إزالة عقبة تعترض تنفيذ الجريمة (الصيفي، 1995)، وفي هذه الجريمة موضوع الدراسة قد يكون بمساعدة المتهم للولوج للحساب الإلكتروني للمجني عليه، أو تمكينه من جهاز حاسب آلي يمكنه من ذلك.

3. 1. 2. الفرع الثاني: الشروع في جريمة التنصت

يُعدُّ الشروع وصفًا قانونيًّا قائمًا بذاته في نطاق الجرائم المعلوماتية؛ إذ حرص المنظم السعودي على إدراجه ضمن أحكام نظام مكافحة الجرائم المعلوماتية. فقد نصت المادة العاشرة على أن: «يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة» (هيئة الخبراء بمجلس الوزراء، 2007).

ومن خلال هذا النص يتضح أن الشروع يتحقق متى بدأ الجاني في تنفيذ الفعل المجرَّم، كأن يُطلق برنامجًا لاعتراض الاتصالات، أو يبدأ في تثبيت وسيلة تقنية تمكّنه من التنصت، لكنه لم يتمكن من إتمام الجريمة لأسباب خارجة عن إرادته. وفي هذه الحالة لا يُنظر إلى اكتمال النتيجة، بل يكفي تحقق بداية النشاط الإجرامي الذي يُظهر نية الجاني في الاعتداء على سرية الاتصالات.

ويمثل النص النظامي في هذا السياق تطبيقًا لمبدأ وقائي في السياسة الجنائية؛ فمجرد الشروع يُعدُّ خطرًا على القيم والمصالح المحمية نظامًا؛ مما يستدعي التدخل بالعقاب ولو كان أخف من عقوبة الجريمة التامة. ومن ثمّ، فإن الشروع في جريمة التنصت يوسّع نطاق الحماية المقررة للأفراد، ويؤكد أن الاعتداء على الحياة الخاصة لا يشترط اكتماله لإثارة المسؤولية الجنائية (غرم الله، 2017).

وتجدر الإشارة إلى أن المنظم اكتفى بوضع قاعدة عامة للشروع في جميع الجرائم المعلوماتية، من غير أن يخص جريمة التنصت بصور تفصيلية للشروع فيها، الأمر الذي يترك مجالًا لاجتهاد القضاء في تحديد الأفعال التي تُعدُّ في حكم البداية الجدية للتنفيذ، مع ضرورة التمييز بين الأفعال التحضيرية التي لا عقاب عليها، وبين الأفعال التنفيذية التي تندرج في نطاق الشروع المعاقب عليه.

3. 2. المطلب الثاني: العقوبات المقررة لجريمة التنصت

حرص المنظم السعودي من خلال نظام مكافحة الجرائم المعلوماتية على وضع عقوبات رادعة لفعل التنصت عبر الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي؛ وذلك بالنظر إلى جسامته، وما يشكله من اعتداء مباشر على الحق في الخصوصية، وتهديد للأمن المعلوماتي. وهذه العقوبات تتنوع بحسب طبيعتها إلى عقوبات أصلية تُفرض مباشرة على الجاني باعتبارها الجزاء الأساسي للفعل المجرَّم، وعقوبات تكميلية تستهدف تحقيق حماية أشمل للمصلحة المعتدى عليها، وتكفل منع الجاني من الاستفادة من نتائج جريمته، فضلًا عن عقوبات تبعية تلحق بالمحكوم عليه بحكم النظام دون حاجة إلى النص عليها في الحكم. ومن ثم فإن دراسة العقوبات المقررة لجريمة التنصت تستوجب بيان صورها من خلال تقسيم هذا المطلب إلى فرعين: يتناول الأول منهما العقوبات الأصلية، بينما يتناول الفرع الثاني العقوبات التكميلية والتبعية.

3. 2. 1. الفرع الأول: العقوبات الأصلية وحالات تشديدها

تُعدُّ العقوبات الأصلية الجزاء المباشر الذي رتبه المنظم السعودي على جريمة التنصت عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي؛ إذ تمثل الأثر القانوني الأساسي للسلوك المجرَّم. غير أن خطورة هذه الجريمة قد تستدعي في بعض الأحوال فرض عقوبات أشد، وذلك متى اقترنت بظروف خاصة نصَّ عليها النظام. ومن ثم، فإن هذا الفرع يتناول العقوبات الأصلية المقررة لهذه الجريمة، إلى جانب حالات التشديد التي قد ترفع من حدتها وفقًا لخطورة الفعل والظروف المحيطة به.

العقوبات الأصلية

يقصد بالعقوبات الأصلية تلك العقوبات التي يضعها المنظم ابتداءً كجزاء مباشر على ارتكاب الجريمة، وهي تمثل الأثر القانوني الطبيعي للسلوك المجرّم. وفيما يتعلق بجريمة التنصت، نصت المادة الثالثة من نظام مكافحة الجرائم المعلوماتية على أن: «كل من يتعمّد التنصت أو الالتقاط أو الاعتراض لما يُرسل عبر الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - يُعاقب بالسجن مدة لا تتجاوز سنة، أو بغرامة مالية لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين» (هيئة الخبراء بمجلس الوزراء، 2007).

ويُستفاد من هذا النص أن المنظم أخذ بمبدأ التخيير بين العقوبتين أو الجمع بينهما، وهو ما يتيح للقضاء المرونة في تقدير

الجزاء بحسب خطورة الفعل وظروف ارتكابه. كما أن الحد الأقصى للعقوبة يعكس توازنًا بين حماية الحياة الخاصة من الاعتداء وضمان عدم المغالاة في التشديد على سلوك قد يُرتكب أحيانًا بوسائل تقنية يسهل استخدامها.

كما نصت المادة العاشرة على أن: «يعاقب كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة» (هيئة الخبراء بمجلس الوزراء، 2007). ويكشف هذا النص عن إدراك المنظم لخطورة الأفعال التي لم تصل إلى مرحلة الجريمة التامة، فجعلها محل مساءلة جنائية، وإن خفّف عقوبتها التزامًا بمبدأ التناسب بين الشروع والجريمة التامة.

أما الأفعال ذات الجسامة الخاصة، فقد وسَّع المنظم نطاق العقوبة في المادة الخامسة لتصل إلى السجن مدة لا تتجاوز أربع سنوات، أو الغرامة بما لا يزيد على ثلاثة ملايين ريال أو الجمع بينهما (نظام مكافحة الجرائم المعلوماتية، م5، 1428). ويكشف هذا الاتجاه عن تبني سياسة الردع العام لمواجهة الأفعال التي تشكل تهديدًا للأمن المعلوماتي أو مساسًا بالحقوق الجوهرية للأفراد، ولا سيما إذا ارتُكبت في ظروف مشددة؛ مثل: العصابات المنظمة أو استغلال الفئات الضعيفة (غرم الله، 2017).

وعليه، فإن العقوبات الأصلية لجريمة التنصت تعكس توازنًا بين ثلاثة اعتبارات: المرونة عبر التخيير في العقوبة، والوقاية من خلال تجريم الشروع، والردع بمواجهة الأفعال الجسيمة بتشديد العقوبات. وهذا التدرج التشريعي يُظهر عناية المنظم بحماية الحياة الخاصة والأمن المعلوماتي مع مراعاة مبدأ التناسب.

2. حالات تشديد العقوبة

إذا تمت جريمة التنصت عبر صورة من صور المساهمة الجنائية، فإنها تكون قد تعدت الفاعل المنفرد الى الفاعل المتعدد الذي يوجب ظرفًا مشددًا للعقوبة، وقد نصت المادة الثامنة على الأحوال التي تؤدي إلى تشديد العقوبة وعرضتها على سبيل الحصر، وهي إذا ارتبطت الجريمة بأي حالة من الحالات الآتية:

- إذا قام الجاني بارتكاب الجريمة من خلال عصابة منظمة.
- شغل وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلًا سلطانه أو نفوذه.
- استغلال القُصَّر، أو من في حكمهم من خلال التغرير بهم، يُعدُّ ظرفًا مشددًا للجريمة؛ لما ينطوي عليه من مساس بالحماية القانونية المقررة لتلك الفئة.
- إذا كان الجاني قد صدر بحقه حكم نهائي، محلي أو أجنبي، بالإدانة في جريمة تماثل الجريمة محل المحاكمة، فإن ذلك يُعدُّ ظرفًا مشددًا يستوجب تغليظ العقوبة (هيئة الخبراء بمجلس الوزراء، 2007).

يتضح أن مبرر التشديد في العقوبة يعود إلى الظروف الملاصقة للجريمة، والتي يُطلق عليها في الفقه الجنائي «الظروف المشدِّدة». ويمكن في ضوء النصوص والنظرية الجنائية تقسيم هذه الظروف إلى صورتين أساسيتين:

1. **العود إلى الإجرام:** ويقصد به عودة الجاني إلى ارتكاب جريمة جديدة بعد أن سبق الحكم عليه محليًّا أو أجنبيًّا في جرائم مماثلة. وفي هذه الحالة تُشدد العقوبة بالنظر إلى خطورة شخصية الجاني وتكرار سلوكه الإجرامي، وهو ما يُعرف في الفقه الجنائي بمفهوم «العود» (سليمان، 1998).
2. **تعدد الجناة:** ويتحقق عندما تُرتكب الجريمة بواسطة أكثر من شخص في إطار عصابة منظمة؛ حيث يرى المنظم أن خطورة الفعل تزداد في هذه الصورة، بما يستوجب تشديد العقوبة تعزيزًا للردع العام والخاص.
3. **النظر إلى صفة الجاني**، أو ما يعرف بالشرط المفترض؛ تُعد صفة الجاني من الظروف المشدِّدة التي ترفع العقوبة، وهو ما يُعرف في الفقه الجنائي بالشرط المفترض. ويتحقق ذلك في حالتين أساسيتين:
   - **صفة الموظف العام**: سواء أكان موظفًا فعليًّا يعمل في إحدى الوزارات أو الهيئات العامة في المملكة، أو موظفًا حكميًّا يباشر خدمة عامة بتكليف نظامي، فإذا استغل هذا الموظف صفته الوظيفية في ارتكاب جريمة التنصت، فإن العقوبة تُشدد عليه؛ نظرًا لما ينطوي عليه فعله من إخلال بواجبات الثقة والوظيفة العامة.
   - **الولاية على الغير**: إذا ارتكب الجاني الجريمة مستغلًا سلطته على من يخضع لولايته، كالقاصر أو من له ولاية قانونية عليه، فإن العقوبة تُشدد عليه أيضًا. ويُعزى ذلك إلى أن فعله يُعدُّ إخلالًا بالواجب القانوني الذي فرضه النظام والدين لحماية هذه الفئة.

واعتبر المنظم السعودي حالة العود إلى الجريمة ظرفًا مشددًا للعقوبة، غير أنه لم يضع تعريفًا دقيقًا لها، بل وسَّع نطاقها؛ فجعل صدور أي أحكام وطنية أو أجنبية بالإدانة ضد المتهم سببًا للتشديد (هيئة الخبراء بمجلس الوزراء، 2007).

ويُعرّف العود اصطلاحًا بأنه ارتكاب الجاني لجريمة جديدة بعد الحكم عليه في جريمة سابقة. وينقسم في الفقه الجنائي إلى نوعين:

- **العود الخاص**: إذا عاد الجاني لارتكاب جريمة من النوع ذاته بعد الحكم عليه فيها، كمن يُدان بجريمة سرقة ثم يعاود ارتكابها.
- **العود العام**: إذا ارتكب الجاني جريمة جديدة تختلف في نوعها عن الجريمة السابقة، كمن يُدان بالسرقة ثم يرتكب جريمة تعاطي المخدرات (سليمان، 1998).

ويُعدُّ العود سببًا شخصيًّا لتشديد العقوبة؛ لأن العقوبات السابقة لم تحقق الردع الكافي؛ مما يدل على خطورة أكبر لشخص الجاني مقارنة بمن يرتكب الجريمة لأول مرة. لذلك قيل: إن العلة في التشديد تعود إلى شخصية المجرم أكثر من الفعل المرتكب (خليل، 1988).

كما نص المنظم في المادة (11) على حالة إعفاء من العقوبة إذا بادر أحد المتورطين بالإبلاغ عن الجريمة، شريطة أن يسفر هذا الإبلاغ عن القبض على باقي الجناة، إن وُجدوا، أو عن ضبط الأدوات المستخدمة في ارتكابها (هيئة الخبراء بمجلس الوزراء، 2007).

3. 2. 2. الفرع الثاني: العقوبات التكميلية والتبعية

يقصد بالعقوبات التكميلية تلك العقوبات التي لا تُفرض على الجاني بصورة مستقلة، وإنما تلحق بالعقوبة الأصلية بشرط النص عليها عند الحكم بها، وتهدف غالبًا إلى حرمان الجاني من الفائدة التي جناها من الجريمة، أو إلى تعزيز الردع العام والخاص. ومن أبرز صورها المصادرة لما تم استخدامه أو الحصول عليه من أدوات ووسائل الجريمة، فضلًا عن إمكان الجمع بينها وبين العقوبة الأصلية من سجن أو غرامة، بما يحقق حماية أكثر فاعلية للمصالح المعتدى عليها في الجرائم المعلوماتية.

وقد نصَّ المنظم السعودي في المادة الثالثة عشرة من نظام مكافحة الجرائم المعلوماتية على جواز الحكم بالمصادرة كعقوبة تكميلية، وتشمل هذه العقوبة مصادرة الأجهزة أو البرامج أو الأدوات التي استُخدمت في ارتكاب الجريمة، وكذلك الأموال المتحصلة منها (هيئة الخبراء بمجلس الوزراء، 2007). كما نصت المادة ذاتها على أن للمحكمة المختصة أن تحكم بإغلاق الموقع الإلكتروني، أو الجهة التي تقدم الخدمة، سواء بصورة مؤقتة أو دائمة، متى ثبت أن الموقع أو الجهة كانت مصدرًا لارتكاب الجريمة، وتم ذلك بعلم مالكها.

ويُعدُّ تقرير هذه العقوبات التكميلية وسيلة رادعة تهدف إلى حرمان الجاني من الاستفادة من نتاج فعله غير المشروع، ومنع تكرار ارتكاب الجرائم عبر ذات الوسائل أو المنصات (القريني، 2021).

أما العقوبات التبعية، فهي تلك التي تترتب بحكم النظام على الحكم بالعقوبة الأصلية، دون حاجة إلى النص عليها في منطوق الحكم؛ إذ تُطبق كأثر قانوني للعقوبة. وقد نصَّ المنظم السعودي في المادة الثالثة عشرة من نظام مكافحة الجرائم المعلوماتية على جواز الحكم بـ التشهير بالمحكوم عليه عند الإدانة في بعض الجرائم المعلوماتية، باعتباره عقوبة تبعية تكمّل العقوبة الأصلية وتلحق بها (هيئة الخبراء بمجلس الوزراء، 2007).

وتتميز هذه العقوبات بطبيعتها التعزيرية، إذ تمس المركز القانوني أو الاجتماعي للمحكوم عليه، وتحقق غاية الردع العام من خلال كشف فعله غير المشروع للرأي العام (عادل، 2018).

الخاتمة

وفي ختام هذه الدراسة التي تناولت المسؤولية الجنائية الناشئة عن التنصت عبر الشبكات المعلوماتية، أو من خلال أجهزة الحاسب الآلي، يتضح أن التطور التقني والتحول الرقمي الواسع في استخدام الإنترنت ووسائل التواصل الاجتماعي قد أفرزا أنماطًا جديدة من السلوكيات غير المشروعة، تُعرف بالجرائم المعلوماتية. ويقصد بها كل فعل يُرتكب باستخدام الحاسب الآلي أو الشبكة المعلوماتية بما يخالف أحكام نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم (م/17) بتاريخ 13 إبريل 2007م، وتوصلت الدراسة إلى النتائج والتوصيات التالية:

النتائج

1. لم يورد المنظم السعودي تعريفًا صريحًا لمفهوم التنصت ضمن المادة الأولى من نظام مكافحة الجرائم المعلوماتية، وهو اتجاه يتماشى مع نهج معظم التشريعات المقارنة التي تتفادى وضع تعريف جامد لهذا المفهوم؛ نظرًا لتعدد صوره ووسائله التقنية (كالاستماع أو الالتقاط أو التسجيل أو الدخول والبقاء في النظام دون تصريح). وبناءً عليه، يمكن فهم التنصت في الإطار النظامي على أنه كل اطلاع غير مشروع على محتوى اتصالات أو بيانات رقمية أثناء انتقالها، أو وجودها في نظام معلوماتي، بأي وسيلة تقنية وبغير رضا صاحبها.
2. جريمة التنصت لا تتحقق إلا بتوافر ثلاثة أركان رئيسة هي: الركن الشرعي، والركن المادي، والركن المعنوي. ولا تقوم المسؤولية الجنائية إلا إذا تحقق الفعل الإجرامي المقترن بالقصد الجنائي. ويتمثل الركن المادي في ارتكاب سلوك غير مشروع يتم عبر الشبكة المعلوماتية، أو باستخدام أحد أجهزة

الحاسب الآلي، ويؤدي إلى نتيجة جرمية محددة تضر بالمجني عليه، مع وجود علاقة سببية مباشرة بين الفعل والنتيجة.

3. ليس الأصل في جريمة التنصت أن تُرتكب بصفة فردية، إلا أنه قد تقع في إطار المساهمة الجنائية بصورها المختلفة كالتحريض أو الاتفاق أو المساعدة.
4. يُستحسن أن ينص المنظم صراحة على أن العود بنطاقه الواسع يُعدُّ ظرفًا مشددًا للعقوبة، حتى ولو كان الحكم السابق صادرًا من محكمة أجنبية، ودون اشتراط مدة زمنية فاصلة بين الحكم الأول والجريمة الجديدة.
5. نص النظام على أن الإعفاء من العقوبة قد يتحقق إذا بادر أحد المشاركين في الجريمة إلى إبلاغ الجهات المختصة عنها، بشرط أن يسهم البلاغ في الوصول إلى بقية المتورطين، أو في ضبط الأدلة والأدوات المستعملة. ويُعدُّ هذا الإعفاء وسيلة لتعزيز التعاون مع السلطات المختصة، وتسهيل إجراءات التحقيق والملاحقة الجنائية.
6. تعددت العقوبات المقررة لجريمة التنصت في نظام مكافحة الجرائم المعلوماتية؛ فالعقوبة الأصلية هي السجن مدة لا تتجاوز سنة أو الغرامة بما لا يزيد على خمسمائة ألف ريال أو الجمع بينهما. أما عقوبة الشروع فلا تتجاوز نصف الحد الأعلى للعقوبة الأصلية. كما نصَّ النظام على تشديد العقوبة في بعض الحالات لتصل إلى السجن مدة لا تتجاوز أربع سنوات، أو الغرامة بما لا يزيد على ثلاثة ملايين ريال أو الجمع بينهما، وأخيرًا، أورد النظام عقوبات تبعية تشمل المصادرة وإغلاق الموقع الإلكتروني، أو مكان تقديم الخدمة متى ثبت أن الجريمة ارتكبت بعلم مالكه.

التوصيات

1. مراجعة العقوبات المقررة لجريمة التنصت في نظام مكافحة الجرائم المعلوماتية، مع إعادة ضبطها وفق معيار خطورة الفعل المرتكب، بحيث تُفرّق النصوص بين حالات التنصت البسيط الذي يقع بدافع الفضول دون قصد الإضرار، وبين الحالات الجسيمة التي ترتبط بالابتزاز أو انتهاك الحياة الخاصة، أو تهديد الأمن الوطني، وبما يسمح برفع الحد الأعلى للعقوبة في الصور المشددة إلى خمس سنوات سجن ومليوني ريال غرامة، مع ترك سلطة التقدير للمحكمة المختصة.
2. تعزيز الردع العام والخاص من خلال تشديد العقوبات المقررة للجرائم المعلوماتية، وخاصة جريمة التنصت؛ لما تنطوي عليه من مساس مباشر بالخصوصية الرقمية وانتهاك للحياة الخاصة، وبما يعزز الثقة في البيئة المعلوماتية بوصفها فضاءً آمنًا خاضعًا للرقابة النظامية.
3. توسيع نطاق التوعية المجتمعية بجرائم المعلوماتية، ولا سيما جريمة التنصت، وذلك من خلال إدماج برامج تثقيفية في المؤسسات التعليمية، ودعم الحملات التوعوية عبر وسائل الإعلام ودور العبادة؛ بهدف نشر الوعي بالمخاطر المترتبة على هذه الجرائم والحد من ارتكابها عن جهل أو بدافع الفضول.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس له أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن المؤلف بأن البحث المنشور لم يتلقَ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

أحمد، عبد الله. (2022). الاشتراك بالتحريض في جريمة غسل الأموال في النظام السعودي. مجلة جامعة الإمام محمد بن سعود الإسلامية للعلوم الإدارية، 1(23)، 77 - 105.

إدريس، محمد. (2020). المواجهة الجنائية لاستخدام تقنية المعلومات في ارتكاب جرائم المخدرات. المجلة الجنائية القومية، 63(2)، 73 - 117.

العجاجي، سليمان. (2021). إجراءات الضبط والتحقيق في جريمة التنصت الإلكتروني: دراسة تحليلية. المجلة العربية للدراسات الشرعية والقانونية، (4)، 5 - 85.

الشهري، حسن. (2012). الأنظمة الإلكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس. المجلة العربية للدراسات الأمنية، 28(56)، 5 - 32.

القريني، مها. (2021). واقع الجرائم المعلوماتية في المملكة العربية السعودية. الدار العالمية لتقنية المعلومات.

حسنين، سعد. (2023). أحكام المسؤولية الجنائية عن الجرائم المعلوماتية: دراسة مقارنة. مجلة الدراسات القانونية والاقتصادية، 9(3)، 1242 - 1395.

حسين، بشيخ. (2022). مراقبة الإنترنت وأثرها على الحريات العامة. المكتب العربي للمعارف.

خليل، عدلي. (1988). العود ورد الاعتبار. دار المطبوعات الجامعية للتوزيع.

الصيفي، عبد الفتاح. (1995). الأحكام العامة للنظام الجزائي (ط. 1). مطبوعات جامعة الملك سعود.

عادل، إيمان. (2018). العقوبة في نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية: دراسة تأصيلية مقارنة. مجلة العدل، (82)، 83 - 170.

فقيه، هانيا. (2018). حماية الحق في الخصوصية المعلوماتية: دراسة تحليلية لواقع الحماية وتحديات العصر. مركز الدراسات والأبحاث في المعلوماتية القانونية.

غرم الله، عبد العزيز. (2017). جرائم الإنترنت وعقوباتها وفق نظام مكافحة جرائم الإنترنت. دار الكتاب الجامعي.

هيئة الخبراء بمجلس الوزراء. (2007). نظام مكافحة الجرائم المعلوماتية.

هيئة الخبراء بمجلس الوزراء. (1992). النظام الأساسي للحكم.

نباش، مريم، وبولقرون، سعاد. (2022). التجسس وانتهاك الخصوصية في العصر الرقمي: دراسة وصفية تحليلية لبرنامج بيغاسوس. مجلة رقمنة للدراسات الإعلامية والاتصالية، 2(3)، 63 - 78.

محمود، مصطفى. (1970). أصول قانون العقوبات في الدول العربية. دار النهضة العربية.

المنشاوي، محمد. (2025). الجرائم المعلوماتية في النظام السعودي. دار الكتاب الجامعي.

المراجع الإلكترونية

الدعدي، حسن. (2024). أركان الجريمة المعلوماتية في السعودية. مكتب الدعدي للمحاماة. https://hd-lawfirm.com.sa/blog/%D8%

فايق، مينا. (2025). جريمة تسجيل المكالمات بدون علم الطرف الآخر. مدونة مينا فايق https://www.menafayq.com/2025/07/blog-post_774.

محامي شركة نخبة. (2023). عقوبة التجسس على خصوصيات الناس في القانون السعودي. شركة نخبة للمحاماة https://elitelawyerssa.com/2023/11/04/%D8%B9