الجمهوريه الجزائريه الديمقراطيه الشعبيه
Peoples democratic republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الإبراهيمي–برج بوعريريج –
University of Mohamed el Bachir el Ibrahimi-BBA
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق

تخصص : قانون إعلام الآلي والأنترنت

الموسومة بـ:

النظام القانوني للتنصت الالكتروني في التشريع الجزائري

إعداد الطالبين:

- جمـال بن براهم
- سعيـــد فـــار

نوقشت وأجيزت يوم: 03 جوان 2025

أمام لجنة المناقشة:

درارجة عبد الجليل	أستاذ محاضر قسم أ	رئيسا
ماني عبد الحق	أستاذ محاضر قسم أ	مشرفا ومقررا
دكدوك هدى	أستاذ محاضر قسم أ	ممتحنا

السنة الجامعية: 2025/2024

* ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020 .....
الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الأول)

أنا الممضي أسفله،
السيد(ة): بن براهم جمال ... الصفة: طالب، أستاذ باحث طالب
الحامل(ة) لبطاقة التعريف الوطنية رقم 117200992 والصادرة بتاريخ 2020.01.18
المسجل(ة) بكلية / معهد المغتون قسم
والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).
عنوانها: النظام القانوني للشغلت الالكتروني في التشريع الجزائري

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: .....

توقيع المعني (ة)

نظير وصدق على التوقيع
السيد: بن براهم جمال
بت و/ وس رقم 117200992
الصادرة في 2020.01.18 ببلدية مارنة
البليدة في: 2021
رئيس المجلس الشعبي البلدي
وبتفويض منه
طواهرية النواري

ملحق بالقرار رقم ....1082.... المؤرخ في ..... 27 ديسمبر 2020

الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

مؤسسة التعليم العالي والبحث العلمي:

نموذج التصريح الشرفي
الخاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

(الطالب الثاني)

أنا الممضي أسفله،

السيد(ة): ..... الصفة: طالب، أستاذ، باحث .....

الحامل(ة) لبطاقة التعريف الوطنية رقم: ..... الصادرة بتاريخ .....

المسجل(ة) بكلية / معهد ..... قسم .....

والمكلف(ة) بإنجاز أعمال بحث (مذكرة التخرج، مذكرة ماستر، مذكرة ماجستير، أطروحة دكتوراه).

عنوانها: .....

.....

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه .

التاريخ: .....

توقيع المعني (ة)

نظر وصدق على التوقيع

الطالب: ..... سمير

رقم: 002229263

الصادر في: 2022.01.04

حرر في: 26 ماي 2025

ع/رئيس المجلس الشعبي البلدي

وبتفويض منه

طواهرية النواري

شكـــر وعرفـــان

نحمد الله الذي جعل العلم يهدي به البشرية، وبالقرآن سراجا وهاجا تهدي بما فيه وتعلم منه ليكون مصباحا ينير ظلمة التائهين.

يطيب لنا ويبهج صدورنا أن نتقدم بالشكر الجزيل والامتنان إلى أعضاء اللجنة المكلفة بالمناقشة، وكذلك الشكر والتقدير إلى كل أساتذة كلية الحقوق والعلوم السياسية.

دون أن ننسى أن نتقدم بالشكر والعرفان والامتنان لما قدمه الأستاذ **ماني عبد الحق**، وكلمة الشكر لا تفيها حقه ونشكره على مجهوداته وتوجيهاته وعلى كل ما قدمه من إرشادات التي كانت تخدم مذكرة تخرجنا وتثريه في أبهى صورة.

إهـــــداء

الحمد الله رب العالمين والصلاة والسلام على خاتم الأنبياء والمرسلين

نهدي عملنا هذا المتواضع إلى من أنار دربنا وأعنونا بالصلوات والدعوات لأغلى الوالدين في هذا الوجود " **أمي**" و "**أبي**" رحمة الله عليه.

إلى من كان لنا عونا وسندا في مشوارنا تعلمي أطال الله في عمرهم.

إلى قرة عيني زوجتي وفلذة كبدي **حذيفة أنس** وإخوتي كل باسمه.

إلى إبنة أخي وردة ادامها الله لنا

إلى كل الأساتذة الذين كان لهم الفضل في تعليمنا العلم النافع.

إلى جميع الأصدقاء والزملاء وكل من مد يد العون وفتح الطريق أمام أبواب المعرفة.

جمال بن براهم

إهـــــداء

نهدي عملنا هذا المتواضع إلى من أنار دربنا وأعنونا بالصلوات والدعوات لأغلى الوالدين

في هذا الوجود " **أمي**" رحمة الله عليها و "**أبي**" حفظه الله.

إلى كل العائلة كبيرا وصغيرا.

إلى الزوجة الكريمة وإلى أولادي "معاذ ومحمد الحبيب وكندة"

سعيد فار

قائمة المختصرات:

ق.ع.ج	قانون العقوبات الجزائري
ق.إ.ج	قانون الإجراءات الجزائية
ط	طبعة
ص	الصفحة
ص.ص	الصفحة إلى الصفحة

مـــقدمـــة

شهد العالم في العقود الأخيرة تطورًا هائلًا في مجال تكنولوجيا المعلومات والاتصـــالات، تجسّد في الانتشار السريع للهواتف الذكية، وخدمات الإنترنت، وشبكات التواصل الاجتماعي، والبريد الإلكتروني، وغيرها من الوسائل الرقمية التي أصبحت جزءًا لا يتجزأ من الحياة اليومية للأفراد، ومكوّنًا رئيسًا في أداء وظائف المؤسسات العامة والخاصة على حد سواء. وقد رافق هذا التطور التقني المتسارع بروز تحديات قـــانونية وأمنيـة خطيرة، من أبرزها مسألة **التنصت الإلكتروني**، الذي يُعدّ أحد أشكال المراقبة السرية التي تمارسها الجهات الأمنية أو أطراف أخرى بهدف جمع معلومات عن الأفراد، دون علمهم أو رضاهم، مما يثير إشكالات عميقة تتعلق بحقوق الإنسان، وعلى رأسها الحق في الخصوصية.

فالتنصت الإلكتروني – كأداة تدخل في الحياة الخاصة – يمسّ بشكل مباشر الحريات الأساسية، ويثير التساؤل حول مدى مشروعيته، والضوابط القانونيـــة التي ينبغـــي أن تؤطره، خاصةً في ظل التوتر القائم بين مقتضيات حماية الأمن العام من جهة، واحترام الحريات الفردية وحقوق الإنسان من جهة أخرى. وفي هذا السياق، أصبح لزامًا على مختلف التشريعات الوطنية، ومنها التشريع الجزائري، أن تواكب هذا الواقع من خلال تنظيم دقيق لمسألة التنصت، يوازن بين متطلبات حفظ النظام العام ومكافحة الجريمة، وبين ضمان عدم الانزلاق نحو الدولة البوليسية أو المساس غير المشروع بحرمة الحياة الخاصة للأفراد.

لقد وقف المشرع الجزائري على ضرورة تقنين التنصت الإلكتروني شأنه في ذلك شأن العديد من الأنظمة القانونية، خاصة بعد تزايد استخدامه من طرف الأجهزة الأمنية والقضائية في مكافحة الجرائم الخطيرة، لاسيما الجرائم الإرهابية، وجرائم الفساد، وتلك المرتبطة بالجريمة المنظمة عابرة الحدود، والجرائم الإلكترونية الحديثة. وقد تجسد هذا الاهتمام من خلال إدراج نصوص قانونية تنظم إجراء التنصت بوضع شروط وضوابط دقيقة، سواء في

قانون الإجراءات الجزائية، أو في القوانين الخاصة كقانون مكافحة الإرهاب، وقانون مكافحة الفساد، وقانون مكافحة الجرائم المعلوماتية.

ومع ذلك، فإن الممارسة العملية لا تخلو من تضارب، في ظل النصوص المتعلقة باحترام الحقوق والحريات للأفراد المنصوص عليها في الدستـــور والقوانين العـادية الاخرى، مما يطرح الحاجة إلى دراسة معمقة لتبيان الإطار القانوني الناظم لهذا الاجراء الخطير.

أهمية الموضوع:

تنبع أهمية هذا الموضوع من كونه يتناول مسألة حساسة تتعلق بحقوق الإنسان في ظل تزايد استخدام التكنولوجيا في المجال الأمني والقضائي، وتزايد حالات انتهاك الخصوصية، سواء من قبل الجهات الرسمية أو من قبل جهات خاصة، باستخدام أدوات تنصت متطورة. كما تكمن أهمية البحث في تسليط الضوء على التحديات القانونية والعملية التي يواجهها النظام الجزائري في هذا المجال.

إشكالية البحث:

يطرح إجراء التنصت الالكتروني إشكالات قانونية وحقوقية بالغة الأهمية، خاصة فيما يتعلق بمدى توافقه مع المبادئ الدستورية، وعلى رأسها الحق في الخصوصية وسرية الاتصالات، فضلاً عن شروطه وضوابطه الإجرائية، ومدى الرقابة القضائية عليه. ومن هنا تبرز الاشكالية الآتية:

- **ما مدى فعالية النظام القانوني الجزائري في تنظيم التنصت الإلكتروني بما يحقق التوازن بين حماية الأمن العام وصون الحريات الفردية والمؤسساتية؟**

المنهج المعتمد:

يعتمد هذا البحث على **المنهج الوصفي** كأساس، من خلال تحليل النصوص القانونية ذات الصلة بالتنصت الإلكتروني في القانون الجزائري. كما تم استخدام **المنهج الوصفي** لتقديم المفاهيم الأساسية.

أسباب اختيار الموضوع:

تم اختيار هذا الموضوع لعدة أسباب شخصية وموضوعية.

أولا: أسباب الشخصية

فعلى المستوى الذاتي راودنا اهتمام خاص بالقضايا القانونية المرتبطة بالتطورات التكنولوجية، وخاصة ما يتعلق بالمساس بالخصوصية في البيئة الرقمية، وهو ما يتماشى مع تخصصنا في قانون الإعلام الآلي والإنترنت، مما جعلنا نرى في هذا الموضوع فرصة علمية مناسبة لتعميق معرفتنا وتوظيف مكتسباتنا الأكاديمية، كما أننا نطمح من خلال هذا البحث إلى المساهمة في تسليط الضوء على موضوع لا يزال يطرح العديد من الإشكاليات القانونية، سواء من حيث النصوص أو التطبيق.

ثانيا: أسباب الموضوعية

أما من الناحية الموضوعية، فإن حداثة موضوع التنصت الإلكتروني وتزايد مخاطرة في العصر الرقمي، وما يطرحه من تحديات تمس الحقوق الأساسية للأفراد، خاصة الحق في السرية والحياة الخاصة، تجعل من هذا البحث ذا أهمية كبيرة. كما أن القصور النسبي في التشريع الجزائري في هذا المجال، وكذا ندرة الدراسات القانونية المتخصصة التي تعالج موضوع التنصت الإلكتروني في التشريع الجزائري بشكل كافي، كذلك تميزه بالطابع العملي وارتباطه الوثيق بالقضايا اليومية في ميدان التحقيق الجنائي والأمن الوطني.

رابعا : أهداف الدراسة

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف، منها:

- بيان الإطار المفاهيمي للتنصت الإلكتروني وتمييزه عن غيره من المفاهيم المشابهة.
- تحليل القواعد القانونية التي تُنظم التنصت الإلكتروني في التشريع الجزائري.

- إبراز صور المخاطر المرتبطة بهذه الممارسات، سواء على مستوى الأفراد أو المؤسسات.
- تبيان وسائل الحماية القانونية من مخاطر التنصت الالكتروني.

خامسا: الدراسات السابقة

من بين الدراسات التي تناولت موضوع التنصت الإلكتروني، نجد مقال للأستاذة **بن مالك إسمهان** بعنوان " أثر إجراءات التنصت الإلكتروني على حقوق وحريات الإنسان والمواطن " والتي نشرت في مجلة البيبان للدراسات القانونية والسياسية في ديسمبر 2017.

حيث ركزت هاته الدراسة على تحديد الحقوق والحريات محل المساس بهذه الإجراءات من خلال معرفة أهم الأسس القانونية سواء كانت وطنية أو دولية.

وقد خلصت الدراسة إلى تحديد الحقوق والحريات محل المساس بإجراءات التنصت التي كفلها القانون حمايته من انتهاك خصوصية عند تطبيق إجراءات التنصت.

تعد هاته الدراسة ذات صلة بموضوعنا، لكنها تركز أكثر على جانب الخصوصية الأفراد، في حين أن بحثنا يتناول النظام القانوني للتنصت الإلكتروني في التشريع الجزائري ككل، مع تسليط الضوء على الجوانب القانونية والتقنية وآليات التصدي للمخاطر المرتبطة به.

صعوبات البحث:

صعوبات التي وجهناها في إعداد هاته المذكرة وخاصة عند تناول الفصل المتعلق المخاطر المرتبطة بالتنصت الإلكتروني في الجزائر، قد تتنوع بين الجوانب القانونية، التقنية والمنهجية. ومن أبرز هذه الصعوبات:

- قلة الدراسات القانونية الجزائرية الحديثة التي تناولت موضوع التنصت الإلكتروني بصفة دقيقة ومباشرة، ونقص التغطية الأكاديمية لهذا الموضوع في المكتبات الجامعية أو في بعض المجلات العلمية.

- أن هذا الموضوع يمتاز بالحداثة كون أن التشريعات المرتبطة بالتكنولوجيا غالباً ما تكون جديدة ومتغيرة، مما يصعّب تتبّع النصوص القانونية أو الأحكام القضائية المستقرة.كما أن قد لا تكون هناك اجتهادات قضائية كافية في الجزائر بخصوص قضايا التنصت الإلكتروني. وتداخل بين القوانين حماية المعطيات الشخصية وقوانين الإجراءات الجزائية، والقوانين الخاصة بالأمن السيبراني.
- كما يغلب عليه الطابع التقني من خلال صعوبة فهم الوسائل التقنية المستخدمة في التنصت الإلكتروني، مثل برامج التجسس، أدوات القرصنة، أو طرق التشفير والحاجة لفهم آليات الحماية التقنية (كالتشفير، الجدران النارية، برامج مكافحة التنصت) مما يتطلب إلماماً بالمجال المعلوماتي أو التعاون مع مختصين.
- كذلك غياب الإحصائيات الرسمية أو الدراسات الميدانية حول حالات التنصت في الجزائر وحساسية الموضوع من الناحية الأمنية والسياسية، مما يجعل الوصول إلى معلومات دقيقة أو شهادات حقيقية صعباً.

خطة البحث:

لتناول موضوع "النظام القانوني للتنصت الإلكتروني في التشريع الجزائري"، تم تقسيم المذكرة إلى فصلين رئيسيين كما يلي الفصل الأول: الإطار المفاهيمي للتنصت الإلكتروني ويتضمن ماهية التنصت الإلكتروني ومظاهره، أما في التفرعة الثانية الرئيسية من هذا الفصل ركزنا على النظام القانوني للتنصت الإلكتروني في الجزائر.

أما الفصل الثاني: المخاطر المرتبطة بالتنصت الإلكتروني في الجزائر، ويتضمن آليات التصدي للمخاطر المرتبطة بالتنصت الإلكتروني، أما التفرعة الثانية من هذا الفصل ركزنا على المخاطر المرتبطة بالتنصت الإلكتروني في الجزائر.

الفصل الأول

الإطار المفاهيمي للتنصت

الفصل الأول:

الإطار المفاهيمي للتنصت الالكتروني

يعتبر موضوع تنصت الالكتروني من المواضيع التي وجب بداية ضبط بعض المفاهيم الأساسية المرتبطة بالتنصت الالكتروني لا سيما من تحديد ماهية التنصت الالكتروني وخصائصه وذكر بعض أنواعه مع تمييزه بالأنظمة المشابهة الأخرى، ناهيك عن الأساس القانوني المنظم للتنصت الإلكتروني في الجزائر من خلال ذكر النصوص التشريعية وذكر الجهات المخولة بإصدار وتنفيذ أوامر التنصت والحالات والضوابط التي يمكن اللجوء إلى التنصت الإلكتروني.

المبحث الأول:

ماهية التنصت الالكتروني

عرف العالم في العقود الأخيرة تطورا مذهلا في وسائل الاتصال وتكنولوجيا المعلومات، مما ساهم في تسهيل التواصل وتبادل البيانات بسرعة غير مسبوقة ، إلا أن هذا التقدم صاحبه بروز تحديات جديدة ، ومن أبرزها المساس بسرية الاتصالات وحرمة الحياة الخاصة من خلال التنصت الإلكتروني ، يعد هذا الأخير من أبرز مظاهر التقدم التكنولوجي في مجال الاتصالات والمعلومات، حيث أتاح استخدام الوسائل التقنية الحديثة إمكانية مراقبة وتسجيل المحادثات والاتصالات بمختلف أشكالها سواءا كانت هاتفية أو عبر الأنترنت، تناولنا في هذا المبحث مطلبين: مفهوم التنصت الإلكتروني **(المطلب الأول)**، أما **(المطلب الثاني)** تناولنا مميزات التنصت الإلكتروني.

المطلب الأول

مفهوم التنصت

في ظل التطور التكنولوجي المتسارع أصبحت المعلومات والبيانات الرقمية عرضة للانتهاك والاختراق مما أدى إلى ظهور التنصت الإلكتروني كأخطر أنواع التهديدات في العصر الحديث، سنتطرق في هذا المطلب إلى: تعريف التنصت الإلكتروني **(الفرع الأول)**، أما **(الفرع الثاني)** نبذة تاريخية للتنصت الإلكتروني.

الفرع الأول: تعريف التنصت الإلكتروني

يعرف التنصت في اللغة مأخوذ من فعل " نصتَ "، أي أصغى السمع خفية، يقال: "تنصتَ الحديث أي استمع إليه دون علم المتحدث وهو غالبا ما يستخدم للدلالة على الاستماع إلى حديث الغير دون إذنه.[1]

[1]– ابن منظور، **لسان العرب**، ط3، مادة نصت، ج14، دار صادر، بيروت، 1414هـ، ص 268.

كما يعرف على أنه استخدام الوسائل والتقنيات الحديثة كالبرمجيات وأجهزة التسجيل والمراقبة لاعتراض أو تسجيل أو متابعة الأجهزة السلكية أو اللاسلكية أو الرقمية (كالرسائل الإلكترونية والمكالمات الهاتفية) دون علم، أو موافقة الأطراف المعنية وغالبا ما يتم ذلك لأغراض أمنية أو تجسسية أو إجرامية.[1]

أولا: في الشريعة الاسلامية

وجاء في الشريعة الإسلامية استنادا إلى قوله تعالى: " **يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ**".[2]

فهذه الآية الكريمة وآيات أخرى تعد دستورا سماويا لحفظ الاسرار بما يتضمنه من النهي عن الظن والتجسس والغيبة وهذا وارد في الآية يشمل التنصت بأي وسيلة كانت مثل السمع أو النظر أو تسجيل المحادثات الهاتفية.

أما بالنسبة للسيرة النبوية فلم تأتي بتعريف للتنصت أو التجسس الذي كان في ذلك الوقت، وإنما اكتفى بذكر صفاته وأثاره وعقوبته وهذا لما رواه ابي هريرة عن رسول الله حيث قال: " **إيَّاكُمْ والظَّنَّ، فإنَّ الظَّنَّ أكْذَبُ الحَديثِ، ولا تَحَسَّسُوا، ولا تَجَسَّسُوا، ولا تَنافَسُوا، ولا تَحاسَدُوا، ولا تَباغَضُوا، ولا تَدابَرُوا، وكُونُوا عِبادَ اللهِ إخْوانًا.**"

حيث أن التنصت يؤدي الى اكتشاف عورات الناس وفضح سمعتهم وشرفهم

ثانيا في القوانين الوضعية

التنصت في التشريع الجزائري هو عبارة عن اعتراض المراسلات السلكيــة واللاسلكية، وحسب المادة 39 من الدستور تنص على أن لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة

[1]– محمد سلامة عبد القوي، **التنصت الإلكتروني في القانون الجنائي–دراسة مقارنة**، دار النهضة العربية، القاهرة، 2010، ص 25.

[2]– سورة الحجرات، الآية 12.

انطلاقا من نص المادة 47، من الدستور الجزائري التي نصت على سرية المكالمات الهاتفية وكل الاتصالات بأشكالها المختلفة من التنصت والمراقبة أو الاستماع أو النشر أو الاطلاع سواء كانت خطابات أو برقيات أو مسندات إلى آخره[1].

بالاستناد إلى نص المادة المجرمة فلقد كرس قانون العقوبات الجزائري ما جاء في الدستور بخصوص حق سرية المكالمات الهاتفية ضمنيا ما لم يتم الاعتـــراض بأمر قانوني، حيث هناك مواد قانونية صريحة في هذا الشأن منها المواد 137/107 قانون العقوبات الجزائري التي تجرم قيام الموظفين بالتعدي على حقوق الأفراد المشروعة منها الخاصة بمراسلتهم بكل أنواعها، ونتناول خاصة ما نصت عليه 303 مكرر وما يليها حول اعتراض المراسلات السلكية واللاسلكية.

المادة 303 من قانون العقوبات الجزائري بكل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير، وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر واحد إلى سنة واحدة وبغرامة 25000 دينار جزائري إلى 100.000دينار جزائري أو بإحدى هاته العقوبتين.

توظيف المادة 303 مكرر 1 على أنه تسلط نفس العقوبة المشار إليها في المادة 303 على كل من يقوم بنشر أو الاحتفاظ، أو وضع في متناول الجمهور تلك التسجيلات المنصوص عليها في المادة 303 مكرر خاصة بواسطة الصحافة ، إن المشرع الجزائري وتحت ضغط تفاقم الجرائم سنه القانون 06-22 المؤرخ في 20/12/2006، الذي شرع اللجوء إلى التنصت تحت عنوان اعتراض المراسلات السلكية واللاسلكية من طرف القضاء في التحري في الجرائم، حيث أدرج مفهوم التنصت دون الإشارة إليه بصريح العبارة في الفصل الرابع من قانون الإجراءات الجزائية تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور[2]، حيث خصص له 6 مواد من المادة 65 مكرر 05 إلى المادة 65 مكرر 10 نتناول فيها:

---

[1]- المادة 39 من الدستور الجزائري 2020، المؤرخة في 2020/12/20، ج.ر، العدد 82.

[2]- المواد 107 و137 و303مكرر، الأمر رقم 156/66، المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم بالقانون رقم 06-23، المؤرخ في 2006/12/20، ج.ر، العدد 84، ص 22.

- السلطة التقدير اللجوء إلى اعتراض المراسلات.
- أوطر التحقيق الممارس فيها اعتراض المراسلات.
- أنواع الجرائم التي تستعمل فيها تقنية اعتراض المراسلات.
- شروط الإذن باعتراض المراسلات الشكلية ومضمونه ومدته.

لم يضع المشرع تعريفا دقيقا لجريمة التنصت مكتفيا بالنص على تجريم الفعل دون تحديد معاييره القانونية، مما يفتح المجال أمام الاجتهاد القضائي لتحديد نطاقه استنادا إلى طبيعة الوسائل المستخدمة والسياق الذي يقع فيه، وبناء على ذلك يصبح من الضروري التطرق إلى خصائص نظام التنصت مع إبراز أنواعه، وهو ما سيتم تفصيله في المطلب الموالي.

غير أن المشرع اللبناني تكلم في نص المادة 8 من الدستور اللبناني على أن التنصت هو: "الحرية الشخصية مصونة وفي حمى القانون». ونصت المادة 9 من قانون تنظيم الأصول الإدارية والمالية في المديرية العامة للبريد والبرق الصادر بالمرسوم الاشتراكي الرقم 59/126 تاريخ 1959/6/12 على أن «سر المراسلات البريدية مصون لا يجوز إفشاؤه".

بينما المشرع المصري أصدر قانون تنظيم الاتصالات رقم 10لسنة 2003 وقام من خلاله بتجريم التعدي على حرمة الاتصالات (محادثات ومراسلات) حيث نصت المادة 83 منه على أنه: "يعاقب بالحبس بمدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تتجاوز خمسين ألف جنيه أو بإحدى العقوبتين كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها أو بأحد الأفعال الآتية:

إذاعة أو نشر أو تسجيل رسالة اتصالات أو لجزء منها

إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات أو لجزء منها تكون قد وصلت إليه.

كما المشرع المصري من القانون نفسه في المادة 88 على تجريم مجرد الأعمال التحضرية التي تمثل خطرا على الاتصالات.[1]

إن معظم التشريعات لم تعرف التنصت الإلكتروني تعريفا صريحا ومباشرا بل يتم تناوله ضمن أحكام أوسع تتعلق بالمراقبة أو الاعتراض أو التنصت على الاتصالات والمراسلات الإلكترونية

الفرع الثاني: نبذة تاريخية حول التنصت الإلكتروني

نشأ جدل كبير حول استخدام هذه التقنية لكشف الجريمة أو لجمع الأدلة للمحاكمة الجنائية يؤكد المعارضون أن المصلحة الحكومية المشروعة في الحد من الجريمة لا تفوق الاحتمال الكبير للانتهاك بناء على الضمانات الدستورية أو الأساسية للمواطنة، مثل الخصوصية الفردية والتحرر من عمليات التفتيش غير المعقولة والنوبات.

تعود أنشطة التنصت على المكالمات الهاتفية إلى قضية **أولمستيد** ضد الولايات المتحدة الأمريكية حيث تعد إحدى أولى المحطات المفصلية في تاريخ التنصت الإلكتروني، تعود وقائع القضية الى قيام الشرطة الفيديرالية بالتنصت على مكالمات **روي اولمستيد** المشتبه فيه في قضايا تهريب الكحول دون الحصول على إذن قضائي واستُخدمت تلك لمكالمات لاحقًا كدليل لإدانته. وعند عرض القضية أمام المحكمة العليا الأمريكية، قضت هذه الأخيرة بأغلبية الأصوات، بأن التنصت الهاتفي لا يُعد انتهاكًا للتعديل الرابع من دستور الأمريكي، ما دام لم يتضمن اقتحامًا مادّيًا لمنزل أو ممتلكات الشخص محل التنصت غير الذي أكد)أن هذا التوجه القضائي قوبل بمعارضة قوية من بعض القضاة، وفي مقدمتهم القاضي **لويس براندیز** في رأيه المخالف أن الحق في الخصوصية لا يقتصر على الحماية من التفتيش المادي، بل يجب أن يشمل حماية الاتصالات الخاصة من تدخل الدولة، وهو ما اعتُبر لاحقًا نواة لتوسيع نطاق الحماية الدستورية للخصوصية

[1]– محمد رشاد إبراهيم مفتاح، **الحماية الجنائية للحق في حرمة الاتصالات الشخصية**، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، 2009، ص 09.

وقد استمر الجدل القانوني حول هذه المسألة إلى أن أصدرت المحكمة العليا الأمريكية لاحقًا، في سنة 1967، حكمًا في قضية **Katz v. United States**، عدلت فيه عن موقفها السابق، حيث أقرت بأن التنصت على الاتصالات الهاتفية دون إذن قضائي يُعد انتهاكًا للخصوصية، حتى في غياب أي اقتحام مادي، مما مثّل تطورًا مهمًا في الفقه الدستوري الأمريكي بشأن حماية الحياة الخاصة في ظل التطورات التكنولوجية1968، أجاز الكونجرس استخدام المراقبة الإلكترونية لمجموعة متنوعة من الجرائم الخطيرة، والتي تخضع لرقابة قضائية صارمة.[1]

وفي أوائل القرن العشرين بدأت الحكومات في استخدام التنصت السلكي، خاصة خلال الحربين العالميتين، حيث استخدمت الاستخبارات ذلك كوسيلة فعالة لجمع المعلومات عن العدو وخططه العسكرية.[2]

أما التحول النوعي فقد حدث خلال الحرب الباردة، حيث شهدت أجهزة التنصت الإلكتروني تطورا كبيرا باستخدام الأقمار الصناعية والتقنيات الصوتية الدقيقة، كما أنشأت الدول الكبرى وكالات متخصصة مثل وكالة الأمن القومي الأمريكية.[3]

ومع نهاية القرن العشرين، أصبح التنصت الإلكتروني أكثر تطورا، خاصة مع ظهور الأنترنت والهواتف الذكية، مما وسّع من نطاق المراقبة ليشمل الرسائل، والتطبيقات، وأنظمة تحديد المواقع.[4]

وقد أدى هذا إلى بروز إشكاليات قانونية وأخلاقية، دفعت بالعديد من الدول إلى سن تشريعات تنظم عمليات التنصت وتحدد ضوابطها القانونية.[5]

---

[1]– WWW.OYEZ.ORG/CASES /1900-1940/277US 438 a، تم الاطلاع عليه في 2025/04/20 على الساعة 11:10.

[2]– حسان عبد الله، **الاستخبارات الحديثة وأثرها على الأمن القومي**، ط1، دار الهدى، بيروت، 2015، ص 34.

[3] –Edward Snowden, **Permanent Record**, London: Macmillan, 2019, P87.

[4] –Bruce Schneier, Date and Goliath: **The Hidden Battles to Collect Your Data and Control Your World**, New York: W.W.Norton & Company, 2015, P 54.

[5]– يوسف مراد، **الخصوصية في العصر الرقمي**، دراسة قانونية مقارنة، ط1، دار الفكر الجامعي الإسكندرية، الإسكندرية، 2021، ص 92.

المطلب الثاني:

مميزات التنصت الالكتروني

في عالم الاتصالات الحديثة أصبح التنصت الإلكتروني واحد من الأدوات الأساسية في جمع المعلومات والمراقبة حيث يمتاز بعدة خصائص في **(الفرع الأول)**، كما ينقسم هذا النوع إلى عدة أنواع في **(الفرع الثاني)**.

الفرع الأول: خصائص التنصت الإلكتروني

يتميز التنصت الإلكتروني بعدد من الخصائص التقنية والقانونية التي تجعله وسيلة خطيرة وفعّالة في الوقت ذاته، وتختلف عن وسائل التتبع التقليدية، ويمكن حصر أبرز هذه الخصائص فيما يلي:

أولا: السرية والخفاء:

يُعدّ التنصت الإلكتروني من الوسائل الخفية التي تعتمد على جمع المعلومات دون علم الشخص المستهدف، وهو ما يهدد بشكل مباشر مبـــدأ الخصوصية والحرمـــة الشخصية، حيث يتم غالبا دون أي مؤشرات مرئية تدل على حدوثه.[1]

ثانيا: الاعتماد على التكنولوجيا المتطورة

يعتمد التنصت الإلكتروني على تقنيات متقدمة تشمل أجهزة وبرمجيات قادرة على اختراق المكالمات والبيانات، مثل برامج التجسس والتطبيقات الخبيثة، إضافة إلى استخدام الذكاء الاصطناعي في تحليل المعلومات.[2]

---

[1]– محمد عبد العزيز، **الجرائم الإلكترونية في القانون الجنائي المعاصر**، دار الفكر الجامعي، الإسكندرية، 2021، ص 112.

[2]– أحمد سلامة، " **التنصت في ظل تطور وسائل الاتصال الحديثة** "، المجلة الجزائرية للعلوم القانونية، العدد 2، 2020، ص 86.

ثالثا: الاتساع في النطاق

لا يقتصر التنصت على أهداف فردية، بل يمكن توجيهه نحن مؤسسات أو مجموعات وحتى دول، حيث تُستخدم فيه أدوات قادرة على مراقبة عدد كبير من الاتصالات في وقت واحد.[1]

رابعا: السرعة والفعالية في جمع المعلومات

تمكن الوسائل الإلكترونية الحديثة من جمع كميات ضخمة من البيانات خلال فترات زمنية قصيرة، ما يزيد من فعاليتها مقارنة بوسائل التنصت التقليدية التي تعتمد على المراقبة الميدانية.[2]

خامسا: الغموض القانوني

يطرح التنصت الإلكتروني إشكالات قانونية معقدة، نظرًا لصعوبة ضبطه من الناحية التشريعية، فغالبا ما يتم بطرق يصعب إثباتها قانونا، وهو ما يخلق حالة الفراغ أو الإبهام التشريعي.[3]

سادسا: التهديد المباشر للخصوصية

يُعدّ من أخطر أشكال التعدي على الحياة الخاصة، لما له من قدرة على اقتحام الحياة الشخصية للأفراد دون إذن أو رقابة، وهو ما يتنافى مع الحقوق الأساسية التي تحميها الدساتير والاتفاقيات الدولية.[4]

الفرع الثاني: أنواع التنصت الإلكتروني

تتعدد أنواع التنصت الإلكتروني ولا يمكن حصرها في نوع محدد نظرا للتطور التكنولوجي الرهيب في مجال برمجيات واستخداماتها، ويستخدم هذا النوع من التنصت في

---

[1]– سمير بن شريف، **الجريمة الإلكترونية بين النظرية والتطبيق**، ط1، دار الجامعة الجديدة، 2022، ص 145.

[2]– المرجع نفسه، ص 147.

[3]– ياسين بوشامة، " **الإشكالية القانونية للتنصت الإلكتروني** "، مجلة الدراسات القانونية المعاصرة، العدد 5، 2021، ص 59.

[4]– الجمعية العامة للأمم المتحدة، الإعلان العالمي لحقوق الإنسان، القرار 217 أ (د–3)، اعتمد في 10 ديسمبر 1948، المادة 12.

مجالات متعددة مثل الاستخبارات والأمن السيبراني والتجسس الصناعي، وأحيانا لأغراض غير قانونية مثل الابتزاز وانتهاك الخصوصية، وعليه يمكن تصنيف التنصت الالكتروني لعدة أنواع أهمها:

أولا: التنصت عن طريق شبكة السلكية واللاسلكية

ظهرت أنواع أخرى للتنصت الالكتروني في الشركات والجهات التي تستخدم الشبكات ما يعرف بـ (sniffer) أو اصطياد حزم البيانات المرسل، ومن أشهر هذه البرامج أنظمة ويندوز وليكنس هو برنامج (Ethereal) للشبكات الداخلية وبرامج (Tc dump) و(windup) وغيرها، وقد تمت تجربة أحد أنواع (sniffer) وهو مختص في اصطياد كلمة المرور في إحدى مقاهي الأنترنت، فكانت النتيجة الحصول على كلمات المرور السرية لايميلات الأشخاص الذين سجلوا الدخول.[1]

ثانيا: التنصت بواسطة الأقمار الصناعية

هذا النوع من أنواع التنصت الإلكتروني يتمتع بالصفة الدولية ويستخدم في أجهزة نادرة جدا والمراجع في هذا المجال جد قليلة إن لم نقل تكاد تكون منعدمة، لكن يمكن القول أن التنصت من خلال الأقمار الصناعية لا يمكن أن يقوم به فرد أو منظمة، وإنما يقتصر على الدولة المتقدمة التي تسيطر على كل البيانات في العالم وتملك أقمار صناعية هي التي قامت بوضعها شخصيا، وتتمتع هذه الأقمار الصناعية بأحدث التكنولوجيا والبرامج على وجه الأرض يتم إطلاقها علنا عادة أمام الرأي العام لأسباب إنسانية أو علمية، لكن وحدها الدول المسؤولة على إرسال القمر الصناعي تعرف الغاية، والهدف الحقيقي لمهمة القمر الصناعي إن كان مبعوثا بهدف التنصت أو غير ذلك.

[1]– عمار محمود، **أمن المعلومات والجرائم الالكترونية**، دار صفاء للنشر والتوزيع، عمان، 2018، ص 112–115.

ثالثا: التنصت باستعمال شبكات الهاتف النقال

التوصل إلى فك الأنظمة الالكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التنصت عن طريق الموجات المرسلة أثناء مكالمة هاتفية، أو رسالة نصية يمكن الاطلاع على ما تحتوي أو تغييرها أو حذفها.

وحول إمكانية اختراق التشفير ممكنة وصحيحة وقد عرضت صور من البرنامج لالتقاط محادثة ورسائل نصية بدقة عالية، حيث أن البرنامج يدعم نظام اليونكود لمختلف اللغات وتوجد بتحديد نسخة لـ GSM والنسخة للثريا فقط، معنى ذلك أنه بالحصول على هذا البرنامج وتركيبه على جهاز يحتوي على وصلة لاسلكية يستطيع أي شخص التنصت على شبكة GSM.[1]

رابعا: التنصت باستخدام البرامج الخبيثة (Spyware, malware)

يتم ذلك عن طريق زرع برمجيات تنصت على أجهـــزة الكمبيوتـــر أو الهواتف الذكية، مما يسمح بتسجيل المحادثات إلتقاط لقطات الشاشة أو حتى تشفير الكاميرا أو الميكروفون عن بعد.

خامسا: التنصت على لوحات المفاتيح (keylogging)

يتم ذلك عبر برمجيات أو أجهزة مغايرة تثبت على لوحات المفاتيح لتسجيل كل ضغطة مفتاح وإرسالها إلى الجهة المتنصة.[2]

الفرع الثالث: تمييز التنصت الإلكتروني مع الأنظمة المتشابهة

يُعدّ التنصت الإلكتروني من أخطر الوسائل المستحدثة التي تعتمدها بعض الجهات الرسمية أو غير الرسمية في سبيل جمع المعلومات والبيانات، وذلك لما يتيحه من اختراق لخصوصيات الأفراد والمؤسسات دون علمهم أو رضاهم، غير أن هذا المفهوم كثيرا ما

[1]– عبيد المنعم وسام، **التحقيق في الجرائم الالكترونية**، دار النهضة العربية، بيروت، 2018، ص 69

[2]– عبد الكريم أحمد حسن، **الاختراق والتجسس الإلكتروني وأساليب الحماية**، دار الكتب العلمية، القاهرة، مصر، 2020، ص 70.

يختلط بمفـــاهيم أخرى قريبـــة منه، مثل اعتـــراض المراسلات والتقاط الصـــور والتجسس، والتسرب، ما يستدعي تمييزه عن باقي الأنظمة.

أولا: التنصت الالكتروني مع اعتراض المراسلات والتقاط الصور الإلكترونية

يشكل التنصت الإلكتروني أحد أبرز أساليب جمع المعلومات الحديثة، حيث يقوم على اعتراض الاتصالات السمعية أو الرقمية التي تتم عبر الوسائط الإلكترونية، سواء بين الأفراد أو بين المؤسسات، وإلى جانبه برزت وسائل أخرى لا تقل خطورة، مثل اعتراض المراسلات الإلكترونية التي تشمل البريد الالكتروني والرسائل النصية، وكذلك التقاط الصور خلسة عبر الكاميرات أو الأجهزة الذكية، ورغم اختلاف هذه الأساليب في الوسائل والتقنيات.

1- التنصت الإلكتروني مع اعتراض المراسلات الإلكترونية:

هي عملية التقاط وفحص البيانـــات المرسلـــة بين طرفيـــن قبـــل أن تصل إلى وجهتها، ويتم ذلك غالبا عبر شبكات الاتصالات، ويختلف اعتراض المراسلات عن التنصت في أنه يركز على البيانـــات المكتوبة والمعلومـــات الرقميـــة أكثر من المحـــادثات الصوتية، ويهدف اعتراض المراسلات إلى سرقة البيانات الحساسة مثل كلمة المرور والمعلومات المصرفية والتلاعب بالمعلومات قبل وصولها إلى طرف المستهدف مع مراقبة الاتصالات لأغراض أمنية أو استخباراتية.

رغم التشابه بين التنصت الالكتروني واعتراض المراسلات في كونها وسيلتين للتنصت والمراقبة إلى أن الفرق الأساسي يكمن في نوع البيانات المستهدفة والأساليب المستخدمة.

التنصت الالكتروني يركز على المحادثات الصوتية والمكالمات، بينما اعتراض المراسلات يركز على اعتراض البيانات المكتوبة مثل الرسائل الالكترونية والمعلومات الرقمية، لذلك يجب اتخاذ إجراءات أمنية لحماية الخصوصية ومنع التسلل الالكتروني.

2-التمييز بين التنصت الالكتروني والتقاط الصور الإلكترونية:

يشير إلى عملية التقاط الصور أو تسجيل الفيديو دون علم أو إذن الشخص المستهدف وذلك عبر الكاميرات المخفية أو استغلال كاميرات لأجهزة الالكترونية مثل الهواتف والكمبيوتر، والكمبيوتر المحمولة ومن أهدافه التنصت على الأفراد أو الشركات مع استخدام

الصور في الابتزاز واستعماله في المراقبة الأمنية أو الاستخباراتية مع سرقة البيانات البصرية مثل مستندات أو أماكن حساسة، فالتنصت الالكتروني يركز على اعتراض المحادثات الصوتية والتنصت على المكالمات، بينما إلتقاط الصور الالكترونية يركز على جمع المعلومات عبر اختراق الكاميرا أو استخدام كاميرات مخفية كلاهما يشكل تهديدا خطيرا للخصوصية، لذا من الضروري اتخاذ تدابير وقائية لحماية من هذه الهجمات[1].

ثانيا: التنصت الالكتروني مع التسرب والتجسس الالكتروني

أصبح التنصت الإلكتروني من أبرز التهديدات التي تواجه الخصوصية في العصر الرقمي، لما يمثله من قدرة على اعتراض المكالمات أو الاتصالات عبر الوسائط التكنولوجية دون علم أو إذن من أصحابها، ويُعدّ هذا النوع من الممارسات جزءا من منظومة أوسع من الاعتداءات الالكترونية، تتضمن كذلك التسرب المعلوماتي الذي يقوم على التسلل الخفي إلى الأنظمة لجمع معلومات حساسة دون إذن مسبق.

1-التنصت الإلكتروني مع التسرب الإلكتروني:

يعد التسرب الالكتروني من الإجراءات المستحدثة للوقاية من الجرائم التي ترتكب باستعمال تكنولوجيات الاعلام والاتصال، وقد أشار إليه المشرع الجزائري في قوانين خاصة كقانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية[2]، وأيضا القانون رقم 15-20 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها[3]، في التسرب الالكتروني هو إجراء يسمح لضباط وأعوان الشرطة القضائية بمراقبة الأشخاص المشتبه فيهم بإلهامهم بأنهم فاعلون معهم أو شركائهم، وذلك بهدف جمع الأدلة والمعلومات حول

---

[1]- عبد القادر يخلف، " **الخصوصية الرقمية في ظل التشريعات الحديثة** "، مجلة البحوث القانونية والاقتصادية، العدد 15، جامعة الجزائر 1، 2022، ص 45.

[2]- قانون 20-05، المؤرخ في 2020/04/28، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج.ر، العدد 25، المؤرخ في 2020/04/29.

[3]- قانون 15-20، المؤرخ في 2020/12/30، المتعلق بالوقاية من جرائم الاختطاف الأشخاص ومكافحتها، ج.ر، العدد 81، المؤرخ في 2020/12/30، ص 05.

الأنشطة الإجرامية يعتبر هذا الاجراء وسيلة فعالة لكشف الجرائم المعقدة مثل الجرائم الالكترونية والاتجار بالمخدرات والجرائم المنظمة.

قد نص المشرع على حماية هوية الضباط المتسربين حيث لا يجوز الكشف عن هويتهم الحقيقية في أي مرحلة الإجراءات إلا لرؤسائهم السلميين، وبالنظر إلى ما سبق يتضح أن الفرق الأساسي بين التنصت الالكتروني والتسرب الالكتروني يكمن في طبيعة الإجراءات والأهداف المرجوة منه.

أ- التنصت الالكتروني:

هو إجراء يهدف إلى اعتراض ومراقبة الاتصالات الخاصة دون علم الأطراف المعنية ويعتبر تعديا على الخصوصية، إلا إذا تم بموجب إذن قضائي وفي إطار تحقيق جنائي محدد.

ب- التسرب الالكتروني

هو إجراء يهدف إلى التوغل داخل الجمعات الاجرامية بإيهامهم بأن الضباط المتسربين شريكين لهم، وذلك لجمع الأدلة والمعلومات من داخل هذه الجماعات ويعتبر هذا الإجراء مشروعا إذا تم بموجب إذن قضائي وتحت اشراف السلطات المختصة.[1]

بالإضافة إلى ذلك تختلف الإجراءات من حيث الضمانات والقيود القانونية المفروضة عليهما، ففي حالة التنصت الالكتروني يتطلب الأمر الحصول على إذن القضاء مسبق وتحديد دقيق للمدة، والجرائم المستهدفة لضمان عدم المساس بحقوق الأفراد وحرياتهم الأساسية.

أما في حالة تسرب الالكتروني فيسمح للضباط المتسربين باستخدام هوية مستعارة والقيام بأعمال قد تعتبر جرائم في ظروف أخرى، وذلك دون أن يكونوا مسؤولين جزائيا عن

[1]- فاتح قيشي، " **آليات الحق في الخصوصية** "، مقال نشر في مجلة حقوق الإنسان، العدد 36، جامعة أدرار، الجزائر، ص 93.

هذه الأفعال بشرط الحصول على ترخيص من السلطة القضائية المختصة والالتزام بالضوابط القانونية المحددة.[1]

2- التنصت الالكتروني والتجسس الالكتروني:

بعد أن تطرقنا سابقا إلى تعريف التنصت الالكتروني نعرف التجسس الالكتروني حسب القانون الجزائري، وما جاء به المشرع التجسس الالكتروني هو الولوج أو محاولة الولوج الغير مشروع إلى منظومة معلوماتية أو البقاء فيها دون إذن شرعي بغرض الحصول على المعلومات، أو بيانات سرية تمس الأمن الوطني أو النظام العام أو المصالح الاقتصادية للدولة.

لقد نص القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها في المادة 04.

نميز بين التنصت الالكتروني والتجسس الالكتروني من حيث:

أ- الأساليب والتقنيات المستخدمة

- أساليب التنصب الالكتروني:

اعتراض الإشارات مثل استخدام أجهزة imisc catcher's لاعتراض إشارات الهواتف المحمولة، أو برامج تحليل الحزم (packet sniffers) اعتراض الشبكة اللاسلكية.

هجمات الرجل في المنتصف (man in the middle) حيث يتم وضع جهة وسيطة بين المرسل والمستقبل لاعتراض وتسجيل المعلومات المرسلة دون غيرها.

- التجسس الالكتروني:

- **الاختراق والقرصنة:** يشمل ذلك استخدام برمجيات خبيثة مثل أحصنة طرواده وبرامج التجسس (spyware) اختراق الأنظمة، واستغلال الثغرات الأمنية بهدف الوصول إلى المعلومات الحساسة المخزنة داخل الأجهزة أو الخوادم.

[1]- نسيمة بطيحي، **الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية القيمة في التشريع الجزائري**، رسالة لنيل شهادة الماستر، جامعة الحقوق والعلوم السياسية، سطيف2، الجزائر، 2019/06/30، ص 48.

- **جمع المعلومات المؤرشفة:** حيث يتم استهداف قواعد البيانات والأنظمة الإدارية للحصول على معلومات متكاملة عن ضحايا، أو المؤسسات مما يتطلب غالبا جهدا منظما ومتعددا للمراحل.

ب- من ناحية الأهداف والنتائج المترتبة

في حالة تنصت الالكتروني يكون لها هدف عادة مراقبة الاتصالات الجارية في الوقت الحقيقي سواء لأغراض أمنية كالتحقيق في جرائم معينة أو لأغراض تجارية واستخباراتية محدودة، كما أن التأطير يكون غالبا محدودا بإمكانية اعتراض المعلومات دون تغييرها أو تخزينها لفترة طويلة مما يقلل من مخاطر كشف العملية في وقت مبكر.

أما التجسس الالكتروني يهدف إلى الحصول على بيانات واسعة النطاق واستخدامها لاحقا لتحقيق مكاسب استراتيجية أو سياسية أو مالية، وغالبا ما تكون هاته أكثر شمولا وتستلزم جهدا أكبر في الاخفاء والتخزين والتحليل مما يزيد من خطورتها وتأثيرها على الأمن السيبراني للجهات المستهدفة.

ج- من ناحية الجوانب القانونية والأخلاقية

يرتكز التمييز بين التنصت والتجسس الالكتروني على إطار قانوني وأخلاقي يميز بينهما من حيث النية والتأثير يعتبر التنصت في بعض الحالات إجراء قانونيا إذا تمت الموافقة عليه من الجهات المختصة، مثل أجهزة المخابرات في حالات مكافحة الإرهاب بينما يعد التجسس الالكتروني انتهاكا صريحا للقوانين والحقوق الفردية والدولية، مما يعارض الجهة المنفذة للعقوبات القانونية والفنية.[1]

ومما نخلص إليه أن التنصت الالكتروني يركز على اعتراض المعلومات أثناء انتقالها دون تغييرها، بينما يسعد تجسس الالكتروني إلى جمع المعلومات والبيانات بشكل شامل ومنهج استخدامها لاحقا في تحقيق أهداف محددة.

[1]- عبد القادر يخلف، المرجع السابق، ص 65.

المبحث الثاني

الأساس التشريعي للتنصت الإلكتروني في الجزائر

يعد التنصت الإلكتروني من أبرز الوسائل الحديثة التي تعتمدها السلطات القضائية لمكافحة الجرائم الإلكترونية والجريمة المنظمة، لهذا حدد المشرع الجزائري إطار قانونيا صارما ينظم إجراءات التنصت الإلكتروني مع تأكيد على الضوابط التي تضمن عدم التعسف في استخدامه، حيث تناولنا في **(المطلب الأول)** النصوص التشريعية المنظمة للتنصت الالكتروني، أما في **(المطلب الثاني)** تناولنا الجهات المخولة بإصدار وتنفيذ أوامر التنصت.

المطلب الأول

النصوص القانونية المنظمة للتنصت الإلكتروني

سنتطرق في هذا المطلب إلى تبيين مختلف النصوص التشريعية، حيث نتنـــاول في **(الفرع الأول)** الاتفاقيات والمؤتمرات الدولية والإقليمية، وفي **(الفرع الثاني)** الدستور الجزائري، وأخيرا قوانين المنظمة لهذا الموضوع في **(الفرع الثالث)**.

الفرع الأول: الاتفاقيات والمؤتمرات الدولية والإقليمية

حرصت معظم الاتفاقيات الدولية والمؤتمرات على حماية حرمة الاتصالات الإلكترونية في إطار حماية حق في الحياة الخاصة بدءا بالإعلان العالمي لحقوق الإنسان، بحيث نصت المادة 12 منه على أنه "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته... ولكل شخص الحق في حماية القانون من مثل تلك التدخلات.

كما تكررت هذه المادة في المادة 17 فقرة أولى من العهد الدولي الخاص بالحقوق السياسية والمدنية، والمادة 08 من الاتفاقية الأوروبية لحقوق الإنسان وعقدت من أجله العديد من الاتفاقيات الإقليمية والمؤتمرات منها الاتفاقية الأمريكية لحقوق الإنسان، إعلان

حقوق المواطن العربي، الميثاق الإفريقي لحقوق الإنسان، المؤتمر الدولي لحقوق الإنسان المنعقد في طهران، المؤتمر الدولي لحقوق الإنسان المنعقد في مونتريال...إلخ.[1]

الفرع الثاني: الدستور الجزائري

أكده دستور 2020 على حرمة الحياة الخاصة، فقد جاء في نص المادة 47 منه الفقرة الثانية على أنه: " لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت"، كما نصت نفس المادة على حماية الأشخاص عند معالجة المعطيات ذات طابع الشخصي حق أساسي.

من خلال هذه المادة سالفة الذكر نجد أن الدستور الجزائري أقر للفرد في أن يحتفظ لنفسه بحق الاطلاع على أشياء معينة، ويمنع غيره من الاطلاع عليها دون رضاه أو إذنه.

الفرع الثالث: القوانين المنظمة

حيث نظمت قوانين الأتية الذكر كل من القانون المدني وقانون العقوبات وقانون الاجراءات الجزائية على تنظيم التنصت الإلكتروني في الجزائر.

أولا: القانون المدني

فحسب القانون المدني الجزائري خاصة في المادة 47 التي تنص على: "لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء والتعويض عما يكون قد لحقه من ضرر".

ثانيا: قانون العقوبات

لقد أقر قانون العقوبات الجزائري حماية لحرمة الحياة الخاصة من أي اعتداء لا سيما من الاستعمالات غير المشروعة لتكنولوجيا المعلومات والاتصالات الحديثة، ذلك أن كل

[1]– شنة زواوي، " **الحماية القانونية للحق في حرمة المحادثات الهاتفية** "، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، مخبر المرافق العامة والتنمية، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، العدد 19، جوان 2018، ص 659.

من النشر والتصوير والاستراق السمعي البصري والمعلوماتي، والاطلاع على المراسلات المكتوبة والهاتفية تشكل صور الاعتداء على حرمة الحياة الخاصة.[1]

أما بالنسبة المراسلات الإلكترونية تقضي المادة 303 مكرر من قانون العقوبات أنه: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة 50.000دج إلى 300.000دج كل من تعمّد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

1-الالتقاط أو تسجيل أو نقل مكلمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

كما تنص المادة 303 مكرر 01 من قانون العقوبات أنه: "يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدام بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها المادة 303 من هذا القانون".

الملاحظ أن المشرع الجزائري جرم وعاقب في قانون العقوبات كل تعدي على جريمة المراسلات والاتصالات، سواء عن طريق نقل المكالمات أو الأحاديث الخاصة أو السرية إذا كانت القاعدة العامة تقضي بعدم مشروعية التنصت على المراسلات والمحادثات الخاصة بكافة أنواعها، فهناك إنشاء يرد عليها حيث يبيح مراقبة المحادثات الخاصة، إذا كان بأمر من الجهة الخاصة المخولة لها بإصدار الإذن بذلك وبصفة قانونية.[2]

ثالثا: قانون الإجراءات الجزائية

فالرجوع لقانون الإجراءات الجزائية المعدل والمتمم في الفصل الرابع في المادة 65 مكرر 05 إلى المادة 65 مكرر 10 والمعنون بـ: "في اعتراض المراسلات وتسجيل

---

[1]- دنون يونس صالح المحمدي ومهدي صالح شحادة العبيدي، " **التعويض الناشئ على الاعتداءات على حرمة الخاصة** "، مجلة جامعة تكريت للحقوق، المجلد 2، الجزء1، العدد3، العراق، مارس 2018، ص ص 162، 163.

[2]- خليدة أوقاسي، **حرمة الحياة الخاصة في قانون الجنائي**، دراسة مقارنة في التشريع الجزائري والفرنسي، مذكرة لنيل شهادة ماجستير، كلية الحقوق، القانون والعلوم الجنائية، جامعة الجزائر1، 2014/2013، ص 32.

الأصوات والتقاط الصور"، قد سمحت بالتنصت في بعض الجرائم أهمها جرائم المخدرات والجرائم العابرة للحدود الوطنية جرائم تبييض الأموال..." أو ما يعرف عليها بالجرائم السبعة وما يضفي صفة المشروعية على عملية التنصت، صدور الإذن من جهة قضائية وهي إما وكيل الجمهورية أو قاضي التحقيق.[1]

فلقد رخص المشرع الجزائري للسلطات القضائية المختصة بموجب نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية إعتراض المراسلات وإلتقاط الصور وتسجيل الأصوات، حيث جاء فيها أنه: "إذا اقتضت ضرورات التحري في الجرائم المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة عبر الحدود والجرائم الماسة بأنظمة المعالجات للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالعرف يجوز لوكيل الجمهورية المختص يأذن بما يلي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية.
- وضع ترتيبات التقنية دون موافقة المعنيين، من أجل إلتقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص.

بالرجوع للمواد من المادة 65 مكرر 05 إلى المادة 08 من قانون الإجراءات الجزائية تتمثل شروط إباحة التنصت فيما يلي:

- أن تكون الجريمة قد وقعت فعلا.
- أن تكون هذه الإجراءات استثنائية مفيدة في كشف الحقيقة.
- أن تكون الجريمة جناية أو جنحة بشرط أن يعاقب عليها لمدة تزيد عن 03 أشهر.
- أن يصدر الأمر أو الإذن من القضاء بمراقبة الأحداث.
- أن يكون الإذن مسببا.

[1]– عيسى العاقب، **حماية الحياة الخاصة**، أطروحة دكتوراه، كلية حقوق والعلوم السياسية، قانون خاص، جامعة سعد دحلب، بليدة، 2014، ص 98.

ونصت المادة 03 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها على أنه: "على مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام والآداب العامة أو لمستلزمات التحريات أو التحقيقات الجارية... وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل معلوماتية".[1]

وتطبيقا لنص المادة 13 من القانون المذكور أعلاه صدر مرسوم الرئاسي المحدد لتشغيله وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، حيث تكلف هذه الهيئة بموجب المادة 04 منه بضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص.[2]

من خلال النصوص القانونية السابقة الذكر نلاحظ أن المشرع الجزائري ضيق من نطاق الحق في حرية المراسلات، والاتصالات الإلكترونية في مكافحة بعض الجرائم التي تتسم بخطورتها منها جرائم المخدرات... إلى غاية جرائم الفساد.

حيث منح المشرع الجزائري صلاحيات للسلطة القضائية المختصة وضباط الشرطة القضائية تمكنهم من مراقبة الاتصالات الإلكترونية، وإلزام مقدمي الخدمات الأنترنت بحفظ بيانات المستخدمين التي تمكن من التعرف عليهم.

وهو ما يتعارض مع الحق في الخصوصية، لأن هذه القواعد تسمح بمراقبة الاتصالات الإلكترونية وجمع البيانات سواء من طرف السلطات الداخلية أو الأجنبية في إطار تعاون

[1]– القانون رقم 04/09 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، المؤرخة في 06 أوت 2009.

[2]– المرسوم الرئاسي رقم 261/15، المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.ر، ع 53.

الدولي والمساعدة القضائية، إلا أن اهمال المشرع الجزائري لحماية الحق في الخصوصية ليس مغيبا تماما، لأنه يمكن أن نلمس إرادته في توفيق بين تبني القواعد الإجرائية الناجعة لمكافحة الجرائم والوقاية منها وبين تكريس هذا الحق المهم.[1]

المطلب الثاني:

الجهات المخولة بإصدار وتنفيذ أوامر التنصت

يعد التنصت الإلكتروني من الإجراءات الاستثنائية التي تمس بحقــوق الأفراد وحرياتهم، ولذلك فإن القانون الجزائري حصر الجهات المخولة بإصدار أوامر التنصت في سلطات معينة وفقا لما تقتضيه ضرورات التحقيق والأمن القومي وتتمثل هذه الجهات في **(الفرع الأول)** الجهات المخولة لإصدار أوامر التنصت، أما **(الفرع الثاني)** ويتمثل في الجهات المنفذة لجهات التنصت.

الفرع الأول: الجهات المخولة لإصدار أوامر التنصت

أولا: السلطة القضائية

تعد السلطة القضائيـــة الجهة الأساسيـــة المخولة بإصـــدار أوامر التنصت الإلكتروني، وذلك في إطار تحقيقات القضائية المتعلقة بالجرائم الخطيرة ويبرز دور القضاء من خلال:

- إذ ينعقد الاختصاص لوكيل الجمهورية إذ توفرت فيه الشروط اللازمة فيما يخص الاختصاص النوعي والإقليمي، فيمكنه مباشرة إعماله في إطار الإذن بإجراءات التنصت بصفة قانونية لضباط الشرطة القضائية وفقا لشروط وضمانات الموجودة في نص أحكام المادة 65 مكرر 05 من قانون الإجراءات الجزائية إلى 65 مكرر 10 رغم أن إجراءات التنصت الإلكتروني إجراء من إجراءات التحقيق، إلا أن

[1]– عقيدة مباركية، " **الحماية الجنائية في الخصوصية الرقمية في القانون الجزائري** "، مجلة الشريعة والاقتصاد، العدد 13، المجلد 7، 2018، ص ص 458، 489.

المشرع رأى عدم إطلاق يد النيابة العامة وهي سلطة التحقيق، إذ حد من صلاحيتها وجعل سلطتها في التنصت الإلكتروني تكون مقيدة بشروط منها: إعطاء الإذن القضائي بإجراءات التنصت على أن يكون مسبب ومحدد، حيث يتضمن هذا الإذن مختلف البيانات والمعلومات عن الشخص محل المراقبة، وكذا الشخص المعني بالقيام بهذه المراقبة والذي يجب أن تتوفر فيه هو الآخر شرط التأهيـــل لأداء المهمة، فيجب أن يكون من ضباط الشرطة القضائية وكذا بيان منها القانونية ونوعية الجريمة محل المراقبة.[1]

كذلك ضرورة التقيد بشروط وحالات إصدار هذا الإذن الذي تضمنه المادة 65 مكرر 05 من قانون الإجراءات الجزائية السابقة الذكر، وهي الجرائم السبعة حيث أن الخروج عنها أو القياس عليها يعد باطلا حتى ولو كان بناء على إذن مسبق من قبل وكيل جمهورية.

بالإضافة إلى شرط المراقبة المباشرة التي يجب على وكيل الجمهورية أن يراقب إجراءات التنصت المأذون بها لضباط الشرطة القضائية القيام بها، وهذا من أجل منع التعسف الذي يحصل من ضباط الشرطة القضائية.

كما يمكن لوكيل الجمهورية المختص أن ينتدب أحد ضباط الشرطة القضائية للقيام بعملية إجراءات التنصت وفق مراعاة الشروط القانونية الواجب توافرها في هذا الشخص المنتدب وهي أن يكون مؤهلا، إذ يجب أن يكون من رجال الضبطية القضائية.

- كما أن لقاضي التحقيق المختص سلطة واسعة في هذا المجال، ومن أهم صلاحياته في هذه الإجراءات الخاصة بالتنصت نجد:

[1]– اسمهان بن مالك، " **أثر إجراءات التنصت على حقوق وحريات الإنسان والمواطن** "، مجلة البيبان للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، العدد 04، ديسمبر 2017، ص 189.

- إصدار إذن قضائي بمراقبة عملية التنصت إلا بناءا على إذن مكتوب ومسبب من قبل القاضي التحقيق المختص، حيث يجب أن يتضمن الإذن القضائي كافة البيانات الخاصة بعنوان الشخص محل المراقبة.
- كذلك انتداب أشخاص مؤهلين ومختصين للقيام بعملية التنصت ويكون من بين رجال الضبطية القضائية لا غيرهم من الأشخاص العاديين، وإلا اعتبرت إجراءات التنصت باطلة.
- ضرورة التقيد بشروط أحكام المادة 65 مكرر 05 من قانون إجراءات الجزائية فيما يخص حالات تطبيق إجراءات التنصت، وهي الجرائم السبعة كالآتي: جريمة المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، الجرائم تبييض الأموال، الجرائم المتعلقة بتشريع الخاص بالصرف، جرائم الفساد.[1]

بعدما تكلمنا عن الجهات المخولة بإصدار أوامر تنصت الإلكتروني، سنتطرق إلى الجهات المنفذة للأوامر الصادرة عن الجهات القضائية وتتمثل هذه الأخيرة في:

الفرع الثاني: الجهات المنفذة لأوامر التنصت.

أولا: الجهات الأمنية

1-الشرطة القضائية (مديرية الأمن الوطني):

تضم وحدة متخصصة في مكافحة الجرائم الإلكترونية، مسؤولية عن تنفيذ أوامر التنصت وجمع الأدلة العلمية، كما تعمل بنسق مباشر مع وكيل جمهورية وقاضي تحقيق.

2-مصلحة مكافحة الجريمة المعلوماتية للدرك الوطني:

تقوم برصد وتتبع المراسلات الإلكترونية المشبوهة بموجب أوامر قضائية، كما تمتلك تقنيات تحليل الاتصالات واعتراض البيانات المشفرة، كما أنها مسؤولة عن تنفيذ عمليات التنصت الإلكتروني في المناطق غير الحضرية، ورصد الشبكات المشبوهة.

[1]- اسمهان بن مالك، مرجع سابق، ص 190.

3-المديرية العامة للأمن الداخلي والمديرية العامة للأمن الخارجي:

تنفذ عمليات التنصت في إطار الأمن القومي، خاصة في قضايا الإرهاب والتجسس الإلكتروني.

كما توجد جهات تقنية متخصصة ومتعاونة مع الجهات الأمنية وتتمثل في:

ثانيا: المؤسسات الخاصة

1-الوكالة الوطنية للأمن السبراني

حيث تقدم الدعم الفني للجهات القضائية والأمنية وتحلل البيانات الرقمية المجمعة عبر التنصت الإلكتروني.

2-شركات الاتصالات ومزودو خدمة الأنترنت:

يلتزمون قانونيا بالتعاون مع الجهات القضائية والأمنية لتوفير البيانات المطلوبة في إطار أوامر التنصت الإلكتروني.[1]

المطلب الثالث

حالات وضوابط اللجوء إلى التنصت الإلكتروني

لقد حصر المشرع الجزائري نطاق تطبيق إجراءات التنصت في جرائم معينة، فقد ورد ذكرها في أحكام المادة 65 مكرر 05 من قانون الإجراءات الجزائية على أنه: "إذا اقتضت ضروريات التحري في الجريمة المتلبس بها، وتحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرام الفساد.

تطرقنا في هذا المطلب إلى فرعين: **(الفرع الأول)** المتمثل في حالات اللجوء إلى التنصت الإلكتروني، أما **(الفرع الثاني)** تناولنا ضوابط اللجوء إلى التنصت الإلكتروني.

[1]- القانون 04/09، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، المرجع السابق.

الفرع الأول: حالات اللجوء إلى التنصت الإلكتروني

أولا: جريمة المخدرات

إذ من الأسباب الدافعة بالمشرع إلى أخذ بجريمة المخدرات ضمن الجرائم المحصورة في أحكام المادة 65 مكرر 05 أن المخدرات أصبحت آفة العصر، إذ بدأت تتسع يوما بعد يوم ولم تقتصر على مجتمع دون آخر، ولذا كان اللازم على الجزائر أن تتخذ مجموعة من الإجراءات سواء وقائية أو عقابية للتصدي لهذه الظاهرة الخطيرة، حيث آخر قانون جاء للمكافحة والوقاية من المخدرات هو القانون رقم 18/04 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشرعين، حيث جاءت فيه نصوص تلزم الشخص المدمن أو المتعاطي للمخدرات اللجوء إلى المعالجة الطبية والتي تكون تحت المراقبة الطبية والمراقبة القضائية.

ونظرا للخطورة التي يشكلها هذا النوع من الجرائم وضع المشرع وسيلة أخرى أكثر حماية ووقاية فجعلها من الجرائم السبعة، أي يخضع فيها المشتبه للمراقبة الهاتفية ضمن إجراءات خاصة.[1]

ثانيا: الجريمة المنظمة العابرة للحدود الوطنية

هي جماعة ذات هيكل تنظيمي مؤلفة من ثلاث أشخاص فأكثر موجودة لفترة من الزمن وتعمل بصورة متظافرة بهدف ارتكاب واحدة أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة من أجل الحصول بشكل مباشر أو غير مباشر على منفعة مالية أو المادية، ومن الأسباب التي دفعت المشرع إلى حصر هذا النوع من الجرائم في أحكام المادة 65 مكرر 05 من قانون 06-22 المتعلق باعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور أنها أصبحت خطرا كبيرا يواجه الدول كافة، ومن بين صورها الاتجار بالأسلحة والبشر وغسيل الأموال...إلخ.

[1]- نصر الدين ماروك، **جريمة المخدرات في ضوء القوانين والاتفاقيات الدولية**، ط1، دار هومة، الجزائر، 2007، ص 181.

ونظرا لخطورة هذا النوع من الجرائم كفل المشرع قانونا من شأنه الحد من تفاقم هذه الظاهرة الاجرامية حق وإن كان فيه اعتداء على الحقوق الفردية، إذ أن الضرورة سمحت بذلك من خلال القانون 06-22 السابق الذكر.

كما وضع المشرع في قانون العقوبات أحكام عقابية من شأنها ردع وعقاب كل من يرتكب، مثل هذا النوع من الجرائم وجعل عقوبة المساهم والمحرض نفس عقوبة الفاعل الأصلي، وهذا يدل على خطورة هذا النوع من الجرائم على الحقوق والحريات.[1]

ثالثا: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

يعتبر اختراق جهاز الحاسوب إحدى قفزات التي تحققت في القرن العشرين، وأي ينظر إليها باعتبارها إحدى عجائب العصر، إذ بات من ضروريات الأساسية في كل شؤون الخاصة والعامة للإنسان، خاصة الدولة ومؤسساتها من خلال ما تتضمنه من أسرار حول نظامها ومشاريعها، ونفس الشيء بالنسبة للإنسان، حيث لم يسلم هو الآخر من الانتهاك والاعتداء عليه ومعرفة أسراره، حيث تشير الاحصائيات إلى وقوع ما بين 200 إلى 250 اعتداء يوميا على الأنظمة المعلوماتية في الجزائر.

ولأجل مكافحة هذا النوع من الجرائم وضع المشرع الآليات وتدابير للحد من هذه الظاهرة، وهذا من خلال أحكام المادة 394 مكرر 1 من قانون العقوبات، حيث مجرد دخول أو البقاء عن طريق الغش في كل بعض المنظومة المعلوماتية فهو معاقب عليه.[2]

رابعا: جرائم تبييض الأموال

أفرد المشرع جرائم تبييض الأموال بقانون خاص وهو قانون رقم 05-01 وهذا لما تشكل من خطورته على المال العام والحياة الاقتصادية خاصة والاجتماعية عامة، إذ لم يكتفي المشرع بوضع قانون خاص بها وإنما زادها تنظيما وحيطة، إذ جعلها من الجرائم المحصورة في نص أحكام المادة 65 مكرر 05 من قانون إجراءات جزائية السابقة الذكر.

---

[1]- محمد علي سويلم، **الأحكام الموضوعية والإجرائية للجريمة المنظمة**، ط1، دار هومة، الإسكندرية، 2007، ص 245.

[2]- عبد الغاني مزياني، **الجرائم الماسة بأنظمة المعالجات الآلية للمعطيات**، جامعة محمد بوضياف، المسيلة، 2007، المتاح على الموقع التالي: www.courdemsila.mjstice.dz/conf.msila/doc10.ppt

إذ بموجب إذن الذي يصدر من وكيل الجمهورية أو قاضي التحقيق المختص يجوز لرجال الشرطة القضائية القيام بإجراءات التنصت على الأشخاص المتهمين بعمليات تبييض الأموال حتى وإن كان فيه مساس لحق من حقوقهم، إلا أنه لا يساوي شيء أمام الهدف المرجو من وراء حماية الأفراد أو المصلحة العامة فالضرورة تبيح المحظور.

خامسا: جرائم الإرهاب

من أجل معرفة سبب جعل المشرع جرائم الإرهاب ضمن جرائم المحصورة في القانون 06-22 المادة 5 مكرر باعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور لابد من تبيان أن مصطلح الإرهاب تشويه الكثير من شبهات والاختلافات الفكرية، حيث خصه المشرع الجزائري بقانون خاص هو قانون رقم 05-01 المتعلق بالوقاية من تبيض الأموال وتمويل الإرهاب ومكافحتها.

حيث جاء في نص المادة 87 مكرر قانون العقوبات تعريف لهذا النوع من الجرائم على أنها... إذ يعتبر فعلا إرهابيا أو تخريب كل فعل يستهدف أمن الدولة والوحدة الوطنية والسلامة الترابية واستقرار المؤسسات وسيرها العادي.

ومن أجل إعطاء فعالية أكبر لحماية الأمن العام والسلامة العامة، فضل المشرع الجزائري الاستمرار في سياسة مكافحة الإرهاب والحد من هذه الظاهرة حتى وإن كان فيها مساس بحق من حقوق الإنسان خاصة حياته الخاصة، غير أن هذا الحق ينتهي عند بداية حقوق لهم وأكبر وهو حق المجتمع في الأمن والأمان.

ثم إدراج هذه الجرائم ضمن الجرائم التي يمكن لوكيل الجمهورية أو قاضي لتحقيق إصدار إذن بالقيام بإجراءات التنصت فيها أغلب التشريعات المقارنة نجدها تتفق في نقطة واحدة، وهي الجرائم الإرهاب لابد أن تكون أولى الجرائم التي يجب أن تخضع لهذه الإجراءات.[1]

[1]- ساسي علي حامد عياد، **استخدام تكنلوجيا المعلومات في مكافحة الإرهاب**، ط1، دار الفكر الجامعي، الإسكندرية، مصر، 2007، ص 223.

سادسا: جرائم الصرف

يحتل المال طبيعة خاصة في الحياة الاقتصادية والاجتماعية والسياسية لجميع الدول ونتيجة لطبيعة الخاصة جعل لها المشرع نظاما قانونيا خاصا ينفرد عن باقي الجرائم خاصة وأنها تمس بعصب الحياة الاقتصادية، حيث كفـل بها المشــرع قانونا خاصا تحت رقم 03-01 المؤرخ في 19 فيفري 2003 المتعلق بقمع مخالفة التشريع والتنظيم الخاصين بالصرف وحركة رؤوس الأموال، كما لم يكتفي المشرع بهذا القانون بل زادها تنظيما وحيطة وهذا لعدم قدرة على السيطرة الكلية لمثل هذا النوع من الجرائم الخطيرة، إذ جعلها من الجرائم سابقة الذكر في المادة 65 مكرر 05 من قانون إجراءات الجزائية، وجعلها ضمن الاستثناءات الذي يجوز فيه الخروج عن القاعدة العامة أي تقضي بحرمة وسرية المكالمات الهاتفية، إذ بموجب الإذن الذي يصدر عن وكيل الجمهورية أو قاضي التحقيق المختص يجوز لرجال الشرطة القضائية ممارسة إجراءات التنصت على الأشخاص المشتبه فيهم بجرائم الصرف.

سابعا: جرائم الفساد

إن جرائم الفساد خطر كبير على استقرار الدول مما جعل المشرع يخصها بالقانون رقم 06-01 المؤرخ في فيفري 2006 المتعلق بالوقاية من الفساد ومكافحته، فمن أهدفه دعم التدابير الرامية إلى الوقاية من الفساد ومكافحة وتعزيز الشفافية والمسؤولية في قطاع العام والخاص، بالإضافة إلى تسهيل دعم التعاون الدولي والمساعدة التقنية من أجل الوقاية من الفساد، بما في ذلك استرداد الموجودات، وهذا ما جعله يصنفها ضمن نطاق جرائم التي تطبق عليها إجراءات التنصت، إذ من شأنها أن تشكل خطرا على المجتمعات وعلى العدالة وسيادة القانون، إذ أصبح الفساد ظاهرة غير وطنية، فالفساد يمس كل القطاعات الحساسة في المجتمع الذي أصبح الحصول فيه على تسهيلات في المعاملات سواء كانت مالية أو إدارية عن طريق دفع رشوة من أجل الإسراع في تمريرها وللفساد عدة صور منها فساد

إداري، فساد قضائي، فساد فكري، فمن أشكاله الوساطة والمحسوبية وكذا الغش الضريبي الذي يضرب باقتصاد الدول، وهذا ما جعل المشرع يعتبرها من الجرائم الخطيرة على الأمن العام والسلامة العامة، خاصة في ظل عدم توفر نظم الرقابة الداخلية الكافية، وكذا عدم وجود فرصة لمشاركة الشعبية، ولذا فضل المشرع حماية المصلحة العامة على المصلحة الخاصة عند تطبيقه لإجراءات التنصت على مثل هذا النوع من الجرائم، لأنه من شأنها المساس بكل الأشخاص سواء كان ذلك على المدى القريب أو البعيد.[1]

بعدما تطرقنا إلى الحالات التي يجب اللجوء إلى التنصت الإلكتروني كآلية لمحاربة هاته الجرائم، إلا أن هاته الآلية تحكمها عدة ضوابط.

الفرع الثاني: ضوابط اللجوء إلى التنصت الإلكتروني

أولا: استصدار الإذن القضائي

ويتم حيث يكون في مضمونه ذكر سبب وهذا ما أكده الدستور الجزائري على شرط التسبيب واعتبره مبدأ دستوريا يجب احترامه من قبل السلطة القضائية المختصة، وذلك بالرجوع إلى أحكام المادة 47 منه، حيث ركز على ضرورة حصول السلطة المختصة بتنفيذ الإجراءات القانونية على ضرورة التقيد بمضمون القانون وعلى تسبيب الأوامر والقرارات وكتابتها، لأنه ليس لأي شخص الحق في استعمال سلطة إصدار مثل هذا النوع من الإجراءات.

ونفس الأمر أكده المشرع الجزائي في أحكام المادة 47 من قانون الإجراءات الجزائية حيث اشترط التسبيب عند الحصول على الأوامر القضائية كالأمر بالتفتيش، إذ يعد هذا الشرط ضمانة أو قيد يجب على الجهة المختصة مراعاتها عند إصدارها للأوامر القضائية الخاصة كالإذن بإجراءات التنصت الالكتروني، فالغرض من شرط التسبيب هو حماية حقوق وحريات الإنسان من التعسف في استعمال هذا الحق.

[1]– أحمد عوض بلال، **قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة**، ط1، دار النهضة العربية، القاهرة، 2005، ص 154.

ثانيا: شروط استصدار الإذن القضائي

1- يجب أن يكون الإذن القضائي محددا من حيث الجرائم وهذا ما نصت عليه أحكام المادة 65 مكرر 05 الفقرة الأولى من قانون الإجراءات الجزائية وهي: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع المتعلق بالصرف وكذا جرائم الفساد".

وهي ضمانة جوهرية يجب على القائم بها احترامها والالتزام بحذافيرها لا يجوز القياس عليها أو الخروج عنها.

2- يجب أن يكون الإذن قضائي محددا من حيث المدة والمقدرة بـ 04 أشهر، وهذا ما جاءت به المادة 65 مكرر 7 من قانون الإجراءات الجزائية، حيث لصحة إجراءات التنصت لابد من التقيد بشرط المدة التي تحددها الجهة المصدرة للإذن بإجراءات التنصت لضباط الشرطة القضائية، حيث إذا وصل هذا الأخير للهدف المنشود من وراء إجراءات التنصت الالكتروني قبل نهاية المدة المحددة قانونا، وجب عليه التوقف عن تأدية هذه الإجراءات، أما إذا انتهت المدة القانونية ولم يصل إلى تحقيق هدفه، فلا يستطيع متابعة عملية التنصت من تلقاء نفسه إلا بعد الحصول على إذن التجديد.[1]

3-يجب أن يكون الإذن قضائي محددا من حيث الأشخاص، فليس كل شخص يعمل لدى سلطة القضائية هو مؤهل للقيام بإجراءات التنصت، بل من تعيينه من قبل وكيل الجمهورية أو قاضي التحقيق المختص، فأعوان الشرطة مثلا مستثنون من

[1]- فوزي عمارة، " **اعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور والتسرب كإجراءات تحقيق القضائي في المواد الجزائية** "، مجلة العلوم الإنسانية، كلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، الجزائر، العدد 33، جوان 2010، ص 242.

هذه المهمة وضباط الشرطة القضائية هم الأشخاص الذي حددتها أحكام المادة 15 من قانون إجراء الجزائية، إذ يجب على هذا أن يباشر نفسه إجراءات التنصت الالكتروني، كما لا يملك سلطة إنابة أعماله إلى غيره إلا في إطار تسخير أعوان مؤهلين، لأن ضباط الشرطة القضائية تنقصهم الخبرة التقنية في هذا المجال.

خلاصة الفصل:

يتضح من خلال هذا الفصل أن التنصت الالكتروني يمثل إحدى أخطر صور الاعتداء على الحياة الخاصة في العصر الرقمي، لما يتميز به من سرية وتعقيد تقنـــي عالٍ، وقد تبين أن المشرع سواء على المستوى الدولي أو الوطني سعى إلى وضع أطر قانونية لتنظيم هذا الاجراء بهدف تحقيق التوازن بين حماية الأمن العام وصون حقوق الأفراد وحرياتهم الأساسية، كما برزت أهمية تحديد الجهات المختصة والحالات التي ينفذ فيها التنصت الالكتروني وفقا لضوابط دقيقة، لضمان عدم تعسف السلطات في استعمال هذه الوسيلة الحساسة.

الفصل الثاني

المخاطر المرتبطة بالتنصت الإلكتروني في الجزائر

الفصل الثاني:

المخاطر المرتبطة بالتنصت الإلكتروني في الجزائر

في ظل التطور التكنولوجي المتسارع وزيادة الاعتماد على الوسائل الرقمية، أصبح التنصت الإلكتروني أحد أبرز التهديدات التي تواجه الأفراد والمؤسسات وحتى الدول.

وفي الجزائر مثلها مثل العديد من الدول، تبرز الحاجة إلى تعزيز آليات الحماية من هذه المخاطر لضمان خصوصية البيانات وسلامة الاتصالات.

وقسمنا فصلنا إلى مبحثين **(المبحث الأول)** آليات التصدي للمخاطر المرتبطة بالتنصت الإلكتروني، أما **(المبحث الثاني)** المخاطر المرتبطة بالتنصت الإلكتروني في الجزائر.

المبحث الأول:

آليات التصدي للمخاطر المرتبطة بالتنصت الإلكتروني

تعتمد آليات الحماية في الجزائر على مجموعة من الإجراءات المتمثلة في استراتيجية الأمن السيبراني، بالإضافة إلى تعزيز الوعي الأمني لدى المستخدمين، كما تشمل استخدام تقنيات وأدوات وقائية لرصد ومنع محاولات التنصت غير المشروع.

في هذه المقدمة، سنستعرض بعض الآليات الأساسية التي يمكن من خلالها الحد من مخاطر التنصت الإلكتروني في الجزائر.

تناولنا في هذا المبحث إلى آليات الحماية من التنصت الإلكتروني **(المطلب الأول)**، أما **(المطلب الثاني)** التقنيات الأدوات الوقائية.

المطلب الأول:

آليات الحماية من التنصت الإلكتروني

في عصر الرقمنة والتكنولوجيا المتقدمة أصبحت الاتصالات الالكترونية من التنصت والاختراق أحد أهم التحديات التي تواجه الأفراد والمؤسسات على حد سواء، ويعد هذا الأخير تهديدا خطيرا يمس الخصوصية ويعرض المعلومات السرية للسرقة أو التلاعب، مما يستدعي تبني آليات حماية فعالة لضمان أمان وسرية البيانات، حيث تناولنا في هذا المطلب فرعيـــن: **(الفرع الأول)** استراتيجيـــة الأمن السيبراني، أما **(الفرع الثاني)** التوعية والتثقيف كآلية حماية من مخاطر التنصت الإلكتروني في الجزائر.

الفرع الأول: استراتيجية الأمن السيبراني

تعد استراتيجية الأمن السيبراني من أهم الآليات الحماية التي تعتمدها الجزائر لحماية فضاءها الرقمي من التهديدات المتعددة، ومن أبرزها التنصت الإلكتروني، الذي يُشكل انتهاكًا خطيرًا لخصوصية الأفراد والمؤسسات، ويهدد الأمن القومي والاقتصادي. وفي هذا

السياق، تبنّت الجزائر استراتيجية وطنية شاملة للأمن السيبراني، تهدف إلى التصدي لمثل هذه التهديدات.

أولا: تعريف الأمن السيبراني[1]

ما تضمنه الفضاء السيبراني من عمليات الدخول والخروج، لمختلف مواقع تداول وتخزين المعلومات والبيانات، يستوجب بالضرورة خلق قواعد وأليات تثبيت أصول الأمن لحماية هذه المواقع وأنظمتها المعلوماتية، لذا يتبادر لذهان كل ممتهن أو مستخدم لهذا الفضاء طرح السؤال التالي: ما هو الأمن السيبراني؟

مختلف الإجابات الواردة من الدوائر الفكرية أو الرسمية، لم تنجح في وضع تعريف دقيق لهذا المصطلح، ومازالت هذه الاشكالية مطروحة بحدة لحد الآن، وهذا بدوره طرح إشكالا آخر يتمثل في عدم نجاعة اليات مواجهة الجرائم السيبرانية وعدم فعالية التعاون الخارجي بالتالي ضمان الأمن.

من خلال التعاريف التي سأذكرها على سبيل المثال، سيتضح للقارئ أن هناك اختلافا في الطرح، بين من يعتمد على الخبرة التقنية والميدانية لتفسير الظاهرة (الباحثون)، وبين من يركز على الجوانب التنظيمية والقانونية) الدوائر الحكومية للأمن السيبراني.

بالنسبة للاكاديميين، يعرف كل من Martti Lehto,Pekka Neittaanmäki على أنه مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها ويتضمن تنفيذ التدابير المضادة المطلوبة أما أستاذ الاتصالات في جامعة كاليفورنيا ريتشارد كمرر Richard.

فيعتبر الأمن السيبراني "مجموعة وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة"، وقد أيده في الطرح واحد من أهم المختصين في الميدان؛ الأستاذ

[1]– جمال بوازدية، " **الاستراتيجية الجزائرية في مواجهة الجرائة السيبرانية** "، التحديات والآفاق المستقبلية، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، ص 1262–1264، أفريل2019،

إدوارد أموروزو،Edward Amoroso الذي عرفه" بأنه تلك الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفـــرة... إلخ.

في الأخير نذكر التعريف الذي جاء به الاتحاد الدولي للاتصالات الصادر في تقريره حول" اتجاهات الاصلاح في الاتصالات للعام2011-2010، والذي يعتبر بمثابة أرضية إجماع لمختلف التوجهات الفكرية والمهنية "هو مجموعة من المهمات، مثـــل تجميع وســائل، وسياسات، واجراءات أمنيـــة، ومبـــادئ توجيهيـــة، ومقـــاربات لإدارة المخـــاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".

من هذا المنطلق، يمكننا إعطاء تعريف شامل بالقول" أن الأمن السيبراني أو الالكتروني هو مجمل القوانين، الأدوات، النصوص، المفاهيم والميكانيزمات المبنية وطرق تسيير الأخطار والممارسات التقنية المتعلقة بتكنولوجيات المعلومات والاتصالات المستخدمة لحماية مصالح الدول والأشخاص .ليبقى الهدف في الأخير، هو قدرة هذه الأدوات على مقاومة التهديدات المتعمدة من طرف قراصنة المعلومات أو غير المعتمدة من طرف المستخدمين الخطأ البشري للتعافي، وبالتالي التحرر من الأضرار الناجمة عن تعطيل أو سوء استخدام تكنولوجيا المعلومات والاتصالات.[1]

ثانيا: التعريف الإجرائي

يُقصد بالأمن السيبراني حماية الأنظمة والشبكات والبرمجيات والمعلومات من الهجمات الرقمية التي تستهدف الوصول غير المشروع إلى البيانات أو التجسس عليها أو تعديلها أو إتلافها، ويعتبر التنصت الإلكتروني أحد هذه الهجمات، حيث يتم من خلاله التقاط الاتصالات الخاصة أو رصد البيانات الحساسة.

[1]– جمال بوازدية، المرجع السابق، ص 1266.

الأمن السيبراني يعمل على تقوية "جدار الحماية الرقمي" للأجهزة والشبكات، وبالتالي يمنع عمليات التنصت أو يقلل من فاعليتها، عن طريق:

- التشفير القوي للاتصالات.
- استخدام أنظمة كشف التسلل.
- تحديثات أمنية مستمرة.
- مراقبة الأنشطة الشبكية بشكل ذكي.

ثالثا: استراتيجية الجزائر الوطنية للأمن السيبراني

اعتمدت الجزائر عدة خطـــوات لتأطيـــر الأمـن السيبراني ضمن استراتيجيـــة وطنية، خاصة بعد التطور الكبير في الهجمات السيبرانية. ويمكن تلخيص ملامح هذه الاستراتيجية كالتالي:

1-الإطار القانوني والتنظيمي:

تمتلك الجزائر إطارا قانونيا يهدف إلى تعزيز أمنها السيبراني بصفة عامة للحماية من التنصت الإلكتروني بصفة خاصة ويتجلى ذلك في:

-**الاتفاقيات الدولية:** والمتمثلة في:

- الاتفاقية الدولية المبرمة في عاصمة المجر بودابيست بتاريخ 23-11-2001 المتضمنة الجرائم السيبرانية وتعتبر هذه الاتفاقية بمثابة المرجعية القانونية لكل التشريعات الدولية الصادرة في هذا المجال، ومن بين حيث كانت التشريعات الداخلية مطابقة لما جاء في هاته الاتفاقية والنقاط التي شملتها المطابقة:
- استعمال المصطلحات المعمول بها في مجال الاعلام الالي وتكنولوجيات الاتصال، معطيات الاعلام، معطيات متعلقة بالاختراق، ممول الخدمات، (حسب المادة الأولـى من الاتفاقيـة ومقدمة القانون 09-04[1] الجزائري)، ليبقـــى

[1]- قانون 09-04، المتعلق بالوقاية من جرائم المتصلة بتكنولوجيات الإعلام والاتصال، المرجع السابق.

الهــدف، تسهيل عمل المختصين في الاعلام الالي من قراءة صحيحة للعمل المطلوب أو الملف المطروح.

- الدخول الغير شرعي للأنظمة المعلوماتية، (حسب المادة الثانية من الاتفاقية والمادة 394 مكرر قانون العقوبات الجزائري)، أهمية تجريم هذا العمل هو تحديد نقاط الضعف للنظام المستهدف مع إمكانية تحديد هوية الجاني.
- الاعتراض الغير شرعي للمكالمات والمعطيات المتبادلة سواء في إطار خاص أو مهني (حسب المادة الثالثة من الاتفاقية والمادة 303[1] من قانون العقوبات الجزائري).

المساس بنزاهة أو استماتة المعطيات (حسب المادة الرابعة من الاتفاقية والمادة 394 مكرر قانون العقوبات الجزائري)، لأن الحصول على المعطيات بطريقة غير شرعية من شأنه أن يحول من مسار المعلومة في جانبها المهنـــي أو الشخصـــي، وهذه الخطوة من أخطر التهديدات الإلكترونية.

- المسؤولية المعنوية للجهات المكلفة بتسيير مجالات تكنولوجيا الإعلام تبقـى قائمة، لأنهم في نظر القانون الضامن الوحيد على حسن وسلامة الأنظمة المعلوماتيـة (حسب المادة 12[2] من الاتفاقيـة والمادة 394 مكرر قـانون العقوبات الجزائري).
- التعاون الدولي من اجل سلامة الاجراءات القانونية (الإنابة القضائية، تسليم المجرمين) وهي من أهم العناصر التي ركزت عليها الاتفاقية في الباب الثالث المادة 65[3] مكرر 5 من قانون الاجـراءات الجزائيـة والمـادة 15 من القانـون 09-04 لن هذه الخطوة تبقى السبيل المثل بالنسبة للخبراء للحد من الجريمة

[1]- المادة 303، من قانون العقوبات، المرجع السابق.

[2]- المادة 12 من الاتفاقية للإعلام العالمي لحقوق الإنسان، المرجع السابق.

[3]- المادة 65 مكرر 5، من قانون الاجراءات الجزائية، المرجع السابق.

الالكترونية وبالأحرى جريمة التنصت الإلكتروني كما تشكل عائق لحسن سير المتابعة القضائية إذا كانت طلبات الإنابة أو التسليم تمس بسيادة الدولة.

- القوانين الوطنية المنظمة للتنصت الإلكتروني

- القانون رقم 09-04 المؤرخ في 5 أغسطس 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته حيث نص هذا القانون في مواده الأولى على أن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال تشمل: اعتراض الاتصالات أو نقل بيانات بصفة غير مشروعة واستعمال وسائل تقنية للاعتداء على سرية أو سلامة البيانات.[1]
- القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي يهدف هذا القانون إلى حماية الخصوصية الرقمية، ويمنع بشكل صريح جمع البيانات أو اعتراضها بدون ترخيص قانوني وبتحليل هذا القانون نجده أنه يجرم التنصت غير المشروع على البيانات الرقمية.[2]
- القانون رقم 66-22 المتعلق بالإجراءات الجزائية لاسيما المادة 65 مكرر 05 التي نصت على حماية الحق في الخصوصية ومقتضيات مكافحة الجرائم الخطيرة.[3]

2-الهيئات الوطنية المكلفة بالأمن السيبراني:

الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

التي أنشئت سنة 2009 ووضعت تحت السلطة المباشرة لوزير العدل حافظ الاختام ولم تدخل حيز التنفيذ إلا بعد صدور المرسوم الرئاسي رقم 15-261 المؤرخ في:2015/10/08 ومن أبرز المهام المنوطة بها:

[1]- قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المرجع السابق.

[2]- قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، العدد 34، ص 11.

[3]- قانون رقم 66-22 المؤرخ في 20-12-2006 المتضمن قانون إجراءات الجزائية، المرجع السابق.

- استغلال المعطيات المتوفرة بطريقة تسمح بمتابعة كل ما يجري في الفضاء السيبراني غير شرعية وبالتالي توجيه القدرات البشريــة والماليــة للحـد من الثغرات، مع العلم ان هذا المجال أصبح مفتوحا على كل الاحتمالات في ظل التطور السريع لتكنولوجيا الاعلام والاتصال.

3-مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية:

وهي هيئة تابعة للقيادة العامة للدرك الوطني، لا تختلف كثيرا في مهام التحقيق والتحريات في هذا المجال عن نظيرتها التابعة للأمن الوطني سواء محليا أو وطنيا، بل بالعكس يتم التنسيق بينهما تحت المسؤولية المباشرة للنائب العام على مستوى دائرة الاختصاص.[1]

الفرع الثاني: التوعية والتثقيف كآلية حماية من مخاطر التنصت الإلكتروني في الجزائر

في ظل التوسع المتزايد لاستخدام تكنولوجيا المعلومات والاتصال، أصبح الفرد الجزائري أكثر عرضة للتهديدات الرقمية، وعلى رأسها التنصت الإلكتروني، الذي يستهدف الخصوصية الفردية والأمن المؤسسي على حد سواء. وأمام محدودية التدخل القانوني أو التقني في كثير من الأحيان، تبرز التوعية والتثقيف كوسيلة وقائية أساسية، تمكّن الأفراد والمؤسسات من فهم طبيعة المخاطر الرقمية وتبنّي سلوك رقمي آمن يحصّنهم من الوقوع ضحية لمثل هذه الاعتداءات.

أولا: مفهوم التوعية والتثقيف السيبراني

يقصد بالتوعية السيبرانية تلك الجهود التعليمية والمعلوماتية التي تهدف إلى رفع مستوى الوعي الرقمي لدى مستخدمي الوسائط الإلكترونية، من خلال تعريفهم بمخاطر الفضاء السيبراني، وأساليب الوقاية منها، وأهم الإجراءات التقنية والسلوكية الواجب اتباعها.

[1]- جمال بوازدية، المرجع السابق، ص 1280-1281.

أما التثقيف السيبراني، فيتجاوز البعد التوعوي ليشمل تعليمًا منهجيًا ومؤسساتيًا في مجالات أمن المعلومات، حماية البيانات الشخصية، واستخدام التقنيات الحديثة بأمان.

ثانيا: أهمية التوعية والتثقيف

1-رفع الوعي المجتمعي: يساهم التثقيف الرقمي في تعريف الأفراد بمخاطر التنصت الإلكتروني، مثل سرقة المعلومات الشخصية أو التنصت على المحادثات الخاصة.

2-تعزيز السلوك الرقمي الآمن: من خلال حملات التوعية، يتم إرشاد المستخدمين إلى ضرورة استخدام وسائل الحماية مثل التشفير، وتجنب الاتصال عبر شبكات غير آمنة.

3-تقوية المناعة المعلوماتية: تعني تمكين الأفراد من التحقق من مصادر التطبيقات والروابط المشبوهة، والوعي بالممارسات التي قد تجعلهم عرضة للتجسس أو الاختراق.

ثالثا: دور التوعية والتثقيف في الوقاية من التنصت الإلكتروني

1- تعريف الأفراد بأساليب التنصت الشائعة:

كثير من المستخدمين لا يدركون الطرق التي يُمكن أن يُستهدفوا بها، مثل:

- اختراق التطبيقات مثل واتساب أو تيليغرام.
- إرسال روابط تجسس عبر البريد أو وسائل التواصل.
- تسجيل المكالمات دون علم الطرف الآخر.
- استخدام الميكروفون أو الكاميرا من خلال برمجيات خبيثة.

2- نشر ثقافة الأمن المعلوماتي:

تقوم المؤسسات المختصـــة مثل CERT-ALGÉRIE بتنظيــم دورات وورشــات تهدف إلى:

- تعليم الأفراد كيفية حماية أجهزتهم.
- اعتماد التشفير في المحادثات.
- تجنّب شبكات الواي فاي العامة غير الآمنة.
- تغيير كلمات السر بشكل دوري واستخدام برامج الحماية.[1]

[1]- الدليل العملي لحماية المستخدم من التهديدات الإلكترونية، المركز الوطني للوقاية من الجرائم المعلوماتية، الجزائر، 2021.

رابعا: مظاهر التوعية في الجزائر

1-برامج التثقيف الإلكتروني في المدارس والجامعات: تسعى بعض المؤسسات التعليمية إلى إدراج مفاهيم الأمن السيبراني ضمن البرامج التكوينية.

2-المبادرات الحكومية والمؤسساتية: مثل حملات التوعية التي تطلقها الهيئات الأمنية أو وزارة الرقمنة أو سلطة ضبط البريد والاتصالات الإلكترونية.

3-دور الإعلام والمجتمع المدني: من خلال نشر ثقافة الحذر الرقمي عبر القنوات التلفزيونية، ومنصات التواصل الاجتماعي، والندوات التوعوية.

خامسا: جهود الجزائر في التوعية من التنصت الإلكتروني

1-مراكز التكوين والإعلام السيبراني

- مركز البحث في الإعلام العلمي والتقني (**CERIST**) ينشر بانتظام نشرات تحذيرية وتوصيات أمنية موجهة لمختلف شرائح المجتمع.[1]
- **CERT-ALGÉRIE** تُصدر تقارير دورية حول التهديدات الرقمية الشائعة في الجزائر، وتقدم نصائح موجهة للمستخدمين حول كيفية حماية بياناتهم من التجسس أو التنصت.

2-إدراج الأمن السيبراني في المناهج التعليمية:

تم إدراج وحدات دراسية في بعض الجامعات الجزائرية، لا سيما في تخصصات الإعلام الآلي والحقوق، حول أمن المعلومات وحماية الخصوصية، مما يُساهم في خلق وعي أكاديمي حول مخاطر التنصت وسبل الوقاية منه.

3-حملات التوعية الوطنية:

أطلقت وزارة البريد والمواصلات حملات توعية عبر وسائل الإعلام ومواقع التواصل الاجتماعي، خاصة خـــلال المناسبـــات العالمية مثـــل "اليوم العالمي لأمـــن المعلومات" للتعريف بمخاطر الاختراق والتنصت الإلكتروني، وتوجيه نصائح عملية للوقاية منه.[2]

[1]- نشرة أمنية حول التنصت الرقمي والتجسس السيبيراني (CERIST)، مركز البحث بالإعلام العلمي والتقني، الجزائر، 2022.

[2]- المرجع نفسه.

سادسا: تحديات تطبيق التوعية في الجزائر

- ضعف الثقافة الرقمية لدى فئات واسعة من المجتمع، خاصة في المناطق الريفية أو النائية.
- نقص المحتوى التوعوي الموجّه باللغة العربية أو الأمازيغية، مما يصعب الوصول إلى جميع شرائح المجتمع.
- قلة التكوين المتخصص للمؤطرين في المجال الرقمي والأمني.

سابعا: مقترحات لتعزيز التوعية

- إطلاق حملات وطنية دورية موجهة لكل فئات المجتمع.
- إدراج التثقيف الرقمي ضمن المناهج الدراسية بمختلف الأطوار التعليمية.
- تعزيز الشراكة بين الدولة والمجتمع المدني والمؤسسات الإعلامية لنشر الوعي الجماعي حول مخاطر التنصت.
- ركز البحث في الإعلام العلمي والتقني**(CERIST)** ، نشرة أمنية حول التنصت الرقمي والتجسس السيبراني، الجزائر،2022.01 .

المطلب الثاني:

التقنيات والأدوات الوقائية

تقنية مكافحة التنصت هي عملية الكشف عن معدات التنصت وتحديد موقعها والقضاء عليها في البيئة المستهدفة والتي قد يتم التنصت عليها بوسائل تقنية. ومبدأها الأساسي هو استخدام أجهزة الاستشعار المتقدمة وتكنولوجيا معالجة الإشارات وطريقة تحليل البيانات لتحقيق التعرف الفعال على معدات التنصت والوقاية منها.

على وجه التحديد، تستخدم أجهزة مكافحة التنصت أولاً مجموعة متنوعة من أجهزة الاستشعار، مثل أجهزة الاستشعار الصوتية وأجهزة استشعار التردد اللاسلكي وأجهزة استشعار الاهتزاز، لالتقاط الإشارات من أجهزة التنصت التي قد تكون في الهواء أو في الجدران أو في الأجهزة القريبة. بعد ذلك، تُستخدم تكنولوجيا معالجة الإشارات المتقدمة

وخوارزمية البرامج لفك تشفير الإشارة الملتقطة وتحليلها، ويتم استخراج المعلومات المميزة للإشارة، مثل التردد والسعة والشكل الموجي. من خلال مقارنة خصائص أجهزة التنصت المعروفة، يمكن لأجهزة مكافحة التنصت تحديد أنواع مختلفة من أجهزة التنصت وتحديد وجودها وموقعه.

تطرقنا في هذا المطلب إلى فرعين **(الفرع الأول)** التقنيات الوقائية، أما **(الفرع الثاني)** الأدوات الوقائية.

الفرع الأول: التقنيات الوقائية

تقنيات الوقائية من التنصت الإلكتروني تعد من أهم الوسائل التي يعتمد عليها الأفراد والمؤسسات لحماية خصوصياتهم وبياناتهم من التطفل أو الاستغلال غير المشروع، خاصة في ظل التطور السريع لوسائل الاتصال والتكنولوجيا الرقمية. وفي السياق الجزائري، وعلى الرغم من التحديات، فقد بدأت بعض الجهود تتبلور لتعزيز هذه الوقاية، سواء على مستوى التشريعات أو من خلال الاعتماد على الحلول التقنية.

للحد من مخاطر التنصت، يتم استخدام مجموعة من الحلول والتقنيات المضادة، منها:

أولا: التشفير كوسيلة وقائية أساسية

التشفير هو إحدى أهم الأدوات التقنية لمنع التنصت على الاتصالات والمراسلات. وتتمثل آليته في تحويل المعلومات إلى صيغة غير مفهومة إلا للطرف المرسل والمستقبل.

1-التشفير في الاتصالات: تعتمد بعض التطبيقات الحديثة التي يستخدمها الجزائريون، مثل "واتساب" و"سيغنال"، على تقنيات تشفير "من الطرف إلى الطرف-End) " to-End Encryption) والتي تمنع حتى الشركة المطورة نفسها من الوصول إلى محتوى الرسائل.

-**تشفير البريد الإلكتروني:** برامج مثل "ProtonMail" و "PGP" تتيح للمستخدم تشفير الرسائل قبل إرسالها، مما يجعلها غير قابلة للقراءة من قبل أي جهة تتجسس على القناة الناقلة.

2-التشفير على مستوى الأجهزة: أنظمة التشغيل الحديثة توفر إمكانية تشفير الملفات والمجلدات الحساسة، مما يحميها في حالة اختراق الجهاز أو فقدانه[1].

ثانيا: استخدام الشبكات الافتراضية الخاصة(VPN)

تتيح شبكات الـ **VPN** للمستخدم الاتصال بالإنترنت عبر قناة مشفرة تمر عبر خادم وسيط، مما يصعب على المتنصتين تعقب النشاطات أو تحديد الهوية الحقيقية للمستخدم في الجزائر، باتت بعض المؤسسات الكبرى تعتمد على **VPN** لتأمين اتصالات موظفيها خاصة في ظل الانتقال نحو الخدمات الرقمية والعمل عن بعد.

رغم أن بعض خدمات الـ VPN قد تُحجب أحيانًا، إلا أن الخيارات المتاحة عبر أدوات مفتوحة المصدر أو الشبكات المشفرة) مثل Tor ما زالت متاحة وتستخدم على نطاق محدود.

ثالثا: جدران الحماية وبرمجيات مكافحة الاختراق

1-الجدران النارية (Firewalls): وهي أنظمة تقوم بمراقبة البيانات الداخلة والخارجة إلى الشبكة، وتمنع الاتصال غير المصرح به، وتُعد من وسائل الوقاية المهمة خاصة للمؤسسات.

2-مكافحة الفيروسات والتجسس :استخدام برامج موثوقة لتأمين الأجهزة ضد البرمجيات الخبيثة التي قد تُستخدم كوسيط للتنصت، مثل برامج تسجيل ضربات لوحة المفاتيح أو اختراق الكاميرات والميكروفونات.

رابعا: التحكم في الأذونات والتحديثات الدورية

- غالبًا ما تعتمد برمجيات التنصت على ثغرات في التطبيقات أو الأنظمة، لذا يُعد تحديث الأنظمة والتطبيقات بشكل دوري أحد أساليب الوقاية المهمة.

[1]- الموقع الإلكتروني: https://itach.dk/index.php/2024/09/07/sp-i-information/ ، تم الإطلاع عليه بتاريخ: 05 مارس 2025، على الساعة 23:05.

- التحكم في أذونات التطبيقات على الهواتف الذكية (مثل الوصول إلى الميكروفون أو الكاميرا) يساعد في تقليل فرص التجسس غير المشروع.

خامسا: التوعية والتدريب التقني

- التقنية وحدها لا تكفي، إذ أن ضعف الوعي بمخاطر التنصت يجعل الأفراد أكثر عرضة له، لذا بدأت بعض الهيئات في الجزائر) مثل CERT الجزائر (بتنظيم حملات توعية حول الأمن السيبراني).
- التكوين في الأمن الرقمي داخل المؤسسات صار أمرًا ضروريًا، خاصة في القطاعات الحساسة مثل البنوك، الصحة، والعدل[1].

سادسا: اعتماد برامج مفتوحة المصدر

في ظل الشكوك حول برمجيات الشركات التجارية، يُنصح باستخدام أنظمة مفتوحة المصدر التي يمكن تدقيق شيفرتها، مثل نظام التشغيل " لينكس" أو متصفحات "تور"، والتي تعطي درجة أعلى من التحكم والخصوصية.

سابعا: الأمن السيبراني

من خلال تعزيز استراتيجيات الأمن السيبراني مثل استخدام جدران الحماية وأنظمة الكشف عن التسلل، يمكن حماية البيانات الحساسة من الوصول غير المصرح به.

ثامنا: استخدام أجهزة الاتصال الآمنة

يمكن الاعتماد على أجهزة مشفـــرة ومتطورة للتـــواصل الآمن بين الجهـــات الحساسة، مثل الدبلوماسيين أو العسكريين

تاسعا: الحماية

يمكن منع مخاطر التنصت عبر إشعاع الكمبيوتر عن طريق تثبيت تدابير أمنية ودرع. على سبيل المثال، تمكّن أجهزة الكمبيوتر المحمية بواسطة TEMPEST المؤسسات من منع الإشعاع غير المقصود والحفـــاظ على أمان بياناتهـــا ومستخدميها، حيث أن

[1]– الموقع الإلكتروني، المرجع السابق.

أجهزة الكمبيوتر تصدر إشعاعات كهرومغناطيسية يمكن أن يستخدمها المتصنتون المتطورون (sophisticated eavesdroppers) لإعادة بناء محتويات شاشة الكمبيوتر، ويمكن حمل هذه الإشارات حتى بضع مئات من الأقدام وتمديدها أكثر من خلال الكابلات وخطوط الهاتف، والتي يمكن استخدامها كهوائيات.

عاشرا: شبكة الرصد

وتقوم هذه الشبكة بمراقبة فرق الأمن الشبكات باستمرار بحثًا عن أي نشاط غير طبيعي باستخدام أنظمة كشف التسلل أو برامج الكشف عن نقاط النهاية والاستجابة لها، حيث يجب على فرق الأمن أيضًا استخدام نفس برامج الشم التي يستخدمها الفاعلون الشائنون لاكتشاف نقاط الضعف على الشبكة.[1]

الفرع الثاني: أدوات الوقائية

أضحى التنصت الإلكتروني من أخطر صور الاعتداء على الحياة الخاصة، لا سيما في ظل تطور الوسائل التكنولوجية، ما استدعى البحث عن سبل فعالة للوقاية من هذه الجريمة، ومن أبرز هذه السبل اعتماد أجهزة وأدوات وقائية تهدف إلى الحد من إمكانية التجسس والتنصت على الأفراد أو المؤسسات. وفي الجزائر، بدأت تظهر بوادر الاهتمام بهذه الوسائل رغم التحديات التقنية والقانونية.

أولا: تعريف الأجهزة الوقائية من التنصت الإلكتروني

تُعرف الأجهزة الوقائية من التنصت بأنها تلك الأدوات أو البرمجيات أو المعدات الإلكترونية المصممة خصيصًا لرصد ومنع أو إعاقة محاولات التنصت على البيانات الصوتية أو الرقمية، سواء عبر الهواتف أو الشبكات أو غيرها من وسائل الاتصال الحديثة.

[1]– الموقع الإلكتروني: https://www.fortinet.com، تم الاطلاع عليه بتاريخ: 07 أفريل 2025، على الساعة 10:00.

ثانيا: أبرز أنواع الأجهزة والأدوات الوقائية[1]

1-أجهزة كشف التنصت(Bug Detectors)

تُستخدم هذه الأجهزة لرصد إشارات التنصت أو التجسس، مثل الميكروفونات المخفية أو كاميرات المراقبة السرية أو أجهزة إرسال الراديو. وتعتمد في عملها على تقنيات تحليل الطيف الترددي واكتشاف النشاطات المشبوهة.

تستخدم هذه الأجهزة في المؤسسات الحكومية، الفنادق، القاعات الحساسة، وأحيانًا في المنازل الخاصة.

من أشهر أنواعها عالميًاRF Detector ، Spectrum Analyzer.

2- الهواتف المشفرة:

وهي أجهزة هاتفية مزودة بتقنيات تشفير للمكالمات والرسائل النصية، مثل استخدام بروتوكولات PGP أوZRTP ، بما يمنع التنصت على الاتصال أو فك تشفيره.

بعض المؤسسات الجزائرية أصبحت تعتمد هذه التقنية خاصة في القطاعات الأمنية والدبلوماسية.

3- أدوات تشويش الإشارة (Signal Jammers)

يتم استخدامها لتعطيل الاتصالات اللاسلكية في منطقة معينة لمنع التنصت أو تسريب المعلومات، خاصة أثناء الاجتماعات الأمنية أو المؤتمرات الحساسة. ولكن استخدامها محكوم بشروط قانونية صارمة لعدم التأثير على السلامة العامة.

4- برامج مكافحة التجسس(Anti-Spyware Software)

وهي برمجيات تُثبت على الأجهزة الذكية أو الحواسيب لاكتشاف وإزالة البرامج الخبيثة المستخدمة للتنصت أو تسجيل النشاطات.

من أبرزهاMalwarebytes، Spybot Search & Destroy، وتُستخدم على نطاق واسع في الجزائر في المؤسسات.

[1] – منصور، رضا، " **وسائل الحماية التقنية من جرائم المعلوماتية** "، مجلة الفكر القانوني، جامعة الجزائر 1، العدد 22، 2021، ص 45.

5- أنظمة الحماية المتقدمة للشبكات(Firewall & IDS/IPS)

تلعب جدران الحماية وأنظمة كشف التسلل دورًا أساسيًا في الحماية من التنصت الذي يتم عبر الشبكات، حيث تقوم برصد الأنشطة غير المصرح بها ومنعها.

ثالثا: بعض أنواع أجهزة التنصت

بعد ما تطرقنا الى إبراز أنواع أدوات الوقائية من التنصت الإلكتروني ارتأينا أن نستعرض بعض أنواع أجهزة التنصت حيث تتنوع هاته الأخيرة فيما بينها، حيث يمكن أن تكون بسيطةً أو معقدةً، مكلفةً للغاية أو غير مكلفةٍ، وبالتأكيد يعتمد ذلك على الهدف من شرائها، فبعض المهن القانونية تتطلب أجهزة تنصت معقدةً نوعًا ما.[1]

تتطور أجهزة التنصت مع تطور التكنولوجيا، ونلاحظ أنه كلما تطورت أكثر يصغر حجمها أكثر. يمكن للعديد من أجهزة التنصت التقاط الصوت أو الفيديو أو البيانات عن بُعد، كما يُمكن استخدام جهاز الكمبيوتر أو الهاتف المحمول كجهاز تنصتٍ، سنذكر لكم بعض أهم أنواع أجهزة التنصت أدناه.

1-كاميرا التجسس: يستخدم هذا النوع من أجهزة التنصت كاميرا صغيرة لالتقاط مقطع فيديو سرًّا، ولصغر حجمها يُمكن إخفاؤها في أيّ مكانٍ كالقلم، أو الساعة، أو حيوان محشو وغيره.

2-مسجل الصوت: يستخدم هذا النوع ميكروفون صغير لنقل ترددات الصوت، ويتطلب البعض منها أن يكون الشخص قريبًا للتمكن من سماع الترددات، أو قد يستخدم مسجلات صوتٍ تعمل عن بعدٍ.

3- أجهزة التنصت الخلوية GSM: تستخدم بطاقة SIM للتجسس على الأصوات، وتعمل من خلال شبكة لاسلكية G3 أو G4، ولذلك تدعى أحيانا باسم أجهزة التنصت اللاسلكية، بحيث يمكن استخدامها في أي مكان يتيح الوصول لشبكتها الخلوية.

[1]- https://tech.mawdoo3.com/ الموقع الإلكتروني تاريخ الاطلاع 16-04-2025 الساعة 14:20

وهناك العديد من الأنواع الأخرى كأجهزة التنصت الليزرية، وأجهزة التنصت عبر الجدران وغيرها.[1]

رابعا: واقع استخدام الأجهزة الوقائية في الجزائر[2]

رغم وجود هذه الأدوات عالميًا، فإن استخدامها في الجـــزائر ما يـــزال محـــدودًا نسبيًا، ويواجه عدة تحديات، منها:

- نقص التكوين في الأمن السيبراني؛
- كلفة بعض الأجهزة المرتفعة؛
- غياب إطار قانوني دقيق ينظم استخدام أدوات مثل أدوات التشويش أو الأجهزة المتخصصة في الكشف؛
- الاعتماد الكبير على الحلول المستوردة دون وجود صناعة محلية للأجهزة الأمنية الإلكترونية.

لكن في المقابل، هناك توجه متزايد لدى بعض المؤسسات، خاصة في قطاعات الدفاع والاتصالات، نحو تحديث أنظمة الحماية واعتماد أجهزة تشفير وشبكات مغلقة.

خامسا: التحديات القانونية المرتبطة باستخدام الأجهزة الوقائية

استخدام هذه الأجهزة قد يطرح إشكاليات قانونية في حالات معينة، منها:

- التضارب بين حماية الحياة الخاصة ومبدأ الأمن العام؛
- احتمال إساءة استعمال أجهزة مثل أجهزة التشويش بما يؤدي إلى تعطيل الاتصالات الحيوية؛
- الحاجة إلى ترخيص قانوني لبعض هذه الأجهزة خاصة تلك ذات الطابع العسكري أو الاستخباراتي.[3]

---

[1]– الموقع الإلكتروني، المرجع السابق.

[2]– منصور رضا، المرجع السابق، ص 48.

[3]– المرجع نفسه، ص 48.

المبحث الثاني:

صور المخاطر المرتبطة بالتنصت الإلكتروني

مع تطور تكنولوجيا الاتصالات والمعلومات أصبح التنصت الإلكتروني من أخطر التهديدات التي تواجه الأفراد والمؤسسات والدول على حد سواء، إذ لم يعد محصورا في الأبعاد الأمنية فحسب، بل امتد ليشمل الجوانب الاقتصادية والاجتماعيـــة وحتى السيـــاسية، وفي ظل هذا التطور وجد المشرع نفسه مطالبا بالتدخل لتنظيم هذا المجال الحساس بغية حماية الحقوق الأساسية للمواطنين من جهة وضمان أمن واستقرار الدولة من جهة أخرى، وهو ما سنتطرق إليه لدراسته في المطلبين لتبيان صور مخاطرهما على الأفراد والمؤسسات والأمن القومي.

المطلب الأول:

صور مخاطر التنصت الإلكتروني على الأفراد

يعد الحق في الخصوصية من أبرز حقوق الإنسان وهو جزء لا يتجزأ من كرامة الإنسان ككل، لأن المس بخصوصية الفرد تؤدي في أحيان كثيرة إلى المس بكرامتـــه وسمعته[1]، فتنوعت مخاطر التنصت على الأفراد في **(الفرع الأول)** تناولنا مخاطر انتهاك الخصوصية، وفي **(الفرع الثاني)** تناولنا الابتزاز والتشهير.

الفرع الأول: مخاطر انتهاك الخصوصية

يعرف انتهاك الخصوصية بأنه أي عمل يتضمن جمع أو استخدام المعلومات الشخصية دون إذن من صاحبها.

[1]– المادة 12 من الإعلان العالمي لحقوق الإنسان لسنة 1948 التي تنص على ما يلي: "لا يجوز تحريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلته".

فقد أولى المشرع الجزائري أهمية بالغة لحماية الحياة الخاصة للأفراد خاصة في ظل التطور التكنولوجي المتسارع الذي جعل الخصوصية عرضة للانتهاكات متعددة الأشكال، وقد تصدى لهذه الانتهاكات من خلال مجموعة من النصوص القانونية التي تهدف إلى صون حرمة الحياة الخاصة، ومنع أي مساس بها دون مبرر قانوني مشروع وفيما يلي أبرز صور هذه المخاطر كما تناولها التشريع الجزائري.

أولا: الاعتداء على سرية الاتصالات والمراسلات

تعد سرية المراسلات والمحادثات الهاتفية من الركائز الأساسية للحق في الخصوصية، وقد جرم المشرع الجزائري كل فعل من شأنه المساس بهذه السرية دون إذن قضائي، حيث تنص المادة 303 مكرر من قانون العقوبات الجزائر على: "أن كل من تعمد بأي وسيلة كانت المساس بحرمة الحياة الخاصة للغير، وذلك بإلتقاط أو تسجيل أو نقل دون إذن صاحبها لمحادثات أو أقوال صدرت على انفراد أو في أي مكان خاص يعاقب بالحبس والغرامة، ويشمل هذا الخطر مختلف الوسائل الحديثة كأجهزة التنصت وبرامج التجسس الإلكترونية.[1]

ثانيا: تصوير الأشخاص أو تسجيلهم دون رضاهم

من صور الانتهاك الواضحة للخصوصية كذلك قيام بعض الأفراد بإلتقاط صور أو تسجيلات صوتية أو بصرية لأشخاص في أماكن خاصة دون موافقتهم وهو ما يشكل جريمة في القانون الجزائري، وقد جاء في المادة 303 مكرر 1 من قانون العقوبات الجزائري تجريم هذه الأفعال، كما شدد العقوبة في حال تم استخدام هذه الصور أو التسجيلات بطريقة تسيء إلى سمعة الشخص أو تم نشرها عبر الوسائط الرقمية أو الإعلامية.[2]

ثالثا: المعالجة غير المشروعة للمعطيات الشخصية

أصبح تداول بيانات الشخصية يمثل أحد أهم مصادر التهديد للخصوصية خاصة في ظل استخدام التطبيقات الرقمية للخصوصية والمنصات الالكترونية، ولهذا الغرض قرر المشرع الجزائري في القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال

[1]- المادة 303 مكرر، من قانون العقوبات الجزائري، المرجع السابق.

[2]- المادة 303 مكرر 1، المرجع نفسه.

معالجة المعطيات ذات الطابع الشخصي الذي وضع إطارا قانونيا صارما لجمع ومعالجة وتخزين البيانات، وفرض الحصول على موافقة صريحة من الشخص المعني بالمعالجة مع وجوب الترخيص المسبق من سلطة حماية المعطيات الشخصية.[1]

رابعا: المراقبة الالكترونية والتنصت بدون سند قانوني

يحظر القانون أي شكل من أشكال المراقبة الالكترونية سواء تعلق الأمر باعتراض المكالمات أو التنصت على المحادثات أو التجسس على البيانات، إلا في حالات محددة يقرها القانون ويشترط أن تكون بناءًا على أمر قضائي، وقد نظم قانون الإجراءات الجزائية هذا الموضوع في المواد 65 مكرر 5 إلى 65 مكرر 15، حيث يبين شروط وإليه الترخيص بالتنصت الالكتروني في إطار التحقيقات الجنائية حماية للخصوصية من أي تعسف في استعمال هذه الوسائل.[2]

خامسا: النشر العلني للمعلومات الخاصة عبر الوسائط الرقمية

مع انتشار وسائل التواصل الاجتماعي ووسائل الاعلام الرقمي أصبحت خصوصية الأفراد أكثر عرضة للانتهاك، سواء من خلال نشر صورهم أو معلوماتهم الشخصية دون رضاهم، وقد تدخل المشرع من خلال القانون رقم 09-04 المؤرخ في 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وجرم كل عمل يتم فيه نشر محتوى رقمي ينتهك الحياة الخاصة للغير، حتى ولو كان المحتوى صحيحا إذا لم يكن مرفقا برضا صريح من الشخص المعني.[3]

---

[1]- القانون 18-07 المؤرخ في 10 يونيو 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المرجع السابق.

[2]- المواد 65 مكرر 05 إلى 65 مكرر 15 من قانون الإجراءات الجزائية، المرجع السابق.

[3]- قانون رقم 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، المرجع السابق.

الفرع الثاني: مخاطر الابتزاز والتشهير

تم تعريف الابتزاز بأنه ما يمارسه المجرم المبتز من تهديد وسلوك للمجني عليه بعد حصوله على معلومات تخص المجني عليه، كالتسجيلات الصوتية أو صور شخصية بهدف تحقيق رغباته التي يسعى إليها سواء كانت مادية أو معنوية.[1]

المادة 303 يعاقب بالحبس من ستة أشهر إلى خمسة سنوات وبغرامة من 50.000دج إلى 500.000 دينار جزائري كل شخص يلجأ إليه الانتقام أو الترهيب أو تهديد بأي طريقة كانت، أو بأي شكل من الأشكال ضد الشهود أو الخبراء أو الضحايا أو المبلغين أو أفراد عائلتهم وسائر الوثيقي الصلة بهم.[2]

المادة 303 مكرر تنص على معاقبة من يستعمل تسجيلات أو الصور التي تم الحصول عليها بطريقة غير مشروعة بقصد الأضرار بصاحبها أو ابتزازه.

ينص قانون العقوبات في المادة 303 مكرر على أن التشهير بأي شخص عبر وسائل الاعلام أو مواقع التواصل، يعتبر جريمة وتشدد العقوبة إذا كانت الضحية قاصرا والعقوبات تشمل غرامة مالية تتراوح بين 100.000 دينار جزائري و500.000 دينار جزائري، وعقوبة الحبس من ستة أشهر إلى خمس سنوات حسب جسامة الضرر.[3]

فيعد الابتزاز والتشهير من أخطر الأفعال التي تنتهك الحقوق والحريات الفردية خاصة ضد الثورة الرقمية وسائل التواصل الاجتماعي التي ارتكاب هذه الجرائم وتوسيع نطاق أثارها، وقد تصدى المشرع الجزائري لهذين النوعين من الجرائم من خلال أحكام قانون العقوبات من كل أشكال الضغط والإضرار المعنوي والاجتماعي كما يلي:

أولا: الابتزاز الإلكتروني والتهديد بنشر معلومات خاصة

يعد الابتزاز صورة خطيرة من صور المساس بالحياة الخاصة ويتجسد في تهديد الضحية بنشر معلومات أو صور تسجيلات تمس بسمعته أو حياته الشخصية مقابل

---

[1]– حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي**، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر، باتنة، 2011–2012، ص 61.

[2]– المادة 45 من قانون العقوبات الجزائري، المرجع السابق.

[3]– المادة 298 مكرر من قانون العقوبات الجزائري، المرجع السابق.

الحصول على منفعة مالية أو مادية، وقد عالج المشرع هذه الجريمة في المادة 371 من قانون العقوبات الجزائري التي تجرم كل من حصل على منفعة غير مستحقة من شخص آخر بتهديده بإفشاء أمور من شأنها أن تضر بشرفه أو باعتباره[1]، كما تم تعزيز الحماية القانونية في هذا السياق من خلال قانون الذي يجرم الابتزاز الالكتروني صراحة ويشدد العقوبات عند ارتكابه عبر وسائط رقمية.[2]

ثانيا: التشهير والمس بالسمعة عبر الوسائط الرقمية

يقصد بالتشهير كل فعل من شأنه الاضرار بسمعة شخص معين عن طريق نشر أقوال وصور أو معلومات كاذبة أو حتى صحيحة، إذا كان الهدف منها الإيذاء المعنوي أو الاجتماعي ويجرم قانون العقوبات هذا الفعل في مواده المتعلقة بالقذف والسب، وخاصة في المواد 296 إلى 298 والتي تعاقب على نشر إدعاءات أو وقائع تمس بشرف أو اعتبار شخص طبيعي أو معنوي.[3]

وفي السياق الرقمي يشدد قانون الوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال قانون 04-09 العقوبة على من ينشر محتويات تتضمن قذفا أو تشهيرا أو تحقيرا، من خلال منصات الأنترنت خاصة إذا ترتب عن ذلك أضرار نفسية أو اجتماعية للضحية.[4]

ثالثا: التحريض على التشهير أو نشر المحتوى المسيء

من بين أخطر صور مخاطر التشهير ليس فقط ارتكاب الفعل نفسه، بل أيضا المساهمة فيه عن طريق التحريض أو المساعدة في النشر أو إعادة تداول المحتوى، وقد نص المشرع على مسؤولية كل من ساهم في هذه الأفعال سواء بالتحريض أو تسهيل أو حتى الاخفاء، ويخضع هؤلاء للنفس العقوبة المقررة للجريمة الأصلية طبقه للمادة 42 من قانون العقوبات.[5]

---

[1]- المادة 371 من قانون العقوبات الجزائري، المرجع السابق.

[2]- قانون رقم 09-04، المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال، المرجع السابق.

[3]- المواد 296 إلى 298 من قانون العقوبات الجزائري، المرجع السابق.

[4]- المواد 22 و23 من قانون العقوبات الجزائري، المرجع نفسه.

[5]- المادة 42 من قانون العقوبات الجزائري، المرجع نفسه.

رابعا: استغلال الصور والفيديوهات بقصد الاضراب

في ظل سهولة إلتقاط صور وتسجيل الفيديوهات أصبحت هذه الوسائط أدوات خطيرة تستعمل في التشهير خاصة حين يتم تعديلها وتركيبها بشكل مخل بهدف الإيذاء، ووفقا للمادة 303 مكرر 1 من قانون العقوبات فإن أي نشر أو استخدام لصور أو تسجيلات تمس بالحياة الخاصة دون إذن صاحبها يعد جريمة، وتشدد العقوبة إذا تم ذلك عبر وسائل الاعلام أو الشبكات الاجتماعية وشبكات التواصل.[1]

المطلب الثاني:

صور مخاطر التنصت الالكتروني على المؤسسات والأمن القومي

التطور الكبير في التكنولوجيا التنصت على المؤسسات والأمن القومي التي تعتبر من أبرز التهديدات المعاصرة التي تواجه الدول لما لها من قدرة على اختراق المؤسسات والتنصت والتجسس على البيانات والمعلومات الحساسة، مما يشكل تهديدا مباشر لمقومات السيادة والأمن القومي والتي لم تكن الجزائر بمنأى عن هذه التحديات خاصة في ظل التحول الرقمي الذي مس مختلف قطاعات الدولة، مما وسع من دائرة تهديدات السيبرانية وفي هذا السياق نلجأ إلى أبرز مدى خطورة التنصت الالكتروني على المؤسسات الاقتصادية والإدارية من جهة والأمن القومي من جهة أخرى، مبرزين صورهما بهدف تقييم مدى نجاعة النظام القانوني الوطني في حماية السيادة الرقمية للدولة وهو ما سيتم تفصيله كالآتي:

الفرع الأول: صور مخاطر التنصت الالكتروني على المؤسسات

تتعرض المؤسسات الجزائري سواء كانت عمومية أو خاصة إلى تهديدات حقيقية بسبب تنصت الأطراف الغير مشروع على مراسلتها واتصالاتها الرقمية، الأمر الذي قد يؤدي إلى المساس بأمنها الوطني والاقتصادي والتنظيمي، وفيما يلي صور التنصت الالكتروني على المؤسسات:

[1]– المادة 303 مكرر 1 من قانون العقوبات الجزائري، المرجع السابق.

أولا: اختراق البيانات الإدارية والوثائق السرية

تمثل الهجمات التي تستهدف الوثائق الملفات الإدارية الحساسة أحد أخطر صور التنصت الالكتروني على المؤسسات، حيث يمكن من خلالها الحصول على قرارات استراتيجية أو مستندات مالية أو معلومات خاصة بالموظفين والمراسلات الرسمية، ويعد هذا الفعل جريمة يعاقب عليها المشرع وفقا القانون رقم 23-05، خاصة إذا كانت الوثائق محل التنصت تخصص مؤسسات ذات طابع سيادي أو مالي أو خدماتي.[1]

هذا وقد جاء في الأمر رقم 21-09 مؤرخ في 8 يونيو 2021 الذي يتعلق بحماية المعلومات والوثائق الإدارية والذي خصص بعض أحكامه[2] للحماية الجزائية لسرية الوثائق والمعلومات الإدارية، فقد ركز في طياته بدرجة أولى في حمايته على تلك التي تحتوي على أسرار لا يجوز الاطلاع عليها إلا من طرف الأشخاص المؤهلين للاطلاع عليها، فقد حددت المادة 33 من الأمر 21-09 الأفعال الجريمة لهذه الجريمة والتي تقوم على عنصرين أساسيين هما:[3]

1- النشاط الاجرامي يتحقق بإحدى صورتين، الصورة الأولى تتمثل في قيام الجاني باطلاع الغير على معلومة أو وثيقة مصنفة مهما كانت درجة حساسيتها الصورة الثانية أن يسير الجاني للغير ذلك.

2- أن يكون الاطلاع بمقابل مهما كانت طبيعته سواء كان مقابل ذو طبيعة مادية أو ذو طبيعة معنوية، وقد يكون صريحا أو ضمنيا مشروعا أو غير مشروع محددا أو غير محدد سواء كان المقابل داخل الوطن أو خارجه.

ويشترط أن يكون الشخص الفعلي الجريمة غير مصرح له بدخول منظومة إلكترونية أو شبكة إلكترونية، أو أي وسيلة أخرى من وسائل تكنولوجيا الاعلام والاتصال للسلطات المعينة المنصوص عليها في المادة 2 من الأمر

[1]- المادة 26 من قانون العقوبات الجزائري، المرجع السابق.

[2]- الأمر رقم 21-09، المؤرخ في 08 يونيو 2021 يتعلق بحماية المعلومات والوثائق الإدارية، ج.ر، عدد 45، مؤرخة في 9 يونيو 2021.

[3]- المادة 33 من الأمر 21-09، المرجع نفسه.

21-09[1]، وهذا الشرط مأخوذ من قول المشرع "دون الاخلال... كل من يدخل دون ترخيص إلى منظومة معلوماتية".

فقد رتب المشرع عقوبة الحبس من خمس سنوات إلى 10 سنوات وغرامة من 500.000 دينار جزائري إلى 1000.000 دينار جزائري دون الاخلال بعقوبات الأشد المنصوص عليها في المواد 394 مكرر 7 قانون العقوبات الجزائرية، وقرر المشرع مضاعفة العقوبة في حال ما قام الجاني بنشر المعلومات أو الوثائق المصنفة التي حصل عليها، بقصد الاضرار بالسلطات المعينة أو الحصول على منافع مباشرة أو غير مباشرة وهذا حسب نص المادة 37 الفقرة 2.[2]

ثانيا: التنصت الصناعي وتقويض التنافسية

في ظل التحولات الكبرى التي تعرفها الأسواق العالمية المعاصرة أضحت المعلومة الصناعية والتجاري من أهم مقومات القوة الاقتصادية، ولعل التنصت الصناعي يمثل اليوم أحد أخطر التهديدات التي تواجه المؤسسات لما له من قدرة على تفويض مبدأ التنفسية العادلة، مما يضعف ديناميكية السوق ويضر بالابتكار والاستثمار طويل الأمد.

يعرف التنصت الصناعي كل ممارسة ترمي إلى الحصول بوسائل غير مشروعة أو غير مصرح به على معلومات سرية تخص مؤسسة اقتصادية، بغرض تحقيق ميزة تنافسية أو ضرر بالمنافس.[3]

وتتخذ هذه الممارسات أشكال متعددة من بينها:

1- سرقة براءة الاختراع أو الأسرار التجارية.

2- اعتراض الاتصالات أو المراسلة الخاصة بالمؤسسات.

3- استغلال موظفين أو متعاملين لنقل بيانات سرية.

4- التنصت الهاتف الغير المشروع.

5- التنصت على الاجتماعيات واللقاءات الرسمية.

---

[1]- المادة 02 من الأمر 21-09، المرجع السابق.

[2]- المادة 37 فقرة 2 من الأمر 21-09، المرجع نفسه.

[3]- عيسى بوشيبة، " **حماية الأسرار التجارية في القانون الجزائري** "، مجلة الدراسات القانونية والسياسية، العدد 5، جامعة باتنة 1، 2017، ص 120.

ويؤدي التنصت الصناعي إلى اختلال مبدأ المساواة بين المتنافسين، حيث يحصل المتنصت الصناعي على معلومات استراتيجية تمكنه من التفوق بطرق غير شرعية، وهذا يؤدي إلى الاضرار بالمنافسين النزهاء وأضعاف ديناميكية السوق وتكريس ممارسات احتكارية، مما ينعكس سلبا على المؤسسات عند الاستثمار في البحث والتطوير خوفا من تسرب أفكارها ومنتجاتها ليبطئ عجلة الابتكار ويؤدي إلى تبعية تكنولوجية قاتلة.

لقد جاء في قانون حماية الملكية الصناعية الأمر 03-07 المادة 06-07 تحميل أسرار الصناعية من الاستخدام الغير مشروع بشرط اتخاذ تدابير كافية للسرية من طرف صاحب الحق.[1]

وجاء في المادة 18 من القانون 03-03 المعدل والمتمم بالأمر المؤرخ في 19 يوليو 2023 المعدل والمتمم بالأمر رقم 10-05 المتعلق بالمنافسة تعد ممارسة مخالفة للمنافسة كل عملية من شأنها أن تقل بمبادئ المنافسة الحرة.[2]

المادة 394 مكرر من قانون العقوبات بعد التعديل يعاقب بالحبس من ستة أشهر إلى سنتين كل من تعمد الدخول أو البقاء في منظومة معلوماتيـــة بصفة غيـــر مشروعة[3]، ومما يلاحظ في كل من جاء به المشرع الجزائري فإنه لم يدرج التنصت الصناعي كجريمة مستقلة خلافا لبعض التشريعات المقارنة، كالتشريع الأمريكي في قانون التجسس الاقتصادي لسنة 1996 (économie espionnage) الذي يجرم التنصت الصناعي سواء تم من جهة فاعلين اقتصاديين أو حتى دول أجنبية.

وتبقى العقوبة المفروضة الحالية غير رادعة مقارنة بخطورة الأفعال المرتكبة والضرر الواقع على الاقتصاد الوطني وعليه وجب:

---

[1]- المادة 06-07، قانون 03-07، المؤرخ في 19 يوليو 2003 والمتعلق بالملكية الصناعية، ج.ر، عدد 42، 2003.

[2]- المادة 18 من قانون 03-03 المعدل بالأمر رقم 10-05، المتعلق بالمنافسة.

[3]- المادة 394 مكرر من قانون العقوبات الجزائري، المرجع السابق.

1- استحداث نصوص صريحة تجرم التنصت الصناعي والتنفسية ضمن قانون العقوبات.

2- مع تعديل قانون المنافسة الذي يشمل ضمن ممارسته المخلة تلك التي تتم عبر وسائل إلكترونية أو معلوماتية.

3- كذا تعزيز الحماية سيبرانية للمؤسسات الاقتصادية من خلال برامج تكوين إلزامية ومرافقة تقنية حكومية.

4- إدراج التنشيط الصناعي الالكتروني ضمن الجرائم الاقتصادية الكبرى باعتباره تهديدا للأمن الاقتصادي الوطني.

ثالثا: تعطيل الأنظمة المعلوماتية للمؤسسة

أصبح تعطيل الأنظمة المعلوماتية للمؤسسات من الأفعال الاجرامية التي اكتسبت أهمية متزايدة في ظل التحول الرقمي الذي تشهده معظم المؤسسات، ومما لا شك فيه سعى المشرع الجزائري بالنظر لخطورة هذا النوع من الأفعال التي تمس بأمن المعلومات واستقرار المصالح العمومية، والخاصة إلى تجريم هذه الأخيرة ضمن إطار قانوني خاص بمكافحة الجرائم المتعلقة بتكنولوجية الاعلام والاتصال.[1]

فقد جاء في قانون رقم 18-07 المؤرخ في 10 ماي 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، ثم جاء بعده القانون رقم 09-04 في 5 أغسطس 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجية الاعلام والاتصال ومكافحتها، فهناك مثلا أنواعا من الأفعال التي تدخل ضمن نطاق تعطيل الأنظمة المعلوماتية مثل:[2]

[1]- المادة 13 من القانون، المتعلق بالوقاية من الجرائم المتصلة بالتكنولوجيا الاعلام والاتصال ومكافحتها، المرجع السابق.

[2]- قانون رقم 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال المعطيات ذات طابع الشخصي، المرجع السابق.

- إعاقة أو تعطيل سير نظام المعلوماتي.
- إدخال أو نشر برمجيات خبيثة malware تؤدي إلى تلف أو شلل النظام.
- الحيلولة دون الوصول إلى معطيات أو التطبيقات المعلوماتية أو تعطيلها.

والهدف منها هو التنصت الغير المشروع على المؤسسات أنظمة معلوماتية.

جاء في نص المادة 13 من القانون 09-04 ما يلي: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة 500.000 دينار جزائري إلى 2000.000 دينار جزائري، كل من قام عمدا بإدخال أو ارسال أو اتلاف أو تعديل أو حذف أو إتاحة بيانات ذات طابع شخصية أو عرقلة سير نظام إلى معالجة المعطيات".[1]

وتمتد هذه الحماية لتشمل أنظمة المعلومات التي تخص الدفاع الوطني أو الأمن العمومي، حيث شدد المشرع العقوبات في حالة كان نظام المستهدف ذا الطابع حساس.

ففي هذه الحالة تصل العقوبة إلى السجن النافذ لمدة 10 سنوات طبقا للمادة 22 من نفس القانون إذا ما أدى التعطيل إلى تهديد فعل الأمن القومي.[2]

وفي قرار صادر عن مجلس قضاء الجزائر سنة 2020 تمت إدانة موظف سابق في مؤسسة اتصالات قام بزرع برنامج خبيث في خوادم المؤسسة، مما أدى إلى توقف خدمات الزبائن لمدة يومين وقد اعتبر القاضي أن هذا الفعل يشكل جريمة كاملة الأركان طبقا لنص المادة 13 من قانون 09-04 لكونه نتج عنه تعطيل، فعلي لنظام معلوماتي حيوي تابع لمؤسسة ذات طابع عمومي اقتصادي.[3]

ومما يلاحظ أن القضاء الجزائري يتشدد في التعاطي مع الجريمة المعلوماتية لما تمثله من خطر لا مادي لكنه فعال، ويتم التركيز في غالب الأحيان على عنصر التعمد في التعطيل وهو ما يجعل عنصر النية الاجرامية جوهريا في قيام الجريمة ويكفي أن يكون هناك تعطيل في الأداء أو حرمان من الوصول إلى النظام المعلوماتي، ويظهر موقف

---

[1]- المادة 13 من قانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، المرجع السابق.

[2]- المادة 22 من قانون 09-04، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، المرجع نفسه.

[3]- قرار مجلس قضاء الجزائر غرفة الجنح القضية رقم 1123، بتاريخ 2020/12/15.

المشرع الجزائري من خلال نصوص المتعلقة بالأنظمة المعلوماتية، والتجريم الصريح لأفعال التنصت الالكتروني وعيا متناميا بمخاطر الهجمات الرقمية على أمن المؤسسات.

الفرع الثاني: مخاطر التنصت الالكتروني على الأمن القومي

لقد اعتبر المشرع الجزائري من خلال جملة النصوص القانونية لا سيما قانون رقم 18-04 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي أن التنصت أو الاعتراض غير المشروع للمراسلة الالكترونية يشكل مساسا خطيرا بالأمن الوطني، باعتباره يهدد سرية المعطيات السيادية ويعرض مؤسسة الدولة للاختراق والتلاعب الخارجي فلا تختصر التنصت الالكتروني على المؤسسات، بل تتعداها إلى تهديد الأمن القومي نفسه خاصة عندما تستهدف الهجمات السيبرانية مصالح الدولة العليا أو تسعى إلى أضعاف سيادتها الداخلية والخارجية ومن هاته الصور:

أولا: المساس بالمصالح الاستراتيجية للدولة

يشكل تنصت الالكتروني الموجه نحو المصالح الاستراتيجية للدولة أحد أخطر صور الجرائم الماسة بالأمن القومي، إذ ينصرف هذا الفعل إلى جمع معلومات سرية أو اعتراض بيانات خاصة بمجالات حيوية كالدفاع الوطني العلاقات الخارجية الاقتصادية الاستراتيجي أو حتى الأمن الطاقوي، وذلك إما لصالح جهات أجنبية أو فاعلين غير حكوميين يهدفون إلى زعزعة استقرار الدولة أو التأثير في قراراتها السيادية، وقد أولى المشرع الجزائري في هذه المسألة أهمية بالغة ضمن سياسته الجنائية الحديثة إدراكا منه لتحول النزاعات المعاصرة إلى حروب معلوماتية تتجاوز في خطورتها الحروب التقليدية.

فمن خلال تعديل قانون العقوبات بموجب القانون رقم 20-05 تم تجريم كل الأفعال التي من شأنها المساس بأنظمة المعالجة الآلية للمعطيات التابعة للدولة، أو للهيئات العمومية ذات الطابع السيادي خاصة إذا تعلق الأمر بنظم معلومات ترتبط بمصالح عليا للدولة، كالجيش الأمن أو الهيئات الاقتصادية السيادية.[1]

فحسب القانون رقم 20-05 المؤرخ في 28 أبريل 2020 المعدل والمتمم لقانون العقوبات الأمر 66-156 جاء فيه:

[1]- المواد 394 مكرر إلى 394 مكرر 8 من قانون العقوبات الجزائري، المرجع السابق.

- إدراج فصل جديد بعنوان المساس بأنظمة المعالجة الآلية للمعطيات والذي قام بتجريم الأفعال التالية:
  - الولوج الغير مشروع إلى نظم معلومات تابعة للدولة أو هيئات سيادية.
  - اعتراض المعطيات أو التنصت عليها أو تعديلها دون ترخيص.
  - المساس بنظم المعلومات التي تهم الدفاع الوطني أو الاقتصاد أو الأمن العام المواد المعنية من المادة 394 مكرر إلى 394 مكرر 8، فيعتبر هذا القانون حجر الزاوية في مواجهة الجرائم السيبرانية.[1]

كما ورد في قانون رقم 20-05 المتعلق بأمن نظم المعلومات الدولة تضع تحت الحماية القانونية كل منظومة تمس الأمن الوطني، أو الاقتصاد معتبرا فعل الاختراق أو الاعتراض للمعطيات تهديدا مباشرا للأمن القومي.[2]

فأبرز ما جاء في قانون 20-05 المتعلق بأمن نظم المعلومات:

- عرف بنظم المعلومات ذات الطابع الاستراتيجي في الفقرة الثانية من المادة 2، أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها أو المرتبطة يقوم واحد منها أو أكثر بمعالجة إليه للمعطيات تنفيذا لبرنامج معين.[3]
- فرض إلزامية حماية الأنظمة الحساسة لدى الإدارات العمومية وشركات الوطنية الكبرى.
- إنشاء الهيئة الوطنية لأمن نظم المعلومات (anssi).
- فرض التبليغ الاجباري عن الحوادث السيبرانية.

كما ورد في الأمر رقم 21-09 المؤرخ في 8 يونيو 2021 المتعلق بحماية المعلومات والوثائق الإدارية ما يلي:[4]

---

[1]- المواد 394 مكرر إلى 394 مكرر من قانون العقوبات الجزائري، المرجع السابق.

[2]- القانون 09-04 المتعلق بقانون الإعلام وتكنولوجيا الاتصال، المرجع السابق.

[3]- المادة 2 فقرة 2 من قانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، المرجع السابق.

[4]- الأمر رقم 21-09، المتعلق بحماية المعلومات والوثائق الإدارية، المرجع السابق.

- تصنيف المعلومات الإدارية وفقا لدرجة سريتها "سري" "سري جدا" "محمي".
- تحديد كيفية تخزين وتداول الوثائق الحساسة داخل الهيئات العمومية.
- تجريم تسريب أو نشر أو نسخ أو تصوير معلومات مصنفة دون ترخيص.

من أهداف هذا القانون هو حماية المعلومات ذات الطابع السيـادي التي إذا تم اختراقها، أو تسريبها قد يؤدي إلى مساس مباشر بالمصالح الاستراتيجية للدولة.

ومن خلال هذه النصوص القانونية الحديثة، فإنه يتكشف لنا تبني الجزائر استراتيجية أمنية شاملة قوامها:

- تجريم صارم لكل الأفعال التي تهدد السيادة والمصالح العليا.
- وقاية تقنية وقانونية عبر أنظمة رقابة وتشفير متقدمة.
- تنسيق مؤسساتي بين الأمن والقضاء والمجتمع الرقمي.
- تعاون دولي لمجابهة الجرائم الالكترونية ذات الطابع العابر للحدود.

ثانيا: تسريب معلومات تمس الأمن العسكري أو الأمن العام

يعد تسريب المعلومات التي تمس بالأمن العسكري أو الأمن العام من أبرز التهديدات الناجمة عن التنصت الالكتروني الغير مشروع، إذ يمكن أن يستغل هذا الأخير كوسيلة لاختراق المؤسسات الأمنية والعسكرية ما يفتح بابا واسعا أمام المساس بالأمن القومي، وقد تنبه المشرع الجزائري لخطورة هذا النوع من الأفعال، وخاصة بنصوص قانونية واضحة لا سيما ما يحدث من تحولات رقمية في العالم.

فقبل أن نتطرق لجملة القوانين الخاصة بتسريب معلومات تمس الأمن العسكري أو الأمن العام لنتعرف عليها، فهي تعد من أبرز التهديدات الناجمة عن التنصت الالكتروني غير مشروع وهي نقل أو إفشاء أو تمكين الغير عمدا، أو بغير قصد من الاطلاع على معلومـات مصنفة تمس بــأمن الدولــة أو سلامتهـا أو تسيير مؤسساتهــا الأمنية والعسكرية، سواء كان ذلك بالوسائل التقليدية أو عبر الوسائل الالكترونية أو برامج التجسس والتنصت الالكتروني.[1]

[1]– جمال غراب، **الثبات الالكتروني كآلية لجمع الأدلة الجنائية**، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2021–2022، ص 32.

فقد نظم المشرع الجزائري ذلك في جملة من القوانين نذكر ما جاء منها:

المادة 47 تكفل حماية المعطيات ذات الطابع الشخصي.[1]

هذا وجاء في قانون العقوبات عدة مواد تجرم أفعال لا تمس بالأمن القومي

المادة 63 من قانون العقوبات على الخيانة والتخابر مع الجهة الأجنبية أو إفشاء أسرار الدفاع الوطني.

المادة 66 قانون العقوبات التي تجرم جمع أو إفشاء أو نقل معلومات تمس بالدفاع الوطني.

المادة 67 تعاقب على الدخول إلى أماكن محمية لأغراض تجسسية.

المادة 107 مكرر تجرم الاعتداء على نظم المعالجة الآلية للمعطيات.[2]

كما عالج القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجية الاعلام والاتصال الجرائم السيبرانية خاصة ما يرتبط باختراق الأنظمة والتنصت الالكتروني، فقد جرم اعتراض الاتصالات الإلكترونية واختراق الأنظمة المعلوماتية وتسريب البيانات المحمية.[3]

والقانون رقم 18-07 المتعلق بحماية المعطيات الطابع الشخصي ينظم معالجة المعطيات ويمنع استعمالها دون ترخيص خاصة، إذا كانت طابع أمني بحيث يلزم الهيئات الرسمية باتخاذ تدابير أمنية صارمة لحماية المعلومات الحساسة.[4]

نظم القانون رقم 06-03 المتعلق بالوظيفة العمومية في طياته بفرض على الموظفين الحفاظ على السر المهني خاصة في الملفات الأمنية، والعسكرية ويعاقب الذي يفشي أسرار المهنة المتعلقة بالأمن.[5]

---

[1]- المادة 47 من الدستور الجزائري المعدل بتاريخ 2020، المرجع السابق.

[2]- الأمر 66-156 من قانون العقوبات، المرجع السابق.

[3]- القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، المرجع السابق.

[4]- القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، المرجع السابق.

[5]- القانون رقم 06-03 المؤرخ في 15 يوليو 2006، المتعلق بالقانون الأساسي العام للوظيفة العمومية، ج.ر، العدد 46، 2006.

المرسوم الرئاسي رقم 22-45 متعلق بالأمن السيبراني ينظم العمل الوقائي في الأمن السيبراني وينشئ الهيئة الوطنية السيبراني، ويكلف الهيئة برصد تهديدات السيبرانية التي قد تمس بالأمن القومي.[1]

التنصت كوسيلة لتسريب المعلومات الأمنية إذ يعد وسيلة فعالة للوصول إلى معلومات مصنفة بسرية عالية خصوصا حين يتم بشكل سري ودون ترخيص قضائي مثل:

- اختراق البريد الالكتروني لضباط مسؤولين في الأجهزة الأمنية.
- تثبيت برمجيات خبيثة (malware) على أجهزة تستخدم في إدارة العملية العسكرية.
- استغلال تطبيقات الاتصال الصوتي المشفرة للوصول إلى مخططات أو تحركات أمنية وعليه يمكن أن تؤدي المعلومات المسربة إلى:
  - إفشال عمليات أو أفراد القوات المسلحة للخطر.
  - تعريض حياة عملاء أو أفراد القوات المسلحة للخطر.
  - زعزع الثقة للمواطنين في مؤسسات الدولة.

وفي الأخير يمكن القول أن المشرع الجزائري قد تعامل مع خطر تسريب المعلومات النتائج عن التنصت الالكتروني بحسب من خلال تجريم الأفعال المرتبطة باختراق نظم المعلومات والتسريب أو إنشاء المعلومات ذات الطابع الأمني، غير أن تطورات التقنية السريعة تفرض عليه مراجعة مستمرة للمنظومة القانونية لضمان حماية حقيقية للأمن القومي في العصر الرقمي.[2]

ثالثا: إثارة الفوضى وزعزعة الاستقرار السياسي

عرفها الدكتور عبد الحميد العربي الشريف بأنه "كل فعل يتضمن استخدام وسائل الاعلام أو التكنولوجيا، أو وسائل الاتصال الحديثة بهدف التحريض على العنف أو نشر

[1]- المرسوم الرئاسي رقم 22-45، المؤرخ في 3 فيفري 2022، المتعلق بالأمن السيبراني، ج.ر، العدد 8، 2022.

[2]- محمد بن مـرزوق، **الجرائم المعلوماتية في التشريع الجزائـري-دراسة مقارنة**، دار هومـة، الجزائـر، 2021، ص 122-126.

خطاب الكراهية أو التلاعب الرأي العام، بما يؤدي إلى تقوية الاستقرار السياسي والنظام الدستوري.[1]

أو هو الدعوة إلى التمرد والعصيان أو التجمهر المسلح.

ففي قانون العقوبات الجزائرية نص على تجريم الأفعال التي تمس أمن الدولة الداخلي والتحريض على العنف.

المادة 77 تعاقب كل من يرتكب فعلا يهدف إلى تحريض المواطنين على حمل السلاح ضد سلطة الدولة.

المادة 78 تعاقب من يقوم بتكوين أو إدارة جمعية أو منظمة تهدف إلى قلب نظام الحكم أو التعدي على أمن الدولة.

المادة 97 تعتبر كل تجمهر مسلحة وغير مسلح يهدد النظام العام، أو الأمن من الجرائم الموصوفة ويعاقب المشاركون فيه.[2]

المادة 96 القانون العقوبات تجرم نشر أو توزيع منشورات من شأنها الأضرار بالنظام العام أو مصلحة الوطنية سواء ورقيا أو إلكترونيا.

المادة 20 قانون 09-04 تجرم صراحة التنصت الغير مشروع أو اعتراض الاتصالات الالكترونية خاصة إن تم بغرض تحريض أو زعزعت النظام.[3]

المرسوم الرئاسي 22-45 لسنة 2022 المتعلق بالأمن السيبراني ينص على تشكيل هيئة وطنية للأمن السيبراني تهدف إلى رصد ومنع أي نشاط إلكتروني يهدد الاستقرار السياسي، أو يستخدم بيانات متحصلة من تنصت إلكتروني.[4]

بالرغم من أن المشرع الجزائري لم ينص صراحة على جريمة إثارة الفوضى وزعزعة الاستقرار السياسي في نص خاص، إلا أنه جمعه بين:

---

[1]- عبد الحميد العربي الشريف، **الأمن القومي في ظل التهديدات الالكترونية – مقاربة قانونية والسياسية**، دار الخلدونية، الجزائر، 2020، ص 97.

[2]- المواد 77 و78 من قانون العقوبات، المرجع السابق.

[3]- المادة 20 من قانون 09-04، المرجع السابق.

[4]- المرسوم الرئاسي 22-45، المرجع السابق.

- تجريم الفعل التحريضي السياسي وتجريم الوسيلـة التكنولوجية (التنصت والاختراق)، مما يعكس موقفا وقائيا واستباقيا يهدف إلى حماية الأمن القومي من التهديدات المعاصرة المتشابكة بين السياسة والتكنولوجيا.

رابعا: تهديد السيادة الرقمية

1- يعد خرق الشبكات الوطنية الحيوية أو أنظمة الاتصالات السيادية تهديدا مباشرا للسيادة الرقمية للجزائر، خصوصا إذا تم التحكم عن بعد في البيانات أو تعطيل خدمات وطنية، فقد نص المشرع على ضرورة تأمين النظم الرقمية السيدية واعتبر المساس بها في حكم الجريمة الماسة بمقومات الدولة، ويعاقب عليها بالسجن المشدد والغرامات الكبيرة.[1]

2- عرفها الأستاذ عبد القادر سعدوني "السيادة الرقمية هي الامتداد السيبراني لسيادة الدولة وتمارس من خلال تشريعات وطنية، آليات رقابية، وحماية للبنية التحتية المعلوماتية.[2]

3- يمثل التنصت الالكتروني أحد أبرز الأدوات المستخدمة لاختراق السيادة الرقمية إذ يمكن من خلاله:

- رصد تحركات الدولة ومسؤوليها عبر اختراق البريد والمكالمات.
- جمع المعلومات الأمنية أو الاقتصادية لصالح جهات أجنبية.
- نشر مضامين رقمية مفبركة لخلق اضطراب في القرار السيادي.

وكل هذه الأفعال تضعف الدولة وقدرتها على التحكم في مجالها سيبراني، مما يشكل أساسا بالسيادة الرقمية وبالتالي بالأمن القومي.

---

[1]- بن عيسى عبد القادر، " **السيادة الرقمية السيبراني في الجزائر بين النصوص القانونية والتحديات الواقعية** "، مجلة الدراسات القانونية والسياسية، العدد 15، 2023، ص 178.

[2]- عبد القادر سعدوني، " **السيادة الرقمية والأمن القومي في ظل التحولات التكنولوجية** "، مجلة الدراسات السياسية والقانونية، العدد 15، جامعة الجزائر3، 2021، ص 88.

المرسوم الرئاسي 22-45 الخاص بالأمن السيبراني ينشئ هذا المرسوم هيئة وطنية للأمن السيبراني، ويعتبر أن حماية السيادة الرقمية من أولويات الأمن القومي حيث يلزم المؤسسات العمومية بالتصريح بالهجمات السيبرانية، ويخوض الدولة إدارة الاستجابة الوطنية لأي اختراق رقمي يهدد سيادتها.[1]

يمكن القول أن المشرع الجزائري أقر ضمنيا بمفهوم السيادة الرقمية عبر قوانين متفرقة تم الإشارة إليها في السابق.

وعمل على تجريم كل فعل يمس القضاء الرقمي الوطني من التنصت الالكتروني إلى القرصنة ونشر الفوضى الرقمية.

كما شرع في الحماية السيبرانية عبر هيئة وطنية في انتظار استكمال هذا المسار بقانون موحد خاص بالسيادة الرقمية.

[1]- المرسوم الرئاسي 22-45، المتعلق بالأمن السيبراني وإنشاء الهيئة الوطنية للأمن السيبراني، المرجع السابق.

خلاصة الفصل:

في ضوء ما تم عرضه في هذا الفصل يتضح أن ظاهرة التنصت الالكتروني تشكل تحديا معقدا يتطلب مقاربة شاملة تجمع بين الجوانب التقنية والقانونية والتنظيمية، فقد أظهرت الدراسة أن المخاطر الناجمة عن هذه الظاهرة لا تقتصر على الجانب الفردي فحسب، بل تمتد لتشكل تهديدا جسيما لأجهزة الدولة وسلامة أمنها القومي.

من النتائج الجوهرية التي توصلنا إليها في هذا الفصل أن فعالية آليات الحماية من التنصت الالكتروني ترتبط ارتباطا وثيقا بمدى تكامل المنظومة الأمنية، حيث يتطلب تحقيق الحماية المثلى تظافر عدة عوامل تشمل التطوير المستمر للنظم التقنية المتقدمة في مجال التشفير، والكشف عن الاختراقات وتعزيز الوعي الأمني على جميع المستويات ووجود إطار تشريعي رادع يتناسب مع التطورات التقنية المتسارعة.

خـــــاتمة

خـــاتمة:

التذكير بالإشكالية والاجابة عليها اجابة مباشرة وهذا يظهر من خلال:

- وجود النظام القانوني حيث أن المشرّع الجزائري سعى إلى تنظيم هذا المجال من خلال وجود ضمانات قانونية حيث فرض المشرع الجزائري ضوابط قانونية مثل الإذن القضائي الذي يحد من التعسف وتحمي الحقوق.
- تنظيم اجراء التنصت وكيفيته من خلال تحديد الاشخاص المؤهلون للقيام بالتنصت مع وضع أجهزة خاصة مستحدثة.
- وضع عقوبات صارمة تتناسب والتنصت الغير المشروع سواء على خصوصية الأفراد أو على مستوى المؤسسات.

غير أننا لاحظنا بعض السلبيات على هذا التنظيم ويظهر من خلال:

- هذا التنظيم لا يزال يعتريه بعض غموض النصوص القانونية، سواء من حيث الدقة في المفاهيم مما يفتح مجالا للتأويل
- قصور في الرقابة من حيث ضمانات الرقابة القضائية الفعالة، أو حتى من حيث توفير الحماية القانونية للمتضررين من التنصت غير المشروع.
- كما أن المخاطر الناجمة عن سوء استخدام التنصت الإلكتروني باتت تمس الأفراد والمؤسسات على حد سواء، مما يفرض حتميـــة تبنّي آليات وقائية وتقنيـــة متطورة، إلى جانب وعي مجتمعي وإطار تشريعي صارم

وفي ختام هذه المذكرة، لا يسعنا إلا أن نذكّر بأن الشرع الحنيف قد صان حرمة الإنسان في عرضه ودمه وماله، وحرّم التجسس والتنصت على الناس بغير حق، قال تعالى: "ولا تجسسوا" [الحجرات: 12] وما ذلك إلا لحماية كرامة الفرد وصون مجتمعه من الفتن والفساد، لذا فإن بناء نظام قانوني يوازن بين مقتضيات الأمن وضرورات الحرية، ليس مجرد خيار تشريعي، بل هو واجب شرعي وأخلاقي، تفرضه مبادئ العدالة وسيادة القانون.

الاقتراحات

- إصدار قانون خاص بالتنصت الإلكتروني، يحدد شروطه وإجراءاته وضماناته بشكل دقيق، مع توضيح الجهة القضائية المختصة بالإذن والرقابة بإدراج نص الخاص سواء فصل في قانون العقوبات أو تقنين مستقل
- تعزيز الرقابة القضائية والإدارية على الجهات التي تمارس التنصت، مع وضع آليات فعالة للتظلم والتعويض في حال إساءة الاستعمال.
- تطوير الإمكانيات التقنية للأجهزة الأمنية والقضائية بما يضمن كفاءة تنفيذ مهامها دون خرق حقوق الأفراد.
- نشر الوعي القانوني والرقمي لدى الأفراد والمؤسسات حول مخاطر التنصت وسبل الحماية منه.
- تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، وتبادل الخبرات والتجارب في مجال تنظيم التنصت الإلكتروني.
- تكوين القضاة والضباط المكلفين بالتنصت في الجوانب التقنية والقانونية الحديثة من خلال دورات تكوينية دورية تواكب المستجدات في ميدان تكنولوجيا المعلومات.
- فرض تسجيل وتوثيق جميع عمليات التنصت إلكترونياً بطريقة مؤمنة لضمان المصداقية وسهولة الرجوع إليها عند الطعن أو التحقيق.
- التنصيص في القانون على وجوب إعلام الشخص المتنصّت عليه بعد انتهاء الإجراءات ما لم تكن هناك ضرورة أمنية لاستمرار التحفظ، وذلك تكريساً لمبدأ الشفافية وضمان حق الدفاع.
- تعزيز العقوبات على من يستعمل وسائل التنصت لأغراض شخصية أو خارج الإطار القانوني بما في ذلك التشهير أو الابتزاز أو المنافسة غير المشروعة.
- تحيين النصوص القانونية بشكل دوري لمواكبة تطور وسائل التنصت وتقنيات الاتصالات الحديثة مثل التنصت عبر التطبيقات المشفرة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: المصادر

- **قرآن الكريم، سورة الأعراف الآية 24.**

1-المصادر القانونية:

أ-التشريعات

1-الجمعية العامة للأمم المتحدة، الإعلان العالمي لحقوق الإنسان، القرار 217 أ (د-3)، اعتمد في 10 ديسمبر 1948، المادة 12.

2- التعديل الدستوري الجزائري ،2020 جريـــدة رسمية عـــدد ،82 بتاريـــخ 30 /12/ 2020

3-الأمر رقم 156/66، المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات الجزائري المعدل والمتمم بالقانون رقم 06-23، المؤرخ في 2006/12/20، ج.ر، العدد 84،

4- قانون 03-07، المؤرخ في 19 يوليو 2003 والمتعلق بالملكية الصناعية، ج.ر، عدد 42، 2003.

5- القانون رقم 06-03 المؤرخ في 15 يوليو 2006، المتعلق بالقانون الأساسي العام للوظيفة العمومية، ج.ر، العدد 46، 2006.

6- قانون 20-05، المؤرخ في 2020/04/28، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج.ر، العدد 25،

7- قانون 15-20، المؤرخ في 2020/12/30، المتعلق بالوقاية من جرائم الاختطاف الأشخاص ومكافحتها، ج.ر، العدد 81، المؤرخ في 2020/12/30،

8- الأمر رقم 21-09، المؤرخ في 08 يونيو 2021 يتعلق بحماية المعلومات والوثائق الإدارية، ج.ر، عدد 45، مؤرخة في 9 يونيو 2021

9-قانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، العدد 34

10-القانون رقم 04/09 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، المؤرخة في 06 أوت 2009.

11- المادة 18 من قانون 03-03 المعدل بالأمر رقم 10-05، المتعلق بالمنافسة 17،

ب-المراسيم:

1-المرسوم الرئاسي رقم 22-45، المؤرخ في 3 فيفري 2022، المتعلق بالأمن السيبراني، ج.ر، العدد 8، 2022.

2-المرسوم الرئاسي رقم 261/15، المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.ر، ع 53.

ثانيا: المراجع باللغة العربية:

1- الكتب:

1- أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة، ط1، دار النهضة العربية، القاهرة، 2005.

2- حسان عبد الله، الاستخبارات الحديثة وأثرها على الأمن القومي، ط1، دار الهدى، بيروت، 2015.

3- ساسي علي حامد عياد، استخدام تكنلوجيا المعلومات في مكافحة الإرهاب، ط1، دار الفكر الجامعي، الإسكندرية، مصر، .

4- سمير بن شريف، الجريمة الإلكترونية بين النظرية والتطبيق، ط1، دار الجامعة الجديدة، 2022.

5- عبد الحميد العربي الشريف، الأمن القومي في ظل التهديدات الالكترونية – مقاربة قانونية والسياسية، دار الخلدونية، الجزائر، 2020.

6- عبد الكريم أحمد حسن، الاختراق والتجسس الإلكتروني وأساليب الحماية، دار الكتب العلمية، القاهرة، مصر.

7- عبيد المنعم وسام، التحقيق في الجرائم الالكترونية، دار النهضة العربية، بيروت، 2018.

8- عمار محمود، أمن المعلومات والجرائم الالكترونية، دار صفاء للنشر والتوزيع، عمان، 2018.

9- محمد بن مرزوق، الجرائم المعلوماتية في التشريع الجزائري–دراسة مقارنة، دار هومة، الجزائر، 2021.

10- محمد سلامة عبد القوي، التنصت الإلكتروني في القانون الجنائي–دراسة مقارنة، دار النهضة العربية، القاهرة، 2010.

11- محمد عبد العزيز، الجرائم الإلكترونية في القانون الجنائي المعاصر، دار الفكر الجامعي، الإسكندرية، 2021.

12- محمد علي سويلم، الأحكام الموضوعية والإجرائية للجريمة المنظمة، ط1، دار هومة، الإسكندرية، 2007.

13- نصر الدين ماروك، جريمة المخدرات في ضوء القوانين والاتفاقيات الدولية، ط1، دار هومة، الجزائر، 2007.

14- يوسف مراد، الخصوصية في العصر الرقمي، دراسة قانونية مقارنة، ط1، دار الفكر الجامعي الإسكندرية، الإسكندرية، 2021.

2-الأطروحات والرسائل الجامعية:

أ-أطروحة الدكتوراه:

1- عيسى العاقب، حماية الحياة الخاصة، أطروحة دكتوراه، كلية حقوق والعلوم السياسية، قانون خاص، جامعة سعد دحلب، بليدة، 2014

2- محمد رشاد إبراهيم مفتاح، الحماية الجنائية للحق في حرمة الاتصالات الشخصية ، رسالة دكتوراه ، كلية الحقوق ، جامعة الإسكندرية ، 2009.

ب-رسائل الماجستير:

1- جمال غراب، الثبات الالكتروني كآلية لجمع الأدلة الجنائية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، 2021-2022.

2- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر، باتنة، 2011-2012.

3- خليدة أوقاسي، حرمة الحياة الخاصة في قانون الجنائي، دراسة مقارنة في التشريع الجزائري والفرنسي، مذكرة لنيل شهادة ماجستير، كلية الحقوق، القانون والعلوم الجنائية، جامعة الجزائر1، 2014/2013.

ج-مذكرات الماستر:

1- نسيمة بطيحي، الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية القيمة في التشريع الجزائري، رسالة لنيل شهادة الماستر، جامعة الحقوق والعلوم السياسية، سطيف2، الجزائر، 2019/06/30.

3-الموسوعات والمعاجم:

1-ابن منظور، لسان العرب، ط3، مادة نصت، ج14، دار صادر، بيروت، 1414هـ.

4-المجالات:

1- أحمد سلامة، " التنصت في ظل تطور وسائل الاتصال الحديثة "، المجلة الجزائرية للعلوم القانونية، العدد 2، 2020.

2- اسمهان بن مالك، " أثر إجراءات التنصت على حقوق وحريات الإنسان والمواطن "، مجلة البيبان للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، العدد 04، ديسمبر 2017.

3- بن عيسى عبد القادر، " السيادة الرقمية السيبراني في الجزائر بين النصوص القانونية والتحديات الواقعية "، مجلة الدراسات القانونية والسياسية، العدد 15، 2023.

4- جمال بوازدية، " الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "، التحديات والآفاق المستقبلية، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، أفريل2019.

5- دنون يونس صالح المحمدي ومهدي صالح شحادة العبيدي، " التعويض الناشئ على الاعتداءات على حرمة الخاصة "، مجلة جامعة تكريت للحقوق، المجلد 2، الجزء1، العدد3، العراق، مارس 2018.

6- شنة زواوي، " الحماية القانونية للحق في حرمة المحادثات الهاتفية "، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، مخبر المرافق العامة والتنمية، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، العدد 19، جوان 2018.

7- عبد القادر سعدوني، " السيادة الرقمية والأمن القومي في ظل التحولات التكنولوجية "، مجلة الدراسات السياسية والقانونية، العدد 15، جامعة الجزائر3، 2021.

8- عبد القادر يخلف، " الخصوصية الرقمية في ظل التشريعات الحديثة "، مجلة البحوث القانونية والاقتصادية، العدد 15، جامعة الجزائر1، 2022.

9- عقيدة مباركية، " الحماية الجنائية في الخصوصية الرقمية في القانون الجزائري "، مجلة الشريعة والاقتصاد، العدد 13، المجلد 7، 2018.

10- عيسى بوشيبة، " حماية الأسرار التجارية في القانون الجزائري "، مجلة الدراسات القانونية والسياسية، العدد 5، جامعة باتنة 1.

11- فاتح قيشي، " آليات الحق في الخصوصية "، مقال نشر في مجلة حقوق الإنسان، العدد 36، جامعة أدرار، الجزائر.

12- فوزي عمارة، " اعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور والتسرب كإجراءات تحقيق القضائي في المواد الجزائية "، مجلة العلوم الإنسانية، كلية الحقوق والعلوم السياسية، جامعة منتوري، قسنطينة، الجزائر، العدد 33، جوان 2010.

13- مجلة الدليل العملي لحماية المستخدم من التهديدات الإلكترونية، المركز الوطني للوقاية من الجرائم المعلوماتية، الجزائر، 2021.

14- منصور، رضا، " وسائل الحماية التقنية من جرائم المعلوماتية "، مجلة الفكر القانوني، جامعة الجزائر 1، العدد 22، 2021.

15- ياسين بوشامة، " الإشكالية القانونية للتنصت الإلكتروني "، مجلة الدراسات القانونية المعاصرة، العدد 5، 2021.

5-النشرات والقرارات:

أ – النشرات:

1-نشرة أمنية حول التنصت الرقمي والتجسس السيبيراني (CERIST)، مركز البحث بالإعلام العلمي والتقني، الجزائر، 2022.

ب- القرارات:

1- قرار مجلس قضاء الجزائر غرفة الجنح القضية رقم 1123، بتاريخ 2020/12/15.

6- المواقع الإلكترونية:

1- https://itach.dk/index.php/2024/09/07/sp-i
2- https://www.fortinet.com
3- https://tech.mawdoo3.com /
4- WWW.OYEZ.ORG/CASES /1900-1940/277US 438

4- عبد الغاني مزياني، **الجرائم الماسة بأنظمة المعالجات الآلية للمعطيات**، جامعة محمد بوضياف، المسيلة، 2007، المتاح على الموقع التالي:

www.courdemsila.mjstice.dz/conf.msila/doc10.ppt

ثالثا: مراجع باللغة الأجنبية

1- Bruce Schneier, Date and Goliath : The Hidden Battles to Collect Your Data and Control Your World, New York: W.W.Norton & Company, 2015.
2- Edward Snowden, Permanent Record, London: Macmillan, 2019.

قائمـــة الملاحق

الجمهورية الجزائرية الديمقراطية الشعبية

مجلس قضاء.....

محكمة .....

مكتب السيد:..... **إذن باعتراض المراسلات**

قاضي التحقيق الغرفة رقم: .....

رقم النيابة: .....

رقم التحقيق: .....

نحن ..... قاضي التحقيق الغرفة ..... لدى محكمة .....

- بعد الاطلاع على ملف القضية المتبعة ضد: .....

من أجل جناية: تهريب الأسلحة, المنصوص و المعاقب عليها بموجب المادة 14 من القانون رقم 06/05 المتعلق بمكافحة التهريب.

- و بعد الاطلاع على المواد 65 مكرر 5 إلى 65 مكرر 10 من ق إ ج.

- و حيث أن التحقيق أسفر على أن المسمى ..... على علاقة مع المسمى ..... , و أنهما يخططان لتهريب أسلحة .....

و نظرا لمقتضيات التحقيق , و لخطورة الوقائع , و لإظهار الحقيقة , و تفادي أي نتائج خطيرة.

نأذن للسيد: .....ضابط الشرطة القضائية بـــ:

.....

بالقيام باعتراض المراسلات السلكية و اللاسلكية التي تتم بين.....و.....

و تسخير أي عون مؤهل لدى مصلحة أو هيئة عمومية أو خاصة للتكفل بالجوانب التقنية للعملية.

نأذن بهذا الإجراء لمدة أقصاها 04 أشهر من تاريخ هذا الإذن, ما لم نأمر بإيقافها قبل انقضاء هذه المدة.

و على ضابط الشرطة القضائية المنسق للعملية موافاتنا بتقرير حول سيرها.

حرر بكتبنا بتاريخ.....

قاضي التحقيق.....

الجمهورية الجزائرية الديمقراطية الشعبية

مجلس قضاء: .....

محكمة: .....

نيابة الجمهورية:.....

إذن بمباشرة عملية التقاط الصور و تسجيل الأصوات

– نحن وكيل الجمهورية لدى محكمة: .....

– بعد الإطلاع على الطلب المقدم من طرف ضابط الشرطة, رئيس فرقة مكافحة المخذرات, بالمصلحة الولائية للشرطة القضائية بأمن ولاية : .....

تحت رقم 00/00/00 بتاريخ: 0000/00/00

حيث أن التحقيق الجاري يتعلق بجرائم المخذرات, و حيث أن ضرورات التحري و التحقيق تبرر اللجوء إلى عملية تسجيل الأصوات و التقاط الصور.

– بعد الاطلاع على المواد 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية.

نأذن

للسيد: (م م) ضابط الشرطة رئيس فرقة مكافحة المخدرات, بالمصلحة الولائية للشرطة القضائية بأمن ولاية ورقلة بمباشرة عملية اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية و اللاسلكية, ووضع الترتيبات التقنية دون موافقة المعنيين, من أجل التقاط و تثبيت و بث و تسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص.

مع التقيد بأحكام المواد 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية و موافاتنا باستمرار بالنتائج المتواصل إليها.

حرر بـــ ..... بتاريخ: .....

وكيل الجمهورية.....

بعض أجهزة التنصت

كاميرا التنصت

جهاز LAMPHONE

بعض أجهزة لمكافحة التنصت

جهاز كشف التنصت bug detectors

جهاز التشويش Singanl jammers

فهـرس المحتويـات

فهـــرس المحتويـــات

العنـــــوان	الصفحة
مقدمة	**01**
الفصل الأول: الإطار المفاهيمي للتنصت الإلكتروني	
تمهيـد	**07**
المبحث الأول: ماهية التنصت الإلكتروني	**08**
المطلب الأول: مفهوم التنصت الإلكتروني	**08**
الفرع الأول: تعريف التنصت الالكتروني	**08**
أولا: في الشريعة الإسلامية	**09**
ثانيا: في القوانين	**09**
الفرع الثاني: نبذة تاريخية حول التنصت الإلكتروني	**12**
المطلب الثاني: مميزات التنصت الإلكتروني	**13**
الفرع الأول: خصائص التنصت الإلكتروني	**14**
أولا: السرية والخفاء	**14**
ثانيا: الاعتماد على التكنولوجيا المتطورة	**14**
ثالثا: الاتساع في النطاق	**14**
رابعا: السرعة والفعالية في جمع المعلومات	**14**
خامسا: الغموض القانوني	**15**
سادسا: التهديد المباشر للخصوصية	**15**
الفرع الثاني: أنواع التنصت الإلكتروني	**15**
أولا: التنصت عن طريق شبكة السلكية واللاسلكية	**15**
ثانيا: التنصت بواسطة الأقمار الصناعية	**16**
ثالثا: التنصت باستعمال شبكات الهاتف النقال	**16**
رابعا: التنصت باستخدام البرامج الخبيثة	**17**

خامسا: التنصت على لوحات المفاتيح	**17**
الفرع الثالث: تمييز التنصت الإلكتروني مع الأنظمة المشابهة	**17**
أولا: التنصت الالكتروني مع اعتراض المراسلات والتقاط الصور الالكترونية	**17**
ثانيا: التنصت الالكتروني مع التسرب والتجسس الالكتروني	**19**
المبحث الثاني: الأساس التشريعي للتنصت الإلكتروني في الجزائر	**23**
المطلب الأول: النصوص القانونية المنظمة للتنصت الإلكتروني	**23**
الفرع الأول: الاتفاقيات والمؤتمرات الدولية والإقليمية	**23**
الفرع الثاني: الدستور الجزائري	**24**
الفرع الثالث: القوانين المنظمة	**24**
أولا: القانون المدني	**24**
ثانيا: قانون العقوبات	**24**
ثالثا: قانون الإجراءات الجزائية	**25**
المطلب الثاني: الجهات المخولة بإصدار وتنفيذ أوامر التنصت	**28**
الفرع الأول: الجهات القضائية	**28**
أولا: السلطة القضائية	**28**
الفرع الثاني: الجهات المنفذة لأوامر للتنصت	**30**
أولا: الجهات الأمنية	**30**
ثانيا: المؤسسات الخاصة	**31**
المطلب الثالث: حالات وضوابط اللجوء الى التنصت الإلكتروني	**31**
الفرع الأول: حالات اللجوء الى التنصت الإلكتروني	**32**
أولا: جريمة المخدرات	**32**
ثانيا: الجريمة المنظمة العابرة للحدود الوطنية	**32**
ثالثا: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات	**33**
رابعا: جرائم تبييض الأموال	**33**
خامسا: جرائم الإرهاب	**34**

سادسا: جرائم الصرف	**35**
سابعا: جرائم الفساد	**35**
الفرع الثاني: ضوابط اللجوء الى التنصت الإلكتروني	**36**
أولا: استصدار الإذن القضائي	**36**
ثانيا: شروط استصدار الإذن القضائي	**37**
خلاصة الفصل	**39**
الفصل الثاني: المخاطر المرتبطة بالتنصت الإلكتروني في الجزائر	
تمهيـد	**41**
المبحث الأول: آليات التصدي للمخاطر المرتبطة بالتنصت الإلكتروني	**42**
المطلب الأول: آليات الحماية من التنصت الإلكتروني	**42**
الفرع الأول: استراتيجية الأمن السيبراني	**42**
أولا: تعريف الأمن السيبراني	**43**
ثانيا: التعريف الإجرائي	**44**
ثالثا: استراتيجية الجزائر الوطني للأمن السيبراني	**45**
الفرع الثاني: التوعية والتثقيف كآلية حماية من مخاطر التنصت الالكتروني في الجزائر	**48**
أولا: مفهوم التوعية والتثقيف السيبراني	**48**
ثانيا: أهمية التوعية والتثقيف	**49**
ثالثا: دور التوعية والتثقيف في الوقاية من التنصت الالكتروني	**49**
رابعا: مظاهر التوعية في الجزائر	**50**
خامسا: جهود الجزائر في التوعية من التنصت الالكتروني	**50**
سادسا: تحديات تطبيق التوعية في الجزائر	**51**
سابعا: مقترحات لتعزيز التوعية	**51**
المطلب الثاني: التقنيات والأدوات الوقائية	**51**
الفرع الأول: التقنيات الوقائية	**52**

أولا: التشفير كوسيلة وقائية أساسية	**52**
ثانيا: استخدام الشبكات الافتراضية الخاصة	**53**
ثالثا: جدران الحماية وبرمجيات مكافحة الاختراق	**53**
رابعا: التحكم في الأذونات والتحديثات الدورية	**53**
خامسا: التوعية والتدريب التقني	**54**
سادسا: اعتماد برامج مفتوحة المصدر	**54**
سابعا: الأمن السيبراني	**54**
ثامنا: استخدام أجهزة الاتصال الآمنة	**54**
تاسعا: الحماية	**54**
عاشرا: شبكة الرصد	**55**
الفرع الثاني: الأدوات الوقائية	**55**
أولا: تعريف الأجهزة الوقائية من التنصت الالكتروني	**55**
ثانيا: أبرز أنواع الأجهزة والأدوات الوقائية	**56**
ثالثا: بعض أنواع أجهزة التنصت	**57**
رابعا: واقع استخدام الأجهزة الوقائية في الجزائر	**58**
خامسا: التحديات القانونية المرتبطة باستخدام الأجهزة الوقائية	**58**
المبحث الثاني: صور مخاطر المرتبطة بالتنصت الإلكتروني	**59**
المطلب الأول: صور مخاطر التنصت الالكتروني على الأفراد	**59**
الفرع الأول: مخاطر انتهاك الخصوصية	**59**
أولا: الاعتداء على سرية الاتصالات والمراسلات	**60**
ثانيا: تصوير الأشخاص أو تسجيلهم دون رضاهم	**60**
ثالثا: المعالجة غير المشروعة للمعطيات الشخصية	**60**
رابعا: المراقبة الالكترونية والتنصت بدون سند قانوني	**61**
خامسا: النشر العلني للمعلومات الخاصة عبر الوسائط الرقمية	**61**
الفرع الثاني: مخاطر الابتزاز والتشهير	**62**

أولا: الابتزاز الالكتروني والتهديد بنشر معلومات خاصة	**62**
ثانيا: التشهير والمس بالسمعة عبر الوسائط الرقمية	**63**
ثالثا: التحريض على التشهير أو نشر المحتوى المسيء	**63**
رابعا: استغلال الصور والفيديوهات بقصد الاضراب	**64**
المطلب الثاني: صور مخاطر التنصت الالكتروني على المؤسسات والأمن القومي	**64**
الفرع الأول: صور التنصت الالكتروني على المؤسسات	**64**
أولا: اختراق البيانات الإدارية والوثائق السرية	**65**
ثانيا: التنصت الصناعي وتفويض التنافسية	**66**
ثالثا: تعطيل الأنظمة المعلوماتية للمؤسسة	**68**
الفرع الثاني: مخاطر التنصت الالكتروني على الأمن القومي	**70**
أولا: المساس بالمصالح الاستراتيجية للدولة	**70**
ثانيا: تسريب معلومات تمس الأمن العسكري أو الأمن العام	**72**
ثالثا: إثارة الفوضى وزعزعة الاستقرار السياسي	**74**
رابعا: تهديد السيادة الرقمية	**76**
خلاصة الفصل	**78**
خاتمة	**80**
قائمة المصادر والمراجع	**83**
قائمة الملاحق	**91**
فهرس المحتويات	**95**

الملخص:

تُعالج هذه المذكرة موضوع النظام القانوني للتنصت الإلكتـــروني في التشريع الجزائري، حيث اعتمدت هذه الدراسة على عرض مختلف المفاهيم من خلال تعريف التنصت الإلكتروني وذكر مميزاته وأنواعه، مع تمييزه بالمفاهيم مشابهة له كالتجسس واعتراض المراسلات. كما تم استعراض النظام القانوني الذي يؤطره في الجزائر، مستندًا إلى الدستور والقوانين العقابية والإجرائية التي تبين الضوابط التي تحكم مشروعية هذا الإجراء مع ذكر الجهات الوصية.

كما شملت الدراسة على ابراز المخاطر المرتبطة بالتنصت الإلكتروني، خاصة فيما يتعلق بانتهاك الخصوصية والابتزاز والتشهير، وتأثيره على المؤسسات والأمن القومي. كما تناولت ايضا آليات الحماية المعتمدة في الجزائـــر، من خلال استراتيجيـــة الأمن السيبراني، وتدابير التوعية والتثقيف، إضافة إلى استعمال التقنيات والأدوات الوقائية مثل التشفير وبرامج مكافحة التجسس وأجهزة كشف التنصت.

كلمات مفتاحية: التنصت الإلكتروني، انتهاك الخصوصية، أجهزة كشف التنصت.

Abstract:

This note deals with the subject of the legal regime of electronic eavesdropping in Algerian legislation. This study relied on the presentation of various concepts by defining electronic eavesdropping and stating its characteristics and types, while distinguishing it from similar concepts such as espionage and interception of correspondence. The study also reviewed the legal system that frames it in Algeria, based on the constitution and the penal and procedural laws that outline the controls governing the legality of this procedure, as well as the competent authorities.

The study also highlighted the risks associated with electronic eavesdropping, especially with regard to privacy violations, blackmail and defamation, and its impact on institutions and national security. It also addressed the protection mechanisms adopted in Algeria, through the cyber security strategy, awareness and education measures, in addition to the use of preventive techniques and tools such as encryption, anti-spyware programmes and eavesdropping detection devices.

Keywords: electronic eavesdropping, invasion of privacy, eavesdropping detectors.