"التجسس الإلكتروني وسلوكياته"

"Electronic espionage and its behaviors"

يزن كامل الأباظة

المستخلص:

في ظل التطور الهائل الذي يشهده العالم في مجال تقنية المعلومات أصبحت الحاجة ماسة وضرورية إلى حماية المعلومات الإلكترونية خاصةً منها ما يتسم بطابع السرية؛ حيث برز على السطح أنواعاً من الجرائم الإلكترونية لم تكن موجودة في السابق، ولعل التجسس الإلكتروني يأتي في مقدمة هذه الجرائم التي وضعت المجتمع الدولي في تحدٍ كبير للحد منه على أقل تقدير، والشريعة الإسلامية – بصلاحيتها لكل زمان ومكان عالجت موضوع التجسس بصفته التقليدية ووضعت له الأحكام المختلفة، وأطرت له القواعد الفقهية المناسبة.

Abstract:

In light of the tremendous development that the world is witnessing in the field of information technology, the need has become urgent and necessary to protect electronic information, especially that which is confidential. Where types of electronic crimes have emerged that did not exist previously, and perhaps electronic espionage comes at the forefront of these crimes, which has placed the international community in a major challenge to reduce it, at the very least, and Islamic law - with its validity for all times and places, has addressed the issue of espionage in its traditional capacity and established provisions for it. different, and appropriate jurisprudential rules were framed for it.

الكلمات المفتاحية:

التجسس الإلكتروني، الجماعات الإرهابية، النظام المعلوماتي، التصريح بالدخول، البريد الإلكتروني.

key words:

Electronic espionage, terrorist groups, information system, access authorization, E-mail.

المقدمة

إن عالم الإجرام عرف تطوراً كبيراً ببروز مجموعة من الجرائم المستحدثة التي تعتمد على أساليب متطورة، ومن أبرز هذه الجرائم ما اصطلح عليه التجسس الالكتروني أو المعلوماتي الرقمي حيث يعتبر التجسس الالكتروني من أبشع وأخطر الجرائم التي ترتكب عبر الانترنت وتهدد العالم بعصره الآلي، حيث يستغل الساحة المعلوماتية أو الفضاء الالكتروني من خلال إنشاء حسابات خاصة للإرهاب في مواقع الانترنت لنشر التطرف والفكر الإرهابي.

تحرص كل دولة من الدول على تحقيق حماية فاعلة لوجودها واستقلالها والحفاظ على أمنها الدفاعي والسياسي والاقتصادي ومركزها الخارجي من مخاطر العدوان، إذ ليس هناك ما هو أكثر أهمية من حماية تلك المصالح الأساسية للدولة، والتي هي محط أنضار المشرع وهدفه الأساسي، لان حماية هذه المصالح تؤدي إلى تحقيق التقدم والرقي من ناحية، وتأمين هذه المصالح من ناحية أخرى، لذا سعى المشرع إلى حماية هذه المصالح من مصادر الاعتداء المختلفة سواء كانت داخلية أم خارجية.

ولما كان حق الدولة في حماية أمنها الخارجي أمراً غاية في الأهمية استدعى تدخلها بتجريم كافة الأنشطة التجسسية الماسة بأمنها وسيادتها، معتبرة إياه واجب أساسياً تلتزم به مثلما هو حق لها، فللدولة، شخصيتها المعنوية التي تستدعى ممارسة هذا الحق في الدفاع عن وجودها وكيانها وإحاطة أسرارها بسياج من الحماية الجنائية حرصاً عليها من الانتهاك.

وتتكبد الدول خسائر مالية ضخمة نتيجة تعرضها للتجسس الإلكتروني وخسارتها لأسرار تمس بأمنها السياسي والاقتصادي والعسكري، تضاف إليها تكاليف عالية تتكبدها من أجل حماية أسرارها، يزيد منها عدم القدرة على حصر المخاطر المتأتية من شبكة الإنترنت وسوء استعمالها. وهي تكاليف تجاوز أضعاف تلك التي يجب تكبدها لمواجهة التجسس التقليدي

الذي قد يكفي فيه حفظ الأسرار في أماكن مادية مغلقة وحصر الدخول إليها بعدد محدود جدا من الأشخاص [1].

يحصل التجسس الإلكتروني، من خلال الدخول غير المشروع إلى نظام معلوماتي والتعرف إلى المعلومات المخزنة فيه من غير الإضرار بها عن طريق الاطلاع عليها أو استخراجها من غير أن ينجم عن هذا الاستخراج أي تعطيل أو تخريب في برامج الحاسوب، أو يحصل من خلال التقاط الموجات الكهرومغناطيسية المنبعثة من حاسب آلي باستخدام آلات خاصة لذلك، من دون الحاجة إلى الدخول مباشرة داخل الشبكة، للوصول إلى المعلومات التي يحتويها، وهو ما يسمى بالاعتراض ويقصد بالمعلومات بطبيعة الحال تلك المتمتعة بالسرية، لا تلك المباحة والمتاحة لجمهور متصفحي شبكة الإنترنت.

أهمية البحث:

تبرز أهمية دراسة التجسس الالكتروني على اعتباره ظاهرة إجرامية خطيرة، تستوجب الدراسة والبحث والتحليل من أجل تأمين أفضل حماية للأفراد والدول من خطر هذه العمليات الأمر الذي يتطلب من الدول إيجاد تشريعات مستحدثة ومواكبة للتطور الدائم في الوسائل التقنية لمواجهة هذه الظاهرة الخطيرة.

إشكالية البحث:

إن الطبيعة الخاصة لجريمة التجسس الإلكتروني والتي يصعب معها تحديد المدلول القانوني للتجسس بسبب تطوره وتشعب أفعاله لكونه يمس جوانب متغيرة ومتجددة عسكرية وسياسية واقتصادية وتجارية، بل وقد تكون علمية واجتماعية تحتاج إلى تحليل العناصر القانونية والموضوعية التي تسهم في تشكيل صور جريمة التجسس، وإيجاد الرابط المكون لنشاط

---

[1] محمد حماد مرهج الهيتي، الجريمة المعلوماتية، الطبعة الاولى، دار الكتب القانونية، مصر، 2014، ص141.

التجسس، من هنا تأتي إشكالية البحث، والتي يمكن التعبير عنها من خلال التساؤل الرئيس الآتي:

ما هي السلوكيات المختلفة لجريمة التجسس الإلكتروني؟

منهجية البحث:

سأتبع في هذه الدراسة المنهج التحليلي من أجل قراءة وفهم وتحليل النصوص القانونية المبينة لعملية التجسس الإلكتروني في التشريع اللبناني، من أجل شرحها وتوضيحها واستخلاص النتائج منها، ومعرفة مدى قدرتها وفاعليتها في الحد من انتشار هذا الإرهاب المستحدث، كما سنعتمد على المنهج المقارن لمقارنة الأحكام التي نظم من خلالها المشرع اللبناني هذه الجريمة مع ما يقابلها في بعض التشريعات المقارنة كلما دعت الحاجة لذلك.

المطلب الأول

دخول نظام معلوماتي بشكل غير مشروع

عرفت المجتمعات البشرية التجسس منذ نشأتها، فهي جريمة قديمة قدم التاريخ، وسعى كل تجمع لمعرفة ما لدى التجمعات الأخرى من أسرار ومعلومات، واعتبره ضروريا لتقرير مصير الحروب ورجحان كفة الأطراف المتقاتلة.

وزادت أهمية المعلومات مع بلوغ البشرية العصر الرقمي حيث باتت الدول تعتمد في تسيير مرافقها ومنشآتها على نظم المعلومات التي باتت مخازن لأسرارها ووثائقها الحكومية، وتحوّل التجسس من الطرق التقليدية التي تقوم على تجنيد أشخاص ذوي قدرات بدنية وذهنية عالية وتدريبهم سنوات عدة قبل دسهم في دولة أخرى إلى عمليات تجسس إلكترونية واختراق النظم معلومات الدولة.

ينصب فعل الدخول على النظام المعلوماتي أو على نظام المعالجة الآلية، وهو مصطلح حديث ظهر استخدامه بعد دمج وسائل الحوسبة بوسائل الاتصال، فلم يعد الحاسوب يقتصر على تلك الآلة التي نعرفها بشكلها التقليدي بل بات يشمل أيضا الهاتف الذكي وساعة اليد الذكية والتلفاز الرقمي [2].

الدخول إلى نظام معلوماتي هو نشاط ذهني يقوم به الجاني ويطلق عليه الدخول المنطقي [3]، وهو يشمل كل الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة أو السيطرة على المعطيات التي يتكون منها أو الخدمات التي يقدمها، أيا كانت الوسيلة المستخدمة لذلك، سواء تمثلت باستخدام كلمة السر الحقيقية غير المخوّل للجاني استخدامها، أو من

---

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي "دراسة قانونية متعمقة في القانون المعلوماتي"، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2007، ص 347

[3] حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها، دراسة مقارنة، مكتبة بدران الحقوقية صيدا – لبنان الطبعة الأولى، 2017، ص449.

خلال استخدام الجاني لبرنامج مخصص للدخول إلى أنظمة المعلومات، أو استخدامه لحساب شخص مرخص له بالدخول، ويستوي أن يحصل هذا الدخول باستخدام حاسب آلي أو هاتف ذكي أو غيرها من أجهزة الحوسبة. ويرى بعضهم أنه لا يتحقق إذا اقتصر دور الجاني على قراءة شاشة الحاسب الآلي فقط [4].

ونعتقد بأنه يمكن في هذه الحال اعتبار الفعل تجسسا بالمعنى التقليدي متى ما تمكن الجاني من الاطلاع على المعلومات التي ظهرت على الشاشة ونقلها إلى مشغله، ويأخذ هذا الفعل صورة سرقة المعلومات أو الاستحصال عليها التي تناولها المشرع اللبناني في المادة /282/ من قانون العقوبات.

ويشترط في هذا النظام ألا يكون مباحاً مفتوحاً أمام الجمهور، بل يقتضي أن يكون الحق في الدخول إليه مقتصراً على عدد محدد من الأشخاص. لذا فإن الدخول إلى نظام معلوماتي ليس بحدّ ذاته فعلاً غير مشروع ما لم يتم ضد إرادة المسؤول عن النظام أو بغير تصريح منه، لذا يسمى بالدخول غير المشروع أو غير المصرح به على أنه لا يشترط لاعتبار الدخول غير مشروع أن يكون النظام متمتعاً بحماية فنية، فيتم خرقها، ويرى بعضهم أن هذه الحماية تشبه تحوّط المجني عليه من تعرضه لأي اعتداء يطال شخصه أو ماله الذي لا يمكن بأي حال من الأحوال أن يكون شرطًا للتجريم [5].

يتحقق الدخول غير المشروع أو غير المصرح به، عندما لا يكون هناك تصريح بالدخول أصلا من قبل الشخص المسؤول عن النظام أو عندما يتجاوز الجاني التصريح الممنوح له، سواء من ناحية مجال التصريح، كأن يكون مصرحًا له بالدخول إلى جزء من النظام فيدخله

---

[4] بهاء المري، شرح جرائم تقنية المعلومات، القانون رقم 175 لسنة 2018، منشأة المعارف، الإسكندرية، مصر، 2019، ص 79.

[5] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص 351.

كله، أو يدخل إلى جزء آخر غير ذلك المصرح له بدخوله، أو أن يتجاوز الغرض الذي من أجله صرح له بالدخول.

والدخول غير المشروع هو بهذا المعنى فعل إيجابي يصدر عن الجاني ولا يقع صدفة أو بطريق الخطأ. فهو عمل عمدي يتطلب القصد الجزائي بعنصريه العلم والإرادة. فيتمثل العلم، بمعرفة الجاني أنه يدخل إلى نظام معلوماتي مملوك لغيره من غير رضاء هذا "الغير"، ومع ذلك تنصرف إرادته إلى الدخول إلى هذا النظام [6].

نادراً ما يحصل الدخول غير المشروع أو غير المصرح به بغير علم الجاني أو بخطأ منه، كونه غالبًا ما يكون مجرما يتمتع بالخبرة. لكن إذا حصل هذا الدخول غير المشروع بطريق الخطأ، واستمر الشخص بالبقاء داخل النظام المعلوماتي بعد تبينه لخطئه وعلمه أنه غير مصرح له بالدخول تحقق ما يسمى فعل البقاء غير المشروع [7].

ويتحقق فعل البقاء غير المشروع إذا حصل الدخول إلى النظام المعلوماتي بطريق الصدفة لكن الفاعل آثر البقاء فيه، فكان من المهم بمكان تجريم هذا الفعل بهدف التصدي لمن كان دخوله إلى النظام المعلوماتي بحسن نية وانتفى لديه القصد الجنائي ومع ذلك بقي داخل النظام وانصرفت إرادته لذلك.

---

[6] نائلة عادل محمد فريد قورة، جرائم المعلوماتية الاقتصادية، الطبعة الاولى، دار النهضة العربية، 2004، ص 321

[7] هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، الطبعة الاولى، دار النهضة العربية، 2009، ص16.

ويتحقق فعل البقاء غير المشروع أيضًا إذا حصل الدخول بطريقة مشروعة أي بموافقة المسؤول عنه لكن كانت الموافقة مشروطة بمدة زمنية محددة، فتجاوزها الجاني، ليصبح كل وجود له بعد انقضاء هذه المدة بقاء غير مشروع داخل النظام المعلوماتي [8].

ولا فرق بين الدخول غير المشروع وبين البقاء غير المشروع داخل النظام المعلوماتي بعد الدخول إليه بطريق الخطأ أو بطريق الصدفة من حيث وجوب التجريم، لأن كليهما يؤدي إلى نتيجة جرمية واحدة تتمثل بوصول الجاني إلى نظام معلوماتي غير مصرح له بالدخول إليه، ولأن المصلحة المحمية هي واحدة في الحالين، وهي النظام المعلوماتي وما يتضمنه من معلومات لا يجوز الوصول إليها إلا من قبل أشخاص لهم الحق في ذلك.

ويرى بعضهم أن فعل الدخول غير المشروع فعل منفصل عن فعل البقاء غير المشروع، فالأول يتحقق منذ اللحظة الأولى للدخول فعلا إلى النظام المعلوماتي وهو أمر يستمر مدة قصيرة جداً من الزمن، بعدها يبدأ فعل البقاء غير المشروع. ونكون في هذه الحالة أمام اجتماع مادي أو تعدد مادي للجرائم، على اعتبار أن فعل البقاء غير المشروع هو فعل مستقل تماماً عن فعل الدخول غير المشروع إذ بإمكانه أن يتحقق وإن سبقه دخول مشروع، متى كان هذا الدخول مشروطًا بمدة زمنية معينة أو نطاق معين داخل النظام المعلوماتي، فتجاوزه الجاني [9].

في حين يرى البعض بأنه متى تحقق فعل الدخول غير المشروع كان البقاء غير المشروع داخل النظام المعلوماتي هو الأثر الجرمي المترتب على فعل الدخول غير المشروع وليس جرمًا ثانيًا تاليا له، أما إذا انتفى فعل الدخول غير المشروع فمن الممكن أن يتحقق فعل

---

[8] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم المعلوماتية، الطبعة الاولى، دار النهضة العربية، 2009، ص 78.

[9] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، المرجع السابق، ص 361

البقاء غير المشروع، كأن يكون الدخول مشروعًا لكن مشروطًا بمدة معينة فتجاوزها الجاني، أو إذا حصل الدخول بطريق الخطأ واستمر الجاني داخل النظام إلى الرغم من علمه بخطئه. هذا ويفترض فعل الدخول غير المشروع أو غير المصرح به وقوع نشاط سابق عليه يتمثل بتشغيل الجاني للحاسب الآلي[10].

تناول المشرع اللبناني فعل الدخول غير المشروع وفعل البقاء غير المشروع كفعلين جرميين قائمين بحدّ ذاتهما، في الفقرة الأولى من المادة /110 من قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي مستخدما تعابير الوصول أو الولوج"، "بنية الغش"، "المكوث فيه"، فنصت على أنه يعاقب بالحبس من ثلاث أشهر إلى سنتين وبالغرامة من مليون إلى عشرين مليون ليرة لبنانية أو بإحدى هاتين العقوبتين، كل من أقدم بنية الغش على الوصول أو الولوج إلى نظام معلوماتي بكامله أو في جزء منه، أو على المكوث فيه". ثم شدّد العقوبة تلك في الفقرة الثانية من هذه المادة متى نتج عن هذا الدخول أو البقاء إلغاء البيانات الرقمية أو البرامج المعلوماتية أو نسخها أو تعديلها، أو نتج عن أي منهما المساس بعمل النظام المعلوماتي.

بدوره عالج المشرع السوري فعل الدخول غير المشروع في البند /أ/ من المادة //15/ من قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية الذي نص على أنه يعاقب بالغرامة من عشرين ألفاً إلى منة ألف ليرة سورية كل من دخل قصدًا بطريقة غير مشروعة إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني على الإنترنت دون أن يكون له الحق أو يملك الصلاحية أو التصريح بالقيام بذلك." وفي البند /ب/ من هذه المادة شدّد المشرع السوري العقوبة إلى الحبس والغرامة في حال قام الفاعل بنسخ البيانات أو المعلومات

[10] عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2011، ص 27.

أو التصاميم التي وصل إليها أو إلغائها أو تغييرها أو تشويهها أو تزييفها أو استخدامها أو إفشائها [11].

أما المشرع المصري فكان أكثر تفصيلا بتناوله هذا الفعل بطريقتيه الدخول غير المشروع والبقاء غير المشروع في قانون مكافحة جرائم تقنية المعلومات، فنص في الفقرة الأولى من المادة /14/ منه على أنه: "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مئة ألف جنيه، أو بإحدى هاتين العقوبتين كل من دخل عمداً، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه".

ثم نص في المادة /15/ من هذا القانون على أنه يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدمًا حقًّا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول".

وشدد العقوبة بموجب المادة /34/ من هذا القانون وجعل الفعل جناية في حال وقع الفعل بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع ممارسة السلطات العامة لأعمالها أو عرقلتها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي[12].

---

[11] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، الطبعة الاولى، دار النهضة العربية، 2011، ص32.

[12] عمر عباس خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، 2021، ص 30.

المطلب الثاني

الاعتراض غير المشروع لإرسالات نظام معلوماتي

يقصد بالاعتراض غير المشروع أو غير المصرح به معرفة محتوى الاتصال الذي يحصل داخل نظام واحد أو بين نظامين مختلفين أو عدة أنظمة ترتبط بعضها ببعض بشبكة معلوماتية، من خلال التقاط المعلومات التي يتضمنها هذا الاتصال.

من هنا ذهب بعضهم إلى أن الاعتراض قد يحصل إما من خلال الدخول إلى شبكة المعلومات أو الاتصالات، أو من خلال التقاط الإشارات المنبعثة عن النقل الإلكتروني للمعلومات باستخدام وسائل فنية من غير الحاجة إلى الدخول مباشرة داخل الشبكة. لذا فهو ليس إلا نموذجًا من نماذج الدخول غير المشروع، ذلك أن المشرع عندما يجزم الدخول فهو لا يشترط لذلك استعمال النظام، فمن الممكن أن يحصل دخول إلى النظام من غير أن يتلوه أي استعمال له وأنه إذا كان كل استعمال للنظام يعد بلا ريب دخولا إليه، فإن الدخول لا يعني بالضرورة استعمال هذا النظام، ومثله ذهب آخرون [13] إلى أن الدخول غير المشروع إلى نظام معلوماتي قد يحصل إما بطريقة مباشرة أي عبر الدخول مباشرة إلى الحاسب الآلي الذي يحتوي على هذا النظام، أو بطريقة غير مباشرة أي عندما يدخل الجاني إلى النظام بواسطة نظام آخر يتصل بالأول بشبكة اتصالات وذلك عن طريق اعتراض النظام الأول. وعليه، فإنه لا يشترط وقوع أي نشاط سابق على هذا الدخول.

في حين ذهب رأي آخر [14] إلى أن الدخول غير المشروع فعل مستقل تماماً عن فعل الاعتراض غير المشروع، وميّز بينهما، بأن الأول يفترض بل يتطلب أن يقوم الجاني بنفسه

---

[13] علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، الطبعة الاولى، منشورات زين الحقوقية، 2013، ص570.

[14] كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت، 2017، ص67

بتشغيل الحاسب الآلي، في حين أنه في الثاني يكون الحاسب الآلي مشغلا إما من قبل المسؤول عنه، أو من قبل شخص غيره ويقتصر دور الجاني على اعتراض المعلومات أو البيانات المرسلة منه فقط. ومثله آخرون ذهبوا إلى أن فعل الدخول غير المشروع يتطلب حكمًا نشاطًا سابقًا عليه يتمثل في إقدام الجاني على تشغيل الحاسب الآلي، أما الاعتراض غير المشروع فيحصل بعد تشغيل الحاسب الآلي بواسطة شخص آخر غير الجاني، الذي يقتصر دوره على اعتراض النظام المعلوماتي بعد تشغيل الحاسب الآلي للوصول إلى المعلومات التي يتم إرسالها، والتي يرجح أن تكون مفيدة له نظرًا إلى أن الجاني هو من يقوم بتحديد المكان الذي يقوم بالتقاط المعلومات منه في النظام المعلوماتي لكن يبقى أن الاعتراض غير المشروع أو غير المصرح به شانه كالدخول غير المشروع، فكلاهما يؤدي إلى نتيجة واحدة تتمثل بالوصول إلى معطيات غير مصرح للجاني بالوصول إليها [15].

ويرى بعضهم [16] أن التجسس الإلكتروني يحصل بمعظمه عن طريق التقاط المعلومات عن بعد أي اعتراضها.

في حين يرى بعض آخر أن الاعتراض هو جريمة مستقلة عن جريمة التجسس الإلكتروني كونه يحصل بعد تشغيل الحاسب الآلي، أما التجسس فيحصل بطريق الاختراق الذي يفترض تشغيل الحاسب الآلي، أي بطريق الدخول غير المشروع أو غير المصرح به. ومثله يرى آخرون أن الاختراق أو الدخول غير المشروع، يختلف تماما عن التنصت المتمثل باعتراض الرسائل المرسلة بواسطة الحاسب الآلي، وأن التجسس الإلكتروني يحصل بعد اختراق النظام المعلوماتي وذلك بالاطلاع على محتوياته.

---

[15] هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 2003، ص23.

[16] عمار عباس الحسيني، جرائم الحاسوب والانترنت (جرائم المعلوماتية)، الطبعة الاولى، منشورات زين الحقوقية، بيروت، 2017، ص 323.

ويمكن تشبيه الاعتراض بالتنصت على مكالمة هاتفية [17]، لذا نرى القانون العربي الاسترشادي استخدم تعبير "التنصت" إلى جانب التعبيرين "الاعتراض" و "الالتقاط" في المادة /8/ منه المذكورة أعلاه.

يتمثل السلوك المادي لهذه الجريمة في قيام الفاعل بالتدخل غير المشروع لمعرفة محتوى الإتصالات التي تتم 8بر شبكات المعلومات داخل نظام المعلوماتية، أو بين أنظمة معلوماتية مختلفة حيث يقوم بالتقاط المعلومات المتضمنة في هذا الإتصال.

الوسيلة الأساسية لإعتراض أنظمة المعلوماتية تتمثل في استخدام الموجات الكهربائية الصادرة عن النظام (Electromagnetic Radiation)، فاعتراض نظام المعلوماتية كما هو معروف في الولايات المتحدة الأمريكية باسم التقاط الموجات الكهربائية (Pikup Electromagnetic) هو جمع للمعلومات عن بعد.

يختلف الدخول غير المصرح به إلى نظام المعلوماتية عن اعتراض هذا النظام من حيث النشاط الإجرامي في كل منهما، فالدخول إلى النظام لا يتأتى إلا بتشغيله للولوج إلى ما يحتوي عليه من معلومات، أما في حالة التقاط المعلومات عن طريق اعتراض النظام فإن عملية تشغيله تكون قد بدأت بالفعل بواسطة شخص آخر غير الجاني، واقتصر دور الفاعل على اعتراضه للوصول إلى المعلومات التي تتضمنها عملية الإتصال.

أدت هذه الإختلافات بين الدخول إلى نظام المعلوماتية وبين اعتراضه إلى الإتجاه نحو إفراد نص خاص بتجريم كل منهما، وقد أوصى المجلس الأوروبي بضرورة إفراد نص خاص لإعتراض أنظمة المعلوماتية يتم بمقتضاه تجريم كل اعتراض لاتصال يتم من أو إلى أو داخل أنظمة المعلوماتية عبر شبكات الإتصالات.

---

[17] أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2014، ص266.

سارت عدة دول على هذا النهج وجرمت سلوك الإعتراض بنصوص خاصة وواضحة،من ذلك مثلا قانون العقوبات الكندي الذي جاء في مادته 430/1 [18].

كما عاقبت المادة 342 من القانون ذاته كل شخص يسعى باستخدام وسائط مغناطيسية، صوتية، أو ميكانيكية أو أي أداة أخرى لوقف أو اعتراض أو التسبب باعتراض بصورة مباشرة أو غير مباشر أي وظيفة لنظام المعلوماتية.

لم يتناول المشرع اللبناني في قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي فعل الاعتراض لإرسالات النظام المعلوماتي. ويرى بعضهم [19]، أن القانون الذي يرمي إلى صون الحق بسرية المخابرات التي تجري بواسطة أي وسيلة من وسائل الاتصال [20]، تناول هذا الجرم، فيكون من غير الضروري إيجاد نص آخر للتجريم.

وقد نصت المادة / 1 / من هذا القانون على أن: "الحق في سرية التخابر الجاري داخلياً وخارجيا بأي وسيلة من وسائل الاتصال السلكية أو اللاسلكية الأجهزة الهاتفية الثابتة، والأجهزة المنقولة بجميع أنواعها بما فيها الخليوي، والفاكس، والبريد الإلكتروني...) مصون وفي حمى القانون ولا يخضع لأي نوع من أنواع التنصت أو المراقبة أو الاعتراض أو الإفشاء إلا الحالات التي ينص عليها هذا القانون وبواسطة الوسائل التي يحددها ويحدد أصولها".

---

[18] المادة 430/1على معاقبة كل شخص يقترف عن قصد أدى باعتراض سبيل أو مقاطعة أو تدخل مع أي شخص في الاستخدام القانوني للبيانات.

[19] ضياء كاظم الكناني، الإرهاب وسائل مكافحته، الطبعة الأولى، منشورات دار السنهوري، بغداد، 2017، ص 51 – 52.

[20] القانون رقم / 140/ تاريخ 27-1-1999، نشر في عدد الجريدة الرسمية رقم /02/ تاريخ 3/11/1999، ص 3160، وهو نافذ منذ تاريخ نشره سندا إلى المادة/22/ والأخيرة منه.

ثم نصت المادة /17/ منه على أنه يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من خمسين إلى مئة مليون ليرة لبنانية كل شخص يعترض أي مخابرة خلافًا لأحكام هذا القانون يعاقب بالعقوبة عينها كل من حرّض أو اشترك أو تدخل في الجرم أو استنسخ أو احتفظ أو أفشى معلومات استحصل عليها لدى اعتراض المخابرات بناء على تكليف السلطة المختصة أو أقدم على اعتراض المخابرات في غير الأماكن المحددة في قرار الاعتراض [21].

ونحن نرى أن نص المادة /1/ المذكورة أعلاه قابل للتطبيق في حالة الاعتراض غير المشروع لإرسالات نظام معلوماتي بأي طريقة كانت خاصة أن النص أورد عبارة "التخابر " وليس "التهاتف" فلم تقتصر على التخابر بواسطة الهاتف. ثم عدّد وسائل التخابر على سبيل المثال بدليل إطلاقه للتعداد بوضع النقاط الثلاث بعد عبارة "البريد الإلكتروني". وذكر الهواتف الخلوية التي باتت اليوم هواتف ذكية وتعد في الوقت عينه حاسبًا آليا، وهي تعمل بنظم المعالجة الآلية كما صار بيانه أعلاه، أي تلك النظم الناجمة عن دمج وسائل الحوسبة بوسائل الاتصال. وذكر أيضاً البريد الإلكتروني وهو وسيلة تخابر تتم عبر شبكة المعلومات أي شبكة الإنترنت ليطلق التعداد بعدها، فتكون كل وسيلة تخابر تتم عبر شبكة معلوماتية داخل نظام واحد أو تجمع بين نظامين أو أكثر داخلة ضمن هذا التعداد.

أما المشرع السوري فقد تناول فعل الاعتراض غير المشروع في الفقرة الأولى من المادة /18/ من قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية التي نصت على أنه يعاقب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من اعترض أو التقط قصدًا بوجه غير مشروع المعلومات المتداولة على منظومة معلوماتية أو الشبكة أو تنصت عليها"[22].

---

[21] المادة /17/ قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي لسنة 2018.

[22] هلالي عبد اللاه أحمد، جرائم الحاسوب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية القاهرة، 2015، ص 27-28.

بدوره فرق المشرع المصري بين فعل الدخول أو البقاء غير المشروع وبين فعل الاعتراض واعتبر كل منهما جريمة مستقلة [23] فنص في المادة /16/ من قانون مكافحة جرائم تقنية المعلومات على أنه: "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها".

وبالتالي نلاحظ نجاح الإرهابيين في توظيف التقنيات التكنولوجية الحديثة في خدمة إجرامهم، وتوسيع نطاق عملهم، وقد انتشر هذا النوع من الإرهاب المعاصر إلى درجة أصبح له تصنيف خاص تحت اسم "التجسس الإلكتروني"، والذي ينطوي على استخدام كافة وسائل التقنيات الحديثة لخدمة العمليات الإلكترونية، والتي باتت تتخذ مظاهر وأشكال مختلفة، مثل تحقيق وتسهيل التواصل بين المجموعات الإرهابية المتباعدة، أو الهجوم على المواقع الالكترونية وتخريب نظم المعلومات، أو خرق نظم معلوماتية بشكل غير مشروع والتجسس على بياناتها، لذلك أصبحت مواجهة ظاهرة التجسس الالكتروني ومخاطره، من أهم التحديات التي تواجه التشريعات الوطنية المعاصرة، من أجل إحداث إطار قانوني معاصر، يحد من انتشار هذه الجرائم المستحدثة.

[23] هشام فريد رستمّ، قانون العقوبات ومخاطر تقنيّة المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 2009، ص198.

الخاتمة

إن التجسس الالكتروني وليد التطور العلمي الهائل ومن مفرزات الثورة التكنولوجيا حيث يعد من الجرائم المستحدثة الذي يعتمد على الموارد المعلوماتية على عكس الإرهاب التقليدي، وهو إرهاب المستقبل، والهاجس الأكبر لدول التي أصبحت عرضة لهجمات الإرهابيين والجمعات المتطرفة الذين يمارسون نشاطهم التخريبي في أي مكان وزمان فهو عالمي لا تربطه أي حدود جغرافية.

تشكل حماية البنية الإلكترونية الحساسة أهم تحديات الدول في عصرنا الحالي؛ أين أصبح الاعتماد شبه المطلق والتبعية لتكنولوجيات الإعلام والاتصال الميزة الغالبة في أسلوب إدارتها وتسييرها لكافة نشاطاتها وشؤونها باختلاف مظاهرها، الأمر الذي سهل في المقابل إمكانية وصول الغير إلى ما يعتبر بالنسبة إليها أسرار دفاع وطني وباستغلال ذات الوسائل والتكنولوجيات؛ وعليه فقد سعت هذه الدول ومن خلال بناء أطر حماية تتماشى مع أشكال التهديدات المستحدثة التي تتخذ من الفضاء الإلكتروني بيئة النشاط ومنطلق وهدف الهجمات إلى مكافحة هذه التهديدات وفي مقدمتها التجسس الإلكتروني.

وقد توصلنا في نهاية هذه البحث الى عدد من النتائج والتوصيات التي سنذكرها تباعاً على الشكل الآتي:

أولاً: النتائج:

1. إن التجسس الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم، نظراً إلى تعدد أشكاله، وتنوع أساليبه، واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات وتقنيات المعلومات مهاجمتها في جو مريح وهادئ، وبعيد عن الإزعاج والفوضى مع توفير قدر كبير من السلامة والأمان للإرهابيين.

2. يعتبر التجسس الإلكتروني أحد أكثر المواضيع القانونية جدلاً وغموضاً؛ لأنه يجمع بين الشيء ونقيضه، فالدولة الواحدة تنظر إليه كتصرف مشروع وغير مشروع في ذات الحين، مشروع إن كانت هي القائم به وغير مشروع إن كانت هي ضحيته، وفي هذا الإطار تبرر لجوئها إليه بسعيها إلى حفظ أمنها وتبرر مكافحتها له أيضا بسعيها إلى حفظ أمنها.

ثانياً: التوصيات:

1. ضرورة السعي لتشريع قوانين خاصة بجرائم التجسس الإلكتروني، ينظم العقاب على هذه الجرائم مع التشديد على أن التجسس ليس له دين معين أو جنسية أو منطقة جغرافية محددة.
2. تطوير التشريعات الجنائية وإقرار سياسة تجريمية تسد أوجه التطور أمام ظاهرة التجسس الإلكتروني وتمنح القضاة فرصة تحقيق العدالة ووضع وصف قانوني لهذه الجرائم يستوعب خصوصيتها وأنماطها.

قائمة المصادر والمراجع

1. أسامة أحمد المناعسة وجلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 2014.
2. بهاء المري، شرح جرائم تقنية المعلومات، القانون رقم 175 لسنة 2018، منشأة المعارف، الإسكندرية – مصر، 2019.
3. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم المعلوماتية، الطبعة الاولى، دار النهضة العربية، 2009.
4. حسين محمد الغول، جرائم شبكة الإنترنت والمسؤولية الجزائية الناشئة عنها، دراسة مقارنة، مكتبة بدران الحقوقية صيدا – لبنان الطبعة الأولى، 2017.
5. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة، الطبعة الاولى، دار النهضة العربية، 2011.
6. ضياء كاظم الكناني، الإرهاب وسائل مكافحته، الطبعة الأولى، منشورات دار السنهوري، بغداد، 2017.
7. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي "دراسة قانونية متعمقة في القانون المعلوماتي"، دار الكتب القانونية، دار شتات للنشر والبرمجيات، مصر، 2007.
8. علي جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، الطبعة الاولى، منشورات زين الحقوقية، 2013.
9. عماد مجدي عبد الملك، جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2011.
10. عمار عباس الحسيني، جرائم الحاسوب والانترنت جرائم المعلوماتية، الطبعة الاولى، منشورات زين الحقوقية، بيروت، 2017.

11. عمر عباس خضير العبيدي، الإرهاب الإلكتروني في نطاق القانون الدولي، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة، 2021.
12. كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت، 2017.
13. محمد حماد مرهج الهيتي، الجريمة المعلوماتية، الطبعة الاولى، دار الكتب القانونية، مصر، 2014.
14. نائلة عادل محمد فريد قورة، جرائم المعلوماتية الاقتصادية، الطبعة الاولى، دار النهضة العربية، 2004.
15. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 2003.
16. هشام فريد رستمّ، قانون العقوبات ومخاطر تقنيّة المعلومات، مكتبة الآلات الحديثة، أسيوط، مصر، 2009.
17. هلال بن محمد بن حارب البوسعيدي، الحماية القانونية والفنية لقواعد المعلومات المحوسبة، الطبعة الاولى، دار النهضة العربية، 2009.
18. هلالي عبد اللاه أحمد، جرائم الحاسوب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية القاهرة، 2015.