جريمة التجسس الإلكتروني

الباحثة نجاري بن حاج علي فايزة
جامعة مولود معمري، تيزي وزو

الملخص

التجسس الإلكتروني وعلى إختلاف أساليبه وأنواعه يعد جريمة تستخدم فيها مختلف الوسائل الإلكترونية والتكنولوجية بشكل سلبي متجاوزاً كل الحدود الجغرافية، محدثاً آثار مدمرة وبغير وجه حق سواء كان ذلك من قِبل دول أو جماعات أو أفراد، وعليه فالحديث عن ضرورة إيجاد استراتيجية تقنية وقانونية لمحاربة هذه الظاهرة يعد حتمية قصد تأمين البيئة الإلكترونية رغم العوائق والتحديات الكبيرة، والجزائر ليست بمعزل عن هذا الأمر حيث أن المشرع الجزائري حاول ولا يزال يحاول مواجهة هذه الظاهرة من خلال تجريمها في قانون العقوبات.

الكلمات المفتاحية: التجسس، اختراق المواقع الإلكترونية، الاستخبارات، الحماية التقنية، الجريمة الإلكترونية، الإجراءات القانونية.

مقدمة

يعد التجسس من أقدم الأنشطة الاستخباراتية التي مارسها الإنسان، فالتاريخ يفصح عن مقدرات فطرية في مجال التجسس شهدتها السياسة وميادين الحروب التي مازالت البشرية تزيدها كل يوم اتساعاً وانتشارا.

أصبح التجسس في الوقت الراهن من الممارسات اليومية التي تعتمد عليها الدول في حماية أمنها، وتطوير صناعاتها، بل وفي التعامل مع الدول الأخرى، إذ تجمع المعلومات السرية والعلنية عن مصادر القوة ومواطن الضعف لديهم سواء كان ذلك في السياسة أو في الاقتصاد، وتسعى كذلك لمعرفة درجة الوعي والروح المعنوية في المجتمع، وحركة الجند، والقوة العسكرية، وعن تجمعات الدول الصديقة وتحالفاتها، وإلى أي مدى تتكامل المصالح بين دولتين صديقتين ضد طرف ثالث.

ولعل التجسس أصبح أكثر خطورة عندما تأثر بالتقدم التقني الذي وفر أجهزة عديدة ومعدات غاية في الدقة وصغيرة الحجم، وذات الكفاءة في التنصت والاستشعار عن بُعد، إلا أنه تجدر الإشارة إلى أن الدول الكبرى تحوز اليوم وحدها الأولوية في عالم التجسس ومعداته، لتجسد خطراً على العالم لا تخطئه عينٌ، بالتالي بات على الدول المستهدفة في الوقت الراهن وضع الخطط والاستراتيجيات ضد مخاطر التجسس.

وعليه فإن إشكالية دراستنا تتمحور في البحث في مفهوم التجسس الإلكتروني كأحد صور الجرائم المستحدثة والآليات التقنية والقانونية الرادعة له؟

للإجابة على تساؤلنا سنتطرق في هذا المقال إلى تعريف التجسس وأنواعه ونسلط الضوء على استخدام الأنظمة الإلكترونية الرقمية سواء كانت في الحفاظ على سرية المعلومات وحمايتها، أو تلك الأنظمة التي تساعد على إخفائها وتشفيرها كمحور أول.

كما نلقي الضوء في المحور الثاني على طرق مكافحة التجسس الإلكتروني ونتحدث عن نوع جديد من الأنظمة الإلكترونية المطورة للحفاظ على سرية المعلومات سواء كانت صوتية أو كتابية (Sound Text)، باستخدام منظومة الإشارات الضوضائية والتي تعرف (Chaotic Signal)، دون أن نهمل الإطار التشريعي في الجزائر الذي حاول ولا يزال يحاول مواجهة هذه الجريمة من خلال تجريمها في قانون العقوبات.

المحور الأول: مفهوم التجسس الإلكتروني

تستحوذ مواضيع التجسس الإلكتروني اهتمام جيل اليوم، خاصة الدخول إلى عالم الهاكرز الذي يعتبر حلماً يسعى إليه الكثير من الشباب، أما شبكة الإنترنت فهي ميدان صراعات من نوع جديد حملت كل أدوات التدمير الإلكتروني كالتجسس والاختراق وتدمير المواقع الإلكترونية الحكومية وغير الحكومية، والتحكم في تغيير قواعد بيانات قد تصل خطورتها إلى تهديد الأمن القومي لبعض الدول، مما دفع بعض خبراء الإنترنت للاعتقاد أن الشبكة العنكبوتية أصبحت على حافة الانهيار، ولخص بعض تقنيي الإعلام الآلي لدى شركة (Kaspersky) ما يحدث بقولهم: إن التكنولوجيا يأكل بعضها بعضا.

ولعل أصعب ما يمكن الاستدلال به كبداية لفهم هذه الظاهرة هو تقديم تعريف لها أو على الأقل إعطاء تفسير لها، بحكم أن كل ما ينشط في العالم الافتراضي يصعب تحديد ماهيته.

أولا: تعريف التجسس الإلكتروني

لا يوجد تعريف محدد للتجسس الإلكتروني، فالتجسس في حد ذاته كلمة متشعبة لا يمكن حصرها بتعريف واحد، إلا أنه يمكن أن نعرف التجسس الإلكتروني بأنه أحد صور الإرهاب الإلكتروني، يقوم باستخدام التكنولوجيا الضارة بشكل سلبي من أجل إحداث آثار مدمرة وأضرار بالغة وكبيرة لمحطات التحكم وأجهزة الكمبيوتر وشبكات الاتصال بدوافع سياسية أو عرقية أو دينية...الخ.

ويمتد التجسس الإلكتروني إلى أبعد من هذا، حيث عرف أيضا بأنه: «العدوان أو التخويف أو التهديد المادي أو المعنوي باستخدام الوسائل الإلكترونية، الصادر من الدول أو الجماعات أو الأفراد على الإنسان بغير حق»[1].

كما يمكن أن نعرفه على أنه استعمال لبرامج تقوم بالتتبع والتطفل على سلوك الجهاز من الكتابة إلى مراقبة المواقع التي يزورها المستخدم وذلك لسرقة معلومات سرية مثل كلمة المرور، إذ أن الوظيفة الأساسية لبرامج التجسس هي مراقبة وتسجيل جميع التحركات والأفعال التي تتم على جهاز الحاسوب، فبعد أن يتم تثبيت البرنامج على جهاز الكمبيوتر، يقوم البرنامج بإخفاء نفسه من النظام بحيث يصعب على المستخدم اكتشاف وجوده[2].

وهناك أنواع أخرى من برامج التجسس، تُجري تغييرات على جهاز الكمبيوتر ونظام التشغيل فقد تتسبب بإبطاء الجهاز أو بتعطيله أو إيذاء نظام التشغيل، وتستطيع أيضا هذه البرامج تغيير الصفحة الرئيسية أو صفحة البحث لمستعرض الويب (web)، أو إضافة مكونات إلى المستعرض لا تحتاج إليها أو لا يرغب فيها، وقد تصعّب هذه البرامج تغيير الإعدادات وإعادتها إلى ما كانت عليه في الأصل، «بالنسبة للتقييمات الحديثة بينت أن أكثر من ثلثي الحواسيب الشخصية تتأثر ببعض أنواع برامج التجسس»[3].

ثانيا: أنواع التجسس

لا يمكن تعداد أو حصر أنواع التجسس الإلكتروني، إلا أننا نحاول ذكر أهمها:

1- التجسس عن طريق الشبكات السلكية واللاسلكية

ظهرت أنواع أخرى للتجسس الإلكتروني في الشركات والجهات التي تستخدم الشبكات بكل أنواعها الصغيرة والكبيرة السلكية واللاسلكية، ومن أشهر أنواع التجسس بداخل الشبكات ما يعرف بـ (Sniffer) أو اصطياد حزم البيانات المرسلة، ومن أشهر هذه البرامج لأنظمة وندوز و لينكس هو برنامج (Ethereal) للشبكات الداخلية وبرامج (Tc dump) و(Win dump) وغيرها، هذه البرامج تستطيع اصطياد البيانات المرسلة داخل الشبكة وتعمل على مراقبة أغلب البروتوكولات ولذلك فإن أي مستخدم بداخل شبكة محلية يستطيع الوصول والتجسس على بقية المستخدمين.

وقد تمت تجربة أحد أنواع الـ (Sniffer) وهو مختص في اصطياد كلمات المرور في إحدى مقاهي الانترنت فكانت النتيجة الحصول على كلمات المرور السرية لإيميلات الأشخاص الذين سجلوا الدخول[4].

2- التجسس بواسطة الأقمار الصناعية

هذا النوع من أنواع التجسس الإلكتروني يتمتع بالصفة الدولية، وتستخدم فيه أجهزة نادرة جداً، والمراجع في هذا المجال جد قليلة إن لم نقل تكاد تكون منعدمة، لكن يمكن القول أن التجسس من خلال الأقمار الصناعية لا يمكن أن يقوم به فرد أو منظمة وإنما يقتصر على الدول المتقدمة التي تسيطر على كل البيانات في العالم وتملك أقماراً صناعية هي التي قامت بصنعها شخصيا، تتمتع هذه الأقمار الصناعية بأحدث التكنولوجيات والبرامج على وجه الأرض، يتم إطلاقها علنا عادة أمام الرأي العام لأسباب انسانية أو علمية لكن وحدها الدولة المسؤولة على إرسال القمر الصناعي تعرف الغاية والهدف الحقيقيين لمهمة القمر الصناعي إذا كان مبعوثا بهدف التجسس.

3- التجسس بالاستعمال شبكات الهاتف النقال

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

عام 2006 شركة كنديك الأوروبية المعروفة في مجال التجسس العسكري والإرهاب، تعرض برنامجاً رقميا اسمه (CrytoPro GSM A5)، ليكشف أن المعلومات

حول إمكانية اختراق التشفير ممكنة وصحيحة، وقد عرضت صورة من البرنامج لالتقاط محادثة ورسائل نصية بدقة عالية، حيث إن البرنامج يدعم نظام اليونكود لمختلف اللغات، وتوجد بالتحديد نسخة لـ (GSM) ونسخة لثريا فقط، معنى ذلك أنه بالحصول على هذا البرنامج وتركيبه على جهاز يحتوي على وصلة لاسلكي يستطيع أي شخص التجسس على شبكة (GSM)[5].

ثالثا: الفرق بين فيروسات التجسس والتجسس الإلكتروني

الفيروسات عبارة عن جزء من شيفرة أو رموز صممت لنسخ نفسها، من حاسوب مرتبط مع حاسوب آخر، وتتكاثر بالاعتماد على ملفات أخرى وعادة ما تنتقل بين الحواسيب بعدة طرق مسببة تدمير الملفات الشخصية أو حتى نظام التشغيل.

أما برامج التجسس من جهة أخرى فهي غير مصممة لتدمير الحاسوب، فبرامج التجسس تعرف على أنها أي برنامج يدخل على جهاز الكمبيوتر بدون إذن، يتخفى ويتجسس على الجهاز وينقل معلومات عن الجهاز ونشاطات المستخدم التي تمت عبر هذا الجهاز، وقد تسبب برامج التجسس تغييرات غير مرغوب فيها وليست متوقعة بالنسبة للمستخدم.

المحور الثاني: الحماية التقنية والقانونية من جريمة التجسس الإلكتروني

بات مؤكدا أن جرائم التجسس الإلكتروني هي جرائم عابرة للحدود أي أنها لا تتم ولا تنتهي في أراضي دولة محددة، وعليه فالحديث عن ضرورة إيجاد إستراتيجية تقنية وقانونية لمحاربة التجسس الإلكتروني وتأمين البيئة الإلكترونية، يأتي نظرا لتزايد عدد الهجمات على المستوى الدولي لأسباب عديدة أبرزها التحديات والعوائق لمحاربة هذه الظاهرة خاصة في المجال الأمني، وهو أحد أهم الأسباب في نجاح الجواسيس في استغلال التكنولوجيا في أنشطتهم، بالإضافة إلى ضعف التشريعات والعقوبات المخصصة لهذا النوع الجديد من الجرائم المستحدثة.

عدم وجود منهج دولي لمكافحة هذه الظاهرة، يظل الجاني يقوم بعملياته بكل حرية متنقلا من دولة إلى أخرى ضامنا عدم القبض عليه، وهو ما كان أحد أهم الأسباب التي أدت إلى ضرورة إيجاد آليات أمنية دولية للحد منه، ثم لا بد من أن يكون هذا التعاون الأمني مصحوبا بنصوص قانونية لحصره، بحكم أنه ينشط في عالم إلكتروني افتراضي.

أولا: الآليات التقنية الدولية لحصر جريمة التجسس الإلكتروني

حتى نستطيع التصدي لجريمة التجسس، لابد من توفير حماية ذات طبيعة تقنية قادرة على تقديم أمن أكثر، فدرجة الحماية المطلوبة تختلف حسب نوع المعلومة المراد حمايتها، بمعنى أن إجراءات الحماية تنطلق من احتياجات الحماية الملائمة كحماية المعاملات المالية، وحماية المواقع الخاصة بالإنترنت والحياة الخاصة.

1- الجدران النارية كوسيلة لحماية المحتوى

يعتبر الجدار الناري وسيلة تستعمل لحماية الشبكات الخاصة من الدخول وتمنع الوصول غير المشروع لها، حيث تحمي وحدات التحكم والإرسال في الإنترنت.

وتتجلى أهمية الجدران النارية في حماية الشبكات، الخاصة التي تعمل على بث متعدد الأطراف باستعمال الأجهزة السمعية والبصرية ومؤتمرات الفيديو لمجموعة من المضيفين ليرى ويسمع كل منهم الآخر، ويوفر الهيكل الإذاعي المتكامل على الإنترنت عن طريق برنامج (Mphone) المتوافر لكل الناس، إلا أن هذا البرنامج يتيح المجال لأي مستعمل آخر للدخول عليه ومراقبته في الإنترنت، لكن بوجود الجدران النارية يستحيل تماما التطفل[6].

وتتجلى مزايا هذه الجدران النارية في:

- توفير الحماية اللازمة للشبكة والمعلومات والحد من تعرضها للأخطار ومتابعة المستخدمين للشبكة ومن يحاول العبث بها؛
- تسجيل وقائع الاستخدام بدقة طالما أن كل الرسائل والأوامر تمر به عند خروجها أو دخولها الإنترنت؛
- تسجيل كافة المعلومات عن حركة مرور المعلومات.

2- نظام المعاملات الإلكترونية الآمنة (SET)

وهو أهم برتوكول متعلق بالنواحي الأمنية وهدفه الأساسي هو تأمين عملية الوفاء والمعاملات المالية التي تتم أثناء المعاملة التجارية.

ويتميز هذا النظام عن الأنظمة التأمينية الأخرى بعدة مميزات كونه[7]:

- يضمن أن طلب الشراء المرسل هو نفسه الطلب الذي يستقبله صاحب المشروع أو التاجر عن طريق بصمة ورقية معينة تكون مميزة لهذا الطلب؛
- يضمن سرية طلب الشراء عن طريق تشفير المعلومات التي يشملها الطلب وكذلك البيانات الخاصة بعمليات الوفاء.
- يضمن للتاجر أو صاحب المشروع أن حامل البطاقة البنكية هو الشخص نفسه، عن طريق الشهادة التي يحملها والصادرة عن البنك الضامن أو شركة الائتمان الضامنة له، والتي تؤكد لصاحب المشروع أو التاجر أن هذا الشخص الراغب في الشراء هو نفسه صاحب رقم الحساب المذكور وليس شخص آخر استعان بمعلومات حامل البطاقة البنكية عن طريق التجسس والقرصنة، كما أنه يعطي للتاجر ضمان بأن حساب المشتري يسمح بشراء هذه السلعة أو الخدمة المراد شرائها دون معرفة البائع برقم البطاقة البنكية الخاصة بالمشتري.

3- نظام التأمين (SSL)

وتكمن مهمة البرتوكول في تشفير جميع الاتصالات في برامج التصفح أو النوافذ على شبكة المعلومات (Bowser) وأحد المواقع أو مقر المعلومات على خادم الشبكة (Server)، وبالتالي فهو يقلل من فرصة وقوع المعلومات أثناء عملية انتقالها في أيدي أي شخص غير مرغوب فيه، إلى أن تصل إلى المستقبل النهائي فهو يعطي للمتعامل الثقة والطمأنينة بأن المعلومات والبيانات الخاصة بهم لن تكون متاحة سوى للتاجر أو المنشأ أو المؤسسة المراد التعامل معها.

ثانيا: الإطار التشريعي في الجزائر ضد جريمة التجسس الإلكتروني

تدارك المشرع الجزائري الفراغ القانوني في مجال الجرائم الإلكترونية عموما والتجسس عبر الإنترنت خصوصا بموجب القانون رقم 04-15[8]، المعدل لقانون العقوبات.

نجد المادة (394 مكرر) تجرم كل دخول غير مصرح به عن طريق الغش على المنظومة المعلوماتية، سواء مسّ ذلك الدخول أو البقاء في كامل المنظومة أو جزء منها.

أما المادة (394 مكرر1)، تجرم كل عملية إتلاف وتدمير للمعطيات، وتليها المادة (394 مكرر2) تجرم كل عملية استيلاء على المعطيات، كما نصت مواد القسم السابع مكرر من قانون العقوبات، وخاصة المادة (394 مكرر2) فقرة ثانية على تجريم أفعال الحيازة، الإفشاء والنشر التي ترد على المعطيات الآلية، بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق، وجميع الأفعال غير المشروعة، وذلك بعقوبتي الحبس والغرامة، إضافة إلى ما نصت عليه المادة (394 مكرر 6) بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محل لجريمة من الجرائم المنصوص عليها في القسم السابع من قانون العقوبات[9].

تتمثل الجزاءات المقررة بموجب الفصل السابع مكرر في العقوبات الأصلية وهي عقوبة الحبس والغرامة، وعقوبات تكميلية بموجب نص المادة (394 مكرر 6) والمتمثلة في مصادرة الأجهزة والبرامج والوسائل المستخدمة، وإغلاق المواقع والمحل أو أماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الإنترنت الذي ترتكب فيه الجرائم بشرط علم مالكه.

أورد المشرع ظروفا تشدد بها عقوبة الجريمة وهي:

- حالة الدخول والبقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب النظام؛
- إذا استهدفت الجريمة الدفاع الوطني، أو الهيئات والمؤسسات الخاضعة للقانون العام.

ولقد دفع القصور الذي عرفه القانون رقم 04-15 والمعدل لقانون العقوبات الذي نص على حماية جزئية نسبية لأنظمة المعلومات، من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، بالمشرع الجزائري إلى إصدار القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

جمع هذا القانون بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصادرها والتعرف على مرتكبيها[10].

يتضمن القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على 06 فصول أهمها:

- الفصل الثاني الذي جسد أحكام خاصة بمراقبة الاتصالات الإلكترونية، وقد راعى في وضع هذه القواعد خطورة التهديدات المحتملة وأهمية المصالح المحمية، إذ نص القانون على أربع حالات يسمح فيها للسلطات الأمنية بممارسة الرقابة على المراسلات والاتصالات الإلكترونية، منها الوقاية من الأفعال الموصوفة بجرائم الإرهاب، أو في حالة توفر المعلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو بمقتضيات التحريات والتحقيق، أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[11].
- أما الفصل الخامس فقد أشار إلى الهيئة الوطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحته، إذ نص القانون على إنشاء هيئة وطنية ذات وظيفة تنسيقية في مجال الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، وقد تمت الإحالة على التنظيم فيما يخص تحديد كيفية تشكيل وتنظيم هذه الهيئة[12].

يعد القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مجالا شاملا في ميدان مكافحة التجسس الإلكتروني، إذ جاء تجريمه للأفعال المخالفة للقانون والتي ترتكب على شبكة الإنترنت، وجهاز الحاسوب الآلي.

خاتمة

في عصر الازدهار الإلكتروني وزمن قيام حكومات إلكترونية، تبدل أسلوب الحياة وتغيرت معه أشكال الأشياء وأنماطها وكذا الجريمة التي قد يحتفظ بعضها باسمها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها والقديمة في اسمها جريمة التجسس الإلكتروني الذي أخذ اشكال حديثة تتماشى مع التطور التقني والأساليب التي يحاول المفسدين الوصول بها إلى أهدافهم، فالتجسس الإلكتروني هو السائد حالياً كمفهوم جديد لحرب التكنولوجيا.

وكغيره من الجرائم المعلوماتية، يصعب إيجاد تعريف موحد له بحكم أنه ينشط في عالم افتراضي صعب رصده، لكن يمكن القول أنه عبارة عن استعمال لبرامج تقوم بالتتبع والتطفل على سلوك الجهاز من الكتابة إلى مراقبة المواقع التي يزورها المستخدم وذلك لسرقة معلومات سرية مثل كلمة المرور أو التجسس على الصور والمراسلات

الإلكترونية والبريد الإلكتروني، بطريقة جد ذكية يصعب رصدها من طرف الضحية أو حتى اكتشاف وجود برنامج للتجسس، كما أن اقتحام المواقع وتدميرها وتغيير محتوياتها والدخول على الشبكات والعبث بمحتوياتها بإزالتها أو بالاستيلاء عليها أو الدخول على شبكات الاتصالات أو شبكات المعلومات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائياً أصبح هو أسلوب التجسس حالياً.

كل هذه التصرفات تدل على أن التجسس الإلكتروني هو إرهاب جديد لا يعتمد على استخدام الأسلحة والمتفجرات، وإنما يستغل التكنولوجيا لدوافع سياسية، اقتصادية واجتماعية ضد أنظمة تكنولوجية كالكمبيوتر ونظام البيانات.

غير أن هذا الخطر الافتراضي المعقد حاولت الجهود الدولية والإقليمية مجابهته من خلال إيجاد اتفاقية دولية شاملة وهي معاهدة بودابست المنعقدة سنة 2001 بـجونيف والتي عالجت مشكل الجريمة المعلوماتية بتعريفها وتبيان أركانها، وكذا متى يمكن تصنيف الفعل بأنه جريمة معلوماتية مع تحديد إجراءات التحقيق وكذا العقوبة المقررة، كما يمكن القول أن هذه المعاهدة تعتبر المرجع الأساسي في مكافحة الجريمة المعلوماتية والتي اعتبرت التجسس الإلكتروني أحد أنواعها.

أما على المستوى الداخلي والمحلي نجد أن بعض البلدان خصصت في تشريعاتها الداخلية مجموعة من النصوص القانونية التي تجرم فعل التجسس إلا أنها تبقى محاولة جد بسيطة مقارنة بالتهديد والتدمير الذي يسببه التجسس، لأن آليات التتبع والتحقيق في المجال التكنولوجي جد معقدة، فطبيعة العالم الافتراضي تجعل من حجية الإثبات أمر جد معقد إن لم نقل مستحيل في بعض الحالات أين يتم مثلا تحويل مبالغ مالية هائلة مكتسبة بطرق غير قانونية في حسابات موجودة على مستوى «الدارك نت» (darknet)، كما أن الدول المستعمرة تكنولوجيا أي التي تشتري التكنولوجيا بدلا من صناعتها، تفتح المجال لكي يتم التجسس عليها طوعا في حين يمكنها تطوير الكفاءات اللازمة -ونأخذ الجزائر كمثال- لكي تتفادى هذا الإشكال أو على الأقل تحد منه بحكم أن الجزائر تملك عباقرة في مجال الإعلام الآلي والتكنولوجي يستطيعون صناعة وإنتاج وسائل تكنولوجية، لو تحصلوا على فرصة لتبيان قدراتهم وكذا تمويلهم ودعمهم ماديا، وهذا إشكال آخر يأخذنا إلى ختم المقال بهذا التساؤل: إلى متى نستطيع الصمود في وجه الجرائم التكنولوجية الحديثة التي تكاد تجعل من التكنولوجيا لعبة ملعونة في يد الدول الضعيفة اقتصاديا، تسيطر عليها دول ليست فقط مصنعة للتكنولوجيا بل محتكرة لها؟

الهوامش

1. https://www.facebook.com/realestateKhal/posts

2. سالم منصور، ماهي برامج التجسس؟ وكيف تتسلل لأجهزتنا؟ على الموقع

http://www.arabs2day.ws/forums/lofiversion/index.php/t172.htm

3. نوف علي الشنيفي، البرامج التجسسية أنواعها وطرق الحماية منها، مركز التميز الأمن المعلوماتي، مصر2011.

4. حسن بن أحمد الشهيري، «الأنظمة الإلكترونية الرقمية المطورة لحفظ وحماية سرية المعلومات من التجسس» المجلة العربية للدراسات الأمنية والتدريب المجلد 28، العدد 56، ص 13-14.

5. نوف علي الشنيفي، مرجع سابق، ص 15.

6. ضياء علي أحمد نعمان، «الحماية التقنية للتجارة الالكترونية»، مجلة القانون، العدد الأول، مطبعة وراقة وطنية، مراكش، المغرب 2011، ص 39.

7. تم تطوير نظام المعلومات الإلكترونية Set بالتعاون بين أكبر شركات البطاقات البنكية وهما شركة (Master card et Visa card)، وذلك نص في تأمين المعاملات المالية عبر شبكة الانترنيت باستخدام البطاقة البنكية، يمثل عملائهما معا أكثر من 8000 مليون، كما انضمت (American axpress) لهذا التحالف ليصبح بذلك أكبر تحالف موجود لتأمين المعاملات الإلكترونية.

8. قانون رقم 04-15 مؤرخ في 2004/11/10، يتضمن قانون العقوبات، الجريدة الرسمية، عدد 17، صادر في 2004/11/10.

9. أنظر المواد 394 مكرر 2 ومكرر 6، من القانون رقم 04-15 المؤرخ في 2004/11/10 المتضمن قانون العقوبات، مرجع سابق.

10. قانون رقم 09-04 مؤرخ في 2009/02/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، عدد 47، صادر في 2009/02/16.

11. المادة 04 من القانون رقم 09-04، مرجع سابق.

12. المادة 13 و14 من القانون نفسه.