التجسس الالكتروني وآليات مكافحته في التشريع الجنائي الجزائري

أ.اوشن حنان
جامعة خنشلة

أ. وادي عماد الدين
باحث دكتوراه

ملخص

يدفع مستخدم الإنترنت نفقات مرتفعة مقابل حصوله على تلك الخدمة، ولكن هل يستفيد منها فعلا؟ أو بمعنى آخر هل يحصل على المقابل الذي يتوقعه بعد دفع هذه النفقات؟

كانت إجابة هذا السؤال بديهية في السابق، حيث كان مستخدم الشبكة يقضي معظم وقته في استدعاء الصفحات والبحث عن المعلومات التي يطلبها، ولكن تطور أساليب الخداع الإلكتروني عن طريــق بــرامج أعدت خصيصا لهذا الغرض جعلت الأمر معكوسا في معظم الأحيان، حيث يدفع مستخدم الشبكة مقابل خدمة الآخرين والترويج لسلعهم والتجسس على تحركاته في الفضاء الإلكتروني!

المثير للدهشة أن معظم قراصنة الإبحار الإلكتروني، لم تعد ترتــدي الأزيــاء التقليديــة للقراصــنة المعروفين في هذا العالم، حيث لا تظهر آثار بريمجاتهم كصفحات تظهر فجأة بصورة مباغتة تعلن عن سلعة ما أو تدعو إلى الاستمتاع بمحتويات موقع معين، ولكنها أصبحت ترتدي الآن ثيابا أكثر براءة وجاذبية

résumé

L'internaute paie les frais sont élevés par rapport à ceux recevant un service , mais ne vous bénéficiez vraiment? Ou en d'autres termes, vous obtenez d'autre part , s'attendre à ce que , après le paiement de ces frais?

La réponse à cette question intuitive dans le passé , où l'utilisateur du réseau passe le plus clair de son temps en appelant la page et la recherche de l'information que vous avez demandé , mais l'évolution des techniques de duperie électronique à travers des programmes spécialement préparés à cet effet a inversé dans la plupart des cas, lorsque l'utilisateur du réseau de rémunération par rapport au service des autres et pour promouvoir leurs produits et espionner ses mouvements dans le cyberespace!

Étonnamment, la plupart du courrier pirates de voile , ne plus porter les costumes traditionnels de pirates connues dans ce monde , ne montrent pas les effets de Premjathm que les pages apparaissent soudainement surpris annonce une marchandise ou des appels à profiter du contenu d'un site particulier , mais il est maintenant de porter des vêtements plus innocent et attrayant.

إن التطور التكنولوجي و التقني في مختلف المجالات و نمو التجارة الدولية و نمو الاقتصاد الـــدولي وتوسيع مناطق التبادل الحر، و فتح الأسواق العالمية أمام التجارة، و كذلك ظهور العولمة التي جعلت العـــالم كالقرية الكبيرة تتفاعل فيه جميع المكونات من أشخاص القانون الدولي، و التي ساهمت في إزالة الحدود بين الدول ،فهذه الظاهرة أدت إلى عولمة الاقتصاد وعولمة الثقافة ، كذلك نتج عنها عولمـــة الجريمـــة، بحيـــث انطلقت من النطاق الداخلي للدولة إلى النطاق الدولي .

إشكالية الموضوع :

تبرز إشكالية هذا الموضوع في معرفة جريمة الجوسسة الرقمية كنمط جديد يهدد أمن الدولة وسلامتها على المستوى الداخلي والخارجي ،وكيفية تعامل المشرع الجنائي مع هذه الظاهرة ؟.

تسعى هذه الدراسة إلى محاولة تحديد معالم الجوسسة ، وذلك من حيث تحديد مفهوم هذه الجريمـــة، وتحديد خصائصها وأهدافها، ومن ثم إبراز أهم مظاهرها وأشكالها، و التحديات التي تطرحها ، والتطرق إلى آليات مكافحتها في التشريع الجنائي الجزائري .

وتبرز أهمية هذا الموضوع من الناحية العملية و العلمية من حيث:

_ موضوع جديد يطرح أنماط جديدة تهدد الدولة في أمنها الداخلي والخارجي .

_ إشكالية قانونية قائمة ،خاصة فيما تعلق بمكافحته

_ ظاهرة إجرامية مرتبطة بالعالم الذي أفرزته العولمة التقنية .

سوف تتم دراسته من خلال الخطة التالية :

المحور الأول: مفهوم التجسس الإلكتروني :

يتناول كل ما يتعلق بالمجال المفاهيمي

المحور الثاني :المعالجة القانونية للتجسس الإلكتروني

يتناول الدراسة القانونية لهذه الظاهرة وكيفية مواجهتها.

المحور الأول: مفهوم التجسس الإلكتروني

عمليات التجسس والتنصت من أجل الحصول على المعلومات هي عمليات قديمة قدم البشرية وقدم النزعات فمنذ قدم العصور كان الإنسان يتجسس على أعدائه لمعرفـــة أخبـــارهم والخطـــط التـــي يعـــدونها لمهاجمته، ولهذا كان للتجسس أهميته الكبرى على كافة مستويات النزاعات الإنسانية التي مر بها البشر منـــذ بدء الخليقة.

إلا أنه وبظهور عصر المعلومات والاتصالات وازدهاره تحولت وسائل التجســـس والتنصـــت مـــن الطرق التقليدية إلى الطرق الإلكترونية ، لا سيما مع استخدام شبكة الإنترنـــت وانتشـــارها الواســـع عربيـــا وعالميا.

أولا : تعريف التجسس الإلكتروني وخصائصه

1. التعريف

التجسس الإلكتروني: أو ما يعرف بحرب التجسس ألمعلوماتي هو عبارة عن عدة طرق لاختـــراق المواقـــع الالكترونية ومن ثم سرقة بعض المعلومات والتي قد تكون في غاية الأهمية والخطـــورة للطـــرف المتلقـــي والمسروق منه وقد انتشرت في الألفية الجديدة بانتشار طرق الاختراق[1]

الجاسوسية الرقمية أي الحاسوبية ترصد ومراقبة ، عن طريق التسلل إلى أجهـــزتهم الحاســـوبية أو محاولـــة اعتراض الإشارات وحزم المعلومات التي ترسل من قبل أجهزتهم عبر الإنترنت. تعتبر الحواسيب أحد أهـــم وسائل التجسس على الخصوصيات الفردية لقدرة المختصين على تلقي معلومات منها دون علـــم أصـــحاب الأجهزة انفسهم. يتم معظم هذا عن طريق شبكات الحاسب التي توصل بها معظم الحواسيب باستخدام ثغرات أمنيـــة أو اختراق أمن الحاسوب security cracking للحصول على وصول للمعلومات المخزنة على الحاسب[2].

غالبا ما تتم عمليات تجسس دولية للحصول على معلومات سرية رسمية لدى الحكومات مـــن قبـــل حكومات دول أخرى، أو قد يتم التجسس من قبل حكومة بلد على أفراد معينين من النشـــطاء السياســـيين أو أفراد الجريمة المنظمة والعصابات الضخمة والمافيات.3.

2. خصائص التجسس الرقمي :

_ الجوسسة الرقمية جريمة معاقب عليها .

_ الجوسسة الرقمية متعدية الحدود أو جريمة عابرة للدول:المجتمـــع المعلومـــاتي لا يعتـــرف بالحـــدود الجغرافية فهو مجتمع منفتح عبر شبكات تختـــرق الزمـــان والمكـــان دون أن تخضـــع لحـــرس الحـــدود. فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومـــات عبـــر الـــدول المختلفة، فالمقدرة التي تتمتع بها لحواسيب وشبكاتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قـــد تتـــأثر بالجريمـــة المعلوماتية الواحدة في آن واحد[4].

فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب التجسس عن طريق حاســـوب موجـــود فـــي دولـــة معينـــة بينمـــا يتحقـــق الفعـــل الإجرامـــي فـــي دولـــة أخـــرى.

_ تتميز الجوسسة الرقمية بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة.

_ صعوبة إثبات التجسس المعلوماتي فالجريمة هنا تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقـــع المادي الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة. ففي هذه البيئة تكون البيانات و المعلومات عبارة عن نبضات إلكترونيـــة غيـــر

1.أحمد حسام طه تمام ،الجرائم الناشئة عن إستخدام الحاسب الآلي ،دار النهضة العربية ،ص،102.

2– فيل وليامز ,الجريمة المنظمة وجرائم الشبكات الالكترونية ,مركز خبرات أمن الأنترنت في جامعه ميلون كارينجي– 2002

3– رمضان الألفي. " العولمة والأمن " الانعكاسات السلبية والإيجابية كدراسات اقتصادية، مركز الدراسات السياسية والإستراتيجية. الأهـــرام ، الســـنة الثانية 1998، العدد 27، ص 5،ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون ،طرابلس 27_2009/10/30..

4 . Herbert Burkert, Privacy-Enhancing Technologies: Typology, Critique, Vision, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, 125,142 (Philip E. Agre & Marc Rotenberg, eds. MIT Press 1997).

مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كلياً من قبل الفاعل أمراً في غايـــة السهولة.

_ الثغرات القانونية بين مختلف الدول: فما هو صارم في نظام ما مخفف في آخر، مما يتـــيح الفرصـــة للمجرمين سرعة التكيف و انتقال من نقطة جغرافية لأخرى أكثر أمانا.

ثانيا : أنواع التجسس الإلكتروني

3. التجسس الإلكتروني على الأفراد و المؤسسات والحكومات:

تتم عملية التجسس هنا بـــ:

1-1التجسس عن طريق الانترنت:

أبسط أنواع التجسس الإلكتروني معروف ومنتشر بين الأفراد وهم مستخدمي الكمبيـــوتر الشخصـــي بشكل عام هذا النوع من التجسس يستخدم فيه "الهكر" أو من يريد التجسس ببرامج خارجية مبنية على أساس العميل والخادم أو ما يعرف client و server يشترط في هذه العملية أن يكون برنامج الخادم يعمـــل فـــي النظام المستهدف ليقوم بعد ذلك الهكر بالاتصال من خلال برنامج العميل لتبدأ عملية التجسس.

هذا النوع من برامج التجسس يعمل على الكمبيوتر الشخصي وقد ظهرت برامج كثيرة لأنظمة وندوز ولينكس

من أشهرها back orifice، net bus، sub7

الجدير بالذكر أنه مع انتشار الأجهزة الخفيفة والهواتف المحمولة في الآونة الأخيرة التـــي تســـتخدم أنظمة تشغيل متطورة مثل نظام Symbian الذي يسمح بتطوير برامج خارجية وتشغيلها على الجوال فقـــد ظهرت لهذه الأنظمة برامج تجسس مشابهة للفكرة السابقة وأمثلة على ذلك برنامج FlexiSPY الذي يثبـــت على الجوال للتجسس على المكالمات والرسائل القصيرة SMS وسجل المكالمات وغيرها .

كيف تعمل هذه البرامج:

فكرة برمجة مثل هذه الأنواع من البرامج بسيطة للغاية ويمكن استخدام لغات البرمجة المعروفة مثل السي،السي، أو لباسكال او باستخدام الفيجوال بيسك وتكون الطريقة كالتالي :

+ برمجة الخادم على ثلاث نقاط أساسية:

- فتح منفذ port في الجهاز المستهدف
- استقبال الأوامر من خلال المنفذ
- تنفيذ الأوامر التي تأتي من المنفذ

++ وبعد ذلك يأتي دور البرنامج العميل في الطرف الآخر ويتم برمجته على أساس:

- إجراء اتصال مع الخادم من خلال المنفذ في الطرف الآخر
- إرسال الأوامر للخادم من خلال المنفذ المحدد
- استقبال المعلومات والنتائج

2.1.التجسس من خلال الشبكات الداخلية:

هناك نوعين من الشبكات كمايلي :

1.2.1. الشبكات السلكية :

بالإضافة للنوع الأول من أنواع التجسس على الأفراد فقد ظهرت أنواع أخرى للتجسس الإلكترونـــي في الشركات والجهات التي تستخدم الشبكات بكل أنواعها الصغيرة والكبيرة اللاسلكية والسلكية ومن أشـــهر أنواع التجسس داخل الشبكات نوع يعرف بـــSniffer أو اصطياد حزم البيانات المرسلة ومن أشـــهر هـــذه البرامج لأنظمة ويندوز ولينكس هي :

ـــــ برنامج ETHEREAL للشبكات الداخلية وبرامجTCPDUMPو WINDUMPوغيرها .

هذه البرامج تستطيع اصطياد البيانات المرســـلة داخـــل الشـــبكة والعمـــل علـــى مراقبـــة أغلـــب البروتوكولات،لذلك فإن أي مستخدم بداخل شبكة محلية يستطيع الوصول والتجسس على بقية المستخدمين[1]

2.2.1. الشبكات اللاسلكية :

بنفس الفكرة في موضوع الشبكات السلكية مع اختلاف بسيط وإضافات جديدة وتدعى هذه الطريقـــة Wireless sniffer والفرق في الشبكات اللاسلكية أن البيانات المرسلة تحتوي على مفتاح تحقـــق يكـــون مشفر لحماية البيانات أثناء الإرسال ،ومن أشهر أنواع مفاتيح الحماية :

_ مفتاح الحماية wep

_ مفتاح الحماية wap.

وكلا النوعين يمكن من الوصول لها وكسر تشفير مفاتيح الحماية، ومن أشهر البرامج التي تســـتخدم للتجسس في هذا المجال :

_ برنامج KISMET لأنظمة لينكس وبرمانج NETSTUMBLERلأنظمة وندوز وتستطيع من خلال البرامج السابقة تحديد البيانات والأجهزة المتصلة وغيرها ،وبعد تحديد الجهاز الهدف ســـيحتاج لحزمة البرامج air crack لالتقاط البيانات أو تزييفها أو كسر مفتاح التشفير وتوجد بين المجموعات التالية:

_air dump لاصطياد حزم البيانات المرسلة بين الأجهزة.

_aireplay لإعادة حقن البيانات في الحزم المرسلة وتستعمل للتزييف عادة .

_ aircrck لكسر تشفير مفتاح التحقق في الشبكات اللاسلكية .

1. التجسس الإلكتروني الدولي والخارجي :

1.2. التجسس من خلال النظام العالمي لاتصالات الهاتف النقال GSM و نظام الثريا :

تشفير A5 يقوم بعمل حماية وتشفير البيانات المرسلة بين الأجهزة المحمولة ومحطـــة الاســـتقبال ويرسل المعلومات في حزمة تمثل محادثة صوتية أو رسالة SMS،أو غيرها ويستخدم GSMفي الهواتف النقالة .

2.2 . التجسس من خلال الموجات والترددات :

إن أغلب الموجات معروفة وهي محطات الراديو التي يمكن لأي أحد إستقبالها ويمكن تصنيفها إلى[2]

_ موجات الراديو البعيدة والقريبة .

_موجات الراديو العالية وهي المستخدمة في لاسلكي الشرطة .

_الموجات الهوائية و الموجات الدقيقة .

---

[1] عبد الفتاح مراد، شرح جرائم الكمبيوتر والأنترنت، دار الكتب والوثائق المصرية، ص 46/45.

[2] أسامة الكشواني ،التجسس الإلكتروني وطرق مكافحته ،جريدة أسواق العرب ،عمود التكنولوجيات العربية ،يوم :2007/6/6، مصر .

ولكن هناك بعض الموجات الغير معروفة والتي تسمى بالترددات السرية الدولية وهي التي تكـــون محـــل تجسس يتم بعد توافر الشروط التالية :

_ امتلاك جهاز التقاط لاسلكي بموجات فوق المتوسطية ،مع الحصول على مجال الترددات.

_ خبرة في البرمجة بشكل عام والتشفير بشكل خاص.

3.2. التجسس من خلال الأقمار الصناعية :

هذا النوع من التجسس لا يمكن أن يقوم به فرد أو منظمة وإنما يقتصر على الدول المتقدمة التـــي تسيطر على كل البيانات في العالم .

ثالثا: مجالات التجسس الرقمي

1. التجسس العسكري:

المؤسسات العسكرية من أهم مؤسسات الدولة وأكثرها استخداما للمعلوماتية ، وبالتالي فهي كانت وما زالت تعد منشطا مهما ومجالا خصبا لمحاولات التجسس والاختراق ، نظرا لما يتوافر لدى العاملين فيها من معلومات تهم أمن البلد.ففي حرب الخليج الأخيرة تمكن مجموعة من القراصنة هولنديو الجنسية من اختـــراق عدد كبير من أجهزة الحاسب الآلي التابعة للدفاع الأمريكي المرتبطة بشبكة الإنترنت ، والتي كانت تحـــوى معلومات عسكرية في غاية الخطورة عن الجيش الأمريكي ومواقعه وتفاصيل الأسلحة المختلفة الموجودة في كل موقع من هذه المواقع. كما تمكنت إحدى المنظمات المتخصصة بالاختراق من الهجوم على موقـــع إدارة معدات شبكة نظم معلومات الدفاع الأمريكية ، وسرقت بعض البرامج والمعلومات المحفوظة علـــى إحـــدى الحاسبات الآلية المزودة[1] SERVER"

2. التجسس التجاري :

مع توسع التجارة الإلكترونية عبر شبكة الإنترنت تحولت الكثير من مصادر المعلومات إلى أهـــداف للتجسس التجاري ، ففي تقرير صادر عن وزارة التجارة والصناعة البريطانية أشار إلى زيادة نسبة التجسس على الشركات من 36% عام 1994م إلى 54% 1999م ، كما أظهر استفتاء أجري عام 1996 لمسئولي الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول وبشكل غير مشروع على معلومات ســـرية لأنشطة تجارية وصناعية في الولايات المتحدة الأمريكية. وفي إسرائيل اعتقلت الشرطة في منتصـــف عـــام 2005م 18 شخصاً من كبار المسئولين في 15شركة على الأقل بتهمة التجسس الإلكتروني على منافســـيهم عبر أجهزة الحاسب الآلي . وكان من ضمن المجموعة المعتقلة مسئولين في شركتين للهواتـــف المحمولـــة وشركة للقنوات الفضائية وشركة لاستيراد السيارات ، بالإضافة إلى عدد من المتحـــريين الخاصـــين، ولقـــد استعمل المتهمون في اختراق حواسيب منافسيهم برامج تجسسية من نوعية حصان طروادة.

3. التجسس الشخصي:

الهجوم على خصوصية الأفراد والتنصت عليهم ومراقبة شؤونهم الخاصة في الفضـــاء المعلومـــاتى أصبح يتزايد وبشكل ملفت للنظر ، وما قامت به الولايات المتحدة الأمريكية من استخدام لبرنامج كارن يفور إلا دليلا على هذه الانتهاكات الواضحة لخصوصية الإنسان .

أيضا قد يتم العبث بالسجلات الرقمية وتغيير مدخلاتها المخزنة في قواعد البيانات .

[1] هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة 1992. ص 180 .

المحور الثاني : المعالجة القانونية للتجسس الإلكتروني

تتفق السياسات التشريعية العقابية لمختلف الدول ومنها السياسة العقابية الجزائرية علـــى أن الجـــرائم بنوعيها المخلة بأمن الدولة الخارجي، والمخلة بأمن الدولة الداخلي هي من اخطر الجرائم المضرة بالمصلحة العامة، وبما أن جريمة التجسس بمفهومها التقليدي من الجرائم الماسة بالأمن الخارجي للدولة عالجها المشرع وحاربها ،لكن كيف ينظر اليوم إلى هذه الجريمة بشكلها الجديد الظاهر في الجوسسة الرقمية ؟

أولا : أركان الجوسسة الرقمية

إن التجسس الإلكتروني كجريمة معاقب عليها لابد من أن تكون له أركان تبين وتثبت وقوعه نميـــزه عن غيره من الجرائم ،لذلك سوف نخصص هذه الجزئية للحديث عنها كمايلي:

1:الأركان العامة للجوسسة الرقمية :

بالرجوع إلى السياسة التشريعية نجد أن المشرع الجزائري في ظل القواعد التقليدية قد نص في **المادة 64 على جريمة التجسس على النحو التالي:**

" يرتكب جريمة التجسس ويعاقب بالإعدام كل أجنبي يقوم بأحد الأفعال المنصوص عليها في الفقرات 2و3و4 من المادة 61 وفي المادة 62 ويعاقب من يحرض على ارتكاب إحدى الجنايات المنصوص عليهـــا في هذه المادة والمواد 61و62و63 أو يعرض ارتكابها بالعقوبة المقررة للجناية ذاتها".

ويستخلص من هذا النص الأمور التالية:

– إن جريمة التجسس هي نفسها جريمة الخيانة إذا أرتكبها الأجنبي، ما عدا الجريمة المنصوص عليها في الفقرة الأولى من المادة 61، وهي جريمة حمل السلاح ضد الجزائر التي لم تخص بالوصف المزدوج: الخيانة والتجسس.

– إن عقوبة التجسس هي نفس عقوبة الخيانة وهي الإعدام.

– ساوت هذه المادة في فقرتها الثانية بين عقوبة المحرض والمساعد والفاعل الأصلي.

ومن ثم يمكن تحديد أركان هذه الجريمة كمايلي :

– **الركن الأول:** وهو كون الجاني أجنبي يقوم بأحد الأعمال التالية :

القيام بالتخابر: مع دولة أجنبية بقصد حملها على القيام بأعمال عدوانية ضد الجزائر...ويقصد بالتخابر هنـــا الاتصال بالدولة الأجنبيـــة أوالتفاهم معها بأية وسيلة كانت فالتخابر سلوك إيجابي من فرد يقدم معلومات تحفز العدو على القيام بأعمال عدوانية ضد الجزائر، فقد تكون من قبل دس الدسائس لدى الدولة الأجنبية أو حثهـــا على مهاجمة الجزائر أو إعطائها صورة عن الوضع الداخلي للبلاد تظهر نقاط الضعف وتشجعها على القيام بأعمال عدوانية ضد الجزائر

تسليم دولة أجنبية ممتلكات جزائرية:(م 61 فـ3) إذ يقدم الجاني فيها على تسليم قوات جزائرية إلى الدولة الأجنبية. ومثالهـــا أن يكون الجاني قائداً عسكرياً فينحاز بقواته إلى الدولة الأجنبية ويجعلها تحت إمرة العدو لمحاربة بلاده، أو يقوم الجاني بتسليم ممتلكات تمتلكها الدولة الجزائرية إلى الدولة الأجنبيـــة أو عملائهـــا، فالتسليم يقصد به هنا تمكين العدو من الشئ وبسط نفوذه عليه وإسقاط سيادة الدولة وحجب نفوذها عن الشئ المسلم.

الإضرار بالاقتصاد الوطني:(م 61 ف4): يمكننا أن نوجز هذا القول بأن الاعتداء على الدفاع الوطني هـــو إبطال مفعول الأشياء المعدة للدفاع عن البلاد، وجعلها غير قادرة على العمل المعدة له أصلا، بفقدها القـــدرة على القيام بوظيفتها أو الانتفاع المرجو منها.

جناية تسليم أو الاستحواذ أو إتلاف معلومات سّرية :

– **التسليم:** هو نقل المعلومات أو الأشياء أو المستندات أو التصميمات بواسطة الفاعل إلى الدولة الأجنبيـــة. فالمقصود بالتسليم إما يتم عن طرق اليد أو بطرق أخرى كالهاتف أو يسهل له عملية الاطلاع عليه.

– **الاستحواذ:** فهو الحصول على الشئ بحيث يمكنه التصرف فيه أو يفضي بأسراره متى شاء .

– **إتلاف المعلومات السرية** : يقصد بالإتلاف تغييب السر وجعله غير صالح ولا ينتفع به على النحو المعد له أصلا.

– **الأشياء** : يقصد بها الاسرار ذات الكيان المـــادي المحســـوس، وتشـــمل الأســـلحة والـــذخائر والمـــواد الكيماوية...الخ.

– **المستندات:** وهي جميع المحررات المكتوبة كالمذكرات والتقارير...الخ.

– **التصميمات:** وهي الرسوم والخرائط التي تبن مشاريع اقتصادية أو عسكرية...الخ

– **الركن الثاني : الركن المعنوي:** يتوافر الركن المعنوي في هذه الجريمة إذا توافر للجاني القصد العـــام أي علمه بأنه يقوم بأعمال معاقب عليها ، وعن وعي وإدراك تام دون إكراه.

– **الركن الثالث :العقوبة : وقد عاقب عليها النص بالإعدام.**

ملاحظة هذه الجريمة تدعونا إلى القول بضرورة التسريع بتعديله .

2 : الركن الخاص :

يتجسد هذا الأخير في نظام المعالجة الآلية للبيانات الذي هو "كل مجموعة مركبة من وحدة أو عـــدة وحدات الإدخال والإخراج والاتصال والتي تساهم في الحصول على نتيجة معينة"[1].

إذا فهو يمثل المسألة الأولية أو الشرط الأولي الذي يلزم تحققه ،فهـــو إذا تعبيـــر متطـــور يخضـــع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية .

ثانيا : عناصر الجوسسة الرقمية

إن التجسس الرقمي كجريمة حديثة يشبه إلى حد بعيد التجسس كجريمـــة تقليديـــة ،فبالإضـــافة إلـــى الأركان فإنه يستلزم وجود عناصر تتمثل في :

1.الجاسوس:

هو الشخص القائم بعملية التجسس، و يمكن أن يكون من إحدى الفئات التالية:

_**العاملون في المنظمة** : وهم غالبا الساخطون على منظماتهم التي يعملون بها فيعمدون إلى تخريب الجهاز أو إتلافه أو حتى السرقة من خلال عملهم على أجهزة منظمتهم أو من خلال الدخول عليهـــا مـــن اتصـــال خارجي، خطورة في معرفة معلومات حساسة و خطيرة.

[1] . محمد راكان الدغمي، المرجعالسابق،ص:100.

_ **المتسللين الهواة الهاركز**:مقصدهم هو المغامرة و إظهار قدرات أمام الأقـــران،ومنهم العـــابثون بقصـــد التسلية،وهناك المحترفون الذين يختارون الأجهزة المختارة بعناية و يبعثون أو يتلفون أو يسرقون محتويـــات ذلك الجهاز وهي أغلب جرائم الانترنت حاليا هدفهم أهداف خاصة بهم و إيجاد الحلول لمشكلاتهم.

_المتسللين المحترفون الكراكز:

وهم الذين يسعون لسرقة معلومات حساسة من جهات تجارية، حكومية لغرض بيعها على جهات أخرى تهمها تلك المعلومة.ومنهم العاملون في الجريمة المنظمة.

_ إدارة المنظمات

وهم الجهات المتنافسة فيما بينهم إذ يسعى بعضها للوصول إلى معلومات حساسة لدى الطرف الآخر، وذلـــك سعيا للوصول لموقف أفضل من الجهة المنافسة، وغالبا ما يتم بتكليف إدارة المنظمـــات للعـــاملين لـــديها أو المحترفين في الجرائم.

_ **الدوليون** : تقوم حكومات بعض الدول،تسعى من خلال حروب جاسوسية إلى الحصول علـــى معلومـــات إستراتيجية و عسكرية و اقتصادية أخرى إلى التلصص من خلال الحاسب على تلك المعلومات لدول أخرى.

2.الوسيلة :

الحديث عن الوسيلة كعنصر من عناصر الجوسسة الرقمية يقودنـــا مباشـــرة للحـــديث عـــن العـــالم الافتراضي (السبرنتيكي) Cyberspace والذي ترعرعت دلالته ضمن ساحة الاصطلاحات التي صاحبت تقنية الحاسوب والمعلوماتية، فصار يُستخدم للإشارة إلى وصف مجموعة البيئات الحاسوبية المترابطة فيمـــا بينها بوشائج الاتصال والمفاهيم المعرفية التي تسود في الكون المعلوماتي، الذي يرتكز إلى شبكة الإنترنـــت، والشبكة العنكبوتية العالمية، والشبكات الحاسوبية الوطنية والمحلية، ونظم النشـــرات الحاســـوبية Bulletin Board Systemsالتي تؤمِّن الاتصال الحي بين جميع الجهات التي استوطنت هذه البيئات الجديـــدة،وهو يمتاز بـــ:

_ يمتاز الفضاء الحاسوبي بكونه يمتلك وجودًا افتراضيًّا .

_ يمتاز الفضاء الحاسوبي لشبكة الإنترنت بامتداد وانتشار هائل[1].

_ سهولة تدفق المعلومات بين المواقع الإلكترونية.

تنشأ الجريمة في الفضاء الافتراضي عبر اعتماد مبدأ الاختراق المعلوماتي لحدود نظام مـــن الـــنظم السائدة في هذا الفضاء؛ وذلك لمباشرة زمرة من الأنشطة غير المشروعة ويمكن تحديد هذه الجرائم حســـب الجدول التالي :

[1]يونس عرب .التشريعات والقوانين المتعلقة بالأنترنت في الدول العربية ،ورقة عمل مقدمة إلى مؤتمر ومعرض التكنولوجيـــات المصـــرفية العربيـــة والدولية ،إتحاد المصارف العربية ،28_2002/11/29،عمان ،الأردن.

الجرائم الماسة بأمن الدولـــة الخارجي.	السعي والتخابر مع دول أجنبية.
	تخريب وسائل الاتصالات، أو مؤسسات حيوية.
	استفادة منفعة مادية من دول أخرى للإضرار بمصلحة وطنية.
	الحصول بطريقة مشروعة على سر من أسرار الدولة.
	إشاعة، أو نشر، أي معلومة من المعلومات الحكومية المحظورة.
الجرائم الماسة بـــأمن الدولـــة الداخلي.	إتلاف جزء من مرافق الدولة، أو المصالح الحكومية.

ثالثا : مواجهة الجوسسة الرقمية

1: المواجهة التقنية

الأفراد في إدارتهم لتعاملهم مع الإنترنت يمكنهم استخدام وسائل جديدة لحماية خصوصياتهم ، فمـــن البريد المتخفي anonymes mailers والمتصفحات التي تسمح بالتجول دون كشف الهوية عبر الإنترنت web browsers That allow individuels to interact anonymously وحتى برمجيات التشفير encryptions programs التي تحمي البريد الإلكتروني والتراسل عبر الشبكة.

2:المواجهة القانونية

يبدو أن الأمر على عكس ما يتمناه كثير من القراصنة ومستغلي الفضاء الافتراضي من أجل ارتكاب جرائم السطو والسرقات، وجرائم التشهير، والمساس بالحياة الخصوصية للأفراد والتجســـس علـــى الـــدول، فالانترنت ليس فضاء اللاقانون، وليس فضاءا تسوده الفوضى، تحت غطاء اعتباره مجالا للحريـــة المطلقـــة الشاملة، وليس عالما افتراضيا لا يحكمه أي ضابط،إنه وسيلة لإرسال واستقبال المعلومات والحصول عليهـــا من مختلف الأماكن وبسرعة مذهلة ،الأمر الذي دفع بالدول إلى وضع قواعد قانونية تحمي من الأخطار التي قد تنجم عنه ،لكن هل عالج المشرع الجزائري مسألة الجوسسة الرقمية ؟أم اكتفى بالقواعد التقليدية ؟

بالرجوع إلى قواعد قانون العقوبات نجد أن المشرع الجزائري اكتفى بالمساواة بين جريمة التجســـس التقليدية وخيانة الأمانة من الناحية العقابية ،دون الإشارة إلى هذا النوع الجديد من الجرائم الماسة بأمن الدولة الخارجي بل حتى الداخلي في الكثير من الحالات مما يدفعنا إلى التساؤل هل يمكن القيـــاس علـــى العقوبـــة المقررة للجريمة التقليدية

فنجيب بالقول أن القاضي لا يستطيع الاعتماد على القياس في الجانب الجزائي .كما أنه لا يســـتطيع تجريم فعل لم يجرمه المشرع ، لذا استدرك المشرع الجزائري الفراغ القانوني من خـــلال تعـــديل قـــانون العقوبات المشار الذي تمم الفصل الثالث من الباب الثاني من الكتاب الثالث من الأمر (156/66) بالقســـم السابع مكرر، عنوانه " **المساس بأنظمة المعالجة الآلية للمعطيات** "، و يشمل المواد من **394 مكـــرر** إلـــى المادة **394 مكرر 7** . دون إشارة منه إلى جريمة التجسس الرقمي .

الخاتمة:

جرائم التجسس تعد أهم الجرائم التي تقع على الدولة مهددتا لكيانها ، والجوسسة الرقمية أو كما يحلو للبعض تسميته بالتجسس الإلكتروني هو النوع الجديد والمتطور للتجسسس كجريمة سياسية .

يقصد به : أحد الأنواع والسبل في الحروب أي أنه يمثل "خطرا داهما" يهدد كيان الدولة كنا يمكن القول بأنه :

- التجسس الإلكتروني يمتاز بالتشعب والتداخل والتغير والتطور السريع .
- نتيجة حتمية لما أفرزته التكنولوجيا وعلوم العصر كالأقمار الصناعية والشبكة العنكبوتية .
- المظهر الجديد والحديث للتجسس.

كما يمكن الوصول إلى جملة النتائج التالية :

- التجسس الإلكتروني محصور ضمن دائرة الجرائم المعلوماتي ذات النوع الخاص
- المشرع الجزائري لم يضع تعريفا واضحا للتجسس الدولي ،وكذلك للتجســـس الإلكترونـــي لكـــي لا يحصره في مجال محدد.
- المشرع الجزائري لم يضع آليات قانونية ولا جنائية لمحاربة هذه الظاهرة الإجرامية رغم خطورتها.

لكي يحارب المشرع الجزائري هذه الجريمة لابد عليه من بناء سياسة دفاعية قانونية واضحة تقـــوم على:

- اعتبار التجسس الرقمي جريمة ذات طبيعة مزدوجة أي جريمة أموال وجريمة سياسية .
- وضع نصوص قانونية واضحة ومحددة تكون بمثابة المبادئ العامة لمكافحته .
- تعزيز وتفعيل التعاون الدولي في مجال مكافحة التجسس الإلكتروني .
- إعادة النظر في مبادئ السياسة الجنائية بما يتماشى والتطور الحاصل ،خاصة فيما تعلق بمبدأ إقليمية وعالمية النص.

المراجع:

1.أحمد حسام طه تمام ،الجرائم الناشئة عن إستخدام الحاسب الآلي ،دار النهضة العربية ،

2. فيل وليامز ،الجريمة المنظمة وجرائم الشبكات الالكترونية ،مركز خبرات امن الانترنت في جامعـــه ميلـــون كـــارينجي- 2002

3. رمضان الألفي. " العولمة والأمن " الانعكاسات السلبية والإيجابيـــة كدراســـات اقتصـــادية، مركـــز الدراســـات السياســـية والإستراتيجية. الأهرام ، السنة الثانية 1998، العدد 27، ص 5،ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتيـــة والقانون ،طرابلس 27_2009/10/30..

4 Herbert Burkert، Privacy-Enhancing Technologies: Typology، Critique، Vision، in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE، 125,142 (Philip E. Agre & Marc Rotenberg، eds. MIT Press 1997).

5.عبد الفتاح مراد، شرح جرائم الكمبيوتر والأنترنت، دار الكتب والوثائق المصرية،

6.أسامة الكشواني ،التجسس الإلكتروني وطرق مكافحته ،جريـــدو أســـواق العـــرب ،عمـــود التكنولوجيـــات العربيـــة ،يـــوم 2007/6/6:، مصر .

7.هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة 1992.

8. محمد راكان الدغمي، المرجعالسابق،

9.يونس عرب .التشريعات والقوانين المتعلقة بالأنترنت في الدول العربية ،ورقة عمل مقدمة إلى مؤتمر ومعرض التكنولوجيات المصرفية العربية والدولية ،إتحاد المصارف العربية ،28_2002/11/29،عمان ،الأردن.