جامعة أبو بكر بلقايد – تلمسان

كلية الحقوق والعلوم السياسية

قسم القانون الخاص

الأسرار المعلوماتية وحمايتها الجزائية

أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص

تحت إشراف

أ .د : تشوار جيلالي

من إعداد الطالبة:

رابحي عزيزة

لجنة المناقشة

أ.د. بدران مراد:	أستاذ التعليم العالي	جامعة تلمسان	**رئيسا**
أ.د. تشوار جيلالي:	أستاذ التعليم العالي	جامعة تلمسان	**مشرفا مقررا**
أ.د.بوسندة عباس:	أستاذ التعليم العالي	جامعة سيدي بلعباس	**مناقشا**
أ.د. بموسات عبد الوهاب:	أستاذ التعليم العالي	جامعة سيدي بلعباس	**مناقشا**

السنة الجامعية

2018-2017

قال تعالى:

" وَأَسِرُّوا قَوْلَكُمْ أَوِ اجْهَرُوا بِهِ إِنَّهُ عَلِيمٌ بِذَاتِ الصُّدُورِ "

سورة الملك، الآية 13

تشـــــــكرات

بسم الله الرحمان الرحيم

"رب أوزعني أن أشكر نعمتك التي أنعمت علي وعلى والدي وأن أعمل صالحا ترضاه وأدخلني برحمتك في عبادك الصالحين".

"سورة النمل الآية 19"

فما يسعني إلا أن أشكر الله سبحانه وتعالى وأسأله التوفيق، وأتقدم بالشكر الجزيل للأستاذ المشرف "الأستاذ الدكتور تشوار جيلالي" الذي تشرفت بالنّهل من علمه والاستفادة بتجربته وتوجيهاته،والشكر موصول إلى السادة أعضاء لجنة المناقشة على تحملهم عناء مطالعة ومناقشة هذه الأطروحة.

إهـــــــــداء

إلى من أوصاني بهما ربي برا وإحسانا والداي الكريمان

حفظهما الله وأدام صحتهما وعافيتهما

إلى رفيق دربي زوجي العزيز، إلى أبنائي وبناتي الأعزاء

إلى البنيان المرصوص إخوتي وأخواتي

وثق الله رباطنا

إلى كل صديقاتي وإلى كل من أحب

أهدي عملي هذا

مقدمة

لطالما سعت التشريعات الجزائية للحفاظ على السرية، وذلك من خلال تجريم إفشاء الأسرار المهنية والتجسس وحماية حرمة الحياة الخاصة والمعلومات غير المفصح عنها[1] وغيرها. إذن لم تكن التشريعات قد تجاهلت حماية حق الأشخاص في الحفاظ على أسرارهم باختلاف أنواعها، ولطالما ارتبطت حماية السرية أساسا بالأسرار المهنية على وجه الخصوص.

ولكن الحماية الجزائية للسرية اليوم وبالمفهوم الحديث لابد أن تتغير، وذلك لارتباطها بتقنية حديثة ألا وهي النظم المعلوماتية، تلك النظم التي اكتسحت الحياة العامة والخاصة وتعالج بواسطتها الأسرار معالجة الكترونية لتختزن أو تنتقل بواسطتها أو من خلالها.

تبعا لهذا المفهوم الجديد كان لزاما على التشريعات الجزائية أن تتغير من أجل تكيف منظومتها القانونية والمفهوم الحديث حتى تكون قادرة على التصدي للأشكال المستحدثة لانتهاك السرية، فالسرية سابقا كانت تنتهك بإفشاء الأسرار المهنية أو انتهاك حرمة الحياة الخاصة للأفراد، بينما اليوم هي تنتهك بأشكال مستحدثة إذن لابد من التصدي لها بنصوص مستحدثة.

إن مفهوم السرية قد تغير في زمن اكتسبت فيه الأنظمة المعلوماتية والأجهزة الالكترونية عموما أهمية كبيرة، وهي بتطورها السريع قد أصبحت عنصرا أساسيا لتحقيق تقدم الأمم وذلك من خلال تسهيل التحكم في المعطيات السرية ومعالجتها واسترجاعها، وتعتبر في الوقت ذاته معيارا لقياس مدى تحضر هذه الأمم. معنى ذلك أن ما يتمتع به الحاسب الآلي والهواتف الخلوية الذكية وشبكة الانترنت من إمكانيات وقدرات جعلتهم يكتسحون الحياة العامة والخاصة، فأينما شئت فأنظر ستجد هذه الأجهزة خاصة الحواسيب في المستشفيات في البيوت في المدارس في البحار في الفضاء وسترى أن جهاز الحاسوب يمتد أثره لكل ما يقع عليه البصر[2].

إذن ما يميز العصر الحالي عن غيره هو ما نشهده اليوم من تطور مثير في المجال الالكتروني، حيث اكتسحت الحاسبات الآلية والهواتف الذكية والأنظمة المعلوماتية بصفة عامة كل المجالات، بحيث يمكن القول أن أهم تكنولوجيا عرفها هذا العصر بل وربما عرفتها البشرية على مر عصورها المختلفة كانت تكنولوجيا الحاسبات الآلية وما ترتبط بها من شبكات اتصال، في حين بالنسبة للهاتف الذكي فإننا يمكننا القول بشأنه أن بعضها لا

1- هناك من التشريعات من اعتبرت حماية المعلومات غير المفصح عنها أو غير المصرح عنها يندرج ضمن حقوق الملكية الفكرية منها المشرع المصري الذي نظمها في المواد 55-62 في قانون حقوق الملكية الفكرية المصري رقم 82 لسنة 2002 المؤرخ في 02 يوليو 2002، مواكبا في ذلك اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تريبس) بتاريخ 1994/04/15 التي أسمتها المعلومات السرية في المادة 39 منها.

2- وعلى هذا الأساس قد تغير حتى مفهوم إفشاء الأسرار المهنية ليتحول إلى مهنية معلوماتية، فأين قد تجد إدارة أو مهني أو حرفي ويمارس وظيفته أو مهنته بدون النظام المعلوماتي.

يمكن أن نجزم إلى أي فئة ينتمي، هل هو هاتف أم حاسوب؟ حيث أنه هناك تشابه كبير بين النظام المعلوماتي للحاسوب والنظام المعلوماتي للهاتف الذكي[1].

ولقد صاحب هذا التطور في الأجهزة الالكترونية تزايدا ملحوظا في الاعتماد على نظم المعلومات الآلية والتكنولوجيا[2] القائمة على الحواسيب كوسائل رئيسية لحفظ ومعالجة وتشغيل البيانات داخل معظم المؤسسات الحكومية وغير الحكومية، بل وبين الأفراد في حياتهم اليومية[3]. وكان من الطبيعي أن يصاحب هذا التطور التكنولوجي ارتكاب بعض الجرائم التي لم تكن معروفة من قبل، أو ارتكاب جرائم تقليدية بأساليب مستحدثة اعتمادا على هذا التطور، وحيث أن الجريمة ظاهرة اجتماعية تعكس الواقع وتتفاعل مع متغيراته وتستجيب لتطوره، فقد أفرزت هذه الابتكارات جرائم جديدة غير معتادة عكست الواقع واستخدمت أدواته واتصفت بسماته حتى أنها اقترنت باسمه فأطلق عليها جرائم الحاسب الآلي.

ولما كانت جرائم الحاسبات الآلية[4]، أو كما يطلق عليها الفقه جرائم المعلوماتية[5] لارتباطها بالمعلومات المبرمجة آليا وارتباطها بتكنولوجيا حديثة هي تكنولوجيا الحاسبات الآلية، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير

---

[1] وتجدر الإشارة إلى أنه من الضروري التفرقة بين النظام المعلوماتي للحاسوب وبين جهاز الحاسوب ذاته، أنظر محمد أحمد فكيرين، أساسيات الحاسب الآلي، دار الراتب الجامعية، بيروت، بدون طبعة، 1993، ص 7.

[2]– التكنولوجيا منهج علمي جديد قوامه أعداد الأجهزة التي يمكن بها نقل العلم النظري إلى التطبيق العلمي.

[3] فهذه الحاسبات مع ما توصل به من أجهزة اتصالات أصبحت موجودة في كل المجالات، وبدونها فإن مجالات عديدة كالصناعة والاقتصاد والتجارة والنقل والطب والدفاع والتعليم والبحوث...وغيرها، كانت ستصبح أقل كفاءة مما هي عليه الآن، ويرجع ذلك بصفة أساسية إلى عاملي السرعة والدقة اللذين توفرهما هذه الحاسبات. بحيث أصبح من الصعب إن لم يكن من المستحيل أن تقوم القطاعات المختلفة بأداء أعمالها دون الاعتماد بشكل أساسي على الحسابات الآلية، ولاشك أن اتصال الحاسبات الآلية بوسائل الاتصال قد ضاعف من أهميتها ومن الاعتماد عليها، كما أن هذا الاتصال قد أثمر عن أوجه أخرى للتقدم العلمي والتكنولوجي في هذا المجال، لعل أبرزها على الإطلاق ظهور شبكات المعلومات والشبكات الاتصالية المتشعبة. كما أن التطور الفائق في أجهزة الهاتف النقال أصبحت بموجبه تلك الأجهزة أكثر من مجرد وسيلة اتصال صوتي بحيث تستخدم كأجهزة كمبيوتر وتصفح الانترنت وإرسال للرسائل وغيرها .

[4]– سنحاول الاقتصار في هذه الدراسة على جرائم الحاسبات الآلية ذلك لأن جرائم الهاتف المحمول هي جرائم معلوماتية ترتكب بواسطة الهاتف المحمول الذكي وكأنه حاسوب وذلك للتشابه بين إمكانياته بالحاسوب وتفاديا للتكرار سنقتصر على جرائم الحاسبات الآلية دون الهواتف الذكية، حيث تمثل جرائم الهاتف المحمول الذكي تقريبا نفس جرائم الحاسب الآلي إضافة إلى البعض الآخر الذي يتميز بها الهاتف المحمول والتي تعتبر هي أيضا تهديدا للسرية كالاعتداء على الحق في الصورة مع العلم أنها ترتكب غالبا بواسطة الهواتف الذكية وفي أغلب الأماكن حتى العامة منها.

[5]– نشير في هذا الصدد أنه لا يوجد مصطلح قانوني موحد للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر وفيما بعد في بيئة الشبكات وهو تباين رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط والمتصل بالتقنية العالية.فثمة تباين كبير بشأن تلك الاصطلاحات فابتداء من اصطلاح احتيال الكمبيوتر فاصطلاح جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر والجريمة المعلوماتية، جرائم التقنية العالية، جرائم الاختراقات أو الهاكرز، الغش المعلوماتي، ظاهرة الاختلاس المعلوماتي، جناح المعلوماتية جرائم التكنولوجيا الحديثة إساءة استخدام تقنية المعلومات، الجرائم المستحدثة، وغيرها إلى جرائم الكمبيوتر والانترنت، أو تقنية المعلومات.

من الغموض، حتى دعا ذلك الكثيرين إلى القول بأن الجريمة المعلوماتية هي أشبه بالخرافة، وأنه لا يوجد تهديد حقيقي منبعه الحاسبات الآلية، وأن كافة أشكال السلوك غير المشروع التي قد ترتبط بالحاسبات الآلية هي في حقيقتها جرائم عادية يمكن بشأنها تطبيق النصوص التقليدية القائمة، دون أن تتميز بأية سمات خاصة.

وقد أسفرت محاولات تطبيق النصوص التقليدية على هذه الأنماط الجديدة من الإجرام عن كثير من المشكلات القانونية، وقد اختلفت آراء الفقهاء في شأن تطبيق النصوص التقليدية عليها، وتضاربت أحكام القضاء في البلد الواحد، فصدرت أحكام تطبق النصوص التقليدية على أي سلوك ينطوي على اعتداء على المعلومات المخزنة في الحاسبات الآلية أو استعمالها غير المشروع، في حين اعتبرته أحكام أخرى فعلا مباحا لم يرد بشأنه نص يجرمه، بينما رأى البعض الآخر أن تلك النصوص ينحصر نطاق تطبيقها على الإحاطة بجرائم الحاسب الآلي لأن موضوعها يكمن في المعلومات التي لا يمكن اعتبارها مالا منقولا لا تنسحب إليه الحماية الجنائية بمقتضى تلك النصوص.

ولما كان القانون هو الوسيلة المثلى لتنظيم المجتمع وضمان أمن واستقرار الأفراد في حياتهم وأعراضهم وأموالهم، ولما كان المجتمع في تطور مستمر ودائم في جميع مجالات الحياة المختلفة فإن ذلك يفرض على التشريعات أن تتطور هي أيضا وبشكل تواكب معه حركة المجتمع المتنامية وتساير التطورات التكنولوجية والاجتماعية وغيرها، من خلال تنظيمها بأحكام تتلاءم مع هذه المتغيرات والتطورات.

وكما أدى ازدياد العمل بالحاسب الآلي إلى نشوء جرائم ناتجة عن ذلك الاستخدام زاد من خطورة هذه الأخيرة ظهور الشبكة العنكبوتية "الانترنت"، واستخدام الوسائط الحاسوبية وشبكات الإنترنت لارتكاب سلوكيات الجريمة أو التخطيط لها، ساهمت التكنولوجيا منذ نشأتها بتغيير الكثير من المفاهيم التي اعتاد الناس عليها، وتباينت هذه التغييرات بين السلبية والإيجابية، ففي الوقت الذي قامت فيه التكنولوجيا على سبيل المثال بتقريب المسافات بين الشعوب، من خلال توفيرها العديد من وسائل الاتصالات ووسائل التنقل التي لم تكن معروفة من قبل، نجد أن تلك التكنولوجيا أفرزت الكثير من السلبيات، لعل أهمها كان صعوبة تحقيق أمن المعلومات وذلك جراء انتشار الكثير من الوسائل التي سهلت الوصول إليها والاعتداء عليها ومن بين صور الاعتداءات تلك انتهاك سريتها.

وحيث تعتبر السرية المعلوماتية بندا ضروريا للحياة الكريمة في المجتمع الحديث وذلك مع انتشار تقنية المعلومات وزيادة الاعتماد عليها، ومع تضخم حجم البيانات والمعلومات المخزنة تضخما هائلا ومع انخفاض

تكلفة معالجة تلك البيانات والمعلومات، فإن الحاجة للسرية المعلوماتية تزداد باستمرار مع زيادة تحول الأنشطة المهمة من العالم المادي إلى عالم الكمبيوتر.

إن الاطلاع على المعلومات المخزنة في جهاز الحاسوب بشكل مباشر عن طريق الولوج إليها من نفس الجهاز، أو غير مباشر عن طريق الولوج إليها عبر شبكة الانترنت والاطلاع عليها قد تنجر عنـه سلوكيات أخطـر، لهذا تم تجريم كل سلوكيات الاعتداء على سرية المعلومات وأيا كانت طريقتها والهدف منها.

فما دفع بي إلى الاهتمام بالموضوع هو ما يتمتع به النظام المعلوماتي من قدرة هائلة على التخزين المعلوماتي ومن إمكانيات تكنولوجية تكاد لا تقف عند حدود، فهي في تطور مستمر وتجدد لا يهدأ وصور استخدام لا تعد، ومنه أصبح بواسطته من الممكن جدا اقتحام الخصوصية الفردية والجماعية وهتك سرية المعلومات بجميع أنواعها وبمختلف أشكال الاعتداء.

ومع تطور الانترنت وتوسع استخداماته وازدياد أعداد المستخدمين له في العالم أصبح الانترنت وسطًا ملائمًا للتخطيط ولتنفيذ عدد من الجرائم بعيدًا عن رقابة وأعين الجهات الأمنية، إضافة إلى أنه ثبت أن المجرمين المعلوماتيين ليسوا بأشخاص عاديين فهم يتمتعون بقدر كبير من الذكاء والدهاء، ويتحكمون في التقنيات التكنولوجية الحديثة وهم قادرون على الذهاب بعيدا في ممارسة الإجرام عن طريق الانترنت، مما يستدعي توفير الأمن المعلوماتي[1].

فعند ذكر كلمة أمن المعلومات[2] فإن أول ما يتبادر إلى الذهن غالبا هو كشف معلومات كان يجب أن تبقى سرا، والحقيقة أن الحفاظ على سرية المعلومات لا يعدو أن يكون جانبا واحدا من جوانب الأمن[3] حيث أن فكرة الأمن المعلوماتي وتطويره بات أمرا حتميا أمام قيام إمبراطورية المعلوماتية[4].

---

[1] يمكن تعريف أمن المعلومات بأنه:" العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أوالاعتداء عليها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية"، عن صليحة علي صداقة، الأبعاد القانوني والأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية الإسكندرية، بدون طبعة، 2017، ص 187.

[2] لأمن المعلومات مكونات ثلاثة على درجة واحدة من الأهمية وهي:

أ-سرية المعلومات: يشمل اتخاذ كل التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات السرية.

ب- سلامة المعلومات:ويقصد اتخاذ الإجراءات اللازمة لحماية المعلومات من التغيير.

ج-ضمان الوصول إلى المعلومات والموارد الحاسوبية: عدم حرمان المستفيد من الوصول إلى المعلومات حيث لا يجوز حذفها مثلا إلا ممن يحق لهم دلك.

أنظر تفاصيل عناصر أمن المعلومات صليحة علي صداقة، مرجع سابق، ص 190-191.

[3] خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، جامعة الملك سعود ، الطبعة الأولى، 2009، ص22.

[4] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دارالهدى للطباعة والنشر ، الجزائر ، 2011 ، ص 7.

وحيث أنه أثيرت الكثير من المشكلات حول المسؤولية الناجمة عن جرائم المعلوماتية فيما يتصل بالاعتداءات الموجهة إلى الكيانات غير المادية للحاسب، وبالتالي فإن الجرائم التي تستهدف الكيانات المادية لأنظمة الحاسب ليست في الحقيقة ضمن مفهوم جرائم الحاسب، على الأقل من الوجهة القانونية ولا يثير تحديد موضوع هذه الجرائم أو محل الاعتداء أية مشكلة، فنصوص التجريم التقليدية والأحكام العامة للجريمة منطبقة دون شك على مثل هذه الجرائم شأنها في ذلك شأن ماديات الحاسب، أي ماديات ممثلة لمنقولات معتبرة مالا بغض النظر على شكلها ودورها أو وظيفتها في النشاط الإنساني، إذ لا نعرف ما يحمل إلينا المستقبل من منجزات ومبتكرات تقنية لا تتجاوز حدود تفكيرنا فحسب بل تتجاوز حدود خيالنا ، ولكن مادامت الطبيعة المادية متوفرة في موضوع الجريمة فإن ما شيد حتى الآن من نظريات وقواعد وأحكام ونصوص في نطاق القانون الجنائي الموضوعي بقسميه العام والخاص نفترض أنها كفيلة بمواجهتها، وما شرع في نطاق الإجراءات الجنائية والإثبات ربما كفيل بسيادة حكم القانون الموضوع عليها.

إن حماية نظم المعلومات (بمكوناتها غير المادية) وما تحمله من معلومات سرية هي مسألة تقنية بالدرجة الأولى يهتم بها صاحب الحق الذي يريد حمايته، كما يهتم بها نظام العدالة الجنائية في المجتمع باعتبار أن موضوع السياسة الجنائية هو تأمين تماسك وبقاء الكيان الاجتماعي بضمان تأمين حماية الأشخاص والأموال في المجتمع.

فاستهداف المعلومات التي في الحقيقة هي موضوع الجريمة ومحل الاعتداء عليها، يأخذ أنماط السلوك الإجرامي التي تطال المعلومات المختزنة أو المعالجة في نظام الحاسب أو المتبادلة عبر الشبكات، وهي إما أن تمثل أموالا أو أصولا أو أسرارا أو بيانات شخصية أو غيرها، وعموما اعتبرت أسرار لكي تخفى عن الغير، معنى ذلك أن صاحبها لا يريد أن يعلم بها غيره أو أن يعلم بها عدد محدود ويريد إخفائها عن البقية.

فتلك المعلومات المعالجة آليا[1] في حاجة للحماية، وهو ما قادنا إلى البحث في الأسرار المعلوماتية وحمايتها جزائيا، فالسرية[2] المعلوماتية سواء تعلقت بالأفراد أو بالمجتمع أو الدولة أو غير ذلك لا يجوز اختراقها أو انتهاكها أو إفشاؤها لغير المخولين الاطلاع عليها أو العلم بها، فالاطلاع على تلك الأسرار قد يكون بقصد الاطلاع وقد

[1] تلك المعلومات تكون مختزنة في النظام المعلوماتي ونحن نؤكد هنا على ذاكرة الحاسوب أوما في حكمه أوالتي في طريقها منه أو إليه.

[2] وفي هذا الصدد نقصد بسرية المعلومة ليس فقط السرية في حد ذاتها، بل أيضا يجب إضفاء السرية على المعلومات التي قد تكون عناصرها معروفة للعامة غير أن تجميعها وترتيبها ربما يحتاج إلى بدل مجهود وإنفاق مبالغ كثيرة ، مثلما هو الشأن بالنسبة لهده الدراسة قبلما تناقش. إضافة إلى أنه لابد من ضوابط للمعلومات محل الحماية يفترض توافرها فيها وهي الجدية وأن يكون لهده المعلومات قيمة معتبرة في مجالها وأيضا أن تتخذ تدابير جدية للمحافظة على سريتها بحسب الظروف وبقدر الامكان من قبل الحائز الشرعي للمعلومات، مثلما هي التدابير التي اتخدتها شركة كوكا كولا للحفاظ على سر الوصفة.

يكون بقصد الإضرار بالغير، كأن يكون الغرض من الحصول عليها الإفشاء أو التشهير أو الابتزاز أو النسخ وفي كل الأحوال هو غير جائز.

إذن لقد بات من المستعجل أن تجرم تلك السلوكيات، وقد تم تجريمها فعلا على جميع الأصعدة الدولية والداخلية كما سيتم التفصيل في متن هذه الدراسة، حيث سارعت الدول إلى سن قوانينها أو تحديثها بما يتناسب وتلك السلوكيات غير القانونية المستحدثة وهو ما عبر عنه بالجريمة المعلوماتية، إذن كانت الحاجة ملحة لتحديث التشريعات.

إن تفاقم الاعتداءات على الأنظمة المعلوماتية، استدعى تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي، فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي وهي اتفاقية بودابست والتي تضمنت مختلف أشكال الإجرام المعلوماتي[1]،إضافة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010[2]، والتي صادقت عليها الجزائر في سنة 2014 [3].

أما على المستوى الداخلي، فكانت السويد أول دولة تضع قانونا لتنظيم سجلات الحاسب الآلي وحماية البيانات، وقادت موجة التشريع في هذا المجال من خلال قانون عام 1973 بشأن حماية البيانات[4].

كما ظهر أول نص قانوني في مجال جرائم المعلوماتية سنة 1988[5] في فرنسا، رغم أنه قبل ذلك كانت أول المحاولات لمد سلطان قانون العقوبات لحماية المال المعلوماتي بفرنسا من طرف وزيرها للعدل وذلك سنة 1985، عندما تقدم بمشروع قانون عقوبات جديد، أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان "الجرائم في المادة المعلوماتية " يتكون من ثمانية مواد(من 1/307 إلى 8/307)، لكن هذا المشروع لم يجد سبيله للتطبيق.

---

[1] اتفاقية بودابست (الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية) بتاريخ 2001/11/08 والتي وضعت للمصادقة في11/23/ 2001 كما أنه على الصعيد الدولي أيضا هناك مقترحات وتوصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات 4-9 جانفي 1994 – البرازيل، ريودي جانيرو بشأن جرائم الكمبيوتر والذي تضمن توصيات في شقين موضوعي وإجرائي، أيضا هناك القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء، هافانا 1990 قرار بشأن الجرائم ذات الصلة بالكمبيوتر وتوصيات لجنة الوزراء بالاتحاد الأوروبي في إطار معالجة المشكلات الخاصة بالجرائم المعلوماتية مثلا التوصية رقم (88) 2 بشأن القرصنة في مجال حقوق النشر والتأليف والحقوق المجاورة والتوصية رقم (95) 4 بشأن حماية البيانات الشخصية في مجال خدمات الاتصالات، للتفاصيل أكثر في ذلك أنظر رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، القاهرة، الطبعة الأولى، 2011 ، ص 64 وما بعدها.

[2] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010.

[3] صادقت عليها الجزائر بموجب مرسوم رئاسي رقم 14-252 مؤرخ في 13 ذي القعدة عام 1435 المافق 8 سبتمبر 2014، الجريدة الرسمية العدد 57، ص 4.

[4] Michael (J) Privacy and Human Rights: An international and comparative study wide special reference to developments in information technology.dartmouth(1994).p.12.

[5]Loi n°88-19 du 05 janvier 1988 relative à la fraude informatique, JORF du 06 janvier 1988.(LOI GODFRAIN).

أما المحطة التالية من محطات التجريم المعلوماتي فكانت عام 1994[1]،ثم توالت التشريعات في سنة 2004[2]، 2009[3]، 2012[4]، 2013[5] ثم 2014 [6]، بينما تعديل 2016 لم يشمل الجرائم المعلوماتية بالتعديل.

وقبل صدور قانون 88-19 لـ 5 جانفي1988 المتعلق بالغش المعلوماتي، الفصل الثالث من قانون العقوبات الفرنسي تحت عنوان "بعض الجرائم في مجال المعلوماتية"، صدر قانون رقم 78-17 المتعلق بالمعلوماتية[7]، والجدير بالذكر أن هذا القانون حدد في المادة 2 منه معنى عبارة المساس بالمعطيات أنها عندما يقوم شخص أو كيان بانتهاك سرية المعطيات.[8]

إذن شهد العالم في الآونة الأخيرة تطورا مذهلا وسريعا في مجال المعلوماتية، ومنه تسارع المشرعين لسن قوانين الهدف منها هو المواجهة الموضوعية والإجرائية لهذا النوع من الجرائم، قياسا على تسارع وتيرة الاعتماد على المعلوماتية في شتى مناحي الحياة، حتى باتت ضرورة لا يمكن الاستغناء عنها، وأصبحت مقياسا لتطور الدول، والجزائر ليست بمنأى عن هذا التحول المعلوماتي، وهي وإن لم تبلغ مصاف الدول المتقدمة، فإنها قد تأثرت بهذه الثورة المعلوماتية سلبا وإيجابا، حيث تأثرت بما جرته هذه الثورة من ألوان جديدة من جرائم لم تشهدها البشرية من قبل ارتبطت ارتباطا وثيقا بالحاسب الآلي وما حواه من معطيات.

هذه الجرائم طالت مصالح جديدة غير تلك التي يحميها قانون العقوبات، فبدت الحاجة شديدة لوضع نصوص جديدة، ولم يجد المشرع الجزائري خيار سوى تعديل قانون العقوبات، ولقد جاء في عرض أسباب هذا

---

[1] Loi n° 92-683 du 22 juillet 1992, portant réforme du code pénal, texte origine au 01 mars 1994.

[2]- Loi n° 2004-575 du juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 200.

- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004 page 14063, texte n° 2.

-Loi n° 2004-575 du juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004

-Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF 10 mars 2004 en vigueur le 1er octobre 2004.

[3] Loi n° 2009-1311 du 28 octobre 2009 relative à la protetion pénale de la propriété littéraire et artistique sur internet, JORF Du 29 Octobre 2009, texte 1 sur 183.

[4] Loi n° 2012-287 Du 1er mars 2012 relative à l'exploitation numérique des livres indisponibles du XXe siècle, JORF Du 2 mars 2012, texte 1 sur 133.

Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, JOPF n°0075 du 28 mars 2012, texte n°2, P5604,(art 9 modifie les articles 323-1,323-2,323-3 de code pénal français).

[5] loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n°0294 du 19 décembre 2013 page 20570 texte n° 1

[6] Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lute contre le terrorisme, art. 16, JOPF n° 0263 du 14 novembre 2014

[7]Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978.

[8] Laure Zicry, Enjeux et maitrise des cyber-risques, édition Largus , France,2014, p.53.

التعديل "أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدت إلى بروز أشكال جديدة للإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجزائر على غرار هذه الدول سعت من خلال قانونها إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وأن هذه التعديلات من شأنها سد الفراغ القانوني في بعض المجالات، وكان التعديل بموجب القانون رقم15/04[1]، والذي أدخل إلى قانون العقوبات بقسم سابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، والذي تضمن ثمانية مواد (من المادة 394 مكرر إلى المادة 394 مكرر07).

إذن لم يقف المشرع الجزائري بالطبع متفرجا، حيث سارع هو أيضا إلى سن قوانين تتلاءم وطبيعة الجرم المستحدث، فقد استدرك الفراغ القانوني من خلال القانون رقم 04-15 سالف الذكر.

كما أصدر المشرع الجزائري القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام[2] والاتصال، إضافة إلى الاتفاقيات الدولية التي أبرمتها الجزائر لمكافحة الجريمة المعلوماتية[3].

وفي إطار مكافحته للجريمة في الجزائر صدر المرسوم الرئاسي رقم 288/15 المتعلق القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره[4]، حيث أن هذا الأخير هو أداة تقنية للاطلاع والاستباق يهدف إلى المساهمة في الوقاية من الأعمال الإجرامية و حماية الأشخاص و الممتلكات و الحفاظ على النظام العام تطبيقا للمادة 2 من المرسوم 288/15.

ورغم استحداث نصوص خاصة بالجرائم المعلوماتية إلا أنه في حالة غياب النص في بعض الأحوال فإنه لا مانع من تطبيق النصوص التقليدية في حالة ارتكاب جرائم تقليدية بواسطة تقنية معلوماتية، إذ أن الجرائم المعلوماتية التي تستدعي تطبيق نصوص عقابية خاصة هي التي استحدث لها نصوصا.

فالسرقة المعلوماتية مثلا يمكن تجريمها من خلال النصوص العقابية التقليدية، ذلك لأن المشرع الجزائري وغيره من غالبية المشرعين لم يخصصوا لها نصا عقابيا مستحدثا.

---

[1] القانون رقم 15/04 المؤرخ في العاشر من نوفمبر عام 2004 الموافق للسابع والعشرين من رمضان لسنة 1425 هجرية المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، جريدة اسمية مؤرخة في 10نوفمبر 2004، عدد 71، ص 8.

[2] القانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 هـ الموافق لـ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها والذي أدخل حيز التنفيذ بموجب الجريدة الرسمية الصادرة بتاريخ 16 أوت 2009، العدد 47.

[3] أبرمت الجزائر العديد من الاتفاقيات الدولية لمكافحة الجريمة المعلوماتية فمثلا من خلال المرسوم الرئاسي رقم 07-375 المؤرخ في أول ديسمبر 2007 المتضمن التصديق على الاتفاق بين الحكومة الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، الموقع في الجزائر في 25 أكتوبر 2003 ، جريدة رسمية عدد 77 المؤرخة في 9 ديسمبر 2007، ففي المادة الأولى منه أشارت في الفقرة 10 منها على التعاون في مجال مكافحة الاحتيالات المرتبطة بتكنولوجيات الإعلام والاتصال الجديدة .

[4] مرسوم رئاسي رقم 288/15 المؤرخ في 22 غشت 2015، جريدة رسمية عدد 45 مؤرخة في 23 غشت 2015، ص 3.

إضافة إلى أن المشرع الجزائري اصطلح على الجريمة المعلوماتية بالجرائم الماسة بالأنظمة المعلوماتية وليس هو الوحيد في ذلك، فهو اختلاف في المصطلحات كما سيتم التفصيل أدناه، فالجرائم الماسة بالأنظمة المعلوماتية وإن كانت تختلف في أركانها وعقوباتها، إلا أن ما يجمعها أنها تحقق حماية جزائية لنظم المعالجة الآلية للمعطيات، أي أن القاسم المشترك بينها هو نظام المعالجة الآلية.

ويشمل نطاق هذا البحث دراسة الجرائم الماسة بالسرية المعلوماتية التي تقع بواسطة النظام المعلوماتي وعلى النظام المعلوماتي نفسه، مع العلم أننا خلال هذه الدراسة لم نعتمد التفرقة بين الجرائم الواقعة بواسطة النظام أو على النظام محاولين تخطي التقسيمات الفقهية للجريمة المعلوماتية.

كذلك شملت هذه الدراسة النظام المعلوماتي للحاسب الآلي دون الهاتف الذكي، نظرا للتشابه الكبير بين الجرائم الماسة بالأسرار المعلوماتية بواسطة الحاسب الآلي والهاتف الذكي، حيث أن إمكانيات الهاتف الذكي الذي يصلح لارتكاب الجرائم المعلوماتية يعتبر في حكم الحاسب الآلي، وأيضا على أساس أن الأنظمة المعلوماتية الغالبة حاليا على مستوى الحياة الخاصة والعامة على وجه العموم هي الأنظمة المعلوماتية للحاسب الآلي، وعلى هذا الأساس أصلا سميت جرائم المعلوماتية باسم الحاسب الآلي أو ارتبطت به كتسمية جرائم الحاسب الآلي والانترنت.

ففي وقت مضى كانت أسرار الشخص تحفظ بوسائل تقليدية، بينما اليوم تحفظ بوسائل متقدمة لها القدرة العالية على حفظها وعدم المساس بها، باعتبارها وسائل معلوماتية لا تزال في تطور دائم لخدمة الشخص، ومع كل ما تتميز به هته الوسائل من قدرات هائلة على الحفظ فهل ستبقى بها المعلومات في مأمن من أيدي مجرمي المعلوماتية، هؤلاء الذين يودون انتهاك الأسرار المعلوماتية ولكل منهم دوافعه.

إن هذا الموضوع له أهمية كبيرة جدا نظرا لحجم الانتهاكات والاختراقات الواقعة على الأنظمة المعلوماتية التي نشهدها يوميا في ظل التطورات التكنولوجية وتزايد المعرفة بالتقنية الحديثة وظهور ما يسمى بالمجرم المعلوماتي، كذلك يمكن للمعلومات أن تنتقل بواسطة الحاسوب والانترنت من أدنى بقاع الأرض إلى أقصاها في ثوان، حيث يمكن تبادلها بيسر كبير بين الحاسبات الآلية وتصبح هذه المعلومات مادة أولية للإضرار بأصحابها خاصة من حيث الإفشاء والابتزاز وغيرها من السلوكيات المجرمة.

ضف إلى ما تقدم، تراجع قدرة الشخص على التحكم في سرية معلوماته في ظل قدرات أجهزة الحاسوب على تخزين واسترجاع قدر كبير من المعلومات في وقت قصير عن مختلف أوجه الحياة، فالقدرة الهائلة للحاسوب في تخزين المعلومات في أقل فترة ممكنة وفي أضيق حيز ممكن وحفظها داخل ذاكرة الحاسب بصفة دائمة

يعني أنها معرضة للاعتداء بخلاف وجودها في صدر الإنسان مع العلم أنها في ذاكرة الحاسب لا يمكن الاعتماد على النسيان كستار للمحافظة على السرية بعدما تم الكشف عن السر.

كما أصبح الفرد في منزله يخاف على حرمة مسكنه وحياته الخاصة خوفا من التطور التكنولوجي الذي يأتي يوما بعد يوما بالجديد، وما يبرر ذلك على سبيل المثال استخدامات الحاسوب الشخصي الذي يتضمن الكاميرا نحن الآن مضطرين لوضع شريط عليها لنستخدمه بارتياح، لأن حتى الطفل الآن يمكنه أن يرى ويسمع ما يدور حولك من خلال حاسوبه وأنت تعمل على حاسوبك المرتبط بالشبكة صوت وصورة إذ هو بالأمر اليسير.

هذا إلى جانب صور عديدة لأشكال الاعتداء على المعلومات السرية الالكترونية لابد من تسليط الضوء عليها ودراسة كيفية حمايتها على الأقل من الناحية القانونية وعلى الأخص جزائيا.

ويوجد سبب آخر، وهو أهمية السرية التي لابد وأن أي شخص وله أسرار يود الحفاظ عليها رغم وجود الحاسوب والانترنت في حياته، فوجود الأسرار والرغبة في حمايتها من الأمور المؤكدة والحتمية والمنطقية التي تلازم الإنسان وجودا وعدما.

وفي ظل سطوة الحاسوب القوية والتي أصبحت أمرا واقعا وفي مجالات الحياة المختلفة، كان لها تأثيرها السلبي على الأسرار المعلوماتية، إذ هي البيانات المعالجة آليا التي لا يراد الاطلاع عليها والتي أصبح لها وصف المعلومة، هذه الأخيرة أصبحت اليوم محل الاعتداء والانتهاك بشتى الطرق، وما يسهل ذلك هو تخزينها في الحواسيب أو يتم تبادلها أو تنتهك بواسطة وسائل الاتصال الحديثة، حيث أصبحت هذه المعلومات السرية داخل الحواسيب الآلية في خطر دائم خاصة في وجود الانترنت فمن السهل انتهاكها أو الاطلاع عليها دون موافقة وعلم صاحبها.

إذن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة، أي ظهور ما يسمى بأزمة القانون الجنائي في مواجهة واقع المعلوماتية، فرض حلها البحث في الأوضاع القانونية القائمة ومدى ملاءمتها لمواجهة هذه المشاكل، ولما كان القاضي الجزائي مقيدا عند نظره في الدعوى الجنائية بمبدأ شرعية الجرائم، فإنه لن يستطيع أن يجرم أفعالا لم ينص عليها المشرع حتى ولو كانت أفعالا مستهجنة وعلى مستوى عال من الخطورة الإجرامية .

إذن بات من الضروري تحقيق حماية جزائية أوسع وأكبر للمعلومات الالكترونية من الحماية المقررة للمعلومات التي تحتويها الملفات الورقية من ضعف النوع الأول من المعلومات ولأهميته في آن واحد، فالمعلومات المعالجة آليا ضعيفة داخل النظام عنها داخل الملفات الورقية، هذه الأخيرة يمكن إخفاؤها بسهولة عن المعلومات داخل النظام، كما أن المعلومات المعالجة آليا تتميز بالضخامة والتنوع.

هذا ونظرا لاختلاف وسائل انتهاك السرية المعلوماتية وتعدد صورها، كان لابد لها من ضابط وهو النص القانوني الذي يجرم هاته الأفعال ويحمي المعلومة السرية أيا كانت وسيلة معالجتها آليا خاصة بواسطة الحاسوب الذي يعتبر من أكبر الوسائل التي ترتكب بها وعليها الجريمة المعلوماتية.

فضلا عن ذلك فجرائم الاعتداء على المعلومات السرية الالكترونية هي جرائم تستهدف معنويات غير محسوسة، وهي بذلك تتسم بالخطورة نظرا لأغراضها المتعددة ونظرا لحجم الخسائر الناتجة عنها، فهي جرائم ترتكب بواسطة الكمبيوتر والانترنت مما يجعل ارتكابها بالأمر السهل واكتشافها وإدانة مرتكبيها وملاحقتهم بالأمر الصعب باعتبارها جرائم لا تحدها حدود، لهذا فإنها تثير تحديات ومعيقات الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق وغيرها من المشكلات.

فرغم أنه كان لابد من التدخل السريع للمشرع بتصديه بنصوص قانونية لأوجه التجريم المستحدثة بما فيها الجرائم ضد الأسرار المعلوماتية وهو ما حدث فعلا لدى غالبية الدول وعلى جميع الأصعدة الدولية والوطنية، ولكن السؤال المطروح هل كان ذلك كافيا خاصة مع اختلاف مفاهيم الجريمة المستحدثة بين الدول من جهة، ومن جهة أخرى اتصافها بالخاصية الخطيرة والمستعصية نوعا ما وهي أنها قد تكون عابرة للحدود في أغلب الأحيان، حيث لا يقتصر الأمر في الجريمة المعلوماتية على مجرد أن تقع الجريمة على الحاسب الآلي ذاته أو تقع بواسطته إذ يعد هذا الحاسب أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية داخل الدولة، بل أصبحت تخرج عن النطاق الوطني الداخلي وتأخذ بعدا عالميا، وذلك بسبب تطور شبكات الاتصالات الالكترونية التي أحاطت بالعالم وجعلت منه قرية صغيرة لا يعترف فيها بحدود جغرافية وسياسية، ومنه كيف سيتم القضاء عليها ومتابعة مرتكبيها في هذه الحالة؟.

هي إشكالية رئيسية مناطها كيف تتم حماية البيانات المعالجة آليا المختزنة أو المتنقلة عبر النظام المعلوماتي جزائيا، مع التركيز في هذه الدراسة على جهاز الحاسب الآلي لارتباطه بالشبكة العنكبوتية على أساس أنهما أهم عناصر النظام المعلوماتي، بل باعتباره الوسيلة الأكثر استخداما واستهدافا من قبل مجرمي المعلوماتية[1]، وفي ذات الوقت نتساءل بشأن الخصوصية المعلوماتية "وداعا للخصوصية في عصر الرقمية"، ونحن نتساءل من جهتنا أيضا حول قول "وداعا للسرية المعلوماتية في عصر الرقمية "؟.

[1] بالرجوع إلى تقسيمات الجريمة المعلوماتية فإننا نجد أن أهم تقسيمات الجريمة المعلوماتية كانت على أساس أنه هل الحاسب الآلي وارتباطه بالشبكة المعلوماتية هو هدف لهده الأخيرة أم هو وسيلة ارتكابها.

وعليه تهدف هذه الدراسة إلى التعرف على السلوكيات المجرمة الماسة بالأسرار المعلوماتية وكيفية إثباتها خاصة إذا كانت عابرة للحدود، وما هي التحديات التي فرضتها هذه الأخيرة على جهات التحقيق والحكم التي تعتبر خط الدفاع الأول في مواجهة ظاهرة الجريمة، والتي تعمل على تنمية قدراتها وتطوير إمكانياتها بصورة تواكب تطور أساليب الجريمة وتنوعها.

وللإجابة على التساؤلات السالفة، سوف نتبع في هذه الدراسة منهجين يتم الاعتماد عليهما هما المنهج التحليلي والوصفي، حيث أنه تم إعطاء بعض الشروحات لبعض المفاهيم كما هو الحال بشأن مفهوم السرية والمعلوماتية والجريمة المعلوماتية هذا من جهة، ومن جهة أخرى سيتم اعتماد منهج تحليلي من أجل محاولة التدقيق في الجرائم الماسة بالسرية دون غيرها من الجرائم المعلوماتية.

إضافة إلى أننا في بعض المحطات من هذه الدراسة سيتم الاعتماد على المنهج المقارن، وسبيل بيان الأهداف المنشودة من هذا البحث تمت معالجة إشكالية الدراسة وفقا لخطة ثنائية تم تقسيمها إلى بابين:

الباب الأول: الأحكام العامة للأسرار المعلوماتية.

الباب الثاني:الجرائم الواقعة على الأسرار المعلوماتية في القانون الجنائي وآليات مكافحتها.

الباب الأول
الأحـــــكام العامة للأسرار المعلوماتية

تعتبر المعلومة ضرورة اقتصادية واجتماعية لاغنى عنها لدفع حركة المجتمع، مما أدى إلى حدوث اشتباك بين مجتمع الأكثر حداثة ومجتمع السرية الأكثر محافظة، وهو ما يتطلب إلقاء الضوء على نوعية المعلوماتية باعتبارها تكنولوجيا حديثة ومقتضياتها، التي لا تتوافق مع السرية حيث تعتبر المعلوماتية أداة في خدمة المعلومة وتنطوي على مخاطر بالنسبة للسرية[1].

إذا كان تقديم المعلومة أمر ضروري تمليه قواعد حسن السلوك الواجب توافرها في المعاملات، فإنه مع دخولنا عصر تقنية المعلوماتية أصبح الحاسب الآلي هو أداة تقديم المعلومة، التي تعتبر أمرا ضروريا وحيويا لتلبية الحاجيات الاجتماعية والاقتصادية وغيرها[2]. ورغم أن الحاجة إلى المعلومة ضرورية، ولكن لا يمكن أن تتحول إلى حق في الحصول عليها لأنها قد تقف حجر عثرة أمام سرية المعلومات فتؤدي إلى الإضرار بأصحابها[3].

إن الحفاظ على السرية يعد أمرا ضروريا، بل وتحتاج بعض المعلومات في كثير من الأحيان إلى أقصى درجات الكتمان[4]، وهذا بالطبع عندما كانت الأسرار تختزن في الصدور بينما ونحن في عصر المعلوماتية تم طرح أحد الأسئلة وبإلحاح، وهو كيف نجمع بين المعلوماتية والسرية؟، فهل يجمعهما التعارض أكثر من الالتقاء، أم التصالح بينهما أمر جعلته معطيات الحياة أمرا حتميا؟ ذلك لأن النظـــم المعلوماتية غزت نشاطات الحياة وجوانبها.

وللإجابـــة علـــى الأسئلـــة المطروحـــة، كان مـــن اللازم دراســـة أوجـــه الحمايـــة[5] الجزائيـــة[6] للمعلومات

---

[1] نادية محمد معوض، أثر المعلوماتية على الحق في سرية الأعمال، ص 52، منشور على الموقع الالكتروني www.flaw.bu.edu.eg/flaw/images/part1.pdf تاريخ الدخول على الموقع يوم 2017/04/24.

[2] SAINT Alary Roger, Le secret des affaires en Droit Français, Travaux de L'association Henri capitant, le secret et le DROIT journées libanniase 1974 , Dalloz, P263 .

[3] نادية محمد معوض، مرجع سابق، ص 15.

[4] هناك من قال " كنت أرتعد من أخون نفسي بزلة لسان، حتى أنني أردت أن أجهل- أنا أيضا- سري"، نادية محمد عوض، مرجع سابق، ص 15.

[5] تعرف مصطلح الحماية، لغة: مصدر حمى، حماه، حماية، دفع عنه، وهذا شيئ (حمى) أي: محظور لا يقرب، و(أحميت المكان) جعلته حمى" . أنظر في ذلك ابن منظور، محمد بن مكرم، لسان العرب، تحقيق، عبد الله علي الكبير وآخرون، دار المعارف القاهرة، مادة (حمى)، ص 1014. وتعرف الحماية اصطلاحا بأنها احتياط يرتكز على وقاية الشخص أو ماله ضد المخاطر، وضمان أمنه وسلامته، وذلك بواسطة وسائل قانونية أو مادية وهذا الاحتياط يتوافق مع من يحميه أو ما يحميه، كما عبر هذا المصطلح عن عمل الحماية ونظامها على حد سواء. أنظر في ذلك ماجد بن عبد الرحمان الكعيد، الحماية الجنائية للمعلومات الرقمية البنكية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض 2011، ص 18، أشار إليه محمود العادلي، الحماية الجنائية لالتزام المحامي بالمحافظة على أسرار موكله،الطبعة الثانية، دار النهضة العربية، القاهرة، 2002، ص 7.

[6] يعرف مصطلح الجنائية، لغة: جنى، الذنب عليه يجني جنايه، جره إليه، والثمرة اجتناها و تجنى عليه، ادعى ذنبا لم يفعله، ويقال: جنى واجتنى. (الفيروز أبادي، محمد بن يعقوب، القاموس المحيط، الطبعة السادسة، مؤسسة الرسالة، بيروت،

الالكترونية السرية ولأجل ذلك كان لابد من تخصيص باب أول يتعلق بالمفاهيم الأساسية لهذه الدراسة، يتضمن فصول ثلاثة أولها خصصناه لماهية السرية المعلوماتية، والثاني للتعرف على ماهية النظام المعلوماتي على أساس أن الحاسب الآلي كجزء منه وسيلة ترتكب بها وعليها الجريمة المعلوماتية (ما تخزنه وتنقله من معلومات)، والانترنت كجزء لا يتجزأ من نظام المعالجة الآلية للبيانات ووسيلة تسهل انتهاك سرية تلك البيانات وتلك البيانات في حد ذاتها كمحل لتلك الجرائم(المعطيات). إضافة إلى الفصل الثالث المتضمن ماهية الجريمة المعلوماتية بصفة عامة مع العلم أن الجرائم الواقعة على الأسرار المعلوماتية[1] هي في الأصل جرائم معلوماتية.

الفصل الأول
ماهية السرية المعلوماتية

مما لا شك فيه أن التقدم التكنولوجي الهائل في كافة مناحي الحياة ولاسيما في مجال تبادل المعلومات والمعلوماتية والاتصالات، واعتمادنا المطرد على الحاسوب والنظم المعلوماتية بصفة عامة في مختلف جوانب حياتنا أدى إلى تعرض سرية المعلومات لأخطار كثيرة، دفع العديد من الدول إلى سن قوانين داخلية ودولية لملاحقة كل منتهك لتلك الأسرار، ذلك أن التطور التكنولوجي الهائل هو ليس في تطور متكافئ مع القيم الأخلاقية.

إنه من الواضح جدا، أن التطور التكنولوجي ولاسيما في مجال تبادل المعلومات والاتصالات قد تخطى بمراحل القيم الأخلاقية، لذلك إنه ليس من الغريب في وقتنا هذا وجود أشخاص على قدر ضئيل من التعليم ويتحكمون في آلة الكترونية قادرة على الإفساد والإضرار والمساس بأسرار وكرامة ومصالح الآخرين. إذن كل هذا التطور جعل بالمعلومات السرية في خطر داهم، حيث أن كل ما يتعلق بحياتنا اليوم معالج في ذاكرة الحواسيب والآلات الالكترونية الأخرى الأمر الذي على أساسه طرأ عنها مفهوم جديد للسرية هي السرية المعلوماتية.

ورغم أن أشكال الاعتداء على السرية المعلوماتية تعد من الجرائم المعلوماتية، والتي تعتبر من الظواهر الإجرامية الحديثة الناشئة في بيئة الحاسب الآلي.تلك الظاهرة الإجرامية التي بدل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدا كبيرا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعتها.

1999، ص 1271). ويعرف مصطلح الجنائية اصطلاحا، إضفاء الحماية التشريعية على المصالح التي يتوخاها المشرع، ويعبر عن ذلك بالجزاء الجنائي أو العقوبة. ماجد بن عبد الرحمان الكعيد، مرجع سابق، 20، أشار إليه مجدي محب، الحماية الجنائية لأسرار الدولة، دراسة تحليلية لجرائم الخيانة، الهيئة المصرية العامة للكتاب، القاهرة، 1997، ص 111.

[1] الأسرار المعلوماتية وسرية المعلومات ذات المفهوم حيث أن المعلومات وكما سريد التفصيل هي البيانات المعالجة آليا بواسطة وسائل معلوماتية وهي على الأغلب الحاسب الآلي وما في حكمه.

إن عدم الاتفاق على تعريف موحد أدى إلى إثارة العديد من المشكلات القانونية خاصة ما يتعلق بإيجاد حلول لمواجهتها.

فالبرغم مما تتمتع به السرية من قدر كبير من الأهمية لارتباطها المباشر بمصالح الأفراد و الجماعة، إلا أنها في عصر المعلوماتية أصبحت أكثر عرضة لكثير من الأنشطة غير المشروعة، المرتبطة بالحاسبات الآلية وما في حكمها. حيث اعتبرت هذه الأخيرة أرض خصبة للاعتداء على كل أشكال السرية المعلوماتية، وذلك بسبب سوء استخدام التقنية المعلوماتية و الانحراف عن الأغراض المتوخاة منها.

فما هو المقصود بالسرية المعلوماتية ؟ وللإجابة على هذا التساؤل كان لابد من التطرق لمفهوم المعلوماتية (المبحث الأول)ثم مفهوم السرية ثم مفهوم السرية المعلوماتية(المبحث الثاني) .

المبحث الأول
ماهيـــــــــة المعلوماتيـــــــــة

تعرض هذا المفهوم-أي المعلوماتية- للكثير من محاولات التعريف، لتحديد ماهيته وأدواته وطبيعته على مدى السنين التي واكبت التطور التكنولوجي، سواء على صعيد معالجة المعلومات أو على صعيد تطور وسائل الاتصال. فقد شاع مصطلح المعلوماتية منذ الستينات وكان أول من استخدمها العالم الروسي "ميخائيلوف" والذي كان مديرا للمعهد

الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفياتي سابقا[1]، ثم شاع استخدامه بعد ذلك على مستوى جغرافي واسع بمفاهيم متباينة حتى أحصى له البعض أكثر من ثلاثين تعريفا مختلفا في الكتابات المخصصة في علم المعلومات[2].

فعلم المعلومات أو المعلوماتية، يقصد بها ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات أو البيانات وتجميعها وتنظيمها واختزانها واسترجاعها، ثم بتفسيرها وإعادة بثها أو تحويلها واستخدامها وبالتالي فهي عملية ديناميكية غاية في التعقيد تتم بدقة متناهية وبسرعة فائقة[3].

و قد صاغت الأكاديمية الفرنسية[4] تعريفا للمعلوماتية على أنها علم التعامل العقلاني، وعلى الأخص بواسطة الآلات أوتوماتيكية، مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعمادا للاتصالات في ميادين التقنية والاقتصاد والاجتماع ولليونسكو أيضا تعريف موسع عن سابقة أو أكثر حادثة لتقنية المعلومات أو ما اصطلح على تسميته بالمعلوماتية، يدرج في مضمونها الفروع العلمية والتقنية الهندسية وأساليب الإدارة الفنية المستخدمة في تداول ومعالجة المعلومات وفي تطبيقاتها المتعلقة كذلك بالحسابات وتفاعلها مع الإنسان والآلات وما يرتبط بذلك من أمور اجتماعية واقتصادية وثقافية[5] .

فكلمة معلوماتية هي اختصار لكلمتي معلومة وكلمة آلي أو آلية، وتعني المعالجة الآلية للمعلومة[6]، ومنه فإن المعلوماتية تعني المعلومات التي تمت معالجتها بوسائل آلية[7].

كما عرفته أي مصطلح معلوماتية[8]، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة الثانية منها

---

[1] مفتاح محمد دياب، معجم مصطلحات نظم وتكنولوجيا المعلومات والاتصالات:انجليزي-عربي ، الدار الدولية للنشر والتوزيع، بدون تاريخ، ص 79.

[2] أنظر سامي علي حامد عياد، الجريمة المعلوماتية واجرام الانترنت، دار الفكر الجامعي الاسكندرية، 2007، ص 35.

[3] أنظر نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي، لبنان،2005، ص 28، أنظر سامي علي حامد، المرجع نفسه، ص 38.

[4]- الأكاديمية الفرنسية هومجمع لغوي هدفه ترجمة المصنفات الأجنبية إلى اللغة الفرنسية ووضع المصطلحات العلمية وتنقية اللغة من كل وحشي ومهجور، صدربقيانها أمر ملكي من ملك فرنسا لويس الرابع عشر سنة 1405-1635 ومنحها جناحا خاصا في قصر اللوقر ليكون قصرا دائما لها وقد كان أعضاؤها أربعون ولا تقتصر عضويتها على الأدباء واللغويين، بل انضم اليها العسكريون والعملاء من رجال الدين، و حيث صاغت هذا التعريف في جلستها بتاريخ 6 أبريل 1967 ، عن الموقع الالكتروني .http://www.islamonline.net/arabic/history/1422/01/article05.shtml

[5] أنظر سامي علي حامد عياد، مرجع سابق، ص 36.

[6] أنظر محمد أمين الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية،الطبعة الرابعة، دار الثقافة للنشر والتوزيع، عمان الأردن، 2011، ص 7عن أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي)،الطبعة الأولى، دار النهضة العربية 2000، ص 270.

[7] أنظر مدحت محمد عبد العزيز ابراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2015، ص 28.

[8] وبمرور الزمن وارتباط المعلوماتية بكثير من العلماء واهتمامهم بها، توسع المفهوم عما كان عليه في الأصل، وظهرت تعاريف جديدة تعبر عن مجال المعلوماتية بمعناها الواسع بطريقة أحسن مما كان عليه الوضع في السابق، وبدون تغاضي عن جوهر المفهوم الأصلي بربط المعلومات بتكنولوجياتها ومن هذه المفاهيم ما يلي:

أنه"تقنية المعلومات: أية وسيلة مادية أو معنوية أو مجموعة وسائل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقا للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكيا أو لاسلكيا في نظام أو شبكة".

"المعلوماتية هي المجال الذي يدرس أساسا ظاهرة المعلومات، ونظم المعلومات، والمعالجة ونقل المعلومات، ولكنه لا يحتم بضرورة استخدام نظم الحاسبات الآلية وشبكات الاتصال عن بعد كأدوات مساعدة" ، هدا المفهوم يركز على دراسات ظاهرة المعلومات وما ينبع منها من نظم وأساليب تتصل بتجميعها ومعالجتها ونقلها واستخدامها وبذلك يبتعد إلى حد كبير عن الوجهة التقنية التي كان يمثلها المفهوم الفرنسي السابق.

وقد تبنى مكتب ما بين الحكومات للمعلوماتية IBI وهو منظمة حكومية دولية مقرها في ايطاليا مفهوما يركز على الفحوى الاجتماعية والاقتصادية والسياسية لتأثير المعلومات على التنمية في المجالات المختلفة ، لهذا فالمصطلح وفقا لهم يراعي شموليه إلى حد كبير وهو"المعلوماتية هي التطبيق المنطقي والمنظم للمعلومات على المشاكل الاقتصادية والاجتماعية والسياسية"، أنظر في ذلك أنظر محمد محمد الهادي، التطورات الحديثة لنظم المعلومات المبنية على الكمبيوتر، الدور الثقافي والتنموي للكتب والمكتبات في عالم متغير، الدار الشرقية القاهرة، 1993، ص 23-24.

وعرف أيضا لفظ المعلوماتية من قبل الأكاديمية الفرنسية في سنة 1996 بما يلي:" المعلوماتية هي علم المعالجة المنظمة والفعالة للمعلومات على وجه الخصوص بواسطة استخدام المعدات الآلية وبذلك فإنه ينظر إليه كوسيلة للمعرفة البشرية ومسار الاتصالات التي تنقلت بالمضامين العلمية والفنية والاقتصادية" ، يلاحظ أن هدا المفهوم اهتم بالجوانب التكنولوجية المتصلة بالمعالجة الآلية للبيانات التي تستخدم فيها الحاسبات الآلية، هدا بجانب الاتصالات المستخدمة في نقل المعلومات من مكان لآخر.

ويرى البعض بأنها:" علم المعالجة المنطقية الآلية للمعلومات"، وورد أيضا أن" المعلوماتية هي المعالجة الأوتوماتيكية للمعلومات بواسطة مجموعة من التقنيات الموضوعة لاستعمال الأجهزة الالكترونية" ، أنظر في ذلك أنظر عبد المحسن الحسيني، المعجم الكامل عن المعلوماتية،الطبعة الأولى، دار القلم بيروت لبنان، 1987، ص 128.

وعند الكثيرين تعني المعلوماتية أوتقنية المعلومات"التزاوج والالتحام بين تقنية الحاسبات والاتصالات والاستعمال المتزايد للالكترونيات في العمليات الصناعية والتجارية ابتداء بالإنسان الآلي المبرمج بالحاسب حتى بطاقة الائتمان التي يحتفظ بها المستهلك في جيبه"، أنظر في ذلك سامي علي حامد عياد، المرجع نفسه، ص 36، أشار إليه راحات نابي خان، الثورة الصناعية الثالثة، نظرة اقتصادية شاملة، مجلة العلم والمجتمع، اليونسكو، الطبعة العربية، مركز مطبوعات اليونسكو، القاهرة، 6-8 سبتمبر- نوفمبر 1987، ص 11، أنظر محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر الإسكندرية، 2001،ص 63.

أي أن البعض يطلق على تقنية المعلومات اصطلاح الحوسبة والاتصال وذلك لأن التقنية تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما وهما الحوسبة والاتصال، أما الحوسبة تقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة المعطيات، أما الاتصال فهو قائم على وسائل التقنية لنقل المعلومات بجميع دلالاتها الدراجة والمعرفة. والتي تعرفها منظمة اليونسكو بأنها تلك الفروع العلمية والتقنية والهندسية المستخدمة في تداول ومعالجة المعلومات والبيانات وفي تطبيقها والمرتبطة بالحاسبات في إطار استخدام الإنسان لها لتحقيق حاجاته الاجتماعية والثقافية والاقتصادية، أنظر في ذلك أنظر أمير فرج يوسف، الجرائم المعلوماتية عبر شبكة الأنترنت، دار المطبوعات الجامعية الاسكندرية، 2008 ، غير مرقم الصفحات..

ويرى الدكتور محمد مؤنس محمد الدين" أن علم المعلومات أو المعلوماتية يقصد بها ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات أو البيانات وتجميعها وتنظيمها واختزانها، واسترجاعها ثم بتفسيرها وإعادة بثها أو تحويلها واستخدامها، وبالتالي هي عملية ديناميكية غاية في التعقيد تتم بدقة متناهية وبسرعة فائقة بهدف إعادة تدويرها أو توظيفها في مجال محدد سواء كان هذا المجال إداري أو صناعي أو تجاري أو سياسي أو أمني وذلك باستخدام رموز خاصة عند نقل أو بث البيانات والمعلومات"،أنظر في ذلك محمد مؤنس محي الدين، اجرام الأنترنت، دبلوم الدراسات العليا، ص1.

ومن العرض السابق لتعريف مصطلح المعلوماتية واختلاف المفاهيم التي تعرض لها في محاولات للوصول إلى مفهوم موحد، نجد أن المعلومات ومسألة تنظيمها ومعالجتها هي المحور الذي يدور حوله مصطلح المعلوماتية.

واسترشادا بما سبق من التعاريف للمعلوماتية، فإن أفضلها وهو أنه المعلوماتية هي علم المعالجة الآلية للمعلومات ومنه وببساطة فإن المعلوماتية هي العلاقة بين المعلومات وبين التقنية الحديثة المستخدمة من أجل معالجة هذه المعلومات، إذ يتضمن المعلومات التي يتم تجميعها بمعرفة الإنسان والتي تتمتع بالتحديد والابتكار والسرية والاستئثار، ويتم تجميعها عن طريق شبكة المعلومات ويتم معالجتها آليا وفقا للأنظمة المعلوماتية.

واستنادا لما سبق و للوقوف على تحديد المفهوم الدقيق للمعلوماتية يتطلب هذا الأمر الوقوف على المفهوم الدقيق للمعلومات، التي تدخل في نطاق الحماية الجزائية من خلال تعريفها و تمييزها عما يرتبط بها من مصطلحات (مطلب أول) و عرض خصائصها(مطلب ثاني).

المطلب الأول
تعريف المعلومات

المعلومات هي أغلى ما يمتلكه الإنسان في حياته على مر العصور، لذا سعى إلى جمعها وتسجيلها على وسائط حفظ مختلفة بدءا من جدران المقابر إلى أن تم اختراع الورق في الصين.

وعرفت أولى محاولات تسجيل المعلومات في التاريخ على أيدي قدماء المصريين الذين سجلوا حضارتهم على جدران المقابر والمعابد وأوراق البردي، وهذا هو السبب في الإبقاء على حضارتهم محفورة في ذاكرة التاريخ. حيث أن حضارات عظيمة اندثرت لعدم تسجيلها، لذلك تعتبر المعلومة رمزا من رموز الحضارة الإنسانية على مدى التاريخ، ومعنى أن يفقد الإنسان معلوماته فإنه يفقد ذاكرته ومن ثم تضييع حضارته[1]. ولقد اكتسبت المعلومات بظهور تكنولوجيا الحواسيب بعدا جديدا أضفى عليها أهمية تفوق ما كانت عليه من قبل،وقد تختلط المعلومات بمفاهيم عدة، مما ينبغي التطرق لتعريفها(الفرع الأول) والتمييز بينها وبين المصطلحات التي ترتبط بها(الفرع الثاني) وتحديد طبيعتها القانونية(الفرع الثالث).

[1] - Rosalind Resnick, exploring the world of services ,sybex inc 1993, p. 5.
أشار إليه ، أنظر أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية، الطبعة الثانية، 2006، ص 71 .

الفرع الأول
تعريف المعلومات[1] كمحل للاعتداء

تعتبر المعلومة شيء غير مادي ولكنها تصلح أن تكون محلا للحقوق المالية وعلى الأخص حق الملكية، وقد تكون المعلومة منتجا أو سلعة مستقلة سابقة على الخدمة التي تكون محلا لها. وعلى ذلك تتميز وتستقل المعلومة عن الشكل المادي الذي تتمثل فيه، كتابة أو صوتا أو صورة، وكذلك عن الخدمة التي تكون محلا لها. فهي بالضرورة سابقة في وجودها على لحظة تقديمها في صورة سلعة أو خدمة. فالمعلومة شيء غير مادي متميز ومستقل لا يختلط بشكل تقديم المعلومة ولا بالخدمة التي تكون محلا لها، وترتب على ذلك أن بعض الفقه سعى نحو إقامة مدخل إلى نظرية قانونية للمعلومة بمقتضاه يتم التعامل مع المعلومة على أنها حقيقة في حد ذاتها لها قيمتها الثقافية والسياسية والاقتصادية الكبيرة. تلك القيمة جديرة بأن ترفعها إلى مرتبة الأموال فيتحدد سعرها بوصفها سلعة تباع وتشترى وفقا لظروف العرض والطلب. وعلى هذا الأساس تقوم وكالات الأنباء ببيع ما تحصل عليه من معلومات أو إخبار، كل ذلك أدى إلى ظهور قيما اقتصادية جديدة لم تكون مألوفة من قبل وأموالا جديدة تعرف بالأموال المعلوماتية[2].

فتعريف المعلومة على الرغم من أنه قد يبدو لا يثير أي صعوبة، حيث أن المعلومات تحيط بنا من كل جانب كما أنها تتعلق بكافة مجالات الحياة، إلا أنه يمكن القول أن المعلومات قد اكتسبت بظهور تكنولوجيا الحاسبات الآلية بعدا جديدا أضفى عليها أهمية تفوق ما كانت عليه قبل ذلك واكسبها شكلا جديدا، بل وتسمية جديدة أصبح يشار إليها بالمعلوماتية إشارة إلى ارتباطها بهذه التكنولوجيا الحديثة[3] .

أولا: تعريف المعلومة لغة

معناها في اللغة مشتقة من كلمة "علم" ، ودلالتها تدور حول المعرفة التي يمكن نقلها واكتسابها وأعلم فلانا الخبر أي أخبره به وأعلم فلانا أمرا حاصلا جعله يعلم والعلم نقيض الجهل، وعلمت الشيء أعلمه علما أي عرفه[4].

وعرفت المعلومة في قاموس المعلوماتية بأنها" الركيزة الأساسية لنقل المعرفة"، أو"بيانات تمت معالجتها من أجل تحقيق غاية معينة أو لاستعمال محدد".كما عرفت في

---

[1] وللإشارة أنه الكثير من يستخدم كلمة البيانات والمعلومات كمترادفتين لكن لكل منهما مدلول مختلف.

[2] - أنظر عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دراسة مقارنة ، دار النهضة العربية، القاهرة ،2000 ، ص 29-30.

[3] - نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية ،الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005، ص 97.

[4] - رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية بيروت، لبنان، 2012، ص 64.

قاموس روبير "بأنها الخبر الذي يتعرض لمعرفة الشخص والعامة، وابتكار جميع أوكل المعلومات، وعمل أخبار للعامة"[1].

ثانيا:تعريف المعلومة اصطلاحا

في المعنى الاصطلاحي، فإنه يوجد للمعلومات المئات من التعاريف التي تعرض لها باحثون من تخصصات وثقافات مختلفة حتى يكاد مستحيلا فهم وإدراك المعنى المراد بمصطلح " المعلومات". ويرى البعض أن المعلومات كالجاذبية والكهرباء لا نستطيع وصفها بدقة، ولكننا نعرف كيف تعمل وندرك أثرها[2].

ويمكن تعريف المعلومة بصفة عامة بأنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال، أو التفسير والتأويل أو للمعالجة بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة[3].

ويعرفها الأستاذ "كاتالا" بأنها رسالة معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير فهي تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير، ثم هي قابلة للتوصيل بفضل علامة أو إشارة من شأنها أن توصل المعلومة للغير فالتعبير وتوصيله للغير يحقق وظيفة المعلومة وهي انتقال أو نقل المعرفة[4]، فكان تعريفه لها تعريفا واسعا للغاية[5].

والواقع أنه أيضا تعريف واسع للمعلومة، وتعرف أيضا أنها مجموعة من البيانات التي قد تمت معالجتها وتحليلها وتلخيصها وتجريبها لتحقيق الأهداف المرجوة منها، واستخدامها في المجالات المختلفة، أي أنها البيانات المجهزة في شكل منظم ومفيد بتسلسل منطقي[6].

وعرفها المشرع الفرنسي كأول مرة في القانون الصادر في 29 يوليو سنة 1982 بشأن الاتصالات السمعية والبصرية إلى أول تعريف عام للمعلومة، والذي ينذر إليها بوصفها رنين صور الوثائق والبيانات أورسائل من أي نوع وعلى هذا الأساس تعنى المعلومة رمزا أو مجموعة رموز تخطوا على إمكانية الإفضاء إلى المعني[7].

وعرفها المشرع الأردني في قانون المعاملات الالكترونية رقم 85 لسنة 2001 أنها" البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج

---

[1] رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2013، ص 10-11.

[2] - نائلة محمد فريد قورة، مرجع سابق، ص97، رشيدة بوكر، مرجع سابق، ص 64.

[3] - نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة عمان، الأردن، 2008 ، ص 101 .

[4] - CATALA Pierre, Ebauche d'une Theorie juridique de l'information,D.1984, chron p. 97.

[5] - أيمن إبراهيم العشماوي،المسؤولية المدنية عن المعلومات،دار النهضة العربية، القاهرة، بدون طبعة ، 2004 ، ص 31.

[6] Kenneth Lauden, Jane Lauden," Management Information System- managing The digital Firm" , seventh edition, prentice-bhall,inc,new jersey,USA, 2004,p 8.

[7] - عمرو أحمد حسبو، مرجع سابق، ص 31.

الحاسوب وما شابه ذلك"[1]، و عرفها في قانون المعاملات الالكترونية لسنة 2015 في المادة الثانية منه أنها" البيانات أو النصوص أو الصور أو الرسومات أو الأشكال أو الأصوات أو الرموز أو قواعد البيانات و ما شابه ذلك"[2]، و يكون بذلك قد وسع من مفهوم المعلومات.كما عرفها في قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 أنها:" المعلومات التي تمت معالجتها وأصبح لها دلالة".[3]

ويعرف البعض الآخر المعلومات أنها" كل نتيجة مبدئية أو نهائية مرتبة على تشغيل البيانات تعليلها أو استقراء دلالاتها أو استنتاج ما يمكن استنتاجه منها وحدها أو متداخلة مع غيرها أو تفسيرها نحو يثري معرفة متخذي القرار ومساعدتهم على الحكم السديد على ظواهر ومشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية"[4].

ويقصد بها أيضا "البيانات التي يجري عليها معالجة معينة وترتيبها وتنظيمها وتحليلها بغرض الاستفادة منها والحصول على نتائج معينة"[5]، من خلال استخدامها[6].

كما تم تعريفها وفقا للمعجم الموسوعي لمصطلحات المكتبات والمعلومات، أنها " البيانات التي تمت معالجتها لتحقيق هذف معين أو لاستعمال محدد لأغراض اتخاذ القرارت أي البيانات التي أصبح لها قيمـــــــــة بعـــــد تحليلها أو تفسيرها، أو تجميعها في شكل ذي معنى[7].

وتعرف أيضا المعلومة أنها "بيان معقول أو رأي أو حقيقة أو مفهوم أو فكرة أو تجميعـــــــها مترابطا لبيانات أو الآراء أو الأفكار"[8]، وهو التعريف الذي نوافقه فقط يمكننا أن نضيف له عبارة معالجة آليا.

---

[1] قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001، جريدة رسمية 2001/4524 المؤرخة في 2001/12/31 رقم الصفحة 6010، عن الموقع الإلكتروني http://www.wipo.int/edocs/lexdocs/laws/ar/jo/jo058ar.pdf ، أطلع عليه بتاريخ 2016/12/20

[2] القانون رقم 15 لسنة 2015، الجريدة الرسمية مؤرخة في 2015/05/19، ص5292 ، عن الموقع الالكتروني http://www.ammanchamber.org.jo/node/news.aspx?id=2085&lang ، أطلع عليه بتاريخ 2016/12/20.

[3] القانون الأردني لجرائم أنظمة المعلومات رقم 30 لسنة 2010، الجريدة الرسمية عدد 5056 المؤرخة في 2010/09/16، ص 5334، عن الموقع الالكتروني http://www.lawjo.net/vb/showthread.php?11651، أطلع عليه بتاريخ 2016/12/20.

[4] - نهلا عبد القادر المومني، مرجع سابق، ص 101.

[5] المشرع الأردني اعتمد ذات التعريف في قانون جرائم أنظمة المعلومات رقم 30 لسنة 2010 في المادة الثانية منه.

[6] - أنظر انتصار نوري الغريب، أمن الكمبيوتر والقانون،دار الراتب الجامعية بيروت لبنان، 1994، ص 81.

[7] ماجد بن عبد الله الرحمان الكعيد، مرجع سابق، ص 22.

[8] أنظر الموسوس عتو، حماية الحق في الخصوصية في القانون الجزائري في ظل التطور العلمي والتكنولوجي -دراسة مقارنة – رسالة دكتوراه جامعة سيدي بلعباس، السنة الجامعية2014-2015 ، أشار إليه جمال عبد الرحمان علي، الخطأ في مجال المعلوماتية، مجلة البحوث القانونية والاقتصادية، 1999، العدد 13 ص 305.

ثالثا: التعريف الفقهي للمعلومات[1]

وبالنسبة للفقه، فعرف المعلومة وفقا لمضمونها واتخذ مواقف ثلاث وعرفها من خلال البيانات، فأما عن هذه الأخيرة تمثلت في ثلاث اتجاهات الاتجاه النفعي والعملي والارتيابي، وكل منها وصفت بتعاريف مختلفة عن بعضها.

1- الاتجاه النفعي:

يعرف أساتذة هذا الاتجاه المعلومة بأنها النشاط القادر على أن يحمل للجهود بعض الوقائع أو الآراء من خلال وسائل بصرية أو سمعية تتضمن رسائل فكرية لهم.

2 -الاتجاه العملي

يقول أصحاب هذا الاتجاه أن المعلومة ليست كل شيء معنوي ولكنها تكتسب هذه القيمة المعلوماتية بسبب شكلها المميز فهي الإبداع المميز بصفة عامة، ويقولون أنها كل شيء له قيمة اقتصادية من وجهة نظر الجمهور الذي يرغبها.

3 - الاتجاه الارتيابي

يقول أنصار هذا الاتجاه، أنه ما دفع البعض إلى التشكيك في إمكانية وضع تعريف للمعلومة هو غياب الإجماع على المفردات وعلى تكوين نظام حقوق الملكية الذهنية. وهو ما لا يسمح بإعطاء تعريف وماهية المعلومة بشكل دقيق وإنما يسمح فقط بتعداد نماذج المعلومات. وفي هذا الصدد يقرر البعض أنه من الملائم تجنب الزعم القائل بقصر المعلومات على مفهوم موحد عن طريق القانون.

والمعلومة بصفة عامة، تتميز بقابليتها للدمج فقد تضاف معلومة إلى أخرى لتكون معا معلومة جديدة تختلف في قيمتها وأهميتها عما كانت عليه قبل الدمج، فمثلا رقم حساب العميل في البنك معلومة على قدر من الأهمية إلا أنه إذا أضفنا إلى هذه المعلومة معلومة أخرى كاسم البنك واسم العميل وحجم الرصيد. فإن قيمة المعلومة وأهميتها في هذه الحالة تتضاعف وتتطلب قدرا أكبر من الحماية، ولهذا السبب تقوم البنوك بإرسال كل معلومة منفردة عن طريق عمليات اتصال مختلفة، فهي على سبيل المثال تقوم بإرسال مجموعة كبيرة من أرقام الحسابات عن طريق عملية اتصال وتقوم بإرسال قيمة الأرصدة عن طريق عملية اتصال أخرى، ويتم تجميع المعلومات المختلفة في مركز معالجتها وذلك بهدف الحفاظ على سرية المعلومات.

الفرع الثاني
الفرق بين المعلومات وما يرتبط بها من مصطلحات[1].

[1] -أنظر سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي الإسكندرية، 2007، ص19-20.

قد يرتبط مفهوم المعلومات بالعديد من المصطلحات و المفاهيم التي يرتبط بها وجودا و عدما ،كما هو الشأن بالنسبة للبيانات و البرامج، لهذا لابد من التطرق إلى التفرقة بين هته المفاهيم على النحو التالي:

أولا:الفرق بين المعلومات و البيانات[2] و طبيعة العلاقة بينهما.

يميز الكثير من الباحثين بين المعلومات و البيانات (المعطيات)، فهذه الأخيرة تعد مطلب أساسي للتعامل مع الحاسوب ومن أجلها يتم إعداد البرامج فلكي يتم التوصل إلى المعلومات باستخدام الحاسوب يتم أولا البحث عن البيانات لتخزينها في الحاسوب ومعالجتها لتحويلها إلى معلومات[3] .

وتعرف البيانات "أنها المعطيات الخام أو الأولية التي تتعلق بقطاع أو نشاط ما"، وتسمى العلاقة بين المعلومات والبيانات بالدورة الإستراتيجية للمعلومات، إذ يتم تجميع وتشغيل البيانات والحصول على المعلومات ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات التي يتم تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يعتمد عليها في إصدار قرارات جديدة[4] . فمصطلح البيانات يرتبط باطراد بالاستخدام المعلوماتي وعلى ذلك فإن كل البيانات هي معلومات وليس كل المعلومات هي بيانات[5].

كما عرفتها الوكالة الفرنسية للتقييس (Afnor) بأنها "كل حادث مفهوم أو تعليمة تقدم في شكل متفق عليه قابلة للبادل عن طريق البشر أو بواسطة الحاسوب أو ينتجها الحاسوب"[6].

والبيانات هي أيضا عبارة عن" التجسيد أو العرض الاتفاقي للمعلومات في شكل معين لتسهيل معالجتها والتعامل معها"[1].

---

[1] هناك مصطلح آخر يرتبط به مصطلح المعلومات كما هو الشأن بالنسبة للبيانات و البرامج هو مصطلح المعرفة، ويمكن تعريف المعرفة أنها:" معلومات تمت معالجتها وتنظيمها لاكتساب مستخدميها مزيدا من الخبرة، والقدرة على اتخاذ القرارات وحل المشاكل."، أنظر صليحة علي صداقة، مرجع سابق، ص 33.

[2] الكثير من الباحثين والمشرعين من يعبر عن مصطلح البيانات بالمعطيات و من بينهم المشرع الجزائري حيث عرفها في المادة الثانية من القانون 04/09 كما سيرد التفصيل في المعطيات باعتبارها من العناصر المعنوية للحاسب الآلي.

[3] - علي جبار الحسناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن، عمان، الطبعة العربية 2009، ص 26-27، أشار إليه عمر محمد أبو بكر يونس، الجرائم الناشئة عن استخدام الانترنت، ص 61.

[4] - نهلا عبد القادر المومني، مرجع لسابق، ص 102.

[5]- أيمن إبراهيم العشماوي، مرجع سابق، ص 21،22 ، أشار إليه محمد حسام محمود لطفي، عقود خدمات المعلومات، دراسة في القانونين المصري والفرنسي، بدون ناشر،القاهرة 1994، ص 64-65 وتجدر الإشارة في هذا المقام أن الأستاذ محمد حسام محمود لطفي يرى أن البيانات بمثابة المواد الخام للمعلومات- كما تم الإشارة أعلاه- وأن التفرقة بينهم غير واضحة - أي المعلومات والبيانات- ولا أثر لها من الناحية القانونية نظرا لأن العبرة في هذا الصدد بالقيمة الاقتصادية لهذه المعلومات والبيانات.

[6] مفتاح محمد ديب، معجم المصطلحات و تكنولوجيا المعلومات و الاتصالات، الدار الدولية للنشر، القاهرة، 1995، ص 42.

كما عرفتها اتفاقية بودابست للجريمة المعلوماتية من خلال مادتها الأولى في الفقرة – ب-أنها" المعطيات هي كل تمثيل للوقائع أو للمعلومات أو المفاهيم تحت أي شكل و تكون مهيأة للمعالجة بما في ذلك برنامج معد من ذات الطبيعة و يجعل الحاسب يؤدي المهمة"[2].

وعرفتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في الفصل الأول المادة الثانية (المصطلحات) أنها" البيانات كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها".

ولذلك فإن عمر الشخص أو تاريخ ميلاده أو دراسته أو حالته الاجتماعية هي بيانات، لكن حين تدون في الحاسب الآلي تصبح معلومات ولذلك يقال على أنظمة الحاسب الآلي أنها نظم المعلومات وليست نظم البيانات[3].

فالبيانات إذن هي مجموعة من الحقائق التي تعبر عن مواقف وأفعال معينة، سواء كان ذلك التعبير بالكلمات أوالرموز ولا تفيد هذه البيانات في شيء وهي على صورتها الأولية، لذلك فإن الأمر يستدعي تحليل هذه البيانات وإجراء العمليات الحسابية والمنطقية عليها، أو بمعنى آخر معالجة البيانات للاستدلال منها على مجموعة من المعلومات، إذن تتحول تلك البيانات إلى معلومات، و بهذا تكون المعلومات هي النتيجة النهائية المترتبة على تشغيل البيانات و تحليلها أو استقراء دلالتها و استنتاج ما يمكن استنتاجه منها[4] .

وعليه فالمعلومات هي ناتج معالجة البيانات تحليلا أو تركيبا، لاستخلاص ما تتضمنه البيانات أو تشير إليه من مؤشرات وعلاقات ومتعلقات وكليات وموازنات ومعدلات وغيرها.[5] فالبيانات هي مدخلات الحاسب الآلي التي تمثل الخادمات التي يتم تشغيلها[6] و المعلومات هي المخرجات بعد عملية المعالجة.

أما عن طبيعة العلاقة بين المعلومات والبيانات، فإنه كثيرا ما يترادف استخدام كلمة البيانات والمعلومات أي استخدام أحدهما مكان الأخرى رغم أنهما ليسا شيء واحد، ورغم أن الخلاف بينهما يكاد يكون خلافا معنويا إذ أن البيانات هي المادة الخام التي يمكن تشغيلها للحصول على شكل أكثر فائدة واستخداما وهو المعلومات أي أنها أي البيانات هي المادة الخام التي تشتق منها المعلومات، فالعلاقة بينهما وطيدة ذات طبيعة دورية حيث يتم تجميع

---

[1]- أيمن إبراهيم العشماوي، مرجع سابق، ص 21.

[2] " .....données imformatiques désigne toute representation de faits , d'informations ou de concepts sous une forme qui se préte à un traitement informatique, y compris un programme de nature à faire en sorte qu'un systéme informatique exécute une fonction ;....."

[3] - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار النهضة العربية الاسكندرية، الطبعة الأولى، 2009، ص 50.

[4] محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، 2012، ص 61.

[5] محمد مصطفى الشقيري، السرية المعلوماتية، ضوابطها وأحكامها الشرعية، الطبعة الأولى، دار البشائر الإسلامية للطباعة والنشر بيروت لبنان، 2008،ص 35.

[6] الموسوس عتو، مرجع سابق، ص 144.

وتشغيل البيانات للحصول على المعلومات، وتستخدم هذه المعلومات في اتخاذ القرار الذي يؤدي بدوره إلى تنفيذ مجموعة من الإجراءات، والتي تؤدي إلى مجموعة إضافية من البيانات، ثم مرة أخرى يتم تجميعها وتشغيلها للحصول على معلومات إضافية أخرى لاتخاذ قرار آخر يؤدي بدوره إلى مجموعة جديدة من الإجراءات.....وهكذا[1]. ويمكن توضيح العلاقة بينهما على الشكل التالي:

الملاحظة + الحدس + التفكير =بيانات

البيانات +التجهيز + التحليل =معلومات [2]

ثانيا: الفرق بين المعلومات و البرامج[3]

يعتبر البرنامج من العناصر الرئيسة للكيان المنطقي إلى جانب المعطيات لأي حاسوب و من دونه يصبح هذا الأخير مجرد مجموعة من معدات و آلات صماء[4]، و باعتبار أن العديد من يرى ضرورة للتمييز بين البرامج والمعلومات. فهناك جانب آخر يرى أنه لا أهمية للتمييز بينهما طالما أن المعلومات هي المعنى المستخلص من المعطيات أو البيانات بعد معالجتها آليا و البرنامج هو المستودع الذي يتم فيه معالجة هذه المعطيات[5]، فالعلاقة بينما هي الجزء بالكل. و نجد أن المشرع الجزائري سار على هذا النحو ذلك أنه في تعريفه للمعطيات أدرج في مفهومها برامج الحاسوب و لم يأبه للجدل الفقهي من حيث التمييز بينهما، حيث نصت المادة الثانية من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال في تعريفها للمعطيات أن هذه الأخيرة هي " أي عملية عرض للوقائع أو المعلومات بما في ذلك البرامج المناسبة التي من شأنها أن تجعل المنظومة المعلوماتية تؤدي وظيفتها".

المطلب الثاني

الشروط الواجب توافرها في المعلومات وطبيعتها القانونية

لتتمتع المعلومات بالحماية الجزائية اشترط الفقه توفر مجموعة من الشروط، هناك منها ما هو متفق عليه وهناك ما هو خلاف ذلك سأحاول التفصيل فيها (فرع أول)، ثم تحديد الطبيعة القانونية للمعلومات (فرع ثان) كما يلي:

---

[1] محمد مصطفى الشقيري، المرجع نفسه، ص 38 - -39.

[2] محمد مصطفى الشقيري، المرجع نفسه، ص 39.

[3] نال البرنامج حظه من التعريفات، التي تباينت بين المفهوم الموسع و الضيق وسيتم التفصيل فيه أدناه باعتباره الكيان المنطقي للحاسب الآلي.

[4] عفيفي كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون، دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، الطبعة الثانية، 2007، ص 25.

[5] محمد خليفة، مرجع سابق، ص 90.

الفرع الأول
الشروط الواجب توافرها في المعلومات لتتمتع بالحماية الجزائية

يرى أنصار حرية تداول المعلومات، أن خصائص المعلومات تتمثل أساسا في الطابع غير المادي لهذه الأخيرة من جهة، وقابليتها للتداول من جهة أخرى. غير أن هذا لا يتناسب والواقع الاقتصادي حيث يكتسب الشيء في الواقع قيمة اقتصادية إذا كان نادرا ومفيدا، وعلى هذا يمكن تقسيم المعلومات إلى معلومات عامة وهي التي يمكن للجميع الحصول عليها، وأخرى خاصة وهي وحدها التي تكون نادرة ومفيدة في الوقت نفسه[1]. ولهذه الأخيرة خاصيتين للتمتع بالحماية الجنائية أولهما التحديد والابتكار(أولا) وثانيهما السرية والاستئثار(ثانيا)، وهي الشروط التي يجب توافرها في المعلومة وعند البعض هناك شروط إضافية حيث يجب أن تكون المعلومة معالجة آليا. ويضيف جانب آخر من الفقه شرط آخر، هو أنه يشترط اتخاذ تدابير جدية للمحافظة على سرية المعلومة (ثالثا) وسنبين كل عنصر من هذه العناصر كالتالي:

أولا: التحديد والابتكار

"يمثل التحديد خصيصة أساسية تفرض نفسها قبل كل شيء، والمعلومة التي تفتقر لهذا الشرط لا يمكن أن تكون معلومة حقيقية، فالمعلومة بوصفها رسالة مخصصة للتبليغ للغير عن طريق علامات أو إشارات مختارة يجب أن تكون محددة، لأن التبليغ الحقيقي يفترض التحديد بالإضافة إلى أن المعلومة المحددة هي التي يمكن فقط حصرها في دائرة خاصة بها من الأشخاص. بيد أن هذا التحديد يبدو أمرا ملحا في مجال الاعتداء على القيم لأن هذا التعدي يفترض دائما شيئا محددا، وينبغي على هذا الشيء أن يكون بدوره محلا لحق محدد. أما فيما يتعلق بالابتكار، فإنه ينبغي أن تنصب هذه الصفة على الرسالة التي تحملها العولمة، فالمعلومة غير المبتكرة هي معلومة شائعة ومتاحة للجميع ويمكن للجميع الوصول إليها ولا يمكن نسبها إلى شخص محدد"[2].

والتحديد خاصية أساسية تفرض نفسها قبل كل شيء وبانعدامها تزول أي معلومة حقيقية، بحيث أن المعلومة قبل كل شيء تعبير وصياغة مخصصة من أجل ذلك وتبلغ أو يمكن تبليغها عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة إلى الغير[3]، وهكذا

---

[1] - أيمن إبراهيم العشماوي، مرجع سابق، ص 40.

[2] - نهلا عبد القادر مومني، مرجع سابق، ص 103, عمرو احمد حسبو، مرجع سابق، ص 32، محمد عبد الله أبوبكر سلامه، مرجع سابق، ص 76.

[3] - احمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الأسكندرية، الطبعة الأولى، 2006 ،ص 75

أشار الأستاذ كاتالا" إن المعلومة قبل كل شيء تعبير وصياغة مخصصة من أجل دلك وتبلغ أو يمكن تبليغها عن طريق علامات أو إشارات مختارة لكي تحمل الرسالة إلى الغير "[1].

أما فيما يتعلق بالابتكار فانه يجب أن تكون المعلومة مبتكرة، وتنبع ضرورة ابتكار الرسالة المحمولة بواسطة المعلومة من أنها مبتكرة وغير شائعة، فالمعلومة غير المبتكرة هي معلومة شائعة ومتاحة للجميع ويمكن الوصول إليها ولا يمكن نسبتها إلى شخص محدد[2].

ثانيا: السرية والاستئثار

السرية أهم الشروط المطلوبة في المعلومة لكي يتم حمايتها جنائيا، فالمعلومات المباحة أو المعروفة للجمهور أولطائفة تضم عددا كبيرا تخرج من نطاق الأسرار المعلوماتية[3]. فالسرية شرط أساسي للقول بحصول تعد على المعلومة، ذلك أن المعلومة إذا كانت مشاعة، فإنه يحق استخدامها من أي كان لأن حق صاحبها يزول بزوال سريتها. فمن غير المتصور أن نطبق هنا جريمة سرقة أو النصب أو خيانة الأمانة على المال غير محفوظ، وهو ما ذهب إليه معظم فقهاء القانون. أضف إلى ذلك أن عنصر السرية يخول لصاحبة كذلك حق الاستئثار بملكية تلك المعلومة والتصرف فيها وفق إرادته هو سواء ببيعها أو إيجارها والتنازل عنها[4]. وقد تستمد المعلومة سريتها من طبيعتها كاكتشاف شيء كان مجهولا أو بالنظر إلى إرادة الشخص نفسه أوكلاهما معا كما هو الحال في الرقم السري لبطاقات الائتمان[5]. فالمعلومة السرية هي التي لا يمكن الوصول إليها بسهولة واستخدامها يكون قليل وبالتالي يكون حصرها في دائرة السرية[6].

إذن كلما اتسمت المعلومات بالسرية كان المجال الذي تتحرك فيه الرسالة التي تحملها محددا بمجموعة من الأشخاص، ودون هذه السرية لا يمكن أن تكون محلا يعتدى عليه، فالسرية صفة لازمة لأن المعلومة غير السرية ونؤكد على ذلك تقبل التداول ولا تكون بعيدة عن حيازة أي شخص وبهذا تفتقر إلى السرية.

أما خاصية الاستئثار، فتعد أمرا ضروريا في المعلومة، لأنه في جميع الجرائم التي تنطوي على اعتداء قانوني على القيم يستأثر الفاعل بسلطة تخص الغير وعلى نحو مطلق، وتتوافر للمعلومة صفة الاستئثار إذا كان الوصول إليها غير مصرح به إلا لأشخاص

---

[1] CATALA Pierre, Les transformations de droit par l informatique, in Emergence du droit de l informatique , éd Parque, 1983, p. 246.

[2] - احمد خليفة الملط، مرجع سابق ، ص 75.

[3] رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنت، دار النهضة العربية ، القاهرة ، 2013، ص 290.

[4] - خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى للطباعة والنشر عين ميلة الجزائر، 2010، ص 16.

[5] - احمد خليفة الملط، المرجع نفسه، ص 75 - 76.

[6] رشدي محمد علي محمد عيد، مرجع سابق، ص 27.

محددين ويمكن أن ينبع الاستئثار من سلطة شخص أوجهة ما على المعلومة أوعلى التصرف فيها[1].

ويمكن أن يرد الاستئثار على الولوج في المعلومة والمخصص لمجموعة من الأشخاص ويمكن أن يرد أيضا لشخص بمفرده باعتباره صاحب سلطة التصرف بالمعلومة[2].

وبالتالي، فان خاصية الاستئثار أمر ضروري للمعلومة فالجاني في الجرائم التي محلها المعلومات يستأثر فيها بسلطة تخص الغير وعلى نحو مطلق، والاستئثار في مجال المعلومات ينظر إلى المعلومة أنها من قبيل الأسرار ويستلزم الاستئثار في المعلومة نوعا من رابطة الأبوة[3].

والاستئثار أمر ضروري أيضا لأنه في جميع الجرائم التي ينطوي فيها الاعتداء القانوني على القيم يستأثر الفاعل بسلطة تخص الغير وعلى نحو مطلق، والاستئثار في مجال المعلومات يمكن أن يرد على الولوج في المعلومة والمخصص لمجوعة محددة من الأشخاص ويمكن أن يرد الاستئثار أيضا لشخص بمفرده باعتباره صاحب سلطة التصرف بالمعلومة، وعندئذ يكون لمؤلف المعلومات أو -صاحبها[4]. وترتبط بهذا الشكل من أشكال الاستئثار بالمعلومة نوع من الرابطة نجدها متحققة في حالتين:[5]

فالحالة الأولى: تتعلق بالمعلومات التي ينصب موضوعها على بيان حقيقة أو واقعة ما، وهذا النوع من المعلومات هو بحسب الأصل قد يكون سري وهنا تتحقق خاصية الاستئثار. أما إذا كان غير سري ومتاح للجميع وقام شخص بتجميع وحفظ هذه المعلومات ذاتها، فهو ينشأ عن طريق هدا التجميع وحفظ معلومة جديدة، ويمكن أن يستأثر بالتصرف فيها بمفرده[6] .

أما عن الحالة الثانية: تتحقق بتوافر الرابطة بين المعلومة وصاحبها عندما يكون موضوع هذه المعلومة فكرة أو عمل ذهني، ففي هذه الحالة ينظر مؤلف هذه المعلومة إليها

---

[1] - محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية القاهرة، 1994، ص 175-176.

[2] - نائلة محمد فريد قورة، مرجع سابق، ص 114- 115.

[3] - محمد عبد الإله أبوبكر سلامة، جرائم الكمبيوتر والانترنت، ، منشأة المعارف بالإسكندرية ، 2006، ص 82.

[4] سالم محمد بني مصطفى، جريمة السرقة المعلوماتية، رسالة حصول على درجة الماجستير قانون عام، جامعة جدارا، اربد الأردن، 2011، ص 17.

[5] سالم محمد بني مصطفى، المرجع نفسه ، ص 17.

[6] HUET Jérome « droit prive et informatique « Alain Bensoussan, Xavier lINANT de BELLEFONDS, Herbert,L emergence du droit de l'informatique, 1983,p . 32 , lucas de LEYSSAC,op.cit.,p 44.

بصفتها ملكا خاصا له، فإذا تمكن الغير من الاستيلاء عليها وعلى نحو غير مشروع، فسوف يشعر صاحبها بأنه قد سلب[1].

ثالثا: الشروط الفنية

إلى جانب السرية و الاستئثار التحديد و الابتكار هناك بعض الشروط غير المتفق عليها يشترطها البعض في المعلومات للتمتع بالحماية الجزائية تتمحور في التالي:

1-المعالجة الآلية:

هناك من يشترط أن تكون المعطيات معالجة آليا لكي تخضع للتجريم، ويقصد بها العمليات المتعددة والتي تتم بصفة آلية عن طريق معالجتها داخل النظام[2]. ونحن من جهتنا نؤيد ذلك لأنه لولا وجودها داخل النظام المعلوماتي لما أثرنا إشكالية هذه الدراسة أساسا.

2- اتخاذ تدابير جدية للمحافظة على سرية المعلومة:

يرى البعض أنه حتى يمكن حماية المعلومات السرية جزائيا، لابد من اتخاذ صاحبها إجراءات وتدابير جدية لحمايتها والمحافظة على سريتها خاصة إذا كانت تلك المعلومات على قدر من الأهمية كالمعلومات السياسية والاقتصادية والتجارية[3]. ومن تلك التدابير استخدام كلمات السر أوعمليات التشفير وغيرها من تدابير الحماية الفنية والتي سيتم التفصيل فيها أدناه.

الفرع الثاني
الطبيعة القانونية للمعلومات

ثار التساؤل حول الطبيعة القانونية للمعلومة محل الجريمة المعلوماتية وهي المعلومة بمنأى عن دعامتها المادية، هل تعتبر من قبيل المال أولها طبيعة خاصة؟، فتنازعت الإجابة على هذا السؤال مذهبين، التقليدي ويرى أنها ذات طبيعة خاصة(أولا) أما الحديث يرى أنها مجموعة مستحثة من الأموال(ثانيا) وتفصيل هاذين الاتجاهين فيما يلي:

أولا:الاتجاه التقليدي

يرى هذا الجانب من الفقه أن المعلومة ذات طبيعة خاصة، ويستوحي هذه النتيجة خلال من تطبيقه للمنهج التقليدي والذي بموجبه يضفي وصف القيمة على الأشياء المادية فقط.

[1] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1995، ص 188.
[2] محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية الإسكندرية، 2004، ص 43.
[3] رشدي محمد علي محمد عيد، مرجع سابق، ص293.

ويرتكز هذا المبدأ على بديهة مسلمة مؤداها أن الأشياء التي توصف بالقيم هي تلك الأشياء القابلة للاستحواذ المادي ومؤدى ذلك أن الأشياء التي يمكن الاستئثار، بها هي فقط التي تعد وحدها من قبيل القيم التي تكون محلا للاعتداءات القانونية. وبالنظر إلى أن للمعلومات طبيعة معنوية فإنه يكون من غير المقبول أن تكون قابلة للاستئثار والاستحواذ المادي، إلا عن طريق حق الملكية الأدبية والفكرية أو الذهنية أوا لصناعية. و عليه فإن المعلومات المختزنة والتي لا تنتمي إلى أي من المفردات أو المواد الأدبية أو الذهنية أو الصناعية لا تندرج حتما في مجموعة القيم المحمية قانونا،[1] وهكذا تستبعد بالضرورة من نظام مجموعة الأموال[2].

ولكن ونظرا للقيمة الاقتصادية للمعلومات التي لم يتمكن أنصار هذا الاتجاه إنكارها، أدى بالبعض منهم إلى إدخال المعلومات في طائفة المنافع، فللمعلومات في رأي هذا الاتجاه علاقة مباشرة بفكرة المنفعة أو الخدمة[3] .

ثانيا: الاتجاه الحديث

إن بعض الفقهاء المهتمين بالمشاكل الناشئة عن تزايد ظاهرة المعلوماتية قد قاموا بإطلاق وتطبيق وصف المال على المعلومة، حيث يرى أصحاب هذا الاتجاه أنه يمكن تقويم المعلومات بالمال وذلك انطلاقا من قيمتها الاقتصادية[4]، حيث يرى البعض أن قيمتها قد تزيد عن الأموال المادية، لذلك فقد تم اللجوء إلى معيار القيمة الاقتصادية للشيء إذ يعتبر مالا ليس بالنظر إلى كيانه المادي الملموس، وإنما بالنظر إلى قيمته الاقتصادية[5].

واعتبر أيضا هذا الاتجاه أن المعلومة واستقلالا عن دعامتها المادية تعد من قبيل المال، وهي قابلة للحيازة وهي قيمة تقوم وفقا لسعر السوق، وأيضا منتج بصرف النظر عن دعامتها المادية وعن عمل من قدمها، وأن المعلومة ترتبط بصاحبها عن طريق علاقة قانونية وهي علاقة المالك بالشيء الذي يملكه وعلى هذا الأساس تخول صاحبها ميزتين مهمتين، الأولى حقه في ضمان سرية المعلومة والثانية حقه في طلب التعويض عن الأضرار المترتبة على أي عمل غير مشروع يتعلق بها[6].

---

[1] محمد عبد الله أبوبكر سلامة، مرجع سابق، ص 75.

[2] سامي علي حامد عياد، مرجع سابق،ص 27.

[3] سامي علي حامد عياد، المرجع نفسه، ص 27 -28.

[4] سعداني نعيم، مرجع سابق، ص 39، مشار إليه لدى محمد حسام لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، خلال الفترة بين 25-20 أكتوبر 1993.

[5] السيد عتيق، مرجع سابق، ص 91.

[6] سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسة تحليلية، دار شتات للنشر والبرمجيات، مصر، 2011، ص 46.

وكخلاصة، فإن المعلومات هي كيان معنوي، لها ذات القيمة الاقتصادية للمال المادي ويعترف لها بالحماية القانونية، وفي إطار الحماية الجنائية يتعين الإقرار بصلاحية المعلومات كمحل للحماية من أنشطة الاعتداء كافة.

و بعدما تم التطرق لماهية المعلوماتية في المبحث الأول يمكن التطرق يعدها لمفهوم السرية بمفهومها الجديد أي المعلوماتي في المبحث الثاني، ويرجع السبب في ذلك لاعتمادنا المطرد على النظم المعلوماتية في كل مجالات الحياة حيث تولد لدينا السر المعالج آليا أو البيان السري المعالج آليا والذي أصبحت تحتويه الأجهزة الالكترونية بدلا من الصدور البشرية.

المبحث الثاني
ماهية السرية في المجال المعلوماتي

يعبر عن السرية في المجال المعلوماتي بالسرية المعلوماتية، والتي أصبحت ضرورية مع انتشار تقنية المعلومات وزيادة الاعتماد عليها من جهة، وانخفاض تكلفة معالجة تلك البيانات والمعلومات من جهة أخرى. فالحاجة اليوم إلى حماية السرية المعلوماتية أصبحت ملحة وضرورية وتزداد باستمرار، خاصة بعدما أصبح الحاسب وسيلة جديدة للحفظ والتخزين وهي مميزات عالية جلبت معها مخاطر كبيرة وأصبحت فرصة الاطلاع على الأسرار المعالجة آليا أكثر سهولة، فضلا على إمكانية نسخها في وقت لا يكاد يلحظ، ناهيك عن إمكانية اختراقها والاطلاع عليها من مسافات شاسعة. ولتحديد المقصود بالسرية المعلوماتية سيتم التفصيل في تعريف كل من السرية بعدما ين التطرق لمفهوم المعلوماتية والربط بينهما(المطلب الأول)، ثم سنحاول التمييز بينهما (المطلب الثاني) بعدها التطرق لماهية الخصوصية المعلوماتية (الطلب الثالث).

المطلب الأول
مفهـــــوم الســـــرية

السرية مفهوم قديم مرافق للإنسان بشكل مرافق لمصالحه الاجتماعية والاقتصادية والسياسية والعسكرية وغيرها، إلا أن هذا المفهوم قد طرأ عليه تغيير كان سببه الثورة الحالية في مجال الكمبيوتر وظهور الانترنت. فأصبح لدينا ما يعرف بالسرية المعلوماتية، فما المقصود بالسرية المعلوماتية؟. للإجابة على هذا السؤال الأمر يتطلب التطرق لمفهوم

السرية بشكل عام بطبيعة الحال في المجال القانوني، ثم التعرف على المقصود بالسرية المعلوماتية.

الفرع الأول
تعريف الســــــــرية وشروطها

سرية المعلومات انشغال لطالما كان من اهتمامات الإنسان مند القدم لارتباطه بجل مصالحة وعلى جميع الأصعدة، إلا أن هدا الانشغال طرأ عليه تغيير نتيجة التطور الحاصل بالتكنولوجيا الحديثة وظهور الثورة الحالية في مجال تقنية الحاسوب والاتصالات فبرز لدينا ما يسمى بالسرية المعلوماتية.

أولا:تعريف السرية

تباينت تعاريف السرية بين اللغوية والاصطلاحية، قد تختلف في صياغتها ولكن دوما تبقى تصب في نفس المضمون، وهي كالتالي:

1- تعريف السرية لغة:

السرية مؤنث السري، والسري المنسوب إلى السر، السري الذي يصنع سرا، والسر ما يكتم ويخفى، والسر من كل شيء: أكرمه وخالصه[1]. والسر ما يسره المرء في نفسه من الأمور التي عزم عليها [2]، قال تعالى: ﴿ وإن تجهر بالقول ، فإنه يعلم السر وأخفى﴾[3]، والسر أيضا من الأسرار التي تكتم و السر ما أخفيت والجمع أسرار، ورجل سري : يصنع الأشياء سرا من قوم سريين[4].

والسر هو ما أخفيه وأكتمه وهو خلاف الإعلان ويستعمل في المعاني والأعيان، والجمع أسرار قولك: أسررت الحديث أي أخفيته[5].

وأسره كتمه، وأسر إليه حديثا:أفضى، كقوله تعالى: ﴿وإذ أسرّ النّبي إلى بعض أزواجه حديثا..﴾[6]، ويرى البعض أن السر هو كل ما يضر إفشاؤه بالسمعة أو بالكرامة[7]، ويرى

---

[1] محمد مصطفى الشقيري، مرجع سابق،ص 266.

[2] المعجم الوسيط، مجمع اللغة العربية، القاهرة، دار ايحاء الترات العربي، بيروت، تحت كلمة سر .

[3] سورة طه، الآية رقم 6.

[4] جمال الدين أبي الفضل محمد بن مكرم ابن منظور الأنصاري الإفريقي المصري، راجعه عبد المنعم خليل إبراهيم، المجلد الثالث،الطبعة الأولى دار الكتب العلمية بيروت لبنان، 2005، ص 333.

[5] الرازي محمد بن أبي بكر، مختار الصحاح، دار الكتب العلمية، بيروت، 1983، ص 146.

[6] سورة التحريم، الآية رقم 3.

[7] عصام أحمد البهجي، حماية الحق في الحياة الخاصة،في ضوء حقوق الإنسان والمسؤولية المدنية، دار الجامعة الجديدة للنشر الإسكندرية، 2005، ص 90.

البعض الآخر أن الواقعة تعتبر سرا إذا كانت هناك مصلحة يعترف بها القانون في حصر العلم بها في شخص أو أشخاص محددين[1].

2- تعريف السرية إصطلاحا:

السر هو ما يفضي به الإنسان إلى آخر مستكتما إياه من قبل أومن بعد، ويشمل ما حفت به قرائن دالة على طلب الكتمان إذا كان العرف يقضي بكتمانه، كما يشمل خصوصيات الإنسان وعيوبه التي يكره أن يطلع عليها الناس، وهو أمانة لدى من استودع حفظه، التزاما بما جاءت به الشريعة الإسلامية وهوما تقتضي به المودة وآداب التعامل[2].

ويعرف أيضا أنه واقعة أوصفة ينحصر نطاق العلم بها في عدد محدود من الناس، إذا كانت ثمة مصلحة يعترف بها القانون لشخص أو أكثر في أن يظل العلم بها محصورا في ذلك النطاق[3].

والملاحظ أن السرية وكما يشير المعنى اللغوي هو صناعة تعتمد على إرادة الشخص نفسه في تحديد مكامن مصالحه، فهل الكتمان وإخفاء السر عن الغير هو الأفضل، لقوله صلى الله عليه وسلم:"استعينوا على قضاء حوائجكم بالكتمان فإن كل ذي نعمة محسود "، أم في الإفشاء وعندها، فعليه تحمل علم الغير بما لم يجب علمهم به.

تم تعريف السرية أيضا بواسطة المنظمة الدولية للتوحيد القياسي (ايزو) على أنها "ضمان أن تكون المعلومات متاحة فقط لأولئك الذين يؤذن لهم بالاطلاع"، وهي أحد الأركان الأساسية لأمن المعلومات، فالسرية هي واحدة من أهداف التصميم لنظم ترميز كثيرة، مما جعلها ممكنة من الناحية العملية عن طريق تقنيات التشفير الحديثة[4] .

وحيث أصبحت الأسرار مخزنة في ذاكرة الحاسب الآلي بعدما كانت توضع في خزانة مقفلة، تولد لدينا الأسرار المعلوماتية والتي نقصد بها الأسرار المعالجة آليا، أي تتناول المعالجة الآلية للمعلومات السرية بشكل منظم وفعال بحيث لا تكون هذه المعلومات في مجموعها أوفي الشكل والتجميع الدقيقين لمكوناتها معروفة عادة أوسهلة الحصول عليها من قبل الأشخاص خاصة الذين يتعاملون في نوع تلك المعلومات.

ثانيا:شروط اتصاف الواقعة بالسرية[5]

بعد التطرق لتعريف السرية قد يصعب علينا أحيانا تحديد وصف الواقعة بالسرية من عدمها، وسواء كان السر بمفهومه الحديث أو التقليدي يشترط لتحديد طبيعته مجموعة من الشروط، يمكن أن تتلخص في الآتي:

---

[1] علي أحمد عبد الزغبي، مرجع سابق، ص 185.

[2] محمد مصطفى الشقيري، المرجع نفسه، ص 267.

[3] عصام احمد البهجي،حماية الحق في الحياة الخاصة،دار الجامعة الجديدة للنشر،الإسكندرية ، 2005 ، ص 90 -91.

[4] أنظر الموقع الالكتروني، http://ar.wikipedia.org/wiki ، يوم الاطلاع عليه 2015/12/08.

[5] أنظر الموقع الالكتروني،http://www.mohamah.net/law ، يوم الاطلاع عليه 2017/05/08.

1 – أن يكون السر بطبيعته أو بسب الظروف المحيطة يه

لقد انقسم الفقه بشأن تحديد طبيعة السر إلى اتجاهين اتجاه أخذ بالمعيار الشخصي، حيث يتم تحديد وصف السرية عن طريق صاحب السر طواعية، أما الاتجاه الآخر فيأخذ بالمعيار الموضوعي الذي يعتمد في تحديد وصف السرية بالنظر إلى الظروف والأحوال الموضوعية التي أحاطت بالواقعة، كالمعلومات التي تتصل بالحياة الخاصة للأفراد، وبأسرارهم المالية والتجارية والشخصية.

2 - أن لا يكون معلوماً للكافة:

يفقد الأمر صفة السرية إذا كانت الواقعة التي تتعلق بها معلومة للكافة، على أنه ينبغي أن يلاحظ هنا بأن الطابع السري للواقعة أو المعلومة لا ينتقي حتى لو كانت معروفة بهذا الشكل أي للكافة، ما دامت غير مؤكدة.

فالسر يمكن أن يكون معلوماً من قبل عدد محدود من الناس حتى لو كان كبيراً ما داموا من محيط عائلي، أو من محيط عمل واحد، وبرغم ذلك يبقى طابع السرية ملازماً له. بينما تنتفي صفة السرية عن الواقعة، حتى لو لم يعلم بها كثير من الناس، إذا علم بها من لا تربطهم بصاحب السر علاقة خاصة، كالعلم بالوقائع عن طريق جلسة محاكمة علنية.

الفرع الثاني
أنواع الأسرار المعلوماتية

تتعدد وتتنوع الأسرار وتختلف باختلاف الأشخاص والظروف فما يعتبر سرا بالنسبة لشخص قد لا يعتبر سرا بالنسبة لآخر وما يعتبر سرا في ظروف معينة قد لا يعتبر كذلك في ظروف أخرى.

فمثلا هناك الأسرار الاقتصادية، والتي تتعاظم أهميتها في الوقت الراهن والمستقبل بالنسبة للدول والمشروعات الخاصة. حيث أصبحت الأسرار الاقتصادية هي أساس المنافسة الاقتصادية بين الدول والكيانات الاقتصادية. كما توجد الأسرار الدبلوماسية ويقصد بها "الحقائق بعلاقات الدولة الدبلوماسية بأشخاص القانون الدولي العام، مثل اعتراف الدولة بقطع علاقاتها السياسية بدولة معينة أو الاعتراف بهيئة ثورية معينة وكذلك المعلومات المتعلقة بسير المفاوضات السياسية". كما توجد الأسرار العسكرية وتشمل كل ما يتعلق بالشؤون العسكرية والإستراتيجية. هذا بالإضافة إلى وجود ما يسمى بالأسرار الإدارية، وأيضا الأسرار الخاصة

بالأفراد، أسرار التقاضي، الأسرار المهنية وغيرها وهكذا يمكن أن نتصور أن السرية بصفة عامة تشبه دائرة كبيرة يتم تقسيمها إلى أجزاء غير متساوية وغير محددة ومن هذه الأجزاء ما يكون متعلقا بسرية المراسلات، وما يكون متعلقا بسرية التحقيقات،....وغيرها[1].

وحيث أنه للتوضيح أكثر بشأن أنواع الأسرار المعلوماتية، كان لابد من التطرق لأنواع المعلومات الالكترونية بصفة عامة، والتي تعتبر المعلومات الالكترونية السرية جزء منها وتفاديا للتكرار فالمعلومات التي تتصف بالسرية هي المعنية بالدراسة، والتي هي خلاف ذلك فليست هي المقصودة بهذه الدراسة مثل المعلومات المتاحة. وتم تقسيم المعلومات عدة تقسيمات كان أهمها تقسيماتها إلى ثلاث طوائف و هي المعلومات الاسمية(أولا)، والمعلومات الخاصة بالمصنفات الفكرية(ثانيا)، وأخيرا المعلومات المباحة(ثالثا).

أولا: المعلومات الإسمية

وتنقسم بدورها إلى مجموعتين وهما المعلومات الشخصية والمعلومات الموضوعية كالتالي:

أ – المعلومات الشخصية:

هي المعطيات المعلوماتية الاسمية أو الشخصية وهي المعلومات المرتبطة بالشخص كالحالة الاجتماعية أو المدنية كالاسم واللقب والجنسية والسوابق العدلية وغيرها. ووفقا أغلبية القوانين انعدام حق الغير في الاطلاع على هذه المعلومات مراعاة للخصوصية إلا في حالة وجود موافقة شخصية من صاحبها أو بأمر من السلطة المختصة.[2]

والجدير بالذكر أن المشرع الفرنسي، حاول إدراج تعريف صريح للمعطيات ذات الصيغة الشخصية وأنشأ لذلك هيئة مكلفة بحماية مصالح الأفراد الطبيعيين والذين تم جمع أو معالجة أو حفظ معلوماتهم ، وذلك من خلال القانون 17/78 السالف الذكر، ويقصد بالمعطيات ذات الطابع الشخصي أي معطيات يمكن أن تحدد شخص معين[3].

ب – المعلومات الموضوعية:

هي بخلاف الشخصية موجهة إلى الغير وليست لصيقة بشخصية صاحبها، ومن أمثلتها المقالات الصحفية والملفات الإدارية للموظفين، وهناك من يرى أنه يمكن الفصل بين مالك المعلومة والشخصية المتصلة بها، فالصحفي الذي يكتب مقالا عن شخص معين له حق على المقال، ولكن لا يجب أن يتعدى على حق الشخص محل المقال نفسه.[4]

ثانيا: المعلومات الخاصة بالمصنفات الفكرية

---

[1] عصام أحمد البهجي، حماية الحق في الحياة الخاصة، في ضوء حقوق الانسان والمسؤولية المدنية، دار الجامعة الجديدة للنشر، 2005، ص 98 وما بعدها.

[2] محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية ، 2004، ص 44.

[3] ZICRY Laure, op.cit, p.15 et 52.

[4] محمد أمين الرومي، المرجع نفسه، ص 44.

وهي عبارة عن معلومات متمثلة في مصنفات فكرية وهذه المصنفات محمية بقوانين الملكية الفكرية ويستوي في ذلك أن تكون تلك القوانين متعلقة بالملكية الأدبية والفنية أو متعلقة بالملكية الصناعية والعلامات التجارية[1] كالمؤلفات والأغاني أوا لأفلام أو البرامج المعلوماتية وغيرها.

ثالثا: المعلومات المباحة

ويقصد بها تلك المعلومات التي يتاح للجميع الحصول عليها لأنها بدون مالك، مثال ذلك تقارير البورصة اليومية والنشرات الجوية، وتنعقد ملكية هذه المعلومات للأسبق إلى جمعها وصياغتها. فإذا تم تجميعها وتخزينها واسترجاعها، أو بقصد تخليق معلومات جديدة فإنها لا تصبح متاحة بل ستتصف بالسرية و تنقسم إلى التالي:

أ – **المعلومات المعالجة:** ويقصد بها المعلومات التي تعالج للتشغيل على جهاز الكمبيوتر بقصد تخزينها وحفظها فيه واسترجاعها وقت الحاجة.

ب – **المعلومات المتحصلة:** ويقصد بها تلك المعلومات التي تنتج عن معالجة مجموعة من المعلومات وتقرر حق ملكيتها هنا طبقا لقاعدة حيازة المال المنقول[2].

الفرع الثالث
أسس السرية

فموضوع حماية السرية المعلوماتية جزائيا هو من الموضوعات ذات الأبعاد المختلفة، فهو يمس الشخص من جميع الجوانب الاقتصادية والنفسية والنظامية وغيرها،ذلك أنه متعلق بضروريات تسعى الإرادة التشريعية للحفاظ عليها. لاسيما وأن كفالة حماية المعلومات السرية تحقق مبدأ عظيم من المبادئ القانونية وهي حفظ المصالح، بينما التعرض للمعلومات السرية بالإفشاء أو الاطلاع أو غير ذلك ينتج عنه أضرار جسيمة تؤثر في كيان الشخص و حتى الدولة.

لذلك كان لابد من التعرض لأسس السرية أو أسبابها، فمنها ما هو نفسي، اجتماعي، اقتصادي، وهناك ما هو قانوني وسيتم التفصيل فيها على النحو التالي:

أولا: الأساس النفسي والاجتماعي

ربما يعتبر السبب النفسي في كتمان السر الأساس الأول الذي يدعو إلى السرية، حيث أن أي شخص ترفض نفسه أن يعلم سره أي شخص غير مخول له بذلك، فيذهب جانب من

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 55.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009، ص 56.

الفقه إلى أن السرية يمكن تحليلها بأنها انعكاس للحذر الذي ينحو صوب الماضي، ويرفض الصراع في مواجهة المجهول[1].

ويبقى الشخص دوما حريص على سرية معلوماته، بينما قد تتعرض هذه المعلومات لخطر الانتهاك بالوسائل الفنية حيث ترك الأفراد الوسائل التقليدية خلفهم في الوصول إلى المعلومات وأصبح اعتمادهم أكثر فأكثر على الانترنت والحاسب الآلي، وهو ما يسبب الأذى النفسي والمعنوي ربما الأكثر إضرارا منه عن المادي.

وعن الأساس الاجتماعي للسرية فهو يرتبط ارتباطا مباشرا بالأساس النفسي، ويمكن وصف السرية بصفة عامة أنها حدث اجتماعي يصف العلاقة بين مجموعة واحدة[2]، هذه العلاقة تحمل بين طياتها وظيفتين، الأولى تتعلق بالسلطة حيث يمنح السر لصاحبه قوة تميزه عن سواه، والثانية تتعلق بالفصل استنادا إلى أن بعض المعلومات يجب ألا تكون مباحة للجميع[3].

فإذا كانت المعلومة هي القوة فإن الحفاظ عليها يعني استمرار القوة، وبالتالي فإن المصلحة تقتضي عدم العلم بها ممن لا يجوز لهم ذلك، وبالتالي فللسرية مدلول خارجي يحدد العلاقة بين من يملك السر و من لا يملكه[4].

ثانيا: الأساس الاقتصادي والقانوني

أصبح للتحكم في المعلومات في المجتمعات المعاصرة دور متنامي وعامل أساسي في النجاح الاقتصادي، فلا شك أن المفاجأة بالنسبة للمنافسين والتشويق بالنسبة للعملاء والمضاربة في السوق أكيد أنها تتم من خلال السرية ولابد من إحاطة النظام المعلوماتي للمؤسسات الاقتصادية بالأمان لتحقيق النجاح.والجدير بالذكر أنه بدون سرية المعلومات من المستحيل خلق مجتمع متماسك على جميع الأصعدة بما فيها الاقتصادية.

وفي نفس السياق يطرح السؤال عن من أين تستمد السرية مشروعيتها القانونية؟، و الإجابة هي ما يعبر عنه بالأساس القانوني. وفي هذا المجال فإن القانون يحمي السرية من جميع الأصعدة المدنية من خلال القانون المدني والجزائية من خلال قانون العقوبات والقوانين المكملة له.

---

[1] نادية محمد معوض، مرجع سابق، ص 33.

[2] SIMMEL(G .),La Sociéte Seréte,Novelle revue Psychanalyse,1976,n° 14 , P.281.
مقتبس عن نادية محمد معوض، مرجع سابق، ص 24.

[3]ZEMPLENI (A.) , La Chàine du secret, Novelle revue Psychanalyse, 1976,N° 14,P .316.
مقتبس عن نادية محمد معوض، المرجع نفسه، ص 24.

[4] SIMMEL(G .), OP.Cit , P.281 .
مقتبس عن نادية محمد معوض، المرجع نفسه، ص 24.

وما زاد من التخوف على السرية من الانتهاك، طبعا التقدم الهائل في المجال المعلوماتي حيث أنه يعتبر سبب أساسي في العصر المعلوماتي. فالثورة المعلوماتية التي ألقت بظلالها على جميع الأصعدة وباتت المعلومات السرية فيها أكثر تعرضا لخطر الانتهاك، والذي سيتم بكل سرعة وسهولة وألقت بظلالها أيضا على المعلومات الخاصة بلأفراد سواء كانت سرية أو لا، وهو الأمر الذي يتطلب البعض من التفصيل حول الفرق بين المعلومات السرية والخاصة بالأفراد.

المطلب الثاني
تمييز السرية عن الخصوصية

كلما مررنا بمصطلح السرية إلا وصادفنا مصطلح الخصوصية، ودراستنا هته تتعلق أساسا بكل جوانب السرية المعلوماتية، ورأينا أنه من الواجب التطرق للخصوصية أو"السرية الشخصية كما يسميها البعض"[1]، ومعرفة العلاقة الموجودة بينها وبين السرية طالما أنه تم التعثر بها في أكثر من محطة ونحن بصدد هته الدراسة.

"الخصوصية كحق عام يمتد لحماية الشخص من كافة أوجه الاعتداءات والتدخل في حياته، ويمكن القول أن كافة دول العالم على وجه التقريب أقرت بشكل أو بآخر الحق في الخصوصية في واحد أو أكثر من مظاهره. فالخصوصية مفهوم يتعلق بالعزلة والسرية والاستقلال الذاتي ولكنها ليست مرادفة لهذه المصطلحات"[2].

فالخصوصية من الناحية اللغوية تقترب من مفهوم السرية لكنها ليست مرادفة له، وذلك لأن السرية تفترض الكتمان والتخفي في حين أن الخصوصية وإن كانت تفرض قدرا من الكتمان والتخفي لكنها قد تتوفر رغم انعدام السرية[3]. كما أن الخصوصية لا تقتصر على عدم الكشف عن الأسرار بل تعني كذلك الامتناع عن الاعتداء على هدوء الآخرين وسكينتهم[4]. ومنه فإن الحق في السرية يعد جوهر الحق في الخصوصية إن لم يكن وجها لازما لهدا الأخير[5].

---

[1] ماجد أحمد عبد الرحيم الحياري، مسؤولية الصحفي المدنية،دراسة مقارنة بين القانونين الأردني والمصري، الطبعة الأولى، دار يافا العلمية للنشر والتوزيع، 2008 ، ص 30.

[2] فريد هكيت، الخصوصية في عصر المعلومات، ترجمة محمد محمود شهاب، الطبعة الأولى ، مركز الأهرام للترجمة والنشر، القاهرة، 1999، ص 34.

[3] ماجد أحمد عبد الرحيم الحياري، مرجع سابق ، ص 29.

[4] علي أحمد عبد الزغبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب طرابلس لبنان، 2006، ص 125.

[5] علي أحمد عبد الزغبي، المرجع نفسه ، ص 180.

ولكن رغم كل هذا، فإن هناك من يرى بأن السرية والخصوصية شيء واحد لهذا كان لابد من التعرض للعلاقة بين الخصوصية والسرية، فهناك اتجاهين تعرضا لهاته المسألة بين اتجاه قضى بضرورة الفصل بين الخصوصية والسرية ولم يعتبرهما شيء واحد واتجاه آخر يرى العكس وسنعرض الاتجاهين كالتالي:

الفرع الأول
الاتجاه الأول القائل بالفصل بين الخصوصية والسرية

يذهب جانب من الفقه إلى أنه لا يجوز الخلط بين الحق في السرية والحق في الخصوصية، فالخصوصية مرحلة وسط بين السرية والعلنية فإذا كان المشرع يحمي الحق في الخصوصية فهو يحمي الحق في السرية من باب أولى ولكن يمكن أن يكون ما هو خصوصي ولكن لا يكون سريا في نفس الوقت. فالسر هو ما يعرفه صاحبه أو أمنية أما الخصوصي فهو ما لا ينشر أي ما لا يعتبر علنا مكشوفا للكافة حتى ولو لم يكن كتمانه قد وصل إلى حد السر[1].

ويؤسس وجهة نظره على الأسانيد الآتية[2]:

1-من الخطأ الكبير الخلط بين السرية والخصوصية فدقائق العلاقة بين الأزواج لا تتصف بالسرية لمعرفة الكثيرين بها من الأقارب والأصدقاء ولكنها مع ذلك تحتفظ بخصوصيتها ويحرص الشخص إلى عدم النشر خارج هذه الدائرة.

2-ويستشهد بما قضى به القضاء من إدخال وقائع تعتبر بعيدة كل البعد عن نطاق الحياة الخاصة وبعيدة عن السرية مثل الاسم فالاسم لا يعتبر سرا ومع هذا يدخلها القضاء في نطاق الحياة الخاصة.

3-ويضيف بأن مجرد النشر لبعض مظاهر الحياة الخاصة وكشف أسرار الحياة الخاصة إلى العلن وكشف النقاب عن السر يستحيل معه القول بأنه مازال هناك سرا فالكشف عن السر يحوله إلى العلن ويظل علنا دائما وأبدا ولا يتصور أن يعود العلن إلى حظيرة السرية وبالتالي يجوز إعادة النشر لهذه الأسرار دون الحصول على إذن أورضاء من صاحب السر ولا يتصور وجود ضرر في إعادة النشر.

فلا يعقل أن يوصف بالسرية والخصوصية ما هو معلن على الملأ ومعروف للكافة فالكشف عن السر ولو مرة واحدة ينفي عنه إلى الأبد صفة السر ويدخله في نطاق العلنية ومن يقبل الكشف عن خصوصيات حياته فهو لم يقبل إلا الكشف عن السر أي نفي هذه

[1] عصام أحمد البهجي، مرجع سابق ، ص 102.

[2] عصام أحمد البهجي، المرجع نفسه، ص 103- 104.

الصفة عنه فإذا تم النشر فعلا في حدود ما سمح به الشخص فلا يقبل ولا يعقل بأن يعود مرة أخرى ويدعى أنه هناك مساسا بخصوصيات حياته قد وقع.

4-ويضيف أصحاب هذا الاتجاه بأنه لا يمكن فهم المسألة إلا إذا فرقنا بين السرية والخصوصية وفهمنا الأخيرة على أنها أكثر اتساعا من الأولى ويذهب البعض من أنصار هذا الاتجاه إلى أن الحياة الخاصة هي التي تدخل في نطاق السرية التي تكون للشخص على بعض أنشطته.

5-كما يضيف هؤلاء بأن الخصوصية لا تكون مرادفة للسرية حيث أن الخصوصية قد تتوافر على الرغم من عدم وجود السرية.

وينتهي هؤلاء إلى القول بأن السرية تفترض إذن الكتمان والخفاء التام أما الخصوصية فلا يلزم لتوافرها هذا القدر من عدم العلانية على الأقل في بعض جوانبها.

وينتصرون بما ذهب إليه إدوارد شليز أن الفارق بين السرية والخصوصية يكمن في أن السرية يحظر القانون الإعلان عنها بأي معلومات أو الكشف عنها أما في الخصوصية فالكشف عن المعلومات أو الإعلان عنها مسألة ترجع إلى تصرف من يملك المعلومات[1].

الفرع الثاني
الاتجاه الثاني القائل بالربط بين السرية والخصوصية

يذهب أنصار هذا الاتجاه إلى الربط الوثيق بين الحق في السرية والحق في الخصوصية ولكنهم اختلفوا في وصف هذا الربط وطبيعة العلاقة، فنجد جانب منهم يذهب إلى إحلال الحق في السرية محل الحق في الخصوصية إذ أنهم يعتبرون أن الحق في الخصوصية أو الحق في احترام الحياة الخاصة هو ما يطلق عليه الحق في السرية، ولكل شخص الحق في المحافظة على سرية خصوصيات حياته وعدم جعلها عرضة لأن تلوكها ألسنة الناس أو أن تكون موضوعا لصفحات الجرائد[2].

ورغم تعرض الآراء الفقهية فيما يتعلق بتمييز السرية عن الخصوصية، إلا أن الرأي الغالب هو الثاني حيث أن السرية والخصوصية هما ليسا شيء واحد، وعلى هذا الأساس كانت هذه الدراسة شاملة لحماية المعلومات الالكترونية السرية، وقد يكون منها ما هو يتعلق بالحياة الخاصة للأفراد ومنها ما هو ليس كذلك.

---

[1] عصام أحمد البهجي، مرجع سابق، ص 105.

[2] عصام أحمد البهجي، مرجع سابق، ص 105.

فكل معلومة تمت معالجتها الكترونيا تتصف بالسرية سنعالج النصوص التجريمية التي جرمت سلوكات انتهاكها كالدخول غير المشروع للنظام المعلوماتي ومشاركة صاحب المعلومة الاطلاع عليها من دون رضاه مثلا، أو الحصول على هذه المعلومة السرية بطريقة غير مشروعة والتعامل فيها بطريقة غير مشروعة أيضا، أو اعتراض رسالة الكترونية بعث بها صاحبها إلى المرسل إليه وأعترض طرقها وأطلع عليها مع ما يمكن أن تحمله هذه الرسالة من أسرار خاصة، وغيرها من صور الاعتداءات التي تتعرض لها المعلومة السرية، وهو ما سيتم التفصيل فيها أدناه مع العلم أنه تم اعتبار مصطلح المعلومات السرية كمرادفة للبيانات التي تمت معالجتها الكترونيا.

إذن كل ما ورد أعلاه كان للتفرقة بين السرية والخصوصية بوجه عام، ولا ننسى أنه ظهر لنا ما يعرف بالخصوصية المعلوماتية وهي أحد الحقوق التي قد تنتهك سريتها بأحد الصور التي سيرد التفصيل فيها ولهذا رأينا أن نفصل فيها بعض الشيء مع ما يخدم الدراسة، باعتبار أن المعلومات فيها هي جزء من الكل من موضوع الدراسة.

المطلب الثالث
ماهية الخصوصية المعلوماتية

إن حاجة الإنسان بأن يخلو إلى نفسه وأن يشعر بالهدوء والسكينة البعيدة عن أعين الناس أومراقبة الفضوليين أو الاحتفاظ بأفكاره أو علاقاته الحميمة أو ارتباطاته وأفراد أسرته وراء ستـــــــــــــار السرية، حاجة قديمة قدم وجود الإنسان نفسه.

لذا تحرص المجتمعات خاصة الديمقراطية منها على كفالة الخصوصية، وتعتبره حقا مستقلا قائما بذاته، ولا تكتفي بسن القوانين لحمايته بل تسعي إلى ترسيخه في الأذهان، وذلك بغرس القيم النبيلة التي تلعب دورا كبيرا وفعالا في منع المتطفلين من التدخل في خصوصيات الآخرين وكشف أسرارهم.

ولقد حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أومن جانب الدساتير والنظم القانونية.

فعلى الصعيد الدولي، نجد أن هذا الاهتمام يبرز في صورة اتفاقيات دولية كالإعلان العالمي لحقوق الإنسان الصادر من الجمعية العامة للأمم المتحدة[1] في المادة 12 التي تنص على أنه " لا يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته

[1] ذلك بموجب قرارها رقم 217 المؤرخ في 1948/12/10.

أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات".

ولقد تضاعف الاهتمام بهذا الحق نظرا لما يتعرض له من مخاطر تحيط به وتهدده أبرزها التقدم التكنولوجي والإعلامي والذي كان له دور كبير في اقتحام حصون هذا الحق واختراق حواجزه وتسلق أسواره، الأمر الذي يقتضي تدخل المشرع لحمايته بالأسلوب الذي يتفق وطبيعة هذه الأخطار .

أما على الصعيد المحلي أو الداخلي فإن الاهتمام بهذا الحق يبرز من خلال ما نصت عليه في الدساتير والنظم السياسية للدول[1] كالدستور الجزائري[2] من خلال المواد[3] 40و 41، بالإضافة إلى ذلك نجد أن غالبية الدول ومن خلال تشريعاتها الوطنية قد أصبغت حمايتها الجزائية لهذا الحق،كالقانون الفرنسي في قانون العقوبات بموجب المواد226-1، 226-2، 226-8 والمواد 309 مكرر و309 مكرر(أ) من قانون العقوبات المصري، والمادة303 مكرر قانون العقوبات الجزائري[4] .كما أنه يمكن إقرار الحق في حرمة الحياة الخاصة من خلال نص المادة 47 من القانون المدني الجزائري[5].

ولهذا الحق العديد من المفاهيم المنفصلة لكنها ترتبط معا في ذات الوقت وهي[6]:

1- خصوصية المعلومات والتي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقات الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية وهي المحل الذي يتصل عادة بمفهوم حماية البيانات .

2- الخصوصية الجسدية أو المادية، والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات، فحص المخدرات، الخصوصية

---

[1] كالنظام الأساسي لسلطنة عمان الصادر بالمرسوم السلطاني رقم 96/101 في المواد 18،27،30 منه والمواد 57، 45 من الدستور المصري ، والمواد7 ، 10 ، 15 من الدستور الأردني 1952م ، والمواد 11 ، 29 ، 30 ، 31 ، 39 من الدستور الكويتي وغيرها.

[2] الدستور الجزائري لسنة 2016 بموجب القانون رقم 01/16 المؤرخ في 6 مارس 2016 ، جريدة رسمية رقم 14 مؤرخة في 7 مارس 2016، ص 3

[3] نصت المادة 40 على أن الدولة ضمن عدم انتهاك حرمة الإنسان كما يعاقب القانون بموجب المادة 41 من الدستور على المخالفات المرتكبة ضد الحقوق و الحريات و على كل ما يمس بسلامة الإنسان البدنية أو المعنوية.

[4] بالنسبة لقانون العقوبات الجزائري صدر تعديل بشأنه بموجب القانون 23/06 المؤرخ في 20 ديسمبر 2006 جريدة عدد 84 صادر بتاريخ 24 ديسمبر 2006 الذي عدل وتمم الأمر 156/66 المؤرخ في 8 يونيو1966 والمتضمن قانون العقوبات الجزائري.

[5] نصت المادة 47 من القانون المدني الجزائري: " 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".

[6] صليحة علي صداقة، مرجع سابق، ص 175، يونس عرب، الخصوصية وحماية البيانات، بحث منشور على شبكة الإنترنت من خلال موقع www.arablaw.net ، ص 12.

الصحية.[1]

3- خصوصية الاتصالات والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الالكتروني وغيرها من وسائل الاتصال والتحادث في البيئة الرقمية.

4- الخصوصية الإقليمية نسبة إلى الإقليم المكاني والتي تتعلق بالقواعد المنظمة للدخول إلى المنازل وبيئة العمل أو الأماكن العامة والتي تتضمن التفتيش والرقابة الالكترونية والتوثق من بطاقات الهوية.

فالخصوصية المعلوماتية مفهوم تولد من خلال المعالجة الآلية و التحليل للبيانات المتعلقة بالحياة الخاصة للأفراد، و يدخل في نطاق هذه الدراسة كل أوجه التجريم المتعلقة بالجانب السري للخصوصية المعلوماتية باعتبار أن المعومات الخاصة هي في الأصل من المعلومات الجديرة بالحماية الجزائية، و كان لزوما ادراج بعض التفصيل في مفهوم الخصوصية المعلوماتية، من خلال التطرق إلى تعريفها (فرع أول) ثم بعض صور الاعتداء عليها (فرع ثان) وسيتم ال تطرق للبعض منها في حدود ما يتعلق بالاعتداء على السرية فقط.

الفرع الأول
تعريف الخصوصية المعلوماتية

يقصد بالخصوصية من الناحية اللغوية حالة الخصوص، والخصوص نقيض العموم، يقال: اختص فلان بالأمر وتخصص له إذا انفرد به واختصه، والخصوص إذا الانفراد ويقابله العموم، كما يفيد الحصر وضده الإطلاق[2].

ويعبر عن الخصوصية في النظام القانوني اللاتيني بمصطلح الحياة الخاصة، ورغم كثرة تعريفات الخصوصية إلا أنها تعتبر في غالبيتها صدى لبعضها البعض[3]، فقد جاء في تعريف بأنها:" حق من طبيعة مادية يرتبط بالشخصية الإنسانية التي لها عليه سلطة تقديرية كاملة".

فهناك نوع من المعلومات يطلق عليها خاصة كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الاسم والعنوان ورقم الهاتف وغيرها من المعلومات، فهي معلومات تأخذ شكل بيانات تلزم الالتصاق بكل شخص طبيعي معرف أو قابل للتعريف[4].

---

[1] أدى التطور التكنولوجي إلى ظهور علم جديد هو علم إدارة وتقنية المعلومات الصحية أو نظام المعلوماتية الصحية حيث أنه علم يجمع بين علوم الحاسب الآلي من جهة وعلوم الطب والرعاية الصحية من جهة أخرى، أنظر صليحة علي صداقة، مرجع سابق، ص 35 .

[2] أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، الطبعة الأولى، 2010، ص 49، عن ابن منظور، لسان العرب، القاهرة، مطبعة بولاق، الجزء الثامن، الطبعة الأولى، ص 390.

[3] أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، الطبعة الأولى، 2010، ص 50.

[4] عمر أبوبكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004 ، ص 614

وهذه النوعية من المعلومات أصبحت في وقتنا الحاضر على درجة كبيرة من الأهمية في ظل فلسفة المعلوماتية المعاصرة ، لاسيما وأن فكرة العالم الرقمي، لا يمكن لها السير في التطور ومواكبة اهتمامات الإنسان سوى باستخدام المعلومات، من هنا ظهر ما يعرف بالخصوصية المعلوماتية.

ويعتبر مبدأ الخصوصية المعلوماتية الذي يقصد به حق الشخص في أن يتحكم بالمعلومات التي تخصه[1]. ويعود الفضل في توجيه الانتباه لمفهوم خصوصية المعلومات في هذه الفترة إلى مؤلفين أمريكيين هامين في هذا الحقل الأول كتاب الخصوصية والحرية لمؤلفه ويستن عام 1967 [2]، والثاني كتاب الاعتداء على الخصوصية لمؤلفه ميلر[3]. وكلاهما قدما مفهوما وتعريفا لخصوصية المعلومات، فويستن ذهب في تعريفه للخصوصية المعلوماتية إلى أنها " حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين، في حين عرَف ميلر الحق في خصوصية المعلومات على أنها قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم.

وعرف البعض الخصوصية أيضا أنها:" حق احترام سرية وخصوصية الأشخاص من أي تدخل مادي أومعنوي، وهو حق عميق الجذور من الوجهة التاريخية"[4]. وعرفه البعض الآخر أنه " حق الإنسان في أن تحترم الحياة الخاصة به وأن تحفظ أسراره التي يجب ألا يطلع عليها الآخرون بغير إذنه، يتمثل في حماية حرمة المسكن وحرمة الاتصالات والمراسلات الخاصة بالإنسان[5].

الفرع الثاني
صور سلوكيات الاعتداء على الخصوصية المعلوماتية

وهي عموما ذات أشكال الاعتداء على الأسرار المعلوماتية بصفة عامة، وفيما يتعلق بتجريم تلك السلوكات سيرد التفصيل فيها في الباب الثاني من هذه الدراسة وذلك لتفادي التكرار، لأن هذه الدراسة لا تعني الأسرار الخاصة بالإنسان فقط وإنما تعني الخصوصية الفردية والجماعية. وبالتالي فهي تخص كل المعلومات السرية الالكترونية أيا كانت الجهة التي تخصها هذه المعلومات، فالخصوصية المعلوماتية هي جزء من هذه الدراسة حيث أنها لا تعتبر هي السرية المعلوماتية، ذلك لأن هذه الدراسة موضوعهاكل معلومة معالجة آليا قد

[1] محمد عبد المحسن المقاطع، نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر، بحث مقدم لمؤتمر الكويت الأول للقانون والحاسب الآلي ، كلية الحقوق ، جامعة الكويت ، الطبعة الأولى 1994، ص174.

[2] يونس عرب دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، ورقة عمل مقدمة إلى ندوة أخلاق المعلومات - نادي المعلومات العربي 16-17 أكتوبر 2002 – عمان – الأردن.

[3] يونس عرب ، المرجع نفسه.

[4] طارق عفيفي صادق أحمد، الجرائم الالكترونية جرائم الهاتف المحمول، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015، ص 149.

[5] طارق عفيفي صادق احمد، المرجع نفسه، ص 150.

تكون خاصة بالأفراد أو تكون خلاف ذلك، ولكنها لابد أن تتصف بالسرية. وتتمثل سلوكات الاعتداء على الخصوصية الفردية في الآتي:

أولا: الاطلاع المجرد

محل الاطلاع في هذه الحالة هو معلومات شخصية وخاصة يريد صاحبها إبقاءها سرية، وأما صورة هذا السلوك هو الاطلاع الكلي أو الجزئي على تلك الأسرار الخاصة بحيث يقوم اليقين بالعلم بها وفهمها، فإذا كانت الأسرار بلغة لا يفهمها الفاعل أولا يحسن تحليلها، لم يتحقق الاطلاع إلا بتكامل الصورة وترابط أجزائها. فإذا لم يكن ما أطلع عليه الفاعل سوى جزيئات غير مترابطة، غير ذات معنى مفيد لم يتحقق الاطلاع أيضا، وهذا الاطلاع يجب أن يكون في ذاته غير مشروع وأن يتم من شخص لا يملك قانونا ترخيصا بالولوج إلى تلك المعلومات، كما يشترط لتحقق هذه الصورة أن يكون الاطلاع مجردا أي أن يكون قصد الفاعل هو الاطلاع فقط على تلك المعلومات السرية ومجرد العلم الشخصي بها[1].

وذلك كأن يقوم الشخص العالم بأوجه الدخول إلى أنظمة الغير بالتسلل إلى أنظمة الحاسب الآلي لشخص آخر وإعطائه الأوامر اللازمة بفتح ملفات الشخص المعتدى عليه والاطلاع عليها عن طريق المشاهدة على شاشة عرض جهازه هو، إن هذا الفعل يشكل خرق للسرية والخصوصية وذلك أن السر إنما جعل سرا لكونه يخفي ما لا يرغب الإنسان في إظهاره لعلة شخصية قد تتعلق بسلوك أو مصلحة إذا أفشت عادت بالضرر على صاحبها[2].

ثانيا:الاطلاع بقصد الافشاء

في هذه الحالة لا يكون الإطلاع على الأسرار الخاصة المخزنة في الحاسب مجردا وإنما لتحقيق غرض أوهدف معين وهو إفشاء تلك الأسرار.

يقوم بهذا السلوك إما الشخص المتاح له بحكم عمله الاطلاع على المعلومات والبيانات الخاصة السرية كموظف في مستشفى أو دائرة الأحوال المدنية أو محكمة، وهذا ما يسمى بإفشاء الأسرار المهنية هذا إذا كانت أسرارا خاصة في حين إذا كانت بيانات اسمية عموما لا تتصف بالسرية هنا نفرق بين سلوكي الاعتداء عليها أدناه فيما يتعلق بإفشاء الأسرار. ولا يفوتنا هنا أن نشير أن نصوص التجريم الحديثة لا تنطبق على هذه الحالة لأن جل القوانين تصدت لهته الجريمة بنصوص عقابية كافية وحددت من خلالها أركان الجريمة والتي لابد أن يكون الإفشاء من طرف موظف أو مستخدم..بينما ما نقصده الآن وهو من يتوصل إلى تلك المعلومات السرية الالكترونية بخبرته ودرايته بأنظمة المعلومات لتحقيق اختراقات أو

[1] سهيل محمد العزام، مرجع سابق، ص 101 و102.

[2] محمد مصطفى الشقيري، مرجع سابق، ص 286.

اتصالات بعدية أو مباشرة مع الحاسوب الموجودة به تلك الأسرار بحيث يتمكن من الاطلاع عليها وإفشائها.

ويمكن أن يشكل الحاسب الآلي وسيلة أكثر فعالية في نشر الأسرار بشمولية وتوسع كبيرين وبسرعة وكفاءة عاليتين، وذلك باستخدام قنوات الاتصال المتعددة التي تتيحها أنظمة الاتصالات المعلوماتية الحديثة، مع ظهور الانترنت بشكل خاص.

ثالثا: الابتزاز

ويمثل التهديد بالاستغلال غير المشروع للأسرار الشخصية، حيث يستغل الفاعل ما يتحصل عليه من معلومات الكترونية سرية وذات علاقة بالحياة الشخصية للأفراد في تحقيق منافع مادية أو معنوية، وذلك بتهديد صاحب الأسرار بإفشائها أو فضح أمرها في حال عدم تحقيق مطالبه، ولابد أن يكون لهذا الشخص القدرة على تنفيذ تهديداته[1].

رابعا: الاحتفاظ بنسخة

قد يتم التوصل إلى المعلومات السرية الالكترونية بكل سهولة ونسخها بسرعة فائقة، والخطورة تكمن هنا في إمكانية استخدام تلك المعلومات السرية الخاصة في المستقبل لتحقيق أغراض غير مشروعة.

فكل أشكال الاعتداء الواقعة على سرية الخصوصية المعلوماتية ترتكب بطبيعة الحال بوسائل تقنية معلوماتية سهلت وبشكل كبير في ذلك الأمر الذي يتطلب دراسة مختصرة عن هته الوسائل، والمتمثلة في عناصر النظم المعلوماتية.

الفصل الثاني
ماهية نظام المعالجة الآلية للمعطيات

يمثل نظام المعالجة الآلية للمعطيات المسالة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أية جريمة من جرائم الاعتداء على هذا النظام[2]، فإذا ثبت تخلف هذا الشرط الأولي لا يكون هناك مجال للبحث حول الجرائم الواقعة

[1] سهيل محمد العزام، مرجع سابق، ص 109.

[2] أطلق الفقهاء على النظام المعلوماتي اسم الحاسب الآلي، حيث أن لفظ الحاسب الآلي يعتبر قاصرا على جهاز الحاسب الآلي بمكوناته من شاشة العرض ولوحة المفاتيح ووحدة التشغيل، بينما أصبح في الوقت الحاضر يتصل بمكونات أخرى

عليه. ونشير هنا إلى أنه وكما سبق الذكر أن الاعتداء على المعلومات المعالجة بواسطة النظام المعلوماتي هي ما يسمى بالجرائم المعلوماتية وهي الطائفة التي تنتمي إليها الجرائم الواقعة على المعلومات السرية المعالجة بواسطة النظام المعلوماتي. ويؤدي توافر هذا الشرط إلى الانتقال إلى المرحلة التالية وهي بحث توافر أركان أية جريمة من الجرائم محل الدراسة، إذ أن هذا الشرط يعتبر عنصر لازما لكل منها، ولذلك يكون من الضروري تحديد مفهوم نظام المعالجة الآلية للمعطيات [1] .

ولإيضاح المقصود بنظام المعالجة الآلية للمعطيات يتعين علينا أن نتعرض لتعريف نظام المعلومات (المبحث الأول)، ثم لتعريف الحاسب الآلي باعتباره الأساس الذي يبنى عليه أي نظام معلوماتي أو اتصالي حديث(المبحث الثاني)[2]، وبعدها التطرق إلى تعريف الشبكة العنكبوتية الانترنت[3] (المبحث الثالث).

المبحث الأول
مفهوم نظام المعالجة الآلية للمعطيات

عبر المشرع الجزائري عن الجريمة المعلوماتية في القانون 04-15 بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات معبرا في ذلك عن النظام المعلوماتي بنظام المعالجة الآلية للمعطيات، ذلك أن هذه الأخيرة ترتكب بواسطة وعلى النظام المعلوماتي رغم أن محلها هو المعلومات، ولأن الأمر يتطلب ضرورة توضيح مفهوم النظام المعلوماتي كان لابد من

كالطابعات والماسحات الضوئية وشبكات المعلومات ويدخل ضمنه البرامج وقواعد البيانات، فأصبح يكون نظاما متكاملا دخل في مجالات حياتنا اليومية، أشار إليه أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص 19.

[1] أنظر في ذلك http://www.startimes.com يوم الاطلاع على الموقع 2015/06/21 .

[2] استخدم العديد من مشرعي دول العالم مصطلح نظام المعلومات مكان مصطلح الحاسب الآلي لذات السبب المذكور أعلاه.

[3] إن شبكة الإنترنت كشبكة معلوماتية تنطبق عليها النموذج المعروف بالمعلومات ذوالأبعاد الثلاثة وهي: أولا سرية المعلومات وذلك يعني ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات أو المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المحولين لذلك.
ثانيا: سلامة المعلومات يتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة علي أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المحولين لذلك.
ثالثا:وجود المعلومات وذلك يتمثل في عدم حذف المعلومات المخزنة علي أجهزة الحاسب إلا من قبل الأشخاص المحولين لذلك. إن جرائم الإنترنت ليست محصورة في هذا النموذج بل ظهرت جرائم لها صور أخري متعددة تختلف باختلاف الهدف المباشر في الجريمة، و إن أهم الأهداف المقصودة في تلك الجرائم هي كالآتي:
أ- المعلومات: يشمل ذلك سرقة أو تغيير أو حذف المعلومات، ويرتبط هذا الهدف بشكل مباشر بالنموذج الذي سبق ذكره.
ب- الأجهزة: ويتمثل ذلك تعطيلها أو تخريبها
ج- الأشخاص أو الجهات: تهدف فئة كبيرة من الجرائم علي شبكة الإنترنت أشخاص أوجهات بشكل مباشر كالتهديد والابتزاز.
علماً بأن الجرائم الذي تكون هدفها المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلي الأشخاص المعينة أو الجهات المعنية بتلك المعلومات أو الأجهزة، أشار إليه محمد الألفي،جرائم التجسس والإرهاب الالكتروني عبر الانترنت، منشور على الموقع الالكتروني http://www.mohamoon-montada.com.

التطرق لتعريفه (مطلب أول) ثم تحديد المقصود بالمعالجة الآلية للبيانات(مطلب ثاني) والتعرف على مكوناته (مطلب ثالث).

المطلب الأول
تعريف نظام المعالجة الآلية للمعطيات

يستعمل مصطلح النظام أو الأنظمة بصورة واسعة في لغة خطابنا اليومي وبأشكال ومضامين مختلفة، فنجد الكثير من الناس يستعملونه للتعبير عن أسلوب ونمط معيشتهم الاجتماعية، الاقتصادية والسياسية فيقال مثلا نظام التعليم، الكمبيوتر، الاقتصاد وغيرها، والملاحظ أن سعة انتشار هذا المصطلح يعود في الواقع إلى أن الإنسانية تعيش في عالم يتكون من عدد غير محدود من الأنظمة إذ أن هذا العصر هو عصر الأنظمة[1].

الحقيقة أن عملية معالجة المعطيات تحتاج إلى آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها، هذا ولّد الحاجة إلى إجراءات ووسائل تساعد على القيام بذلك فظهر مصطلح "نظم المعلومات" والتي تعرف أيضا أنها "مجموعة الإجراءات التي تقوم بتجميع ومعالجة وتخزين وتوزيع المعلومات بهدف دعم عمليات صنع القرار"، وفي نفس الوقت ظهر مصطلح نظام المعالجة الآلية باعتباره الوساطة التي أفرزتها عمليات الدمج بين كل وسائل الحوسبة والاتصال والوسائط المتعددة بما قدمته من قدرة على رقمنة الصوت والصورة وتحويلها إلى مادة تفاعل بين المستخدم وبين المحتوى[2]. وعلى الدمج بين النظام والمعالجة لابد من التطرق إلى تعريف النظام المعلوماتي من جهة (الفرع الأول) وتحديد المقصود بالمعالجة الآلية للبيانات من جهة أخر(الفرع الثاني).

الفرع الأول
تعريف النظام المعلوماتي

تتعددت التعريفات التي قيلت في النظام المعلوماتي بين الفقهية والتشريعية، سيتم التطرق إليها كالتالي:

أولا: التعريف الاصطلاحي للنظام المعلوماتي

فالنظام هو مصطلح مشتق من الكلمة اللاتينية "systema" ، التي تعني الكل المركب من عدد من الأجزاء ووفقا للمعجم الشامل فإن النظام هو عنصر مركب يتم تشكيله من عدة وحدات متميزة متصلة مع بعضها البعض بواسطة عدد من العلاقات، التي تنشأ لتحقيق التفاهم والترابط بين هده المكونات أو الوحدات المختلفة، وفي معجم" la rousse" في

[1] أنظر رشيدة بوبكر، مرجع سابق، ص 49.

[2] رشيدة بوبكر، مرجع سابق ، ص 50، مشار إليه لدى أيمن عبد الله فكري، جرائم نظم المعلومات، دراسة مقارنة، دار الجامعة الجديدة الاسكندرية، 2007، ص 224.

الجزء العاشر منه تم تعريف النظام بأنه يتحقق في مفهومين الأول "اعتبار النظام مجموعة من العناصر التي تمارس وظائفها من خلال علاقتها بطريقة مماثلة"، والثاني يقصد به م"جموعة الأوامر التي تتم بوسائل متعددة من أجل الحصول على نتائج محددة"[1]، وعرف أيضا أنه" مجموعة من العناصر أو الأجزاء المترابطة التي تعمل بتنسيق تام وتفاعل، تحكمها علاقات وآلية عمل معينة في نطاق محدد لتحقيق غايات مشتركة وهدف عام".[2]

وعرفه بعض الفقهاء أيضا" أنه مجموعة المكونات ذات علاقة متداخلة مع بعضها تعمل على نحو متكامل داخل حدود معينة لتحقيق هدف أو أهداف مشتركة في بيئة ما وفي سبيل ذلك يقبل مدخلات ويقوم بالعمليات وينتج مخرجات ويسمح باستقبال مدخلات مرتدة"[3]، وكان هذا التعريف على أساس أن النظام يختلف باختلاف المجال الذي ينتمي إليه.

ثانيا: التعريف القانوني للنظام المعلوماتي

لم يعرف المشرع الفرنسي النظام المعلوماتي، في حين اقترح مجلس الشيوخ الفرنسي مفهوم لنظام المعالجة الآلية للمعطيات بمناسبة تعديل قانون العقوبات هو:" أنه كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها تتحقق نتيجة معينة وهي معالجة المعطيات، وعليه يكون هذا المركب خاضع لنظام الحماية الفنية"[4].

وتجدر الإشارة أن القانون الفرنسي المسمى بقانون "قودفران" LOI GODFRAIN[5] نسبة إلى أحد نواب البرلمان الفرنسي المسمى بقودفران الذي عدل بصفة نهائية نظرة المشرع الفرنسي حول اعتبار الأنظمة المعلوماتية عبارة عن مال في حد ذاته، ولابد على قانون العقوبات أن يحميه من المساسات غير المشروعة[6].

وعرفته نص المادة الأولى من الفصل الأول تحت تسمية المصطلحات من اتفاقية بودابست كالتالي:" كل آلة سواء بمفردها أو مجموعة عناصر أخرى، تنفيذا لبرنامج معين، بأداء معالجة آلية للبيانات"، ومنه يعتبر نظام المعلومات جهاز يتكون من معدات وبرامج

---

[1] رشيدة بوبكر، مرجع سابق ، ص 49-50 .

[2] صليحة علي صداقة، الأبعاد القانوني والأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية، الإسكندرية، 2017، ص 23.

[3] طارق طه، مقدمة في نظم المعلومات الإدارية والحاسبات الآلية، الطبعة الثالثة، منشأة المعارف الإسكندرية، 2000، ص 16.

[4] Houande Alain . .LINANT de Bellefant Xavier, Pratique du droit de l'informatique , edition Delmas (5eédition) avril 2002, (France) p . 250.

[5] القانون رقم 575/2004 لجوان 2004 المتعلق بالثقة في الاقتصاد المعلوماتي، المتمم في 11 جويلية 2010 الفصل الثاني من الباب الأول تحت عنوان "حرية الاتصال في الشبكة"، الفصل الثاني من الباب الثالث من هذا القانون تحت عنوان " مكافحة الاجرام المعلوماتي" الجريدة الرسمية رقم 143 المؤرخة في 24 جوان 2004.

[6] Lucas André , jean devréze, jean frayssinet, Droit de l'informatique et l'internet ,éditions dalloz,collection thémis (droit privé) 2001 (France), p. 679- 680.

قائمة للمعالجة الآلية للبيانات الرقمية ويمكن أن تشتمل على طرق سهلة لإدخال واستخراج وتخزين البيانات، ويمكن أن تكون منفردة أو متصلة مع أجهزة مماثلة أخرى داخل شبكة[1].

وعرفته الاتفاقية العربية[2] لمكافحة جرائم تقنية المعلومات لسنة 2012 في الفصل الأول منها في المادة الثانية في تعريفها لبعض المصطلحات أنه" النظام المعلوماتي: مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات". ومهما كان أسلوب معالجتها للمعطيات فإنها تشكل نظام معلوماتي[3].

ويقصد أيضا بنظم الحاسب الآلي كل مكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، الأشخاص والتي يمكن بواسطتها تحقيق وظيفة أوهدف محدد[4]، ويعرف أيضا أنه" هوالنظام الذي يحتوي على معلومات آلية تقنية مسماة محمية بإجراء أمني"[5].

كما أورد قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية في مادته الثانية تعريفا للنظام المعلوماتي باعتباره" النظام الذي يستخدم لإنشاء رسائل البيانات وإرسالها واستلامها أو تخزينها أو لتجهيزها على أي وجه آخر"[6].

وعرفه المشرع الجزائري[7] بموجب الفقرة ب من المادة 2 من القانون رقم 04/09 لسنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنه " أي نظام منفصل أومجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

---

[1] كما عرفت المذكرة التفسيرية لاتفاقية بوادبست المعالجة الآلية على أنها:" تعني مجموعة من العمليات التي تطبق على البيانات من خلال برنامج معلوماتي".

[2] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2012 عن الموقع الالكتروني
. http://www.lawjo.net/vb/showthread.php?26439

[3] Hollande Alain, op. cit, page 250.

[4] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر الإسكندرية، 2004، ص 56.

[5] Guillaume Champy, La fraude informatique, tome 1, Presses Universitaires d Aix-Marseille, 1992, p. 88 .

[6] قانون الاونيسرال كان بموجب القرار الذي اتخذته الجمعية العامة للأمم المتحدة بناء على تقرير اللجنة السادسة (A/51) 628.

[7] عرفه قانون سلطنة عمان رقم 69 لسنة 2008 بشأن المعاملات الالكترونية في المادة الأولى المخصصة للتعريفات:" النظام المعلوماتي نظام إلكتروني للتعامل مع المعلومات والبيانات بإجراء معالجة تلقائية لها لإنشاء أو إرسال أو تسلم أو تخزين أو عرض أو برمجة أو تحليل تلك المعلومات والبيانات." كما عرف نظام جرائم المعلوماتية للمملكة العربية السعودية الصادر في 2008 بأن " مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية." وفي نفس السياق عرف قانون دبي للمعاملات الالكترونية رقم 2 لسنة 2002 أنه " نظام إلكتروني لإنشاء أو استخراج أو إرسال أو استلام أو تخزين أو عرض أو معالجة المعلومات أو الرسائل إلكترونيا."، وكذلك الشأن بالنسبة لمشرعين كثر والجدير بالذكر أن قانون التوقيع الالكتروني المصري رقم 15 لسنة 2004 صدر خاليا من تعريف للنظام المعلوماتي، مشار إليه لدى خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009 ، ص 22-21.

أما المشرع الفرنسي، فلم يتطرق لتحديد مفهوم نظام المعالجة الآلية للمعلومات[1] موكلا مهمة ذلك إلى الفقه والقضاء، حيث عرفه الفقه الفرنسي أنه"كل مركب يتكون من وحدة أو مجموعة وحدات معالجة تتكون كل من منها من الذاكرة البرامج و المصطلحات و أجهزة الربط و التي يربط بينها مجموعة من العلاقات عن طريقها تحقق نتيجة معينة و هما معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية[2].

ومما سبق نستنتج أنه هناك من يأخذ بالمفهوم الموسع للنظام والعكس وفي الحقيقة ويمكن القول أن نظام المعالجة الآلية للمعطيات هو تعبير يخضع للتطور السريع الذي يلحق بالبيئة الرقمية .

الفرع الثاني
مفهوم المعالجة الالكترونية للبيانات

المعالجة بصفة عامة هي تحويل شيء ما من صورته الطبيعية إلى صورة أخرى تعبر عن نتيجة ما يمكن الاستفادة منها،أي أن عملية المعالجة هي تحويل أي شيء من شكله الخام إلى شكل جديد يستفاد منه، أي أن المعالجة الإلكترونية هي عبارة عن معالجة بواسطة أجهزة إلكترونية وهذه الأجهزة بها يقصد على العموم الحاسوب لأنه مكون من عدة أجهزة تعمل كلها بواسطة شرائح إلكترونية، وهذه الشرائح الإلكترونية هي المتحكم في كل عمليات المعالجة وبالتالي فهي معالجة إلكترونية[3]، وللتفصيل أكثر سيتم تحديد المقصود بالمعالجة والمعالجة الآلية (أولا)، وفقا لفكرة أساسية للحاسب الآلي (ثانيا).

أولا: المقصود بالمعالجة والمعالجة الآلية للبيانات

[1] في الحديث عن نظم المعلومات هناك أيضا مصطلح آخر تردد في العديد من المراجع محل الدراسة، وهو مصطلح قواعد البيانات فما المقصود منه؟ قواعد البيانات هو نظام معالجة تخزيني يحتاج إلى الارتباط بنظام معالجة استردادي يتخذ طبيعته أو شكله بحسب أسلوب إنشائه، مع العلم أنها تعرف من الناحية الفقهية أنها مجموعة مهيكلة من التسجيلات النصية أو غير النصية متاحة للقراءة آليا عبر خط مباشر مرتبط بخادم ملقم، عن عمر محمد أبو بكر بن يونس، رسالة دكتوراه، جامعة عين شمس القاهرة، 2004، ص 346، والأمر ذاته بالنسبة لمصطلح بنوك المعلومات، فما المقصود بها؟ عرفها الدكتور ربحي مصطفى عليان على أنها :" مجموعة ملفات ضخمة من المعلومات بكافة أشكالها وصورها مختزنة ومحتفظ بها بشكل يسهل التعامل معها والبحث عنها بواسطة الحاسوب"، عن .http://www.alyaseer.net/، والجدير بالذكر أن بنك المعلومات هو نتيجة دمج مجموعة قواعد بيانات ترتبط فيما بينها بعلاقات تكاملية تخصصية محددة الهدف والوظيفة، وفق منظومة منسجمة، أشار إليه حسين الإبراهيم مقال منشور على الموقع الالكتروني ./http://infomag.news.sy

[2] http://www.droit-dz.com/forum/showthread.php?t=5955 يوم الاطلاع على الموقع 2016/3012.

[3] أنظر في ذلك،

https://faculty.psau.edu.sa/filedownload/doc-13-ppt-03f84bb247bf032f7a7d94d5852caec7-original.ppt، تاريخ الاطلاع على الموقع 2017/05/07.

يمكن للحاسب الآلي القيام بالمعالجة الالكترونية للبيانات، ولكن بشرط وجود خطوات المعالجة أي وجود برنامج المعالجة وهذا البرنامج هو عبارة عن خطوات متسلسلة كتبت بأسلوب يفهمه الحاسوب وزود بها الحاسوب بطريقة ما كي يقوم بتطبيقها كلما دعت الحاجة[1] .

آ- المقصود بالمعالجة:

المعالجة بصفة عامة هي تحويل شيء ما من صورته الطبيعية إلى صورة أخرى، تعبر عن نتيجة ما يمكن الاستفادة منها فمعالجة الحديد الخام يمكن أن تعطينا أشكال عديدة من معدات حديدية ومعالجة بعض الأرقام قد تعطينا إجمالي المصروفات أوالربح وهكذا وبعبارة أخرى إن عملية المعالجة هوتحويل أي شيء من شكله الخام إلى شكل جديد يستفاد منه في حياتنا بشكل عام. ويعنى بكلمة آلية أي بدون تدخل بشري مباشر[2]. كما تعني المعالجة عملية تحويل البيانات من شكل إلى آخر[3] .

ب- المقصود بالمعالجة الإلكترونية للبيانات :

المعالجة الالكترونية هي ليست معالجة يدوية أو ميكانيكية أو حرارية، بل هي وبكل بساطة عبارة عن معالجة بواسطة أجهزة الكترونية ومن هذه الأجهزة هي الحاسوب لأنه مكون من عدة أجهزة تعمل كلها بواسطة شرائح الكترونية وهذه الشرائح الالكترونية هي المتحكم في كل عمليات المعالجة وبالتالي فهي معالجة الكترونية.

والمعالجة الآلية للمعطيات وفق ما هو متعارف عليه في المجال التقني "مجموعة من العمليات المترابطة والمتسلسلة بدءا من جمع المعطيات وإدخالها إلى نظام المعالجة الآلية ومعالجتها وفقا للبرامج التي تعمل به نظم المعالجة الآلية وصولا إلى تحليلها وإخراجها بصورة معلومات".[4]

وعرف القانون الفرنسي[5] رقم 17/78 من خلال المادة 5 منه عملية المعالجة الآلية أنها "عبارة عن مجموعة من العمليات التي تتم آليا، وتتعلق بالتجميع والتسجيل والإعداد والتعديل والاسترجاع والاحتفاظ ومحو المعلومات ومجموعة العمليات التي تتم آليا بغرض استغلال المعلومات وخصوصا عمليات الربط والتقريب وانتقال المعلومات ودمجها مع بيانات أخرى أو تحليلها للحصول على معلومات ذات دلالة خاصة".

---

[1] أنظر في ذلك الموقع الالكتروني، http://www.mprog.org/Ccomp1.htm ، يوم الاطلاع عليه 2017/05/08.

[2] المادة الأولى من الفصل الأول – المصطلحات- من اتفاقية بودابست السالفة الذكر.

[3] http://www.vercon.sci.eg/Matrials/1_4.html يوم الاطلاع على الموقع 2016/12/30.

[4] رشيدة بوكر، مرجع سابق، ص 52 هامش رقم 03.

[5] القانون رقم 17/78 المؤرخ في 16 جانفي 1978 المتعلق بالحريات والمعلوماتية المعدل بموجب القانون رقم 2004/801 المؤرخ في 6 أوت 2004 الخاص بالمعالجة الآلية للمعلومات الرقمية .

أما عن المقصود بمعالجة المعطيات فهي مجموعة العمليات التي تحوّل المعطيات إلى معلومات، حيث إن المعطيات أو البيانات هي مجموعة الحقائق الأولية والأشكال التي عادة ما تكون غير منظمة أو معالجة؛ في حين أن المعلومات هي البيانات المعالجة[1].

وفي إطار المادة الأولى من اتفاقية بودابست من الفصل الأول يقصد بمعالجة البيانات هي مجموعة عمليات تطبق على بيانات ويتم تسجيلها عن طريق تنفيذ برنامج المعلوماتية[2].

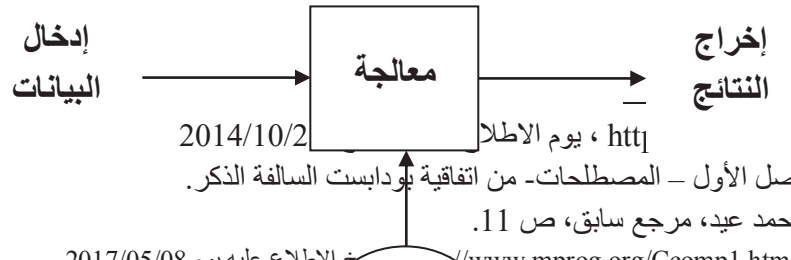
تأسيسا على ما سبق فإن المعلومة الخام هي البيانات ويمكن أن تقدم تحت أشكال مختلفة كالأرقام والكتابات المجمعة والرموز والإحصائيات الخام، وأن كل معلومة ليست بيان ولكن كل بيان هو معلومة[3]، ومنه يعتبر صوت الإنسان بيانات وضغط دمه بيانات وقوة الرياح بيانات وكثافة الضباب بيانات والضحك بيانات وغيرها وقد سبق التفصيل في مدلول البيانات أعلاه.

ثانيا: المقصود بفكرة عمل الحاسوب

تتلخص فكرة عمل الحاسوب، في كونه جهاز لديه القدرة على المعالجة وذلك من خلال الشرائح الالكترونية التي حاول صانعيها أن يقلدوا فيها عمل الدماغ البشري وكيفية معالجته لأمور الدنيا بشكل عام.

من ذلك يمكننا أن نقول أن الحاسوب يمكنه القيام بالمعالجة ولكن بشرط وجود خطوات المعالجة أي وجود برنامج المعالجة وهذا البرنامج هو عبارة عن خطوات متسلسلة كتبت بأسلوب يفهمه الحاسوب، وزود بها هذا الأخير بطريقة تقنية يقوم بتطبيقها كلما دعت الحاجة، حيث تمثل البرامج الكيان المعنوي إضافة إلى المعطيات[4].

جهاز الحاسوب هو عبارة عن جهاز له القدرة على المعالجة وهي أهم ميزة يمتلكها، ولكي تنجح عملية المعالجة يجب تزويد الحاسوب بالبرنامج ولكون المعالجة ستتم على بيانات ما، فانه يجب أن يتم إدخال هذه البيانات إلى الحاسوب وسيقوم بمعالجتها وفقا للبرنامج المستخدم، وفي النهاية سيقوم الحاسوب بإخراج المعلومات أو النتائج التي تحصل عليها كحصيلة نهائية للمعالجة[5].



[1] / imes.com :htt ، يوم الاطلا 2014/10/2

[2] المادة الأولى من الفصل الأول – المصطلحات- من اتفاقية بودابست السالفة الذكر.

[3] رشدي محمد علي محمد عيد، مرجع سابق، ص 11.

[4] أنظر الموقع الالكتروني www.mprog.org/Ccomp1.htm// خ الاطلاع عليه يوم 2017/05/08.

[5] كما سبقت الإشارة أن الهواتف الذكية التي تعتبر بم ا القدرة على المعالجة الآلية للبيانات والمعلومات التي تتضمنها تلك الهواتف قد تتعرض لنفس الأخطار التي سيب أو تتناقلها بواسطة الشبكة المعلوماتية، حيث أن الهواتف الذكية أيضا ترتبط بالشبكة المعلوماتية كما هو الحال بالنسبة للحواسيب فهي تعتبر كالحاسوب ، لهذا سبق وأشرنا أننا تفاديا للتكرار سنحاول الاقتصار على الحاسوب في بعض محطات هذه الدراسة.

المطلب الثاني
مكونات نظام المعالجة الآلية للمعطيات[1]

ولمزيد من التوضيح سنعرض في هذا المطلب لمكونات النظام المعلوماتي[2] حيث أنه يتكون من ثلاث عناصر أومكونات رئيسية هي كالتالي[3]:

1 – مدخلات: وهي البيانات التي تغدي بها النظام، فجميع أنواع البيانات وبعض المعلومات المسترجعة أحيانا، توضع في نظام الحاسوب من خلال وسائل إدخال مناسبة، وفي مقدمتها لوحة المفاتيح والفأرة والماسح الضوئي.

2 – مخرجات: وهي المعلومات التي تنتج عن النظام، وهنا ينبغي أن تنتقل البيانات والمعلومات المعالجة من وحدة المعالجة المركزية إلى وسيلة إخراج مناسبة للمعلومات، مثل شاشة الحاسوب أو وسيلة إخراج مناسبة أخرى.

3 - تشغيل وتحليل: وهي الطرق والوسائل المختلفة، لتشغيل المدخلات حتى يمكن التوصل إلى المخرجات ويطلق على عملية التحليل والتشغيل اسم **"المعالجة".**

والحقيقة أن وجود نظام المعالجة الآلية للمعطيات هو شرط أساسي لكي نبحث ما إذا كان هناك اعتداء على نظام المعالجة الآلية من عدمه، وبالنظر إلى أهمية المعلومات المعالجة آليا وقيمتها فقد اعتبرت مالا بل وتفوق المال في قيمتها وبالتالي جرم الاعتداء عليها[4].

فكما يعتبر وجود النظام المعلوماتي شرط أولي في الجرائم المعلوماتية، فهل يعتبر أيضا إخضاعه للحماية الفنية شرط أساسي أم لا؟. و هذا ما سيتم التفصيل فيه من حيث التطرق إلى أهمية إخضاع نظام المعالجة الآلية للمعطيات للحماية الفنية.

---

[1] بالنسبة لمكونات النظام المعلوماتي من وجهة نظرنا أنه اختلفت الآراء بشأن المكونات الأساسية لهدا النظام. راجع المكونات الأساسية للنظام المعلوماتي خالد ممدوح إبراهيم، مرجع سابق، الصفحة 24 وما يليها.

[2] المقصود هو النظام المعلوماتي للحاسوب والأمر ذاته بالنسبة لمكونات النظام المعلوماتي للهاتف الذكي.

[3] عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات دراسة مقارنة، دار النهضة العربية القاهرة، 2000، ص 39، كذلك أنظر صليحة علي صداقة، مرجع سابق، ص 25.

[4] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار النهضة العربية الإسكندرية، 2009، ص 66.

المبحث الثاني
أهمية إخضاع نظام المعالجة الآلية للحماية الفنية

بمناسبة دراسة الحماية الجزائية للمعلومات الالكترونية السرية أو ما تم التعبير عنه بالأسرار المعلوماتية، والتي يتم معالجتها بواسطة النظام المعلوماتي من جهة، و من خلال هذه الدراسة لطالما تم طرح سؤال مضمونه هل يشترط إخضاع نظام المعالجة الآلية للبيانات للحماية الفنية من عدمه ليحظى بالحماية القانونية؟

بعبارة أخرى هل من الضروري حتى يحمي القانون البيانات السرية المعالجة آليا داخل النظام المعلوماتي أن يكون المسؤول عنه قد عني بتأمين ذلك النظام، بأن يخضعه لحماية فنية أولا يشترط دلك؟ ومنه فأي نظام معلوماتي فهو محل حماية قانونية رغم عدم تأمينه فنيا.

للإجابة على هذا التساؤل سنتعرض لبض الآراء الفقهية أحدهم يذهب إلى ضرورة تأمين النظام العلوماتي ليحظى بالحماية الفنية (مطلب أول) وآخر يرى العكس(مطلب ثان).

المطلب الأول
الاتجاه المقيد للحماية الفنية

يذهب رأي إلى ضرورة وجود نظام أمني، ذلك أن القانون يجرم الاعتداء على نظم الأمن المتضمنة في النظام المعلوماتي ويستند أنصار هذا الرأي لعدة حجج منها إن الاعتداء على النظام الأمني – شرط مفترض – لقيام الجرائم التي تتعلق بالمعلوماتية، والعدالة تقتضي عدم العقاب على فعل يعد اعتداء على حق لم يتحوط له صاحبه فضلا عن أن التسليم برأي غالبية الفقه يعني توسعا في مجال التجريم، فكل دخول غير مشروع جريمة وذلك أمر غير منطقي[1].

فيرى أصحاب هذا الاتجاه ضرورة قصر الحماية الجنائية على تلك الأنظمة التي وفر لها أصحابها حماية فنية فحسب، ويستندون في تبرير رأيهم هذا إلى الحجج الآتية:

* أن المنطق السليم والعدالة، يقتضيان قصر الحماية الجنائية على الأنظمة المحمية بأنظمة أمان فحسب ذلك لأن القانون الجنائي لا يساعد إلا الأشخاص المجتهدين، ومن غير المعقول حماية معلومات هامة تركها المسؤولون عنها دون أية إجراءات تكفل لها الحماية، ولا ينبغي حماية حق لم يتحوط له صاحبه، وهذا يجعل الأشخاص لا يلجأون إلى القانون الجنائي إلا عندما تعجز تلك التدابير الوقائية عن حماية أنظمتهم.

[1] - خثير مسعود، مرجع سابق، ص 112.

وقد قاس أصحاب هذا الرأي جريمة الدخول غير المصرح به على جريمة انتهاك حرمة المسكن حيث أن هذه الأخيرة لا تقوم بمجرد دخول المسكن بغير رضا صاحبه، وإنما يجب لقيامها أن يصحب ذلك الدخول استعمال وسائل تدل على عدم رضا صاحب المسكن، كالتهديد أو الاحتيال[1].

*ومن جهة أخرى أن أنظمة الحاسبات تتميز بالانفتاح على الخارج عبر شبكات المعلومات، هذه المعلومات قد تكون من الأهمية بحيث يصبح من الواجب حمايتها، وإلا أصبح الدخول إليها سهلا، فهذه الأنظمة لها القابلية للتعرض لهجومات ولهذا وجبت حمايتها[2].

*إن القانون المعلوماتية والحريات الفرنسي الصادر في 6 جانفي1978 يعتبر سابقة تشريعية مهمة في هذا الشأن، إذ يفرض هذا القانون على مالك النظام أو المسؤول عنه التزاما بتأمين هذا النظام وذلك وفقا للمادة 29. وكذلك المادة 226 فقرة 17 من قانون العقوبات تعاقب على كل إجراء أو معالجة آلية لمعلومات اسمية دون اتخاذ الإجراءات اللازمة لتأمين هذه المعلومات، ولا ينبغي حصر هذا الأمر في المعطيات الشخصية، وإنما يجب أن يشمل كل المعطيات بما فيها تلك التي تحميها المادة 323-1 من قانون العقوبات الفرنسي، فلا تحظى بالحماية منها إلا تلك المعطيات المحمية بأجهزة أمان.

إن إقامة الدليل على قيام الركن المادي للجريمة والتحقق من توافر القصد الجنائي لدى فاعلها يتطلب وجود أنظمة الأمان، فاختراق هذه الخيرة يسهل عملية الكشف عن الجريمة لأنه يترك في العادة أثرا يدل عليه، كما أن هذا الاختراق يساعد على التحقق من وجود القصد الجنائي لدى الفاعل، وعليه فإن التفسير السليم لنص تجريم الدخول غير المصرح به، يقتضي قصره على اختراق الأنظمة المحمية دون سواها، فبينما يتطلب فعل الدخول اختراق الأنظمة الأمنية التي تحمي النظام فإن فعل البقاء لا يتطلب ذلك، لأن الدخول كان مشروعا[3].

إن اشتراط النص بأن يكون الفعل قد تم عن طريق الغش وهو شرط يتصل بمجريات الجريمة لأن فعل الدخول في حد ذاته، هو أسلوب محايد لا يدل بنفسه على عدم المشروعية ولم يجد المشرع أبدا من اشتراط الغش وهو الذي يتحقق باختراق نظم الأمان[4].

المطلب الثاني
الإتجاه الموسع للحماية الجنائية

[1] - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي ، دار الجامعة الجديدة للنشر الإسكندرية، بدون طبعة، 2007 ، ص 134.

[2] - محمد خليفة، المرجع نفسه ، ص134.

[3] - محمد خليفة، ، مرجع سابق ، ص 135.

[4] - محمد خليفة، المرجع نفسه ، ص 136.

ورأي آخر يقضي بعدم ضرورة وجود الحماية الفنية رغم قوة حجج المنادين بتضييق الحماية الجنائية وحصرها في الأنظمة المحمية فقط فإن هناك اتجاه آخر يرى بأن أنظمة الحاسبات الآلية وما تحويه من المعطيات لابد أن تحظى بالحماية بغض النظر عن احتوائها على أنظمة الأمان أو عدم إحتوائها.

ويرد أن سكوت القانون يدل على عدم اشتراطه لهذا الأمر، ومن المعروف أن المبادئ العامة في تفسير القانون الجنائي تقتضي عدم إضافة شرط لم ينص عليه القانون، فالنص جاء عاما ولم يفرق بين نظام محمي وآخر غير محمي.

إن الأخذ بفكرة نظام الأمان يضعنا أمام مشكل عويص الحل، وهو تحديد متى يصلح نظام ما لأن يكون نظام أمان؟ وما هو الحد الأدنى من الأمان ؟ أي كيف نحدد نوع الأمان وكمه ؟.

هذا وقد كان القضاء الفرنسي واضحا في عدم أخذه بالشرط المتقدم، وتأكد ذلك في حكم لمحكمة استئناف باريس صدر سنة 1994 ، بين أنه ليس من اللازم لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تم بمخالفة تدابير أمنية، وأنه يكفي لقيام الجريمة أن يكون الدخول قد تم ضد إرادة المسؤول عن النظام[1].كما ان الاجتهاد القضائي الفرنسي يعتبر أن جريمة الدخول تتحقق حتى في غياب الحماية الفنية[2].

وفي حكم أخر ذهبت إليه محكمة استئناف باريس أدانت المتهم في قضية " bluetouf" حيث قام القرصان بإختراق نظام معلوماتي لوكالة الوطنية لأمن الصحة و التغذية و البيئة والعمل و سرقة الملفات بالرغم من أن دخول النظام لم يكن محميا.[3]

---

[1]Dans une **décision du 5 Avril 1994, la cour d'appel de Paris** a précisé que : « pour être punissable, cet accés ou ce maintien doit etre fait sans droit et en pleine connaissance de cause, étant précisé à cet égard qu'il n'est pas nécessaire pour que l'infraction existe que l'accès soit limité par un dispositif de protection….. ».

De plus, dans un arrêt du 3 octobre 2007, la Cour de Cassation estime que « Doit être censuré l'arrêt qui relaxe un prévenu du chef de maintien frauduleux dans un système de traitement automatisé de données alors qu'il relève que celui-ci, quand bien même il y aurait accédé régulièrement, a utilisé pendant plus de deux ans, et avec un code qui ne lui avait été remis que pour une période d'essai, une base de données qui n'était accessible qu'aux personnes autorisées. » **Murielle CAHEN** , Intrusion dans un systeme informatique , Avocat on ligne , Sur le site suivant ; www.murielle-cahen.com

[2]- **Valérie SEDALLIAN** ; Légiférer sur la sécurité informatique : la quadrature du cercle? 5décembre 2003, P11 sur le site www.juriscom.net

[3] Dans l'affaire **Bluetouff,** un pirate s'était introduit dans les systemes informatiques de l'ANSES(l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail). Après une première décision de relax(TGI Créteil, 23 avril 2013) des fait

والوضع في قانون العقوبات الجزائري مشابه للوضع في قانون العقوبات الفرنسي، إذ لم تشر المادة 394 مكرر إلى ضرورة أن يكون نظام المعالجة الآلية للمعطيات محميا بجهاز أمان، وإنما جاء النص عاما، وعليه فإن جميع الأنظمة سواء كانت محمية أوغير محمية تحظى بحماية هذا القانون.

إلا أنه وكما يذهب الرأي الأول أن المسألة واضحة ولا تحتاج إلى تفسير، ذلك لأن النصوص المتعلقة بجرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات صدرت دون أن تتضمن شرط الحماية فنية، والمبادئ المستقرة في القانون الجنائي أنه لا يجوز تقييد النص المطلق أو تخصيص النص العام طالما لم ينص المشرع على ذلك، سيما إن عدم ذكر شرط الحماية الفنية يعني أن المشرع قد أراد استبعاد هذا الشرط صراحة.

كما أن المناقشة البرلمانية تؤكد أنها كانت ضد اشتراط هذه الحماية، وحتى ولو ورد ذكر النص على هذه الحماية كشرط ضمن الأعمال التحضيرية للقانون، فإنه لا يكتسب أهمية لعدم إلزامية هذه الأعمال التحضيرية وإنما يستعان بها في تفسير ما غمض من النصوص أو تعارض مع بعضه البعض. وتطبيقا لذلك فإنه يمكن القول أنه لا يشترط لوجود الجريمة أن يكون الدخول إلى النظام مقيدا بوجود حماية فنية[1].

و كذلك يذهب أنصار هذا الرأي في الفقه الفرنسي دائما وفي تعزيز وجهة نظرهم إلى قياس جريمة الدخول غير المشروع على جريمة السرقة، بحيث أن المال يتمتع بالحماية الجنائية من السرقة سواء كان في حماية صاحبه أو لم يكن، فالجريمة تمت بغض النظر عن الصعوبة التي يتلقاها الجاني، وأنه لا يمكن للجاني أن يدفع بعدم تحوط صاحب المال فتمت سرقته.[2]

وبناء على ما تقدم فإن نظام الحماية الفنية لا يدخل عنصرا في جرائم المعطيات، فهذه الأخيرة تقوم بالاعتداء على نظام المعالجة الآلية للمعطيات سواء كان محميا بنظام للأمان، أم لم يكن محميا فالحماية الجنائية إذا عامة على كل الأنظمة[3].

وإضافة إلى هذه النتيجة، يقال أن الوقاية خير من العلاج وبالتالي نحن نرى أنه لابد من الحماية الفنية رغم أن المشرع لم يشترطها[1]، لأنه كما توضع الأوراق التي تحمل أسرار في

---

d'accès frauduleux à un STAD (systèmes de traitement automatisé de donnée) le prévenu est au contraire condamné en appel(Cour d'Appel de Paris, 5février 2014) pour maintien frauduleux dans un système automatisé de donnée et vol de fichiers, même si leur accès n'était pas protégé.

ZICRY Laure, Enjeux et maitrise des cyber risque, éd LARGUS de l'assurance, France, 2014,P 63

[1] - خثير مسعود، مرجع سابق، ص 112-113.

[2] أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة للنشر الأسكندرية ، بدون طبعة، 2007، ص 333 ، كذلك أنظر رشيدة بوكر، مرجع سابق، ص 168.

[3] - محمد خليفة، مرجع سابق ، ص 137-138.

خزانة ويقفل عليها بإحكام فإنه في المقابل لابد من تأمين النظام المعلوماتي للحفاظ على الأسرار الموجودة بداخله لأنه ليس من المعقول أن تخزن فيه أسرار من دون حماية فنية تحميها.

و باعتبار أن مجال الدراسة يتعلق أساسا بالجرائم المعلوماتية الماسة بالسرية، كان لابد من التعرف على وسائل ارتكاب الجريمة وتم التطرق للوسيلة الأكثر استخداما وتسهيلا لارتكابها، وهي الحاسوب(المبحث الأول) والانترنت (المبحث الثاني).

المبحث الثالث

مـــــــــــاهية الحاسب الآلي

يعتبر الحاسب الآلي من أبدع ما ابتكره عقل الإنسان على مدى الأزمان، هذه الآلة الصغيرة التي ارتبطت بها معظم نشاطات الإنسان وباتت تقدم له خدمات هائلة، كانت تتطلب منه في الماضي الكثير من الجهد والمال والوقت وأصبح من غير الممكن أن يستغني الإنسان عنها في مجالات شتى بالنظر للخدمات الكبيرة التي تقدمها له هذه الآلة، وهو في نفس الوقت وعلى وجه الخصوص الأساس الذي يبنى عليه أي نظام معلوماتي.

المطلب الأول

تعريف الحاسب الآلي[2]

لم يتفق الباحثون في مجال تسمية وتعريف الحاسب الآلي، هذا الجهاز الذي يتولى معالجة المعلومات بشكل آلي وقد جرت العادة على إطلاق اسم الحاسب الآلي أو الحاسب الالكتروني على ذلك الجهاز الذي أصبح ضرورة عصرية، وهناك من يسميه أيضا بالعقل الالكتروني رغم أن هذه التسمية الكثير من لا يوافق عليها على أساس أن المدلول الظاهر لهذه الأخيرة لا يعبر عن مضمونها الحقيقي، فلا يمكن أن تستوي آلة أو مكانة مع ما يتميز به العقل البشري، إذ أنه من سماته التخيل والابتكار والتفكير وتلك الآلة لا يمكن أن تقوم بما يقوم به العقل البشري فهي لا تبتكر لأنها في حد ذاتها ابتكار لهذا لا يمكن وصفها بالعقل الالكتروني، وتتعلق دراسة جرائم المعلوماتية أو جرائم الحاسب الآلي بالتقنية الفنية والتكنولوجية لعمل الحاسب الآلي[3].

---

[1] وجود الحماية الفنية يثبت أركان الجريمة حيث أن مخترق النظام المحمي يعني أن إرادته كانت متجهة إلى الدخول غير المصرح به أما في حالة انتفاء الحماية فإن دلك يصعب إثباته.

[2] - تعريف الكمبيوتر لغة: من حسبها فالحسب العد وما عد، والحساب والحسابة عدك الشيء وحسب الشيء يحسبه، عن خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، دار الهدى للطباعة والنشر والتوزيع عين مليلة الجزائر، 2010 ، ص 21 .

[3] - محمد عبد الله أبوبكر سلامة، جرائم الكمبيوتر والانترنت، منشأة المعارف بالإسكندرية، 2006، ص 23.

وقد بنيت الحاسبات الآلية على فكرة تقليد النماذج بطريقة الكترونية، تتعامل بالرموز والمعالجة الرياضية حيث فكر الإنسان بأنه عندما يقوم بإجراء عملية حسابية، فإنه يلزمه ورقة وقلم (أي طريقة لإدخال وكتابة البيانات) والتي يقابلها في الحاسب الآلي وحدة للمدخلات على ورقة أي وحدة تخزينية (ذاكرة)، ثم تتم عملية معالجة البيانات حسابيا (وحدة حسابية ومنطقية)، للحصول على النتيجة مسجلة على هذه الورقة (وحدة المخرجات)[1].

فيتكون الحاسب الآلي من العديد من المكونات اصطلح تسميتها بنظم الحاسوب الآلي، منها ما هومادي ومنها ما هو معنوي أو منطقي، ومنها شبكات الاتصالات الخاصة بالحاسب الآلي بالإضافة إلى الأشخاص حيث يمكن بواسطة كل هذه المكونات تحقيق العديد من الوظائف والأهداف المحددة للحاسب الآلي[2].

إن السبب في اختلاف التسميات التي أطلقت على الجهاز الآلي لمعالجة المعلومات يعود إلى الترجمة للكلمات التي تدل على ذلك في اللغات الأجنبية وعلى وجه الخصوص في اللغتين الفرنسية والانكليزية التي نقلت عنها تسميت الحاسب الآلي إلى اللغة العربية.

ففي اللغة الانكليزية يسمى computer، والفرنسية ordinateur[3] أما كلمة informatique فتعني باللغة العربية المعالجة الآلية للمعلومات بالحاسب الآلي.

كما قد اختلف الباحثين في التسمية اختلفوا أيضا في التعريف، فقد عرف بعض الباحثين الحاسب الآلي على أنه :" مجموعة متداخلة من الأجزاء لديها هدف مشترك من خلال أداء التعليمات المخزنة "[4].

ويعرف أيضا أنه "مجموعة متكاملة من الأجهزة التي تعمل مع بعضها البعض بهدف تشغيل مجموعة البيانات الداخلية طبقا لبرنامج تم وضعه مسبقا للحصول على نتائج معينة". ويعرف بأنه" آلة تقوم بمعالجة المعطيات أوالبيانات طبقا لمجموعة من الأوامر والتعليمات تسمى بالبرنامج، ويتم تخزينها في الذاكرة الخاصة بالحاسوب للرجوع إليها في حالة التشغيل لمعالجة البيانات"[5]. إذن[6] هو جهاز الكتروني قادر على استقبال المعطيات التي ترغب في إدخالها وتخزينها ومعالجتها به، وكذلك تخزين التعليمات الخاصة بالبرامج

[1] - هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة)، الطبعة الأولى، دار النهضة العربية، القاهرة، 1998، هامش (2)، ص15.

[2] - هلالي عبد الله أحمد، المرجع نفسه، ص15.

[3] ROBERT Paul , le Petit Robert , Dictionnaire Alphabetical et la Anallogique logos de la langue francaise, val,l,Paris 1983 ,p.1319.

[4]- محمد عبد ابو بكر سلامه ، مرجع سابق، ص 26.

[5] رشدي محمد علي محمد عيد، مرجع سابق، ص 46.

[6] - الحاسب الآلي هو التسمية العربية الشائعة، وقد استخدم المجمع اللغوي تسمية الحاسب الالكتروني، بينما اعتمدت المنظمة العربية للمواصفات والمقاييس مصطلح الحاسوب، وهناك من يعبر عنه بمصطلح الكمبيوتر ولكن الأفضل مصطلح الحاسب الآلي لأنه الترجمة لاسمه بالانجليزية.

التطبيقية للقيام بالمعالجة تلك المعطيات وإيجاد الحل، وقادر على إخراج هذا كل بسرعة شديدة ، قد تصل لملايين العمليات في الثانية[1].

ويعرفه البعض أنه "آلة حاسبة الكترونية[2]تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرنامج معين بعملية تشغيل هذه البيانات للحصول على النتائج المطلوبة"[3].

ويعرف أيضا أنه "آلة تتولى معالجة المعطيات المخزونة في الذاكرة الرئيسية في صيغة معلومات تحت إشراف برنامج مخزون سلفا في الجهاز"[4].

ويعرف أنه" منظومة سريعة ودقيقة لها القابلية على التعامل مع المعلومات ومرتبة بصورة يمكنها قبول وخزن ومعالجة البيانات وإخراج النتائج بدون تدخل يذكر من قبل الإنسان بموجب أوامر وايعازات تقدم لها سابقا"[5].

ومن خلال كل هذه التعاريف، يمكن أن نستنتج أنها تختلف من حيث الصياغة ولكنها تتضمن نفس المعنى أي أنه آلة تقوم بمعالجة المعطيات وتحويلها لمعلومات الكترونية إذ تعتبر هذه الوظيفة الأساسية للحاسب الآلي إضافة إلى وظائف أخرى لا تقل أهمية خاصة لما يرتبط هذا الأخير بشبكة الانترنت.

المطلب الثاني
وظائف الحاسب الآلي

يلعب الحاسب الآلي دورا رهيبا وخطيرا في الحياة، حيث جعل العالم قرية صغيرة كما يقال ولا يعترف فيها بحدود طبيعية أو سياسية مما أدى إلى نشوء علاقات قانونية تجاوزت البعد الوطني إلى البعد الدولي، مما يشكل خطورة على جميع الدول وليس دولة بعينها، ولذلك اكتسبت جرائم الحاسب الآلي بعدا آخرا لأنها نمط من العلاقات القانونية التي أنشأها التعامل بالحاسب الآلي.

فيستخدم الحاسب الآلي في جميع النشاطات وذلك لزيادة السرعة والدقة، فالحاسب الآلي يساعدنا في أن نعمل بشكل أسرع عن طريق تقليل الفترة الزمنية التي تستغرقها

---

[1] - محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي 2007 دار الجامعة الجديدة للنشر الإسكندرية، ص 17، أشار إليه صالح محمد الموسوعة العربية للكمبيوتر والانترنت http://www.c4arab.com .

[2] والمقصود منه أيضا آلة حاسبة الكترونية وهو أن الحاسب الآلي يستطيع بواسطته حل المشاكل الرياضية المعقدة والطويلة التي تتضمن الملايين من العمليات الحسابية المعقدة وحتى قيامه بعمليات التحليل الإحصائي التي يستعصى حلها بالوسائل اليدوية. ولكن لا يقتصر دوره فقط على هذه الأمور إذ يمكن له القيام بأكثر من ذلك الأمر الذي يجعل منا تجاوز أصحاب التعريف المذكور أعلاه وبالتالي الحاسب الآلي لا يمكن وصفه بالآلة الحاسبة الالكترونية فقط لأنه يقوم بوظائف أخرى زيادة على الحساب الالكتروني.

[3]- محمد حماد مرهج الهيتي، جرائم الحاسوب، الطبعة الأولى، دار المنهاج للنشر والتوزيع، عمان الأردن، 2006، ، ص 22.

[4] - سامي علي حامد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص10 .

[5] - انتصار نوري الغريب، أمن الكمبيوتر والقانون، دار الراتب الجامعية، بيروت لبنان، 1994، ص 13.

العمليات الحسابية والمنطقية داخله وهذه الفترة قصيرة جدا حتى لا تكاد تلاحظ في كثير من الأحيان. فالدقة وثيقة الصلة بالسرعة إذ أن السرعة بلا دقة أمر لا فائدة منه. كذلك يساعدنا على تقليل التكاليف[1] وتحسين نوعية العمل[2] ويساعدنا أيضا بقدرته الهائلة على تخزين واسترجاع البيانات،[3] إضافة إلى أن للحاسب الآلي فوائد ترجع حتى على الشخص الذي تعلمه[4] .

ونشير في هذا الصدد، إلى أن الحاسب الآلي ليس حاسبة الكترونية بالمعنى المتعارف عليه لهذه العبارة إذ لديه وظائف كثيرة يقوم بها، إذ يمكن أن القول أن هذا الأخير فتح الأفاق أمام الفكر الإنساني وأدى إلى أحداث الثورة التي يعيشها العالم اليوم، بعد أن ظهر باعتبارها جهازا يقوم بعمليات حسـابية معقدة وبسرعة، فإنه تطور بسرعة وأصبح بدلا عن ذلك مخازن كبيرة قادرة على تجميع كم هائل لا حدود له من المعلومات وذا قدرة فائقة على استرجاعها بسرعة أكبر، حتى أنه غزى جميع مجالات الحياة وأصبح الاستعانة به ضرورة لا غنى عنها سواء على مستوى أجهزة الدولة وإدارتها المختلفة أو على مستوى المشروعات الخاصة أو العامة بل وحتى الأفراد.

إذ أصبحنا نقضي أعمالنا اليومية عن طريق الحاسب الآلي حتى أصبح لكل منا حاسبه الشخصي بل لا يمكن أن تجد اليوم عملا، على مختلف أصعدة الحياة ليس للحاسب الآلي دور فيه، ولا تكاد تجد مكتبا إلا وجهاز الحاسب الآلي يتربع عليه قبل صاحبه فقد أغلق المنافذ وسد جميع السبل والطرق أما الإنسان فلا يكاد يسلك طريقا إلا كان قد سبقه إليه إن صح التعبير.

كما أن كل أجهزة الدولة وإداراتها تعتمد اليوم وبشكل كبير على الحاسب الآلي، ما جعل بالإدارة اليوم إلا أن أصبحت الكترونية، فالإدارة الالكترونية هي العملية الإدارية القائمة على الإمكانيات المتميزة للحاسب الآلي وللانترنت حيث أنها تعتمد على الأرشيف

[1] - بالرغم من أن ثمن الحواسيب في انخفاض مستمر إلا أنها تعتبر غالية الثمن نسبيا ولكنها في الكثير من الحالات تقلل تكاليف تنفيذ وظيفة معينة بشكل كبير، فمثلا استخدام الأقمار الصناعية في الاتصالات أدى إلى تقليل تكلفة الهواتف.

[2] - تعمل الحواسيب في بعض المواطن الإنتاج بموثوقية أكبر ودقة أعلى من المهارات البشرية، فاستخدامها يحسن نوعية البضائع والخدمات.

[3] - يستطيع الحاسب الآلي تخزين كم هائل من المعلومات واسترجاع هذه البيانات عند الحاجة بسرعة كبيرة جدا، ويرجع ذلك للطاقة التخزينية الهائلة التي يمتاز بها الحاسب الآلي.

[4] - تعلم الحاسب الآلي ضروري إذ أننا لا نستطيع تكوين مستوى تعليمي جيد دون تعلم شيء عن الحواسيب التي أصبح لها تأثير كبير على حياتنا إذ أنها تدخل في جميع نواحي حياتنا سواء على صعيد استخدامها من قبل الأشخاص داخل الدوائر والمؤسسات أو على صعيد استخدامها في كثير من اللوازم الحديثة والماكينات والناقلات، كما أن تعلم الحاسب الآلي يفيد صاحبه في الحصول على وظيفة إذ أن معظم أصحاب العمل يحتاجون إلى موظفون يجيدون التعامل مع الحاسبات الإلكترونية ، مشار إليه لدى عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، الطبعة الأولى، دار وائل للنشر عمان، الأردن، 2005، ص 33.

الالكتروني، البريد الالكتروني، الأدلة والمفكرات الالكترونية، الرسائل الصوتية، وهي إدارة شبكية ذكية تعتمد على إعمال المعرفة.[1]

ويشير مصطلح الإدارة الالكترونية إلى مقدرة الدولة على تحسين الخدمات المقدمة إلى المواطنين باستخدام التكنولوجيا[2]، وفي الغالب يكون مرتبطا باستخدام وتيسير تكنولوجيا الحاسب الآلي والانترنت[3].

ويرتبط تعريف الإدارة الالكترونية بالدور المهم المتنامي لاستخدام التكنولوجيا الحديثة للمعلومات من أجل تيسير وفعالية العمل الإداري أو الخدمات الحكومية بصفة عامة، والقضاء على المشكلات الإدارية الناجمة عن استخدام الأوراق في التعامل الإداري[4].

كما أن مفهوم الإدارة الإلكترونية أوسع من كونه وجود حواسيب وبرمجيات وانترنت وغيرها من التقنيات إذ أنها إدارة شاملة لمختلف أوجه الأعمال الإلكترونية وإدارة العلاقات العامة، وتلبية حاجيات عميل الإدارة، وهو المواطن أو المستفيد من الخدمات وتنظيم العلاقة بين مؤسسات الدولة والقطاع الخاص والهيئات الرسمية وغير الرسمية[5] وهكذا.

وعن المفهوم الذي تبناه الاتحاد الأوروبي للإدارة الالكترونية بأنها :" حكومة تستخدم تكنولوجيا المعلومات والاتصالات لتقدم للمواطنين وقطاع الأعمال الفرصة للتعاون والتواصل مع الحكومة باستخدام الطرق المختلفة للاتصال مثل: الهواتف، الفاكس، البطاقات الذكية، البريد الالكتروني والانترنت، وهي تتعلق بكيفية تنظيم الحكومة نفسها في الإدارة والقوانين والتنظيم ووضع إطار لتحسين وتنسيق طرق إيصال الخدمات وتحقيق التكامل بين الإجراءات"[6].

من خلال ما سبق وإن تم إدراج بعض الوظائف التي يؤديها الحاسب الآلي إذ لا يمكن حصر هذه الأخيرة، فالحاسب الآلي للقيام بكل تلك الوظائف لابد له من متخصصين في

---

[1] صليحة علي صداقة، مرجع سابق، ص 141، أشارت إليه إيمان محمد الغراب، التعلم الالكتروني مدخل إلى التدريب غير التقليدي، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، جمهورية مصر العربية، القاهرة، 2003، ص 15-16.

[2] من الإيجابيات المهمة لتكنولوجيا المعلومات هي تحسين دور الإدارات وتحولها إلى إدارات إلكترونية عموما وكان لذلك أثره المباشر والمستحسن من قبل المواطن ونأخذ على سبيل المثال وهو استخراج شهادات الميلاد الأصلية عبر كامل التراب الوطني الجزائري خلافا لما كان عليه سابقا وهو ضرورة تنقل المواطن للولاية التي ولد فيها واستخراج تلك الشهادة والعناء الذي كان يتعرض إليه خاصة في حالة بعد المسافة بين الولايتين التي ولد فيها والتي يسكن فيها، أيضا استخراج شهادة الجنسية أصبح اليوم عن طريق شبكة الانترنت، ونحن اليوم لسنا مضطرين إلى السفر مسافات بعيدة لرؤية إعلان قامت به أحد الإدارات بل ندخل على شبكة الانترنت فقط نجده متاحا وغيرها من التسهيلات التي تقدمها الإدارة الإلكترونية مقارنة بالإدارة الورقية.

[3] صليحة علي صداقة، المرجع نفسه، ص 143.

[4] عبد الله الشيخ عصمت، دور النظم وتكنولوجيا المعلومات في تيسير وفعالية العمل الإداري، دار النهضة العربية، القاهرة، 1998، ص 139.

[5] صليحة علي صداقة ، المرجع نفسه، ص 144.

[6] صليحة علي صداقة، المرجع نفسه، ص 144.

المجال المعلوماتي يستطيعون التعامل به ومن خلاله، ذلك لما لهذا الأخير من مكونات مادية ومعنوية ربما يستعصى على غير المختص التعامل معها.

المطلب الثالث
مكونات الحاسب الآلي

على كل دارس للجرائم المعلوماتية وجرائم المعطيات أن يحيط علما بالأدوات التي ترتكب بها هذه الجرائم، أو ترتكب عليها وهو في سبيل ذلك لا غنى عن معرفة الشرط البديهي والمفترض في هذه الجرائم وهو الحاسب الآلي.ويشتمل الحاسب الآلي على مكونات مادية (الفرع الأول) وأخرى معنوية(الفرع الثاني)، ولابد من الإشارة بخصوص مكونات الحاسب الآلي أن هناك من يدرجها ضمن مكونات النظام المعلوماتي، في حين أن النظام المعلوماتي لا يشمل فقط الحاسب الآلي وحده فقد يشمل عدة حاسبات آلية وقد ترتبط هذه الأخيرة بشبكة الانترنت.

الفرع الأول
المكونات المادية للحاسب الآلي

تتألف المكونات المادية للحاسب الآلي من عناصر رئيسية أهمها: وحدة التشغيل، ووحدات الإدخال والإخراج، ووحدات التخزين، وحدة التحكم، وحدة الذاكرة المساعدة، وحدات الحساب والمنطق وسنفصل في البعض منها خدمة للموضوع كالتالي:

أولا: وحدات الإخراج والإدخال

وهي تستخدم في إدخال البيانات والأوامر والمعلومات إلى وحدة التشغيل أو المعالجة المركزية في الحاسب الآلي، أو إخراجها منها لاستخدامها بواسطة مستخدم الحاسب وذلك بتوجيه من وحدة التحكم، أوهي على حد تعبير بعض الفقه بمثابة " الوسائط المستخدمة لإظهارها نتائج التشغيل ومعالجة البيانات ".

أ. **وحدات الإدخال:**

هي الوحدات المصممة للقيام بإدخال المعلومات والمعطيات المطلوب معالجتها إلى وحدة المعالجة الرئيسية، وتتألف هذه الوحدات بدورها من العديد من المكونات، ومن بينها لوحة المفاتيح، الماسح، الفأرة، مشغل الأقراص[1].

ب- وحدات الإخراج:

بعد أن يتم إدخال البيانات والأوامر والمعلومات إلى الحاسب الآلي ومعالجتها، فإنه يمكن من خلال ذلك الحصول على المعلومات وناتج معالجة البيانات بواسطة وحدات الإخراج المختلفة، فوحدات الإخراج هي الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات الموجودة والمخزنة في الحاسب الآلي[2].

فتستخدم وحدات الإخراج لعرض نتائج العمليات التي أتمها الكمبيوتر على المعطيات التي تم إدخالها إليه عن طريق وحدات الإدخال، فهي مجموعة الوحدات المسؤولة عن إظهار ما يحتاجه المستخدم للتفاعل مع الحاسوب[3]، ومن أمثلتها الطابعات والشاشات، ومن أمثلة وحدات الإخراج أيضا وحدة تخزين البيانات على الأقراص الممغنطة أو على الشرائط الممغنطة والتي تستخدم كوحدة إدخال أيضا[4].

ثانيا: وحدة الذاكرة والتحكم

آ-وحدة الذاكرة: وتقوم هده الوحدة بتخزين البرامج والبيانات وهذه الوحدة على صنفين[5]:

1 – وحدة الذاكرة الرئيسية: تستخدم لتخزين البرامج والبيانات التي تقع تحت المعالجة.

2 – وحدة ذاكرة القراءة فقط: حيث تتم برمجة هذه الذاكرة أثناء مرحلة التصنيع ويمكن قرائتها عند الحاجة، ولا يمكن تخزين أي معلومات جديدة أثناء استخدامها.

ب - وحدة التحكم:

تنظم علاقة وحدة المعالجة المركزية مع الوحدات الأخرى لاستلام البيانات وإرسال النتائج بعد المعالجة فتقوم بالتحكيم بعمل وحدات الحاسوب وتنسيق تبادل البيانات والأوامر، وتحتوي على مجموعة من المسجلات والعدادات ودوائر فك الرموز وتحليلها ومولدات إشارات التزامن والتحكم[6].

---

[1] علي جبار الحسيناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن، بدون طبعة، 2009، ص 23.

[2] أنظر رشيدة بوكر، مرجع سابق، ص 62.

[3] علي جبار الحسيناوي، مرجع سابق، ص 25.

[4] الطابعات أنواع فمنها الحرارية التي تعمل بالتأثير الحراري للتيار الكهربائي ، ومنها من تعمل بطريقة مصفوفة للنقط وهناك طابعات العجلة، كما توجد طابعات تعمل بأشعة الليزر، والأخرى تعمل بالحبر العادي في أقلام خاصة.

[5] علي جبار الحسيناوي، المرجع نفسه، ص 24.

[6] علي جبار الحسيناوي، المرجع نفسه، ص 24.

الفرع الثاني
المكونات غير المادية للحاسب الآلي

سبق وأن عرفنا الحاسب الآلي عدة تعاريف من ضمنها أنه " آلة تقوم بأداء العمليات الحسابية، واتخاذ القرارات المنطقية على البيانات الرقمية بوسائل الكترونية وذلك تحت تحكم البرامج المخزنة فيها"[1]، وتتم هذه المعالجة باستخدام المكونات المنطقية للحاسب الآلي أو البرامج[2].

فإلى جانب المكونات المادية للحاسب الآلي، هناك مكونات غير مادية أوما يطلق عليها بالكيان المعنوي للحاسب الآلي وتتمثل في البرامج والمعطيات.

تشكل المعطيات والبرامج معا المكونات غير المادية لنظام المعالجة الآلية، إذ بدونها يعتبر الحاسب الآلي مجرد آلة كباقي الآلات، فلها درجة كبيرة من الأهمية ذلك أنها تعتبر الروح بالنسبة للحاسب الآلي، والعدوان عليها هو الذي يشكل الجريمة المعلوماتية بالمعنى الدقيق.

وتجدر بنا الإشارة في هذا المقام إلى أن هناك ما يسمى الكيان المعنوي للحاسب الآلي فقط بالبرنامج، في حين مصطلح الكيان المنطقي يعتبر مصطلح غامض لا يتناسب والمكونات غير المادية ويشمل هذا الأخير البرامج والمعطيات، وسيتم التفصيل فيهما كالآتي:

أولا: البرامج

للحاسب الآلي كيانان مادي ومعنوي بينهما ترابط هذا الترابط من شأنه أن يؤدي إلى صعوبة الفصل بينهما من الناحية العملية، إلا أن ضروريات الدراسة تقتضي هذا الفصل وإنما هو ليس إلا فصلا نظريا، ونشير في هذا الصدد إلى ضرورة الكيان المعنوي للحاسب الآلي إذ أنه بالنسبة لهذا الأخير بمثابة القلب إلى جسد الإنسان، أو العجلات بالنسبة للسيارات إذ بدونها تظل مجرد كتلة صلبة هامدة، وأنه أي الحاسب الآلي قيمته من قيمة البرامج والمعلومات المخزنة به، إذ أن قيمته من غير البرامج لا تساوي إلا قيمة المواد التي يتكون منها، وهي بالقياس إلى مكوناته المعنوية لا تقارن.

وسنحاول التفصيل في المقصود بالبرامج لمقارنتها بالبيانات المعالجة الكترونيا هذا من جهة، ومن جهة أخرى لأن محل هذه الدراسة الاعتداء على المعلومات الالكترونية[3].

---

[1] - عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، الطبعة الأولى، دار وائل للنشر الأردن عمان، 2005 ص 26، أشار إليه محمد الفيومي ، مقدمة الحسابات وتشغيل الحسابات الصغيرة ، المكتب الجامعي الحديث الإسكندرية 1998، ص8.

[2] - محمد عبد الله أبوبكر سلامة، مرجع سابق، ص 53.

[3] الأصل أننا نعني المعلومات الالكترونية السرية لأنها هي الجديرة بالحماية الجزائية ، أنظر في شروط المعلومات الجديرة بالحماية الجزائية بينما المعلومات الالكترونية المتاحة تخرج من نطاق هذه الدراسة.

1- معنى البرنامج في اللغة:

البرنامج في اللغة يعني نشرة تبين وقائع ما وضعت لأجله أو عمل، والبرنامج يعني المناهج وهوا لخطة التي تختط لعمل معين، ويعني أيضا الورقة الجامعة للحاسب، والخطة المرسومة لعمل ما كبرنامج الدرس والإذاعة، ويقال برمج أعماله، وضع لها برنامجا ومخططا، وبرمج الكمبيوتر زوده بتعليمات لإنجاز عمل معين، وهو يختلف عن البرمجة، حيث أن المقصود بها العملية المنهجية لوضع الإجراءات والخطوات الواجب اتخاذها لتحقيق أهداف محددة بصورة فعالة[1].

فإذا يعني البرنامج منهاج أو خطة يتم رسمها ووضع خطواتها، تعني البرمجة العلمية المنهجية لوضع الإجراءات والخطوات موضع التطبيق لتنفيذ البرنامج ، أي ما تم رسمه وتخطيطه، أي الخطة[2].

2-تعريف البرنامج في الاصطلاح العلمي:

عرفه البعض أنه "مجموعة من التعليمات المتسلسلة التي تخبر الحاسوب ماذا يفعل"[3] ،أو أنه " مجموعة من الأوامر والإرشادات والايعازات التي تحدد لجهاز الحاسوب العمليات التي يقوم بتنفيذها بتسلسل وخطوات محددة، وتحمل هذه العمليات على وسيط معين يمكن قراءته عن طريق الآلة وبعد ذلك يمكن للبرنامج عن طريق معالجة البيانات أن يؤدي وظائف معينة ويحقق النتائج المطلوبة منه "[4].

3- معنى البرنامج في الاصطلاح القانوني:

هو مجموعة من الأوامر وضعت بترتيب معين وبلغة معينة وأسلوب خاص لوضع حل، أو علاج لمشكلة ما أوتنفيذ عملية بواسطة الحاسب الإلكتروني[5]، أو هو عبارة عن " مجموعة من التعليمات التي من أجلها نفذ البرنامج، فهو يرسل الأوامر إلى الجهاز، ليقوم بتنفيذها، مع العلم بأن البرنامج يقوم بإصدار الأوامر بناء على توجيهات المستخدم "[6]، أو هو

---

[1] - جورج متني عبد المسيح، لغة العرب، الجزء الأول، مكتبة لبنان، بلا سنة طبع، ص 84.

[2] - محمد حماد مرهج الهيتي، جرائم الحاسوب، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان الأردن، 2006، ص 44.

[3] - رشيدة بوبكر، مرجع سابق، ص 68 ، أشار إليه محمد بلال الزغبي، أحمد الشرايعة، منيب قطيشات، مهارات الحاسوب والبرمجيات، الطبعة الخامسة، دار وائل للنشر عمان، 2008، ص 36.

[4] - رشيدة بوبكر، المرجع نفسه، ص 68، عن علي فاروق الحفناوي موسوعة قانون الكمبيوتر ونظم المعلومات ، قانون البرمجيات دراسة متعمقة في الأحكام القانونية برمجيات الكمبيوتر، الكتاب الأول، دار الكتاب الحديث، القاهرة، 2003، ص 79.

[5] - محمد حماد مرهج الهيتي، المرجع السابق، ص 45.

[6] - رشا علي الدين،النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة الإسكندرية، 2007، ص 12 عن http://arabic2000.topcities.com/soft.htm,10-02-2012.

عبارة عن " مجموعة من تعليمات الحاسب الالكتروني المدونة بنوع من الوضوح والتفصيل "[1].

ويعرفه البعض أنه " مجموعة من البرامج والتعليمات التي تستخدم في إدارة ومراقبة وتشغيل أجهزة الحاسب الالكتروني"[2].

وعرفته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 2 من الفصل الأول أنه" مجموعة من التعليمات والأوامر قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لانجاز مهمة ما".

فالكيان المعنوي للحاسب الآلي يشمل البرامج المختلفة التي يتحقق من خلالها قيام الحاسب بوظائفه المختلفة بالإضافة إلى المعلومات المطلوب معالجتها بالفعل[3]، وهذا ما أكدته المنظمة العالمية للملكية الفكرية بعدما عرفت الكيان المنطقي أوضحت أنه هو برنامج أو أكثر بالإضافة إلى وصف البرنامج ومستنداته الملحقة[4].

وعرفه جانب من الفقه القانوني بأنه " تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقني معقد يسمى بالحاسب الالكتروني بغرض الوصول إلى نتيجة معينة ".[5] وعرفه جانب آخر من الفقه أنه "عبارة عن سلسلة من التعليمات التنفيذية المباشرة الموجهة إلى جهاز الكمبيوتر"[6].

ويظهر من خلال التعاريف السابقة أن البرنامج ما هو إلا عبارة عن تعليمات مفصلة للغاية وهذه التعليمات توجه للجهاز لتنفيذ ما يريده المبرمج، وبذلك يمكن للجهاز القيام بالعمل الذي من أجله صمم البرنامج، وتتواجد هذه البرامج عادة في اسطوانات مدمجة CD [7] أو أقراص مرنة DVD أوDISK[8].

---

[1] - قاموس المصطلحات الصادرة عن المنظمة العربية للعلوم الادارية (انجليزي، فرنسي، عربي)، 1980.

[2] - D.CASSEL et M.JACKSON, introduction to computers and information processing, london,1980,p.30.

أشارت إليه رشا علي الدين، مرجع سابق، ص 12.

[3] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية ،دار هومه للطباعة والنشر والتوزيع، 2007، ص 15.

[4] رشا مصطفى أبوالغيط، تطور الحماية القانونية للكيانات المنطقية،دار الفكر الجامعي الإسكندرية،2006 ، ص 5.

[5] - رشا علي الدين، مرجع سابق، ص12 ، أشارإليه محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الالكتروني، دار الثقافة للطباعة والنشر، القاهرة، 1987، ص8.

[6] - BEllEFONDS, X.L. HOLLANDE Pratique de droit d'informatique, DELMAS,Paris, 1998 ,P.171.

أشارت إليه رشا علي الدين، المرجع السابق، ص 12 .

[7] - يقصد بها الإشارة إلى القرص المدمج أوما يعرف بأسطوانة متراصة عالية السعة تستخدم بصفة ذاكرة للقراءة منها فقط البيانات التي تم تسجيلها باستخدام تقنية للتخزين الضوئي بأشعة الليزر.

[8] - يقصد به وسيط آلي يستخدم لتخزين البيانات بصفة ذاكرة خفية للكمبيوتر مكونة من عدد من الأقراص المسطحة ذات أسطح مغطاة بطبقة رقيقة من مادة قابلة للمغنطة ، وكل سطح منها مقسم إلى عدد من الدوائر أو المسارات المخصصة لتسجيل البيانات الثنائية عليها أو قراءتها منها بواسطة رؤوس مغناطيسية مثبتة على ذارع توصيل يحركها للداخل أو

ورغم كل هذه التعريفات إلا أنها غير كافية لتضع الباحث أمام صورة واضحة فيما يخص البرنامج، إذ هناك تعريف واسع وآخر ضيق لهذا الأخير كل منهم حسب الزاوية التي ينظر إليها لتعريفه. فإذا تم النظر إليه من زاوية التعليمات التي توجه إلى الآلة فحسب كان التعريف ضيقا وإذا تم النظر إليه من زاوية التعليمات التي توجه ليس إلى الآلة وحدها وإنما إلى العميل أيضا كان التعريف موسعا، وستتم مناقشة التعريفين كالتالي:

أ- التعريف الضيق لبرنامج الحاسب الآلي:

تتنوع التعريفات التي قيلت وفقا لهذا الاتجاه، فعرفه البعض بأنه مجموعة التعليمات التي يخاطب بها الإنسان الآلة فتسمح لها بأداء مهمة محددة.[1] وعرفه البعض على أنه : " مجموعة من التعليمات الموجهة إلى الحاسب الإلكتروني ليستطيع القيام بالمهام المراد منه القيام بها "[2]، وأخذت بهذا التعريف اتفاقية تربس وهي اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية حيث نصت المادة العاشرة منها أن " تتمتع برامج الحاسب الآلي سواء كانت بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن 1971 ".

وفي هذا النطاق تنصرف الحماية القانونية إلى أكثر صور البرمجيات انتشارا، حيث تنصرف الحماية إلى كل من برامج المصدر وبرامج الهدف[3]، هذا ما ذهب إليه الحديث في مفاوضات وفد مصر في فصل الانعقاد الثالث لجمعية خبراء القانون الدوليين المنعقدة في جنيف بمقر المنظمة العالمية الفكرية في الفقرة من 5 إلى 9 ديسمبر 1994.

وقد أثر التعريف الضيق في بعض التشريعات المقارنة مما جعله مرحبا به لديها، فعلى سبيل المثال[4] أخذ به المشرع الأمريكي في المادة 101 من قانون المؤلف الصادر في 19 أكتوبر 1976 حيث عرفها " مجموعة من التعليمات والأوامر التي يمكن استعمالها من

الخارج بواسطة سواقة القرص للتواصل مع مسار التسجيل المطلوب بطريقة مباشرة دون الحاجة للتعامل المتتابع للمسارات السابقة.

[1] - محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، للنشر، الإسكندرية، 2001، ص 33.

[2] - رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة، الإسكندرية، 2007، ص 13.

[3] - برامج المصدر هي برامج يتم تحريرها بلغة منخفضة المستوى أوعالية المستوى وهي لا تخاطب الآلة إلا بعد تحويلها إلى لغتها أي ترجمتها إلى لغتها، ويقصد ببرنامج الهدف برنامج المصدر الذي تم تحويله إلى برنامج بلغة الكمبيوتر عن طريق برنامج الترجمة الذي يستعمل لتحويل لغة البرنامج المصدر الذي تم تحويله إلى برنامج الكمبيوتر، وإن كان التطور العلمي يذهب إلى إمكانية كتابة البرنامج بلغة الآلة (الكمبيوتر)مباشرة ومنه فبرامج الترجمة هي برامج تستعمل لتحويل برامج المصدر إلى برامج الهدف. انظر رشا علي الدين ، المرجع السابق، ص 14 ومحمد محمد شتا، المرجع السابق، ص 35.

[4] - عرفه المشرع المصري أنه : "مجموعة من التعليمات المعبر عنها بأي لغة أورمز ومتخذة أي شكل من الأشكال ويمكن استخدامها بطريقة مباشرة أوغير مباشرة في حاسب لأداء وظيفة أووصول إلى نتيجة محددة سواء كانت هذه التعليمات في شكلها الأصلي أوفي شكل آخر تتحول إليه بواسطة الحاسب. " قرار وزير الثقافة المصري رقم 82 لسنة 1992، بشأن تنفيذ قانون حماية حق المؤلف فيما يتعلق بمصنفات الحاسب الآلي، أنظر محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، المكتبة العصرية للنشر والتوزيع، مصر، الطبعة الأولى 2010، ص 70.

خلال طريقة مباشرة على جهاز الكمبيوتر بغرض الحصول على نتائج معينة"، والمشرع الياباني في قانون المؤلف رقم 48 لسنة 1970 في المادة 10 فقرة 1 و2 حيث وصفته بأنه "مجموعة من التعليمات التي من شأنها جعل الكمبيوتر يقوم بأداء وظيفة معينة "[1].

نستنتج من خلال التعريفيين أنهما في وصفهما لبرامج الحاسب الآلي لم يمتد إلى وصف البرنامج والمستندات الملحقة به. وما تجدر به الإشارة في هذا الصدد أن المفهوم الضيق لم تتأثر به التشريعات الوطنية المقارنة فقط بل تبنته اتفاقيات دولية كذلك، منها المنظمة العالمية للملكية الفكرية WIPO إذ تعرف في نسختها العربية من معجم المصطلحات لحق المؤلف والحقوق المشابهة برنامج الكمبيوتر بأنه: " مجموعة من التعليمات التي تسمح بعد نقلها على دعامة مقروءة من قبل الآلة ببيان أو أداء أو إنجاز وظيفة أو مهمة أو نتيجة معينة عن طريق آلة قادرة على معالجة المعلومات "، وهوما يتفق مع التعريفيين السابقين الأمريكي والياباني[2].

ب- التعريف الموسع لبرامج الحاسب الآلي :

البرنامج وفقا لمفهومه الواسع، لا يقصد به مجموعة الأوامر والتعليمات الموجهة للحاسب الآلي (المفهوم الضيق للبرنامج) فقط، إنما يضم إلى جانب ذلك وصف البرنامج والمستندات الملحقة التي تساعد على تبسيط فهم البرنامج وتيسير تطبيقه[3].

أي يقصد به كل التعليمات التي يوجهها مصممي البرامج إلى مستخدمي الحاسب الآلي وتعينهم على فهم عمل البرنامج وتطبيقه، هذا إلى جانب المفهوم الضيق للبرنامج، الذي يتحدد بالتعليمات الموجهة للحاسب الآلي فقط. أي أن البرنامج وفقا للمفهوم الواسع يضم نوعين من التعليمات، التعليمات الموجهة للكيان المادي للحاسب الآلي والذي يشتغل على ضوئها، والتعليمات الموجهة للعميل مثل تعليمات استعمال البرنامج وكيفية المعالجة الآلية للمعلومات، أي كافة البيانات والتعليمات التي يتم إلحاقها بالبرنامج، والتي تساعد مستخدم الحاسب على سهولة فهمه وتطبيقه، باعتبار أن هذه التعليمات تتضمن وصفا تفصيليا لكافة مراحل التطبيق وهذه البيانات عبارة عن تعليمات موجهة من المبرمج – من يتولى إعداد

[1] - رشا علي الدين، مرجع سابق، ص 15.

[2] - يقال عن التعريف الياباني أنه أفضل من التعريف الأمريكي وذلك في عدم تمييزه بين التعليمات والأوامر والاكتفاء بالتعليمات لأن الأوامر نوع من التعليمات ومع ذلك فإن الأوامر في حد ذاتها لها وظيفة تؤثر في المعلومات كما أن القانون الأمريكي لم يربط بين التعليمات والتأثير المباشر في الحاسب ذلك أن التعليمات في حد ذاتها من شأنها التأثير في الحاسب وجعله يؤدي وظيفة معينة، أما الاستعمال فأمر مفترض، كما أن النص القانوني الياباني على الهدف وهو أداء الحاسب وظيفة معينة أعم في الدلالة وأقرب للدقة من التعريف الأمريكي الذي يتبين أن الهدف هو الحصول نتائج معينة، لأن النتائج مجرد جزء من الوظائف التي يؤديها الحاسب من خلال برمجته، أشار إليه محمد محمد شتا، مرجع سابق ، ص 39.

[3] - محمد محمد شتا، مرجع سابق، ص 40.

البرامج – إلى الذي يتعامل مع الحاسب الآلي[1]. فالتعريف الواسع يتضمن عناصر ثلاثة هي[2]:

1-التعليمات والأوامر الموجهة للجهاز (الحاسب الآلي) للقيام بوظيفة أو مهمة معينة.

2-طريقة تشغيل البرنامج ذاته أي التعليمات التي يتعين إتباعها من المستخدم للبرنامج حتى يتسنى له تشغيل البرنامج وهي ما يعبر عنها بوصف البرنامج، أي تقديم شرح تفصيلي عن مهام البرنامج والعمليات التي يقوم بها وتكون على شكل تعليمات مكتوبة، أو على شكل خطي أو غيرها ويتم من خلاله إبراز وتحديد مجموعة التعليمات المشكلة للبرنامج والصلة التي تربط كل واحدة منها بالأخرى، كل هذا لمساعدة العنصر البشري على فهم البرنامج.

3-المستندات الملحقة بالبرنامج والتي تبسط فهم وتطبيق البرنامج حتى يتمكن مستخدم البرنامج من التعامل معه[3]، فهي مستندات موجهة للعنصر البشري وتتعلق بكيفية إعداد البيانات، واستخدام البرنامج ، وأنواع الحاسبات التي تستخدم فيها هذه البرامج[4].

ولذلك يمكن وصف البرنامج والمستندات الملحقة به بأنهما كافة البيانات الأخرى الملحقة بالبرنامج التي تيسر فهم كيفية تطبيقه لما تنطوي عليه من وصف تفصيلي، وبيان لمراحل تطبيقه بعدها من يقوم بإعداد البرنامج ويوجهها لمن يقوم بالتعامل مع الحاسب الآلي[5].

تأثر بالمفهوم الواسع لبرامج الحاسب الآلي عدة مشرعين كان من بينهم المشرع الفرنسي، إذ لم يتبين موقفه من تعريف البرنامج لا في قانون العقوبات ولا في إطار القانون رقم 85-690 المتعلق بحقوق المؤلف والقوانين المعدلة له، إلا أن موقفه عكسه القرار الوزاري الصادر من وزير الصناعة والتعليم الوطني في 22 نوفمبر 1981 بشأن إثراء اللغة الفرنسية الذي أخذ بموجبه بالمفهوم الواسع للبرنامج[6].

وبخصوص المشرع الجزائري فإنه لم يتول إيراد نص خاص يحدد فيه مفهوم البرنامج على غرار التشريعات الجزائية الأخرى، وبالرجوع إلى قانون حق المؤلف الجزائري نجد أن المشرع الجزائري قد وسع من قائمة المؤلفات المحمية حيث أدمج المصنفات المعلوماتية ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي مواكبا بذلك اتجاه التشريعات في تعديل قوانين حقوق المؤلف. وكان ذلك بموجب الأمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة[7]، حيث اعتبر بموجب الفقرة (أ)[1] من

---

[1] - محمد حماد مرهج الهيتي، مرجع سابق، ص 51.

[2] محمد حماد مرهج الهيثي، المرجع نفسه، ص 52.

[3] - رشا علي الدين، مرجع سابق، ص 18.

[4] - محمد حماد مرهج الهيتي، مرجع سابق، ص 52.

[5] - محمد حماد مرهج الهيثي، المرجع نفسه ، ص 52.

[6] - رشيدة بوبكر، مرجع سابق، ص 73.

[7] القانون 05/03 المؤرخ في 19 يوليو 2033 ،المتعلق بحقوق المؤلف و الحقوق المجاورة، جريدة رسمية عدد 44 مؤرخة في 23 يوليو 2003، ص 3.

المادة 4 والفقرة 2 من المادة الخامسة 5 الواردتين ضمن الفصل الأول المصنفات المحمية، مصنفات قواعد البيانات[2] وبرامج الحاسب الآلي. وحددت المادة 153 من هذا نفس الأمر العقوبات الناجمة عن المساس بحقوق مؤلفي المصنفات المعلوماتية[3].

ج-التعريف الجامع والمانع لبرامج الحاسب الآلي[4] :

اقترحت عدة تعاريف جامعة ومانعة لبرامج الحاسب الآلي، وهناك من أطلق عليها بالتعريف الأصح لهذه الأخيرة، ومن ضمن تلك التعاريف أنه "عبارة عن مجموعة التعليمات والأوامر الموجهة لجهاز الكمبيوتر سواء كانت بلغة الجهاز أو يمكن تحويلها إلى لغة قادرة على القيام بوظيفة معينة، ويعتبر جزءا من هذه التعليمات الأوامر والمستندات والتعليمات الخاصة بتبسيط تسير فهم وتطبيق البرنامج، ويتفق هذا التعريف في مفهومه مع اتفاقية[5] تريبس"[6].

---

[1] نصت المادة الرابعة الفقرة-أ- على أنه:" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية: أ- المصفات الأدبية المكتوبة مثل ...برامج الحاسوب..."كما تضمنت الفقرة 2 من المادة 5 قواعد البيانات بنصها:" تعتبر أيضا مصنفات محمية الأعمال التالية: -المجموعات و المختارات من المصنفات .....وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى".

[2] - يعرف قرار وزارة الثقافة في مصر رقم 82 لسنة 1993 قاعدة البيانات بأنها : "أي تجميع متميز للبيانات يتوافر فيه عنصر الابتكار أو الترتيب أوأي مجهود شخصي يستحق الحماية وبأي لغة أو رمز، وبأي شكل من الأشكال يكون مخزنا بواسطة حاسب ويمكن استرجاعه بواسطته أيضا " أشارت إليه شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 20.

[3] - رشيدة بوبكر، مرجع سابق، ص 70-71.

[4] أنواع البرامج:

أ- برنامج المصدر: هي الأوامر التي يضعها المبرمج أو مؤلف البرنامج وتكون مدركة له لكنها غير مدركة للآلة التي هي الكمبيوتر كجهاز مادي (وحدة المعالجة تحديدا) ويستخدم في تأليفها أو وضعها لغات البرمجة التي شهدت تطورا مذهلا عبر السنوات الخمسين المنصرمة، هذه اللغات التي تختلف من حيث سهولتها وتعقيدها ومن حيث فعاليتها في انجاز البرنامج للغرض المخصص له.

ب- برنامج الآلة: وهو عكس مفهوم برنامج المصدر تماما، إذ تدركه الآلة وتستطيع التعامل معه وتشغيله، وبين برنامجي المصدر والآلة توجد برامج ذات غرض تحويلي أو(برامج ترجمة) بموجبها تتحول برامج المصدر إلى برامج آلة.

أ- **الخوارزميات:** العناصر والرموز الرياضية التي يتكون منها بناء البرنامج وهي كالأفكار والحقائق العلمية ليست محل حماية لأنها ليست موضعا للاستئثار (مادة 2/9 من اتفاقية تربس) لكنها متى ما نظمت على شكل أوامر ابتكاريه لتحقيق غرض معين أصبحنا أمام برنامج، وهو بهذا الوصف إن توفرت له عناصر الجدة والابتكار والأصالة محل للحماية شانه شان أي من مصنفات الملكية الفكرية الأدبية الأخرى ، أشار إليه العربي بن حجار ميلود، تشريعات الملكية الفكرية في حقل حماية البرمجيات بالجزائر ، العدد 26، سبتمبر 2011 ، عن الموقع الالكتروني
http://journal.cybrarians.info/in يوم الدخول على الموقع 2015/05/14.

[5] - نصت المادة العاشرة فقرة 1 و2 من اتفاقية تريبس على الآتي" تتمتع برامج الحاسب الآلي (الكمبيوتر) سواء أكانت بلغة المصدر أو بلغة الآلة بالحماية باعتبارها أعمالا أدبية بموجب معاهدة برن 1971 ، تتمتع بحماية البيانات المجمعة أو المواد الأخرى سواء أكانت في شكل مقروء آليا أوأي شيء آخر إذا كانت تشكل خلقا فكريا نتيجة انتقاء أو ترتيب محتوياتها وهذه الحماية لا تشمل البيانات أو المواد في حد ذاتها ولا تخل بحقوق المؤلف المتعلقة بهذه البيانات أو المواد ذاتها."

[6] - رشا علي الدين، مرجع سابق، ص 20.

وهو أيضا "مجموعة الأوامر والتعليمات التي تسمح بعد تحويله إلى لغة الآلة القادرة على معالجة المعلومات بإنجاز وظيفة معينة، على أن تكون هذه الأوامر والتعليمات مشفوعة بوصف البرنامج والمستندات التي تبسط فهمه وتيسر تطبيقه"[1].

ثانيا:المعطيات

تشمل المعطيات إلى جانب البرامج روح الحاسب الآلي، إذن المعطيات هي المعلومات في حالة كمون والمعطيات هي معلومات تم تنظيمها ومعالجتها داخل نظام المعالجة الآلية للمعطيات، تخزينها بغية استرجاعها عند طلبها، وكون المعطيات غير مادية لأنها عبارة عن نبضات الكترونية داخل لحاسب الآلي لا يمكن لمسها[2]، فترتكز آلية التشغيل في الحاسب الآلي على المعلومات التي يتم حبسها وتخزينها في هذه الآلة[3].

فالمعطيات في اللغة تقابل "البيانات" والبيان في اللغة من مشتقات كلمة "بين" ومن معانيه فيها ما يتبين به الشيء من الدلالة وغيرها [4]، وتقابلها في اللغة اللاتينية كلمة "datum" وتعني شيء معطى أو مسلم به أوشيء ما معروف أو مسلم بصحته كحقيقة أو واقعة، وجمعها بيانات وهي التي تستخدم كلاسيكيا في اللغة الانجليزيةdata "" بينما تستخدم اللغة الفرنسية مقابلا لها كلمة معطيات[5]، وهي الكلمة التي آثر على استعمالها المشرع الجزائري في مقابل كلمة البيانات. مع العلم أن كلا من القانونين يخلوان من ذكر كلمة المعلومات رغم أن البعض فضلوا استخدام هذا المصطلح لأنه من الضروري التفرقة بين المعطيات والمعلومات، فالمعطيات عندما تعالج آليا تأخذ تسمية المعلومات.

عرف المشرع الجزائري المعطيات في المادة الثانية من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بنصه في المادة الثانية منه في الفقرة "ج" على أن

" المعطيات المعلوماتية هي أي عملية عرض للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

والملاحظ على النص أن المشرع الجزائري أدرج البرنامج ضمن مفهوم المعطيات رغم الفارق بينهما كما سبق التوضيح، ولا يفوتنا في هذا المقام أن نشير إلى أنه اعتبار البيانات هي نفسها المعطيات والتي تختلف عن المعلومات كما سبقت الإشارة.

---

[1] رشا علي الدين، المرجع نفسه، ص 20.

[2] - محمد خليفة، مرجع سابق، ص 25.

[3] نعيم مغبغب، حماية برامج الكمبيوتر، دراسة في القانون المقارن، الطبعة الثانية، منشورات الحلبي الحقوقية بيروت لبنان، 2000، ص 205.

[4] محمد خليفة، مرجع سابق، ص 86.

[5] محمد خليفة، المرجع نفسه، ص 86- 87 .

و إلى جانب الحاسب الآلي باعتباره أحد عناصر النظام المعلوماتي هناك الانترنت الذي أعتبره من أهم عناصر النظام، ذلك أنه لولا هذا الأخير لكان مستوى الجريمة المعلوماتية أقل بكثير لذلك لابد من التفصيل في المقصود بالانترنت.

المبحث الرابع
ماهية الشبكة الدولية للمعلومات

في أوائل التسعينات ظهر ما يسمى بالشبكة الدولية للمعلومات، وظهرت العديد من التقنيات والأدوات والوسائل التي أسهمت في تطوير هذه الشبكة[1]. ولذلك فإنها تعد من أحدث خدمات التقدم التقني، ويمثل التطور التقني في هذا الجانب واقعا علميا يأتي كل لحظة بالجديد[2]، الذي هو حلقة متقدمة في مجال المعلومات والاتصالات له فوائد كثيرة، وهو يقدم خدمات واسعة في مجال تبادل المعلومات بين مختلف المستفيدين في العالم فضلا عن استقبال وبث المعلومات وتسهيل الخدمات المعرفية الجديدة[3].

وقد أظهرت الشبكة الدولية للمعلومات قيمة اقتصادية كبرى للمعلومات، بحيث أصبحت المعلومات في العصر الحالي تمثل قوة كبيرة، وبالتالي ازدادت الاعتداءات الموجهة ضدها، وذلك بالاعتداء على المعلومات المبتكرة والمحمية بموجب قوانين حقوق الملكية الفكرية، كذلك الاعتداء على البيانات الاسمية، سرقة الأسرار السياسية والتجارية ، وغيرها من أشكال الاعتداءات الماسة خصوصا بسرية وسلامة وإتاحة المعلومات.

ورغم تلك الاعتداءات إلا أنه لا يمكن لأحد أن ينكر خدمات الانترنت، ذلك يعني أن لهذه الأخيرة دورها السلبي والايجابي وقبل التطرق إليها، سنحاول تعريف الشبكة الدولية للمعلومات، نشأتها وتطورها (المطلب الأول) وخدماتها (المطلب الثاني).

المطلب الأول
تعريف الشبكة ونشأتها وتطورها

[1] - عبد الله ذيب محمود، حماية المستهلك في التعاقد الالكتروني دراسة مقارنة، دار الثقافة للتوزيع والنشر عمان الأردن، الطبعة الأولى، 2012 ص 59 ، أشار إليه عبد العال طارق التجارة الالكترونية – المفاهيم- التجارب- التحديات – الأبعاد التكنولوجية والمالية التسويقية والقانونية، الطبعة الأولى، مصر، الدار الجامعية، 2003 ، ص 37، أنظر أيضا http://www.arablaw.org/arablaw.net يوم الاطلاع على الموقع2012/12/10 .

[2] - عبد الله ذيب محمود ، المرجع نفسه، ص 60.

[3] - وليد الزيدي، مرجع سابق، ص 15.

هي الشبكة الدولية التي اصطلح على تسميتها بالإنترنت[1]، وهي عبارة "عن شبكة من أجهزة الحاسوب متصلة ببعضها البعض، عن طريق مزود الخدمة والخادم في جميع دول العالم، فالحاسوب الذي لم يرتبط بمزود الخدمة لا يمكن أن يتصل بالشبكة الدولية للمعلومات، ولا يستفيد من خدمات الانترنت، كما أن جريمة الاختراق وما يتبعها من جرائم الكترونية، لا يمكن أن تتم إلا عن طريق هذه الشبة فالمعلومات المدونة في الحاسوب الخاص، الذي لم يرتبط بالإنترنت لا يمكن اختراقه"[2]. وللتعرف على المقصود بشبكة الانترنت وما لها من ايجابيات وسلبيات سنحاول التفصيل فيها من خلال تعريفها (الفرع الأول) ونشأتها وتطورها(الفرع الثاني).

الفرع الأول
تعريف الشبكة العالمية للمعلومات

وتعرف الشبكة العالمية للمعلومات أو الانترنت بأنها توصيات تعاونية لعدد من شبكات الحاسبات الآلية وهي مكونة من كلمتين هما Inter connection وكلمة Network، وهذا يعني" أن مئات الشبكات المربوطة مع بعضها البعض مكونة من حواسيب آلية مختلفة وكذلك تكنولوجيا مختلفة ، تم توصيلها ببعضها البعض بطريقة بسيطة وسهلة بحيث تبدو وكأنها قطعة واحدة أو نظام واحد دون إحساس أي من الأطراف بأنه يختلف فنيا عن الآخر"[3].

فالانترنت عبارة "عن حاسب آلي يتحدث إلى حاسب آلي آخر يرتبطان بواسطة سلك التليفون العادي أو أي فرع آخر من الكوابل، وإذا كانت الحواسيب موجودة في أماكن بعيدة ومتفرقة فيمكن استخدام الأقمار الصناعية للربط بينها ليتحقق بذلك الاتصال الدولي عبر الانترنت، وحتى في داخل الدولة ذاتها تعتمد شبكة الإنترنت على الوصلات الوسيطة بين نقطتين، وهكذا كانت بداية انترنت في وزارة الدفاع الأمريكية"[4].

الفرع الثاني
نشأة وتطور الشبكة العالمية للمعلومات

[1] اعتبر البعض أن كلمة انترنت انجليزية الأصل واعتبروها أنها اختصار مزجي للحروف الأولى من كلمتي international بمعنى دولي، وnetwork بمعنى شبكة، أشار إليه محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دراسة مقارنة، الطبعة الثانية دار النهضة العربية، 2009، الهامش رقم 1، ص 20.

[2] - لا يمكن اختراقه ولكن ترتكب عليه جرائم أخرى كفتح الحاسوب الخاص والإطلاع على المعلومات السرية الموجودة فيه وسيتم التفصيل في ذلك لاحقا.

[3] - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 80 - 81 ، أنظر أيضا سهيل محمد الغرام، الوجيز في جرائم الانترنت، مكتبة الجامعة الأردنية، الطبعة الأولى، 2009 ، ص 6.

[4] سهيل محمد العزام، مرجع سابق،ص 7 .

"الشبكة العالمية للمعلومات أو الانترنت كفكرة ولدت في وزارة الدفاع الأمريكية، وتم تطبيقه كتجربة داخل الولايات المتحدة بمعرفة الهيئات العلمية المتخصصة عام 1969م فكانت الفكرة في البداية تقوم على ربط الحواسيب الآلية ببعضها البعض في مراكز البحث، وفي كل منطقة، وفي كل مدينة على حده، إلى أن قامت مؤسسة العلوم القومية (NSF) بشراء حواسيب آلية عملاقة وتزويد مراكز الحاسب الآلي العملاق بها، تم توزيعها على كل مناطق الولايات المتحدة الأمريكية حتى تعمل إقليميا مع بعضها البعض في شكل شبكة قومية، وفي كل هذه المراحل كانت شبكة الإنترنت مخصصة لأغراض البحث العلمي، وتتعامل مع مراكز البحث ومع الجامعات وتسيير العلماء، الاستفادة من إمكاناتها الهائلة في القيام بالعمليات الرياضية المعقدة، والتي تعجز الحاسبات الآلية على القيام بها"[1].

وعندما استقرت الشبكة على مدى عشرين عاما على هذا النمط، ظهرت الحاجة الماسة إلى استخدام نفس الشبكات لأغراض تجارية يستفيد منها الأفراد والمؤسسات والشركات ورغم عدم ارتياح "NSF " وبعض المشتغلين بالشبكات الرسمية لهذا التطور، إلا أن الشركات استطاعت من خلال نفوذها داخل الحكومة الفدرالية ودوائر الحكومة الأمريكية أن تفتح المجال للاستخدام التجاري للشبكة محليا وعالميا، ولذلك يمكن القول أن الشبكة بدأت تعمل بشكل تجاري عام 1993.

والإنترنت لا يملكها أحد، ولا يسيطر عليها أحد، إنما هي ملكية تعاونية للبشرية بقدر إسهامهم فيها، وقد كانت خدمات شبكة الإنترنت في البداية مجانية وبغير مقابل، وكانت قاصرة على الاستخدامات العلمية والبحثية وليس لها الصفة التجارية[2].

وفي الوقت الحالي تقوم شركات تجارية بإدارة شبكة الإنترنت على أسس تجارية، لذلك فمن الضروري أن يدفع المشترك مبلغا من المال مقابل استخدامه للمعلومات، وكذلك لتطوير الشبكة نفسها والمحافظة على تطويرها وتحسين استخداماتها ، وذلك بالطبع إضافة إلى ما يدفعه المشترك في الشبكة إلى شبكة المعلومات مقابل استخدامه لبرامجها والاستفادة من المعلومات التي تبيعها للمستهلك مقابل إنتاجها وما بذله من جهد للحصول عليها مع تحقيق الربح المعقول[3].

وشبكة الإنترنت أو كما يطلق عليها الشبكة العالمية الإلكترونية، أو شبكة الشبكات، أو الشبكة العنكبوتية، تقدم للفرد والمجتمع كل ما تقدمه وسائل المعرفة السابقة مجتمعة، بل وتقدم – وذلك هو الأهم – المعلومات التي قد تمنعها السلطة ممثلة في الدولة أوالدين أو العلم

[1] - خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت ، دار الثقافة للنشر والتوزيع عمان الأردن ، الطبعة لأولى، 2001، ص 50-51.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 81.

[3] سهيل محمد العزام، مرجع سابق،ص 7، عن إسماعيل عبد النبي شاهين، أمن المعلومات في الانترنت،بحث مقدم لمؤتمر القانون والكمبيوتر والانترنت،جامعة الإمارات، ص 3.

أو الرقيب المتمثل في المدرسة أو المعلم أوا لوالدين، كما تقدم هذه الشبكة معلومات لنا، لم تكن تصلنا بسبب عوامل جغرافية أو سياسية أو اجتماعية[1].

كذلك قد يعجب الكثيرون حينما يعلمون أنه لا توجد إدارة مركزية للانترنت، وهي شبكة وصفها البعض بأنها فوضى تعاونية، ذلك أن كل شبكة مشتركة في الإنترنت لها قواعدها الخاصة والهيكل التنظيمي لإدارتها، ولكن لا يمكن الاتصال بين الشبكات إلا إذا كان هناك تعاون بينهما. ولذلك نجد أن هناك الكثير من اللجان ومجموعات العمل، التي تمثل فيها كل شركات المعلومات، وهي في اجتماعات مستمرة من أجل الوصول إلى وضع الأسس والضمانات التي تكفل تحسين الأداء في الشبكة العالمية، وتطوير أسلوب التشغيل والاتفاق على المصطلحات والمستجدات التكنولوجية التي تطرأ من حين لآخر[2].

ومن المشكلات القانونية التي تثيرها شبكة الإنترنت، القانون الواجب التطبيق في شأن جرائم الإنترنت وجوهر المشكلة أن الجريمة عبر الشبكة لا تعرف الحدود الجغرافية، فالجاني قد يكون في دولة أوروبية ومحل الجريمة في آسيا أوفي إفريقيا، كما في حال اختراق الشبكة بقصد التجسس المعلوماتي، كما أن بعض هذه الأفعال قد يكون مجرما في بلد الجاني دون بلدان أخرى، ومنها الدولة التي وقعت فيها الجريمة أو العكس، ولذلك فجرائم الانترنت بصفة عامة تتطلب التعاون الدولي لمكافحتها.[3]

إذن الإنترنت هو الشبكة الدولية للمعلومات[4]، وهي تعرف أيضا " أنها شبكة عالمية من الحاسبات الآلية تحتوي على شبكات منفصلة بعضها مع بعض عبر العالم مما يعطي لكل مستخدم للانترنت القدرة على الاتصال بحاسب آلي في أي مكان في العالم له اتصال بالشبكة".[5] أو هو" شبكة الشبكات وإحدى وسائل الاتصال الحديثة التي هي عبارة عن حوار عالمي بلا نهاية ".[6] ويعرفها بعضهم بأنها شبكة طرق المواصلات السريعة.[7]

وهناك من يعتبره أنه البيئة التخزينية والتبادلية التي تسهل ارتكاب الجرائم، خاصة العابرة للحدود، أوهو الهدف التي تتوجه إليه الأنماط الحديثة من السلوك الإجرامي التي تستهدف المعلومات[8].

---

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 82.

[2] عبد الفتاح بيومي حجازي، المرجع نفسه ، ص 82.

[3] سهيل محمد العزام، مرجع سابق،ص 8 -9.

[4] - خالد عياد الحلبي، مرجع سابق، ص 50.

[5] - وليد الزيدي، مرجع سابق، ص 15 ، عن مفيد الزيدي، الانترنت وآفاق البحث العلمي العربي " مجلة الأمن والحياة، العدد 198، مارس 1999، ص 52-53."

[6] - وليد الزيدي، لمرجع سابق، ص15 وهو تعريف المحكمة العليا الأمريكية في إحدى مقرراتها المؤرخ في 11 حزيران 1996.

[7] - علي جبار الحسناوي، مرجع سابق، ص 27.

[8] محمد الألفي، دور المجتمع المدني في مكافحة مظاهر العدوان الإجرامي عبر الانترنت، عن الموقع الالكتروني http://www.minshawi.com تاريخ الاطلاع على الموقع 2014/10/23.

المطلب الثاني
خدمات الشبكة الدولية للمعلومات

إن سهولة استخدام شبكة الانترنت والخدمات المتعددة والمتنوعة التي تقدمها في جميع مجالات الحياة ساهم بشكل فعال في زيادة أعداد المستفيدين منها، وسنقوم باستعراض أهم الخدمات الالكترونية التي تقدمها الشبكة العالمية للمعلومات" الانترنت" و من أهمها البريد الالكتروني وشبكة الويب العالمية (الفرع الأول)، محركات البحث والتخاطب (الفرع الثاني)، المجموعات الإخبارية والتجارة الالكترونية (الفرع الثالث)، وغيرها من الخدمات التي لا يمكن حصرها باعتبار أن البيئة الافتراضية دوما يأتي بها الجديد.

الفرع الأول
البريد الالكتروني[1] وشبكة الويب العالمية[2]

يعتبر البريد الالكتروني من الاستخدامات الشائعة التي توفر إمكانية الاتصال بملايين البشر حول العالم كبديل للبريد التقليدي. والبريد الالكتروني عبارة عن رسالة لكنها تتم بطريقة الكترونية يكتبها المستخدم على جهاز الحاسوب، وذلك بعد أن يفتح الصفحة الخاصة ببريده الالكتروني التي لها رقم سري واسم للمستخدم ولا يمكن لغيره الدخول إليها، وبعد إتمام كتابة الرسالة التي يقوم المستخدم بالضغط على أمر معين في الصفحة وهو(SEND) أي أرسل وفي حال تمام إرسال الرسالة يظهر على جهاز الحاسوب ما يفيد تمام العملية بنجاح، وإذا كان هناك خطأ ما يظهر للمرسل رسالة موجزة تشير إلى موضع الخطأ.

---

[1] يرجع الفضل في اختراع البريد الإلكتروني للعالم الأمريكي Ray Tomlinson في عام 1971 وهو مبرمج يعمل في شركة أمريكية ذات طاب حكومي، وكان أول مكتشفات تقنيات الانترنت، وقد أحدث هذا الاكتشاف ثورة حقيقية في عالم التليماتيك نظرا لحدوث تطور هائل نتيجة مزج وسائل الاتصال بالمعلومات، وما ينتج عنه من تأثير كبير في تبادل الرسائل، أشار إليه رشدي محمد علي عيد، مرجع سابق، ص 52.

[2] تم اكتشاف نظام الويب في سويسرا عام 1989 من قبل الاختصاصي في المعلوماتية الانجليزي Tim Berners وهومهندس اتصالات انجليزي الذي صمم برنامج اطلق عليه اسم World Wide WEB ويرتكز على فكرة تخزين المعلومات مع القدرة على إقامة صلات وعلاقات ترابطية مباشرة فيما بينها على غرار الترابط الحاصل في نسيج الشبكة التي يصنعها العنكبوت، ومن هنا جاءت تسمية الويب على هذا البرنامج الذي وزعه مبتكره مجانا عبر شبكة الانترنت في العام 1991، أشار إليه محمد عبيد الكعبي، مرجع سابق، ص 113.

يتيح البريد الالكتروني إمكانية نقل الرسائل بطريقة سريعة للغاية وكلفة المكالمة الهاتفية المحلية. وتتوافر في البريد الالكتروني عوامل الأمان والسرية، فلا يمكن اختراق البريد الالكتروني شخص إلا بمعرفة كلمة السر الخاصة به أومن خلال طرق فنية معقدة لا يجيدها إلا محترفي عمليات اختراق شبكات الحاسوب[1].

فهو خط مفتوح على كل أنحاء العالم يستطيع الفرد من خلاله إرسال واستقبال كل ما يريده من رسائل سواء كتابة أو صوتا أو صورة[2].

أما عن شبكة الويب العالمية والمعروفة بـ (www)[3] يمكن أن تعرف أنها "عبارة عن كم هائل من المستندات المحفوظة في شبكة الحاسوب، والتي تتيح لأي شخص أو لأي جهة الاطلاع على معلومات تخص جهات أخرى أو أشخاص آخرين قاموا بوضعها على هذه الخدمة"[4]. أي تتيح للمستخدم تصفح مواقع المعلومات وهذه الخدمة تجمع النصوص والصور والأصوات والأفلام المتحركة، مما يتيح للمستخدم الحصول على المعلومات التي يريدها في أسرع وقت.

الفرع الثاني
محركات البحث والتخاطب عبر الانترنت

محركات البحث هي عبارة عن برامج تساعد في الحصول على المعلومات، فكما هو معروف هناك كم هائل من المعلومات في شبكة الانترنت يرغب المستخدم في معرفة المواقع التي تمكنه من الوصول مباشرة إلى مبتغاه، فيتم في هذه الحالة إخبار خدمة البحث باسم

---

[1]- خدمة أخرى تلحق بالبريد الالكتروني على الانترنت تسمى القوائم البريدية، ويقصد بالقائمة البريدية " نظام إدارة وتصميم الرسائل والوثائق على مجموعة من الأشخاص المشتركين في القائمة – عبر البريد الالكتروني – وتغطي القوائم مواضيع ومجالات شتى وتتناول كل قائمة عادة موضوعا محددا. وحتى يمكن للمستخدم الانترنت الاشتراك في إحدى قوائم البريد الالكتروني فلابد أن يكون له صفحة وموقع في البريد الالكتروني حتى تتم مراسلته على ذلك العنوان، انظر عبد الفتاح بيومي حجازي، الأحداث والانترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2002 ، ص 23، 24. "

[2] محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دراسة مقارنة، الطبعة الثانية، دار النهضة العربية القاهرة، 2009 ص 110.

[3] World Wide WEB وتعني شبكة المعلومات الدولية والتي تختصر بـ www.

[4] بريستزن جرالا، مرشد الأذكياء الكامل إلى حماية جهازك أثناء التواجد على الانترنت، ترجمة خالد العامري، مروة السيد، دار الفروق، القاهرة، 1999، ص 154.

الموضوع الذي يهم المستخدم ومن ثم يتم تزويده بقائمة المواقع التي تتطابق مع المعلومات التي يرغب في الحصول عليها. وهناك عدة محركات بحث كل منها يستخدم طريقة معينة أوخاصة في إجراء عملية البحث[1].

أما عن التخاطب عبر الانترنت، فيقوم المستخدم في عملية التخاطب بكتابة رسالة يجري عرضها مباشرة أمام شخص آخر في أي مكان في العالم الذي يقوم بدوره بالرد مباشرة على هذه الرسالة.يشغل التخاطب عبر الانترنت مساحة كبيرة من حزمة البيانات التي يتم تبادلها بين مستخدمي هذه الشبكة العالمية، وبالرغم من أن التخاطب وسيلة اتصال إلا أنها الدافع الرئيسي لأكثر من 25 % من المستخدمين لهذه الشبكة. ومن مزايا التخاطب عبر شبكة الإنترنت : أنه نوع من الحوار الفكري الذي إذا تم بالشكل والأسلوب الصحيحين فإن سيؤدي إلى التبادل الثقافي بين الحضارات[2].

الفرع ثالث

المجموعات الإخبارية و التجارة الإلكترونية

مجموعات الأخبار عبارة عن أماكن وساحات افتراضية للقاء والتحادث بين مستخدمي شبكة الانترنت من ذوي الاهتمامات المشتركة، الذين يؤلفون فيما بينهم مجموعات نقاش وتبادل للبيانات والمعلومات والأفكار حول موضوع معين.[3]

ويعكس مدلول التجارة الالكترونية استخدام التقنيات الحديثة في المعلومات والاتصالات من أجل إبرام الصفقات وعقد المبادلات التجارية[4]. وقد أتاحت شبكة الانترنت لطرفي العقد التقابل وجها لوجه بالصوت والصورة رغم تباعدهما آلاف الأميال والاتفاق على التفصيلات الدقيقة بعد إبداء الإيجاب، ثم القبول بطريق الإنترنت، ثم إبرام العقد والتوقيع عليه بطريق التوقيع الالكتروني دون حاجة لاجتماع المتعاقدين في مكان واحد. وإبرام العقد يتم بعد أن يكون البائع أو المورد أو مقدم الخدمة قد أعلن عنها بصورة واضحة وكافية على شبكة الانترنت، حيث يكون الطرف الآخر قد اطلع على هذا الإعلان وحصل على الإيضاحات والتفسيرات المطلوبة بشأن السلعة ويمكن للمشتري أو المستورد أن يسدد قيمة بضاعته عن طريق الدفع بواسطة شبكة الانترنت ويكفيه في ذلك رقم حسابه البنكي ورقم بطاقة الائتمان الخاصة به.

ونمو التجارة الالكترونية يرتبط بمدى التقدم التكنولوجي، ولذلك فالدول المتقدمة معلوماتيا تقوم غالبا بدور المنتج، في حين تبقى الدول الناشئة في دور المتلقي لهذه التقنيات

---

[1] نهلا عبد القادر المومني، مرجع سابق، ص 40.

[2] نهلا عبد القادر المومني، المرجع نفسه، ص 40.

[3] محمد أمين الشوابكة، جرائم الحاسوب والانترنت، الجريمة المعلوماتية، الطبعة الرابعة، دار الثقافة للنشر والتوزيع، عمان الأردن، 2011، ص 42، أنظر أيضا نهلا عبد القادر المومني، مرجع سابق، ص 41.

[4] وليد الزيدي، القرصنة على الانترنت والحاسوب ، الطبعة الأولى، دار أسامة للنشر ، عمان، بدون سنة نشر، ص 59.

إذ تكون غالبا في عداد المستهلكين في شأن التجارة الالكترونية[1]. و لشبكة الانترنت خدمات أخرى، كبروتوكول نقل الملفات حيث تمكن هذه الخدمة المستخدم من نسخ الملفات من جهاز حاسوب إلى جهاز آخر، وعليه يستطيع الباحثون الحصول على أحدث الأبحاث العلمية من الجامعات ومراكز البحوث بسرعة كبيرة[2]. وعرفته المادة الثانية (2) من المرسوم التنفيذي 98-256 السالف الذكر أنه:" خدمة تعبئة الملفات عن بعد بصيغة نقطة إلى نقطة".

وحيث سبقت الإشارة أن للشبكة الدولية للمعلومات العديد من الخدمات التي تقدمها للبشرية جمعاء إلا أن لهذه الأخيرة أيضا العديد من المخاطر والمتمثلة في الجريمة المستحدثة، أو ما يعبر عنها بالجريمة المعلوماتية كأفضل تعبير.

الفصل الثالث
ماهية الجريمة المعلوماتية وأساليب ارتكابها

في إطار التصدي للسلوكات الإجرامية المستحدثة والمتمثلة في الجرائم المعلوماتية والتي تفطنت[3] لها جل التشريعات العربية والغربية واستحدثت لها نصوصا، وحرص مجلس أوروبا على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وتجلى ذلك في اتفاقية بودابست الموقعة في 23 نوفمبر 2001 المتعلقة بالجرائم المعلوماتية، إيماناً من الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على هذه الاتفاقية " بالتغيرات العميقة التي حدثت بسبب الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية.

والجدير بالذكر أيضا أن العديد من مشرعي دول كانت تشريعاتهم في مجال الجريمة المعلوماتية تتماشى مع مقتضيات اتفاقية بودابست ومن بينهم المشرع الجزائري، وما نود

---

[1] نهلا عبد القادر المومني، مرجع سابق، ص 41.

[2] نهلا عبد القادر المومني ، المرجع نفسه، ص 42، وأنظر أيضا شلباية مراد وفاروق علي، مقدمة إلى الانترنت، الطبعة الأولى، دار الميسرة للنشر والتوزيع، عمان، 2001، ص 20-21.

[3] كانت السويد هي أول الدول من سنت التشريعات الخاصة بجرائم الحاسب الآلي والانترنت، حيث صدر قانون البيانات السويدي عام 1973 ، تتبعها في دلك الولايات المتحدة الأمريكية حيث شرعت قانونا خاصا بحماية أنظمة الحاسب الآلي في سنة 1985، وفي هدا الخصوص أيضا كان للسودان قانون مكافحة تقنية المعلومات سنة2006 ، أيضا الإمارات العربية المتحدة من خلال القانون الاتحادي رقم 12 لسنة 2006 ، المشرع الجزائري من خلال القانون 05/04 وغيرها، أشارت إليه مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد 21 جوان 2012، ص 18 -19.

الإشارة إليه في هذا المقام هوأن النصوص المستحدثة في هذا المجال من طرف مشرعين كثر لا نظير لها في التشريع المصري[1].

وقد تم تخصيص فصل في هذه الدراسة لمفهوم الجريمة المعلوماتية ذلك أن هدف هذه الدراسة هو البحث في أشكال الاعتداء على الأسرار المعلوماتية. وتعتبر كل تلك الاعتداءات تقريبا جرائم معلوماتية لأن موضوع الجريمة المعلوماتية في الأساس هو المعلومات[2].

وكان ينبغي أيضا أن توضح بعض المفاهيم الضرورية في هذه الدراسة، والتي هي مضمون مفهوم الجريمة المعلوماتية (المبحث الأول) وأساليب ارتكابها (المبحث الثاني) باعتبارها جريمة تقنية فإنها بالضرورة ترتكب بوسائل فنية وتقنية تتناسب وطبيعة المعلومات محل الجريمة.

المبحث الأول
ماهية الجريمة المعلوماتية

كانت تستلزم دراسة ماهية الجريمة المعلوماتية، التعرض لمفهوم المعلوماتية باعتبارها ظاهرة اجتماعية وعلمية نشأت وازدهرت مع تقدم الحضارة الإنسانية وهي أحد النعوت التي تطلق على العصر الذي نشهده اليوم من جهة ومفهوم المعلومات كونها المحل الذي يقع عليه الاعتداء في الجريمة المعلوماتية من جهة أخرى، وهو الأمر الذي فصلنا فيه في الفصل الأول من الباب الأول لهذه الدراسة.

واستنادا على ما سبق، فإن المعلوماتية هي علم المعالجة الآلية للمعلومات أي المعلومات التي تمت معالجتها بوسائل آلية، فانطلاقا من العلاقة الموجودة بين المعلومات والتقنية المستحدثة في معالجتها للقول بأن المعلوماتية هي المعلومات المعالجة آليا باستخدام الحاسبات الآلية وأنظمتها[3].

تعتبر الحاسبات الآلية من المخترعات الحديثة التي تؤثر على الإنسان كيانا ونشاطا ولذلك فإنها تثير موضوع الحماية منها، أي حماية الإنسان وضمان حقوقه وحرياته الأساسية

---

[1] لا يوجد قانون خاص بتجريم الجرائم الإلكترونية في مصر كما أن قانون العقوبات المصري لم ينص هو الآخر على الجرائم المعلوماتية ولا يتناول موضوعها في أي مادة من مواده المتعددة غير أن هناك قانون الأحوال المدنية رقم 143 لسنة 1994 نص في بعض نصوصه على النظام المعلوماتي والجرائم المتصلة به في المواد(75-74-72) وهي مواد خاصة بالأحوال المدنية فقط فهي لا تسري على غيرها، فالمشرع المصري بحاجة إلى سن قانون يتعلق بالجريمة المعلوماتية.

[2] والمعلومات كما سبقت الإشارة أنها البيانات السرية المعالجة إلكترونيا وهي محل الحماية الجزائية وبالتالي فإن الاعتداء عليها بمختلف الأشكال يعد جريمة معلوماتية سواء المساس ما تعلق بسريتها أو سلامتها أو إتاحتها، مع العلم أننا نود دراسة أشكال الاعتداء الماس بالسرية فقط.

[3] مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2015، ص 28-29.

في مواجهة الغزو الذي تفرضه تلك الحاسبات على جوانب من النشاط الإنساني، حيث كانت تلك الحقوق والحريات إلى وقت قريب من المحرمات التي لا يجوز الإطلاع أو الاعتداء عليها.

إذن شيئا فشيئا أصبحت تظهر مشكلة الحسابات الآلية والتي تتمثل في تحقيق التوازن بين مصلحة المجتمع في الاستعانة بهذه التقنية الحديثة ومصلحة الإنسان في حماية حياته الخاصة والحفاظ على أسراره سواء هو أوأي شخص اعتباري، حيث أن هؤلاء فعلا تضرروا من جراء استخدام التقنية الحديثة بأشكال إجرامية مختلفة أدت بالعديد من الأشخاص الاعتبارية إلى الخسارة المادية والمعنوية على حد السواء[1].

إذ أن الملاحظ وبشكل جدي أن وسائل التقنية الحديثة خاصة الحاسب الآلي وشبكة الإنترنت والهاتف المحمول- خاصة المزود بتقنية البلوتوث- وكذلك الكاميرات المزودة بها تلعب دورا رئيسيا في ارتكاب هذه الجرائم وبالتالي، فقد حدث تطور نوعي ملحوظ في وسيلة ارتكاب الجريمة سواء تعلقت بالأموال أو الأشخاص أوالحياة الخاصة أوا لمال العام كلها أنماط ونماذج من الجرائم ترتكب حاليا عن طريق وسائل التقنية الحديثة.

وبخصوص العلاقة التي تربط الحاسب الآلي والجريمة المعلوماتية ولمزيد من التوضيح بخصوص اختيارنا للحاسب الآلي وتركيزنا عليه باعتباره الوسيلة الالكترونية الأهم في ارتكاب الجريمة المعلوماتية، وخاصة فيما يتعلق بالاعتداء على السرية المعلوماتية والسلامة والإتاحة فيما يتعلق بالبيانات، فلا يخفى على أحد مدى العلاقة الوثيقة بين استخدامات الحاسب الآلي وارتكاب الجريمة المعلوماتية.

وفي إطار معالجة ماهية الجريمة المعلوماتية سيتم ذلك من خلال تحديد مفهومها (المطلب الأول)، والتعرف على أطرافها ودوافع الجناة فيها(المطلب الثاني)، مع التطرق لتصنيف الجناة فيها اعتمادا على أحد التصنيفات الفقهية (المطلب الثالث).

المطلب الأول
مفهوم الجريمة المعلوماتية

لبيان مفهوم الجريمة المعلوماتية ولكي يتم رسم الصورة العامة لهذا البناء المعرفي يجب أن نتطرق لكل جزئياته فلابد من تعريفها (الفرع الأول)، والتعرف على سماتها الأساسية(الفرع الثاني)، كما أنه لابد من التطرق لمحل هذه الأخيرة باعتبار أن مجال هذه الدراسة هو المعلومات السرية (الفرع الثالث).

[1] مثلا اختراق أنظمة الأجهزة الأمنية والإطلاع على أسرارها واختراق أنظمة المؤسسات التجارية وسرقة أسرار التصنيع وغيرها.

الفرع الأول
تعريف الجريمة المعلوماتية

استخدمت من أجلها عدة مصطلحات للدلالة عليها وتحديد مفهومها، فهناك من يطلق عليها جرائم الحاسب الآلي وإساءة استخدام الحاسب الآلي، وهناك من يطلق عليها مصطلح جرائم الكمبيوتر أو الجرائم الإلكترونية، وهناك من يطلق عليها جرائم الحاسب الآلي والإنترنت، وهناك من يسميها بالجرائم المعلوماتية[1]، لهذا قال البعض أنها جريمة مستعصية على التعريف ويستدلون في ذلك بالمحاولات العديدة التي بدلت لتعريفها[2]، فلا يوجد تعريف موحد على الصعيد الدولي للجريمة المعلوماتية سبب الخلاف حول العناصر المكونة، لها ما جعل اللجنة الأوروبية الناظرة بمشاكل الجريمة المعلوماتية في المجلس الأوروبي، تترك لكل دولة من الدول المعنية، الحرية في وضع تعريف للجريمة المعلوماتية بما يتوافق مع نظام كل منها وتقاليده[3].

هذا الخلاف حول تعريف الجريمة المعلوماتية، جعل بعض الدول تفضل عدم وضع تعريف لجرائم المعلوماتية في تشريعاتها، تحسبا للتطور العلمي والتقني المستمر، ولعدم إمكان حصر قاعدة التجريم في نطاق أفعال معينة قد تتغير أو تتبدل في المستقبل، واكتفت في قوانين متعاقبة بتجريم أفعال الجريمة المعلوماتية بعد أن تصنفها تبعا لأهدافها. في حين هناك مشرعين في دول أخرى قد نحوا آخر وأتوا على تعريف صريح للجريمة المعلوماتية، وعلى هذا الأساس سنتعرض للتعريف الفقهي والتشريعي للجريمة المعلوماتية على النحو التالي:

---

[1] نحن من جهتنا نفضل تسميتها بالجريمة المعلوماتية لأنها تشمل الحاسب الآلي والانترنت وسائر المبتكرات التقنية الراهنة والمستقبلية المستخدمة في التعامل مع المعلومات كالهواتف الذكية مثلا فقط سبق وأشرنا أن الاعتداءات على المعلومات بواسطة الأجهزة الالكترونية المعادلة للحاسوب كالهاتف الذكي من الناحية القانونية تأخذ نفس التكييف خاصة بالنسبة للمشرع الجزائري حيث اعتبر الجريمة المعلوماتية جريمة ماسة بالأنظمة المعلوماتية وهذه الأخيرة تشمل النظام المعلوماتي للحاسوب والهاتف الذكي وممكن أن يكون هناك في المستقبل نظام معلوماتي لمبتكر آخر. في ذات الوقت نحن لسنا ضد تسمية الجريمة المعلوماتية بجرائم الحاسب ذلك لأن تلك المبتكرات على العموم هي كالحاسبات الآلية من حيث القدرات، وبخصوص جرائم الانترنت فارتباط الحاسب الآلي أوالهاتف الذي بالانترنت هوما يساعد الجاني على ارتكاب أخطر وجل الجرائم المعلوماتية.

[2] فتوح الشادلي وعفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت لبنان،2003 ، ص 31.

[3] رامي متولي القاضي، مكافحة الجرائم المعلوماتية، في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية القاهرة، الطبعة الأولى، 2011، ص 25.

أولا: التعريف الفقهي للجريمة المعلوماتية

نتناول فيما يلي بعض التعريفات الفقهية التي قيلت في تعريف الجريمة المعلوماتية بالنظر إلى اعتبار المعلوماتية كموضوع للجريمة أو كوسيلة لارتكاب الجريمة، وذلك على النحو التالي:

فباعتبار المعلوماتية كموضوع للجريمة عرفها البعض أنها" كل فصل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية "[1].

ويعرفها البعض أيضا أنها " كل فعل إجرامي متعمدة أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الفاعل "[2].

وعرفتها منظمة التعاون الاقتصادي والتنمية بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية " ويعرفها البعض الآخر، بأنها " سلوك غير مشروع يتعلق بالمعلومات المعالجة ونقلها "[3].

وعرفت أنها "جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات"[6]. وتبنى البعض تعريفا للجريمة المعلوماتية اقتراحاته مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية كأساس للنقاش في اجتماع عقد بباريس سنة 1983 لبحث الإجرام المرتبط بالمعلوماتية مقتضاه أنها:" كل سلوك غير شرعي أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها "[4] .

وهناك جانب من الفقه الجنائي من ذهب إلى تعريف الجريمة المعلوماتية بالنظر إلى اعتبار الحاسب الآلي كوسيلة لارتكاب الجريمة، إذ عرفها أنها:" أشكال السلوك غير المشروع الضار بالمجتمع الذي يرتكب باستخدام الحاسوب"، وقد عرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية " أنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا"[5]، ويعرفها البعض الآخر بأنها " نشاط إجرامي تستخدم فيه تقنية

---

[1] - فتوح الشاذلي، عفيفي كامل ، جرائم الكمبيوتر ، منشورات الحلبي الحقوقية بيروت لبنان ،2003، ص 32 .

[2] - فتوح الشاذلي، ص 32 عن محمد سامي الشوا ثورة المعلومات وانعكاساتها على قانون العقوبات دار النهضة العربية ، 1984، ص 6.

[3] - فتوح الشادلي، المرجع نفسه ،ص 32.

[6]– عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي ، الطبعة الأولى، دار الفكر الجامعي ، الإسكندرية ، 2006، ص33.

[4]- سامي علي حامد عياد، المرجع السابق، ص43.

[5] مدحت محمد عبد العزيز إبراهيم، مرجع سابق، ص 23.

الحاسب الآلي بطريقة مباشرة أوغير مباشرة كوسيلة أوهدف لتنفيذ الفعل الإجرامي المقصود "[1].

ويقصد بالجريمة المعلوماتية أيضا كل فعل غير مشروع يرد على الكمبيوتر أويتم استعماله، ويعرفها البعض أنها كل نشاط إجرامي يؤدي في النظام دور لإتمامه أو يقع على النظام نفسه[2].

وتعرف كذلك الجريمة المعلوماتية أنها ذلك النوع من الجرائم التي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها، كما تعرف بأنها" الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسب الآلي بعمل غير قانوني "، وهناك من يعرفها أنها " أي عمل غير قانوني يستخدم فيه الحاسب كأداة، أوموضوع للجريمة "[3].

وكتعريف شامل للجريمة المعلوماتية إلى جانب التعاريف السابقة، هناك من وضع تعريفا شاملا للجريمة الإلكترونية، يتمثل في تعريفها بأنها تتضمن كافة أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب أوالجرائم التي تلعب فيها البيانات التكنولوجية والبرامج المعلوماتية دورا رئيسيا". أو هي" أي فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية أونشا غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه، أو أية جريمة يكون متطلبا لاختراقها توافر لدى فاعلها معرفة تقنية الحاسب"[4]. وهناك جانب من الفقه يعرف الجريمة المعلوماتية، كما تعرف أيضا أنها:" استخدام غير مشروع للحسابات والتي تتخذ صورة فيروس يهدف إلى تدمير الثروة المعلوماتية"[5].

أوهي "كل فعل أو امتناع من شأنه الاعتداء على الأحوال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أوغير مباشرة عن تدخل التقنية المعلوماتية، أو سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[6] ،وهو التعريف الشامل حقيقة لمعنى الجريمة المعلوماتية بخلاف التعاريف السابقة.

ثانيا: التعريف التشريعي للجريمة المعلوماتية

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي ،مرجع سابق ص 17.

[2]- شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 12.

[3] - عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، ص232.

[4] رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011، ص 24.

[5]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، مرجع سابق، ص 18

[6] رامي متولي القاضي، المرجع نفسه، ص 24.

رغم خلو بعض التشريعات من تعريف الجريمة المعلوماتية[1] إلا أن هناك البعض من التشريعات من أشار إلى تعريفها كما هو الشأن بالنسبة للمشرع الجزائري من خلال المادة 1/2 من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[5]على" أنها كل الجرائم سواء المتعلق بالمساس بالأنظمة أو غيرها من الجرائم الأخرى التي ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو أي نوع آخر من نظم الاتصال الالكتروني".

ويمكن أن أشير في هذا المقام أن المشرع الجزائري بداية بموجب القانون 15/04 المعدل والمتمم لقانون العقوبات قد عبر عن الجريمة المعلوماتية بالجرائم ضد الأنظمة المعلوماتية على أساس أنه قد قدر بذلك أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي، فتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة. لذلك آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها.

وأما عن المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهو التعبير الذي استخدمه المشرع الجزائري للتدليل على الجريمة المعلوماتية[2]. فإنه وقبل صدور القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كانت الجريمة المعلوماتية في النظام العقابي الجزائري تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وهي وفقا لدلالة الكلمة تنصرف إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكة المعلومات وهذه الأفعال في الحقيقة ما هي إلا جزء من الظاهرة الإجرامية.

لأجل هذا فقد تبنى المشرع الجزائري حديثا بموجب القانون 04/09 تعريفا موسعا للجرائم المعلوماتية واعتبر أنها تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 07 أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على

---

[1] خلو معظم التشريعات من تعريف الجريمة المعلوماتية سببه هو تجنب المشرعين مسألة إيراد تعريف الجريمة المعلوماتية ولم يعاب عليهم ذلك لأن المشرع من جهة غير ملزم بإيراد التعاريف ومن جهة أخرى تعتبر الجريمة المعلوماتية ذات بعدين أحدهما قانوني والآخر فني، وهو ما يجعل تعريفها أمرا مستعصيا على المشرعين، والدليل أنه لم يعاب عليهم ذلك هو خلو ساحتهم من الانتقاد، أنظر في ذلك مدحت محمد عبد العزيز إبراهيم، مرجع سابق، ص 31.

[5]– المؤرخ في 14 شعبان عام 1430 الموافق لـ 5 أوت 2009 والذي دخل حيز النفاد بموجب الجريدة الرسمية العدد 47 الصادر بتاريخ 16 أوت 2009.

[2] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير في العلوم الجنائية، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012- 2013، ص 46 و47.

الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء بل توسع نطاقها لتشمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها.

من خلال ما سبق من تعريفات نستنتج أن الوسيلة الأكثر استخدما للجريمة المعلوماتية هي الحاسب الآلي وما يسهلها ويزيد من خطورتها هو ارتباطه بالانترنت ومنه نخلص إلى تعريف خاص بنا وهي أن الجريمة المعلوماتية هي: " كل فعل غير مشروع وغير قانوني يتم باستعمال الحاسب الآلي أو أي وسيلة معالجة آلية للمعطيات قام به شخص ما مستخدما معرفته وقدراته بالحاسب الآلي أو وسيلة المعالجة الآلية للمعطيات، واستخدام فيها الجهاز كأداة أو موضوع للجريمة ، سواء كان الجهاز مربوط بشبكات الاتصال أم لا".

الفرع الثاني
خصائص الجريمة المعلوماتية

وكما سبقت الإشارة أنه صاحب ظهور الحاسب الآلي تحديات جديدة للقانون الجنائي فظهرت طائفة من الجرائم المستحدثة التي اتخذت من الثورة المعلوماتية والتكنولوجية التي جاء بها الحاسب الآلي بايجابياته إذ لا يمكننا أن ننكر هذه الأخيرة بيد أن هذا الجانب المضيء سرعان ما تناوشته الظلمة، وذلك باستخدامه استخداما غير مشروع. وشكل ذلك انقلابا ربما يعطي تفسيرا لما نراه اليوم من النمو المتزايد والمطـــــــــرد للجرائم الإلكترونيـــــــــــة أو المعلوماتية، والتي اختلفت وتميزت عن الجريمة التقليدية في عدة نقاط سيرد التفاصيل فيها أدناه ولكن قبل ذلك لابد من الإشارة إلى ما يلي:

1- أن الاعتداء على الكيانات المالية للحاسوب يخرج عن نطاق جرائم الحاسوب لأن هذه الكيانات المادية محل صالح لتطبيق نصوص التجريم التقليدية الناظمة للجرائم الواقعة على الأموال[1].
2- أن محل جرائم الحاسوب هو دائما المعطيات إما بذاتها أو بما تمثله وقد تكون هذه المعطيات مخزنة داخل النظام أو على أحد وسائط التخزين أو تكون في طور النقل أو التبادل ضمن وسائل الاتصال المدمجة مع نظام الحوسبة[2].
3- أن المصلحة محل الحماية في هذه الجرائم هي الحق في المعلومات ككيان معنوي ذو قيمة اقتصادية عالية[3]، إذن فمحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها

[1] - سهيل محمد العزام، الوجيز في الجرائم الانترنت ، الطبعة الأولى، دائرة مكتبة الجامعة الأردنية، 2009، ص 79.
[2] - سهيل محمد العزام، المرجع نفسه ، ص 79.
[3] - سهيل محمد العزام، مرجع سابق، ص 79.

الواسعة (بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة، البرامج بأنواعها، المعلومات المستخرجة والمتبادلة بين النظم)[1] .

فنظرا لوقوع الجريمة المعلوماتية في غالبية الأحيان في بيئة المعالجة الآلية للبيانات حيث تكون المعلومات محل الاعتداء، ووقوع هذه الجريمة في بيئة المعالجة الآلية للبيانات يستلزم التعامل مع بيانات مجمعة ومجهزة لدخول الحاسب بغرض معالجتها الكترونيا بما يمكن المستخدم من إمكانية كتابتها في الحاسب الذي يتوفر فيه إمكانيات لتصحيحها وتعديلها ومحوها وتخزينها واسترجاعها وطباعتها وهذه العمليات وثيقة الصلة بارتكاب الجرائم ولابد من فهم الجاني لها كما تكون أيضا البرامج والبيانات محلا للاعتداء أو تستخدم وسيلة للاعتداء[2]، ومن هذا المنطلق تتميز الجرائم المعلوماتية عن نظيرتها التقليدية بالخصائص التالية:

أولا - أنها ترتكب من مجرم غير تقليدي وهي جرائم ناعمة:

يختلف المجرم مرتكب الجريمة المعلوماتية عن المجرم في الجرائم التقليدية ذلك لأن له سمات مختلفة عن غيره كما أن له طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لارتكاب الجريمة مختلفة عنه أيضا،[3] فسمات هذا المجرم عموما هو أنه إنسان اجتماعي، أي أنه متوافق مع مجتمعه وغالبا ما تكون له مكانة معتبرة فيه ويحظى بالاحترام منه، كما أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة في هذا المجال، أو عن طريق الخبرة والاحتكاك بالآخرين، كما أن هذا المجرم إنسان ذكي ويستغل ذكائه في تنفيذ جريمته ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا.

كما تعتبر الجريمة المعلوماتية جرائم ناعمة لا عنف فيها ولا وجود لجثث قتلى وآثار لدماء أو اقتحام من أي نوع، فإذا كانت الجرائم التقليدية تحتاج من مرتكبيها إلى قوة عضلية

[1] - علي جبار الحسناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، الأردن، الطبعة العربية، 2009، ص 32.

[2] - فتوح الشادلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية بيروت لبنان، 2003، ص 34.

[3] - سبق وأن شرحنا دوافع مرتكبي الجريمة المعلوماتية والتي كان من بينها التباري الفكري أو التنافس بين أصحاب المهارة أو الهواة وتجدر بنا الإشارة في هذا المقام إلى أنه يعتقد بعض المتخصصين في تقنية الحاسبات والمعلوماتية أن من مزايا مراكزهم الوظيفية ومهارتهم الفنية استخدام الحاسبات الآلية وبرامجها وتقنياتها لأغراض شخصية، أو للتباري الفكري فيما بينهم، أو ممارسة بعض الهوايات في فلك هذه التقنية، وهو ما يعبر عنه بأعراض النخبة ، وقد يدفع ذلك بعضهم إلى التمادي في استخدام نظم الحاسب الآلي بطريقة غير مشروعة قد تصل إلى حد ارتكاب الجرائم الخطرة.

لتنفيذها فإن هذه الجرائم لا تحتاج إلى مثل تلك القوة العضلية وإنما تحتاج إلى قوة علمية وقدر من الذكاء ومهارة في توظيف ذلك، والجاني في سبيل ذلك لا يحتاج من الوقت إلا ثواني أو دقائق معدودات، ولا يحتاج من القوة العضلية غير تحريك الأنامل من على وسائل الإدخال وقد يتسبب بذلك في حصول خسائر فادحة رغم أن جريمته لا ترى بالعين فنعومة هذه الجريمة وما تدره من أرباح ومن إشباع الفضول عند البعض، جعلها من الجرائم المغرية للمجرمين.

ثانيا-جرائم خفية وعابرة للحدود وصعبة الاكتشاف والإثبات:

أ-خفاء الجريمة: تتسم الجريمة المعلوماتية بأنها مستترة خفية في أغلبها حيث أن المجني عليه لا يلحظها غالبا مع أنها قد تقع أثناء وجوده على شبكة الانترنت ولكن لا يكون عالما بها ولا ينتبه إليها إلا بعد فترة من وقوعها وفي بعض الأحيان لا يكتشف أمرها[1]، وقد يتم اكتشافها بالصدفة البحتة، إضافة إلى أنها ترتكب في الخفاء ولا يوجد لها أثر كتابي في أغلب الأحيان ، مع العلم أن للجاني فيها قدرة عالية على تدمير ما قد يعتبر دليلا يمكن أن يستخدم لإدانته وذلك في أقل من ثانية واحدة[2]، وهذا ما جعل نسبة الجرائم المعلوماتية المكتشفة ضئيلة[3].

وتعتبر خفية أيضا لأن الجاني يتعامل مع نبضات إلكترونية غير مرئية لا يمكن قرائتها إلا بواسطة الحاسب كما أن توافر المعرفة الفنية لدى الجاني في مجال المعلوماتية يؤدي إلى صعوبة اكتشاف جريمته، وذلك بإتباعه لطرق وأساليب لا يفطن إليها المستخدم العادي للشبكة، ومن أمثلتها إرسال الفيروسات، سرقة البيانات الخاصة، التجسس وغيرها كما قد يدس بعض البرامج الخاصة وتغذيتها ببعض البيانات التي تؤدي إلى عدم شعور المجني عليه بوقوع هذه الجرائم[4].

ب - جرائم عابرة للحدود: حيث أن الانترنت وكما يشاهد الجميع ربطت العالم بشبكة الاتصال المتميزة والفعالة، قربت شعوب العالم بأجناسهم وثقافاتهم المختلفة من بعضهم بصورة لم تكن متاحة من قبل بأي وسيلة من وسائل الاتصال حتى كادت أن تلغي الحدود القائمة بين الدول بأن جعلت العالم قرية صغيرة.

واستخدام هده الشبكة الحديثة أدى إلى سلبيات تمثلت في انتشار الجريمة، وأصبحت الجرائم المستحدثة منتشرة بواسطة الانترنت والمشكلات المصاحبة لها، مشكلة عالمية لا تعترف بالحدود الإقليمية للدول ولا بالزمان، ولا بالمكان، وأصبح العالم بأجمعه ساحة لتلك الجرائم.

---

[1] محمد عبيد الكعبي، مرجع سابق، ص 38.

[2] - فتوح الشادلي، عفيفي كامل عفيفي، مرجع سابق، ص 35.

[3] يكون اكتشافها في الغالب بالصدفة لأسباب عدة سيتم التفصيل فيها خصائص الجريمة المعلوماتية أدناه.

[4] محمد عبيد الكعبي، المرجع نفسه، ص 38.

وفي مجتمع الانترنت تذوب الحدود الجغرافية بين الدول لارتباط العالم بالشبكة الواحدة، ومن الملاحظ أن أغلب الجرائم المرتكبة عبر شبكة الانترنت يكون الجاني في دولة والمجني عليه في دولة أخرى، ومن ذلك على سبيل المثال اختراق أنظمة الحواسيب الآلية من خارج إقليم دولة المجني عليه.

معناه أنه يمكن أن تقع الجريمة من جان في دولة معينة على مجني عليه في دولة أخرى في وقت يسير جدا مكبدة أفدح الخسائر، لاسيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت فإمكانية ارتكاب هذا النوع من الجرائم من خلال مسافات بعيدة قد تصل إلى دول وحتى قارات.

ج- صعوبة اكتشاف واثبات هذه الجرائم:

تقع هذه الجريمة على الكمبيوتر وشبكة الانترنت ونظمها[1]، وهي جريمة ناعمة ترتكب دون عنف وفي الخفاء ولا أثر خارجي لها وممكن تدمير أي دليل عليها في ثانية واحدة أو عدة ثوان.

وذلك أيضا لإحجام المجني عليهم[2] عن الإبلاغ عن هذه الجرائم في حال اكتشافها لما يؤدي إليه هذا الإبلاغ من عواقب وخيمة في مجتمع الأعمال الذي ينتمون إليه وحتى لا تهتز ثقة جمهور المتعاملين معهم. وقد يحاول الضحية حتى تضليل المحققين حتى لا يكتشفوا هذه الجرائم، إضافة إلى أنه يجب أن يكون لهؤلاء المحققين إحاطة واسعة بالتكنولوجيا الحديثة حتى يتمكنون من اكتشاف وإثبات هاته الجرائم.

فتتميز الجرائم المعلوماتية أيضا عن سائر الجرائم التقليدية بصعوبة إثباتها، ويرجع ذلك إلى عدة أسباب، من أهمها[3]:

1-انعدام الآثار التقليدية للجريمة

أغلب المجرمين يتركون أثرا يؤدي إلى اكتشافهم والعثور عليهم ولو بعد حين من الزمن أما الجرائم المرتكبة بواسطة الانترنت فلا تترك في الأغلب آثارا خارجية أو مادية تدل على الجريمة أو مرتكبها، فلا يوجد جثث لقتلى أو آثار لدماء.

2-عدم ترك هذه الجرائم لأي أثر خارجي بصورة مرئية والذي يمكن فهمه بالقراءة

[1] - فريد منعم جبور، حماية المستهلك عبر الانترنت ومكافحة الجرائم المعلوماتية (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010، ص 183.

[2] - للمجني عليهم في الجريمة المعلوماتية أيضا دور مهم إذ هو أيضا يعتبر ميزة تميزها عن الجريمة التقليدية، حيث يعتبر الضحية غالبا شخصية غير متجلية أمام الجاني ولا يرى هذا الأخير أمامه سوى الحسابات وما تحتويه أنظمتها من معطيات دون أن يدرك قيمتها وما قد تمثله في الواقع.

[3] محمد عبد الرحيم سلطان العلماء، جرائم الانترنت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث ،الطبعة الثالثة، 2004 ، ص 877.

أغلب البيانات والمعلومات التي يتم تداولها من حاسب آلي إلى آخر عبر الشبكة الانترنت تكون في هيئة رموز مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا بواسطة الحاسب الآلي ولا زالت الأجهزة المعنية في سبيل الجمع أو الكشف عن أدلة من هدا النوع لإثبات وقوع الجريمة والتعرف على مرتكبها تعاني الكثير.

3-إعاقة الوصول إلى الدليل بوسائل الحماية الفنية

الذين يرتكبون الجرائم الالكترونية أنفسهم بتدابير أمنية واقية تزيد صعوبة من صعوبة التفتيش عن الأدلة التي تؤدي إلى الإدانة ودلك باستخدام كلمات السر، أو دس تعليمات خفية لتصبح بينها كالرمز أوتشفير التعليمات باستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها غاية في الصعوبة.

4- سهولة إتلاف الدليل المادي وتدميره في زمن قياسي

يسهل غالبا على الجاني في ارتكاب الجرائم الالكترونية محو أدلة الإدانة في زمن قياسي بحيث لا تستغرق أكثر من ثوان معدودة، وذلك بتعريض البيانات المخزنة لديه على وسائط ممغنطة إلى مجال مغناطيسي قوي قادر على محوها في طرفة عين، أو تزويد الحاسب ببرامج من شأنها تدمير وتخريب البيانات في حال استخدامه من قبل شخص غير مرخص له.

ثالثا- هي جرائم فادحة الأضرار وذات أساليب سريعة التطور:

إن الاعتماد على الحاسب الآلي في إدارة مختلفة الأعمال في شتى المجالات ضاعف من الأضرار والخسائر التي تخلفها الجريمة المعلوماتية (الاعتداء على معطيات الحاسب الآلي)[1].

وتتميز الجرائم المعلوماتية خاصة جرائم الانترنت[2] بارتباطها بالتطور السريع الذي تشهده اليوم تكنولوجيا الاتصالات، مما يؤثر بدوره على مرتكب الجريمة وأسلوب ارتكابه لها من خلال تبادل الأفكار والخبرات الهدامة مع

---

[1] - محمد خليفة، مرجع سابق، ص 38.

[2] التفرقة بين جرائم الحاسوب والانترنت من خلال هذه التعريفات كالتالي:

إن جرائم الانترنت هي امتداد لما عرف بجرائم الحاسوب، والمقصود بجرائم الحاسوب: " كل عمل إجرامي غير قانوني يرتكب باستخدام الحاسوب كأداة أساسية، ودور الحاسوب في تلك الجرائم قد يكون هدفا للجريمة أوأداة لها". وعندما ظهرت شبكة الانترنت ودخلت جميع المجالات كالحاسوب، بدءا من الاستعمال الحكومي ثم المؤسساتي والفردي، كوسيلة مساعدة في تسهيل حياة الناس اليومية، انتقلت جرائم الحاسوب لتدخل فضاء الانترنت كأداة أساسية وكما هو الحال في جرائم الحاسوب، كذلك جرائم الانترنت قد تكون الانترنت هدفا للجريمة أوأداة لها.

والمقصود بجرائم الإنترنت في نظر البعض والمسماة أيضاً الجرائـــــم السيبرنـية أوالسبرانية ، هو:" أي نشاط غير مشروع ناشئ في مُكوّن أوأكثر من مكونات الإنترنت، مثل مواقع الإنترنت، وغرف المحادثة، أوالبريد الإلكتروني، ويمكن أن تشمل أيضاً أي أمر غير مشروع، بدءاً من عدم تسليم البضائع أوالخدمات، مروراً باقتحام الكمبيوتر (التسلل إلى ملفات الكمبيوتر)، وصولاً إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي (سرقة الأسرار التجارية)، والابتزاز على الإنترنت، وتبييض الأموال الدولي، وسرقة الهوية، وقائمة متنامية من الجرائم الأخرى التي يسهلها الإنترنت."، ولقد

العديد من المجرمين حول العالم عبر الشبكة الالكترونية وتطور التقنيات المستخدمة[1].

كما تبرز ذاتية الجرائم المعلوماتية بصورة أكثر وضوحاً في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعاً من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هوا لحال في جريمة القتل أو الاختطاف، أوفي صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة، فإن الجرائم المعلوماتية هي جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة.

وتحتاج كذلك إلى وجود شبكة المعلومات الدولية(الإنترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير كل ذلك دون حاجة لسفك الدماء، وبخصوص التفصيل في أساليب ارتكاب الجريمة المعلوماتية تفاديا للتكرار سيرد التفصيل فيها أدناه.

الفرع الثالث
محل الجرائم المعلوماتية (موضوعها)

كان الحاسب الآلي آلة هامة في حياة الإنسان وله كل القدر من الأهمية والفائدة التي سبق ذكرها، فإن هذا الأخير عبارة عن جهاز ضعيف أمام الإنسان لأنه- أي الحاسب الآلي- مصمم لتلقي الأوامر ولا يمكنه التمييز بين أمر وآخر، ولا يمكنه إدراك الغايات التي يصبو إلى تحقيقها الإنسان من خلال استعماله لهذا الحاسب، خاصة إذا كان مربوطا بشبكة الانترنت التي ساهمت بشكل كبير في تسهيل ارتكاب الجريمة بواسطة هذا الجهاز الذي أسهم بايجابياته العجيبة في حياة الإنسان وسلبياته الخطيرة في هدمها.

فالإنسان هو الذي صنع الحاسب الذي قد يستعمله في أغراض مشروعة ومفيدة كما قد يستعمله في أغراض غير مشروعة وخطيرة ، ولا يمكن للحاسب أن يميز بين هذا وذاك، وإنما يقوم بالوظيفة التي صنع من أجلها فهو بمكوناته المادية وغير المادية تحت سلطة وأمر

عرف الدكتور عبد الفتاح مراد جرائم الانترنت على أنها :" جميع الأفعال المخالفة للقانون والشريعة، والتي ترتكب بواسطة الحاسب الآلي، من خلال شبكة الانترنت، وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات سواء لارتكابها أو للتحقيق فيها " ، ويقصد بها أيضا : " أي نشاط غير مشروع ناشئ في مكون أوأكثر من مكونات الانترنت مثل مواقع الانترنت، وغرف المحادثة أو البريد الالكتروني"، كما تسمى كذلك في هذا الإطار بالجرائم السيبيرية أو السيبرانية، لتعلقها بالعالم الافتراضي، وتشمل هذه الجرائم على: أي أمر غير مشروع بدءا من عدم تسليم الخدمات أو البضائع، مرورا باقتحام الكمبيوتر- التسلل إلى ملفاته - وصولا إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي (سرقة الإسرار التجارية)، والابتزاز عبر الانترنت وتبيض الأموال الدولي وسرقة الهوية والقائمة مفتوحة لتشمل كل ما يمكن تصوره ، بما يمكن أن يرتكب عبر الانترنت من انحرافات ، كما تعرف بالجرائم التي لا تعرف الحدود الجغرافية، التي يتم ارتكابها بأداة هي الحاسوب الآلي عن طريق شبكة الانترنت وبواسطة شخص على دراية فائقة.مشار إليه على الموقع الالكتروني http://www.startimes.com/.

[1] محمد عبد الرحيم، مرجع سابق، ص 875

من يجلس أمامه ويقوم باستخدامه حتى وإن كان مجرما وتسمى الجريمة المرتكبة في هذه الحالة جريمة كمبيوتر (جريمة معلوماتية)، وهي نوع جديد من السلوكيات المنحرفة التي يتعرض لها كل من الحاسوب ومكوناته من خلال أشخاص مؤهلين وذوي خبرة علمية وعملية في كيفية التعامل معه، أو مع تلك المعطيات أو البيانات أو المستخرجات، ومن هذا التعريف نتصور أنه قد تكون المكونات المادية أو المعنوية محل تلك الجريمة المعلوماتية، كما قد يتصور وقوع هذه الجريمة من خلال الاستخدام غير المشروع للحاسوب.

والجدير بالذكر هنا أن العديد من الدارسين أكدوا أن الجرائم الواقعة على المكونات المادية للكمبيوتر تعتبر من قبيل الجرائم التقليدية وهو الموقف الغالب إذ أن الجديد في القانون الجنائي وفيما أثير من مشكلات حول المسؤولية الجنائية عن جرائم الكمبيوتر، إنما يتصل بالاعتداءات الموجهة إلى الكيانات غير المادية لنظام الكمبيوتر والتي عبر عنها بمعطيات الكمبيوتر (المعلومات)، إذا فإن وقوع الجريمة على المكونات المادية لا تثير مشكلة على أساس أنها تتمتع بالحماية الجزائية وفقا للقواعد العامة (قانون العقوبات) بخلاف المكونات المعنوية، رغم أن البعض يعتبرها ضمن جرائم الكمبيوتر ولكنه رأي غير متفق عليه والغالب هي جرائم تقليدية كما سبقت الإشارة.

إذن فموضوع الجريمة المعلوماتية أي محلها، يتمثل في المعطيات و المصلحة التي تهدرها والحق الذي تعتدي عليه هو الحق في المعلومات بذاتها، وبما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية أولها قيمة بذاتها كالبرامج [1].

فالمعلومات الالكترونية جديرة بالحماية حتى عن المعلومات الورقية، فتظهر جدارة المعلومات المبرمجة آليا بالحماية الجنائية عن المعلومات التي تحتويها الملفات الورقية من ضعف النوع الأول من المعلومات ومن أهميته في آن واحد، فالمعلومات المعالجة آليا ضعيفة داخل النظام عنها داخل الملفات الورقية. هذه الأخيرة يمكن إخفاؤها بسهولة عن المعلومات داخل النظام. كما أن المعلومات المعالجة آليا تتميز بالضخامة والتنوع، ومنها ما يتعلق بالحياة الخاصة للأفراد. كل هذه العبارات دعت مشرعي كثير من البلاد إلى استحداث صور من التجريم لحماية المعلومات داخل الكمبيوتر من الاطلاع عليها، بينما لا يوجد مثيل لتلك النصوص بالنسبة للمعلومات المسجلة داخل الملفات الورقية[2].

فمن اللافت للنظر أن المشرع يعلق أهمية واضحة على حماية نظام المعلومات بالكمبيوتر، الأمر الذي لم يوفره قانون العقوبات للملفات الورقية التقليدية التي تحتوي على معلومات من أهمية مماثلة.

---

[1] - علي حسن الطوالبة، مرجع سابق، ص 82.

[2] - Marise CREMONA JONATHAN HERRING, criminal law, ibid,p234.

أشارت إليه شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة، الاسكندرية، 2007، ص 94.

ويرجع السبب في ذلك إلى أن من يدخل نظام الكمبيوتر غالبا ما يكون قد اخل بحرمة المكان دون أن يقوم بدخول هذا المكان في حالات كثيرة. يضاف إلى ذلك أن نظام الكمبيوتر يتيح التعرف على كمية هائلة من المعلومات بسهولة ويسر وفي وقت قصير، الأمر الذي لا يتوافر في حالة الملفات الورقية التقليدية[1]. ورغم أن الدخول إلى النظام يعتبر أمرا بسيطا إلا أن الأضرار الناتجة عنه تعتبرا أمرا خطيرا، وتختلف طبعا الدوافع في ارتكاب هذا النوع من الإجرام تتباين بين المدادية والتنافسية وغيرها.

المطلب الثاني
دوافع مرتكبي الجريمة المعلوماتية وأطرافها

حيث أن الجريمة المعلوماتية أضافت شكلا جديدا من المجرمين و الضحايا، وحيث اصطلح على تسمية المجرم فيها بالمجرم المعلوماتي كما توسعت دائرة المتضررين من هؤلاء الجناة، و من خلال هذا المطلب نحاول التفصيل في كل من دوافع مجرمي المعلوماتية (فرع أول)و أطرافها (فرع ثان).

الفرع الأول
دوافع مرتكبي الجريمة المعلوماتية

إذن الدافع يشكل أحد الركائز في جميع الجرائم وبالنسبة للجرائم المعلوماتية فهي لا تختلف في وضعها العام عن التقليدية فثمة دوافع عديدة لمرتكبي جريمة المعلوماتية تحركهم لارتكاب أفعال الاعتداء المختلفة المشكلة لما يسمى بالجريمة المعلوماتية وتختلف هذه الدوافع من إنسان لأخر وتتمثل هذه الدوافع أساسا فيما يلي :

أولا: السعي إلى تحقيق الكسب المالي

يعتبر هذا الدافع أكثر الدوافع التي تؤدي إلى تحريك بالجناة إلى ارتكاب هذا النوع من الجرائم على وجه الخصوص وغيرها ذلك لأن حجم الربح الكبير الممكن تحقيقه من بعضها يتيح تعزيز هذا الدافع.

فقد تدفع الحاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الاطلاع على معلومات معينة أساسية وذات أهمية خاصة لمن يطلبها، ولذلك تتعدد الأساليب اللازمة للوصول إلى هذا الهدف المنشود[2]، حيث أنه قد تطلب بشأن تلك المعلومات مبالغ طائلة ولكن لا تعتبر كذلك بالنظر إلى الخسائر التي ستلحق أصحابها لوتم إفشاؤها.

[1] - شيماء عبد الغني محمد عطا الله، المرجع نفسه، ص 94.

[2] محمد علي العريان. الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص 66.

ثانيا:الانتقام من رب العمل وإلحاق الضرر به

هناك أثار سلبية في سوق العمل من جهة وفي البناء الوظيفي من جهة أخرى ، وقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى ويتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية، ومن طبيعة العلاقات العمل المنفرة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح لكنها في حالات كثيرة مثلث قوة محركة لبعض العاملين لارتكاب جرائم الكمبيوتر باعثها الانتقام من النشأة أورب العمل[1]، أي أن الحقد على رب العمل الدافع المحرك لارتكاب الجريمة.

ثالثا: الرغبة في قهر النظام والتفوق على تعقيد وسائل التنقنية[2]

وهناك دافع أقوى من شهوة الحصول على الربح وهو الرغبة في قهر النظام رغم أن السعي إلى تحقيق الربح يظهر دافعا أكثر تحريكا للمجرمين الكمبيوتر إلا أن الدافع إلى قهر النظام أيضا تجسدت لدينا نسبة معتبرة من تلك الجرائم الالكترونية خاصة ما يعرف بأنشطة المتطفلين، وهؤلاء ليسوا على جانب كبير من الخطورة الإجرامية وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوافر لديهم أية نوايا سيئة.[3]

رابعا: دوافع سياسية وتجارية

وهي عموما محرك أنشطة الإرهاب الإلكتروني فكثيرة هي المنظمات في عصرنا الحالي والتي تتبنى بعض الآراء والأفكار السياسية أو الدينية أو الإيديولوجية، ومن أجل الدفاع عن هذه الآراء تقوم بأفعال إجرامية ضد معارضيها.[4]

---

[1] - محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية (جرائم الكمبيوتر والانترنت)، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع ، مصر، 2010، ص 51.

[2] ومن أشهر القضايا التي وقعت في مثل هذه الحالة قضية كان قد تعامل معها مكتب التحقيقات الفدرالية أطلق عليها اسم مجموعة الجحيم العالمي تتلخص وقائعها في تمكن مجموعة من الأشخاص من اختراق مواقع البيت الأبيض والشركة الفدرالية الأمريكية والجيش الأمريكية ووزارة الداخلي الأمريكية، وقد أدين اثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة، وقد ظهر من التحقيقات أن هذه المجموعات تهدف إلى مجرد الاختراق أكثر من التدمير أوالتقاط المعلومات الحساسة، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها، مشار إلى هذه القضية لدى نسرين عبد الحميد نبيه، مرجع سابق، ص 85.

[3] محمد علي العريان، مرجع سابق، ص 65.

[4] - نسرين عبد الحميد نبيه، مرجع سابق، ص 45

فمثلا هناك العديد من عمليات الاختراق تعود لأسباب عقائدية، حيث يقوم بعض المجموعات التي تتبنَّى فكرة الإصلاح، بعملية رقابة أخلاقية أو اجتماعية أو دينيـــــــــة، فتتجسّس علـــــى المواقـــــع التـــــي تقـــــدِّم خدمات أو معلومات تتعارض مع قناعاتها، وتعمل على كشف أسرارها أو حتى تدميرها، فهناك بعض المواقع أخذ على عاتقه مهمة التجسّس على مواقع حكومية وكشف الأسرار الدبلوماسية والعسكرية[1]. أما عن دوافع الحصول على المعلومات التجارية بمختلف الأشكال فهي عموما دوافعها المنافسة.

الفرع الثاني
أطراف الجريمة المعلوماتية

من خلال ما سبق فإن الجريمة المعلوماتية هي جرائم نتجت عن التزاوج بين انفجار المعلومات وتطور وسائل الاتصال، فهي نوع جديد من السلوكيات المنحرفة التي يتعرض لها كل من النظام المعلوماتي ومكوناته من البيانات أو معطيات من خلال أشخاص مؤهلين وذوي خبرة علمية أو عملية في كيفية التعامل معه أو مع تلك المعطيات أوالبيانات أو المستخرجات، فهي كأي جريمة لابد لها من فاعل (جان) وواقع عليه الفعل (مجني عليه) وسيتم التفصيل فيهما كالتالي :

أولا:الجاني في الجريمة المعلوماتية

بالإضافة إلى الشروط العامة الواجب توفرها في مرتكب الجريمة المعلوماتية من سلوك منحرف (فعل) وعلم وإرادة في نتائج هذا السلوك، ينبغي أن يكون هذا الشخص على درجة معينة من العلم والخبرة في شؤون عالم الحاسوب وتقنية المعلوماتية[2]، وهذا يعني أنه لا يتصور أن يكون الجاني في الجريمة المعلوماتية إلا شخصا طبيعيا ذا أهلية وقدرة على أن يكون محلا لتوقيع العقوبة وهو الأمر الذي لا يتصور حدوثه إلا بالنسبة للشخص الطبيعي دون الشخص المعنوي، كما لا يتصور أن يكون الجاني هنا إلا شخصا ذا خبرة ودراية في علم الحاسوب سواء أكان مستخدما أو مبرمجا أو مجرد هاو أو محترف لجرائم الحاسوب

[1] http://www.lebarmy.gov.lb/article.asp?ln=ar&id=27286 يوم الاطلاع على الموقع 2015/05/10.

[2] - الفاعل في جرائم المعلوماتية: يتميز عن غيره من الجناة الآخرين في الجرائم التقليدية في العديد من الصفات أهمها أن يكون على درجة كبيرة من العلم والحرفية في مجال الحواسيب وشبكة المعلومات، كما يجب أن تكون له رغبة جامحة في تحدي كل ما هوجديد ومبتكر، حيث أن الإحصائيات العملية أفادت أن العديد ممن تم القبض عليهم من المجرمين المعلوماتيين أفادوا بمحاضر التحقيقات أنهم قاموا بتلك الجرائم رغبة منهم في تحدي وقهر الأنظمة المحوسبة، أويكون ذلك الفاعل (الجاني في الجريمة المعلوماتية) لديه طمع مادي مبالغ فيه فهؤلاء الجناة من هذا الصنف لا يرضون بالكسب غير المشروع القليل بل عيونهم دائما تكون مشرعه شطر الكسب الكبير جدا ولهذا نراهم لا يستهدفون إلا المؤسسات المالية الكبيرة وبنوك المال والمعلومات أيضا.

وتقنية المعلومات[1]، حيث تتوفر لدى الجناة مرتكبي جرائم المعلوماتية أو معظمهم مجموعة من السمات أو الخصائص، التي تميزهم عن غيرهم من الجناة أوالمتورطين في أشكال الانحراف والإجرام الأخرى وعلى هذا الأساس يمكن أن نلخص السمات التي يختص بها الجناة في الجريمة المعلوماتية وبإيجاز كالتالي[2]:

1. المهارة اللازمة عن طريق الدراسة، والخبرة المكتسبة في تكنولوجيا المعلومات والمعرفة الكاملة بمحيط الجريمة وظروفها والوسيلة التي يتزودون بها والقدرة على ابتكار الأساليب اللازمة والسلطة المباشرة أو غير المباشرة في الوصول إلى المعلومات والحصول على الشيفرة[3].
2. ارتفاع مستوى الذكاء، حيث يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية لأن ذلك ينتج منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي وارتكاب مختلف أشكال الجرائم .
3. خشية الضبط وافتضاح الأمر، لما يترتب على ذلك من ارتباك مالي وفقد للمركز والمكانة[4].
4. يفرق معظم مرتكبي جرائم المعلوماتية لاسيما الهواة منهم تفرقة واضحة بين الإضرار بالأشخاص العاديين الذي يعتبرونه غاية في اللاأخلاقية والإضرار بمؤسسة أوجهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم وهو ما لا يجدون غضاضة في تقلبه[5].

ثانيا: المجني عليه في الجرائم المعلوماتية

إذا كان الغالب الأعم بأن مرتكب الجريمة المعلوماتية لا يتصور أن يكون إلا شخصا طبيعيا، فإن المجني عليه هنا هو بالغالب الأعم شخص معنوي كالبنوك والشركات الكبرى والمؤسسات الحكومية والوزارات والمنظمات والهيئات المالية الضخمة، وغيرها من الأشخاص الاعتبارية التي تعتمد في انجاز أعمالها على الحواسيب[6].

وبالنسبة للأشخاص العاديين، فمن غير المستبعد أن يكونوا هم أيضا ضحية الجرائم المعلوماتية خاصة الذين يحفظون أسرارهم وأعمالهم وشؤونهم داخل الحاسوب خاصة الأشخاص الذين يكون لهم منصب سياسي رفيع أو رجل أعمال مرموق أو صاحب شهرة عالمية في قطاع من القطاعات الاقتصادية أو الاجتماعية أو العسكرية.

---

[1] - عامر محمود الكسواني، التجارة عبر الحاسوب، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 180-181.

[2] أيمن عبد الحفيظ، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، الناشر المؤلف، 2003، ص 243.

[3] - فريد منعم جبور، مرجع سابق، ص 189.

[4] - محمد عبد الله أبوبكر سلامه، مرجع السابق، ص 98.

[5] - محمد عبد الله أبوبكر سلامه، المرجع نفسه، ص 98.

[6] - عامر محمود الكسواني، مرجع سابق، ص 181.

وعلى الرغم من إمكانية تعرض الجميع للجريمة المعلوماتية سواء أكانوا أشخاصا معنوية أو طبيعية إلا أننا يمكننا الجزم بأن معظم الجرائم المعلوماتية ترتكب من أجل أمرين لا ثالث لهما وهما: المال والمعلومات، وبالتالي يمكننا الجزم أيضا بأن الغالبية العظمى من المجني عليهم[1] في الجرائم المعلوماتية هم إما مؤسسات مالية كالبنوك والمصارف وشركات الصرافة وإما شركات المعلومات يصرف النظر عن نوع هذه المعلومات وقيمتها إذ قد تكون بالغة الأهمية كالمعلومات العسكرية والمخابراتية وقد تكون معلومات رياضية أو اجتماعية بسيطة[2].

المطلب الثالث
تصنيف جناة الجريمة المعلوماتية

اتفق الباحثون على أن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء، ومن بين هذه التصنيفات لمجرمي التقنية هو تصنيفهم إلى ثلاثة طوائف وهي المخترقون(الفرع الأول)، المحترفون والحاقدون (الفرع الثاني).

الفرع الأول
المخترقون

كانت حقبة الستينات هي البداية في تاريخ ما يطلق عليهم المخترقون وقد تم تصميم برنامج UNIX الذي كان يعد أسرع البرامج في تلك الحقبة من الزمن، وكان من أشهر هؤلاء المخترقون (دينيس) و(ريتشي) و(كين تومسون) وبعد أن تم بنجاح إنتاج الكمبيوتر الشخصي بدأ عمل هؤلاء المخترقون في اكتشاف كيفيات عمل هذا الجهاز، وماهية البرامج التي ثبت عليه وكيفية اختراقه وتعتبر الفترة الزمنية من عام 1979 وعام 1989 هي العصر الذهبي لهؤلاء المخترقون.

أما عام 1983 فشهد القبض على أول عصابة من نوعها تتهم باختراق[3] أجهزة الحاسب الآلي. والمفاجأة أن أعضاء العصابة كانوا من المراهقين والتي أطلق عليها فيما بعد عصابة 414 ووجه إليها اتهامات باختراق 60 جهاز كمبيوتر من بينها معمل يقوم بتطوير الأسلحة النووية الأمريكية[4].

---

[1] - غالبية المجني عليهم في الجرائم المعلوماتية يتخذون الموقف السلبي وهوعدم القيام بالتصريح عن تعرض أجهزتهم ومعلوماتهم للاعتداء والتي يفترض فيها الأمان والسرية ويفضلون في غالب الأحيان السكوت عن ذلك الدخول غير المشروع أوالانتهاك، وهوالأمر الذي يشكل في حد ذاته سببا في ازدياد معدل الجرائم المعلوماتية وصعوبة الحد منها.

[2] - عامر محمود الكسواني، المرجع نفسه، ص 182.

[3] - محمد منير الجنيهي، ممدوح محمد الجنيهي، امن المعلومات الالكترونية ، دار الفكر الجامعي الاسكندرية، 2005، ص 29.

[4] - محمد منير الجنيهي، ممدوح محمد الجنيهي ، المرجع نفسه، ص 29.

وانتهت تلك المجموعات إلى مجموعتين فقط هم : مجموعة LOD ومجموعة MOD وسيتم التفصيل في هاتين المجموعتين في الفرع الخاص بالهاكرز.

فالمخترقون[1] هم أشخاص لهم القدرة على التعامل مع أنظمة الحاسب الآلي والشبكات بحيث تكون لهم القدرة على تخطي أي إجراءات أو أنظمة حماية اتخذت لحماية تلك الحسابات أو الشبكات فتشمل هذه الفئة نوعين من المخترقين أو ما يسمون بالمتطفلين إذ تم تصنيفها إلى نوعين الهاكرز، والكراكرز .

أولا: الهاكرز [2]

[1] وهاتين المجموعتين كانتا في الولايات المتحدة الأمريكية وما لبث أن بدأ التنافس بينهما إلى أن انقلب إلى حرب بين المجموعتين وقد أطلق على تلك الفترة التي اشتعلت فيها الحرب بين تلك المجموعتين من الهاكرز باسم حرب الهاكرز وقد امتدت إلى نحوأربع سنوات انتهت بعد جهد جهيد بالقبض على أفراد المجموعتين، وقد أصدرت الولايات المتحدة الأمريكية في عام 1986 قانون لمعاقبة الهاكرز بالسجن ولكنه أي القانون لم يظل الأحداث فقد قام روبرت موريس: وهو طالب متخرج حديثا من الجامعة بإطلاق أول دودة ذات نسخ ذاتي على نظام يونكس تعرض التجربة والاختبار وكان ذلك على شبكة الحكومة الأمريكية APPA NET ولكنه فقد السيطرة على الدودة لتنتقل إلى حوالي 6000 كمبيوتر على نفس الشبكة ليوضع روبرت تحت الملاحظة والمراقبة لثلاث سنوات وغرامة قدرها 10 آلاف دولار.أما أول قضية دولية في هذا الشأن فكانت من نصيب ألمانيا الغربية عام 1989 بعد اتهام أربعة من الهاكرز الألماني (انتحر أحدهم قبل القبض عليه) باختراق أجهزة حكومية أمريكية وسرقة المصدر البرمجي لنظام تشغيل وبيعه للاتحاد السوفياتي. وقد برزت مجموعات من الهاكرز بعد ذلك وبدأ التنافس بين تلك المجموعات في اختراق كافة أنواع أجهزة الحاسبات.

=وفي عام 1993 فاز ثلاثة من الهاكرز بسيارتي بورش ورحلة مجانية و20 ألف دولار بعد مشاركتهم في مسابقة ما تعنيه قاموا فيها باختراق الخطوط الهاتفية ومنع أي مكالمات من الوصول إلا مكالماتهم هم وتم سجنهم جميعا وكان من بينهم الأسطورة **كيفن بولسن** الصحفي المتعاون مع صحف كثيرة في مجال الكمبيوتر والانترنت.

وفي عام 1995 تم فيها اعتقال أشهر هاكر كيفن ميتنك وبقي 4 سنوات من دون محاكمة في السجن وفي التوقيت نفسه استطاع هاكرز من دولة روسيا سرقة 10 ملايين دولار من (سيتي بانك) أكبر بنك تجاري في الولايات المتحدة وتقريبا في العالم.وفي عام 1998 تم إطلاق برنامج التجسس الشهير باك أورافيس في مؤتمر ديفكون السنوي أما أكدت الأشهر في العام نفسه فهو سرقة برمجيات سرية من أجهزة وزارة الدفاع الأمريكية وقادت التحقيقات لمراهقين أمريكيين أحدهما يهودي والذي ترأس بعد ذلك إدارة إحدى الشركات التكنولوجية.وبعد إصدار ويندوز 98 وما تلاه من مناقشات، وفي 1989 شهد اكتشاف ثغرات كثيرة لنظام التشغيل الأسهل والأكثر شعبية في العالم لتجد الشركات سوقا جديدا لتسويق منتجات ضد الاختراق.فأولى الحروب الدولية على الانترنت شهدها عام 2000 عندما اندلعت حرب الكترونية بين العرب والمسلمين ضد اليهود وكان نتيجتها اختراق وتعطيل الكثير من المواقع الإسرائيلية كما واجهت الهند مصيرا مشابها من قبل الهاكرز الباكستانيين.

وفي العام نفسه استطاع الهاكرز اختراق شبكة عملاقة البرمجيات مايكروسوفت وسرقة المصدر البرمجي لمنتجات كبيرة مثل ويندوز وأوفيس كما كان هذا العام أول ظهور لهجمات الإغراق POPS ATTACKS والتي نجحت في تعطيل مواقع ياهووأمازون وسي أن وغيرها، أما عام 2001 فشهد =اختراقات DNS والتي استطاع من خلالها الهاكرز حجب موقع شركة مايكروسوفت عن ملايين المستخدمين لمدة يومين وكذلك الحرب الأمريكية الصينية وراح ضحيتها الكثير من المواقع والشبكات، راجع في ذلك الموقع الالكتروني http://mtnsh.com/12547 يوم 2016/09/27.

[2] - يذكر أنه تعرض 26 موقعا حكوميا في ثلاث دول هي الولايات المتحدة الأمريكية وبريطانيا، وأستراليا لاختراقات الهاكرز في نهاية يناير عام 2001 وتدور في موقع يسمى (اثرينشون) بالانترنت أن أعضاء جماعة (ينتجارد) قاموا باختراق تلك المواقع الحكومية في نفس الوقت ووضعوا نفس الرسالة التي تشمل مضامين جنسية كما هي عادتهم حين يفعلون مثل هذه الأعمال التي يعدونها للتسلية فقط، وأوضح أحد المسؤولين بالموقع المذكور والمعروف بتتبعه لمثل هذه الحالات، أنه من غير العادة أن يقوم الهاكرز باختراق عدد كبير من المواقع الحكومية في دول مختلفة ذات تواقيت مختلفة أيضا في نفس الوقت، مشيرا إلى ما قاله الخبراء الأمنيون على الشبكة لأن الهاكرز أصبحوا يعملون وفق تخطيط محكم

الهاكر هو اللفظ العربي للكلمة الانجليزية(hacker) وهي تحمل عدة معان، إلا أننا في هذه الدراسة نحن معنيون بمعنى واحد وهو المخترق أو الهاتك.

فالهاكر هو شخص بارع في استخدام الحاسب الآلي وبرمجته، ولديه فضول في استكشاف حاسبات الآخرين وبطرق غير مشروعة، فالهاكرز وكما يدل اسمهم هم متطفلون يتحدون إجراءات أمن نظم الشبكات، لكن لا تتوفر لديهم في الغالب دوافع حادة أو تخريبية وإنما يطلقون من دوافع التحدي وإثبات الذات[1]، وتتألف هذه الطائفة أساسا من المراهقين وشباب (طلبة وتلاميذ ثانويات) وشباب عاطل عن العمل، وهو شخص يتمتع بتعليم لغة البرمجة وأنظمة التشفير الجديدة، ويستمتع أيضا بعمل البرامج أكثر من التشغيل وهو شخص يؤمن بوجود أشخاص آخرين يستطيعون القرصنة ويستطيع أن يصمم ويحلل البرامج أو أنظمة التشغيل[2].

إذن هم أشخاص لهم قدرة فائقة على اختراق الأجهزة والشبكات أيا كانت إجراءات وبرامج وتدابير الحماية التي تم اتخاذها إلا أنهم لا يقومون بأي من الإجراءات التي تؤدي من تم اختراق جهازه أوشبكته[3]، وقدرتهم على اختراق كافة الشبكات تمكنهم من الإبحار في عالم البيانات دون أهمية لحواجز كلمات المرور أو الشفرات[4].

وقد صنفت إحدى أهم شركات حفظ أمن المعلومات في أمريكا الهاكرز بأنهم ثلاث نماذج :

1-المتشردون وهم عادة ما يكونون كالأطفال في أعمالهم.

2-المستغلون أو ذو القبعة السوداء وهم الذين يعملون من أجل الربح الشخصي أومن أجل الثأر وتأكيد مواقف سياسية.

وتنسيق جماعي وللعلم أن هذه الجماعة مشهورة في أوساط الهاكرز. مشار إليه لدى عبد الفتاح بيومي حجازي، نحوصياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، الطبعة الأولى منشأة المعارف الإسكندرية ، 2009، ص 34.

[1] - ويطلق علي هذه الفئة أيضا اسم الهواة وهم أشخاص عاديون، وغالبا يتمتعون بالثقة ، ويحوزون معرفة معلوماتية بدرجة أوبأخرى، ورغم أن هؤلاء الهواة يواجهون بعض المشاكل المهنية والشخصية، لعدم العثور على العمل المناسب، والمشاكل المالية بسبب نقص النقود التي في حوزتهم لإنفاقها في شراء مستلزمات المعيشة المختلفة ، وحل هذه المشاكل يمثل الباعث الأساسي لهؤلاء الأشخاص لارتكاب جرائمهم، ولقد ساهمت التكنولوجيا في جذب طائفة من الهواة الذين يستمتعون باللعب والمزاح أمام الحاسب الآلي أكثر من محاولة إلحاق أي ضرر عن طريق هذه التكنولوجيا. ومرتكبو هذه الأفعال في الغالب هم من الطلبة أوالشباب الحائز عن معرفة جيدة في مجال المعلوماتية، ويحاول إثبات مهاراته وقدراته عن طريق اكتشاف أو إظهار مواطن الضعف في أحد الأنظمة دون إلحاق أي ضرر به، وفي الغالب أيضا فإن هؤلاء الهواة لا يملكون وسائل مالية ذات شأن يذكر، وإنما يعتمدون بالدرجة الأولى على معرفتهم في مجال المعلوماتية، أشار إليه فهد سيف بن راشد الحوسني، جرائم التجارة الالكترونية، دراسة مقارنة،السحاب للنشر والتوزيع سلطنة عمان، 2010، ص 229.

[2] - عبد الصبور عبد القوي على مصدي، الجريمة الالكترونية، دار العلوم للنشر والتوزيع، ص 55، الطبعة الأولى، 2008، ص 40-41.

[3] - منير محمد الجنيهي، مرجع سابق، ص 28 .

[4] رشدي محمد علي محمد عيد، مرجع سابق، ص 74.

3-ذو القبعات البيضاء وهم الذين يعملون من أجل أغراض البحث.[1]

وقد ضايق الهاكرز الجيش الأمريكي عندما تصاعدت الأزمة في الخليج، لقد قال وزير الدفاع الأمريكي بأن الهاكرز استطاعوا الدخول إلى مناطق محظورة واستطاعوا تثبيت مفاتيح كي تمكنهم من الوصول للمعلومات في وقت لاحق. وقد أعلن مكتب التحقيقات الفيدرالي بأن مخترقي أنظمة الكمبيوتر هم الأكثر خطورة على الولايات المتحدة وأن أمريكا تواجه تهديدات كبيرة بسبب الهجوم على بنيتها الإلكترونية مما يسبب خطر أكبر حتى من أي مواجهة محتملة[2].

فقال رئيس المركز الوطني لحماية البنية التحتية في أمريكا وهو المخول إليه الحماية من التجسس الالكتروني بأن خارقي أنظمة الكمبيوتر يرون في نظام دفاع حكومة الولايات المتحدة هو الامتحان الأخير لهم وأقصى تحدي لاختبار مهاراتهم. وأضاف بأن كثير من الحوادث كان السبب فيها هم الشباب الصغار وهؤلاء كان أثر اختراقهم تافه ولكن حذّر من الأعداء ذو المهارات العالية لأن عملهم خطير[3].

ثانيا: الكراكرز

الكراكرز أو المقتحم هو شخص يقوم بالتسلل إلى نظم الحاسوب للاطلاع على المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها، ولقد تم استعمال هذا المفهوم الجديد سنة 1985 من طرف الطائفة الأولى طائفة الهاكرز للرد على الاستعمال السيئ للصحفيين لمصطلح الهاكرز. ولقد استفادة هذه الطائفة كثيرا من التقنيات التي طورتها فئة الهاكرز وبدؤوا يستخدمونها استخداما سيئا في اعتداءات تتم على ميولات إجرامية، فالمقتحمين يتميزون بصفة وهي تبادلهم للمعلومات فيما بينهم[4].

ويطلق على هذه الفئة أيضا اسم القراصنة المخادعين وهؤلاء يحدثون أضرارا كبيرة على الصناعات وعلى أنظمة المعلومات لأنهم يؤلفون نوادي لتبادل المعلومات فيما بينهم وهي الميزة التي سبق وأشرنا إليها وهم يقسمون أيضا على أساس جرائمهم إلى:

1 - المخادعون :

وهم أشخاص يتمتعون بقدرات عالية باعتبارهم من المتخصصين في المعلوماتية، ومن أصحاب الكفاءات وتنص جرائمهم في أغلبها على الأموال، والتلاعب في حسابات المصارف والمؤسسات المالية والاقتصادية ولديهم القدرة الفائقة على إخفاء الأدلة التي من الممكن أن تختلف عن جرائمهم[5].

---

[1] - منير محمد الجنيهي،ممدوح محمد الجنبيهي، مرجع سابق، ص 32 .

[2] - منير محمد الجنيهي،ممدوح محمد الجنبيهي، المرجع نفسه ، ص 32 .

[3]- منير محمد الجنيهي،ممدوح محمد الجنبيهي، مرجع سابق، ص 32.

[4]- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف الإسكندرية، 2008، ص41.

[5]- محمد حماد مرهج الهيثي، مرجع سابق، ص 136.

2 - الجواسيس :

وهؤلاء مهمتهم خلاف مهمة الفئة السابقة، إذ أن مهمتهم استخبارية، تقتصر على جمع المعلومات لمصلحة الجهات التي يعملون لحسابها، سواء كانوا يعملون لمصلحة دولهم أو لمصلحة بعض الأشخاص أوالشركات التي تتنافس فيما بينها، ومن مقتضيات عملهم أن لا يتركوا دليلا عن عملهم. لذلك فهم يتمتعون بالصفات التي يتمتع بها أعضاء الفئة السابقة من كونهم أشخاص من أصحاب الكفاءات ويتمتعون بقدرة عالية على التعامل مع الحاسب الآلي، إلى جانب قدرتهم على طمس الأدلة التي تتخلف عن جرائمهم[1].

ويعرف الجاسوس" بأنه الشخص الذي يقوم بمجموعة من الأعمال المنجزة لصالح بلد أجنبي تهدف إلى إيقاع الضرر بسلامة بلد آخر، وتكون غالبا معلومات سرية عن الجيوش أو أجهزة المخابرات وسواها، وذلك بطرق ملتوية ومخالفة للقانون، مما يعرضه لعقوبات قاسية".[2] كما ورد تعريف للجاسوس في القانون الدولي العام أنه" هو الشخص الذي يعمل في خفية، أو تحت ستار مظهر كاذب في جمع أو محاولة جمع معلومات عن منظمة الأعمال الحربية لإحدى الدول التجارية بقصد إيصال هذه المعلومات لدولة العدو"[3]. والملاحظ على هادين التعريفين هو اقتصار التجسس على الأسرار العسكرية فقط بينما مفهوم التجسس يتعدى ذلك إذا ما تعلق الأمر بمعلومات الكترونية سرية فلا تقتصر على العسكرية فقط بل تتعدى ذلك لكل أنواع المعلومات السرية الالكترونية كما سيرد التفصيل أدناه في المبحث الخاص بجريمة التجسس الالكتروني.

الفرع الثاني
المحترفون والحاقدون

تعتبر فئة المحترفين أخطر طوائف مجرمي المعلوماتية حيث تهدف اعتداءاتهم إلى تحقيق الكسب المادي لهم وللجهات التي كلفتهم وسخرتهم لارتكاب جرائمهم كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي، وإلى تحقيق جانب المعرفة التقنية المميزة والتنظيم العالي. ويتصف هؤلاء الطائفة بالتكتم، فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ويحاولون قدر الإمكان عدم كشف طرقهم التقنية لارتكاب جرائمهم، وبشأن أعمارهم فأشارت الدراسات إلى أنهم الشباب الأكبر سنا مقارنة بالطائفة الأولى فتتراوح أعمارهم ما بين 25 و40 سنة[4].

---

[1]- محمد حماد مرهج الهيثي، المرجع نفسه، ص 137.

[2] القاموس القانوني الثلاثي، قاموس قانوني موسوعي، شامل ومفصل عربي- فرنسي-انجليزي، موريس نخلة وآخرون، منشورات الحلبي الحقوقية، سوريا، 1992، ص 614.

[3] علي صادق أبوهيف، القانون الدولي العام، الطبعة السابعة، منشأة المعارف الإسكندرية، 1965، ص 846.

[4] - نسرين عبد الحميد نبيه، مرجع سابق، 42.

أما عن الحاقدون، فهم طائفة يغلب عليها عدم توافر أهداف وأغراض الجريمة المتوفرة لدى الطائفتين المتقدمتين فهم لا يسعون إلى إثبات القدرات التقنية والمهارة وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية. إنما يحرك أنشطتهم الرغبة بالانتقام والثأر كثأر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي النظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم.

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يشقى الواحد منهم في الوصول إلى كافة عناصر المعرفة المتعلقة بالفعل الذي ينوي ارتكابه، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم أو إتلاف كل بعض معطياته أو نشاط إنكار الخدمة تعطيل النظام أو الموقع المستهدف إن كان من مواقع الانترنت. وليس هناك ضوابط محددة بشأن أعمارهم، كما لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة، ولا يفاخرون بأنشطتهم بل يعمدون على إخفائها وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد على ذلك[1].

هذه إذن أصناف مجرمي المعلوماتية والذين يسلكون خطورة تكمن خطورتهم في قدرتهم على اختراق الأنظمة التقنية والفنية التي توضع لحماية المعلومات، وفي كونهم أيضا ممن يعملون داخل المؤسسات وممن يعملون في مجال إدارة وتشغيل الحاسب الآلي، وتكمن خطورتهم في أن الذي يعمل في المؤسسة قد يجعل أي نظام من أنظمة الحماية التي تستخدمه المؤسسة عديم القيمة والنفع، لأنه على دراية به وبأسلوب عمله، ذلك يشجعهم على ارتكاب جرائمهم أولا وسهولة وصولهم إلى ما يبغون كونهم ممن يتعاملون مع الحاسب الآلي ثانيا، الأمر الذي لا يجعل الشكوك تحوم حولهم لأي سبب وكون فرصهم أكبر من غيرهم سواء بالدخول إلى المعلومات السرية أو الاطلاع على الأسرار التجارية فيسهل عليهم ارتكاب جرائمهم، وإخفاء الأدلة التي تدينهم مما يشكل صعوبة في اكتشافهم، وفي ذلك تكمن خطورتهم[2].

وبشكل عام فإن المجرم المعلوماتي تكون غايته البحث عن معلومات يمكنه استخدامها كوسيلة لتنفيذ جرائمه وتتمثل عموما مميزاته بأنه:

- يتميز المجرم المعلوماتي بقدرته العالية والفنية في مجال تقنية الحاسب الآلي.

[1] - نسرين عبد الحميد نبيه، مرجع سابق، ص 43.

[2] - محمد حماد مرهج الهيثي، مرجع سابق، ص 140.

- قدرتهم العالية على التحرك عبر حدود الدول دون قيود بفضل قدرتهم على اختراق أنظمة الحاسب الآلي في مختلف البلدان عبر ما توفره لهم شبكة الاتصالات العالمية للانترنت.
- إن مرتكبي هذه الجرائم قد يكون الدافع إليها غرض شخصي كالتيار الفكري بين مرتكبيها لاسيما تعتمد على مقدار الإلمام بتقنية الحاسب الآلي، ويكون مجال التياري بينهم هو قدرة مجرم معلوماتي ما دون غيره على اختراق أنظمة الحماية التي يتمتع بها برنامج معين.
- في الكثير من الأحيان تتركز نشاطاتهم الإجرامية على الاعتداء على الحقوق المالية للأفراد والشركات والمؤسسات المالية والاقتصادية، فهم مجرمون يسببون أضرارا اقتصادية ومالية باهظة دولية ومحلية هذا ما تكشف عنه معظم الإحصائيات الجنائية في هذا الإطار وهؤلاء المجرمون دوافعهم مختلفة كما سبق الشرح. إذن الدافع في الجريمة المعلوماتية يختلف من جريمة لأخرى، حسب الحق الذي تنال منه الاعتداء أو المصلحة التي تتعرض لها فمثلا الدافع الذي يدفع الجناة لارتكاب جرائمهم عند المؤسسات والشركات المالية والاقتصادية الغالب فيه هو الإضرار بهذه الشركات والحصول على نفع مادي سواء بالمتاجرة بأسرارها الصناعية أو الاعتداء على حقوقها في الإنتاج أو الاعتداء على ذمتها المالية، ولكن دوما كما يقال الأمور تقاس بالغالب لأن الغالب أن المجرم المعلوماتي من خلال جرائمه يسعى لتحقيق الكسب المادي رغم أن هناك دوافع أخرى كالانتقام وغيره وسيتم التفصيل في الجرائم المعلوماتية خاصة ما يتعلق منها بالاعتداء على الأسرار المعالجة آليا.

فالجرائم المعلوماتية هي التي تستهدف المعلومات، فهي أنماط السلوك الإجرامي التي تطال المعلومات المخزنة أو المعالجة في نظام الكمبيوتر أو المتبادلة عبر الشبكات، لهذا هي ترتكب بوسائل معلوماتية تتماشى مع التطور المستمر للتقنيات المستحدثة، وكان لزوما التعرض لبعض هذه الوسائل ببعض من التفصيل على النحو الوارد أدناه.

المبحث الثاني
أساليب ارتكاب الجرائم المعلوماتية[1]

[1] إضافة إلى الاختراق و الفيروسات التي تعتبر أساس القيام بالجرائم المعلوماتية و الاعتداء على سرية المعلومات هناك أيضا بعض الطرق الفنية التي ترتكب بواسطتها الجرائم ضد السرية المعلوماتية من بينها ما يلي:

- **تزييف رسائل البريد الإلكتروني:**لقد شاعت عملية تزييف رسائل البريد الإلكتروني، وذلك حتى تبدو صادرة من شخص آخر، نظرا لاتساع شبكة الانترنت وصعوبة التحقق من الشخصية الحقيقية لمرسل البريد الإلكتروني، وأكثر الطرق كفاءة للتعرف على شخصيته هي الاستعانة بطرق ثالث مستقل وموثوق به يسمى " سلطات الإجازة " والتي يمكن من

تتنوع الوسائل التي تستخدم للعدوان على الأسرار المخزنة في الحاسوب فإضافة إلى الاطلاع عليها بمجرد فتح الحاسوب فهناك تقنيات غالبا ما تستعمل من طرف مجرمي التقنية الحديثة لأنه عموما تؤمن هذه الأسرار بواسطة تقنيات لتأمينها من الانتهاك، حيث أصبح من السهل انتهاك هذه السرية إذ انتشرت في الفترة الأخيرة الكثير من الكتب التي تتيح معرفة مختلف الأساليب والتقنيات التي يمكن استعمالها لانتهاك سرية المعلومات وتلك التقنيات[1] هي كالتالي:

المطلب الأول
الاختـــــــــــراق

خلالها الحصول على " التوقيع الرقمي " و" العنوان الرقمي " وإتمام تشفير الاتصال وتتحقق سلطات الإجازة من شخصية المستفيدين وتجيزها عن طريق تبادل بعض المعلومات الشخصية التي لا يعرفها إلا الطرفان (السلطة المجيزة والمستفيد) كما تقوم بتسجيل الرسائل المتبادلة للتحقق منها لاحقا، كما تستخدم بعض برمجيات التحقق لتتبع مصدر الرسائل والتأكد من صحته ، لكن هذه الطريقة ليست مضمونة تماما، لأن المجرم إذا توصل إلى الحاسب الشخصي للمستفيد الحقيقي وكانت لديه المعلومات الكافية لاستخدام كلمة المرور الصحيحة أمكنه ذلك من خداع سلطات الإجازة وانتحال شخصية المستفيد الحقيقي.

- **إخفاء الشخصية على الإنترنت:** يحتاج المجرم كثيرا من إخفاء شخصيته، كمن يقوم بإرسال خطاب تهديد عبر الانترنت وبما أن هذه الأخيرة تحتوي نظاما آليا يضع عنوان المرسل في مقدمة كل جزاء الرسالة المرسلة عبر الشبكة، فإن المجرم يتجاوز هذا النظم عن طريق تغيير عنوان المصدر لبروتوكول الانترنت (IP) الذي يظهر في مقدمة أجزاء الرسالة ليستبدل به عنوانا آخرا مغلوطا، بحيث يصبح تتبع المصدر الأصلي للرسالة عملية صعبة أو مستحيلة، ويطلق على هذه العمليات اسم IP Spoofing ، وأحيانا يختار المجرم عنوانا لجهاز خاص يستطيع الوصول إليه واستخدامه حتى يستطيع معرفة رد فعل الضحية ومدى استجابته للتهديد، لكن ويوما بعد يوم تزداد هذه العمليات صعوبة بما فيها تعديل بروتوكولات الاتصال بشبكة الانترنت واستخدام توقيع طرف ثالث.

- **الإغراق بالرسائل:** لا تقتصر وسائل الإضرار بمعطيات الحاسب الآلي على الفيروسات وحدها، فهناك طرق أخرى كالإغراق بالرسائل، وهذه الطريقة تقوم على إرسال كم هائل من الرسائل عبر البريد الالكتروني لأجهزة الحاسب الآلي لمستخدم واحد أو للعديد من المستخدمين، والتي يراد تعطيلها وتوقيفها عن العمل، ولا يشترط في تلك الرسائل أن تكون ذات محتوى معين، غير أنه لابد أن تكون محملة بملفات كبيرة الحجم وكفيلة باستغراق المساحة المحددة للبريد الالكتروني هذه الرسائل ترسل مرة واحدة في وقت واحد تقريبا، فتعمل على توقف الجهاز على الفور نظرا لما تسببه من ملء منافذ الاتصال وكذلك ملء قوائم الانتظار، وليست هناك فائدة يرجوها من يقومون بهذا الإغراق في أغلب الأحيان غير إبراز تفوقهم وإظهار قدراتهم على التأثير على أجهزة أخرى.

وقد بدأت هذه العملية في عام 1996 عندما أرسلت إحدى الشركات إعلانات عنها بالبريد الإلكتروني إلى الآلاف من مواقع الانترنت، فتم تعطيل الشبكة فضلا عن تكليف متلقي هذه الرسالة كثيرا ودفعهم ثمن مدة الاتصال اللازمة لاستقبال هذه الرسائل مع ما يصاحبها من ملفات، وتجري حاليا محاولات من جانب شركات نظم المعلومات لتطوير برامج تتعامل مع هذه الحالات باستقبال جزء محدود من الرسائل عندما يحدث سيل مفاجئ منها حتى لا تنقطع الخدمة، راجع في ذلك محمد خليفة، مرجع سابق، ص 56-58.

[1] الأساليب الواردة في هدا المبحث هي أهم الوسائل المستخدمة حاليا في انتهاك سرية المعلومة والوارد أنه يمكن تطويرها يوما بعد يوم فمن الممكن ظهور أساليب أخرى في أي وقت ربما حتى بعد حين، ودلك للتطور السريع في مجال التكنولوجيا الحديثة.

رغم أننا ندين لمن اخترعوا أبجديات الشبكة العنكبوتية "الانترنت" إلا أننا بتنا نخاف من هتك سرية معلوماتنا، حيث أن هتكها أو اختراقها بات هاجسا يخافه الجميع، هذا من جهة ومن جهة أخرى فإن الاختراق أساس جل جرائم الاعتداء على السرية المعلوماتية.

فالاختراق والمخترقون أو الهاكرز كلمة تخيف كثير من الناس، وخصوصا مستخدمي الانترنت الذين يطمحون إلى حماية أسرارهم من هؤلاء الهاكرز، وكثيرا ما تكون عملية الاختراق عشوائية، بمعنى أن المخترق لا يعرف جهاز أحد الأشخاص بعينه ويقوم باختراقه.

الفرع الأول
تعريف الاختراق

عرف الاختراق في القانون العربي النموذجي الموحد في شأن جرائم إساءة استخدام تقنية المعلومات بأنه: " الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية"، ونحن من جهتنا نود الإشارة فقط إلى أن الاختراق كسلوك فني لا يعني جريمة الدخول غير المصرح به للنظام المعلوماتي كما يخلط بينهما البعض ولكننا يمكن أن نعرفه أنه سلوك فني يترتب عليه الدخول غير المصرح به للنظام المعلوماتي[1].

ويعرف الاختراق أيضا أنه عمليات غير شرعية تتم عن طريق فتحات موجودة في النظام يستطيع المخترق من خلالها الدخول إلى جهاز الضحية من أجل إتمام غرض معين يسعى إليه المخترق[2].

إن عملية الاختراق الالكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الانترنت وهي عملية تتم من أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات المعلوماتية ولا تزال نسبة كبيرة من الاختراقات لم تكتشف بعد بسبب التعقيد الذي تتصف به نظم تشغيل الحاسبة الالكترونية والشبكات المعلوماتية[3].

فالاختراق بشكل عام هوالقدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة بالهدف، فالمخترق لديه القدرة على دخول أجهزة الآخرين عنوة دون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية أو نفسياتهم فما الفرق بين مخترق الأجهزة الشخصية ومقتحم البيوت الآمنة[4].

---

[1] لتأكيد ما قلناه يمكن أن نسمي الاختراق الاقتحام أو التسلل.

[2] http://ar.wikipedia.org يوم الاطلاع على الموقع 2016/03/15.

[3] علي عدنان الفيل، الإجرام الالكتروني، منشورات زين الحقوقية، ص 87، أشارإليه موزة المزروعي، الاختراعات الالكترونية خطر كيف نواجهه مجلة آفاق اقتصادية،الإمارات العربية المتحدة،العدد 9 ، 2000 ص 54.

[4] نسرين عبد الحميد بنية، مرجع سابق، ص 143.

الفرع الثاني
أنواع الاختراق ووسائله

يعتبر الاختراق أهم وسائل ارتكاب الجريمة المعلوماتية وقد يطال الأجهزة والوسائل الفنية المؤمنة لتلك الأجهزة وغيرها وسنحاول إيجاز ذلك كالتالي:

أ- اختراق المزودات" مزودات الخدمة" أو الأجهزة الرئيسة للشركات أو المؤسسات أو الجهات الحكومية، وذلك باختراق الجدران النارية التي عادة ما توضع لحمايتها، وغالبا ما يتم ذلك باستخدام المحاكاة وهي مصطلح يطلق على عملية انتحال شخصية للدخول إلى النظام[1].

ب- التعرض للبيانات أثناء انتقالها والتعرف على شفرتها إن كانت مشفرة وهده الطريقة تستخدم في كشف بطاقات الائتمان وكشف الأرقام السرية للبطاقات البنكية[2].

ت- اختراق الأجهزة الشخصية، وهي الطريقة الأكثر شيوعا نظرا لتوفر العديد من برامج الاختراق سهلة الاستخدام[3].

ويحتاج التسلل إلى جهاز الضحية دون علمه إلى مجموعة من الأدوات والوسائل الخاصة، فهذه الأخيرة قد تكون بعض البرامج الموجودة داخل نظام التشغيل نفسه أو بعض البرامج التي صممت خصيصا لتسهيل عمليات الاختراق وتجنب استخدام العديد من الأوامر المعقدة[4]، ومن أهم أساليب الاختراق ما يلي:

1- الاختراق عن طريق استعمال نظم التشغيل : [5]

لأن نظم التشغيل مليئة بالثغرات، فإنه يتم استغلالها في عمليات الاختراق، ولكن الأهم هو القيام بذلك عن طريق البروتوكولات[6]التي يستخدمها النظام للتعامل مع شبكة الإنترنت أو الشبكات الداخلية بأنواعها.

ويمر المتسلل بعدة مراحل حتى يتمكن من اختراق الحاسب الآلي لغيره وهي :

يبحث المخترق أولا عن ضحيته، وذلك بمعرفة رقم (IP) الخاص به والبحث عن هذا الرقم يتم بمجموعة من الخطوات يقوم بها المخترق على جهازه، لكن يجب كذلك أن يكون

---

[1]- نسرين عبد الحميد نبيه، المرجع نفسه،ص 145.

[2] -نسرين عبد الحميد نبيه، المرجع نفسه،ص145 ، أنظر أيضا محمد خليفة، مرجع سابق، ص 41.

[3]- محمد خليفة، المرجع السابق، ص 41.

[4] -محمد خليفة، مرجع سابق، ص 41.

[5] -محمد خليفة، المرجع نفسه، ص 42.

[6] - البروتوكولات هي مجموعة من القواعد التي تستخدمها أجهزة الكمبيوتر للاتصال مع بعضها البعض عبر الشبكة. والبروتوكول هو وجود اتفاقية أو ضوابط أو لقياسية التي تمكن من الاتصال، والاتصالات، ونقل البيانات بين نقاط النهاية الحوسبة في أبسط أشكالها، يمكن تعريف بروتوكول تكون القواعد التي تحكم بناء الجملة، ودلالات، وتزامن الاتصال قد تكون البروتوكولات التي تنفذها الأجهزة والبرامج، أو مزيج من الاثنين معا. عند أدنى مستوى، وهو بروتوكول يعرف سلوك أجهزة اتصال عن http://ejabat.google.com

متصلا بجهاز الضحية عن طريق شبكة الإنترنت أو شبكة داخلية، وذلك في لحظة معينة، لأن هذا الرقم يتغير دائما مع كل اتصال جديد بالانترنت.

بعد تحديد رقم IP يحدد المخترق إمكانية اختراق جهاز الضحية عن طريق مجموعة من الخطوات ورقم "اللآي بي" رقم ديناميكي متغير، فهو يتغير في كل مرة يدخل الشخص على شبكة الانترنت[1].

"فالآي بي" IP هو بمثابة البطاقة الشخصية للمستخدم على شبكة الانترنت، يمنحه مزود الخدمة للمشترك آليا بمجرد طلب الخدمة ليمكنه من الولوج إلى الشبكة العالمية وينتج عن الآي بي معرفة بعض المعلومات الشخصية عن المستخدم في عالم الانترنت، كنوع من البريد المرسل والمواقع التي قام بزيارتها وغرف المحادثة التي قام بالدخول إليها، وذلك في سجل خاص لدى مزود خدمة الانترنت وهو ذا أهمية بالغة إذ أنه يعتبر من الأمور المهمة والمساعدة في عملية الاختراق، فهويشبه إلى حد كبير رقم الهاتف المنزلي، فعندما يريد شخص الاتصال بآخر، يقوم بطلب رقم هاتفه المنزلي ليستطيع الاتصال به أو التحدث إليه، كذلك رقم الآي بي فعندما يريد شخص أن يخترق جهاز شخص آخر فلا بد له من معرفة رقم الأي بي، حتى يتسنى له إدخال إحدى البرامج المتخصصة في عملية الاختراق ليتمكن من الاتصال بجهازه[2].

2- الاختراق باستخدام البرامج :

لابد لقيام الاختراق بهذه الطريقة من وجود برنامجين، أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم server لأنه بمثابة الخادم الذي يأتمر بأوامر المخترق وينفذ المهام الموكلة إليه داخل جهاز الضحية وثانيهما برنامج يوجد بجهاز المخترق ويسمى ببرنامج المستفيد العميل client، وأشهر مثال على هذه البرامج وأخطرها هو برنامج حصان طروادة ، فهو يتمتع بمجموعة من المميزات تجعل الأقدر على عملية الاختراق دون القدرة على كشفه وتتبعه والقضاء عليه[3].

برنامج حصان طروادة في أبسط صوره، يقوم بتسجيل كل ما تقوم بكتابته على لوحة المفاتيح منذ أول لحظة للتشغيل، وتشمل كل البيانات السرية أو الحسابات المالية أو المحادثات الخاصة على الانترنت أو رقم بطاقة الائتمان الخاصة أوحتى كلمات السر التي تستخدمها للولوج إلى الشبكة العنكبوتية[4]، والتي قد يتم استخدامها بعد ذلك من قبل الجاسوس الذي قام بوضع البرنامج على الحاسب الشخصي للضحية[5].

---

[1] محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، الإسكندرية ، 2003، ص 137.

[2] مصطفيى الشقيري، مرجع سابق، ص341-342.

[3] محمد خليفة، مرجع السابق، ص 42 .

[4] مصطفى الشقيري، مرجع سابق، ص 346.

[5] يوسف أبوالحجاج، أشهر جرائم الكمبيوتر والانترنت، دار الكتاب العربي، القاهرة، الطبعة الأولى، 2010، ص 134.

ويتم إرسال هذا البرنامج إلى جهاز الضحية بعدة طرق، لعل أشهرها إرسال بالبريد الإلكتروني، إذ يقوم المخترق بإرسال رسائل إلى الضحية يرفق بها ملفا يحمل حصان طروادة، ليقوم الضحية بفتحها وتحميل الملف المرفق على أنه أحد البرامج المفيدة، ليكتشف بعدها أنه لا يعمل، فيظن أنه به عطلا ليقوم بإهماله، فيحتل حصان طروادة مكانه داخل النظام ويبدأ مهامه التجسسية، وحتى لو قام الضحية بحذف البرنامج فلا فائدة من ذلك، إذ يكفي أن يعمل هذا البرنامج لمرة وحدة فقط حتى يقوم بمهامه[1].وهناك طرق أخرى لإرسال هذا الملف، كاستخدام برامج الدردشة مثل برنامج ICQ أوMSN أو YAHOO MESSENGER .

3- تشمم كلمات السر جمعها والتقاطها[2]:

إذا كانت أنشطة الاعتداء التي تتم باستعمال كلمة السر تتم غالبا فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوع اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسري أومحيط العمل أو حياتهم الشخصية، فإن الجديد استخدام برمجيات يمكنها تشمم أو التقاط كلمات السر خلال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة، بحيث يقوم هذا البرنامج من حيث الأصل بجمع أول 128 بايت أو أكثر مثلا من كل اتصال بالشبكة التي تجري مراقبتها تتبع حركة الاتصال عليها. وعندما يطبع المستخدم كلمة السر أو اسمه، فإن البرنامج (الشمام) يجمع هذه المعلومات وينسخه إضافة إلى أن أنواعا من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطه معا، كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها[3].

4- المسح والنسخ :[4]

هو أسلوب يستخدم فيه برنامج الماسح وهو برنامج احتمالات يقوم على فكرة تغيير التركيب أوتبديل احتمالات المعلومة، ويستخدم تحديثا بشأن احتمالات كلمة السر أو رقم هاتف الموزع أو نحو ذلك، وأبسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصول إلى احدها الذي يستخدم موزع للاتصال بالإنترنت،

---

[1] محمد خليفة، مرجع سابق، ص 43.

[2] محمد خليفة، مرجع سابق، ص 44- 45.

[3] ففي واقعة حدثت في بريطانيا تمكن تلميذ في الخامسة عشرة من عمره من الوصول إلى معظم الملفات السرية المخزنة بحاسوب إحدى الشركات الكبرى التي تدير نظاما للمشاركة الزمنية في خدمات الحاسب الآلي عن طريق الحصول على كشوف نظام تشغيل البرامج وتحليلها إلى أن توصل إلى اكتشاف الرموز التعريفية الخاصة بالمشتركين المتمثلة في كلمات السر التي تتيح لهم الدخول إلى النظام مما أتاح له ذلك الاطلاع على الملفات السرية المخزنة والقدرة على تعديلها. أشار إليه PETER SWIFT , HACK MAN MENACE OF THE KEYBOARD CRIMINAL BRITICH TELECOM WORLD MAG ,HALF OF SEPT 1989 P 13-14

[4] محمد خليفة، مرجع سابق، ص 44.

أو إجراء مسح لاحتمالات عديدة لكلمة سر للوصول إلى الكلمة الصحيحة التي تمكن المخترق من الدخول للنظام، ومن جديد فإن هذا أسلوب تقني يعتمد واسطة تقنية هي برنامج الماسح بدلا من اعتماد على التخمين البشري.

5- هجومات استغلال المزايا الإضافية[1]:

الأمر هنا يتصل بواحد من أهم استراتيجيات الحماية فالأصل أن مستخدم النظام – تحديد داخل المؤسسة – يحدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، ولكن في الواقع العملي يحدث أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك أو دون علم من الشخص نفسه أنه يحظى بمزايا تتجاوز اختصاصه ورغباته. في هذه الحالة فإن أي مخترق للنظام لن يكون قادرا فقط على تدمير معطيات المستخدم أو التلاعب بها، من خلال اشتراكه أو عبر نقطة الدخول الخاصة به وبكل بساطة سيتمكن من تدمير مختلف ملفات النظام حتى تلك غير المتصلة بالمدخل الذي دخل منه لأنه استثمر المزايا الإضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله، وأعظم مثال على هذا الخطر في العالم المادي أنه يمكن شخص من دخول غرفة مدير فندق لقصد سرقته فيجد في غرفته مفاتيح كافة قاصات الأمانات، أو مفتاح الماستر الذي يفتح غرفة الفندق جميعها.

ولهذا فتحديد الامتيازات والصلاحيات قد يمنع في حقيقته من حصول دمار شامل ويجعل الاختراقات غير ذات أثر.

6- استراق الأمواج[2]و الهندسة الاجتماعية:

فيتم استراق الأمواج ذلك باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم باختلاف أنواعه كالتقاط موجات شاشات الكمبيوتر الضوئية أو التقاط الموجات الصوتية من أجهزة الاتصال.

أما عن الهندسة الاجتماعية فهي أسلوب من أساليب الاختراق التي تعتمد على العنصر البشري وليس لها أية أبعاد تقنية بحيث يستمل فيها أساليب الخداع والكذب للحصول على معلومات ذات طابع تقني حتى أن أشهر الهاكرز كيفن ميتينك ذكر في كتاب ألفه بعنوان "فن الخداع " أن أكثر الاختراقات التي قام بها كانت باستخدام هذا الأسلوب[3].

وفي هذه الطريقة يحصل المخترق على معلومات تهيئ له الاختراق من خلال علاقات اجتماعية وذلك باستغلال الشخص أحد عناصر النظم – أشخاصه – بإيهامه بأي أمر يؤدي إلى حصوله على كلمة مرور أوعلى أية معلومة تساعد في تحقيق اعتدائه، كأن يتصل شخص بأحد العاملين ويطلب منه كلمة سر النظام تحت زعم أنه من قسم الصيانة أو قسم

[1] محمد خليفة، مرجع سابق، ص 45.

[2] محمد خليفة، المرجع نفسه، ص 46.

[3] حسين بن سعيد الغافري، مرجع سابق، ص 341 -342.

التطوير أو غير ذلك، وطبيعة الأسلوب الشخصي في الحصول على معلومة الاختراق سميت بالهندسة الاجتماعية[1].

7- التفتيش في مخلفات التقنية[2] وانتحال شخصية الأفراد[3]:

التفتيش في مخلفات التقنية هو القيام بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة بحثا عن أي شيء يساعده على اختراق النظام، كالأوراق المدون عليها كلمات السر، أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة، أو الأقراص الصلبة المرمية بعد استبدالها، أو غير ذلك من المواد المكتوبة أو الأقراص أو الملاحظات أو أي أمر يستدل منه على أية معلومة تساهم في الاختراق، وقد حدث أن بيعت من قبل وزارة العدل الأمريكية مخلفات أجهزة تقنية بعد أن تقرر إتلافها، وكان من ضمنها نظام كمبيوتر يحتوي قرص الصلب على كافة العناوين الخاصة ببرنامج حماية الشهود، وبالرغم من أنه لم يتم فعليا استثمار هذه المعلومات، إلا أن مخاطر كشف هذه العناوين استدعى إعادة كافة الشهود وتغيير مواطن إقامتهم وهوياتهم وهو ما ألحق تكلفة مالية باهظة.

بينما انتحال شخصية الأفراد هو قيام شخص باستخدام شخصية إنسان آخر للاستفادة من سمعته مثلا أو ماله وصلاحياته هذا الانتحال يمكنه القيام بذلك عن طريق المعلومات التي تتعلق بتلك الشخصية، كالاسم والعنوان ورقم الهوية مثلا ويستغلها استغلالا سيئا، والتي يحصل عليها من الإنترنت ويمكن أن تؤدي هذه الجريمة إلى استنزاف رصيد الضحية في البنك أو السحب من البطاقة الائتمانية أو الإساءة إلى سمعة الضحية وقد تكون وسيلة المجرم إلى ارتكاب جريمة النصب، مستفيدا من السمعة الطيبة لتلك الشخصية أو شركة قد استغرقت السنوات الطوال لبناء تلك السمعة. وكثيرا ما يقوم المجرم بتغيير العنوان البريدي للضحية إلى عنوانه لكي يستقبل بنفسه الفواتير والمطالبات التي قد تنبه الضحية إلى أي شيء مريبا يحدث، وفي إحدى القضايا تم انتحال شخصية امرأة من كاليفورنيا. وبعد القبض على المجرم لم تتمكن الضحية من الحضور إلى المحكمة للإدلاء بشهادتها، لأن المحكمة أرسلت إليها استدعاء على عنوان المجرم وليس على عنوانها هي.

وتعتبر وسيلة انتحال الشخصية من أسهل الطرق المستحدثة في الدخول إلى أنظمة الحاسب الآلي [1] وهناك وسيلتان لانتحال الشخصية هما:

---

[1] محمد خليفة، مرجع سابق، ص 46.

[2] محمد خليفة، المرجع نفسه، ص 46.

[3] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص 61.

[2]– أيمن عبد الحفيظ عبد الحميد سليمان، استراتيجية مكافحة جرائم استخدام الحاسب الآلي، بدون ناشر ، بدون طبعة ، 2003، ص 131 مشار إليه لدى ريتشارد مانسفيلد، ترجمة خالد العامري، دار الفاروق للنشر والتوزيع، القاهرة، 2001، ص 46.

1-انتحال الشخصية باستخدام التقنيات غير عالية الكفاءة أو ما يطلق عليها الانتحال للشخصية بدائيا فقط، ويتم ذلك عن طريق استخدام المجرم لبطاقة أو كارت خاص بشخص مسموح له بالدخول وهذا النوع يعتبر بسيط من الناحية التقنية على الرغم مما يسببه من إخطار ونتائج ضارة[2].

2-انتحال الشخصية باستخدام التقنيات العالية، أو ما يطلق عليه التنكر الالكتروني بحيث ينتحل الشخص شخصية آخر باستخدام اسم هذا الشخص عن طريق إرسال بريد الكتروني مدعيا انه شخص آخر وهي من أسهل أنواع التنكر الالكتروني[31].

8- انتحال شخصية المواقع [2]:

هذا الأسلوب يعتبر حديثا نسبيا بين الجرائم المعلوماتية، ولكنه الأشد خطورة والأكثر صعوبة في اكتشافه من انتحال شخصية الأفراد، ويقوم الفاعل بهذه الجريمة من خلال وضع نفسه في موقع بيني بين البرنامج المستعرض Browser للحاسب الخاص بأحد مستخدمي الانترنت وبين الموقع Web ومن هذا الموقع البيني يستطيع حاسب المجرم أن يتصرف وكأنه صاحب الموقع الحقيقي، ويستطيع مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه كما يستطيع سرقة هذه المعلومات أو تغييره، ولكن القيام بهذه العملية حتى لوتم الاتصال بالموقع من خلال ما يسمى بالنظم الاتصال الآمنة.

وكل ما يحتاجه من يقوم بهذه العملية هو السيطرة على أحد المواقع التي تتم زيارته بكثرة وتحويلها ليعمل كموقع بيني، وتحتاج عملية التحويل هذه إلى مهارة خاصة في برمجة المواقع أو إلى قيام المجرم باختراق موقع أحد مقدمي الخدمة المشهورين، ثم يقوم بتركيب البرنامج الخاص به هناك وبمجرد أن يكتب مستخدم الإنترنت اسم هذا الموقع فإنه يقع في المصيدة ويدخل إلى الموقع المشبوه الذي أعده المجرم، إذا أن هذا الأخير قام بتغيير أحد الروابط في الوسط بين المستفيد والموقع الشهير، ويستطيع من ذلك أن يتلصص على المعلومات المتبادلة بينها.

الفرع الثالث
الحماية الفنية من الاختراق[3]

هناك من يوصي إجراءات وقائية لتجنب الاختراق، كإخفاء الملفات وإغلاقها بكلمات سرية وعدم ترك أي ملفات مهمة على الجهاز، بل تحفظ في اسطوانة خارجية وتشغل عند الحاجة، فلا يجد المخترقون إليها سبيلا. لكن ليس هذا بالحل المثل لأنه كفيل بتجريد

[3]- أيمن عبد الحفيظ عبد الحميد سليمان، المرجع نفسه، ص 313.

[2] أيمن عبد الحفيظ عبد الحميد سليمان، المرجع نفسه، ص 313.

[3] محمد خليفة، مرجع سابق، ص 48 -49.

المستخدم من منافع الحاسب الآلي والحل يكمن في حماية الحاسب بمجموعة من البرامج تثبت عليه، وهي تنقسم إلى قسمين هما برامج مضادات للفيروسات والجدران النارية.

فأما الأولى فتقوم بمراقبة أي ملف يقوم المستخدم باستخدامه للتأكد من خلوه من الفيروسات لأنه تعتبر ملفات أحصنة طروادة بمثابة فيروسات وتعطي المستخدم الخيار في استخدام الملف من عدمه، أما الجدران النارية فهي برامج صغيرة تثبت داخل النظام بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الإنترنت، وذلك عن طريق مراقبة الحزم التي يتم إرسالها واستقبالها من الكمبيوتر الخاص بالمستخدم والحزمة هي الأجزاء الصغيرة التي يتم تجزئة الملفات إليها. وعند مراقبة الحائط الناري لهذه الحزم والمنافذ التي ترسل وتستقبل من خلالها، فإن عليه السماح أو الاعتراض على دخول هذه البيانات أو خروجها، وتنبه المستخدم لذلك وإخباره بالمنفذ وإلى أي جهة يريد الخروج إليها، ليقوم المستخدم بالسماح بذلك أو عدم السماح به، وفيما يلي تفاصيل أكثر عن الجدران النارية باعتبارها أحد وسائل الحماية الفنية من الانتهاكات التي تتعرض لها المعلومات.

وإضافة إلى الحماية الفنية هناك طريقة أخرى للحد من تزايد عمليات الاختراق وهي الاستعانة بخبرات بعض محترفي التسلل ذلك لأن المتسللين عادة يطورون تقنياتهم بصفة مستمرة ويملكون مهارات متقدمة، لهذا فقد اضطر مسئولو أمن الحاسبات الآلية وشبكات الانترنت وكذلك رجال الأمن بالاستعانة بخبرة هؤلاء المحترفين ليستطيعوا تطوير نظم الحماية ضد المتسللين، فمثلا قامت وكالة المباحث الفدرالية بالاستعانة بخبراء في التسلل لتدريب مسئولو الوكالة على طرق التسلل لتنمية خبراتهم وقدراتهم في هذا المجال وليستطيعوا مواكبة خبرات وقدرات المتخصصين من المتسللين.

المطلب الثاني
الفيروسات المعلوماتية

تعتبر الفيروسات المعلوماتية من أهم وسائل المساس بالأنظمة المعلوماتية والمعطيات المعلوماتية وأكثرها استعمالا، فهي تعد بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب إلى كلتا الحالتين بفائدتها، وفيروس الحاسب الآلي يشبه الفيروس الذي يصيب الإنسان إلى حد كبير فانتقاله من حاسب لآخر إلى حد كبير عدوى الفيروسات التي تصيب الإنسان وتنتقل من جسم إلى آخر. كما أن هذه الفيروسات عديدة ومتنوعة، وقد أنشئت شركات ضخمة تقوم بتصنيع برامج للحماية منها، وما أدى انتشار الفيروسات هو الاستخدام الواسع للحاسب الآلي، والشأن هنا شأن السلاح كلما أنتج نوع أنتج

النوع المضاد له وهكذا، فإثر انتشار الواسع لفيروسات أنتجت العديد من الشركات برامج كمنع الإصابة بالفيروس، ثم ظهرت فيروسات جديدة محصنة ضد هذه البرامج، ولازال الأمر كذلك مستمر.

فلابد إذا من وجود أحد هذه البرامج المضادة للفيروسات على جهاز الحاسب الآلي والقيام بتحديثها دوريا من الإنترنت حتى تلم بكل جديد في عالم الفيروسات، لتكون رقيبا على أي ملفات جديدة تدخل للحاسب، وسنتناول فيما يلي تعريف الفيروسات وآثار الإصابة منها وأنواعها .

الفرع الأول
تعريف الفيروس المعلوماتي وخصائصه

فالفيروس هو برنامج يكرر نفسه على نظام الكمبيوتر عن طريق دمج نفسه في البرامج الأخرى وكما أن الفيروسات خطيرة للإنسان لدرجة أنها قد تقضي عليه، فالفيروسات التي نتحدث عنها قد تقضي على الكمبيوتر[1]، وقد تأتي في مختلف الأشكال والأحجام بل وبعض الفيروسات ليست خطيرة وإنما مزعجة.[2]

فالفيروس هو عبارة عن برنامج يحتوي على مجموعة من الأوامر الخاصة بكيفية انتشاره داخل الملفات، ويتم كتابة هذا البرنامج باستخدام إحدى لغات البرمجة منخفضة المستوى[3]، ويحدث أثارا تخريبية[4].

أو هو برنامج أو جزء في الشفرة التي تدخل إلى الحاسب الآلي بهدف التخريب وتتميز بقدرتها على نسخ نفسها إلى نسخ كثيرة وقدرتها على الانتقال من مكان إلى مكان أومن حاسب إلى حاسب والاختفاء وتغطية محتوياتها[5]،وله القدرة على ربط نفسه بالبرامج الأخرى ويقوم بالانتشار بين برامج الحاسب المختلفة وبين المواقع المختلفة في الذاكرة[6].

وهناك فارق بين فيروس الحاسب الآلي وفيروس الانترنت، حيث يتميز فيروس الانترنت بإمكانية انتشار هائلة وغير محدودة، كونه يستمر في الانتشار ولول م يتم إغلاق الحاسب أو النظام كله. كما يختلفان من حيث الدور حيث يقوم فيروس الانترنت بدور المخرب والمختلس للمعلومات خلافا لفيروس الحاسب الذي يقتصر دوره على التخريب فقط. كما أن فيروس الانترنت تفوق قدرته قدرة فيروس الحاسب الآلي ، فالأول يقوم بدوره طالما أن

---

[1] رغم أن بعض الفقهاء يعرفون الفيروس أنه مرض يصيب الحاسب الآلي ولكنه ليس فيروسا بالمعنى البيولوجي أو الطبي المعروف .

[2] أمير فرج يوسف، مرجع سابق، ص 68.

[3] لغات البرمجة منخفضة المستوى هي اللغات التي تتعامل مباشرة مع الآلة وتتيح أن يكون ملف الفيروس صغير الحجم ليكون قادر على التخفي.

[4] محمد خليفة، مرجع سابق، ص 50.

[5] http://ejabat.google.com يوم الاطلاع على الموقع 2015/03/18.

[6] فهد بن سيف بن راشد الحوسني، مرجع سابق،ص 66.

شبكة الانترنت تعمل ولوتم إغلاق أجهزة الحاسب الآلي، في حين النوع الثاني يبقى في الجهاز المصاب به، ولا ينتقل إلى الجهاز الآخر إلا بالعدوى، عن طريق ملف أو برنامج ما من الجهاز المصاب إلى آخر، أو ينتقل عن طريق القرص المرن أو القرص الصلب أوا لقرص الممغنط أو جهاز USB[1] .

ويقوم الفيروس عادة بإصابة الحاسب بدون أن يشعر بدلك المستخدم، فهي برامج تتم كتابتها بغرض إلحاق الضرر بكمبيوتر آخر، أو السيطرة عليه[2]. حيث أن الأوامر المكتوبة في هذه البرامج تقتصر على أوامر تخريبية تلحق ضررا بنظام المعلومات أو البيانات[3].

ومن خلال التعريفات السابقة يمكن استخلاص أهم الخصائص التقنية للفيروس المعلوماتي وهي:

- هو عبارة عن برنامج صغير يختفي بسهولة في النظام المعلوماتي، واستغل المجرمون المعلوماتيون هذه الخاصية حيث وضعوا فيروسات من الصعب العثور عليها بالبرامج المضادة للفيروسات.
- له قدرة فائقة على مهاجمة المكونات المعنوية للجهاز الحاسب الآلي والشبكات المعلوماتية التي تربطها فيما بينها مما يزيد في قدرته على الانتشار والسرعة في تنفيذ أهدافها[4].

الفرع الثاني
آثار الإصابة بالفيروس

الفيروسات هي أحد أنواع الحاسب الآلية إلا أن الأوامر المكتوبة في هذا البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز[5]، إذن هي برامج خبيثة بطبيعتها فهي تؤثر سلبيا في الحواسيب بشكل مباشر وفي غير الحواسيب بشكل غير مباشر فالفيروس عندما يحذف ملفات مهمة للعملاء يتعدى الحاسوب إلى العملاء وسمعة الشركة[6]، وتختلف الآثار التي يخلفها الفيروس بحسب نوعه، وهي تتدرج من أقلها ضررا إلى أكبرها كما يلي :

- البطء الشديد في الحاسب بما يجعل التعامل معه مستحيلا.
- عدم القدرة على تشغيل معظم التطبيقات، وظهور رسائل خطأ كلما تمت محاولة تشغيلها.
- مسح الملفات التنفيذية كالبرامج سواء المثبتة داخل نظام التشغيل أو التي يحتفظ بها داخل الحاسب مما يسبب عدم القدرة على تشغيل هذه التطبيقات.

---

[1] الموسوس عتو، مرجع سابق، ص 135.

[2] عبد الصبور عبد القوي علي مصري، الجريمة الالكترونية، الطبعة الأولى، دار العلوم للنشر والتوزيع، القاهرة، 2008، ص 47.

[3] عمرو عيسى الفقي، الجرائم المعلوماتية ، جرائم الحاسب الآلي والانترنت في مصر والدول العربية، المكتب الجامعي الحديث، ص 230.

[4] محمد ساميي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1993، ص 189.

[5] يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والانترنت، دار الكتاب العربي، القاهرة، الطبعة الأولى، 2010، ص 137.

[6] خالد بن سليمان الغثير ومحمد بن عبد الله القحطاني، مرجع سابق، ص 66.

- حذف ملفات (FAT) مما يعني حذف جميع المعطيات الموجودة داخل القرص الصلب، وهو الأمر الأكثر خطورة.
- إصابة أحد أجزاء المكونات الصلبة، كما يحدث مع فيروس " تشير نوبل " الذي يصيب نظام الإدخال والإخراج الأساسية، مما يؤدي إلى توقف الحاسب بالكامل.

ويمكن حماية نظم المعالجة الآلية للبيانات ضد الإصابة من الفيروس المعلوماتي عن طريق وضع نظم أمنية ضد البرامج والبيانات والنظم الفيروسية، وبالتالي حماية البرامج والبيانات داخل النظام من الاعتداء عليها بهذا الأسلوب[3].

الفرع الثالث
أنواع الفيروسات

الفيروسات كثيرة جدا لا يمكن حصرها ذلك أن الانترنت ساهمت بشكل كبير في انتشارها وكثرتها إذ أصبحت قادرة على الانتقال بكل سهولة من أي مكان في العالم وإلى أي مكان دون تلقي أي عوائق تمنع تنقلها. ويمكن ذكر بعض أنواع الفيروسات المتميزة والشائعة كفيروسات التلاعب بالبيانات الذي هو برنامج فيروسي يتم إنشاؤه ليتحرك بصفة خاصة من ملف إلى آخر، كي يحصل على معلومات محددة أو يعدلها أو يحل محلها[1]، ومن هده الفيروسات:

أولا:فيروس الحب

يتمثل هذا الفيروس في شكل رسالة أو صورة مثيرة للإغراء، ترسل إلى البريد الالكتروني للمستخدم لحثه على فتحها وتكون ملحقة برسالة عادية، ويتنكر الفيروس في شكل رسالة بريدية آمنة وبمجرد فتح الرسالة يقوم الفيروس بنسخ نفسه مرات عديدة، مما يضاعف قدرته على الانتشار لحذف الملفات أو إخفائها ويستبدلها بنسخ منه، ويقوم أيضا بإرسال رسالة بريد إلكتروني لكافة العناوين الإلكترونية الموجودة في سجل العناوين الالكترونية[2].

يعتبر فيروس الحب من الفيروسات التي سببت أضرارا فادحة حيث لم يسبق أن تمكن فيروس في عام 2000 من الانتشار بالسرعة والكثافة التي حققها ذلك الفيروس، حيث يعتمد مبدأ عمله على الانتشار عبر البريد الالكتروني، مسببا أضرار كتدمير بعض الملفات وسرقة

[3]– بلال أمين زين ، مرجع سابق، ص 383.
[1] مليكة عطوي، مرجع سابق، ص 15.
[2] محمد سامي الشوا، مرجع سابق، ص 145.

كلمات السر وكان من أبرز ضحاياه وزارة الدفاع الأمريكية ووكالة الاستخبارات الأمريكية وجهات حكومية بريطانية[1].

ورغم أن هدف الفيروس ليس الحصول على الأسرار المخزنة في الحاسب الآلي بل تدميرها إضافة إلى أنه قد يهدد تلك الأسرار بطريق غير مباشر حيث أننا نعلم جميعا حجم الأسرار التي تحملها خاصة الحواسيب الشخصية الخاصة، حيث أن صاحبها لن يحس بالارتياح والاطمئنان عرض حاسوبه على المصلح مما يجعل بهذا الأخير أن يجد نفسه مضطرا للإطلاع على ما كان يحمله الحاسوب من معلومات.

ثانيا:دودة الإنترنت

هي فيروس تنتقل عبر شبكة الإنترنت، ويعتمد على استخدام برنامجOutlook Express بشكل أساسي للقيام بعملية الانتشار وإصابة اكبر عدد ممكن من الأجهزة، ويقوم مصممه بزرعه داخل رسالة بريد الكتروني، ويرسلها إلى عدد كبير من مستخدمي الشبكة، وبمجرد قيامهم بفتحها يبدأ الفيروس في الحصول على دفتر العناوين Address Book الخاص بكل واحد منهم ثم إرسال هذه الرسالة للعديد من أصدقائهم، فيفتحونها دون أدنى شك لمعرفتهم للمرسل، فيقعوا ضحية هذا الفيروس وهذا ما أدى إلى انتشاره بنسبة كبيرة في العالم.

ويعمل هذا الفيروس على نسخ نفسه أوتوماتيكيا نسخا عديدة، فيقوم بوضع أصفار في الأماكن الموجودة بالذاكرة التي يمر عليها أو يبدل محتويات مكان في الذاكرة مع محتويات المكان المجاور له مما يجعل من الصعوبة اكتشافه، وعند إصابة الجهاز به تستمر برامج هذا الجهاز بالعمل ولكن بقيم مختلفة عن المعطيات التي تعمل عليه القيم الأصلية نظرا لتحويل بعض منها إلى أصفار أو بتبديل أماكن المعطيات مع بعضه البعض فيحصل مشغل البرنامج على نتائج زائفة دون أن يشعر بذلك ويتم على أساسها اتخاذ قرارات خاطئة[2].

ثالثا: فيروس القنابل المنطقية

يعمل هذا الفيروس كالقنبلة إذ يظل في حالة سكون حتى يتم تفجيره في الوقت المناسب، إذ يظل البرنامج موجودا ولا تأثير له حتى يجد بيانات مخزنة في مكان محدد لها قيمة معينة أو بعد تشغيل البرنامج لعدة مرات معينة وفي المرة التالية يبدأ الفيروس في العمل.

---

[1] محمود احمد عبابنة، مرجع سابق، ص 102.

[2] أنتج لطالب روبرت موريس (طالب دكتوراه في علم الكمبيوتر) بجامعة كورنيل عام 1988 برنامج الدودة حيث أراد موريس أن يثبت عدم ملائمة أو فعالية الإجراءات الأمنية القائمة لحماية شبكات الكمبيوتر وإظهار العيوب فيها، لهذا قام بذلك التصميم ومنه سيربط بعد تشغيله عن طريق حاسب محلي مرتبط بالانترنت ويربط بين مجموعة من شبكات الكمبيوتر الأمريكية المتصلة مع الجامعات والجهات العسكرية، واكتشف موريس حينها أن البرنامج يقوم بالانتشار بسرعة كبيرة الأمر الذي ترتب عليه تلف الكثير من برامج الكمبيوتر وتوقيفها عن العمل وبعد إلقاء القبض عليه تمت محاكمته بمقتضى النص الذي يجرم الدخول إلى الأجهزة الفدرالية بدون تصريح، وتمت إدانته والحكم عليه بالوضع ثلاث سنوات تحت المراقبة والقيام بعمل لخدمة المجتمع لمدة 400 ساعة وغرامة عشرة آلاف وخمسين دولارا أمريكيا، أنظر في هذا محمود أحمد عبابنة، مرجع سبق، ص 103.

وتأثير الفيروس يتراوح بين التغيير العشوائي لمحتويات مكان محدد على وسط التخزين أوفي الذاكرة لجعل كل محتويات قرص التخزين الصلب غير قابلة للقراءة بأي حال من الأحوال، وهذا الفيروس يصمم لإصابة برامج محددة وتطبيقات معينة يوجه إليها، فهو ليس فيروسا عاما.

لقد أدى الانتشار الواسع لاستخدام الحاسب الآلي إلى انتشار الفيروسات، والشأن هنا شأن السلاح كلما أنتج نوع أنتج النوع المضاد له وهكذا، فإثر انتشار الواسع لفيروسات أنتجت العديد من الشركات برامج كمنع الإصابة بالفيروس، ثم ظهرت فيروسات جديدة محصنة ضد هذه البرامج، ولازال الأمر كذلك مستمر .

فلابد إذا من وجود أحد هذه البرامج المضادة للفيروسات على جهاز الحاسب الآلي والقيام بتحديثها دوريا من الإنترنت حتى تلم بكل جديد في عالم الفيروسات، لتكون رقيبا على أي ملفات جديدة تدخل للحاسب.

ولمقاومة هذه الفيروسات هناك عدة وسائل من ضمنها استخدام البرامج المضادة للفيروسات وكذا حماية النظام والمعطيات المحتواة فيه حماية فنية.

المبحث الثالث

الوسائل الفنية لحماية المعلومات من خطر الانتهاك

إن المنع الجنائي وتحديد عقوبات لجرائم المعلوماتية بصفة مسبقة بها يتماشى مع مبدأ الشرعية وإن كان يوفر حماية أساسية للنظام وللمعلومات ضد المخاطر والأضرار الناجمة عن هذه الجرائم باهظة التكلفة في حالة الوصول إلى معلومات سرية، إلا أنه غير كاف لوحده، فحتى تكون هناك الفعالية في الحركة والأداء لابد أن تعززها حماية فنية تعمل على الحيلولة دون وقوع هذه الجرائم أوالتخفيف من آثارها إذا وقعت[1].

وحيث تتعرض الأسرار المعلوماتية للانتهاك اللامتناهي خاصة عند ارتباط الحاسوب بشبكة الانترنت ما تطلب ضرورة اتخاذ تدابير احترازية ووسائل حماية سرية تلك المعلومات، وجعلها في مأمن وكثيرة هي الطرق الفنية للتأمين خاصة في الوقت الحاضر، ويمكن إجمال أساليب الحماية الفنية في أساليب الحماية الفنية عن طريق البرامج (المطلب الأول)، والحماية الفنية عن طريق نظام الرقابة الوقائية عبر الوسائل الالكترونية (المطلب الثاني).

[1] وهذا ما أكدت عليه المذكرة التفسيرية لاتفاقية بودابست حينما ذهبت إلى القول من أن الوسيلة الأكثر فعالية لمنع الولوج غير المصرح به تتمثل بطبيعة الحال في التهديد بقانون العقوبات، ومع ذلك فإن هذا العرض لا يكون مكتملا دون تبني ووضع إجراءات أمنية فعالة .أنظر في ذلك هلالي عبد الله أحمد، الجوانب الإجرائية والموضوعية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة ، 2003 ، ص 71.

المطلب الأول
أساليب الحماية الفنية عن طريق البرامج

تنقسم أساليب الحماية الفنية عن طريق البرامج إلى ما يلي:[1]

1 - الوسائل المتعلقة بالتعريف بشخص المستخدم و موثوقية الاستخدام ومشروعيه : وهي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام وتضم هذه الطائفة كلمات السر بأنواعها، البطاقات الذكية المستعملة للتعريف، وسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي كما تظم أيضا ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ.

2 - الوسائل المتعلقة بالتحكم في الدخول والنفاذ إلى الشبكة: وهي الوسائل التي تساعد على التأكد من أن الشبكة قد استخدمت بطريقة مشروعة ومن أهم الوسائل الفنية المعتمد عليها ما يعرف بالجدران النارية والتي هي عبارة عن برامج تثبت داخل النظام بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الإنترنت، فيتم إجبار جميع عمليات الدخول إلى الشبكة أو الخروج منها بأن تمر من خلال هذا الجدار الناري والذي يمنع أي مخترق أو متطفل من الوصول إلى الشبكة. وذلك عن طريق مراقبة الحزم الذي يتم إرسالها واستقبالها من الحاسب الآلي الخاص بالمستخدم. وعند مراقبة الجدار الناري لهذه الحزم والمنافذ التي ترسل وتستقبل من خلالها فإن عليه السماح أو الاعتراض على دخول هذه البيانات أو خروجها، وتنبه الاستخدام لذلك.

3 - الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المخولين أو المصرح لهم بذلك وتهدف هذه الوسائل إلى ضمان سرية المعلومات وتشمل تقنيات تشفير المعطيات والملفات، إجراءات حماية الموجات، نسخ الحفظ الاحتياطية، برامج الفلترات غيرها.

4 - الوسائل التي تهدف إلى حماية التكاملية وسلامة المحتوى وهي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة لها ذلك، ومن أهمها برامج تحري الفيروسات ومضادات الفيروسات

5 - الوسائل المتعلقة بمنع الإنكار: وتهدف هذه الوسائل إلى ضمان عدم قدرة الشخص المستخدم على إنكار أنه هو الذي قام بالتصرف، وترتكز هذه الوسائل بصفة أساسية على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة من طرف ثالث.

[1] سعيداني نعيم، مرجع سابق، ص 71 و72.

6 - وسائل مراقبة الاستخدام وتتبع سجلات النفاذ والأداء وهي التقنيات التي تستخدم لمراقبة مستخدمي النظام وتحديد الشخص الذي قام بالعمل المعين في الوقت المعين وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.

وهذه الوسيلة قد أشار إليها المشرع الجزائري في القانون 04/09 في المادة 10 منه، حينما ألزم مقدمي الخدمات العمل على حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة المتعلقة بتاريخ ووقت ومدة كل اتصال بالإضافة إلى حفظ المعطيات التي تسمح بالتعرف على المرسل إليه الاتصال وعنوان الموقع المطلع عليه.

وخدمة لموضوع الدراسة سنحاول التفصيل في بعض الأساليب الفنية ذلك لعلاقتها الوطيدة بالحماية الجنائية للمعلومات السرية.

الفرع الأول
تشفير المعلومات[1]

من أهم وسائل تأمين المعلومات السرية الالكترونية أسلوب التشفير فهو الأسلوب الأكثر شيوعا في التعامل عبر المنظومة المعلوماتية عامة وفي شبكة الانترنت خاصة، ويرجع ظهوره إلى قديم الأزل حيث كانت هنالك حاجه ماسة لحماية البيانات، ومنذ ذلك الحين ظهر نوعان من الناس نوع يكتب ولا يريد أن يطلع أحد من الغرباء على ما يكتب، والنوع الآخر هو الذي يتجسس ويريد الإطلاع على ما يكتبه الآخرون رغم محاولاتهم الدائمة لإخفاء ما يكتبونه عن ناظريه. وفي عام 1900 قبل الميلاد لم تكن هناك سوى مصطلحات هيروغليفية، أستخدم الإنسان التشفير منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية، وبلغ هذا الاستخدام ذروته في فترات الحروب، خوفا من وقوع الرسائل الحساسة في أيدي الأعداء. أولى الطرق المستخدمة قديما في التشفير هي طريقة الألغاز فكانوا مثلا يأخذون جملة مثل(ادفع لي أجرا) ويدخلون كل حرف في بداية كلمة فتصبح (إذا دخل فاروق عليه لباس يبدو أكثر جمالا راتبه أكثر) وللحصول على الجملة المطلوبة نأخذ كل حرف من بداية كل كلمة بحيث نكون الجملة الأصلية وهي: (ادفع لي أجراً).

لكنها طريقة صعبةً جداً خاصة إذا كانت المعلومات المراد إرسالها كبيرة حيث أن صعوبتها تكمن في إيجاد جمل تحمل المعلومات المطلوبة ولها مدلول واضح لا يثير الشك، لذا فأن هذا النوع نادراً ما تستخدم في الوقت الحالي.

[1] يسعى المتخصصون بأمن المعلومات للحفاظ على خصوصية البيانات المتناقلة عبر الشبكات وبالأخص حاليا فهم يسعون لتامين سرية الرسائل الالكترونية وسرية البيانات المتناقلة وخاصة بالأعمال التجارية الرقمية. ويمثل التشفير أفضل وسيلة للحفاظ على سرية البيانات المتناقلة ، ويرى الخبراء ضرورة استخدام أسلوب التشفير لمنع الآخرين من الاطلاع على الرسائل الالكترونية .

تلك الطريقة وأمثالها يصعب تمثيلها بواسطة الحاسب، وبلغ هذا الاستخدام ذروته في فترات الحروب، خوفا من وقوع الرسائل الحساسة في أيدي الأعداء وكانوا يأخذون الرجال ذوي الرؤوس الكبيرة ويحلقون لهم ومن ثم يكتبون ما يريدون إخفاءه على الرأس وبعد أن ينمو شعره ويصبح كثيفا يرسل بالرسالة فإذا وقع في أيدي العدو وقاموا بتفتيشه لم يجدوا معه شيئا وأطلقوا سراحه وإذا وصل برأسه (الرسالة) يتم حلق رأسه لقراءة الرسالة ومن ثم بدء اكتشافها مع كثرة استخدامها.

بعد فشل طريقة الكتابة على الرؤوس ظهرت أول طريقة تشفير (بمعنى هذا المصطلح) وهي شفرة قيصر، ونلاحظ أن الحروب دائما كانت الملهم الأهم لظهور خوارزميات التشفير[1].

فتشفير المعلومات أو كما يطلق عليه علم الكتابة السرية هو فن حمايتها والمحافظة على سريتها عن طريق تحويلها إلى رموز معينة غير مقروءة[2]، فالتشفير هو علم إخفاء معنى ومفهوم المعلومة السرية وليس إخفاء وجودها، أي تحويل المعلومات إلى شيفرات غير مفهومة، بحيث لو وقعت الرسالة المرسلة في يد أي شخص غير المستقبل المقصود سيكون غير قادر على فهم محتواها لأنه غير مخول لقراءتها، وإذا وصلت الرسالة المشفرة إلى المستقبل المعني فإنه يقوم بعملة عكسية للتشفير وتسمى فك التشفير للحصول على النص الأصلي وقراءته، وهي عملية تحويل الشيفرات غير المفهومة إلى معلومات واضحة ومفهومة ويستطيع المستقبل فك التشفير باستخدام "مفتاح سري" يسمى مفتاح التشفير حيث يتم تحويل النص إلى نص عادي مقروء أو نص كامل، وتستخدم هذه التقنية في مجالات الاتصالات الالكترونية وبصفة خاصة شبكة الانترنت لحماية الرسائل الالكترونية والمعلومات الضخمة المنقولة إلكترونيا[3]، وبدلك يكون التشفير سلاح ذو حدين يحمي محتوى البيانات ولكن بضياع ذلك المفتاح السري أو البرنامج الذي شفر المحتوى فلا فائدة ترجى من وراء المحتوى المشفر[4].وبذلك هو علم تحويل الكتابة إلى أسرار بالنسبة لغير الصرح لهم بالإطلاع عليها، ويأتي مصدر قوة إخفاء المعلومة من عدم إمكانية اكتشاف المعلومات السرية من قبل غير المصرح لهم بذلك[5].

---

[1] http://www.ejabah.info/ يوم الاطلاع على الموقع 2015/03/20.

[2] رشدي محمد علي محمد عيد، مرجع سابق، ص 276.

[3] رشدي محمد علي محمد عيد، مرجع سابق، ص 288.

[4] خالد بن سليمان الغثير ومحمد بن عبد الله القحطاني، مرجع سابق، ص107.

[5] وتطبق شركة كرايزاليس الكندية نظاما أمنيا جديدا لتطبيقات شبكات الانترنت الداخلية المعروفة بشبكات الانترنت، وهذا النظام عبارة عن بطاقة كمبيوترية تعرف " ببطاقة لونا " يتم فيها تخزين بيانات التشفير والتواقيع الالكترونية الخاصة بحامل البطاقة بحيث تخزن هذه المعلومات السرية داخل البطاقة بالذات وليس داخل ذاكرة الحاسب، وتقوم هذه الشركة بتسويق بطاقتها الجديدة على مستعملي شبكات الإنترنت الداخلية بحيث يحصر الولوج على هذه الشبكات لحاملي هذه البطاقات فقط.

أولا: تعريف التشفير

ولمصطلح التشفير عبر الانترنت معنى يستخدمه الفقه كناية عنه وهو مصطلح التخفي أو الإخفاء وهو يفيد إخفاء المعلومة في أساس بياناتها بحيث إذا ظهرت تلك البيانات فإنها لن تعبر عن فحواها الحقيقي، فالتشفير عبارة عن برمجية تتولى فرض شفرة تحمي ظاهر المعلومات، بحيث تمنع الغير ممن ليس لهم الحق في التعامل مع الموقع الدخول إليه ما لم يصرح له المالك بذلك، فهوعلى هدا النحوعلم تحويل الكتابة إلى أسرار، ويكون تصريح المالك للغير بالاطلاع على المعلومات المشفرة باستخدام مفتاح إزالة التشفير وهذا الأخير عبارة عن منتج أو آلة أومركب تم تصميمه لكي يقوم بفك شفرة الدخول[1]،أي يقصد بتشفير البيانات كتابتها برموز سرية بحيث يصبح فهمها متعذرا على من لا يحوز مفتاح الشفرة التي استخدمت.

ويعرف أيضا أنه" آلية يتم بمقتضاها ترجمة معلومة غير مفهومة إلى معلومة مفهومة، وذلك عبر تطبيق بروتوكولات سرية قابلة للانعكاس، أي يمكن إرجاعها إلى حالتها الأصلية"[2].

عرف التشفير في القانون العربي النموذجي بأنه" تحويل البيانات المعالجة الكترونيا إلى رموز لعدم تمكين الغير من انتهاك سريتها"[3]، ويعرف التشفير بأنه "مناهج لخط البيانات من خلال لوغارتميات أو خوارزميات بحيث لا يمكن قرائتها من خلال طرف ثالث متطفل، فالتشفير عبارة عن فلسفة معينة يتم بها حصر معلومة في نطاق محدد، فيتم اللجوء إليه بقصد حجب معلومة ما عن التداول "[4].

ولقد عرف مجلس الدولة الفرنسي التشفير بأنه" كل عمل يوجه لتحويل – بمساعدة مصطلحات سرية – معلومات أو إشارات غير مفهومة للغير، أو بإخراجها بعملية معكوسة، بفضل وسائل مادية أو برمجية مصممة لدلك.[5] ويعرف القانون الفرنسي[6] التشفير أنه:" كل فعل يؤدي إلى تحويل معلومات أو إشارات غير مقروءة للغير، أويخرجها بطريقة معكوسة وذلك بالاستعانة بوسائل مادية أو برامج مصممة لذلك".[7]

---

[1] عمر محمد أبوبكر يونس، مرجع سابق، ص 379.

[2] وليد الزيدي، المرجع السابق، ص 93.

[3] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، دار النهضة العربية الإسكندرية، 2009، ص 75.

[4] عمر محمد أبو بكر يونس، مرجع سابق، ص 379.

[5] عمر محمد أبو بكر يونس، مرجع سابق، ص 383.

[6] القانون رقم 90/1170 الصادر بتاريخ 1990/12/29 المتعلق بتنظيم الاتصالات في فرنسا، بموجب المادة 28 منه.

[7] تم تعديل المادة 28 من القانون رقم 90/1170 بموجب المادة 17 من القانون رقم 96/659 الصادر بتاريخ 1996/07/26 حيث تطلب هذا القانون ضرورة الحصول على تصريح من السلطات الفرنسية عند القيام ببيع أواستيراد التشفير من خارج الاتحاد الأوروبي أوتصدير أدوات التشفير إذا كانت ذات طبيعة سرية.

وفي الولايات المتحدة الأمريكية كانت تعتبر تقنيات التشفير من قائمة الأسلحة بعيدة المدى وذلك قبل عام 1998، ولذلك كانت تعتبر من ضمن الأسرار القومية وفي نهاية عام 1999 بدأت الحكومة الأمريكية تخفف من عملية التشديد على تصدير تقنية التشفير، وفي سبيل ذلك رفعت هذه التقنية من قائمة الأسلحة التي تعد حيازتها من قبل الغير هو بمثابة تهديد للأمن القومي الأمريكي ووضعت الحكومة مشروع قانون الأمن الالكتروني في العالم الافتراضي عام 1999 وتضمن هذا المشروع السماح بتصدير تقنيات التشفير سواء كانت برامج أو قطع صلبة وذلك حتى 40 bit واشترطت للموافقة على ذلك أن تحصل الحكومة الأمريكية على نسخة من المفاتيح الاستردادية لهذه التقنيات وذلك من شأنه أن يعطي الحكومة الحق في مراقبة استخدامات التشفير.والجدير بالذكر أن نظم التشفير أصلا تعتبر من المعلومات التي حظيت بالحماية الجنائية باعتبارها تدخل في نطاق المعلومات الالكترونية السرية وأن الاعتداء عليها بأي شكل من الأشكال يعتبر جريمة في نظر القانون.

ثانيا: مناهج التشفير

تنوعت مناهج التشفير فمنها ما يتعلق بالخصوصية ومنها ما يتعلق بقداسة المعلومة ومنها ما يتعلق بأصالة المعلومات، مع العلم أن هذا التنوع ليس له تأثير من الناحية القانونية، ونعالج هذه المناهج كالتالي[1]:

1- التشفير المتعلق بالخصوصية

ويعد استخدام التشفير الذي يتعلق بالخصوصية من أشهر الأساليب حيث يترتب على استخدام ردع كل من لم يكن مصرح له بالإطلاع على المعلومة من فهم مضمونها أو التعرف على كنهها، سواء كان ذلك قراءة لها أواستماع إليها، كذلك الحال كونها مسجلة أو مرئية، ومع ذلك يلزم التمييز بين التشفير المتعلق بالخصوصية وبين الحق في الخصوصية ذاته الذي يعطي صلاحية التشفير.

2- التشفير المتعلق بقداسة المعلومة

أما التشفير الذي يشمل قداسة المعلومة فإنه ذلك النوع الذي يحيط المعلومة بحصار آمن، بحيث يردع التشفير هنا كل محاولة من قبل غير المصرح له بالتعرض للكيفية التي كتبت بها المعلومة خاصة عند إرسالها عبر الانترنت ، فلا يستطيع تغيير موضوعها تعديلا أو حذفا.

3- التشفير المتعلق بأصالة المعلومات

[1] عمر محمد أبو بكر يونس ،المرجع نفسه، ص 380 وما بعدها.

أما التشفير المتعلق بأصالة المعلومات فتستخدم في تقنيات المحافظة على تأصيل المعلومة واستمرارها صحيحة، بحيث تدل على الراسل والمرسل إليه، وبما يعني أن المرسل لا يستطيع إنكار إرساله لهذه الرسالة.

ثالثا: التشفير كمعوقات في الإثبات

تعتبر تقنية التشفير سلاح دو حدين ففي الوقت الذي تستخدم فيه كوسيلة حماية من الجرائم التي تستهدف سرية المعلومات الالكترونية إلا أنها قد تستخدم لإخفاء الأدلة بعد حدوث الجريمة، فكما يعتبر وسيلة لإخفاء المعلومة السرية وحجبها عن الغير يستعمل أيضا في إخفاء أدلة الإدانة في حال الاعتداء على تلك المعلومات ووقوع الجريمة، حيث يتم تشفير الملفات التي تحوي على العدوان، مما يصعب المهمة على الجهات القضائية المختصة بالتحقيق والحكم بالإدانة.

ففي مثل هذه الحالات تواجه العدالة الجنائية تحديات كبيرة في قدراتها على مواجهة الجريمة حيث تتلقى العقبات التالية:

1- تفسير وتحليل الملفات أو السجلات المعالجة آليا المخزنة، والتي يتم التوصل إليها بمقتضى أمر قضائي أو بالإجراءات المقررة لذلك.

2- تنفيذ أمر قضائي بالمراقبة الإلكترونية.

ومعلوم أن كل محاولة للحصول على ملفات وسجلات مشفرة إنما تعد محاولات فاشلة لكونها تفيد كثيرا في الكشف عن الحقيقة، كما أنها تعد محلا للطعن فيها، وما يساعد على أن التقرير بأن التشفير قد يستخدم لإعاقة البحث عن الأدلة ، إذا كان المتهم ليس له سوابق قضائية يمكن الاستعانة بها لمواجهته.

ومنه قد يستخدم التشفير كوسيلة غطاء لطمس الأدلة والاستعانة بأدلة أخرى تساعد على القول بالإدانة وذلك حتى لا يفلت المجرم من العقاب[1].

وما تجدر الإشارة إليه أنه في إطار التشفير يلزم التمييز بينه وبين موضوع آخر وإن كان يرتبط به من حيث البناء العضوي أوالبرمجي وهوالتوقيع الالكتروني، فكل منهما يستخدم تقنية الإخفاء إلا أن لكل منهما منهج للتعامل به.

الفرع الثاني
الجدران النارية

تم أخد مفهوم الجدار الناري من الاستعداد الأمني القديم والمتمثل في حفر خندق حول قلعة، مما يمنع أي شخص من الدخول أو الخروج من جسر القلعة ويمكن تفتيشه من قبل المعنيين، إذ يعمل الجدار الناري كالجسر الالكتروني يراقب الدخول إلى الشبكة والخروج

[1] عمر محمد أبوبكر يونس ، مرجع سابق، ص 385.

منها، ويعرف أنه" مجموعة أنظمة توفر أساليب أمنية بين الانترنت وشبكة المؤسسات أو الشركات وغيرها، لكي تجبر جميع عمليات الدخول إلى الشبكة، الخروج منها أن تمر من خلال الجدار الناري الذي يقوم بصد اختراقات المستخدمين المتطفلين، وهو يوفر في ذات الوقت حواجز أمنية قبل الدخول إلى الموقع المعني، مثل التحقق من المستخدمين المحليين والخارجيين ونظام الدخول والخروج[1].

ونشأت فكرة جدران الحماية أو ما يسمى بالجدران النارية لكثرة الأخطار التي تهدد شبكات المعلومات والتي يمكن وصفها بأنها نظام مؤلف من برنامج يعمل في الحاسوب، ويمكن أن تشبه أيضا بنقطة التفتيش التي تسمح بمرور أناس وتمنع مرور آخرين[2].

وتنحصر وظيفة الجدار الناري في أنه يقوم بعملية مسح للمعلومات التي تصل إليه من شبكة الانترنت ويقوم بتحليلها وعندما يجد أي شك في المعلومات التي تصل إليه لمحاولة الدخول أو الاختراق إلى المناطق المؤمنة فإنه يقوم بمنع هذه المحاولة وطردها خارج الشبكة أما إذا كانت المعلومات عادية وآمنة فإن الجهاز يسمح لها بالمرور والدخول على أجهزة الحاسبات الآلية[3].

فعملية تحديد صلاحية المعلومات للمرور داخل الشبكة أو عدم السماح لها بالمرور هي عملية معقدة وعلى درجة كبيرة من الأهمية، لأن ذلك يعتمد على ضبط جهاز الجدار الناري وهو أمر بالغ الدقة لأنه إذا تم ضبطه بدرجة حساسية مبالغ فيها فإن ذلك يتسبب في بطء التعامل مع الشبكة.

ويؤدي أيضا إلى رفض بعض المعلومات الآمنة التي يكون المستخدم في حاجة إليها، ولكي يقوم جهاز الجدار الناري بأداء وظيفته لابد من وجود برنامج داخل الجهاز يتم تزويده بكافة المعلومات عن البرامج غير المسموح لها بالمرور مثل الفيروسات[4]، وتعتبر أفضل الجدران النارية ما يلي:

1- **Mod_Security**: يعد برنامج Mod_Security من أفضل وأقوى البرامج المجانية المتوافرة على شبكة الإنترنت التي توفر حماية كبيره لتطبيقات الويب الخاصة، لأنه يوفر مجموعة من القواعد المدفوعة وغير المدفوعة التي تضمن بالفعل حماية كبيره

[1] وليد الزيدي، مرجع سابق، ص 101.
[2] خالد بن سليمان الغثير ومحمد بن عبد الله القحطاني، مرجع سابق، ص 91.
[3] أيمن عبد الحفيظ، مرجع سابق، ص 394-395.
[4] أيمن عبد الحفيظ، مرجع سابق، ص 395.

ولكنه يحتاج إلى معرفه كبيره بإدارة السيرفرات[1] والتعامل مع خوادم الويب لكي يمكن التعامل معه بشكل احترافي دون وجود أي أخطاء[2].

2-**برنامج Zone alarmM: يعتبر من أشهر برامج** الجدران النارية نظرا لكفاءته غي المحدودة في ضبط ورصد كافة محاولات الاختراق على الأجهزة وقيامه بإعطاء إشارة عند حدوث أي اعتداء كما أن هذا البرنامج يمكنه القيام بتفقد مرفقات البريد الالكتروني والتي أصبحت أحد مصادر الفيروسات بحيث يقوم باحتجازها أوطردها أومسحها، كذلك يمكن لهذا البرنامج قبل قيامه بحذف أي من البرامج يتيح للمستخدم فرصة تفحص الملفات ثم يقرر تشغيلها أم لا[3].

3- **نظام Snort الأمني** : وهونظام رائع جداً يقوم بعدة وظائف ومهام تساعد على زيادة أمن تطبيقات الويب الخاصة، وزيادة مستوى حماية السيرفر أيضاً بشكل عام لكي تضمن بالفعل حماية متكاملة للسيرفر أوالنظام المتوفر لديك.

الفرع الثالث
استخدام كلمة السر

وهي عبارة عن" رقم رمزي لا يتيح التعامل مع نظام الحاسب سواء من نهاية طرفية معينة أو لإدخال بيانات إلا بذكرها وتتكون هذه الكلمة من حروف أو أرقام توصف بصورة عشوائية "، وينصح بضرورة إتباع خطوات عند وضع كلمة السر على النحو الآتي:

1. يجب أن يتم تبديل كلمات السر بصورة دورية لتجنب إمكانية الاطلاع عليها من قبل أشخاص غير مؤهلين، والفترة التي تتجدد فيها كلمة السر تحدد حسب طبيعة نشاط مستعمل الكمبيوتر ويمكن التبديل مرة كل ثلاثين يوما.
2. يجب أن تتألف كلمات السر من خمسة أحرف على الأقل ويفضل أن تتألف من ثمانية أحرف وذلك يجعل محاولة التكهن بها عن طريق التجربة مهمة صعبة بالنسبة إلى القرصان.
3. يفضل عدم إعادة استعمال كلمة السر القديمة قبل مرور سنة على الأقل بعد التخلي عنها.

---

[1] المقصود بالسيرفر أو الخادم هو جهاز كمبيوتر عادي مثل أي جهاز كمبيوتر خاص يستخدم في المنزل أو العمل ولكنه يتوفر على بعض المواصفات الخاصة التي تفرق بين أي جهاز كمبيوتر عادي والسيرفر وهي أن يستطيع أن يتسع لأكثر من معالج ويقوم بتشغيل على سبيل المثال 4 جيقا رام، عن http://www.traidnt.net/ تم الاطلاع عليه يوم 2011/12/13.

[2] مقال لمحمد عسكر، بعنوان تعريف بجدران الحماية الخاصة بتطبيقات الويب، في ماي 2013 عن http://www.isecur1ty.org.

[3] أيمن عبد الحفيظ، مرجع سابق، ص 396.

4. يفضل عدم اختيار كلمة السر من بين الكلمات المعهودة مع تفضيل استعمال رمز غير متوافر في القاموس مثل استعمال أحرف مبعثرة لا تشكل كلمة معروفة أو خليط من الكلمات والأرقام وغير ذلك.

طبعاً جميع الأنظمة التي تم ذكرها ما هي إلى وسيله فقط لحماية وزيادة الأمن الفعلي ولا تعتبر حلول نهائيه للحد من المخاطر التي تهدد الأسرار المعلوماتية فبالطبع لكل نظام مما سبق طرق لتخطي الحمايات هذه ويمكن تخطيها فكما نعلم لا يوجد نظام أمن كامل ولا يوجد أيضاً حماية كاملة لأي نظام.

المطلب الثاني

الحماية الفنية عن طريق نظام الرقابة الوقائية عبر الوسائل الالكترونية

من القواعد الفنية الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة على النظام والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها نظام المراقبة الإلكترونية، إذ يعد هذا النظام من بين أهم آليات الوقاية من جرائم المعلوماتية وفي نفس الوقت تعتبر من القواعد الإجرائية الخاصة باستخلاص الأدلة المعلوماتية ويسمح القانون بهذا الإجراء في مجال التحقيق الجنائي، فعن المشرع الجزائري نص بخصوص هذا الأخير في المواد من 64 مكرر إلى 65 مرر10 من قانون الإجراءات الجزائية [1].

ويقصد بمراقبة الاتصالات الإلكترونية، العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني، والجدير بالكر أن المشرع الجزائري عرف الاتصالات الالكترونية من خلال نص المادة 02 من القانون 04/09 بأنها " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية ."

نص المشرع الجزائري على مراقبة الاتصالات الالكترونية في المادة 03 من القانون04/09 السالف الذكر والتي تنص على إمكانية وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، إذا تطلبت ذلك حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية، وذلك مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والاتصالات.

وخلاصة لما سبق فإن ضرورة مراقبة الاتصالات الالكترونية ترجع من ناحية إلى ازدياد معدلات الجريمة ومن ناحية أخرى إلى ازدياد استخدام المجرمين للتقنية المعلوماتية

[1] سنورد تفصيل عن اعتراض المراسلات السلكية واللاسلكية باعتبارها إجراء تحقيق في فصل التحقيق الجنائي في الجريمة المعلوماتية.

لإعداد وارتكاب جرائمهم، وما أقرها المشرع سوى لإقامة التوازن بين حق المجتمع في الأمن ومنع الجريمة، وحق الأفراد في السرية.

كما أنه يعتبر من آليات المكافحة الفنية للجريمة المعلوماتية، أيضا المرسوم الرئاسي رقم 228/15[1] المتعلق بالقواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو و الذي بدوره يساهم في المساهمة في الوقاية من الأعمال الإجرامية و حماية الممتلكات و الأشخاص بصفة عامة.

[1] مرسوم رئاسي رقم 228/15 المتعلق بالقواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو المؤرخ في 22 غشت 2015،جريدة رسمية عدد45، ص3.

الباب الثاني

الجرائم الواقعة على السرية المعلوماتية في إطار القانون الجنائي وآليات مكافحتها

جاءت ثورة المعلومات لكي تفرض على العالم تحديات كثيرة، ولّدها التطور العلمي والتكنولوجي والذي أدى إلى تهديد لبعض الحقوق والحريات وكان لابد للقانون أن يتحرك لمواجهة المتغيرات الاقتصادية والاجتماعية التي ولّدتها التكنولوجيا الحديثة.

وحيث ترتب على هذه الثورة الهائلة في مجال تكنولوجيا المعلومات والاتصالات، أن أصبح العالم يعيش حياة زاخرة بالاتصالات السريعة ونقل المعلومات عبر المسافات، والتحاور مع قواعد البيانات المحلية العالمية والتعامل مع نظم متقدمة للخبرة والذكاء الاصطناعي. كل هذا ما كان يمكن له أن يتحقق إلا بوجود هذا الشيء الرائع المسمى الحاسبات، والذي تتجلى عظمته عند ارتباطه بشبكات الاتصالات.ونحن الآن نجد أنفسنا أمام عالم مزدحم بشبكات اتصالية دقيقة تنقل وتستقبل المعلومات من مناطق جغرافية مختلفة دون عناء التنقل والترحال وأصبحت فيه للمعلومات بالغ الأهمية [1].

ومع ظهور الحاسبات، بدأت مسألة الحصول على المعلومات أيا كان نوعها تأخذ بعدا بل أبعادا جديدة وما يترتب على ذلك من جرائم مستحدثة، تلك الجرائم التي أطلقت عليها العديد من المصطلحات التي يمكن استعمالها للتعبير عن تلك الجريمة وهي الجريمة المعلوماتية، وتجدر الإشارة إلى أن هناك اختلاف كبير بشأن المصطلحات المستخدمة للدلالة على الظاهرة الجرمية في بيئة الكمبيوتر والانترنت، ومن بين أهم المصطلحات مصطلح الجريمة المعلوماتية، جرائم الكمبيوتر، جرائم التقنية العالية، جرائم الانترنت والإجرام في الفضاء الخيالي وغيرها.

كما اختلفت تقسيمات هذه الجرائم ومن ضمن تلك التقسيمات التقسيم الذي اعتمدته الاتفاقية الأوروبية "بودابست"، فقد تضمنت أربع طوائف رئيسة لجرائم الكمبيوتر والانترنت (الجريمة المعلوماتية) كالتالي:

الأولى وهي الجرائم التي تستهدف عناصر (السرية والسلامة والإتاحة) المعطيات والنظم وتضم الدخول غير قانوني، الاعتراض غير القانوني، تدمير المعطيات، إساءة استخدام الأجهزة. و**الثانية** تتعلق بالجرائم المرتبطة بالكمبيوتر وتضم التزوير والاحتيال المرتبط بالكمبيوتر. بينما **الثالثة** تضم الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية والأخلاقية. في حين تتعلق **الرابعة** **ب**الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة.

[1] - ويقرر في هذا الشأن أحد الخبراء أنه " لم تعد القوة النارية التي تمتلكها الجيوش وحدها هي التي تقرر مصير الحروب ورجحان كافة الأطراف المتقاتلة، وإنما المعلومات التي يملكها كل طرف حول الطرف الآخر، ويؤكد خبير أخر في هذا الصدد أن الحرب اليوم أصبحت حربا كلية، وهناك ثلاثة خطوط رئيسية تدور حولها: المعلومات السياسية والمعلومات العسكرية والمعلومات الاقتصادية، ولا يمكننا تمييز هذه المعلومات عن الأخرى. فكلها معلومات حيوية يجب أن يتحصل عليها من البلاد المعادية قبل وأثناء القتال لتتضح لنا الصورة عن قوة العدو. أنظر في ذلك منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات صورها ومشاكل إثباتها، رسالة دكتوراه جامعة القاهرة ، كلية الحقوق،سنة 2013، ص 151-152.

وتجدر الإشارة هنا أنه تم تخصيص هذه الدراسة للجرائم ضد السرية فقط، كما أنه تم الجمع بين قرصنة البيانات والبرامج في جريمة واحدة تحت تسمية سرقة المعلومات، رغم أن العديد يربط بين مصطلح القرصنة بالبرامج ولا يخصها بالبيانات. أي أن في نظرهم هناك سرقة البيانات المعالجة آليا أي معطيات الحاسوب وقرصنة البرامج وفي مضمونها يقصدون سرقة البرامج، وإنما هو تخصيص للمصطلحات فقط.

والأمر ذاته بالنسبة للاعتراض غير القانوني للبيانات وهو ما سميناه التجسس الالكتروني كما سيرد التفصيل فيه أدناه، بينما لا إشكال فيما يتعلق بباقي جرائم الدراسة.

وتجدر الإشارة أيضا إلى أنه تم الاقتصار على أهم الجرائم الماسة بالسرية المعلوماتية، وتم تجاوز بعض الجرائم التي قد يكون فيها إضرار بالمعلومات السرية وإضرار بأصحابها، هي في الواقع تنتمي إلى تقسيم آخر أكثر منه علاقتها بانتهاك السرية كجريمة الإتلاف، والذي بدوره قد يكون محله معلومة سرية ولكنه لم يستهدف سريتها بقدر ما يستهدف وجودها، حيث يكون المقصود منه هو ضياعها.

إن الاعتداء على الأسرار المعلوماتية هي سلوكات تم تجريمها من خلال نصوص عقابية من طرف جل دول العالم نظرا لخطورة هذه الجرائم وما يحققه مرتكبيها من أرباح مادية ومعنوية في مواجهة ضحاياها وذلك باستخدام وسائل التقنية الحديثة ونحن نعني في هذا المقام الحاسوب والانترنت على وجه الخصوص، ذلك أنه أصبح أي الحاسوب هو هدف ووسيلة الجريمة المعلوماتية وذلك كما في حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وكما في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم وهو وسيلة أيضا لمعالجة المعلومات السرية وتخزينها وعلى الأغلب إحاطتها بكل وسائل الحماية الفنية الحديثة لحمايتها من خطر الانتهاك.

والملاحظ أنه كلما كان صاحب السر حريصا على المحافظة على سره داخل الحاسوب وتأمينه ورغم ذلك فالواقع أن هناك من هو أحرص منه على هتك تلك الحماية إن وجدت وانتهاكه بكل الطرق والأغراض وراء ذلك تتعدد كما سبق وأن أشرنا في دوافع ارتكاب الجريمة المعلوماتية. ورغم تزايد الأبحاث ومحاولات ابتكار أنظمة تكفل لأي نظام معلوماتي الحماية اللازمة إلاّ أنه في المقابل يتم تطوير الإجراءات المضادة لهذه الحصون الأمنية.

وأمام المخاطر الجسيمة التي تتسبب فيها هذه الجرائم، بادرت كثير من الدول إلى تبني سياسة جنائية جديدة تتوائم مع هذا النمط المستحدث من الإجرام. فذهبت بعض الدول إلى

إدخال تعديلات جزئية في التشريعات الجنائية القائمة بما يكفل توفي الحماية للسرية المعلوماتية، في حين خطا بعضها الآخر خطوات متقدمة بسن تشريعات خاصة .

ونظرا لما تتميز به الجرائم الماسة بالسرية المعلوماتية من خصوصية خاصة أخذها أحيانا البعد الدولي فكان لابد من تخصيص زاوية في هذه الدراسة، تعنى بها الإجابة عن كيفية التحقيق في هذه الجرائم ومن هي الجهة المختصة في إصدار الأحكام القضائية في مواجهة مرتكبيها إن تم الكشف عنهم. إضافة إلى أنه لابد من تعاون دولي للقضاء عليها، وكل ذلك سيتم التفصيل فيه على النحو التالي:

الفصل الأول: الاعتداءات على الأسرار المعلوماتية و تجريمها

الفصل الثاني: الجوانب الإجرائية و الأمنية لمكافحة الجرائم الواقعة على الأسرار المعلوماتية

الفصل الأول

الاعتداءات على الأسرار المعلوماتية وتجريمها

قد ألقت الثورة المعلوماتية بظلالها على قوانين العقوبات، خاصة في تلك الدول التي استفادت من ثمار هذه الثورة ووجب عليها في الوقت ذاته أن تتلافى عيوبها، وما أوجدته من جرائم فتاكة تصدت لها جل القوانين العقابية. والملاحظ في هذا المجال أنه كلما كان الاعتماد أكبر على التقنية المعلوماتية كلما كانت الحاجة أكثر إلحاحا لوضع نصوص لحماية هذه المعلوماتية. لهذا نرى أن الدول المتقدمة معلوماتيا كانت السباقة في مجال التجريم المعلوماتي.

ولما كانت أيضا الحاجة ملحة لحماية المعلومات السرية الالكترونية ضمن أوجه التجريم المعلوماتي، كان لابد من الوقوف عند الجرائم الماسة بالسرية المعلوماتية، دون الجرائم المعلوماتية الأخرى التي لا تدخل في موضوع هذه الدراسة وسيكون التفصيل في الجرائم ضد الأسرار المعلوماتية في نطاق قانون العقوبات (مبحث أول) من جهة ومن خلال نصوص الملكية الفكرية (مبحث ثان) من جهة أخرى.

المبحث الأول

تجريم الاعتداء على الأسرار المعلوماتية في نطاق القانون الجنائي

تتخذ السرية المعلوماتية أشكالا متعددة، ويأتي التعدد فيها كنتيجة طبيعية لتنوع المجالات التي تستخدم فيها المعلوماتية، حيث أن وكما سبقت الإشارة أصبح للحاسب الآلي قوة هائلة وانخفاض مثير في السعر والحجم ما أدى إلى بزوغ استعمالات هائلة لهذا الأخير من الأفراد والمؤسسات ولم تكن لتلك الاستعمالات ايجابياتها فقط بل كان لها سلبياتها أيضا، كذلك الشأن بالنسبة للمعلومات المخزنة أو المتناقلة عبر الهاتف الخلوي الذي يعتبر أحد الأجهزة الذكية التي تدار بواسطة أحد البرامج المعلوماتية حيث أصبحت المعلومات المعالجة بواسطته تعتبر جزء منه، ما جعل المعلومات السرية داخلها والمتنقلة عبرها في خطر دائم استوجب المداهمة.

فإلى جانب الاتفاقيات الدولية، تصدت نصوص التجريم من خلال قانون العقوبات و القوانين المكملة له لكل السلوكات المستحدثة الواقعة على الأسرار المعلوماتية، و حيث تعددت سلوكات انتهاك السرية المعلوماتية والتي من خلال هذه الدراسة سنحاول الوقوف عند أهمها كالدخول والبقاء غير المصرح بهما لنظام المعالجة الآلية للمعطيات (مطلب أول)، جريمة التعامل في معلومات غير مشروعة (مطلب ثان)، سرقة المعلومات (مطلب ثالث)، التجسس المعلوماتي (مطلب رابع)، إفشاء الأسرار المعلوماتية المهنية(مطلب خامس).

المطلب الأول

جريمة الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات [1]

[1] - جريمة الدخول غير المصرح به إلى أنظمة المعالجة الآلية للمعطيات تقع عدوانا على سرية المعطيات، وهي تتم بغض النظر عما تم الإطلاع عليه من معطيات داخل النظام، وبغض النظر عن طبيعة هذه الأخيرة والوضع هنا شبيه بجريمة انتهاك حرمة العقار فهي تتم بالدخول إلى العقار بصرف النظر عما يحويه هذا العقار داخله وعن طبيعة هذا المحتوى.

لقد تم تصنيف هذه الجريمة تحت باب الجرائم المعلوماتية المرتكبة بواسطة النظام المعلوماتي وتم البدء بهذه الجريمة في هذه الدراسة لأنها تعتبر أهم الجرائم أو بالأحرى يعد الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي المرحلة السابقة والضرورية لارتكاب الجرائم المعلوماتية الأخرى مثل سرقة المعلومات وتزويرها، التجسس المعلوماتي ، الاعتداء على حرمة الحياة الخاصة، وغير ذلك من الجرائم التي سيتم التفصيل في بعضها دون الآخر. إذ سيتم مناقشة الجرائم التي يتم من خلالها الاعتداء على المعلومات (السرية بالضرورة لأن غير السرية سبق وأن أشرنا أنها لا تعني بالحماية القانونية محل الدراسة).كما أن مرتكب هذا الجرم قد لا يقصد بالضرورة ارتكاب جريمة من ورائه بل يقصده بحد ذاته أي الدخول والبقاء فقط، وهي الحالة التي أثارت نقاش وخلاف الفقه حول مدى انطباق وصف الجريمة المعلوماتية على مجرد الدخول والبقاء إلى النظام المعلوماتي؟ وهل تستوجب الحماية الجنائية أم لا؟، ونتيجة الخلاف انقسم الفقه إلى اتجاهين إذ أن أحدهما نادى إلى تجريم الفعل والآخر نادى إلى أنه لا داعي لتجريمه لمجرد الدخول.
وللتفصيل في هذه الجريمة سنحاول التطرق إلى مدى تجريمها على الصعيدين الدولي والداخلي (الفرع الأول) وكذا أركانها (الفرع الثاني).

الفرع الأول
تجريم الدخول والبقاء على الصعيد الدولي والداخلي

نصت اتفاقية بودابست[1] على هذه الجريمة في المادة الثانية تحت عنوان " الدخول غير القانوني" والتي تشير إلى أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا للقانون الداخلي الولوج العمدي لكل أو لجزء من جهاز الحاسب الآلي بدون حق. كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن بغية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى أو ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد بحاسب آلي آخر.[2]

وأشارت المذكرة التفسيرية لاتفاقية بودابست بأن الدخول غير المشروع يعد الجريمة الرئيسية التي تنطوي على التهديد والتعدي على الأمن المعلوماتي، بمعنى السرية والسلامة وإتاحة النظم والبيانات المعلوماتية. إذ أن هذا الدخول يمكن أن يترتب عليه الوصول إلى

[1] - اتفاقية بودابست المبرمة في 8 نوفمبر سنة 2001 والخاصة بحماية المعلوماتية ومنع وقمع الإجرام المعلوماتي.
[2] رشيدة بوبكر، مرجع سابق، ص 162.

بيانات سرية مثل كلمة المرور، أو معلومات عن النظام الهدف وأسرار تسمح باستخدام النظام مجانا[1]. فتعرضت الكثير من أنظمة الحاسبات الآلية، وبصفة خاصة تلك التي تعمل من خلال شبكات المعلومات، إلى اختراق بواسطة أشخاص غير مصرح لهم بالدخول إليها، وفي الولايات المتحدة الأمريكية حيث كان الظهور الأول لهذه الظاهرة، حيث أطلق آنذاك على هؤلاء الذين يدخلون إلى أنظمة الحسابات الآلية بدون تصريح القراصنة قياسا على الأشخاص الذين كانوا يقومون في الماضي باعتراض البرامج الإذاعية.[2]

وجرم السلوك أيضا القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لعام 2004 في المادة الثالثة:" كل من دخل عمدا وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس..... والغرامة.....أو بإحدى هاتين العقوبتين"[4]، وجرمت هذه الجريمة أيضا في المادة 06 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[3].

وأما عن المشرع الفرنسي، فجرم هذا الفعل في المادة 1/323 من قانون العقوبات[4] وعاقب من خلال النص مرتكب فعل التوصل غير المصرح وفعل البقاء بصورة غير مصرح بها داخل النظام.

---

[1] هلالي عبد الله، مرجع سابق، ص 69.

[2] تم التعبير عن مجرم معلوماتي في فرنسا بنفس المصطلح أي القرصان وهو شخص دخل في النظام المعلوماتي لهيئة ANSES وهي الوكالة الوطنية للحماية الصحية للتغذية البيئة والعمل، وهي أشهر القضايا في فرنسا في 2013، مشار إليه لدى

Laure ZICRY, Enjeux et maitrise des cyber-risques ,largus , edition , France2014, p.63.

[4] القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتي وما في حكمها لعام 2004 والذي اعتمدته جامعة الدول العربية.

[5] المادة 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المؤرخة في ديسمبر 2010 تنص على الآتي:" جريمة الدخول غير المشروع:

- 1الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

- 2تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ – محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال وإلحاق الضرر بالم ستخدمين والمستفيدين.

ب - الحصول على معلومات حكومية سرية".

[4] Article 323-1 , de la loi n°2015-912 du 24 juillet 2015 :

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende..”

أيضا فقد عاقب القانون الفرنسي المساهمين في ارتكاب هذه الجريمة بنفس العقوبة المقررة للفاعل الأصلي وفقا للمادة (4/323)[1]، كذلك فقد تم العقاب أيضا على الشروع في هذه الجرائم بالعقوبة المقررة أصلا للجريمة التامة وفقا للمادة (7/323)[2]. ويعتبر هذا اتجاه منتقد من المشرع الفرنسي، ذلك لأن فيه إفقاد لمعنى ظروف التخفيف، ولا يشجع الفاعل على العدول عن ارتكاب الجريمة متى ما بدأ بتنفيذها[3].

وأدرك المشرع الجزائري أيضا الطبيعة الخاصة للولوج إلى النظام وحرص بدوره على تجريم الفعل والنتيجة في المادة 394 مكرر من قانون العقوبات. فأما الفعل فهو الدخول غير المصرح به وأما النتيجة فهي تشديد المشرع للعقاب إذا ترتب على هذا الفعل حدوث أضرار بالمعلومات ونظم معالجتها فضلا عن تجريم فعل البقاء.

فللولوج أو الدخول إلى النظام المعلوماتي يكفي معرفة الطريقة الواجب إتباعها، مما يفسح المجال للمتدخل الحصول على كل ما يريد من معلومات مخزونة في هذا النظام، وأكثر من ذلك فإن عملية الدخول تسمح له بالدخول إلى شبكات المؤسسات والإدارة الحائزة لهذا النظام كما تسمح له بالوصول إلى شبكات أخرى تكون مرتبطة به[4]، ويضم الولوج غير المصرح به الاختراق الذي يحدث للنظام بأكمله أو جزء منه.

فإذا دخل شخص النظام فكان بمقدوره معرفة كل المعلومات التي يريد الحصول عليها والمعلومات المقصودة هنا هي المعلومات والبيانات المخزونة داخل النظام لاستخدامها في غرض ما، أول لمجرد التسلية والرغبة في الاستطلاع، أو لإشباع الشعور بالنجاح في اختراق النظام على الرغم من الاحتياطات الأمنية.

أما المعلومات فهي تشمل كل ما يمكن أن يحتوي عليه النظام من بيانات كالسجلات والبيانات الخاصة بالعملاء في البنوك، والبيانات الشخصية للمواطنين في السجلات المدنية والأسرار العسكرية للدولة وبرامج الكمبيوتر بصفة عامة[5]. وقد يتعرض النظام المعلوماتي

---

[1] Article 323-4, La Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004 ":La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée".

[2] Article 323-7 En savoir plus sur cet article.modifié par Loi n°2004-575 du 21 juin 2004 - art. 46 JORF 22 juin 2004 ":La tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines".

[3] محمد احمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع عمان الأردن ، الطبعة الأولى،2009، ص 86-87.

[4] - نعيم مغبغب، حماية برامج الكمبيوتر، دراسة في القانون المقارن، الطبعة الثانية، منشورات الحلبي الحقوقية بيروت، 2009 ، ص 234.

[5] - نعيم مغبغب، المرجع نفسه ، ص 234-235.

إلى الاختراق من قبل أفراد غير مصرح لهم بالدخول إليه أوالبقاء فيه وقد ساهم في انتشار هذه الظاهرة تطور الاتصالات وتنامي شبكات المعلوماتية[1].

فبعد ظهور الإنترنت ازدادت عملية التدخل خطورة، وإذا هم أي الجناة يدخلون في الشبكات المرتبطة بالانترنت فيتوصلون إلى المعلومات ولو كانت محمية. مما قاد إلى زيادة درجة حمايتها، وإزاء هذه المخاطر نادت الدول لعقد المؤتمرات بهدف وضع الاتفاقيات الدولية للحد من مخاطر استعمال هذه التقنيات[2].

ويمكن تصور هذا المجرم عندما يتم الدخول إلى النظام والوصول إلى البيانات والبرامج المخزونة أو اعتراض عمل الحاسب الآلي أثناء قيامه بإحدى العمليات، أو مجرد استعمال الكمبيوتر ونظامه فجريمة الدخول بدون إذن أو غير المصرح به إلى نظام الحاسب يعني اختراق الفاعل لهذا النظام مما يفرض عليه معرفة تقنية الكمبيوتر [3].

ويتحقق الدخول غير المشروع، متى كان ذلك الدخول مخالفا لإرادة صاحب النظام أو ممن له حق السيطرة عليه، ويتحقق الاختراق أو الدخول غير المشروع كذلك حين يضع مالك النظام قيودا على الدخول إلى ذلك النظام، ولا يحترم الجاني هذه القيود، أو كان الأمر يتطلب سداد مبالغ من النقود لم يسددها الجاني الذي قام بالدخول غير المشروع إلى النظام[4].

ويمكن القول بصفة عامة، إن الدخول غير المصرح به إلى النظام المعلوماتي يتحقق بالوصول إلى المعلومات والبيانات المخزونة داخله دون رضاء المسؤول عن هذا النظام أو المعلومات التي يحتوي عليها، أو هو بقول آخر إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه، للوصول إلى المعلومات والبيانات المخزنة بداخله لاستخدامها في غرض ما، أو لمجرد التسلية والرغبة في الاستطلاع، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي على الرغم من الاحتياطات الأمنية التي يحتويها نظامه للحيلولة دون ذلك وهو ما يطلق عليه الدخول المجرد إلى النظام المعلوماتي.

وتجدر الإشارة إلى أنه يقصد المعلومات هنا بمعناها الواسع[5]، فتشمل كل ما يمكن أن يحتوي عليه الحاسب الآلي من بيانات، كالسجلات الطبية، والبيانات الخاصة بالعملاء في البنوك، والبيانات الشخصية للمواطنين في السجلات المدنية، والأسرار العسكرية للدولة،

---

[1] - نهلا عبد القادر مومني، مرجع سابق، ص 156.

[2] - مثلا انعقد مؤتمر عالمي في الصين في سنة للحد من مخاطر اختراق الأنظمة المعلوماتية ووضع المجلس الأوروبي في 1989 توصية لاستصدار قوانين جزائية تعاقب المتدخلين وتمكن من ملاحقتهم دوليا.

[3] - نعيم مغبغب، مرجع سابق، ص 235.

[4] - عبد الفتاح بيومي حجازي، مرجع سابق، ص 79.

[5] المقصود بالمعلومات بمعناها العام أي المعلومات والبرامج وليس المعلومات بالمعنى العام أي كل ما يمكن أن يطلق عليه مصطلح المعلومة بالمفهوم المجازي.

وبرامج الحاسب الآلي بصفة عامة[1] ،والمعلومات التي قد يقع عليها هدا السلوك أي الدخول أو البقاء غير المصرح به على قدر من الأهمية[2].

ولقد ثار جدل ضخم بين الفقهاء ما بين مؤيد ومعارض لتجريم الدخول غير المصرح به إلى النظام المعلوماتي، والحقيقة أنه إذا ما استعرضنا الاحتمالات المختلفة التي قد تعقب هذا الدخول فسوف نجد أن هذا الدخيل قد يقوم بإحدى الأعمال الآتية، فقد يقوم بمجرد قراءة هذه المعلومات أوقد يقوم بنسخها والتي قد تكون في غاية السرية أوقد يقوم بمحو أو تغيير كل أو بعض المعلومات، وقد يضيف شيئا إلى هذه المعلومات. ولا شك أن الدخول غير المصرح به إلى نظام الحاسب الآلي سواء كان مقصودا في ذاته أو كان بغرض ارتكاب جريمة أخرى قد يكون له الكثير من الآثار السلبية التي تلحق صاحب هذه المعلومات.

وبالإضافة إلى ما سبق فإن قابلية المعلومات للوصول غير المشروع إليها يفوق كثيرا ما كان عليه الحال قبل عصر الحاسبات الآلية، ذلك أن المعلومات الهامة والمدونة في أوراق وسجلات كان يتم حفظها في أماكن يصعب الوصول إليها، مما يجعلها بمنأى عن التلاعب بها .

في حين أن المعلومات المبرمجة آليا، والتي تصل فيما بينها عن طريق شبكة اتصالات تكون أكثر عرضة للوصول غير المشروع إليها، فالأمر هنا أشبه بصندوق مغلق يحتوي على سجلات هامة ومتروك في مكان عام، بحيث لا يتعدى الأمر إيجاد المفتاح المناسب لهذا الصندوق، ولا يخفى هنا الوقت المتسع الذي يتمتع به الفاعل في البحث عن هذا المفتاح[3].

ويترتب في كثير من حالات الدخول غير المصرح به خسائر مادية كبيرة، بل قد تترتب هذه الخسائر على مجرد محاولة وقف هذا الدخول ولو لم يترتب عليه أضرار فعلية تلحق بالنظام وبالمعلومات التي يحتوي عليها. مثال ذلك الحالة التي تمكن فيها أحد الأشخاص من الدخول إلى نظام الحاسب الآلي الخاص بأحد المعامل الخاصة بتصنيع وتجربة الأسلحة النووية بكاليفورنيا بالولايات المتحدة الأمريكية، وقد تحمل المعمل خسائر مدية قدرت بحوالي مائة ألف دولار أمريكي وهي تكلفة آلأبحاث التي أجريت لمحاولة وقف هذا الدخول غير المصرح به[4].

وعلى الرغم مما قد يترتب على الدخول غير المصرح به لنظام الحاسب الآلي من أضرار، وهو ما دفع بالكثيرين إلى المطالبة بضرورة تجريمه، إلا أن هناك رأيا يذهب إلى

[1] نائلة عادل محمد فريد قورة، مرجع سابق، ص 316.
[2] - رشيدة بوبكر، مرجع سابق، ص 160.
[3] - نائلة عادل محمد فريد قورة، مرجع سابق ، ص 317.
[4] - نائلة عادل محمد فريد قورة، المرجع نفسه ، ص 317.

خلاف ذلك[1]. إذ يرى أصحاب هذا الرأي أنه لا توجد ضرورة تستدعي تجريم مجرد الدخول أو البقاء غير المصرح بهما إلى نظام المعالجة الآلية، وخاصة إذا لم يكن لدى الفاعل فيه لارتكاب جريمة لاحقة على هذا الدخول أو البقاء، ويبرر هذا الاتجاه رأيه أن هذا السلوك لا يخرج عن كونه عن طريقة لعرض القدرات التقنية والذهنية التي يتمتع به الشخص الذي قام بهذا الفعل[2] وهذا الأمر لا يشكل بحد ذاته جريمة تستدعي معاقبة الفاعل[3].

إلا أن الحجج السابقة التي ساقها أنصار هذا الرأي المتقدم لا يجب أن تقف حائلا دون تجريم الدخول غير المصرح به إلى نظام الحاسب الآلي[4]، والجدير بالذكر أن أغلبية الفقه الذي رأى ضرورة تجريم هذا الفعل ذلك أنه يعد مرحلة أساسية لارتكاب بقية جرائم تقنية المعلومات الأخرى[5].

ولقد تم بالفعل تجريم الدخول والبقاء غير المصرح به إلى النظام المعلوماتي من طرف العديد من الدول[6] وإن اختلفت فيما بينها من حيث الشروط المتطلبة لأعمال نصوصها، فالدخول غير المصرح به إلى النظام ا وإن كان يتم بوسيلة منطقية وحيدة قومها البحث والوصول إلى المعلومات باستخدام وسائل إلكترونية، إلا أنه ينبغي تحديد مواصفات هذه الوسيلة والتي قد تتخذ شكل القيام بعملية دخول غير مصرح به أو البقاء غير المشروع داخل النظام بعد عملية دخول مشروعة أو غير مشروعة.

كما أنه ينبغي تحديد المحل الذي ينصب عليه فعل الدخول، والذي قد يكون معلومة أو نظم للحاسب الآلي أو شبكة معلومات. ومن ناحية أخرى، فإن تحديد الهدف الذي يعقب عملية الدخول قد آثار خلافا أظهرته النصوص القانونية المختلفة التي تناولت هذه الجريمة.

---

[1] - نائلة عادل محمد فريد قورة، المرجع نفسه، ص 315-318.

[2] - يستلزم القيام بمثل هذا العمل الإجرامي أي – الولوج غير المشروع للمعلومات المعالجة آليا – وجود المجرم المعلوماتي داخل أحد المراكز المعلوماتية حيث أن كل ما يهمه في هذا العرض هو الولوج إلى المعلومات التي تمت معالجتها بأي من الأنظمة المعلوماتية والاطلاع غير المصرح به على ذلك المعلومات المخزنة في ذاكرات النظم المعلوماتية ، مشار إليه لدى احمد خليفة الملط، مرجع سابق، ص 190.

[3] - نهلا عبد القادر مومني، مرجع سابق، ص 157.

[4] - نائلة عادل محمد فريد قورة، مرجع سابق، ص318.

[5] - رشيدة بوبكر، مرجع سابق، ص 160.

[6] - المادة 394 مكرر من قانون العقوبات الجزائري، 1/323 قانون عقوبات فرنسي، المادة الأولى من القانون الانجليزي الخاص بإساءة استخدام الحاسبات الآلية لعام 1990، المادة 1/202 قانون عقوبات ألماني ، المواد 7 و8 من القانون البرتغالي لجرائم المعلوماتية لعام 1991، المادة 263 قانون العقوبات الدانماركي المادة 3/370 من قانون العقوبات اليوناني، المادة 21 من القانون السويدي للمعلوماتية لعام 1973، المادة 138 قانون العقوبات الهولندي، المادة 1030 من القانون الفيدرالي لإساءة استخدام الحاسبات الآلية في الولايات المتحدة الأمريكية، الفقرة الثانية والرابعة من المادة 76 من قانون العقوبات الاسترالي، الفقرة الأولى من المادة 342 من قانون العقوبات الكندي، المادة 525 من قانون العقوبات التركي، المادة الثامنة من الفصل 38 من قانون العقوبات الفنلندي، الفقرة الأولى من المادة 509 من قانون عقوبات لوكسمبورج، المادة 143 مكرر من قانون العقوبات السويسري، المادة 145 من قانون العقوبات النرويجي، مشار إليه لدى نعيم مغبغب، حماية برامج الكمبيوتر، المرجع السابق، ص 235-236.

فالدخول غير المصرح به إلى النظام المعلوماتي يستمد عدم مشروعيته من كونه غير مصرح به أو كونه مخالفا لأحكام القانون، إلا أن هذا الدخول قد يكون مقصودا في ذاته، كما قد يكون مقصودا باعتباره وسيلة لتحقيق غاية أخرى سواء تمثلت هذه الغاية في الحصول على المعلومات لتحقيق غرض ما، أو كان الدخول في النظام ممرا يتم من خلاله الدخول في نظام آخر من الصعب على الفاعل الدخول إليه[1].

الفرع الثاني

أركان جريمة الدخول أو البقاء غير المصرح بهما إلى نظام المعالجة الآلية للمعطيات

الأصل أن جريمة الدخول إلى النظام جريمة نشاط وليست جريمة ضرر في غالبية التشريعات المقارنة، مادام أنه لا يلزم لوقوعها تحقق ضرر من نوع معين، ومما يدل على أنها جريمة ضرر أن المادة 323 -1 من قانون العقوبات الفرنسي تتضمن فقرة ثانية تشدد عقوبة الدخول إذا ترتب عليه ضرر وكذلك الشأن بالنسبة للمادة 394 مكرر من قانون العقوبات الجزائري.

وقد تعتبر الجريمة مستمرة إذا اتخذ السلوك المكون لها صورة البقاء في النظام أو جزء منه، ويكون مرد هذا الاستمرار في موقف الجاني، أما إذا اتخذ السلوك المكون للجريمة صورة الدخول إلى النظام، فإن الجريمة تكون وقتية لأن هذا السلوك يبدأ ويتم في آن واحد، فضلا على أنه غير قابل بطبيعته للاستمرار، فجريمة الدخول إلى النظام أو البقاء فيه تتكون من ركنيين مادي ومعنوي.

أولا: الركن المادي

انطلاقا من نص المادة 394 مكرر من قانون العقوبات الجزائري والنصوص القانونية السابقة فإن تحقق الركن المادي لجريمة الدخول[2] أو البقاء بغش[1] أو غير المصرح به يتسم

---

[1] - نائلة عادل محمد فريد قورة، ص 319-320.

[2] تعددت التعريفات التي قيلت بشأن الدخول ومن أهمها ما يلي: عرف الدخول على أنه " عملية ولوج غير شرعي إلى نظام التشغيل في الحاسب من قبل أشخاص لا يملكون صلاحيات الدخول وذلك بهدف القيام بأعمال غير قانونية مثل التجسس أو السرقة أو التخريب مع الأخذ بعين الاعتبار قدرة هؤلاء الأشخاص على نقل ومسح أوإضافة ملفات وبرامج، والقدرة على التحكم بنظام التشغيل وإصدار الأوامر". أنظر في ذلك رشيدة بوكر، مرجع سابق، ص 178 ، أوأنه " الولوج إلى المعلومات داخل نطاق الاختراق الذي يحدث للنظام المعلوماتي بأكمله أولجزء منه أيا كان سواء كان جزءا ماديا أو برامج جزئية أو مجرد بيانات مخزنة في نظام النصيب عن طريق التوصل إلى الأرقام أو الكلمات أو الشفرات أو الحروف أو المعلومات السرية".أنظر في ذلك بلال أمين زين الدين، مرجع سابق، ص 259 ، ويعرف أيضا أنه " عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الالكترونية بواسطة برامج متطورة يستخدمها كل من خبرة في استعمالها."أنظر في

بسلوك إجرامي يرتكبه الجاني قد يتخذ صورة الدخول المنطقي وذلك لفتح باب يؤدي إلى نظام المعالجة الآلية بمكوناته المختلفة، وأحيانا يتخذ صورة البقاء وينصب هذا السلوك على محل معين هو المعلومات ونظم معالجتها وهذا السلوك قد يلحق أضرار في بعض الحالات بهما[2] إذن فالركن المادي هو عبارة عن نشاط ايجابي من جانب الجاني، ويكون الاتصال بطريق الغش متى كان الجاني لا يحق له الدخول لأي سبب من الأسباب ، وهو تعبير يتسع لاستعمال كل الوسائل المتاحة للدخول إلى النظام ولكن الضابط والمعيار في ذلك هو انعدام حقه في الدخول بهذا النظام المعلوماتي كله أو جزء منه، فمدلول كلمة دخول تشير إلى كل الأفعال التي تسمح بالولوج إلى نظام معلوماتي والإحاطة والسيطرة على المعطيات والمعلومات التي يتكون منها.[3]

ويتحقق الركن المادي بإحدى الصور التالية : أولهما : اختراق الأجهزة الرئيسية بطريق الغش إلى نظام المعالجة الآلية للمعطيات، وثانيهما : البقاء أو المكوث بطريق الغش في نظام المعالجة الآلية أو جزء منه ، فمن الواضح من خلال نص المادة 394 مكرر أنه هناك صورة بسيطة للدخول إلى النظام أو البقاء فيه وأخرى شدد فيها المشرع العقوبة إذ نصت المادة 394 مكرر من قانون العقوبات أنه " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين، والغرامة من 50.000 دج إلى150.000 دج ".

ومن خلال استقراء نص المادة 394 مكرر نجد أنها قد نصت على ظرفين تشدد بهما عقوبة الدخول، أو البقاء داخل النظام، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أ وتعديل البيانات التي يحتويها النظام، أو عدم قدرة النظام على تأدية وظيفته، ويكفي لتوفير هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام، أو عدم قدرته على أداء وظيفته، أو تعديل البيانات.

هذا خالد ممدوح ابراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008، ص 84. كذلك يعرف أنه " الولوج غير المصرح به أوبشكل غير مشروع إلى نظام المعالجة الآلية للبيانات باستخدام الحاسوب" أنظر في ذلك رشيدة بوكر، مرجع سابق، ص 179 ، مشار إليه لدى فتحي محمد أبو عزت، الحماية الجنائية الموضوعية والإجرائية، الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي، دار النهضة العربية، القاهرة ، 2007، ص 128.

[1] – يقصد بالغش الدخول في النظام المعلوماتي مع العلم بأنه غير جائز أو مباح من طرف مالكها، وهنا يتم الدخول مثلا بعد التلاعب بوسائل الحماية التقنية لهذا النظام محل الجريمة، مشار إليه لدى دردور نسيم، مرجع سابق، هامش 3، ص 30 .

[2]- رشيدة بوكر، مرجع سابق، ص 163.

[3] - نهلا عبد القادر مومني، مرجع سابق، ص 158.

وهذه الجريمة عمدية يتعين لقيامها توافر القصد الجنائي العام لدى الجاني بعنصرية العلم والإرادة فإذا أثبت الجاني انتفاء العلاقة السببية بين السلوك الإجرامي – الدخول أو البقاء غير المشروع – والنتيجة الإجرامية التي هي ذات الظرف المشدد في الجريمة، كأن يثبت أن تعديل أو محو المعطيات أو أن عدم صلاحية النظام لقيام بوظائفه يرجع إلى القوة القاهرة، أو الحادث المفاجئ، انتفى السلوك الإجرامي، وانتفى بذلك معه القصد الجنائي.

إذن السلوك في جريمة الدخول أو الولوج إلى النظام أو البقاء فيه غير المصرح بهما يتحقق بفعل الدخول أوالبقاء وسنتعرض لكلا السلوكين كالتالي:

أ-فعل الدخول غير المصرح به[1]

لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، إنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان،أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات. ولم يحدد المشرع وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة ويستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر[2]، تقوم هذه الجريمة بتحقق فعل الدخول إلى النظام المعلوماتي، ومدلول كلمة الدخول تشير إلى كل الأفعال التي تسمح بالولوج إلى نظم المعلومات والإحاطة أو السيطرة على المعطيات والمعلومات التي يتكون منها.

وفعل الدخول الذي يشكل الركن المادي في هذه الجريمة لا يقصد به الدخول المادي إلى المكان الذي يتواجد به الحاسوب ونظامه، بل يقصد به الدخول باستخدام الوسائل الفنية والتقنية إلى النظام المعلوماتي أي الدخول المعنوي أو الإلكتروني[3].

ويقصد بالدخول أيضا الاتصال بجهاز حاسب آلي خاص بشخص الغير بدون موافقته. ويتخذ الدخول صورا مختلفة؛ فمنها أن يقوم الفاعل بتشغيل جهاز مغلق وبالتالي الاطلاع على ما به من بيانات. ومنها ما يقوم به الفاعل من استخدام برامج للدخول في النظام بدون إذن صاحبه فيطلع على ما يقوم به صاحب الجهاز أوينتقل بين أجزاء الجهاز ليطلع على ما يحتويه أقسام هذا الجهاز من معلومات.

---

[1] هناك اختلاف بين المفهوم القانوني والمفهوم التقني للدخول بطريق الغش لأي نظام معلوماتي، للتفاصيل راجع في ذلك CHAMPY Guillaume, La fraude informatique, tome 1, Presses Universitaires d Aix-Marseille, 1992, p73.

[2] فشار عطا الله ، مواجهة الجريمة المعلوماتية في التشريع الجزائري ، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية،بأكاديمية الدراسات بليبيا في أكتوبر 2009 ، منشور على الموقع الالكتروني http://www.droit-dz.com/.

[3] نهلا عبد القادر مومني، مرجع سابق، ص 158.

غير أن الدخول لا يلزم فيه أن يقوم الفاعل بالاطلاع على ملفات صاحب الجهاز أو على ما يقوم به من أعمال، بل يكفي لوقوع النشاط المعاقب عليه أن يقوم المتهم بفتح الجهاز أو أن يتمكن من الدخول عن بعد بالنظام، حتى ولو كانت الملفات محمية بكلمة المرور ولم يتمكن من فتحها[1].

ويتساوى في هذا المجال إن تم هذا الدخول بطريق مباشر إلى المعلومات أو تم عن طريق الاعتراض غير المشروع لعمليات الاتصال من أجل الدخول إلى النظام المعلوماتي[2].

وفعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع، وإنما يتخذ هذا الفعل وصفة الجرم انطلاقا من كونه قد تم دون وجه حق، أو بمعنى آخر دون تصريح، ومن الحالات التي يكون فيها الدخول غير مصرح به إلى النظام المعلوماتي[3]، دخول الفاعل إلى النظام المعلوماتي دون الحصول على تصريح من المسؤول عن النظام أو مالكه، وقد يكون الفاعل مصرحا له بالدخول إلى جزء من النظام إلا أنه يتجاوز التصريح الممنوح له ويدخل إلى كامل النظام أو إلى جزء آخر يحظر عليه الدخول إليها، وهذا الفرض يتم في الغالب من قبل العاملين في المؤسسات التي يوجد بها النظام المعلوماتي[4].

كما أن عدم التصريح بالدخول ينصرف إلى الحالات التي يكون فيها هذا الدخول مشروطا بدفع ثمن محدد وبالرغم من ذلك يدخل الفاعل إلى النظام دون أن يقوم بتسديد هذا الثمن، أما إذا كان الولوج إلى النظام المعلوماتي بالمجان وكان متاحا للجمهور، ففي هذه الحالة يكون الدخول إليه حقا من الحقوق[5].

وقد حدث خلاف في الفقه[6] حول مدى أحقية النظم المعلوماتية التي لا يحميها نظم أمنية معينة بالحماية الجنائية ضد الدخول غير المصرح به[7]، وقد كان هناك اتجاهان: وهما

---

[1] شيماء عبد الغني محمد عطا الله، مكافحة جرائم المعلوماتية في المملكة العربية السعودية وفقا لنظام مكافحة جرائم المعلوماتية الصادر في 7/ 3/ 1428 هـ الموافق 26/ 3/ 2007 المنشور على الموقع الالكتروني http://faculty.ksu.edu.sa، أطلع عليه بتاريخ 2015/02/02.

[2] نهلا عبد القادر مومني، مرجع سابق، ص 158.

[3] نهلا عبد القادر مومني، المرجع نفسه، ص 159.

[4] أنظر تفاصيل أكثر حول انعدام التصريح بالدخول للنظام المعلوماتي لدى مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، دراسة مقارنة، مرجع سابق، ص 80-82.

[5] نهلا عبد القادر مومني، المرجع نفسه، ص 159.

[6] المشرع الجزائي الجزائري عموما لم يعتبر إخضاع النظام المعلوماتي للحماية الفنية من عدمه شرط ليحظى بالحماية الجزائية من خلال قانون العقوبات والقوانين المكملة له وهو نفسه الرأي الراجح في غالبية التشريعات بينما الفقه تنازع حول رأيين أحدهما يشترط ضرورة إخضاع النظام المعلوماتي للحماية الفنية ليحضى بالحماية الجزائية ورأي يقول العكس.

[7] ضرورة اخضاع النظام المعلوماتي للحماية الفنية من عدمه ليخضع للحماية الجزائية هوما يعبر عنه بالعنصر المفترض في جريمة الدخول غير المصرح به، حيث أن المشرع الجزائي اشترط وجود ركنين في هذه الجريمة المادي والمعنوي في

الاتجاهان اللذان اختلافا للإجابة على السؤال المطروح رغم أن لا المشرع الجزائري ولا الفرنسي ولا أغلبية المشرعين الآخرين أشاروا إلى ذلك[1].

فيرى **أصحاب الاتجاه الأول** أنه من غير المعقول توفير الحماية الجنائية لمعلومات على درجة من الأهمية، تركت دون أية إجراءات أمنية تكفل لها الحماية اللازمة[2]. أي يرى هذا الجانب ضرورة وجود نظام أمني.ويعزز أصحاب هذا الرأي وجهة نظرهم بالإشارة إلى أن القانون الجنائي لا ينبغي أن يقوم بحماية الأشخاص الذين يأخذون الاحتياط اللازم من الإنسان متوسط الذكاء فوجود نظام حماية يمكن اعتباره التزاما مفروضا على كل من يقوم بإدارة نظام معلوماتي[3]. وهو شرط تقتضيه متطلبات العدالة والمنطق على حسب رأيهم[4].

أما أنصار الاتجاه الثاني و هو الغالب يرى الرأي الغالب أنه ينبغي حماية الأنظمة المعلوماتية سواء أكانت هناك تدابير أمنية تحيط بها وتحميها أم لم تكن أي يذهب هؤلاء إلى عدم ضرورة انتهاك نظام الأمن لكي تقوم الجريمة، واستنادا إلى هذا الرأي لم تتضمن النصوص القانونية المتعلقة بجرائم الاعتداء على نظام المعالجة الآلية ضرورة أن لا يكون نظام المعالجة الآلية محميا بجهاز أمان[5].

ويعزز هذا الاتجاه وجهة نظره بالإشارة إلى أن تطلب هذا الشرط يؤدي إلى قصر نطاق الحماية على الأنظمة المحمية فقط دون الأنظمة المفتوحة للجمهور مثل الدليل الالكتروني، مما يعني توسيع دائرة الإفلات من العقاب.كما يذهب أنصار هذا الرأي إلى أنه لا ينبغي أن ينظر إلى الأنظمة الأمنية باعتبارها شرطا لتجريم الدخول غير المصرح به إلى النظام المعلوماتي وإنما يمكن النظر إليها باعتبارها قرينة على تحقق القصد الجنائي.[6] رغم

حين هناك عنصر مفترض وهو إخضاع النظام للحماية الفنية ونحن من جهتنا نضم صوتنا للرأي الفقهي القائل بضرورة إخضاع النظام للحماية الفنية.

[1] عموما يعتبر المنع الجنائي للدخول غير المصرح به للنظام المعلوماتي وتحديد عقوبات لمرتكبيه يتماشى مع مبدأ الشرعية، ويوفر حماية أساسية للنظام وللمعلومات ضد المخاطر والأضرار الناجمة عن هذا الفعل المجرم، إلا أن ذلك لوحده غير كاف فحتى تكون هناك الفعالية الأمنية لابد أن تعززها حماية فنية تعمل على الحيلولة دون وقوع هذه الجريمة أو التخفيف من آثارها إذا وقعت، وهذا ما أكدت عليه المذكرة التفسيرية لاتفاقية بودابست حينما ذهبت إلى القول أن الوسيلة الأكثر فعالية لمنع الولوج غير المصرح به تتمثل بطبيعة الحال في التهديد بقانون العقوبات، ومع ذلك فإن هذا الغرض لا يكون مكتملا دون تبني ووضع إجراءات أمنية فعالة. وعادة ما يلجأ أصحاب نظم المعالجة الآلية كثيرا إلى وسائل الحماية الفنية لتأمين الحماية للمعلومات التي تحتويها أنظمتهم في حين يتركها البعض الآخر بدون حماية. فأكدت اتفاقية بودابست على استخدام وسائل الحماية الفنية لمنع الولوج أوالدخول غير المصرح به إلى النظام المعلوماتي باعتباره المرحلة السابقة والضرورية لارتكاب الجرائم المعلوماتية الأخرى مثل سرقة المعلومات وتزويرها، التجسس المعلوماتي، الاحتيال، الإعتداء على حرمة الحياة الخاصة وغيرها.

[2] - نهلا عبد القادر مومني، المرجع نفسه ، ص 159.

[3] نهلا عبد القادر مومني، مرجع سابق، ص 160.

[4] - رشيدة بوكر، مرجع سابق، ص 165,

[5] - رشيدة بوبكر، المرجع نفسه، ص 168.

[6] - قورة، مرجع سابق ، ص 371.

أن الأخذ بالرأي الأول يعتبر غير ملائم من الناحية المنطقية، ذلك أن الواقع العملي يكشف أن غالبية نظم المعالجة الآلية تتمتع بحماية فنية على درجة عالية من الكفاءة، بل هناك شركات متخصصة في تقديم خدمات التأمين الفني المعلوماتي وذلك في طل تنامي الاعتماد على نظم المعالجة الآلية[1].

ب- البقاء غير المصرح به [2]

ويتحقق الركن المادي لهاته الجريمة أيضا إذا اتخذ صورة البقاء في النظام ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام[3].

ومما لا شك فيه أن البقاء داخل نظام الكمبيوتر بعد دخوله عن طريق الخطأ، لا يختلف عن الدخول غير المصرح به من حيث وجوب التجريم، بينما هناك فرق بين الدخول والبقاء[4]. فاتجاه إرادة الفاعل إلى البقاء داخل هذا النظام على الرغم من معرفته أنه غير مصرح له بالدخول، لا يختلف في جوهره عن الدخول غير المصرح به إلى النظام [5].فالنتيجة الإجرامية في الحالتين واحدة وهي الوصول إلى النظام بشكل غير مصرح به فالمصلحة التي يحميها القانون هي حماية النظام المعلوماتي في الحالتين[6].

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، وذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له الحق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الاجتماعي المادي لجريمتي الدخول والبقاء غير المشروع في النظام[7].

والإشكالية التي تثور في هذا الصدد، متى تنتهي جريمة الدخول ومتى تبدأ جريمة البقاء ؟

ذهب رأي من الفقه إلى أن جريمة الدخول تتحقق منذ اللحظة التي يتم الدخول فيها فعلا إلى البرنامج، ويبقى مدة قصيرة من الزمن داخله، وبعد تلك اللحظة تبدأ جريمة البقاء وتنتهي

---

[1] رشيدة بوكر، مرجع سابق، ص 168.

[2] - البقاء غير المشروع جريمة مستمرة كما سبق الذكر ودلك نظرا لاستمرار الاعتداء على المصلحة التي يحميها القانون طالما استمر البقاء غير المصرح به داخل النظام وهي أيضا من الجرائم صعبة الإثبات دلك لأن المتهم فيها في حالة القبض عليه يزعم أنه كان على وشك الانفصال عن النظام المعتدى عليه، مشار إليه لدى نهلا عبد القادر مومني، مرجع سابق، ص 161.

[3] - علي عبد القادر قهوجي، مرجع سابق، ص 133.

[4] CHAMPY Guillaume, op.cit,pp.78-80.

[5] - خثير مسعود، مرجع سابق،116.

[6] - نائلة عادل محمد فريد قورة، مرجع سابق، ص 346.

[7] - علي عبد القادر قهوجي، مرجع سابق، ص 133.

بانتهاء حالة البقاء، ويذهب رأي آخر إلى تحديد تلك اللحظة منذ الوقت الذي يعلم فيه أن بقاءه داخل النظام غير مشروع[1].

بينما يذهب رأي راجح من الفقه إلى أن جريمة البقاء دخل النظام تبدأ منذ اللحظة التي يبدأ فيها الجاني التحول داخل النظام، أو يستمر في التجول داخله بعد انتهاء الوقت المحدد، أي منذ علم الجاني أنه ليس له حق الدخول، فإذا دخل وظل ساكنا تظل الجريمة جريمة دخول إلى النظام، أما إذا بدأ في التجول فإن جريمة البقاء داخل النظام تبدأ من تلك اللحظة لأنه يتحول في نظام يعلم مسبقا أن مبدأ دخوله واستمراره فيه غير مشروع، ومنذ تلك اللحظة تبدأ جريمة البقاء داخل النظام[2].

وتم التساؤل أيضا فيما لوتم الدخول إلى النظام بموافقة المسئول عنه إذا كانت مشروطة بزمن محدد وحدث تجاوز لهدا الزمن أو أن يكون الدخول فقط للرؤية والاطلاع دون استخراج نسخة من المعطيات التي يحويها النظام، هل يعد البقاء هنا غير مشروع؟

إذا كانت الحكمة التي من أجلها تم تجريم البقاء غير المشروع والدخول غير المشروع إلى النظام والمتمثلة في حماية المعطيات التي يحتويها النظام من الوصول إليها من قبل أناس غير مسموح لهم ابتداء من الدخول إلى هذا النظام لا تتحقق في هذه الحالة، فالدخول في الحالتين الواردتين في التساؤل تم بموافقة المسؤول عن هذا النظام مما يعني السماح له بالاطلاع على تلك المعلومات التي يحتويها النظام لهذا البقاء هنا لا يعتبر غير مشروع ولكن يمكن اعتبارها سرقة وقت الحاسب الآلي[3].

ثانيا: الركن المعنوي (القصد الجنائي)

إن الركن المعنوي في الجريمة هو عبارة عن القصد الجنائي بعنصرية العلم والإدارة، فيتحقق علم الجاني بأنه يدخل بصورة غير مشروعة في نظام المعالجة الآلية للغير. وحيث أن صورة الركن المعنوي تتمثل بالقصد الجنائي فإن هذه الجريمة لا تتحقق بالخطأ[4].

إن جريمة الدخول أو البقاء إلى نظام المعالجة الآلية بطريق غير مشروع، يتطلب القصد فيها علم الجاني بأنه يدخل إلى نظام المعالجة الآلية للمعطيات الخاصة بالغير، وأن تتجه إرادته إلى ارتكاب هذه الجريمة، أي أن اكتمال هذه الجريمة يستدعي توفر الركن المعنوي.

---

[1]- خثير مسعود، المرجع نفسه ، ص 117.

[2] خثير مسعود، المرجع نفسه ، ص 117.

[3] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، مرجع سابق، ص 355.

[4] معناه إن الدخول بالصدفة غير معاقب عليه، ومنه يجب أن يكون مرتكب الجريمة على علم بأنه دخل إلى النظام المعلوماتي بطريقة غير عادية أي أنه على علم بأن الدخول إلى هذا النظام ممنوع، والجريمة لا تكون مؤسسة أمام القاضي الجزائي إلا بإثبات عملية الدخول .

وبتوافر سوء نية الجاني، إذا كان دخوله إلى النظام نتيجة اختراقه لجهاز الأمن الذي يحمي النظام أومعرفة الرقم السري أو الشيفرة بطريق غير مشروع ودخل بواسطتها إلى النظام، أما إذا كان الجاني سبق له الاشتراك في النظام، ولكن انتهت مدة الاشتراك ودخل إلى نظام معتقدا خطأ بأنه ما زال له الحق في الدخول إليه. فإن ذلك يعد جهلا بالواقع مما ينفي القصد الجنائي لديه، أما إذا دخل شخص إلى النظام بطريق الخطأ وبحسن نية وخرج منه فورا عند علمه بأنه لا يحق له الدخول إلى هذا النظام، فإنه لا يسأل جنائيا لانتفاء القصد الجنائي لديه، أما إذا دخل بطريق الخطأ ولكنه بقي يتجول داخل النظام مع علمه بذلك فإنه يقع تحت طائلة المسؤولية.

و كما سبقت الاشارة فإن جريمة الدخول أو البقاء غير المصرح به للنظام المعلوماتي هي جريمة ماسة بالسرية المعلوماتية و رغم خطورتها إلى أن هناك بعض الجرائم الأخرى والتي لا تقل عنها خطورة كجريمة التعامل في معلومات غير مشروعة و التي سيتم التفصيل فيها في المطلب الموالي.

المطلب الثاني
جريمة التعامل في معلومات غير مشروعة

تعتبر من أهم الجرائم ضد المعلومات وأخطرها انفرد بها المشرع الجزائري على غرار المشرع الفرنسي واتفاقية بودابست من خلالها أراد المشرع الجزائري الحفاظ على ما تبقى من سرية المعلومات المتحصل عليها بطريقة غير مشروعة بتجريم التعامل في هده المعلومات من خلال نص المادة 394 مكرر 2 .

فقد حرص المشرع الجزائري من جانبه على التخفيف من آثار الاعتداءات على المعلومات فيما إذا تم الحصول عليها بطرق غير مشروعة من خلال تجريم التعامل في معلومات غير مشروعة، هذا وقد جرم بداية كل الأفعال التي بواسطتها يتم الحصول على هذه الأخيرة من خلال نصوص المواد 394 مكرر و394 مكرر 1، تماشيا مع أشارت إليه المذكرة الت فسيرية لاتفاقية بودابست فقالت:" ... ومن أجل وقاية أكثر من هذه المخاطر فإنه يجب على قانون العقوبات أن يحظر الأفعال الراجحة الخطورة من المنبع، قبل ارتكاب الجرائم المشار إليها في المواد من 2- 5"، كذلك نص عليها قانون العقوبات الفرنسي في المادة 323-3-1 [1].

[1] Article 323-3-1 La LOI n°2013-1168 du 18 décembre 2013 - art. 25 ":Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou

فالغاية إذن من تجريم مثل هذه الأفعال هي وقائية، لأن هذه الجرائم هي جرائم يهدف المشرع من خلال تجريمها إلى منع وقوع الضرر[1]، لهذا فخطورة هذا التجريم تكمن في غيابه، فقد تكون المعلومات المتحصل عليها من الجرائم محل الدراسة في حوزة صاحبها أو تحت تصرفه، فقد يقوم بإفشائها أو نشرها أو استعمالها وهي الصورة الغالبة دون أن تكون هناك إمكانية لمعاقبته نظرا لعدم تقنين هدا النوع من السلوك في صورة جريمة ينص عليها المشرع، وهو ما أيقض الحس التشريعي لدى المشرع الجزائري بقيامه بتجريم هدا الشكل من التعاملات[2]، وجريمة التعامل في معلومات غير مشروعة مثل كل جريمة تتكون من ركنيين مادي ومعنوي كالتالي:

الفرع الأول
الركن المادي لجريمة التعامل في معلومات غير مشروعة

جريمة التعامل في معلومات غير مشروعة بصورتيها جريمة شكلية، أي أنها تقع وتكتمل بمجرد وقوع الفعل المكون لها، أو جريمة خطر لا يعتد المشرع في قيامها بتحقق نتيجة معينة فيكفي أن يقوم الجاني بأحد الأفعال التي نصت عليها المادة 394 مكرر 2 الجزائري والمادة 323-3-1 من قانون العقوبات الفرنسي والمادة 6 من اتفاقية بودابست حتى يكتمل الركن المادي لهذه الجريمة، وسيتم التفصيل في الر كن المادي من خلال النقاط التالية:

أولا : التعامل في معلومات صالحة لارتكاب جريمة

جرم المشرع الجزائري وكذا الفرنسي واتفاقية بودابست مجموعة من الأفعال لأن تركها من دون عقاب يؤدي إلى مضاعفة جرائم الاعتداء على نظم المعالجة الآلية.ولا يشترط أن تقع هذه الأفعال مجتمعة لتقوم الجريمة، بل يكفي أن تقع إحداها فقط. والمقصود بالتعامل ليس هو التعامل بمفهومه في القانون المدني، وإنما هو التعامل بمفهوم أوسع، إذ يقصد به في الجريمة محل الدراسة كل سلوك له علاقة بإعداد وإنتاج المعطيات غير المشروعة، أوكل سلوك يكشف عن وجود صلة معينة بين شخص ومعطيات غير مشروعة، هذه الصلة تتمثل في القيام بأحد أنواع السلوك التي نصت عليها المادة 394 مكرر 2 والمواد المماثلة لها والتي جرمت نفس السلوك[3].ومحل هذه الجريمة طبقا للمادة 394 مكرر02 من

---

plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée."

[1] محمد خليفة، مرجع سابق، ص 195.

[2] رشيدة بوكر، مرجع سابق، ص 277.

[3] محمد خليفة ، مرجع سابق، ص 200

قانون العقوبات الجزائري هو المعطيات المخزنة أوالمعالجة أو المرسلة عن طريق منظومة معلوماتية[1].

تشمل هذه الأفعال كافة العمليات السابقة على استعمال هذه المعلومات ابتداء من تصميمها وبحثها مرورا بتجميعها وصلا إلى توفيرها أو نشرها أو الاتجار بها، وهو الأمر الذي لم يخلو منه المشرع الفرنسي في المادة 323-3-1- وتم الدعوة إلى تجريمه من طرف اتفاقية بودابست[2].

ولم يكتف المشرع الجزائري بتجريم التعامل في المعلومات الصالحة لارتكاب جريمة، بل جرم أيضا التعامل في معلومات متحصلة من جريمة وهي الصورة التي انفرد بها مقارنة بالمشرع المشرع الفرنسي واتفاقية بودابست.

وبالتالي فإن جريمة التعامل في معلومات غير مشروعة تطبيقا للقانون الجزائري لها صورتين، فإذا كان يهدف من الأول منع حدوث الجريمة فإنه في الثانية يحاول أن يقضي ما أمكن القضاء عليه من آثار هذه الجريمة، فهذه الأخيرة قد تسفر على الحصول على معلومات معينة ويكون من الخطر وجودها في حوزة غير صاحبها.

أ- التصميم :

هو أول عملية في سلسلة التعامل في المعلومات تتمثل في إعداد معلومات صالحة لارتكاب جريمة، وهذا العمل يقوم به عادة المختصون في هذا المجال كالمبرمجين ومصممي البرامج[3]، ومثال هذه الجريمة تصميم برنامج يحمل فيروسا، وهذا ما يطلق عليه بالبرامج الخبيثة أو تصميم برنامج اختراق[4].

وفي هذا مساس بالأسرار المعلوماتية على أساس أنها سلوكات تمهد لاختراق النظم المعلوماتية، وهو سلوك مجرم وفقا لاتفاقية بودابست والمادة 323-3-1 قانون عقوبات فرنسي والتي أشرات إلى نفس السلوك "..conçus.." كذلك المادة 394 مكرر2" ..تصميم..".

وعن تجريمه وفقا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 9 منها، حيث عبر عنه بمصطلح "انتاج".

ب- البحث :

[1] محمد خليفة ، المرجع نفسه، ص196.

[2] رشيدة بوبكر، مرجع سابق، ص 279.

[3] - رشيد بوبكر، المرجع السابق، ص 279-280.

[4] - محمد خليفة، المرجع السابق، ص 200-201.

طرحت بشأن فعل البحث الواردة في نص المادة 394 مكرر2 تساؤلات وهي هل المقصود من البحث هو البحث عن معلومات تصلح أن ترتكب بها جريمة؟ أو البحث عن كيفية تصميم هذه المعلومات أي إجراء أبحاث فيما يتعلق بهذه المعلومات؟

ورجحت فيما يتعلق على هذه الأسئلة أن المقصود من البحث هو البحث في كيفية تصميم هذه المعلومات وإعدادها ليس مجرد البحث عنها لأن هذا الفعل في حد ذاته لا يعتبر جريمة[1]، مع العلم أن هذا السلوك وارد فقط في النص الجزائري أي في المادة 394 مكرر 2 ولا مثيل لذلك لا في النص الفرنسي ولا في الاتفاقية العربية ولا في اتفاقية بودابست ولا في الاتفاقية العربية.

ج.التجميع :

هو القيام بتجميع قدر من المعلومات فمن يحوز معلومة لا يعتبر خطر بالقدر الذي يكون عليه من يحوز أكثر من ذلك، والجدير بالذكر أن اتفاقية بودابست استخدمت مصطلح الحصول من أجل الاستخدام بدلا من مصطلح التجميع[2] والأمر ذاته في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 9 في الفقرة الثانية " ..يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأي من الجرائم المبينة في المادة..." .

د. التوفير :

وهو الفعل الذي جرمته المادة 394 مكرر 2 من قانون العقوبات الجزائري :"...أو توفير ..." وهو نفس المعنى المنصوص عليه في المادة 323-3-1 عقوبات فرنسي" ... توفير أو وضع تحت التصرف... "، نفس الأمر في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 9 " ... أو توفير."، وكذا الشأن بالنسبة لاتفاقية بودابست تحت عبارة "أي أشكال أخرى للوضع تحت التصرف ". والمراد بذلك أي من التوفير وهو توفير معطيات يمكن أن ترتكب بها جريمة ، وهذا الوضع تحت التصرف وهو تقديم المعطيات وإتاحتها لمن يريدها، أي جعلها في متناول الغير ووصفها تحت تصرفه وهو المبتغى من التوفير، والجدير الإشارة إليه أن المشرع الفرنسي استخدم مصطلح الوضع تحت التصرف تعبيرا منه عن التوفير[3].

فضلا على أن المذكرة التفسيرية أشارت إلى أن مصطلح الوضع تحت التصرف يشير إلى أن وضع أجهزة على الخط ليتم استخدامها بواسطة الغير، كما يضم هذا المصطلح من ناحية أخرى إنشاء وتجميع الروابط بين الخطوط المتشعبة من أجل تسهيل الوصول إلى

[1] - رشيدة بوبكر، مرجع سابق، ص 281 ، أنظر أيضا ومحمد خليفة، مرجع سابق، ص 201.

[2] - هلالي عبد اللاه أحمد، مرجع سابق، ص 103.

[3] - رشيدة بوبكر،مرجع سابق، ص 282 ، و أيضا أنظر محمد خليفة، مرجع سابق، ص 202-203.

هذه الأجهزة، وذلك عن طريق الإحالة لبرنامج يتصل ببرامج مصممة على سبيل المثال لإتلاف أو حتى هدم البيانات، أومن أجل التدخل في عمل النظم مثال ذلك برامج الفيروسات أو البرامج المصممة أو الموفقة من أجل الوصول إلى نظم الحاسب[1].

هـ النشر[2] :

بينت المذكرة التفسيرية معاني بعض المصطلحات فتذكر أن مصطلح النشر ينبغي أن يمتد ليشمل كل نشاط من شأنه نقل البيانات إلى آخرين[3]، كمصطلح التوزيع المنصوص عليه في المادة 9 الفقرة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

وهو الفعل الذي تناولته المادة 394 مكرر 2 من قانون العقوبات الجزائري في حين أن المشرع الجزائري جرم الفعل في كلتا صورتي جريمة التعامل في معطيات غير مشروعة.

ويقصد بالنشر إذاعة المعلومات محل الجريمة وتمكين الغير من الاطلاع عليها، وذلك مهما كانت الوسائل التي يتصور النشر بها ومهما كانت طبيعتها[4]، وفي هذا السلوك هتك واضح للسرية المعلوماتية.

و. الاتجار:

نص عليه المشرع في المادة 394 مكرر 2 من قانون العقوبات، وفي المقابل استخدم المشرع الفرنسي مصطلحا آخر وهو "الاستيراد" بينما اتفاقية بودابست استخدمت مصطلحي البيع والشراء والاستيراد كذلك الأمر بالنسبة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 9 الفقرة الأولى.

ولم يقصد المشرع الجزائري بالاتجار بمفهومه التجاري، بل يشمل كافة الأفعال التي تكون بمقابل ولم ينص عليها القانون التجاري ضمن الأعمال التجارية التي ينظمه، ويقصد بالاتجار بالمعلومات هو تقديمها للغير بمقابل ولا يهم هذا المقابل إذ يستوي أن يكون نقديا أو عينيا أو خدمات أو غير ذلك[5]. وهو يختلف عن التوفير في مسألة المقابل إذ أن التوفير بدون مقابل بينما الاتجار بمقابل.

ثانيا : التعامل في معلومات متحصل عليها من جريمة

---

[1] - هلالي عبد اللاه أحمد، المرجع نفسه، ص 101.

[2] يقابله مصطلح التوزيع في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 9 منها في الفقرة الأولى.

[3] - هلالي عبد اللاه أحمد، مرجع سابق، ص101.

[4] - محمد خليفة، مرجع سابق، ص 203.

[5] - رشيدة بوبكر، مرجع سابق، ص 284.

هي الصورة الثانية من جريمة التعامل في معلومات غير مشروعة، وهي الصورة التي لم نجدها لا عند المشرع الفرنسي ولا في اتفاقية بودابست، ونص عليها المشرع الجزائري في المادة 394 مكرر2 الفقرة الثانية وتتمثل في أحد الأفعال التالية: حيازة، إفشاء، نشر، استعمال معلومات متحصلة من جريمة. وكل منها كافي لتحقيق الركن المادي للجريمة، بمعنى أنه يكفي أن يقوم الجاني بأحد هذه الأفعال لنعتبر أن الركن المادي لجريمة التعامل في معلومات متحصل عليها من جريمة قد توفر.

أ. الحيازة [1]:

تعرف الحيازة بأنها" سيطرة فعلية على شيء يجوز التعامل فيه أو يستعمل بالفعل حقا من الحقوق"[2]، وهي "سيطرة واقعية وإرادية للحائز على المنقول تخوله من الانتفاع به أو تعديل كيانه أوتحطيمه أو نقله، فهي إذا سيطرة إرادية للشخص على الشيء"[3]. والحيازة في القانون الجنائي ليست حقا، بل هي مركز واقعي، وعليه يمكن أن تكون مشروعة تستند إلى سبب صحيح قانونا كما يمكن أن تكون غير مشروعة[4].

فالحيازة في نطاق القانون الجنائي رابطة واقعية بين شخص ومال (منقول) تتيح للأول أن يسيطر على الثاني سيطرة مستقلة مقترنة بنية الاحتباس وتكون السيطرة على المال مستقلة إذا كان يمكن للشخص أن يمارس أي عمل مادي على الشيء بدون رقابة من شخص آخر له على المال سلطة قانونية أعلى بمقتضى حق من الحقوق.

فلا يعتبر حائزا للعامل الذي تربطه علاقة العمل بالمعطيات، لأنه لا يسيطر عليها بنية الاحتباس ولا يمكنه أن يمارس أي عمل عليها بدون تصريح من رب العمل.

كما أن الحيازة لا تقوم إلا بسيطرة الحائز على المعطيات، بحيث يكون باستطاعته التأثير عليها تأثيرا يتفاوت حجمه تبعا لنوع الحيازة، إذ قد تكون السيطرة مطلقة يستطيع معها الحائز أن يفني المعطيات أو يعدل فيها أو يستعملها، كما قد تكون هذه السيطرة من الناحية الواقعية محدودة تمكنه فقط من الانتفاع بالمعطيات أوالإستغلال في وجه معين، وعليه يكفي للقول بتوافر السيطرة مجرد استطاعة هذه السيطرة دون عقبات واقعية تحول بين الشخص وبين التمتع بها[5].

ولا تكفي مجرد سيطرة الحائز على المعلومات لكي تقوم الحيازة بل يلزم أن تكون هذه السيطرة إرادية أي أنها مقترنة بنية احتباس المعلومات، والسيطرة عليها وهذا لا يتحقق إذا

---

[1] في المادة 394 مكرر 2 من قانون العقوبات الجزائري النص يعني حيازة المعلومات في حين في الاتفاقية لعربية لمكافحة جرائم تقنية المعلومات لسنة 2010 في المادة 9 الفقرة الثانية تقصد "حيازة أي أدوات أوبرامج ...بقصد استخدامها لغايات ارتكاب جريمة.."، والأمران مختلفان.

[2] قدري عبد الفتاح الشهاوي، الحيازة كسبب من أسباب كسب الملكية في التشريع المصري والمقارن، منشأة المعارف، مصر، 2003، ص 12.

[3] - محمد خليفة، المرجع السابق، ص 205.

[4] - رشيدة بوبكر، مرجع سابق، ص 285-286.

[5] - رشيدة بوبكر، المرجع نفسه، ص 286.

كان تمتع الحائز بسلطاته على المعطيات لم يكن إلا أمرا عرضيا أوجدته المصادفة أو تم بنية عدم التكرار، لأنه يلزم أن تكون سيطرة الشخص على المعلومات مقترنة بنية احتباسها على الدوام أو مدة معينة. وما دامت نية الاحتباس ركنا أصليا من أركان الحيازة فإن العلم يكنه المعطيات المتحصلة من جريمة وبدخولها في نطاق السيطرة لازم لا تقوم الحيازة بدونه، لأنه من لا يعلم لا يحوز[1].

ب .الإفشاء :

تتمتع الحاسبات الآلية بقدرة هائلة على تخزين للمعلومات، مما جعلها مستودعا لأهم المعلومات وأكثرها حساسية سواء كانت متعلقة بمصالح الدولة أو تعلقت بالأفراد أو بالمصالح الاقتصادية لمختلف المؤسسات أوتعلقت بالمجالات العلمية. ومع ازدياد أهمية هذه المعلومات وكثرة الاعتماد على تخزينها داخل أنظمة الحسابات تزداد المخاوف من الحصول عليها بطريقة غير مشروعة عن طريق اختراق تلك الأنظمة ثم القيام بإفشائها لتحقيق مصالح عديدة.

وعليه اعتبر الإفشاء غير المشروع جريمة معاقب عليها جرمته العديد من التشريعات[2]، من ضمنها المشرع الجزائري في المادة 394 مكرر2 من قانون العقوبات.حيث قام بتجريم إفشاء معلومات متحصلة عليها من جريمة دخول أو بقاء غير مصرح بهما أومن جريمة تلاعب.

ولا يتطلب القانون الجزائري حدوث نتيجة معينة من وراء فعل الإفشاء بل يجرم هذا الأخير في حد ذاته، والفرق بين الحيازة والإفشاء أو النشر إن الحيازة تقتصر على وجود معلومات غير المشروعة لدى الحائز فحسب دون قيامه بتقديمها لغيره، أما الإفشاء والنشر فهما يفترضان انتقال هذه المعلومات من حيازة هذا الشخص إلى غيره من الأشخاص، أي أنه يقوم بتقديم هذه المعطيات غير المشروعة لأشخاص غيره ولا يقصرها عليه. والذي يقوم بفعل الإفشاء هذا ليس شخصا مؤتمنا على هذه المعطيات فهو ليس ملتزما بكتمان هذه المعطيات بمقتضى وظيفة أو عقد ما، وإنما هو شخص تحصل على هذه المعطيات بطريقة غير مشروعة وأراد المشرع أن يمنعه من إفشائها ونشرها سعيا لتضييق انتشارها فليس هناك التزام سابق على هذا الشخص بالمحافظة على سر ما، وإنما هو أي شخص يتحصل

---

[1] - رشيدة بوبكر ، المرجع نفسه، ص 286-287.

[2] - المشرع الفرنسي لم يخصص لهذا الفعل نصا خاصا في حين أنه بالنسبة للقانون الأمريكي فان القانون الفدرالي لجرائم الحاسبات الآلية لسنة 1984 يعاقب في مادته 1030 أ – 3- كل من يقوم بالدخول غير المصرح به إلى نظام الحاسب الآلي وعن طريق هذا الدخول يقوم فإفشاء معلومات توجد داخل الحاسب الآلي متى كان هذا الحاسب يستعمل من طرف حكومة الولايات المتحدة الأمريكية أو لمصلحتها، أو ترتب على هذا السلوك الإضرار بهذا الاستعمال، لكن التعديلات اللاحقة للقانون تجاهلت هذا النص، وكذلك يعاقب قانون العقوبات الهولندي في مادته 139 على الإفشاء العمدي للمعلومات المتحصل عليها بطريقة غير مشروعة عن طر يق تسجيلها أثناء نقلها بواسطة نظام الحاسب الآلي، مشار إليه لدى محمد خليفة، مرجع سابق، ص 207-208.

على المعطيات بطريقة غير مشروعة[1]. ويقصد بالإفشاء الإطلاع على السر بأي طريقة كانت، ويعد في حكم السر كل أمر يكون سرا ولو لم يشترط كتمانه صراحة[2].

وللتفرقة بين هذه الجريمة وهي جريمة اعتداء على معلومات تم الحصول عليها بعد اختراق نظام معلوماتي والتي هي جريمة تشبه جريمة إفشاء البيانات الاسمية، والمقصود بهذه الأخيرة نقل تلك البيانات إلى جهة غير مخول لها بتلقي تلك المعلومات، وهي جنحة الإفشاء غير المشروع للبيانات الشخصية من قبل الموكل لهم حفظها وتخزينها ومعالجتها .

فعلى أساس أن البيانات الشخصية هي من بين الخصوصيات المحمية قانونا، فإن إفشاؤها سواء عن طريق الخطأ أو بقصد التشهير أو الإساءة أو التهديد بنشرها، يعد اعتداء على الحياة الخاصة للإنسان، لأن قيام شخص بإيداع بياناته لدى مؤسسة ما، وقيام تلك المؤسسة فإفشاء تلك البيانات بقصد أو بدون قصد منها والتشهير به يعد منة الجرائم التي تمس حياته الخاصة المعاقب عليها قانونا[3]. وقد يكون الإفشاء لأشخاص معينين كما يمكن أن يكون هذا الإفشاء بشكل عام بحيث يستطيع الجميع معرفة هذه المعلومات والعلم بها، كنشرها على شبكة الانترنت بحيث يستطيع أي شخص الاطلاع عليها[4].

ولمزيد من التوضيح نحن الآن بصدد جريمة إفشاء بيانات اسمية معالجة من طرف ذي صفة في تسجيل أو فهرسة أو نقل هته البيانات الاسمية المعالجة آليا وتسريبها وإفشائها، بخلاف الجريمة سابقة الذكر وهي اختراق البيانات الاسمية المعالجة آليا وإفشائها[5].

ولمزيد من التوضيح أيضا بخصوص هذه الجريمة ومقارنتها بجريمة إفشاء الأسرار المهنية التي نص عليها المشرع الجزائري في نص المادة 1/301 من قانون العقوبات، حيث أن المشرع الفرنسي جرم إفشاء البيانات الاسمية في المادة 22/226 من قانون العقوبات فعلى الرغم من وجود اختلاف بين الجرمين إلا أنهما تتفقان في الهدف وهو حماية المعلومات الشخصية[6].

---

[1] - محمد خليفة، مرجع سابق، ص 208-209.

[2] - محمد خليفة ، المرجع نفسه، ص 209.

[3] أسامة المناعسة، جرائم الحاسب الآلي والانترنت، دراسة مقارنة، دار وائل للنشر والتوزيع عمان، الطبعة الأولى،2001، ص 229.

[4] الموسوس عتو، مرجع سابق، ص 350.

[5] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، الطبعة الأولى، 2009، ص 646.

[6] المشرع الجزائري ليس لديه نصوص مماثلة للمواد (16/226 إلى 24/226) والمتعلق بحماية معالجة المعطيات أوالبيانات الاسمية، وهذه النصوص هي من القانون رقم 526/2009 المؤرخ في 12 ماي 2009 وهو تعديل للقانون 17/78 والمتعلق بالمعلوماتية.

بين الجريمتين اختلاف[1] من حيث الموضوع فجريمة إفشاء الأسرار المهنية موضوعها المعلومات ذات الطبيعة السرية، أما جريمة إفشاء البيانات الشخصية فموضوعها البيانات الشخصية التي يتم معالجتها عن طريق الحاسب الآلي، والتي لا تعتبر في غالبيتها سرية أو تتعلق ببعض المهن والوظائف التي تفترض الثقة الضرورية في ممارستها كالطب والمحاماة والصيدلة والقضاء[2]. ولهذا وبالنظر إلى هدا الفارق اعتبرت جريمة إفشاء البيانات الاسمية أوسع نطاقا من جريمة إفشاء الأسرار والتي سنقف عندها في مطلب موال[3].

ج-النشر :

تؤدي عملية الدخول غير المصرح به في كثير من الأحيان إلى الحصول على معطيات غير مرخص بالإطلاع عليها، سواء كانت هذه المعطيات شخصية أم تعلقت بالمجالات الاقتصادية والمالية أم تعلقت بالدولة ومصالحها. والمشرع أراد أن يضيق إلى حد كبير من دائرة الأشخاص الذين يمكن أن يطلعوا على هذه المعطيات فجرم أنواعا من السلوك تتعلق بهذه المعطيات رغبة منه في ردع الأشخاص عن الاقتراب من المعطيات غير المشروعة، ومن ذلك قيام المشرع بتجريم نشر المعطيات المتحصلة من جريمة. وفعل النشر هو الفعل الوحيد المشترك بين صورتي جريمة التعامل في معطيات غير مشروعة.

ومن قبيل النشر ما يقوم به المخترقون من اختراقات لمواقع معينة وحصولهم على كلمات العبور فيها والقيام بنشرها على الجميع نكاية بأصحابها وتحديا لهم.

ولم تشترط المواد القانونية التي تجرم النشر عددا معينا من المرات التي يتم النشر فيه، بل جاءت المادة مطلقة مما يفهم معه أن النشر يتم ولو لمرة واحدة فقط.

كما لم تحدد المادة أن يكون النشر بمقابل أو بغيره، وبالتالي فهو يتحقق في كلتا الحالتين، كما لم تذكر المادة وسيلة معينة يتم بها النشر وبالتالي فهويتم بكل وسيلة يمكن تصورها. سواء كانت وسيلة معلوماتية كالنشر عن طريق شبكة الانترنت أو الأقراص المضغوطة، أو كانت تقليدية كالنشر عن طريق الكتابة مثلا[4].

د. الاستعمال:

يعتبر الاستعمال أخطر سلوك يمكن أن يقع على المعلومات المتحصل عليها من جريمة ذلك أنه إذا كانت حيازة المعلومات غير المشرعة وإفشاؤها ونشرها أمورا خطيرة فإن الأخطر من ذلك كله هو القيام باستعمال هذه المعطيات، كأن تستعمل شركة ما معطيات أو معلومات عن شركة منافسة لها تم الحصول عليها بطريقة غير مشروعة – عن طريق دخول

---

[1] وهناك أيضا للتفرقة بين الجرمين وجهات نظر أخرى لم نعتبرها مقنعة من جهتنا، راجع بخصوص دلك عبد الفتاح بيومي حجازي، المرجع السابق، ص 648-651.

[2] الموسوس عتو، مرجع سابق، ص 351 .

[3] عبد الفتاح بيومي حجازي، مرجع سابق، ص 651.

[4] - عبد اللطيف الهميم، احترام الحياة الخاصة، الطبعة الأولى، دار غمار للنشر والتوزيع عمان، 2004، ص 324.

غير مصرح به – ويشمل هذا التجريم كل استعمال للمعطيات مهما كان الهدف منه ومهما كان نوعه ، وقد نصت المادة السابقة على ذلك صراحة بقولها: " أو استعمال لأي غرض كان " حتى تغلق كل باب أمام من يريد استعمال هذه المعطيات .

ويستفاد من نص المادة المطلق أن الاستعمال ولو لمرة واحدة تقوم به الجريمة لأنه لم يرد تحديد لعدد المرات اللازمة لقيامها[1].

الفرع الثاني

الركن المعنوي لجريمة التعامل في معطيات غير مشروعة

جريمة التعامل في معطيات غير مشروعة عمدية، ويستفاد من ذلك عبارة المادة 394 مكرر 2 عمدا وعن طريق الغش لكن هذه العبارة نفسها تثير اللبس، إذ لماذا اكتفى المشرع في المواد السابقة الخاصة بالدخول أو البقاء غير المصرح بهما وبالتلاعب بالمعطيات، اكتفى في تدليله على عمدية تلك الجرائم بلفظ " عن طريق الغش " بينما أضاف في هذه الجريمة لفظ " عمدا " إلى جانب " عن طريق الغش "، فهل يعني هذا أن لفظ " عن طريق الغش " في هذه الجريمة يعني شيئا آخر غير العمد[2].

أولا: القصد الجنائي العام

يتحقق القصد الجنائي العام في جريمة التعامل في معلومات غير مشروعة شأنها شأن الجرائم التقليدية على عنصري العلم والإرادة كالتالي:

1- العلم:

لابد أن يحيط الجاني علما كافيا بكافة العناصر الداخلة في تشكيل الجريمة، ومن قبيل ذلك ضرورة علم المتعامل أنه يقوم بالتعامل في معلومات غير مشروعة، وأن هذا السلوك يحمل تهديدا للمصلحة المحمية سواء كان من شأن المعلومات التي يتعامل فيها أن يستعمل في ارتكاب الجرائم بالنسبة للصورة الأولى من الجريمة، أوكان من شن التعامل في المعلومات المتحصلة من إحدى جرائم الاعتداء على نظام المعالجة الآلية زيادة الضرر الذي قد يترتب على تلك الجريمة، ولابد أن يعلم الجاني بالصفة غير المشروعة للمعلومات بأن يعلم أنه يمكن أن ترتكب بها جريمة، أو أنها متحصلة من جريمة، وإذا انتفى العلم بأحد العناصر السابقة انتفى القصد الجرمي[3].

2- الإرادة:

[1] - محمد خليفة، المرجع السابق، ص 210.

[2] - محمد خليفة، مرجع سابق، ص 211.

[3] محمد خليفة، المرجع نفسه، ص 112.

لا يكفي أن يكون المتعامل عالما بما يفعل لقيام جريمة التعامل بمعلومات غير مشروعة، بل يجب أن تكون إرادته متجهة إلى تحقيق وإتيان أحد المظاهر السلوكية التي نص عليها المشرع ومن قبيل ذلك نشر واتجار وحيازة المعلومات وذلك رغم علمه بصفتها غير المشروعة.

ولما كانت جرائم التعامل في معلومات غير مشروعة من الجرائم الشكلية فإن الإرادة فيها لا تنصب إلا على النشاط الجرمي فحسب ولا تتعداه إلى النتيجة، ذلك أنه لا توجد نتيجة يعتد بها في البناء القانوني للجريمة، وطبقا للقواعد العامة فان القصد الجرمي لا يتوافر لدى المتعامل إلا إذا كان حرا فإذا ثبت أن هذا الأخير كان تحت تأثير الإكراه، أوثبت أنه كان في حالة ضرورة فإن القص الجرمي يكون منتفيا لديه[1].

ثانيا: القصد الجنائي الخاص

بما أن جريمة التعامل في معلومات غير مشروعة تتخذ صورتين فما مدى ضرورة توفر القصد الجنائي الخاص في كلتى الصورتين؟.

1- القصد الخاص في جريمة التعامل في معلومات صالحة لارتكاب جريمة:

اشترطت اتفاقية بودابست صراحة في المادة6 منها، أنه لا يعاقب على التعامل في الوسائل الصالحة لارتكاب جريمة إلا إذا كان الغرض هو التعامل بنية ارتكاب جريمة من الجرائم المنصوص عليها في المواد من 2 إلى 5 من الاتفاقية، معنى هذا أنه يشترط لتوافر الجريمة القصد الخاص والقصد العام وحده غير كافي لقيامها، والمقصود بذلك اتجاه القصد في التعامل بهذه المعلومات إلى الإعداد والتمهيد لاستعمالها في ارتكاب جريمة من جرائم الاعتداء على النظم المعلوماتية.

والأمر ذاته بالنسبة للمشرع لجزائري، رغم انه لم يشترط القصد الخاص صراحة من خلال المادة 394 مكرر2 ولكنه ليس من مقتضيات العدالة مساءلة شخص يقوم بالتعامل في معلومات، إلا إذا كان قصده سيء يتمثل في إعدادها ولاستعمالها في جريمة ما، ذلك أن النص عبر عنها " صالحة لارتكاب جريمة ... "، وليست معدة خصيصا لارتكاب جريمة أي أنه يمكن أن تستعمل لأغراض مشروعة إذا لم تكن له نية الاستعمال غير المشروع.

وليست هي المرة الأولى أين يتم اشتراط توفر القصد الجنائي الخاص في الجزائر رغم عدم النص عليه صراحة، إذا استقر الفقه والقضاء الجزائري في العديد من الجرائم رغم انه لم يشترط النص صراحة القصد الجنائي الخاص ويرى ضرورة توفره لقيام الجريمة وبالتالي بدون توفره إلى جانب القصد الجنائي العام فإن الجريمة لا تقوم وهو ما حدث بشأن جريمة التعامل في معلومات صالحة لارتكاب جريمة فإذا كان الأمر هكذا بالنسبة لهذه

[1] - رشيدة بوبكر ، مرجع سابق، ص 295-296.

الصورة فما هو الشأن بالنسبة للصورة الثانية من صورتي جريمة التعامل في معلومات غير مشروعة ألا وهي التعامل في معلومات متحصلة من جريمة.

2- القصد الجنائي الخاص في جريمة التعامل معلومات متحصلة من جريمة:

من الواضح انه في هذه الصورة يكفي توافر القصد الجنائي العام، ذلك لأن المعلومات المتحصل عليها من جريمة وطبيعتها الثابتة هذه تؤكد على أن القصد العام كافي لقيام الجريمة، إذ لا يسأل الفاعل عن قصده الخاص ما دام يعلم أنه تحصل على هذه المعلومات من جريمة وليس هناك من مبرر لاشتراط القصد الخاص في هذه الحالة. فالعلم بصفة هذه المعطيات غير المشروعة لا يدخل في تكوين قصد خاص وإنما هو صميم القصد العام[1].

وتشير المذكرة التفسيرية لاتفاقية بودابست لأهمية تطلب القصد الخاص إذ كانت الأجهزة والوسائل محل الجريمة يمكن أن تستخدم لأغراض مشروعة، فتقول" من أجل تجنب حضر العقاب المبالغ فيه حيث يتم إنتاج هذه الأجهزة وعرضها في الأسواق لأغراض شرعية من أجل التصدي لاعتداءات على أجهزة الحاسب الآلي، فإنه يجب إضافة عناصر أخرى من أجل تضييق نطاق الجريمة وبالإضافة إلى اشتراط القصد العام فإنه يجب توافر نية خاصة أوقصد خاص لاستخدام الجهاز من أجل ارتكاب جريمة من الجرائم المشار إليها في المواد من 2 إلى 5 من الاتفاقية"[2].

وأخيرا نخلص إلى أن جريمة التعامل في معلومات متحصلة من جريمة، تقوم على القصد الجنائي العام وحده ولا تتطلب قصدا خاصا.

وما تجدر الإشارة إليه هو أن المشرع الجزائري من خلال نص المادة 394 مكرر 2 و استنادا إلى الاتفاقية العربية لجرائم تقنية المعلومات من خلال المادة 9 تم تجريم التعامل في معلومات غير مشروعة إلا أنه من الأفضل صياغة المادة 9 من الاتفاقية من ناحية الصياغة و من ناحية تسمية الجريمة كالتالي: "جريمة اساءة استخدام وسائل تقنية المعلومات" ، ورغم ذلك فحسنا فعل المشرع الجزائري أنه على العموم تصدى للسلوك المستحدث بنص تجريم مستحدث بخلاف السرقة المعلوماتية.

المطلب الثالث

سرقة المعلومات (سرقة البيانات والبرامج المعلوماتية)

واكب انتشار استخدام الحاسبات الآلية والأنظمة المعلوماتية على وجه العموم وترتب على ذلك تغيير في النمط العام للتعامل واختلاف في طريقة تناول المعلومات، ومن ذلك أخذت المعلومات في حد ذاتها أهمية غير مسبوقة وأصبحت مستهدفة، وأصبح أيضا لها

[1] - الأمر نفسه بالنسبة للمشرع الفرنسي، ففي هذه الجريمة لا يتطلب القصد الجنائي الخاص وما يؤكد ذلك العبارة التي استخدمها المشرع الفرنسي في المادة 323-3-1 وهي : ".. بدون مبرر شرعي ".

[2] - هلالي عبد الله أحمد، مرجع سابق، ص 103-104.

سوقها الخاص بها وثمنها المرتفع جدا، وترتب على ذلك أن أصبحت تلك المعلومات هدفا للسرقة[1]، فتم استهداف كل أنواع المعلومات المالية والتجارية والشخصية والعسكرية وغيرها[2].

ويعبر البعض عن سرقة المعلومات بقرصنة المعلومات، وهي سرقة المعلومات من برامج وبيانات بصورة غير شرعية وهي مخزونة في داكرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية وتتم هذه العملية إما بالحصول على كلمة السر أو بواسطة التقاط موجات كهرومغناطيسية بحاسبة خاصة، ويمكن إجراء عملية القرصنة بواسطة رشوة العاملين في المنظمات المنافسة. أما عن الهدف من عمليات القرصنة فهو سرقة الأسرار أو المعلومات التجارية أو التسويقية أو التعرف على حسابات المنظمات أو أحيانا بهدف التلاعب بقيود المصارف أو المؤسسات المالية بهدف سرقة الأموال، أو يكون الهدف الكشف عن أسرار صناعية (تصاميم منتجات) بهدف إعادة تصنيعها دون إجازة قانونية، أو لأهداف سياسية وعسكرية من أجل الحصول على الملفات والخطط السرية العسكرية أو الحكومية. والأمثلة على حالات القرصنة عديدة فقد قامت الشركات الصينية بنقل أسرار تكنولوجيا صناعية من الولايات المتحدة وكندا مستخدمة الحاسوب ومن ثم القيام بإنتاج سلـــــــــع على ضوء ذلك وتصديرها لهاتين الدولتين لتباع في أسواقها بثلث الأسعار الأصلية[3]. وذلك ما حدث لأكبر شركة أمريكية متخصصة في توفير خدمات الانترنت في عام 2001 والتي تخدم أكثر من 23 مليون مستخدم للانترنت، عندما قام شاب يبلغ من العمر تسعة عشر عاما يدعى "جاي ستيرو" بإقناع مسؤوليها بأنه مفيد للشركة، فقاموا بتعيينه على الفور وعندما أظهر مهارة في العمل تطورت صلاحياته، وبدأ يطلع على بيانات مهمة خاصة بتلك الشركة، وظل طوال سنتين متواصلتين يجمع معلومات سرية مهمة عن الشركة، وفجأة قرر الاستقالة بحجة الحصول على وظيفة أخرى. لكنه في الحقيقة كان يجهز لاستخدام ما جمعه من بيانات في شن هجمات شديدة القصوى على موقع الشركة، وبعد فترة من استقالته لاحظ المسؤولون عن تأمين موقع الشركة أن هناك شخصا يهاجم الموقع باحتراف شديد، تنهار أمامه جميع إجراءات التأمين ويخترقها بسرعة، ثم يقوم باستبدال البرامج الخاصة بالموقع ببرامج أخرى من عنده تعطل العمل وتسبب مضايقات عديدة للعاملين في الشركة، وبعد فترة طور هذا القرصان عملياته وبدأ يسرق الأرصدة المدفوعة من اشتراكات

---

[1] محمد عبد الله أبو بكر سلامة، مرجع سابق، ص 129.

[2] فالمعلومات المالية مثلا المتعلقة بالمركز الأموال، بينما التجارية ما تعلق منها مثلا الدراسات الخاصة بمشروعات التصنيع والإنتاج أما عن الشخصية فتتعلق بالمعلومات الماسة بسرية الحياة الخاصة والمخزنة في الحواسيب وعن العسكرية فمثلا ما تعلق بأسرار الدولة و المشروعات النووية و التصنيع الحديث للأسلحة وغيرها، أنظر عبد العال الديربي، محمد صادق إسماعيل، الجرائم الالكترونية، دراسة قانونية قضائية مقارنة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 170-170.

[3] http://www.ao-academy.org/docs/45D0 تاريخ الاطلاع على الموقع 2015/05/10.

الخدمات، وقد كلفت هذه العمليات غير المشروعة الشركة خسائر خلال وقت قصير جدا[1]. كذلك ما نشهده بشأن السرقة العلمية حيث يمكن لأي شخص عادي وبكل سهولة اختراق الحاسوب الشخصي للضحية واختلاس بحثه مثلا ونسبته لنفسه .

وفي إطار حماية المعلومات من أخطار القرصنة وهي المسألة التي سيتم التطرق إليها من خلال تعريف السرقة المعلوماتية (الفرع الأول) ومحلها (الفرع الثاني) إضافة إلى التطرق إلى أركانها و المتمثلة في الركن المادي (الفرع الثالث) والمعنوي (الفرع الرابع).

الفرع الأول

تعريف السرقة المعلوماتية[2]

تعرف السرقة[3]في مفهومها العام" بأنها الحصول على شيء من طرف آخر بدون علم منه"، وفي الغالب سيترتب عليه أضرار بهذا الطرف الآخر سواء كان هذا الضرر ماديا أو معنويا أو أدبيا.[4] أما بالنسبة لتعريف الفقه للسرقة قد جرى تعريفها أنها:"اختلاس مال منقول مملوك للغير بنية تملكه"[5] .

لا تثور المشكلة عندما يتم سرقة المعلومات المخزنة على أدوات التخزين ذات الكيان المادي المحسوس كاسطوانات الحاسب، لأن السرقة هنا تنصرف إلى مال منقول مادي يتم إخراجه من حيازة مالكه أوحائزه الشرعي إلى الغير وهو الأسطوانة بما عليها من معلومات، ولكن يثور الخلاف عندما يتم الاستيلاء على المعلومات المخزنة داخل الجهاز دون وجه حق أو نسخ هذه المعلومات، وهو ما يعبر عنه حاليا بالقرصنة[6]. والقرصنة المعلوماتية ليست إلا ظاهرة من بين عدة ظواهر إجرامية متعددة الأوجه تمس بأمن النظام المعلوماتي للأشخاص إضافة إلى مساسها بالحريات الفردية والحياة الشخصية للأفراد[7].

---

[1] محمد عبد الله أبو بكر سلامة، مرجع سابق، ص 132.

[2] هناك فرق بين سرقة المعلومات وسرقة وقت الآلة، حيث أن هذه الأخيرة معناها هو استخدام غير مشروع للحاسب في أماكن العمل لأغراض شخصية حيث يتم اختلاس وقت الحاسب بمعرفة المستخدمين غير الأمناء من اجل انجاز عمال خاصة بهم وبدون علم الحائز الشرعي لنظام المعلومات، انظر أيمن عبد الحفيظ عبد الحميد سليمان، إستراتيجية مكافحة جرائم الحاسب الآلي، بدون طبعة وبدون ناشر ، 2003 ، ص 44.

[3] جرائم السرقة في التشريع الجزائري منصوص عليها في المادة 350 إلى 371 من قانون العقوبات في القسم الأول من الفصل الثالث تحت عنوان " السرقات وابتزاز الأموال". ويمكن استنباط تعريف السرقة من المادة 350 من قانون العقوبات الجزائري والمادة 1/311 من قانون العقوبات الفرنسي، مع الإشارة إلى أن كلاهما لم يمدد مضمون المواد المذكورة لتشمل السرقة المعلوماتية.

[4]محمد عبد الله أبو بكر سلامة، مرجع سابق، ص 128.

[5] محمد محمود المكاوي، الجوانب الأخلاقية والمهنية للحماية من الجرائم المعلوماتية، الطبعة الأولى ،المكتبة العصرية للنشر والتوزيع مصر، 2010 ، ص 297 وأيضا مأمون سلامة ، قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة ، 1986، ص 146.

[6] محمود أحمد عبابنة، مرجع سابق، ص 93.

[7] Laure Zicry, Enjeux et maitrise des cyber-risques,largus , edition2014, France, p 23.

تُستخدم عبارة القرصنة المعلوماتية للإشارة إلى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، تستهدف التحايل على أنظمة المعالجة الآلية للبيانات لكشف البيانات الحسّاسة أوالتأثير على سلامتها أو حتى إتلافها ويندرج في هذا الإطار قرصنة البرامج، أي نسخ البرامج الخاصة بالكمبيوتر أوالأفلام والموسيقى والمجلات والكتب الإلكترونية بصورة غير قانونية وتوزيعها أو إعادة بيعها من دون ترخيص. وتشير الإحصاءات إلى وجود عدد هائل من المواقع على الإنترنت تبيع برامج مسروقة، ما يكبّد صناعة برامج الكمبيوتر خسائر سنوية تصل إلى مليارات الدولارات. ونشير إلى أن القرصنة أصبحت خطرا كبيرا على الملكية الفكرية خاصة اقتصاد السوق العالمي في مجال الموسيقى أو إنتاج الأفلام أو تسويق البرامج المعلوماتية[1].

ولا تقتصر أعمال القرصنة على البرامج، وإنما تشمل أيضًا المعطيات كسرقة الأرقام السرية لبطاقات الائتمان المستعملة في عمليات الشراء عبر الإنترنت، كذلك تجتاح القرصنة المؤسسات المالية والمصرفية من خلال دخول القراصنة الأنظمة الالكترونية لتلك المؤسسات، والعبث بحسابات الزبائن وتحويل مئات الملايين لأرصدتهم الخاصة[2]، فالقرصنة الالكترونية خطر يجتاح العالم مهدِّدا سرية المعلومات الخاصة بالأفراد والمؤسسات وحتى الدول.

عرف البعض القرصنة، بأنها " سرقة المعلومات من برامج وبيانات مخزنة في ذاكرة الكمبيوتر بصورة غير شرعية أو نسخ برامج معلوماتية بصورة غير شرعية بعد تمكن مرتكب هذه العملية من الحصول على كلمة السر أوبواسطة التقاط الموجات الكهرومغناطيسية الصادرة عن الحاسب الآلي أثناء تشغيله وباستخدام هوائيات موصلة بحاسبة خاصة"[3].

وتتم عملية قرصنة المعلومات بأشكال مختلفة، فقد تتم عن طريق الالتقاط الذهني للبيانات بالنظر والاستماع، وقد تتم عن طريق نسخ البيانات المخزنة الكترونيا داخل الحاسب الآلي سواء أكانت مخزنة داخل نظام الحاسب الآلي أو على وسائط التخزين المتعارف عليها، وقد ترتكب بعد التمكن من اختراق نظام الحاسب الآلي، (التوصل المصرح به) وأخيرا قد ترتكب عمليات القرصنة عن طريق اعتراض معطيات الحاسب خلال عملية نقلها.[4] ويكون هدف الفاعل في قرصنة البرامج والبيانات إما إعادة إنتاجها أو نسخها للاستفادة منها أولبيعها والحصول على منفعة مادية منها[1].

---

[1] Laure Zicry, op.cit, p.94.

[2] في دراسة قامت بها Symantec في 2013 فإن التكلفة العادية للمساس بالمعطيات البنكية يقارب 188000 دولار وأن عمليات القرصنة تلك تؤدي بعد فترة وجيزة إلى اختفاء تلك المؤسسات نظرا لحجم الخسائر التي تسببها القرصنة، عن Laure Zicry, op.cit, p.17.

[3]- انتصار نوري الغريب، مرجع سابق، ص 57.

[4] محمود أحمد عبابنة، مرجع سابق، ص 94.

إن جريمة السرقة حسب القواعد العامة في القانون الجنائي التقليدي هي سرقة المال المنقول المملوك للغير دون رضاه بغية تملكه، وعلى ذلك فإن فعل الاختلاس في جريمة السرقة يرد على المال المنقول المملوك للغير. لكن الأمر يختلف في جريمة السرقة المعلوماتية والتي تنصب السرقة فيها بصفة أساسية على المعلومات، بحيث أن المعلومات هي محل السرقة في جريمة السرقة المعلوماتية[2].

الفرع الثاني
محل جريمة السرقة المعلوماتية

إنه وفقا للقواعد العامة لجريمة السرقة بمفهومها التقليدي أن محل السرقة ينصب على مال منقول مملوك للغير وهو كل شيء يصلح للحيازة والنقل والتملك[3]، ولا يشترط أن يكون للمال قيمة محددة حتى يكون صالحا للسرقة. وأساس الخلاف بين الفقهاء فيما يخص سرقة المعلومات هو المال محل الجريمة باعتباره من العناصر الأساسية للجريمة وكذا انتفاء عنصر الإكراه في هذه الجريمة بالنظر إلى الوسيلة المستعملة فيها.

أولا:طبيعة المال في المعلوماتية

لتوضيح طبيعة المال في المعلوماتية يجب التفرقة بين أمرين:

أ- المال المعلوماتي الطبيعي (الأجهزة):

ويقصد به المكونات المادية لعناصر النظام المعلوماتي التي تحتوي على المعلومات ولها كيان مادي ظاهر وملموس والمتمثلة بوحدات العرض والتسجيل والشاشة وملحقات الجهاز والحاسب الآلي من أجهزة إدخال وإخراج (الطابعات، السماعات وغيرها) وكذلك الشرائط الممغنطة والدسكات.

والمال المعلوماتي الطبيعي يصلح لأن يكون محلا للسرقة باعتباره مال مادي ملموس ويمكن نقله وحيازته والاستيلاء عليه ومن ثم فالمعلومات المخزنة عليه تصلح لأن تكون محلا للسرقة[4].

---

[1] عايد رجا الخلايلة، مرجع سابق،ص101.

[2] القانون العربي النموذجي في المادة الرابعة عشر نص على سرقة المعلومات، بتجريم كل عمليات نسخ ونشر لمصنفات الفكرية أو الأدبية أوالأبحاث العلمية أوما في حكمها إذا ما ارتكب دون وجه حق، ويعاقب مرتكبها بعقوبة الحبس الذي ترك تقديرها وفقا لقانون كل دولة ودون الإخلال بنصوص الخاصة بالملكية الفكرية لكل بلد. ولاحظنا على النص اقتصاره على بعض المعلومات متناسيا البعض الآخر مثل المعلومات المتعلقة بحرمة الحياة الخاصة للفرد.و الأمر المهم أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لم تتعرض لهذا السلوك بالتجريم تماما وهو الأمر المستغرب.

[3] رشدي محمد علي محمد عيد، مرجع سابق، ص 209.

[4] هدى قشقوش، جرائم الاعتداء على الحاسب الآلي في القانون المقارن، دار النهضة العربية، 1990، ص 56.

ب- المال المعلوماتي المنطقي:

يقصد به العناصر المنطقية في النظام المعلوماتي، وهي ما تحتويه هذه العناصر من برامج وبيانات صالحة للمعالجة آليا، والمقصود هنا المعلومات المختزنة داخل النظام المعلوماتي وليست المنتقلة من خلاله، وهنا يثور التساؤل على هذا المال المعلوماتي بغض النظر عن دعامته المادية طبعا هل يصلح محلا للسرقة أم لا؟

وانقسم الفقهاء في ذلك إلى رأيين، فيرى أصحاب **الرأي الأول** أن المعلوماتية ليست مالا ويخضع للسرقة.

وباعتبار أن المعلوماتية ليست مالا[1]، فذهب رأي منهم إلى أن المقومات المعنوية من النظام المعلوماتي يمكن أن تستغل ماليا فالقابلية للاستغلال المالي لا تعني أنها وارده على شيء يعتبر مالا في ذاته، ومن هنا لا يمكن وقوعها محلا لجريمة السرقة.

وتبرير ذلك أن هذه المقاومة التي تتكون أصلا من البرامج والبيانات والمعلومات بالإضافة جهد الآلات تقوم بإجراء المعالجة الآلية للمعلومات،بحيث أن البرامج هو إبداع أو ابتكار فكري وذهني قابل للرد والاستغلال المالي وهو يقوم بمعالجة المعلومات، ولذلك فإن الاعتداء عليه هو اعتداء على حقوق المؤلف في هذا استغلال مصنفه استغلالا ماليا ومن ثم يرد عليه أحكام حماية حق المؤلف وليست السرقة[2].

أما بالنسبة للمعلومات فقد تكون سرية والاطلاع عليها أو حيازته محظور وبالتالي فإن الحصول عليه ممن ليس لديه الحق يمثل انتهكا لسرية المعلومات وليست سرقة لها.أما إذا كانت المعلومات غير سرية فهي مجانية وشائعة ولا جريمة للحصول عليها، وقد تكون بالمقابل وهنا نكون أمام سرقة منفعة وينتهي هذا الرأي إلى الجانب غير المادي من النظم المعلوماتي يجب فهمه على انه يعني القابلية للاستغلال المالي[3].

ورأي آخر يرى، أن المعلوماتية لا تصلح أن تكون مالا أو محلا للسرقة إلا إذا اقترنت بالمادية لذلك فإن التعدى عليها بالسرقة لا يعتد به، إلا في حالة وجودها مسجلة على دعامات أو اسطوانات فهي تصبح في ذلك أموالا تصلح محلا للسرقة[4].

---

[1] عن موقف القضاء الانجليزي فقد قرر في قضية Oxford V ,Moss براءة الأشخاص المتهمين بسرقة أسرار ومعلومات لعدم اعتبارها أموالا بالمفهوم القانوني، عن كامل السعيد، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 أكتوبر 1993، ص 349.

[2] سالم محمد سالم بني مصطفى، جريمة السرقة المعلوماتية، مذكرة ماجستير، جامعة جادارا، اربد، الأردن، سنة 2011 ، ص 54.

[3] عمر الفاروق الحسيني،المشكلات الهامة في الجرائم المتعلقة بالحاسب الآلي وأبعادها الدولية، دار النهضة العربية القاهرة ، 1992،ص 93.

[4] محمود أحمد عبابنة، مرجع سابق،ص 98.

أما عن أصحاب **الرأي الثاني** أن المعلوماتية تعتبر مالا ويخضع للسرقة، إذ يرى هذا الجانب أن المعلوماتية لها قيمة مالية ويمكن من خلالها أن تخضع للسرقة، حيث أن المعلومات من الأفكار تحتوي على رسالة يمكن إدراكها عند الحفظ أو النقل أو المعالجة.

فالمعلومات ناتج تكوين نسق فكري لمبتكرها أو مبتدعها ويترتب عليها وجود علاقة بين المعلومات ومبتكرها فيكون له نقلها وإيداعها وحفظها وتأجيرها وبيعها، فالمعلوماتية تعتبر أموالا ذات قيمة اقتصادية حيث أنها تطرح في الأسواق للتداول مثل أي سلعة ولها سوق تجاري يخضع لقوانين السوق الاقتصادي[1]. والبعض يعتبر المعلومات أموالا بالنظر إلى الاستدراكية التعاقدية والحق في المنافسة لأن ذلك يخضع بالاعتبار القيمة الاقتصادية للمعلومات مع إسباغ الحماية التي يقررها القانون حق المؤلف على الإبداعات المعلوماتية وهي حماية حقيقية[2]. إضافة إلى ظهور اتجاه حديث في فرنسا ينادي أيضا بصلاحية المعلومات بذاتها لتكون محلا للسرقة استنادا إلى لفظ الشيء[3]، التي وردت في تعريف السرقة وفقا للقانون الفرنسي تمتد لتشمل الأشياء المعنوية ومنها المعلومات. ويقال أيضا أن الشيء يعتبر مالا ليس بالنظر إلى ما له من كيان مادي ملموس، وإنما بالنظر إلى قيمته الاقتصادية وأن القانون الذي يرفض إسباغ صفة المال على شيء له قيمة اقتصادية هو بلا جدال قانون ينفصل تماما عن الواقع[4]. ولهذا يكون مقبولا أن يكون موضوع المال شيئا غير مادي متى كانت له قيمة اقتصادية ومن تم لا مانع من إضفاء وصف المال على المعلومات، كما أن الفقيه السنهوري يرى أن التطور قد زاد من عدد الأشياء المعنوية بحيث تفوق بعضها قيمة الأشياء المادية مما استدعى الأمر إلى إعادة النظر في حصر الأموال على الأشياء المادية وحدها، والبحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الحق المالي حتى يمكن إسباغ صفة المال على الشيء المعنوي، وبهذا يكون قد أخذ بالمفهوم الواسع للمال[5]. وإلى جانب هذا الاتجاه ظهر اتجاه آخر ينادي بأن المعلومات ذات طبيعة مادية لأنها تشغل

---

[1] قد قضي في الولايات المتحدة الأمريكية في قضية Hancock v. state والتي تتلخص وقائعها في أن أحد المبرمجين بشركة تكساس للمعدات قام بنسخ 59 برنامج مملوك لشركته وتقدم بعرضها للبيع لشركة أخرى منافسة مقابل خمسة ملايين دولار وقد تمسك المتهم في دفاعه أن قيمة البرامج لا تتعدى 35 دولار وهي قيمة الورق الذي استخدمه لنسخها، وكان ذلك بهدف إلى الاستفادة من تدرج العقوبات في ولاية كاليفورنيا التي حدثت بها الواقعة في جسامة السرقة وعقابها وفق لقيمة الشيء محل السرقة، ولم تقبل المحكمة دفاع المتهم استنادا إلى تقرير الخبرة حيث قررت أن قيمة الشيء المسروقة تساوي 205 مليون دولار وليست قيمة الأوراق المستخدمة في نسخها وقضت بإدانة المتهم، مشار إليه لدى رشدي محمد علي محمد عيد ، مرجع سابق، ص211.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، مرجع سابق، ص 239-240.

[3] المقصود بالمال في القانون الجزائري ورد في القانون المدني في المادة 682 منه وعرفه أنه :" أنه كل شيء خارج عن التعامل بطبيعته أوبحكم القانون"، والشيء كما عرفته ذات المادة أنه ما يصلح لأن يكون محلا لحق من الحقوق المالية.

[4] السيد عتيق، جرائم الانترنت، دار النهضة العربية، القاهرة، بدون طبعة، 2000، ص 91.

[5] عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء الثامن المتعلق بالملكية، منشورات الحلبي الحقوقية، بيروت،2011 ، ص 72.

فراغا في الحيز الخارجي، ولكن إذا ما تم تطبيق هذا على البيانات التي يتضمنها الكمبيوتر سنجد أن هذه البيانات ما هي إلا نبضات رقمية ينشغل بها حيز معين لتخزين البيانات في الحاسب الآلي ويمكن تحديدها وقياسها بواسطة وحدات القياس الميجابايت[1].

وهناك أيضا رأي في الفقه الحديث، يرى أن المشرع حينما نص على السرقة لم يذكر المال ولم يذكر طبيعته سواء كانت مادية أو معنوية وترك الأمر للفقهاء والقضاء لتحديد ذلك، وقد سمح للقضاء بالقول بصلاحية الأموال المعنوية لتكون محلا للسرقة[2].

أما ما ذهب إليه الرأي الأول باعتباره أن المعلومات ليست مالا، فهو يرى أن الوقت الذي وضعت فيه نصوص السرقة القديمة كانت فيه الأموال المعنوية قليلة القيمة، وكان التركيز على حماية الأموال المنقولة ذات القيمة الكبيرة، فضلا على أن لأموال المعنوية والمعلوماتية أصحت في هذا العصر بفضل التطور العلمي والتقني تشكل قيمة اقتصادية كبير بدرجة تفوق الأموال المادية المنقولة والعقارات، كما أن هذه المعلوماتية لم تكن في ذهن المشرع عندما وضع نصوص السرقة[3].

ومما سبق فإن الآراء قد تضاربت حول الطبيعة القانونية للمعلومات والأجدر تأييد الفقه الحديث الذي أخذ بالمفهوم الموسع للمال ليشمل إلى جانب الأشياء المادية تلك الأشياء غير المادية ومنه اعتبر المعلومات مالا .

ثانيا: طبيعة المنقول في جريمة السرقة المعلوماتية

بداية يعرف المال، بأنه كل عين أو حق له قيمة مادية في التعامل ويمكن حيازته ماديا أو معنويا وبالانتفاع به انتفاعا مشروعا ولا يخرج عن التعامل بطبيعته أو بحكم القانون ويصح أن يكون محلا للحقوق المالية. وتم تعريف العقار بأنه كل شيء مستتر بحيزه ثابت فيه لا يمكن نقله منه، دون تلف أو تغيير هيئته فهو عقار، وكل ما عدا ذلك فهو منقول[4].

فحتى ولو كانت المعلومات تثير إشكالا في مدى اعتبارها من الأموال التي يمكن سرقتها، إلا أنه من المسلم به أن هذه المعلومات يمكن أن تترجم إلى قيم مالية نظرا لقابليتها للاستغلال مقارنة بالبرامج التي هي نوع من الغداء الذهني والفكري. وبما أن البرامج عبارة عن أسلوب ينظم العمل والمعالجة، فإن استخدام هذا الأسلوب بصورة غير مصرح بها من قبل مالكها أو حائزها الشرعي يشكل اعتداء على حقوق الاستغلال المالي. وكذلك فإن المعلومة بما تمثله من صفة السرية يمكن الاعتداء عليها بمجرد الإطلاع عليها دون إذن صاحبها لأن

---

[1] محمود أحمد عبابنة، المرجع السابق،ص 98.

[2] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للنشر والتوزيع، الإسكندرية، 1992، ص 320.

[3] سالم محمد سالم بني مصطفى، مرجع سابق، ص 55.

[4] محمود احمد عبانة، مرجع سابق، ص 95.

هذا يمثل انتهاكا لسرية المعلومة، أما إذا كانت هذه المعلومة من النوع المتاح الإطلاع عليه للجميع، فهي إما أن تكون مجانية ولا تثور هنا مشكلات أبدا، وإما يكون الإطلاع عليها بمقابل وهنا فإن الإطلاع عليها دون مقابل بعد انتهاكا للمنفعة التي تجسدها المعلومة[1].

وسيتم التفصيل في ما يثار حول المعلوماتية، هل هي منقول يمكن اعتبارها محلا للسرقة أم لا ؟وذلك من خلال الآراء الفقهية التي انقسمت إلى رأيين، الرأي الأول يرى أن المعلوماتية ليست منقولا ولا تصلح للسرقة أما الرأي الثاني يرى أن المعلوماتية منقولا وتصلح للسرقة وفيما يلي بيان لذلك.

فيرى أصحاب **الرأي الأول** أن المعلومات ليست منقولا ولا تصلح محلا للسرقة ويستندون في ذلك إلى الآراء التالية:

- ذهب رأي إلى أنه قد يقع اعتداء على المعلوماتية الموجودة على الشيء المادي الدعامة المادية (الأقراص،الشريط) على سبيل المثال، ويترتب على هذا الاعتداء أضرار تفوق القيمة الحقيقة للدعامة ذاتها، وترجع الأضرار إما لأن إخفاء المعلومات سيتبعه إفشاء الأسرار التي تتضمنها المعطيات التي كانت متوقع بقائها في نطاق الأسرار وإما أن هذا الاعتداء يتعلق بمعطيات لم يتم نسخها بعد، وفي الحالتين لا تتوفر عناصر جريمة السرقة، فالسرقة لا تقع إلا على الأشياء والمعلومات لا تعتبر من قبيل الأشياء حيث تم الحصول عليها بالسمع أو بالقراءة على الشاشة أو بإعادة نسخ الأسطوانة التي يملكها الجاني نفسه[2].
- ذهب رأي آخر إلى أن المعلومات المخزنة سواء بالنظام المعلوماتي أو أي وسيط لا تعد في حد ذاته أشياء مادية ولا يتصور انتزاعها وحيازتها ولا تكون محلا للسرقة إلا أن المستندات المثبتة لها أو التي تكون وسيلة التسجيل عليها هي التي تصلح للسرقة لأن لها كيان مادي، ولكن إذا تجسدت تلك المعلومات على أي ركيزة فهي تعد من الأشياء وتصلح للسرقة كما أن الصورة التي تظهر على شاشات النظام المعلوماتي ولو أنها تبدو نتاجا لنشاط إنساني يكمن بالجهد الفني الذي يبذله في إعدادها إلا أنها لا تعتبر بمثابة الشيء حيث أصبحت لا تصلح لأن تكون محلا للسرقة[3].

أما عن أصحاب **الرأي الثاني** فيرون أن المعلوماتية منقولا وتصلح للسرقة حيث قاموا بالرد على رأي القائل بأن المعلوماتية ليست منقولا، واستندوا في رأيهم بأن المعلوماتية منقولا وتصلح أن تكون محلا للسرقة على ما يلي:

---

[1] محمود احمد عبانة، مرجع سابق، ص 95 ، 96.

[2] سالم محمد سالم بني مصطفى، مرجع سابق، ص 56، أشار إليه عمر إبراهيم الوقاد، الحماية الجنائية للمعلومات، جامعة طنطا، ص8.

[3] سالم محمد سالم بني مصطفى، مرجع سابق، ص 56.

- ذهب رأي إلى كلمة " شيء " الواردة في القانون والتي وردت عموما في تعريف السرقة ووفقا لذلك فهي تمتد لتشمل الأشياء المادية والغير المادية وإذا كان من الممكن حيازة الأشياء الغير مادية مثل حق الانتفاع والدين فإنه من الممكن حيازة المعلومات ويمكن سلب حيازتها وبذلك تكون محلا للسرقة وذهب رأي آخر إلى أن الاستيلاء على المعلومات يمكن أن يتحقق عن طريق السمع أو المشاهدة ذلك بما تمثله من صفة السرية فان مجرد الاطلاع عليها دون إذن صاحبها لأن هذا يمثل انتهاكا لسريتها[1]، ومن ثم فإن المعلومات يمكن أن تنتقل من عقل لأخر وفي هذا الحال يمكن صب المعلومات في إطار مادي عن طريق تحيزها داخل الإطار والاستئثار بها وينتج عن ذلك قيام الشخص الذي التقط المعلومة عن طريق السمع أو المشاهدة بتدوينها أو تحليلها على دعامة ثم يعرضها للبيع مثلا ففي هذه الحالة تنتقل المعلومات من ذمة شخص إلى ذمة آخر وبالتالي يمكن أن ينطبق عليها وصف المال المنقول وتكون محلا للسرقة[2].
- ويذهب رأي أن حماية هذا النوع من الأموال عن طريق النص الجنائي الخاص بالسرقة أمر مقبول ويمكن اختلاس المعلومات ويمارس عليها تصرفات حيازة ضد إرادة صاحبها الشرعي لأنه بإمكانه حيازة المعلومة فالأشياء المعنوية قابلة للحيازة وليست فقط الأشياء المادية وطالما بالإمكان حيازة الأولى فيمكن أيضا نزع حيازتها ومن ثم يصبح وصف السرقة مقبولا لها[3]، وفي هذا نشير أن المشرع الجزائري من خلال نص المادة 350 من قانون العقوبات لم يشترط صراحة أن يكون المال موضوع الجريمة ماديا، مما يجعل وقوع الجريمة على مال معنوي لا يصطدم بمبدأ شرعية الجريمة والعقوبة.
- ورأي آخر يرى أن سرقة المعلومات وليست الدعامات المخزنة عليها المعلومات هو السبب الذي من أجله أدانت محكمة النقض الفرنسية في قضية " Logabax " العامل الذي قام بنسخ المستندات سرية بدون علم ورضاء صاحب المشروع[4].

وفي الحقيقة الكثير من يؤيد الرأي الثاني القائل بصلاحية المعلومات لأن تكون منقولا لأن البرامج والمعطيات وإن لم يكن شيء ملموس أو محسوس إلا أنها لها كيانا ماديا يظهر من رؤيتها على شاشة النظام المعلوماتي، وتنتقل عبر الأسلاك وعن طريق نبضات ورموز وشيفرات أي أن لها أصلا أو أمول صادر عنه ويمكن سرقته وبالتالي له محلا مادي ويمكن الاستحواذ عليها ونقلها، ولكننا هنا فقط نود الإشارة أنها سرقة ولكن هل من الجائز تطبيق النص المتعلق بالسرقة عليها أم لابد من استحداث نص جديد؟.

---

[1] محمود أحمد عبابنة، مرجع سابق، ص 96.

[2] احمد خليفة ملط، مرجع سابق، ص 243-244.

[3] محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات، مطابع الهيئة المصرية للكتاب، 2003، ص55.

[4] رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنت، دار النهضة العربية، القاهرة، 2013، ص 216.

ثالثا: ملكية الغير للمال المعلوماتي

تشترط القواعد العامة للسرقة لوقوع الجريمة شرطين الأول، عدم ملكية المال محل السرقة للسارق والثاني ملكية المال محل السرقة للغير[1]، وذهب رأي إلى أن القواعد العامة لملكية الغير في السرقة تسري كلها على الأموال المعلوماتية من البرامج والمعدات والأسطوانات وأجهزة وشاشات أما بالنسبة للبرامج فإن العقبة في تحديد صاحب الحق على البرامج والمعلومات فالبرامج والابتكارات الفكرية محمية بحماية حق الملكية الفكرية وحقوق المؤلف فالبرنامج ملكا لمن ابتكره[2].

وذهب رأي آخر إلى أن جوهر الاختلاس في السرقة هو دخول الشيء في حيازة الجاني وهو شرط مفترض لوقوع السرقة على شيء منقول مملوك للغير مثال ذلك المعلوماتية باعتبارها ذات أهمية اقتصادية وسياسية، وهو ما أكده الفقه الفرنسي، بأن سبب وجود المعلومات ليس إلا قابليتها للنقل للغير وبذلك فالمعلومات المنسوخة من على الدعامات والمعالجة آليا يعترف بحقوق الملكية لمن قام بعمل المعالجة الآلية لها ويوضح ذلك أن سرقة الدعامات المملوكة للغير والمنسوخ عليها معلومات هي سرقة للمعلومات نفسها لأن الدعامات بدون معلومات لا قيمة له، وبالتالي في حالة السرقة ينتقل المال المعلوماتي من حيازة مالكه إلى حيازة الغير الجاني[3].

وإذا كان الاستيلاء على المعلومات المنسوخة على دعامات هي سرقة للمعلوماتية ذاتها، وإن كانت تحميها قواعد الملكية الفكرية. وينتج عن ذلك قبول السرقة حماية لمبدعها وأصحاب المؤسسات المنتجة لبرامج المعلوماتية فإذا كان المال المعلوماتي محل السرقة مملوك للغير، فقد تحقق بذلك الاعتداء على الملكية ويعد الفعل سرقة سواء كان اسم صاحب المال معروفا أولم يكن معروفا، وسواء كان مملوكا لشخص طبيعي أو شخص معنوي أوعدة أشخاص[4].

إذن المعلوماتية تصلح بأن تكون محلا للملكية باعتبار أن التحليل المنطقي الذي لا يمكن إنكاره هو ملكيتها لشخص ما وبالتالي فهي ليست ملكا للسارق بل يقوم بالاستحواذ عليها ،كشيء ليس مملوكا له وهذا هو جوهر الاختلاس في السرقة[5].

الفرع الثالث

الركن المادي في جريمة السرقة المعلوماتية

[1] نبيل صقر، الوسيط في شرح جرائم الأموال، دار الهدى، الجزائر، 2012، ص 236.

[2] عبد المهيمن بكر، قانون العقوبات القسم الخاص، دار النهضة، الطبعة السابعة، 1977، ص 771.

[3] - أحمد خليفة الملط، مرجع سابق، ص 246-247.

[4]- نبيل صقر، مرجع سابق، ص 237، علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر ،1999 ، ص 94.

[5]- هدى قشقوش، مرجع سابق، ص 483.

الركن المادي وفقا للقواعد العامة للسرقة هو الاختلاس، ولم يعرف المشرع الجزائري الاختلاس ولكن اتفق الفقه والقضاء على اعتبار أنه "أخذ مال الغير دون رضاه ". أي لابد أن يتم نزع المال من مالكه بالقوة وهو الاستيلاء على حيازة الشيء بغير رضى مالكه أو حائزه، ويتوفر الاختلاس إذا قام الجاني بحركة مادية لينقل الشيء إلى حيازته أيا كانت الطريقة ويشترط أن يكون الاستيلاء بفعل الجاني[1]. والاختلاس لايعني مطلق الاستيلاء على مال الغير وإنما انتزاعه من صاحبه وإنما فقط الاستيلاء عليه بوسيلة معينة[2]. ولإيضاح الركن المادي لجريمة السرقة المعلوماتية سنتناول فيه عناصر فعل الاختلاس في الجريمة المعلوماتية والعنصر المعنوي والذي يتمثل في عدم رضى المجني عليه ونية تملك الجاني.

أولا:فعل الاختلاس وعناصره في جريمة السرقة المعلوماتية

لا خلاف بين الفقهاء على أن الاختلاس الذي يقع على المكونات المادية للحاسب الآلي وملحقاته والبرامج والبيانات المدونة على دعامات مادية كالاسطوانات والشرائط وغيرها والتي يتم نقلها أو الاستيلاء عليها وحيازتها دون رضاء مالكها أو حائزها وبغية تملكها تخضع وفقا للمفهوم التقليدي للقواعد العامة للسرقة، فسرقة دعامة مادية (اسطوانة أو أي قرص مضغوط) محمولة بمعلومات في شكل معطيات هو كسرقة كتاب مملوك للغير باعتبار، هو أيضا محمول بمعلومات[1]، ولا يشترط أن تكون الحيازة الجديدة للمتهم نفسه بل من الممكن أن تكون لشخص آخر غيره ولذلك من يقوم باختلاس برامج معالجة المعلوماتية ويسلمها لشخص آخر لتدخل في حيازة هذا الأخير تقوم بها جريمة السرقة حال اكتمال أركانها لأنه يفترض هنا دخول الشيء في حيازة المتهم قبل دخوله في حيازة الآخر[3].

والخلاف بين الفقهاء يثور من خلال تطبيق فعل الاختلاس وعناصره على المكونات غير المادية للنظام المعلوماتي وسنوضح ذلك من خلال عنصري الاختلاس.

أ-العنصر الموضوعي (الاستيلاء على المعلوماتية):

نشأ الخلاف بين الفقهاء حول الاستيلاء على المعلوماتية من خلال رأيين، الأول يرى عدم توافر ركن الاختلاس في حالة الاستيلاء على المعلوماتية، والثاني يرى توافر ركن الاختلاس في حالة الاستيلاء على المعلوماتية.

وقد ظهرت أوجه هذا الخلاف من خلال الصور التالية: الأولى الطبيعة المعلوماتية، والثانية المعلوماتية المخزنة بالنظام المعلوماتي، الثالثة المعلوماتية المخزنة على دعامات.

---

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت، دراسة متعمقة في القانون المعلوماتي، دار الكتب القانونية، مصر، 2008، ص 408.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنت، دراسة متعمقة في القانون المعلوماتي، المرجع نفسه، ص 407.

[1]– دردور نسيم ، مرجع سابق، ص 56.

[3] محمود نجيب حسيني، مرجع سابق، ص 84، دروس في القانون الدولي الجنائي، دار النهضة العربية، القاهرة، 1960.

الصورة الأولى: الطبيعة المعلوماتية

تنازع موضوع الطبيعة المعلوماتية جانبان من الفقه حيث يرى أنصار **الرأي الأول** عدم خضوع المعلوماتية إلى اختلاس ويرجع ذلك لأن طبيعة المعلوماتية طبيعة معنوية بينما طبيعة الاختلاس طبيعة مادية[1] ويستندوا إلى الأدلة التالية :

1. المعلومات غير قابلة للقياس أو التحديد، بالإضافة إلى أن هناك اختلاف من حيث الطبيعة بين المعلومات المخزنة في النظام المعلوماتي والتي يجري البحث عن محتواها المعنوي وبين الطاقة الكهربائية التي هي حقيقة مادية حتى لو كانت غير ملموسة.[2]
2. إن الاختلاس اللازم لوقوع السرقة بمعناها المعروف غير متحقق لأنه ينطوي على تبديل الحيازة وينحصر في الحصول على منفعة الشيء فقط دون أصله الذي يبقى في حيازة صاحبه ولا صعوبة في القول بأننا نكون هنا أمام سرقة منفعة بشرط وجود نص بهذا الأمر وفي حالة عدم وجود نص فلا سرقة في الأمر[3].
3. يرجع السبب لعدم وجود قوانين خاصة بسرقة المعلومة بحد ذاتها تغل يد القضاء في بعض الحالات التي يستحيل فيها تطبيق نصوص السرقة على سرقة المعلومات اللامادية[4].

بينما يرى أنصار **الرأي الثاني** خضوع المعلوماتية إلى الاختلاس للأسباب التالية: [5]

1. إن المعلومات قابلة للتحديد والقياس مثل الطاقة الكهربائية ويمكن قياسها عن طريق كمية المعلومات الموجودة بالشريط أو الاسطوانات أو عن طريق طول الشريط أو الفترة التي يستغلها.
2. إن كلمة الشيء الواردة في أحكام قانون العقوبات الخاصة بجريمة السرقة تشمل الأشياء المادية وغير المادية ويكون من الممكن حيازة المعلومات وطالما من الممكن حيازتها فمنه يمكن الاستيلاء عليها وتستند هذه النظرية إلى مقولة أن القانون الجاني يجب أن يتطور لكي يمكن حماية الممتلكات الحديثة (المعلوماتية).
3. يمكن اختلاس المعلوماتية باعتباره خلق فكري، وركن الاختلاس سيكون من نفس طبيعة الشيء أي الحيازة الفكرية لهذا الشيء المعلوماتي.

---

[1] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، مرجع سابق، ص 339، جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، 1992، ص 73.

[2] عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2001، ص 167.

[3] محمود أحمد عبابنة، مرجع سابق، ص 96-97.

[4] سالم محمد سالم بني مصطفى، مرجع سابق، ص 61.

[5] احمد خليفة ملط، مرجع سابق، ص 255.

وحيث أن الرأي الثاني القائل بصلاحية المعلومات للاختلاس يعتبر الأقرب إلى الترجيح لهذا لابد من تصدي المشرع لهذا الشكل من الجريمة بنصوص مستحدثة غير نصوص السرقة عامة. رغم أنها في الواقع لا تتعارض مع هذا الرأي كما سبقت الإشارة. حيث أن تلك النصوص ومنها المادة 350 من قانون العقوبات الجزائري تتضمن السرقة المعلوماتية لأن النص لم يحدد طبيعة الشيء المسروق ماديا كان أو معنويا.

ولكن يبقى دوما لزوم تحديث النص أو إيراد نص جديد دلك أن السرقة بمفهومها التقليدي لا تتناسب مع صور السرقة المعلوماتية والأفضل أن نسميها القرصنة للتمييز بينهما من حيث المصطلحات.

الصورة الثانية: صور سرقة (قرصنة) المعلوماتية المخزنة في النظام المعلوماتي

نعرض في هذه الصورة مدى صلاحية المعلوماتية المخزنة بالنظام المعلوماتي من خلال حالتين الأولى تتمثل في نسخ ونقل المعلوماتية من النظام المعلوماتي، أما الثانية فهي الالتقاط الذهني والسمعي للمعلوماتية من النظام المعلوماتي.

الأولى : النسخ غير المشروع للمعلومات من النظام المعلوماتي

إن الشخص الذي يحصل على معلومات مختزنة في جهاز حاسوب شخص آخر بحيث لا يؤدي إلى حرمان الشخص صاحب المعلومات من المعلومات المختزنة في جهازه إذ لم يؤخذ منه شييء، وكل ما في الأمر أن المعتدي قام بنسخ هذه المعلومات أو تصويرها ويكون بدلك قد تقاسم الاطلاع على هذه المعلومات مع صاحبها بالإضافة إنه لم تقم لديه نية حرمان صاحب المعلومات مما أخده مؤقتا أو دائما،والمشكلة هل هذه الواقعة تعد من قبيل السرقة[1].

نشأ خلاف بين الفقهاء من حيث صلاحية نسخ ونقل المعلومات من النظام المعلوماتي للاختلاس إلى رأيين، يرى أنصار **الرأي الأول منهما** عدم صلاحية نسخ ونقل المعلوماتية في النظام المعلوماتي حتى لوأدى ذلك في بعض الأحيان إلى الإضرار بها وإتلافها أوالتأثير على قيمتها مستندا إلى ما يلي :

1. أن المعلومات المخزنة على النظام المعلوماتي، وإن كانت لا تعتبر في ذاتها أشياء مادية فلا يتصور انتزاع حيازتها ولا تكون محلا للسرقة إلا إذا وقعت داخل إطار مادي[2] .
2. الصعوبة التي تثار في عدم اعتبار نسخ ونقل المعلوماتية اختلاس يرجع إلى أن الجاني لم يستولي على أصل المعلومة، ولكنه نقل صورة منها وبالتالي لا ينطبق عليه السرقة ومما لا شك فيه، أن عدم مشروعية هذا الفعل قد يعد تقليدا أوسرقة منفعة بشرط وجود نص خاص

[1] علي حسن الطوالبة، مرجع سابق، ص125.

[2] سالم محمد بني مصطفى، مرجع سابق، ص 62.

في هذا الشأن أما في حالة عدم وجود هذا النص فلا يوجد سرقة ، كما أن ذلك لا يعد سرقة لا صل المعلومة حتى لوتم تدميرها أو إتلافها[1].

بينما يرى أنصار **الرأي الثاني** صلاحية اختلاس نسخ ونقل المعلومات في النظام المعلوماتي ويؤيد هذا الرأي ما يلي :

1. يقع فعل الاختلاس على المعلوماتية لوجودها بكل فوائدها الاقتصادية تحت فعل الجاني فيصبح بمقدوره التصرف فيها بحرية ويظهر عليها بمظهر المالك ويغتصب سلطة أو ميزة إعادة الإنتاج التي تخصه ويجرد المعلوماتية كليا أو جزئيا من القيمة وبخاصة القيمة الاقتصادية التي تمثلها في الذمة المالية للمجني عليه، ويؤيد أصحاب هذا الرأي ضرورة وجود نشاط مادي بعد هذا الاختلاس ويتمثل في بيع المعلوماتية أو وضعها موضوع التنفيذ[2].
2. فكرة الاستيلاء الاحتيالي لنسخ ونقل المعلوماتية، هي إحدى صورة التفسير الواسع للاختلاس وأيدت المحكمة ذلك في قضية (Logbax) التي أدانت إحدى العمال بالسرقة عن حالة النسخ الفوتوغرافي للمستندات السرية، حيث أن هذه المستندات ثم الاستيلاء عليها احتيالا. وأنه وفق لرأي فقهاء المعلوماتية بأن سرقة المعلومات تختفي وراء سرقة الأوراق والمستندات[3].

الثانية : الالتقاط الذهني والسمعي للمعلومات

عرفت المادة الأولى في الفقرة 11 من القانون العربي النموذجي الموحد لمكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات الالتقاط الذهني أنه:"الالتقاط يقصد به الالتقاط البصري أي الاستحواذ البصري على البيانات بمعنى حيازتها والتقاطها ذهنيا وبصريا من الشاشة" ، ومن خلال هذا النص يتضح أن المقصود بالالتقاط هو ذلك الذي يتم بالبصر دون الاعتماد على وسيلة إلكترونية[4]. وأما عن الالتقاط السمعي والذهني فهنا نود أن نشير إلى أن هذا الفعل لا يعتبر من قبيل التجسس، حيث أن الالتقاط الذهني والسمعي في جريمة السرقة المعلوماتية يكون محله المعلومات المختزنة في النظام ليس كما هو الشأن بالنسبة للمعلومات المنتقلة عبر النظام والتي تعتبر اعتراضا لمسار المعلومات وحينها تعتبر تجسسا وليس سرقة.

اختلف الفقهاء في صلاحية الالتقاط السمعي والذهني (البصري) للمعلوماتية للاختلاس إلى رأيين، يرى أنصار **الرأي الأول** عدم الصلاحية للاختلاس ويؤيد هذا ما يلي :

---

[1] عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وابعادها الدولية ،القاهرة ،1992، ص106.

[2] احمد خليفة ملط، مرجع سابق، ص 256.

[3] علي عبد القادر القهوجي ، مرجع سابق، ص62.

[4] علي حسن الطوالبة، مرجع سابق، ص 124.

1. أن الصورة التي تظهر على شاشة النظام المعلوماتي ولو أنها تبدو كنشاط إنساني يمكن تقديرها بالجهد الفني الذي يبذله المختص إذ انه لا تعتبر مكتوبة ولا تصلح للسرقة[1].
2. عدم الصلاحية لعدم وجود النشاط مادي في هذه الحالة وقع تحت سيطرة الجاني كما أن السلوك الشخصي في هذه الحالة لا يتوفر فيه مقاومات النشاط المادي ذو المظاهر الخارجية الملموسة الذي يقتصر التجريم عليه في الشرائع الحديثة وأن وجود جرائم تتمثل مادياتها في محض النشاط الذهني تفتح مجالا لتجريم ما يدور في العقول والأذهان وهذا غير معقول كما أن القول بأن مجرد الإطلاع على المعلومات دون علم ورضى صاحبها يمثل جريمة سرقة يؤدي إلى نتائج غير معقولة ومبالغ فيها وأن التعليق للعقاب على سرية المعلومة ليس به شيء من الواقعية[2].

و يرى أنصار الرأي الثاني صلاحية الالتقاط الذهني والسمعي للمعلوماتية للاختلاس ويؤيد هذا ما يلي :

1. أن الاستيلاء على المعلومة يمكن أن تتحقق عن طريق السمع أو المشاهدة ومن ثم فإن المعلومة يمكن وضعها في إطار مادي عن طريق تحيزها داخل إطار معين والإستئثار به ويتحقق ذلك إذا قام الشخص الذي التقط المعلومة بتدوينها أو تسجيلها على دعامة ثم يعرضها للبيع وفي هذه الحالة تنتقل المعلومة من ذمة مالية إلى ذمة مالية أخرى حيث لم يعد صاحب المعلومة الشرعي هو الوحيد صاحب الحق في احتكارها[3].
2. يمكن الحصول على البرامج والمعلومة بتشغيل الجهاز ورؤية المعلومة على الشاشة فإن المعلومة تنتقل من الجهاز إلى ذهن المتلقي وحيث أن موضوع حيازة حيازتها المعلوماتية غير مادي فإن واقعية الحيازة تكون من نفس الطبيعة أي غير مادي " ذهنية " وبالتالي نتوصل إلى إمكانية حيازة المعلوماتية عن طريق الالتقاط الذهني عن طريق البصر أو السمع[4].

يعتبر الرأي الثاني أكثر منطقية ذلك والقائل أن المعلومات يمكن اختلاسها، لأن المعلومات الموجودة على الجهاز سواء كانت برامج أو بيانات طالما تم وضعها والتعامل فيها فإنها تصلح ماديا وماليا، وبالتالي فإنها تصلح لأن تكون محلا للاختلاس سواء تم نقلها أو الاطلاع عليها بالبصر أو السمع أي عن طريق الالتقاط الذهني.

---

[1] جميل عبد الباقي الصغير، مرجع سابق، ص68.

[2] هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ، 1992، ص 234.

[3] هشام فريد رستم، المرجع نفسه، ص 234.

[4] هدى قشقوش، مرجع سابق، ص 56.

الصورة الثالثة: المعلومات المخزنة على دعامات

اختلف الفقهاء حول صلاحية المعومات المخزنة على دعامات للاختلاس إلى رأيين، فيرى أنصار **الرأي الأول** عدم الصلاحية للاختلاس بل أنه ينطبق على سرقة الدعامة ذاتها[1] ،التي توجد عليها المعلومات ويؤيد هذا بما يلي :

1. أنه يترتب على سرقة المعلومات والبرامج الموجودة على الدعامة المادية أضرارا تزيد عن قيمتها الحقيقية للدعامة المادية لأنه يتبع سرقة المعلومات إفشاء للأسرار الموجودة بها كما أنه يتسبب بضياع عمل له قدر كبير من الأهمية ولهذا بعد بعضهم سرقة منفعة[2].
2. إنه في حالة افتراض وقوع الاختلاس على الأشياء المعنوية فيجب أن يقابله تشدد في تحقيق طبيعة هذا الاختلاس، بضرورة تحققه في نشاط مادي بأن ينقل على دعامة مادية، فأخذ الشيء غير مادي مثل المعلومات لا يكون ماديا إلا إذا كان قد تجسد في هيئة مادية[3].

أما أنصار **الرأي الثاني** يرى الصلاحية للاختلاس ويؤيد ذلك ما يلي:

1. أن سرقة المعلومات وليست الدعامة، هي السبب الذي أدانه من أجله محكمة النقض الفرنسية في قضية " lagbax " العامل الذي قام بنسخ المستندات السرية بدون علم ورضى المالك [4].
2. أن محكمة النقض الفرنسية أدانت شخص، عن جريمة إخفاء لأنه قدم للمحكمة صورة منسوخة كان قد أعدها بنفسه من مستند مسروق بمعرفة شخص مجهول الهوية، فالاختلاس هنا انصب على المعلومات بحد ذاتها[5]. و الرأي الثاني القائل بصلاحية المعلوماتية المخزنة على دعامات للاختلاس هو الرأي الأكثر تأييدا من جهة الأغلبية.

ب ـ العنصر المعنوي (عدم رضاء المجني عليه ونية تملك الجاني):

يجب أن يتوفر القصد الجنائي العام ، و يتمثل في تيقن الجاني أنه يأخذ مال الغير وليس ماله. فالشخص الذي يخرج من المطعم ويحمل معطف غيره معتقدا أنه معطفه لتشابههما لا يتوفر فيه القصد الجنائي العام. و عن القصد الجنائي الخاص والذي يتمثل نية تملك الشيء المختلس، فمن يأخذ شيئا من صاحبه بغية استعماله ثم إرجاع له أو الإطلاع

---

[1] يؤيد ذلك حكم محكمة فرنسية في قضية بوركان porguin الذي أدانت المحكمة فيه شخصين بالسرقة لقيامهما بالإستيلاء على مجموعة من الأسطوانات الممغنطة التابعة للمؤسسة التي يعملون فيها ونسخها ، ومن خلال الحكم أن المحكمة لم تمل إلى اعتبار الاستيلاء على المعلومات من قبيل السرقة إلا بشرط أن تكون مثبتة على دعائم مادية كالأسطوانات، عن محمود أحمد عبابنة، مرجع سابق، ص 190، علاء منصور مغايرة، الأوجه الحديثة التي ترتكب باستخدام الحاسوب، بحث مقدم إلى المعهد القضائي الأردني، 1997 ،ص 95.

[2] ALIAN Bensaussan, Le vol des programmes et des fichier,un grand malentendu expertisés,1981 .n° 26. P.15.

[3] أحمد خليفة الملط، مرجع سابق، ص 259.

[4] سالم محمد سالم بني مصطفى، مرجع سابق، ص 65.

[5] أحمد خليفة الملط، المرجع نفسه، ص 260.

عليه فقط فلا يعتبر سارقا .لأنه لم يقصد نقل الملكية له كالذي يأخذ كتبا من زميله لقراءته ثم يرجعها له ،أو الذي يأخذ سيارة صديقه للنزهة ثم يرجعها فلا يعتبر سارق[1].

ففي القواعد العامة للسرقة العنصر المعنوي في ركن الاختلاس يتمثل في عدم رضاء المجني عليه، هو عنصر مفترض بالنسبة لصاحب الحق في الشيء المعلوماتي المعنوي حيث أنه لا يرضى بما يخصه من أشياء معنوية مثال ذلك لو قام أحد الأشخاص بالدخول إلى جهاز الكمبيوتر الذي يخص شركة معينة وقام بأخذ المعلومات المخزنة فيه دون رضى أصحاب هذه الشركة فإن ما قام به يعد جريمة لسرقة المعلومات.

أما إذا قام بهذا الفعل واطلع على المعلومات التي تخص هذه الشركة بعد أخذ الموافقة من أصحابه أوالمسؤولين عنها فإن فعله لا يشكل جريمة سرقة المعلومات وذلك لانعدام ركن من أركان السرقة وهو عدم رضى المجني عليه.

ويتطلب العنصر المعنوي في الاختلاس أن يكون نية لدى الجاني في تملك الشيء المختلس وحيازته الحيازة الكاملة وهو ما أيدته محكمة النقض الفرنسية في قضية " lagbax " الذي كان يعمل موظفا في شركة وقام بتصوير مستندات سرية دون رغبة صاحبها وذلك بنية تملك هذه المستندات لمصلحته الشخصية[2] .

ثانيا: التسليم في المعلوماتية

يعتبر من القواعد العامة أن الاختلاس في جريمة السرقة لا يقع إذا كان المال في حوزة الجاني أو سلم إليه من مالكه، وتتحقق به الحيازة وليس وضع اليد فقط، وفي هذا المقام سنحاول توضيح التسليم الذي ينفي الاختلاس في المعلوماتية .

انقسمت الآراء القائلة فيما يتعلق بالتسليم فيما يخص المعلوماتية وأثره بالنسبة لجريمة السرقة، بينما كانت تلك الآراء الفقهية والقضائية تتعلق بالتسليم الصادر من الحاسب الآلي لتوزيع النقود، في حين أننا نود أن نتحدث عن تسليم المعلومات الموجودة داخل الحاسوب لمختلسها ذلك يقتضي من وجهة نظرنا تطبيق القواعد العامة المتعلقة بالتسليم في جريمة السرقة التقليدية .

الفرع الرابع

[1] - http://www.4algeria.com يوم الاطلاع على الموقع 2015/05/10.

[2] عبد القادر قهوجي، مرجع سابق، ص 62.

الركن المعنوي لجريمة السرقة المعلوماتية

جريمة السرقة هي جريمة عمدية والقصد الجنائي فيها قصد خاص يتطلب إلى جانب القصد العام توافر نية التملك للشيء المختلس لدى الجاني، وسيتم التفصيل فيهما من خلال مطلبين الأول القصد العام والمطلب الثاني القصد الخاص.

أولا: القصد العام

يتوافر القصد العام في السرقة بتوافر عنصريه العلم والإرادة والعلم ينصرف إلى العناصر المكونة للواقعة الإجرامية، فيجب أن يعلم الجاني بأن المال الذي اختلسه ونقل حيازته من مالكة أو حائزة دون رضاه ليدخله في حيازته هو أو تحت سيطرته، كما يجب أن يعلم أن المال ليس ملك له وأن تتجه إرادته إلى ارتكاب فعل الحيازة وتحقيق النتيجة الإجرامية[1] .

وعدم توافر عنصر الإرادة في الفعل ينفي القصد الجنائي، فمن يقوم بأخذ اسطوانة من صاحبها بدون علمه بمعرفة البرامج المسجلة عليها ثم يعيدها إلى صاحبها فلا يتوافر لديه نية الاختلاس والخطأ الذي ينصب على رضاء المجني عليه ينفي فعل العلم وينفي القصد الجنائي ،كمن يأخذ برنامج معتقدا أن صاحبه راضي عن ذلك فينتفي هنا عنصر العلم ومن يستولي على دعائم بها معلومات أودخل خطأ على برنامج بالرقم السري فإنه لا يعد مرتكب لجريمة السرقة[2].

ويذهب رأي إلى أن سحب العميل مبالغ تجاوز رصيده من جهاز التوزيع الآلي للنقود لا يعتبر سرقة، على أساس أن التسليم لأوراق النقد بواسطة جهاز التوزيع الآلي للنقود – الذي ينفذ أوامر المصرف – تعني أن البنك فتح له اعتمادا تلقائيا لمصلحة العميل لاعتقاده أنها ملكه فهو بذلك لا يتوافر لديه القصد الجنائي[3].

إن المجرم المعلوماتي مرتكب لجريمة سرقة المعلومات، يسعى بإرادته إلى الاستحواذ عليها بتشغيله للجهاز ويعلم أنها مملوكة لغيره وفي قيامة باختلاسها أو نسخها يعتبر قد توافر لديه عنصر القصد العام .كما وأن استخدم العميل للسحب من جهاز التوزيع الآلي للنقود لن يتم التغلب عليه إلا إذا تم الربط بين هذه الأجهزة وبين حسابات العملاء وفي هذه الحالة لن تقوم الأجهزة بصرف الوراق النقدية إلى العميل إلا في حدود الرصيد الذي يوجد في حسابه وقت السحب، وهوما جرى العمل عليه حاليا في نظام السحب من أجهزة التوزيع الآلي للنقود.

---

[1] سالم محمد سالم بني مصطفى، مرجع سابق، ص 67، مشار إليه لدى مأمون سلامة، قانون العقوبات، القسم الخاص، دار الفكر العربي، 1988، ص 25.

[2] سالم محمد سالم بني مصطفى، المرجع نفسه، ص 67.

[3] سالم محمد سالم بني مصطفى، المرجع نفسه، ص 67.

ثانيا: القصد الخاص

السرقة جريمة عمدية يفترض لقيامها توفر قصد جنائي خاص، وهو الذي يعبر عن نية التملك لأنها هي التي تكشف عن نية الجاني في حيازته للشيء المعلوماتي، ويستدل على توافر القصد من القرائن والظروف ونية التملك التي تتجه إليها إرادة الجاني، وهي عنصر آخر يضاف إلى عنصري القصد العام. فبالإضافة إلى ضرورة اتجاه إرادة الجاني إلى اختلاس شيء معلوماتي مع علم الجاني أنه يختلس شيئا مملوكا للغير يضاف إليه عنصر نية الاستحواذ على الشيء المسروق.

فجريمة السرقة المعلوماتية جريمة حديثة تبدأ من أول الدخول غير المشروع إلى النظام المعلوماتي و القصد فيها يتخذ صورتين الأولى تتمثل في حالة الدخول العام، وهو الذي يدخل فيه المستخدم للجهاز والحصول على المعلومات وهولا يمثل سرقة، أما الثانية والتي تتمثل في انتهاك للنظام المعلوماتي الخاص، والذي له كلمة سر ونظام أمني خاص يدل على وجود قصد وسوء النية من مرتكب الفعل. ويتوفر فيها القصد العام والخاص ويظهر القصد الخاص في فترة البقاء غير المشروع إلا أن المشكلة التي تعترض ذلك هي كيفية إثبات سوء النية[1].

وخـــلاصة لما سبق يمكن القول أن جل القوانين تقريبا لم تطلق مصطلح سرقة المعلومات على النشاطات غير القانونية السالفة الذكر التي تمارس على المعلومات المخزنة في النظام المعلوماتي[2]، ومنه ونخلص إلى أن عدم إشارة التشريعات إلى سرقة المعلومات وكأن بهذا إشارة إلى أن هذه التشريعات لا تعترف بسرقة المعلومات بل الوصول غير المصرح لها واختراقها وتقليدها والاستيلاء عليها ونسخها نسخا غير مشروعا.[3]

ومن خلال ماسبق يمكن أيضا أن نخلص لعدم وقوع السرقة، في الحالات السابقة لأن طبيعة البرامج والبيانات تأبى تحقيق الأخذ أو الاختلاس بمعناه الدقيق المسلم به في جريمة السرقة والذي يعني الاستيلاء على الحيازة الكاملة للشيء بدون رضا مالكه أو حائزه السابق، لأنه إذا تصورنا وقوع الاختلاس من خلال النسخ أو التصوير على المعلومات فإن هذه المعلومات الأصلية ذاتها تظل في نفس الوقت كما كانت من قبل تحت سيطرة صاحبها الأصلي ولا تخرج من حيازته، ولما كان قانون عقوبات الجزائري لا يجرم سرقة الاستعمال بصفة عامة، فإن المخرج الوحيد لا يكون إلا بتدخل صريح من المشرع لتفادي الجدل حول سرقة المعلومات الالكترونية ذلك لأن النصوص العقابية التقليدية للسرقة لا يمكن أن تنطبق على سرقة المعلومات السرية الالكترونية.

---

[1] أحمد خليفة ملط، مرجع سابق، ص 275.

[2] ليس كل التشريعات لان التشريع السويسري تناول سرقة المعلومات المبرمجة آليا في المادة 143 من قانون العقوبات لسنة 1995 فالمادة 143منه تم تعديلها لاحقا ومنه جرمت صراحة سرقة المعلومات.

[3] محمود أحمد عبابنة، مرجع سابق، ص 99.

وفي هذا الشأن أيضا نحن نقترح أن يستخدم المشرع الجزائري في حين تصديه للسرقة المعلوماتية بنص خاص بها أن يعبر عنها بمصطلح القرصنة هذا للتفرقة بين السرقة التقليدية وبين السرقة المعلوماتية.

ولنا وقفة أيضا في هذا الشأن تتعلق بقرصنة البرامج حيث أن أغلبية المشرعين يحمون البرامج حماية جزائية بموجب قوانين الملكية الأدبية والفكرية وتفاديا للتكرار فإن الحالات التي يجوز تطبيق تلك النصوص تطبق فيها عادي، بينما حالة عدم تطبيق النص لانعدام شرط مثلا من شروط تطبيق النص نطبق بشأنها نص القرصنة المعلوماتية باعتبارها معلومات الكترونية سرية، والأمر ذاته في حالة غياب نصوص حماية الحقوق الفكرية أوفي حالة عدم جدية تطبيق تلك النصوص إن وجدت.

فجريمة السرقة المعلوماتية جريمة قد تطال المعلومات و تتسبب عنها خسائر غالبا ما تكون مادية، بينما جريمة التجسس المعلوماتي جريمة ربما الأضرار فيها تكون معنوية أكثر منها مادية و منه سنحاول التفصيل فيها في المطلب الرابع.

المطلب الرابع
التجسس المعلوماتي

التجسس المعلوماتي هو جريمة ذات أصل تقليدي قديمة قدم البشر وقدم النزعات البشرية، جريمة نمت وازدهرت في عصر المعلومات واتخذت أبعادا جديدة وآفاقا أرحب مع تطور الحاسبات والشبكات ووسائل الاتصال. ويمكن أن نطلق عليها تسمية جريمة الاعتراض غير القانوني للبيانات وهي التسمية التي اعتمدتها اتفاقية بودابست، حيث أن التجسس الالكتروني هو الاعتراض غير القانوني للبيانات، ذلك أنه في عصر المعلوماتية وبفعل وجود تقنيات عالية التقدم تحولت الطرق التقليدية للتجسس من الطرق التقليدية للطرق الالكترونية.

فالتجسس من العمليات القديمة حيث كان الإنسان يتجسس على أعدائه لمعرفة أخبارهم والخطط التي يعدونها لمهاجمته، ولهذا كان للتجسس أهميته الكبيرة على كافة مستويات

النزاعات الإنسانية التي مر بها البشر منذ بدأ الخليقة، فتطورت عمليات التجسس طبقا لما يسود المجتمع من تطورات علمية وتكنولوجية[1].

حيث كان نتيجة الثورة المعلوماتية وانتشار شبكات الاتصالات وتزاوجها مع شبكات المعلوماتية وظهور شبكة الانترنت وأضحت المعلومات المخزنة على هذه الشبكات هدفا للمحتالين ومحترفي الأعمال التجسسية وذلك باستخدام التكنولوجيا المعلوماتية، حيث تمكن العديد من الجواسيس من اختراق العديد من أجهزة الحاسب والشبكات المؤمنة الخاصة بالدول والشركات والأفراد دون أن يغادروا أماكن وجودهم ودون أن يتركوا أي أثر يذكر[2] .

فكان نتيجة استخدام الشبكات المعلوماتية والإقليمية والعالمية والربط بينها عن طريق الخطوط التليفونية والقمر الصناعي والوسائل الحديثة أن العالم تحول إلى قرية صغيرة نتيجة ربط هذه الحاسبات بعضها بالبعض عن طريق شبكات الاتصال، وتدفق المعلومات بين أرجائه في مختلف صورها مما أدى إلى تقريب المسافات واختفاء الحواجز الجغرافية[3]. ومنه ازدهرت وتحولت وسائل التجسس والتصنت من الطرق التقليدية إلى الطرق الالكترونية وانتشارها عبر العالم[4]. فقد أدى الاستخدام المتزايد للحاسبات الآلية سواء في المجال العسكري أو الاقتصادي أوالسياسي أو الصناعي أو الإداري أو حتى الشخصي، إلى مركزية المعلومات بدرجة كبيرة في جميع الدول المستخدمة للنظام المعلوماتي وأدى تخزينها على هذا النحو إلى سهولة التجسس على تلك الأسرار[5]. فبظهور الحسابات بدأت مسألة الحصول على المعلومات أيا كان نوعها تأخذ بعدا بل أبعادا جديدة، حيث تطورت أساليب جمع هذه المعلومات " ولم تعد تقتصر على الجاسوسات الفاتنات اللواتي يقمن بإغواء قادة الأعداء لقد باتت هذه الأساليب تعتمد اعتمادا كبيرا على التكنولوجيا الرقمية".[6]

---

[1] - عياد رجا الخلايلة، مرجع سابق، ص 106.

[2] - محمد عبد الرحيم، مرجع سابق، ص 880.

[3] حيث تم كشف النقاب عن شبكة دولية ضخمة للتجسس الالكتروني تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كندا وبريطانيا واستراليا ونيوزلندا، عرفت باسم أشيلون لرصد المكالمات الهاتفية والرسائل بكافة أنواعها البرقية والتلكسية والالكترونية ، وخصص هذا النظام للتعامل مع الأهداف غير العسكرية وبطريقة تجعله يعترض كميات هائلة من الاتصالات والرسائل الالكترونية عشوائيا، باستخدام خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة، والتي تم إنشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية، منها محطة رصد الأقمار الصناعية الواقعة في منطقة واي هوباي بجنوب نيوزلاندا ومحطة الدتون الموجودة بأستراليا وغيرها. مشار إليه لدى يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الكتاب العربي، القاهرة، 2010، ص 161.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي الإسكندرية، 2009، ص 338.

[5] أيمن عبد الحفيظ، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، الناشر هو المؤلف ، 2003، ص 153-154.

[6] من أساليب التجسس الالكتروني استخدام الفيروسات للاختراق، كما يمكن أيضا الحصول على المعلومات السرية من خلال اختراق البريد الالكتروني للأشخاص للاطلاع على بياناتهم ومراسلاتهم ومخاطباتهم والاستفادة منها، للتفاصيل أكثر في طرق للتجسس الالكتروني، أنظر علي عدنان الفيل، الإجرام الالكتروني، مرجع سابق، ص 98.

وقد أضحت هذا الشبكات بنكا زاخرا بالمعلومات وأمام هذا الكم الهائل منها تضعف قبضة الأمن والتحكم والمراقبة، وتعد بيئة صالحة لعمليات التجسس خاصة على المعلومات الخاصة بالهيئات الحكومية والخاصة. وهذه المعلومات إذا ما تم التجسس عليها والحصول عليها قد يساء استخدامها سواء من قوى داخلية أوخارجية معادية للدولة التي جمع هذه المعلومات عنها[1].

إن ما تحققه شبكة الانترنت من خدمات كخدمة المحادثات الشخصية والبريد الالكتروني وغيرها سهل من انتهاك الأسرار المرسلة عبر الشبكة، وهو ما يعتبر تجسسا فالتصنت مثلا على المحادثات الشخصية عبر الانترنت قد تهتك أسرار خاصة عدة. والمسألة هنا تتضح معالمها يوما بعد يوم فلم يبقى اليوم شخص يجهل أنه معرض للتشهير والابتزاز وغيرها من السلوكات التي قد يتعرض لها صاحب معلومات سرية ،كالصور الشخصية والأسرار التجارية وصاحب الاتصالات الالكترونية وغيرها، إذا لم يتخذ احتياطات تأمين الحاسوب الفنية. فالكل اليوم يتهافت حول معرفة أساليب تأمين الحاسوب خاصة من يحمل الكاميرا وذلك كله خوفا من المحترفين في استخدام التقنية بطريقة سلبية.

ويؤكد الخبراء أنه بعد انتهاء الحرب الباردة وحرب الخليج الثانية في عام 1991 أن دول أوربا الغربية والولايات المتحدة قد قرروا وضع نظام من شأنه أن يوفر الرقابة المتواصلة والمستمرة لمناطق التوتر في العالم[2].

---

[1] حيث يقرر في هذا الشأن أحد الخبراء أنه " لم تعد القوة النارية التي تمتلكها الجيوش وحدها التي تقرر مصير الحروب ورجحان كفة الأطراف المتقاتلة وإنما المعلومات التي يملكها كل طرف حول الطرف الآخر هذه الحقيقة ثابتة منذ فجر التاريخ ولقد أتت التطورات السياسية والعسكرية خلال السنوات الخيرة لتؤكدها"، ويؤكد خبير آخر في هذا الصدد أن الحرب اليوم أصبحت "حربا كلية وهناك ثلاث خطوط رئيسية تدور حولها المعلومات: هناك المعلومات السياسية والمعلومات العسكرية والمعلومات الاقتصادية ولا يمكننا تمييز هذه المعلومات عن بعضها فكلها معلومات حيوية يجب أن تحصل عليها من البلاد المعادية قبل وأثناء القتال لتتضح لنا صورة عن قوة العدو " ، أشار إليه خالد ممدوح ابراهيم، مرجع سابق، ص 338.

[2] - حيث قاموا بتطوير جيل جديد من أقمار التجسس وتؤكد بعض المصادر أن ثلاثة أقمار من طراز " كيهول " موضوعة في مدار فضائي حاليا وتستطيع التقاط صور من الأرض لا تتجاوز قياساتها 15 سم أي ما يكفي للتمييز بين شاحنة ودبابة ، بالإضافة إلى انه توجد أقمار من طراز " لا كروس " تستعمل تقنية التصوير المعروفة بـ " رادار الفتحة التركية " ثبت موجات صفرية باتجاه الأرض ثم تلتقط انعكاساتها المرتدة إلى القمر ويمكن تحليل هذه الصور الرادارية بواسطة برامج كمبيوترية خاصة لتحويلها إلى صورة مفهومة والميزة الرئيسية لهذه التقنية هي أنها تسمح بتخطي الغيوم والمطار والغبار وأنها تصلح للاستعمال أثناء الليل. كما طورت الولايات المتحدة الأمريكية طائرات التجسس خاصة حين أصبح بالإمكان تحليقها بدون طيار وخاصة بعد حادثة سقوط إحدى طائراتها فوق الإتحاد السوفياتي " وأسر طيارها لمدة سنتين قبل أن يتم تبادله مع جاسوس سوفياتي كان مسجونا في الولايات المتحدة ."وكانت أولى الطائرات الأمريكية دون طيار هي tagoard وكانت تتم الملاحقة فيها بواسطة برنامج كمبيوتري حددت فيه مسارها الجوي ذهابا وإيابا وكانت الطائرات تقوم بتصوير المناطق وفي نهاية المهمة يتم إلقاء آلة التصوير والصور ونظام التوجيه في مكان محدد بواسطة مظلة ليلتقطها الفريق المشرف على العملية في حين يتم تدمير بقية الطائرة بصورة ذاتية إلا أن استخدام هذه الطائرات لم يحقق النجاح المطلوب الأمر الذي دفع الولايات المتحدة الأمريكية إلى صنع طائرات صغيرة واقتصادية دون طقم قيادة وذلك منذ العقد الثامن من هذا القرن وقد استخدمت إسرائيل هذه الطائرات أثناء عملياتها في لبنان عام 1982.وتعد طائرة " دارك ستار " من النماذج

أما على المستوى الداخلي فان الاضطراد في استخدام الحاسبات في تخزين وحفظ المعلومات الأمر الذي قد جعلها هدفا مغريا لمحترفي التجسس سواء كان ذلك في المجالات التجارية والصناعية والعسكرية والأبحاث العلمية خاصة المتعلقة فيها بأبحاث الطاقة النووية، الأمر الذي دعا إلى تشبيه هذه الحسابات بأنها خزائن بلا أبواب وأكد على أنه لو أدرك كبار المسؤولين الإداريين حقيقة المسؤولية والمخاطر المحتملة التي تهدد أصول الشركات وسمعتها لأغلقوا جميع شبكات ومراكز الحاسبات الآلية.

ولا يقتصر خطر اختراق الشبكات والأنظمة والمواقع والوصول إلى المعطيات الموجودة بها على العابثين من مخترقي الأنظمة أومن الهاكر أو منظمات عالم الانترنت السفلى التي تحاول دائما توجيه محاولات الاختراق نحو أنظمة وشبكات ومواقع في العالم أجمع[1]، فمخاطر هؤلاء خطيرة والأخطر منها هو عمليات التجسس التي تقوم بها الأجهزة الاستخباراتية للحصول على أسرار أو معلومات الدولة، وقد يكون ذلك لإفشائها لدولة أخرى تكون معادية لها، أو استغلالها بما يضر المصلحة الوطنية للدولة، لأن معظم الدول تحتفظ بوثائقها السرية مخزنة بهيئة رقمية في مزودات سرية[2].

الشديدة التعقيد وهي مصنوعة وفق هندسة الطائرات الخفية التي تنص الموجات الرادارية وبالتالي تحول دون أن تكتشفها الرادارات المعادية وتتم عملية الملاحة في هذه الطائرات بواسطة برنامج كمبيوتري خاص. واستخدمت الولايات المتحدة بخصوص إعادة إعمار أجزاء من دولة البوسنة طائرة تعمل دون طيار من طراز "بريدايتور" وهذه الطائرة تلتقط صورا رادارية حتى حجم 30 كم ولا تتأثر بالظروف المناخية مثل الغيوم والظلام كما أنها تعمل لمدة 24 ساعة بصورة متواصلة ، وفي أوائل شهر ماي 2006 أطلقت إسرائيل قمرا صناعيا للتجسس فوق مصر وإيران وسوريا ولبنان، وهو من الأقمار الصناعية المتطورة في التجسس مزود بنظام تصوير شديد الدقة يسمح بالتقاط صور بدرجة من الوضوح والمثير أنه ليس القمر الأول الذي تبعث به إسرائيل ولكنه ساعد من قدرة إسرائيل التجسسية على جيرانها، أنظر في ذلك عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، رسالة دكتوراه ، جامعة القاهرة، بدون سنة، ص 466-467.

[1] خالد ممدوح إبراهيم، مرجع سابق، ص 339.

[2] هنا سنطرح تساؤل حول هل سيتم تطبيق النصوص العقابية المتعلقة بجريمة التجسس الالكتروني على دولة تجسست الكترونيا على أفراد دولة أخرى، أوأن النصوص تعني فقط الأفراد؟.

الإجابة هنا حسب رأيي أنها تعني الأفراد فقط معنى ذلك أي فرد يقوم بالتجسس على شخص عام أو خاص،سواء داخل الدولة أو خارجها في حين أن النص لن يطبق على دولة متجسسة وإنما يمكن أن تطالب الدولة المعتدى عليها من الدولة المعتدية بتقديم اعتذار رسمي والتوقف عن تلك العمليات التجسسية. رغم أنه في الواقع أن العمليات التجسسية لن تتوقف أبدا، ونسجل في هذا الصدد على سبيل المثال تجسس المخابرات الأمريكية على الرؤساء الفرنسيين من بينهم الرئيس الحالي فرانس وهولند، حيث أن التجسس كان حتى على مكالماته الشخصية، وبعدما تحرت فرنسا على وثائق تؤكد دلك، اتصل الرئيس الفرنسي بنظيره الأمريكي ورد هدا الأخير بأنه سيتم توقيف تلك العمليات التجسسية على الرئيس، وطرحت عدة أسئلة فيما يتعلق بهذا الرد، حيث رأى البعض هل هذا يعني أنه يجوز التجسس على أفراد الشعب العاديين بينما الرئيس فلا؟.

ومن جهة أخرى نحن نعلم أن التجسس الالكتروني وارد بين الدول وبين الدولة نفسها على أفراد ينتمون إليها وآخرون لا وذلك حماية للأمن القومي، ولكن السؤال المطروح وهوهل المحادثات الخاصة ممكن أن تمس بالأمن القومي، قد تكون الإجابة نعم و يعتبر حينها التجسس الالكتروني حماية للأمن القومي حيث يكون حتى على المحادثات الخاصة ذلك عموما للسيطرة على زمام الأمور الأمنية خوفا من هاجس الإرهاب وعلى وجه الخصوص الالكتروني.

وهنا نشير أن جريمة الاعتراض غير القانوني للمعلومات أو التجسس المعلوماتي تختلف عن جريمة الدخول غير المصرح به للنظام المعلوماتي، ذلك لأن الاعتراض لا يتضمن تدخلا في نظام كمبيوتر معين ولكنه يتمثل في التلصص على المعلومات المرسلة بين جهازين أو أكثر وذلك في المسافة بينهما[1]. وللتدليل على ذلك هو أنه من أساليب[2] ارتكاب جريمة التجسس اختراق الأنظمة المعلوماتية وهو السلوك المادي الذي بواسطته تتم جريمة الدخول غير المصرح به للنظام المعلوماتي لكن في جريمة التجسس الهدف من الاختراق هو التصنت والتلصص على المعلومات[3]. والجدير بالذكر أن المشرع الفرنسي يعتبر جريمة التجسس المعلوماتي ضمن جريمة الدخول غير المصرح به للنظام المعلوماتي، و للتفصيل أكثر في سنتطرق لتعريف الجريمة ومجلاتها(فرع أول) و موقف التشريعات منه(فرع ثان)، إضافة إلى التطرق لأركان الجريمة (فرع ثالث)، وأخذ نموذج عن جريمة التجسس المعلوماتي(فرع رابع) عن طريق التطرق لحماية البريد الالكتروني و المحادثات الالكترونية.

الفرع الأول

تعريف التجسس و مجالاته.

التجسس لغة، مصدره حبس وحبس الخبر أي بحث عنه وفحص والجاسوس من يتجسس ليأتي بها [4] ويعرف سلوك التجسس اصطلاحا أنه فعل ايجابي قوامه الكشف واستظهار الحقائق المخفية، ولكنه استظهار غير مشروع إما بوسائله أو بغايته، وهو لذلك فعل لا يقره الشارع ويفرد لمرتكبه العقوبة الجزائية الرادعة دون تهاون [5]. والمقصود أيضا بالتجسس هوا لإطلاع على المعلومات الخاصة بالغير مؤمنة وليس مسموحا لغير المخولين بالإطلاع عليها[6].

إذن محل التجسس هو المعلومات الشفهية منها والمكتوبة، أيا كان نوعها إذا اتسمت بطابع السرية فالفاعل يسعى لكشف الأسرار أو معناها أوجهتها أو صاحبها أو قيمتها. المهم

---

[1] شيماء عبد الغني محمد عطا الله، مرجع سابق، ص 104.

[2] أساليب ارتكاب الجريمة هناك من يستخدم بشأنها مصطلح صور ارتكاب الجريمة وهو أمر غير صحيح حيث أن هناك فرق بينهما حيث أننا من البداية قد اعتبرنا الاختراق أسلوب من أساليب ارتكاب الجريمة المعلوماتية والجرائم ضد الأسرار المعلوماتية هي جرائم معلوماتية، ونفس الشيء بالنسبة لتسمية الدخول غير المصرح به للنظام المعلوماتي هناك من يسميها جريمة الاختراق ونحن من جهتنا نرفض هذه التسمية.

[3] كذلك من أساليب ارتكاب جريمة التجسس استخدام الأبواب الخلفية أو الخفية واعتراض الاتصالات التي تبث من المحطات الأرضية، أنظر في ذلك أيمن عبد الحفيظ، مرجع سابق، ص 156.

[4]- جابر يوسف المراغي، جرائم انتهاك أسرار الدفاع عن البلاد، دار النهضة العربية، 1998، ص 93.

[5] - جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة ، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن ، 2010، ص 258.

[6] - محمد عبد الرحيم، مرجع سابق، ص 880.

أن تتمتع تلك المعلومات بخاصية الإخفاء ومشتملات المعنى الواضح للسر، والذي لا يجوز الإطلاع عليه إلا من قبل فئة محددة محصورة، وضمن قواعد تضمن حماية تلك السرية[1].

فالتجسس المعلوماتي لا يشمل فقط الجانب العسكري فهو متعدد بتعدد المجالات وأوجه النشاطات المختلفة، حيث يمكننا القول بصفة عامة أن التجسس المعلوماتي أصبح يشمل الجوانب الصناعية والتقنية والتجارية للمؤسسات الاقتصادية كما يشمل الجوانب المتعلقة بالجانب العسكري والأمني للدولة[2] ،كما يشمل الحياة الخاصة للأفراد فعلى سبيل المثال نجد أنه في مجالات النشاط التجاري، ترتكز عمليات التجسس المعلوماتي على كشف الأسرار التسويقية والتجارة(كحسابات التكلفة،كشوف الميزانية،حالة الأسواق وعناوين لعملاء...وغيرها). وفي مجالات النشاط الصناعي والتقني، تسعى عمليات التجسس بصورة كبيرة إلى (كشف نتائج الأبحاث والتطوير، والبيانات المتعلقة بعمليات الإنتاج، وأسرار تصميمات المنتجات ولاسيما تصميمات الشرائح الصغيرة من أشباه المواصلات)، وفي المجالات الأمنية والعسكرية الاستخباراتية والنووية، تكشف نشاطات التجسس جل جهودها نحو اختراق النظم الأمنية والعسكرية الاستخباراتية والنووية للوصول إلى أدق تفاصيل أسرار البيانات والمعلومات المتعلقة بتلك الشؤون، بما يكون له من بالغ الأثر على أمن وبقاء الدول والحكومات[3].

للتجسس المعلوماتي أيضا في مختلف المجالات أبعاد خطيرة غير مسبوقة، فالتكثيف لمراكز المعلومات في ذاكرات الحاسبات الآلية يجعلها هدفا مغريا لأي متلصص يملك خبرة كافية وتجهيزات جيدة،لاسيما مع إمكانية الاستعانة بالحاسبات الآلية في فرز المعلومات المخزنة وتصنيفها ونسخها بسهولة وسرعة فائقة، دون أن يخلف ذلك أي أثر[4]، وللإحاطة بمجالات التجسس كان لابد من التطرق إلى بعض صور التجسس كالتالي:

أولا: التجسس العسكري

نجد أن أشهر أنواع التجسس هو التجسس العسكري وهو يهدف لمعرفة أسرار الدول الأخرى المتعلقة بالجيوش والخطط الحربية والأسلحة والمواقع والعدة العسكرية والمشروعات النووية وصناعة الأسلحة، كل هذه المعلومات الحساسة والسرية هي كذلك في أي دولة، ورغم سريتها وحساسيتها فإنها في ظل الثورة المعلوماتية يتم تخزينها في ذاكرة الحاسوب ومعالجتها آليا أو وضعها على قرص مغناطيسي سهل الحمل. فالمؤسسات

[1] - جلال محمد الزغبي، أسامة أحمد المناعسة، مرجع سابق، 258.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان الأردن، الطبعة الثانية، 2010، ص 209.

[3] محمد عبد الله أبو بكر سلامة، مرجع سابق،ص 147.

[4] محمد عبد الله أبو بكر سلامة ،المرجع نفسه، ص 147.

العسكرية من أهم مؤسسات الدولة وأكثرها استخداما للمعلوماتية، وبالتالي فهي كانت ولا تزال منشطا مهما ومجالا خصبا لمحاولات التجسس والاختراق[1]، ويمكن في ظل هذا الوضع للمخترقين أن يقوموا باستخدام الوسائل التقنية خلال فترة زمنية قصيرة من أي مكان في العالم بالوصول إلى هذه المعلومات[2].

فالتجسس العسكري[3]من أول أنواع التجسس وأقواها، فكل دولة تسعى للحصول على المعلومات العسكرية الضرورية عن الدول المعادية والصديقة على حد سواء. والتجسس العسكري أو الحربي يهدف إلى معرفة أسرار الدول الأخرى المتعلقة بالجيوش والأجهزة العسكرية والخطط الحربية والأسلحة والصواريخ والذخائر والقنابل الذرية والتجهيزات والمواقع والعديد والعدة العسكرية، وقد أعطت العديد من الدول التجسس العسكري رعاية مميزة من خلال رصد الأموال، وإنشاء دوائر ومكاتب مختصة بشؤون التجسس، وتدريب الجواسيس، وتنظيم شبكات التجسس بصورة علمية دقيقة. ولا يقتصر التجسس العسكري على زمن الحرب بل ينشط أيضاً في زمن السلم تحسباً للحرب وتوخياً لتحقيق المخططات العسكرية، وقد قال أحد العلماء إن الحروب هي من صنع الجواسيس والجواسيس المضادين[4].

وتبدو خطورة وحساسية المعلومات العسكرية والأمنية للدولة إذا علمنا أن البنتاغون يقوم بتغيير أنظمة الترميز السرية لبياناته ولمعلوماته الحساسة يوميا، كما أنه ينفق على أحد برامجه 200 مليون دولار كل سنة ويقوم هدا البرنامج بإلغاء وكتم الإشارات الصادرة من الآلات المستخدمة بواسطة العسكريين ووكالات الأمن ومتعهدي الدفاع[5].

ثانيا: التجسس الاقتصادي

لم تعد الحروب تقتصر على النواحي العسكرية بل تخطتها إلى الشؤون الاقتصادية، ويهدف التجسس الاقتصادي إلى الوقوف على المقدرات الإقتصادية للدول الأخرى العدوة والصديقة،

[1] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت ، مرجع سابق، ص 378.

[2] نهلا عبد القادر المومني، مرجع سابق، ص 212.

[3] مثلا نجح الألماني ماركوس هيس البالغ من العمر 24 سنة في التغلغل بطريق الاتصال البعدي في منظومات 30 حاسب بالولايات المتحدة الأمريكية تتعامل في معلومات عسكرية، والحصول منها على معلومات لها هذه الصفة، فضلا عن بيانات تتعلق بأبحاث علمية، أنظر في ذلك هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة بأسيوط، 1992، ص 138.

[4]- http://www.lebarmy.gov.lb/ar/news/?5302#.Ui4gvD_4xkg يوم 2015/05/10.

[5] نهلا عبد القادر المومني، مرجع سابق، ص 212.

لمعرفة مواردها وثرواتها ووضعها المالي والنقدي ومستوى تجارتها وصناعتها وزراعتها وطرق استثمارها وتحويلها[1].

ومما لا شك فيه أن الاقتصاد من يعتبر من العوامل الرئيسية في سيادة مختلف الدول وأمنها وتهدف أعمال التجسس على المعلومات التجارية والصناعية والمالية إلى معرفة الثغرات الاقتصادية في دولة ما ومواطن الضعف في هيكلها الاقتصادي، وكذلك يهدف إلى التفوق اقتصاديا على تلك الدولة كما أن التجسس المعلوماتي قد يتم على المستوى الداخلي بين المؤسسات المختلفة في ذات الدولة[2].

ومع توسع التجارة الالكترونية تحولت العديد من مصادر المعلومات إلى أهداف للتجسس التجاري ففي تقرير صادر عن وزارة التجارة والصناعة البريطانية أشار إلى زيادة نسبة التجسس على الشركات من 36 بالمئة عام 1994 إلى 54 بالمئة عام 1999[3].

عرفت التوصية الصادرة عن المجلس الأوروبي الخاصة بجرائم الحاسوب المعلومات الصناعية والتجارية السرية أنها:" مجموعة من مجموعة من الحقائق لها قيمة معلوماتية ولها صلة بشخص أو بمؤسسة محددة وتتميز هده الحقائق بكونها سرية، أي غير معلومة للجميع، وأن الدخول إلى الأنظمة التي تحتوي عليها مقصور على دائرة محددة من الأشخاص، وتظل هده السرية رهنا بإرادة الشخص المسؤول عن المؤسسة[4].

فيرجع السر في تفوق شركة كوكا كولا الأمريكية في مواجهة الشركات المنافسة في مجالها إلى نجاح هذه الشركة في المحافظة على سر الوصفة الخاصة بالمادة التي تستخدم في صناعة مشروب كوكا كولا منذ مدة تزيد على قرن من الزمان حتى الآن، حيث أن سر الوصفة محفوظ في بنك معلومات في ولاية أتلانطا ومحظور الإطلاع عليه إلا بقرار من مجلس إدارة شركة كوكا كولا وهو غير معروف إلا لعدد من كبار العاملين في الشركة[5].

ثالثا: التجسس السياسي والدبلوماسي

[1] تمكن أشخاص أحداث في الثالثة عشر من عمرهم من الوصول إلى منظومات حاسب مركزي وشبكة معلومات محمية من الاختراق، وذلك في كندا بإحدى شركات الإسمنت بمونتريال ، حيث لوحظ أن مجهولا سنة 1985 قد تمكن من الوصول إلى بيانات الشركة المخزنة ببنك المعلومات عن طريق الاتصال عن بعد، وعن طريق التحقيقات التي تناولتها الشرطة الكندية بالتنسيق مع مكتب التحقيقات الفدرالي الأمريكي من تتبع مركز الاتصال الهاتفي حتى تبين أن مصدره أجهزة تليفون بإحدى المدارس بمدينة نيويورك، عن هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 134 .كذلك شركة أمريكية للبترول عانت الفشل في مناقصاتها واستمر هذا الوضع لعدة أشهر حيث كانت العقود تبرم لصالح شركة منافسة كانت تقدم أسعار تقل ببضع دولارات عن الشركة الأولى، ثم تبين بعد ذلك أن هناك توصيلات سرية على الحاسب الآلي الخاص بها تسمح للشركة المنافسة بالتعرف على أسعار العروض المقدمة، أنظر في ذلك عمر أبوالفتوح عبد العظيم الحمامي، مرجع سابق، ص 468.

[2] نهلا عبد القادر المومني، المرجع نفسه ، ص 213.

[3] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنت، مرجع سابق، ص 379.

[4] نهلا عبد القادر المومني، المرجع نفسه، 214.

[5] رشدي محمد علي محمد عيد، مرجع سابق، ص 293-294.

لا يقل التجسس السياسي خطورة عن أنواع التجسس الأخرى، وهو يرمي إلى مراقبة أوضاع وأسرار سياسات الدول الأخرى، إن على الصعيد الداخلي أو على الصعيد الخارجي. ويتم التجسس السياسي من خلال رصد تحركات ونشاطات ومواقف القادة والزعماء والحكام والأحزاب والمنظمات السياسية والأمنية. وهو يهدف إلى التحكم في سيادة الدول واتجاهاتها، أو إلى اغتيال بعض السياسيين أو إلى زرع بذور الفتنة، أو تحطيم الأنظمة السياسية المعادية.

أما عن التجسس الدبلوماسي فهو التجسس الذي يمارسه أفراد البعثات الدبلوماسية، ويتمثل في جمع المعلومات بطريقة غير قانونية من دون أن يخفي القائمون به صفتهم الدبلوماسية، مما يميزه عن صور التجسس الأخرى ويصنف ضمن التجسس زمن السلم. ويزخر تاريخ العلاقات بين الدول بالمشاكل والنزاعات الناجمة عن التجسس الدبلوماسي.[1]

رابعا:التجسس الشخصي والعلمي

تعد جريمة التجسس من أخطر جرائم الهجوم على خصوصية الأفراد وبشكل صارخ حيث يتم والتصنت عليهم ومراقبة شؤونهم الخاصة في الفضاء المعلوماتي وأصبح هذا الاعتداء يتزايد وبشكل ملفت للنظر مما شكل خطرا محدقا على خصوصية الإنسان.

ويمثل وعاء أسرار الأفراد كيانين هما الكيان الداخلي للإنسان والكيان الخارجي، فأما عن الداخلي فيشمل جسمه والحالة النفسية والعقلية، الصورة ونشير هنا أنه يشترط فيها أن يكون الإنسان يمارس حياته الخاصة وتم التقاطها بآلة معينة إذ إذا كان في مكان عام له الحق في صورته وليس له الحق في أسرارها[2]، بينما عن الكيان الخارجي فيمكن تلخيصه في مسكن الإنسان، الذمة المالية المحادثات الشخصية، المراسلات[3].

وبمناسبة المراسلات وبما أنها أهم وسائل الاتصال حاليا وذلك مع ما تشهده الحياة من تطورات في هذا المجال، كذلك لما تحمله من أسرار إذ تعتبر مجالا هاما لإيداع أسرار الأفراد وفي معنى المراسلة أجمعت التشريعات على اعتبارها إما خطابا أو برقية أو على شكل تلكس أو شكل استحدثته التكنولوجيا ، وسنأخذ على سبيل المثال البريد الالكتروني لما له من أهمية ولاتساع مجالات استخدامه في عصر المعلوماتية، وللإشارة سنتناول في هدا الجزء من البحث حماية مضمون الرسالة الالكترونية من الانتهاك .

---

[1] .http://www.lebarmy.gov يوم الاطلاع على الموقع 2015/07/24.

[2] طارق أحمد فتحي سرور، الحماية الجنائية لأسرار الأفراد في مواجهة النشر، دار النهضة العربية القاهرة، 1991 ، ص 47.

[3] طارق أحمد فتحي سرور، المرجع نفسه، ص 48-51.

أما عن التجسس العلمي فتمارس الدول خصوصاً الدول العظمى التجسس العلمي بهدف الإطلاع على الأسرار العلمية وسرقتها، أو بهدف اتخاذ الاحتياطات اللازمة لمواجهتها، ويهتم التجسس العلمي بالكشف عن الأبحاث والدراسات والاختراعات العلمية وغيرها.

الفرع الثاني

موقف التشريعات من جريمة التجسس المعلوماتي

اختلفت التشريعات في تسمية هذا النوع من السلوكات المجرمة، فكما سبق الذكر هناك من يطلق عليها اسم الاعتراض غير القانوني للبيانات وهي التسمية الغالبة، بينما ربما لابد من تسميتها بالتجسس المعلوماتي لأن الاعتراض غير القانوني هو الفعل المادي لارتكاب الجريمة ولابد من توافر الركن المعنوي والشرعي لاكتمال عناصر جريمة التجسس المعلوماتي.

نصت على هذه الجريمة المادة 3 من اتفاقية بودابست بقولها" يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا لقانونه الداخلي واقعة الاعتراض العمدي وبدون حق، من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب في مكان الوصول في المنشأة أوفي داخل النظام المعلوماتي، بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية أو ترتكب الجريمة في حاسب إلى يكون متصلا عن بعد بحاسب آخر".

والهدف من النص على هذه الجريمة في سياق المادة 3 من اتفاقية بودابست ،كما هو مبين هو حماية الحق في حرية الاتصالات واحترام نقل البيانات دون التدخل من أطراف أخرى، وفي الحديث عن المكالمات التيليفونية التقليدية أو المراسلات البريدية أو عبر الانترنت أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب الآلي وصولا إلى البيانات ذلك يكون بالنقل أو التسجيل باستعمال أي من الأجهزة الفنية للإرسال غير العلني للمحادثات أو البيانات أو الملفات أو المراسلات ، وسواء أكانت البيانات متداولة عبر الأجهزة الداخلية لنفس الحاسب أو عن طريق الاتصال عن بعد باستخدام حاسب آخر ،كذلك الذي يحدث عبر الشبكات المختلفة. كما ينطبق هذا الوصف الإجرامي على كل أشكال النقل الالكتروني للبيانات سواء تم عن طريق التليفون أوالفاكس أو البريد الالكتروني[1].

كذلك الشأن في المادة 7 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 حيث اعتبرت الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية

[1] بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية، 2008، ص 305.

وقطع بث أو استقبال بيانات تقنية المعلومات من قبيل التجريم، إضافة إلى أن المادة 5 من ذات الاتفاقية تلزم كل دولة من الدول الأطراف بتجريم الأفعال التي تم تجريمها وفقا للاتفاقية، وذلك وفقا لتشريعاتها وأنظمتها الداخلية. وبالنسبة لتجريم السلوك من قبل المشرع الجزائري فإننا لم نلمس نصا صريحا بخصوص الاعتراض غير القانوني للمعلومات الالكترونية رغم مصادقته على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب المرسوم الرئاسي 14-252 السالف الذكر، وفي نفس الوقت لقد تم تجريم التعامل في معطيات تم الحصول عليها بطريق الاعتراض من خلال نص المادة 394 مكرر 2 من قانون العقوبات، أي أنه جرم التعامل فيها ولكنه لم يجرم إعاقة أو اعتراض طريق نظام المعلومات أوالمعطيات المرسلة عن طريق نظام المعلوماتية بصفة مباشرة ولا صريحة.

ولربما لأول وهلة يمكن اعتقاد أن المشرع الجزائري قد جرم اعتراض المعطيات المرسلة عن طريق منظومة معلوماتية والاتجار فيها بموجب المادة 394 مكرر 2 ، ولكنه حتى بمفهوم المخالفة من خلال النص فإنه لا يشير إلى ذلك، وما يلاحظ على المشرع الجزائري أنه لم يجرم بشكل مباشر وبنص خاص الأفعال التي قد يرتكبها المجرم المعلوماتي باعتراضه طريق المراسلات الالكترونية أو المعلومات المرسلة عن طريق الأنظمة المعلوماتية وإعادة سيرها.

في حين أن مشرعين آخرين جرموها حيث تصدوا لها بنصوص التجريم الخاصة بها، وذلك لما قد تحمله تلك المعلومات من أسرار وخصوصيات لا يجوز الاطلاع عليها.

والملاحظ على النصوص السابقة أنها جرمت الاعتراض غير القانوني للمعلومات ولم تصطلح على السلوك بالتجسس في حين أنه من الأصح أن يصطلح على هذه الجريمة بالتجسس المعلوماتي، لأن من يؤمن أن الهدف من الاعتراض هو التصنت والتلصص على المعلومات والرغبة في الحصول عليها دافعه هو التجسس، أكيد أنه سيعتبر الاعتراض غير القانوني للمعلومات هو الركن المادي للجريمة الأصلية والتي هي التجسس، ومادام هو يرتكب في بيئة رقمية إذن هو تجسس معلوماتي.

ورجوعا للمشرع الجزائري و من خلال قانون العقوبات الذي جرم التجسس وبأي وسيلة كانت، معناه قد تكون وسيلة الكترونية وذلك وفقا للمادة 63 في الفقرة الثانية منه حيث نصت أن" الاستحواذ بأي وسيلة على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى حد عملائها". فمن خلال المادة نستطيع القول أن المشرع الجزائري جرم التجسس الالكتروني ولكن العسكري فقط.

ومن خلال ما سبق ومن خلال استقراء النصوص العقابية المتعلقة بالتجسس كما هو الأمر في نص المادة 61 وما بعدها من قانون العقوبات الجزائري نستنتج أن التجسس كان

منحصرا في المجال العسكري[1] وخيانة أفراد لدولة لصالح دولة أخرى، وهو ذات الأمر المستنتج من التعريف الخاص بالجاسوس السابق الذكر في أصناف المجرم المعلوماتي. ولكن تجدر الإشارة إلى أن التجسس بمفهومه التقليدي، صحيح قد ينحصر في المعلومات التي يتجسس عليها الفرد لصالح دولة أخرى والأمر مقبول إذا ما حصرناه فيما يسمى بالتجسس العسكري، في حين أن الأمر غير مقبول أن نحصر التجسس المعلوماتي في المعلومات العسكرية فقط، ذلك لأن الاعتراض غير القانوني للبيانات المعالجة آليا والوارد فعلا قد تكون محله المعلومات العسكرية، المعلومات التجارية والمعلومات الشخصية وغيرها.

إذن لابد على المشرع الجزائري التصدي لهذا السلوك بنص خاص تماشيا مع نص المادة الثالثة من اتفاقية بودابست، والمادة السابعة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 ، والأمر ذاته بالنسبة للمشرع الفرنسي والأردني وغيرهم، إلا أن هناك البعض من الدول من جرمت التجسس المعلوماتي بنص خاص[2].

والجدير بالذكر أنه من خلال استقراء القانون الفرنسي نستنتج أن المشرع الفرنسي لم يشر إلى جريمة التجسس المعلوماتي، حيث جرم الدخول والبقاء غير المصرح بها للنظام المعلوماتي سواء كان لمجرد الدخول أو القصد منه التجسس.

الفرع الثالث
أركان جريمة التجسس المعلوماتي

في الحقيقة طيلة عمر هذه الدراسة تم استخدام مصطلح المعلوماتية بدلا عن الالكترونية، بينما فيما يتعلق بأركان التجسس المعلوماتي نفضل لو أننا اعتبرنا التجسس يكون الكترونيا أدق من أن يكون التجسس معلوماتيا ذلك أنه سيتم اعتراض المعلومات الكترونيا.

أولا-الركن المادي:

[1] هذا الموقف ليس فقط بالنسبة للمشرع الجزائري وحيث أننا نؤمن أن التجسس المعلوماتي طال كل المعلومات السرية بمختلف أنواعها وأشكالها، ومنه إنه يقع على عاتق المشرع الجزائري التعديل.

[2] - نذكر على سبيل المثال المادة 370/ب من قانون العقوبات اليوناني[2]،المادة السابعة (7) والثامنة (8) من القانون البرتغالي رقم 109 لعام 1991 الخاص بجرائم المعلوماتية[2] والفقرة (أ/4) من المادة (31) من القانون السوري ذي الرقم (4) بتاريخ 2009/2/25 الخاص بالتوقيع الالكتروني وخدمات الشبكة وإن اختلف مجال تطبيقها، إذ تنص الفقرة (أ/4) من المادة (31) على انه " التوصل بأي وسيلة كانت إلى الحصول بغير حق على بيانات إنشاء توقيع الكتروني أو منظومة إنشاء توقيع الكتروني أو وثيقة الكترونية، أو اختراق أي منها، أو اعتراضها أو تعطيلها عن أداء وظيفتها "، فكما هو ملاحظ فإن المشرع السوري قد استخدم مصطلح الاعتراض إلى جانب اختراق بيانات إنشاء التوقيع الالكتروني أو الوثيقة الالكترونية ، وان كان كلا المصطلحين ما هما إلا نموذج من نماذج الدخول بغش لنظام المعالجة الآلية ، عن رشيدة بوكر، المرجع نفسه، ص 209.

يتمثل الركن المادي في هذه الجريمة في فعل الاعتراض، الذي يجب يقوم به الجاني في الجريمة بدون حق وباستخدام وسائل فنية غير علنية. ولهذا فإنه لابد أن يتوافر في الركن المادي في جريمة الاعتراض شروط معينة لقيامه وبالتالي لوجود هذه الجريمة وفقا للمادة الثالثة من اتفاقية بودابست مع الإشارة إلى أنه يمكن للدول الأطراف في الاتفاقية إضافة شروط أخرى خلال تناولهم لجريمة الاعتراض غير القانوني للبيانات في قوانينهم الجنائية الداخلية أوفي قوانين أخرى تعتبر هذا الفعل جريمة. حيث أن الاتفاقيات السالفة الذكر في تناولها لهذا الفعل قد وضعت الإطار العام الذي تستطيع الدول الأعضاء أن تتحرك من خلاله بحرية في وضع وتحديد أركان وشروط هذه الجريمة وما يتلائم مع كيانها الداخلي.

آ- المقصود بالاعتراض:

ويقصد بالاعتراض في إطار نص المادة الثالثة من الاتفاقية الدولية بشأن حماية المعلومات أنه " التصنت أو نقل البيانات التي تتم داخل جهاز الحاسب أو التي تتم عبر جهازين عن بعد عبر الشبكات المعلوماتية المختلفة أو بترجمة الانبعاثات الكهرومغناطيسية الصادرة من الحاسب إلى البيانات أو التي تتم عبر الأجهزة اللاسلكية وذلك عن طريق أي من الوسائل الفنية غير العلنية"[1].

ومن هذا التعريف يتضح أن نص المادة الثالثة يشمل وسائل الاتصالات التقليدية بالإضافة إلى وسائل الاتصالات الحديثة في إطار المعالجة الآلية للبيانات. ففعل الاعتراض غير القانوني كما يشمل التصنت ونقل وتسجيل المحادثات التليفونية بين الأشخاص يمتد ليشمل علاوة على ذلك كل أشكال النقل التي تتم من خلال التعامل مع الأجهزة الآلية لمعالجة للبيانات مثل نقل البيانات والملفات الذي يتم داخل الحاسب الآلي نفسه أوطريق نقل البيانات التي تتم عبر الاتصالات والمراسلات البريدية الالكترونية من خلال الشبكات المعلوماتية، أوالتي تكون عبر الاتصالات اللاسلكية المتطورة التي نعرفها في العصر الحاضر كالفاكس أو طريق قيام الجاني في هذه الجريمة باستعمال أجهزة معدة للاستقبال الانبعاثات المختلفة الكهرومغناطيسية التي تنبعث من أجهزة الحاسب الآلي ثم فك رموزها وشفراته لتحويلها إلى البيانات التي يرغب في نقلها أو تسجيلها أو التصنت عليها لتحقيق غايته الإجرامية[2].

وعن تجريم هذا السلوك لم يشترط نوعية معينة من البيانات أو المعلومات فقد تكون معلومات تخص الدولة أمنية أو سياسية أو اقتصادية ، وقد تكون معلومات أو بيانات خاصة بأحد الأشخاص الطبيعيين أو المعنويين، فالنص لم يضع شروطا تتعلق بطبيعة البيانات والمعلومات محل الاعتراض (التجسس)، ولم يشترط تبعيتها لجهة معينة وإنما جاء النص عاما ليشمل كافة أنواع المعلومات والبيانات سواء أكانت تابعة لجهة حكومية أو خاصة .

[1] بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات في التشريع المقارن والشريعة الإسلامية، دار الفكر الجامعي الإسكندرية، بدون طبعة، 2008.ص 306.

[2] بلال أمين زين الدين، مرجع سابق، ص 307.

وتقع هذه الجريمة من أي إنسان أيا كانت صفته، سواء كان يعمل في مجال الأنظمة الحاسوبية أم لا علاقة له بذلك بيد أنه يجب أن لا يكون الجاني أو الفاعل من أولئك المصرح لهم بالحصول على تلك المعلومات ، لأن في هذه الحالة تنتفي صفة غير المشروعية، كذلك وكما يتضح من سياق النص السابق أنه جرّم اعتراض (التجسس) المعلومات أو البيانات بغض النظر عن كونها تتمتع بحماية النظم الأمنية من عدمه[1].

هذا ولم يتطرق المشرع الجزائري إلى تحديد المقصود بهذا السلوك شأنه شأن أغلب التشريعات المقارنة في حين نجد أن بعض الفقه قد تصدى إلى هذه المهمة.

وفي ذلك نجد أن البعض قد عرفه[2]على أنه: " قيام الجاني بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي" أو أنه:"رصد إشارات إلكترومغناطسية في الأنظمة المعلوماتية أو تحليلها بغية استخراج المعلومات المفهومة أو المقروءة منها"[3].

وفي الفقرة (و) من المادة الثانية من الفصل الأول من القانون رقم (04-09) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أورد المشرع الجزائري تعريفا للاتصالات الالكترونية على أنها أي " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[4].

والملاحظ على نص هذه المادة، أن المشرع قد توسع في تحديد مفهوم الاتصالات الالكترونية ليشمل وسائل نقل المعلومات فضلا عن الموجات المنبعثة أثناء انتقالها. فباستخدامه مصطلح "الوسائل الالكترونية " إنما أراد وسائل نقلها، وباستخدامه مصطلح"علامات أو إشارات"إنما أراد انبعاثات الإشعاعات الكهرومغناطيسية أوالضوئية أو الرقمية أو غيرها المنبعثة أثناء انتقال المعلومات.

---

[1] حسين بن سعيد بن سيف الغافري، جريمة الاعتراض، عن الموقع الالكتروني http://www.omanlegal.net/ يوم 20 سبتمبر 2016.

[2] - يونس عرب، البنوك الخلوية، التجارة الخلوية ، المعطيات الخلوية، ثورة جديدة تبئ بانطلاق عصر ما بعد المعلومات، عن الموقع الالكتروني:

http:// www.arablaw.org/download/m-banking-article.doc.

[3] - وليد الزيدي، المرجع السابق، ص 51.

[4] - هذا ولم يحدد المشرع الجزائري من جانبه ما الذي يقوم بتغطيته مصطلح " الوسائل الإلكترونية " ، وفي ذلك عرف المشرع السوري الوسائل الإلكترونية بموجب المادة الأولى من الفصل الأول من القانون رقم (4) الخاص بالتوقيع الالكتروني وخدمات الشبكة على أنها "وسائل الكترونية أو كهربائية أو مغنطيسية أو كهرطيسية أو ضوئية أو رقمية أو أي وسائل مشابهة تستخدم في تبادل البيانات أو المعلومات أو معالجتها أو حفظها أوتخزينها "، عن رشيدة بوكر مرجع سابق،ص 206.

والاتصال على شكل نقل المعلومات يمكن أن يحدث داخل نظام معالجة آلية واحد كما في حالة الدورة بين وحدة المعالجة المركزية والشاشة أو الطابعة، أو بين نظامين لنفس المالك أو بين نظامين متصلين ببعضهم البعض عبر الشبكات المعلوماتية كما هو الشأن في البريد الالكتروني، أو بين نظام وشخص، كما هو الحال في حالة تعامل الشخص مع لوحة المفاتيح.

ومما تجدر الإشارة إليه في هذا المقام أن نظام المعالجة الآلية- كما سبق ورأينا – يغطي أيضا الاتصالات اللاسلكية بما في ذلك شبكة wi-fi ، إذ أنها تحدث على نحو مفتوح يمكن الوصول إليه ولذلك من السهل اعتراضها.

بل إن المذكرة التفسيرية لاتفاقية بودابست قد توسعت في ذلك لتشمل كافة أنواع النقل الالكتروني للمعلومات سواء التقليدية منها أو المستحدثة، إذ جاء فيها "... والجريمة المنصوص عليها في المادة الثالثة تطبق هذا المبدأ على كل أشكال النقل الالكتروني للبيانات سواء تم هذا النقل عن طريق التلفون أوالفاكس أو البريد الالكتروني أو نقل الملفات..."[1].

فبذكرها " تلفون أو فاكس " إنما هي إشارة إلى وسائل الاتصال التقليدية، وبذكرها "البريد الالكتروني أونقل الملفات " إنما هي إشارة إلى وسائل الاتصال الحديثة.

والاعتراض بهاذ المعنى يتم باستخدام وسائل فنية يمكن أن تؤدي إلى اعتراض كافة أشكال النقل الالكتروني للمعلومات، ومن ذلك الوسائل التي تتعلق بالتحكم أو المراقبة محتوى الاتصالات وللحصول على المحتوى بطريقة مباشرة من خلال طريقة الولوج إلى داخل نظام المعالجة الآلية واستخدامه، أو بشكل غير مباشر عن طريق استخدام أجهزة التنصت كذلك تسجيل المعلومات، ليس هذا فحسب بل إن مدلول الوسائل الفنية يمكن أن يمتد ليشمل الأجهزة الفنية المتصلة بخطوط النقل أو الاتصال مثل أجهزة تجميع وتسجيل الاتصالات اللاسلكية، كذلك المكونات غير المادية ككلمات المرور والشفرات.

فظلا عن ذلك استخدام الموجات الكهربائية المنبعثة عن نظم المعالجة الآلية، إذ تعد هذه الأخيرة الوسيلة الأساسية لاعتراض نظام المعالجة الآلية، وهي بذلك تعد من أهم التقنيات المستخدمة في التجسس المعلوماتي[2].

---

[1] - هلالي عبد الله أحمد، الجوانب الموضوعية والإجرامية لجرائم المعلوماتية ، مرجع سابق، ص 78.

[2] - يقول (دولف هيغل) رئيس إدارة شرطة الجرائم الخطيرة في أوربا (بالنسبة لجرائم الحاسوب والانترنت) " يبدوأننا خسرنا المعركة قبل أن نبدأ القنال... إذ أننا لا نستطيع مجاراتها فالحواسيب وما يرتبط بها من شبكات تبدومثل بوابة بلا حارس، بل كساحة الإجرام تتحدى الأجهزة الأمنية بثغرات قانونية ضخمة، الأمر الذي أتاح المجال أمام الأفراد والجهات الأخرى للتجول دون رقيب والحصول على المعلومات الأمنية والسرية التي قد تكون على درجة عالية من الحساسية ويبدو أن شكل الحروب في الوقت الحاضر في تغير مستمر، حيث ستنتقل المعارك من ميادين القتال العادية إلى الحاسوب وشبكة الانترنت، فالحرية المتاحة عبر الشبكة تتيح التوصل إلى المعلومات والوثائق السرية التي قد تخفيها الدول، كما أن البعض قد يتمكن من اختراق مواقع استراتيجيه عسكرية وصناعية هامة تلك الدول على الشبكة المعلوماتية أوتدمير تلك المواقع بالفيروسات"، عن رشيدة بوكر، المرجع السابق،ص 207.

فاعتراض نظام المعالجة الآلية كما هو معروف في الولايات المتحدة الأمريكية تحت تسمية " إلتقاط الموجات الكهربائية " هو جمع للمعلومات عن بعد.

هذا وقد تباينت مواقف التشريعات بخصوص تضمين فعل الاعتراض ضمن النص الخاص لجريمة الدخول أولا، ففي حين ذهبت بعض التشريعات المقارنة نحوأفراد نص خاص لتجريم اعتراض نظام المعالجة الآلية منفصل عن تجريم الدخول غير المصرح به قامت دول أخرى بالعكس.

ب- القيام بالاعتراض باستخدام وسائل فنية غير علنية:

وفعل الاعتراض باعتباره يشكل الركن المادي لجريمة الاعتراض الغير القانوني للبيانات يجب أن يكون باستخدام وسائل فنية معينة وغير علنية، معدة لتصنت أو نقل البيانات وتسجيلها أو التحكم الحصول على المحتويات بصورة مباشرة عن طريق الولوج إلى نظم المعالجة الآلية للبيانات واستخدامها أو بشكل غير مباشر عن طريق استخدام أجهزة التصنت أو بتسجيل البيانات على أي من الأشرطة أو الدعامات المغناطيسية المعدة للتسجيل أو الأوراق أو البطاقات المثقبة[1].

كما يمكن أن يتعدى نطاق هذه الوسائل إلى الأجهزة الفنية المتصلة بخطوط النقل أو الاتصال مثل أجهزة تجميع وتسجيل الاتصالات اللاسلكية، أيضا يمتد إطاريا ليشمل الكيانات المنطقية كالبرامج المعلوماتية وكذلك كلمات المرور والكودات السرية أو الشفرات[2] .

ووسائل الاعتراض غير القانوني للنظم والبيانات المعلوماتية هي وسائل توصف بأنها غير علنية، وهذه الصفة تلحق الوسيلة نفسها من أجهزة ومعدات وأدوات وطرق معدة للتسجيل أو النقل أو التصنت أو للالتقاط للبيانات وليس للبيانات المرسلة في حد ذاتها والتي قد تكون متاحة للغير والعامة من الجمهور أي لكل الناس. فأطراف الحديث أو المكالمة أو المراسلة قد يرغبون في الاتصال بصورة سرية أما لاعتبارات شخصية أو سياسية أوتجارية على سبيل المثال عبر الشبكات المعلوماتية الداخلية أو الدولية كالانترنت ولكن وبالرغم من ذلك فإن مصطلح غير العلنية لا يستبعد الاتصالات في حد ذاتها التي تكون متاحة لأي من الأشخاص الذين يرغبون في استعمال هذه الشبكات لهذه الغاية.[3]

ومما تجدر الإشارة إليه، أن الاتصال بنقل البيانات قد يكون في حدود نفس الحاسب الآلي المختلفة من وحدة المعالجة المركزية ووحدات الإدخال والإخراج وأيضا يمكن أن يتم الاتصال بين العاملين والمستخدمين. كما يمكن أن يتم الاتصال عبر الشبكات المحلية التي ترتبط بنشاط واحد كالشبكة البنكية أو الشبكات العسكرية أوالاقتصادية داخل حدود الدولة

[1] بلال أمين زين الدين، مرجع سابق، ص 307.

[2] حسين بن سعيد بن سيف الغافري ، جريمة الاعتراض،مرجع سابق.

[3] بلال امين زين الدين، مرجع سابق، ص 308.

الواحدة.كما يمكن أن يكون الاتصال من خلال الشبكات الدولية أو الانترنت والتي تتعلق بكافة الأنشطة والمجالات المختلفة والتي تغطي معظم أرجاء الكرة الأرضية[1].

ونظرا للثورة المعلوماتية الجامحة وما يلازمها من ثورة تكنولوجية في جميع الاتجاهات العلمية، وما قد أدى إليه من التصاق واضح وبينها وبين التقدم في وسائل الاتصالات السلكية واللاسلكية، فإن عبارة النظام المعلوماتي الذي يقوم على بنيان الحاسبات الآلية يمكن أن يمتد مفهومها ليشمل الاتصالات اللاسلكية استنادا إلى أن معظم الاتصالات التي تتم حاليا من خلال الأنظمة المعلوماتية، تكون عبر الشبكات والأجهزة التي تعتمد على أجهزة الاتصالات اللاسلكية في إتمام وإجراء هذه الاتصالات، وبالتالي فإن من شأن اعتراضها ونقل أو تسجيل بياناتها أوالتصنت عليها أن يقع تحت طائلة التجريم لحماية المعلوماتية وذلك بتجريم كل الأفعال التي تشكل انتهاكا لها[2].

ج- القيام بالاعتراض بدون حق:

يشترط كذلك في فعل الاعتراض المكون للجريمة التجسس الالكتروني أن يكون بدون حق، فإذا قام المتهم بالتصنت على المحادثات الشخصية أو بنقل أو تسجيل البيانات المعلوماتية قد أوجد من الأسانيد والأدلة على أن القيام بذلك قد تم بناء على ما له من حق استمده من أطراف المكالمة أو الحديث الشخصي أو البث حيث سبق وأن صرح له بذلك أو أنه قد تصرف بناء على أمر قد صدر له منهما أومن السلطة المعنية بمراقبة الاتصالات أو بناء على تصريح من الأطراف المعنية باختبار أجهزة الاتصالات والحاسبات الشخصية والنظم المعلوماتية الخاصة بالمنشأة أو بالشركة أو الإدارة والذي عن طريقه قد تمكن من الاستماع إلى الأحاديث والمكالمات الشخصية أو الاطلاع على البيانات ونقلها وتسجيلها لأغراض تتعلق بتجربة واختبار الأجهزة والمعدات لوضع أفضل السبل الأمنية لحماية هذه البيانات والمعلومات من الانتهاكات التي يمكن أن تتعرض إليها بدون أنظمة الأمان، أو أنه قد قام بالمراقبة بناء على تصريح من السلطات المختصة لاعتبارات تتعلق بالأمن القومي للدولة التي ينتمي إليها أو لأغراض مخابراتية للبحث والتنقيب عن الأفعال الإجرامية وأعمال الجاسوسية أو مكافحة الإرهاب بتعقب مراسلاته واتصالاته عبر الشبكات المختلفة والمستترة في الغالب تحت أقنعت مزيفة تبث عبر المقالات والمنشورات والمراسلات والمجالات التي لا تحمل في مضمونها سوى الدفع بالمستمع إليها أو قارئها إلى هوة الفكر الأعمى والمتعصب نحو مبادئ مجهولة الهوية لا أساس لها من الشرع أو قواعد المنطق

[1] بلال امين زين الدين، المرجع نفسه، ص 308.

[2] بلال امين زين الدين، المرجع نفسه ، ص 309.

والعدالة، ففي كل هذه الحالات وما يماثلها فإن هذا الشخص يكون قد لجأ إلى ارتكاب الفعل بحق ، ونشير أنه لكل دولة الحق في أن تشترط القصد من الاعتراض ليكون جرما بما تراه مناسبا [2].

ثانيا:الركن المعنوي

الجريمة وفقا للنص السالف الذكر تعد من الجرائم العمدية التي تقوم بالقصد الجنائي العام بعنصرية العلم والإرادة، فيجب أن يعلم الجاني بأن حصوله على تلك المعلومات أو البيانات تم بوجه غير مشروع وضد إرادة ورغبة صاحب السيطرة عليها، هذا من جهة ومن جهة أخرى لا بد وأن تتجه إرادته إلى إتيان هذا الفعل بالمخالفة للقانون وبالمخالفة لإرادة صاحب المعلومات أو البيانات[1] .

وما تجدر الإشارة إليه أن هناك من التشريعات من خصصت للتجسس الالكتروني نصا خاصا مثلما هو الشأن بالمشرع العماني في المادة 276 في البند الثالث حيث نصت على الآتي" يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين وبغرامة .....كل من تعمد استخدام الحاسب الآلي في ارتكاب إحدى الأفعال التالية:3- التجسس والتصنت على البيانات والمعلومات."[2]، وهناك من تناولته في النص العام الخاص بالتجسس مثلما هو الأمر في مصر، في حين أن المشرع الجزائري رأينا أنه تصدى له بنص خاص عدا النص العام التعلق بجريمة التجسس وهو نص المادة 394 مكرر 2 وهو ذات الأمر بالنسبة للمشرع العماني في المادة 286 مكرر من قانون الجزاء العماني.

الفرع الرابع

حماية البريد الالكتروني والمحادثات الالكترونية من الاعتراض غير القانوني.[3]

---

[2]- بلال امين زين الدين، مرجع سابق، ص 309-310

[1] http://www.omanlegal.net/ يوم الاطلاع على الموقع

[2] للتوضيح من خلال النص لم يضع المشرع شروطا تتعلق بطبيعة البيانات والمعلومات ولم يشترط تبعيتها لجهة معينة ومن جهة أخرى لم يحدد وسيلة معينة للتجسس أو التصنت المعلوماتي فقد يكون عن طريق الاختراق أو اصطيادها وهي مرسلة أو غير دلك.

[3] أثير تساؤل حول حق رؤساء المصالح والهيئات العامة في مراقبة البريد الالكتروني للموظفين المرؤوسين لهم حيث تفجرت موجة من الجدال بالولايات المتحدة الأمريكية حول حق المديرين داخل الشركات والمؤسسات المختلفة في مراقبة البريد الالكتروني الصادر والوارد من وإلى الموظفين الدين يعملون تحت إشرافهم، وتفجر الجدل عقب الإعلان عن نتائج دراسة أجرتها جمعية الموارد البشرية الأمريكية مع مجموعة "ويست جروب ".وأظهرت أن84% من الموظفين المسؤولين عن الموارد البشرية في شركاتهم يراقبون العاملين في الشركة تفاديا لانخفاض إنتاجية العمل. وللتعرف على التصرفات غير اللائقة ويعتقد أغلب المسؤولين عن الموارد البشرية الدين استطلعت أرائهم في استطلاع الخصوصية في مكاتب العمل أن الشركات تمتلك الحق في التعرف على أنواع مواقع الانترنت التي يزورها موظفوها إضافة إلى حقها في

يعتبر البريد الالكتروني والمحادثات الالكترونية إحدى الخدمات المهمة التي تقدمها الانترنت كما سبقت الإشارة، ونظرا للمخاطر التي تعترض البيانات الالكترونية التي تنتقل من خلالها تصدى المشرع لتلك المخاطر بنصوص تجريمية وعقابية ردعا لكل معترض لتلك الأسرار المعلوماتية، وسنحاول التطرق إليها كالتالي:

أولا: جريمة انتهاك سرية البريد الالكتروني[1]

أصبح البريد الالكتروني الآن وسيلة لا غنى عنها في الكثير من مجالات العمل، خاصة في الاتصالات الثنائية فقد بدأ يقترب في شيوعه وانتشاره من الهاتف، ولكن مستخدمي البريد الالكتروني لا يأخذون قضية الأمن بالجدية اللازمة، بل يكتفون باستخدام كلمة السر في الدخول إلى الحاسب كوسيلة تأمين، وهي بالقطع ليست وسيلة تأمين مثالية، هذا وفي الوقت الذي أصبحت فيه إجراءات تأمين البريد الالكتروني سهلة وممكنة وتقنياته متاحة ومتوفرة، مثل تقنيات التشفير حائط النار وغيرها.

فكلما ازداد انتشار البريد الالكتروني وازداد اعتماد المجتمع عليه ازدادت المخاطر الأمنية التي تحيط به، ومع تزايد كم المعلومات المنقولة عبر الشبكات وعبر شبكة الانترنت على وجه الخصوص يصبح مسار هذه المعلومات محفوفا بالمخاطر، كذلك مجرد الدخول إلى البريد الإلكتروني الخاص بالغير ومجرد الإطلاع على الرسائل الموجودة بداخله يعتبر جريمة انتهاك لسرية المراسلات المكفولة بموجب الدستور[2].

فكل من يتصنت عن طريق شبكة المعلومات أو أجهزة الحاسوب وما في حكمها على الرسائل أو يلتقطها أو يعترضها دون تصريح بذلك من النيابة العامة أو الجهة المختصة أو الجهة المالكة للمعلومة، يعد انتهاكا لسرية المراسلات بمعنى لا يجوز الكشف على محتوياتها لأن طبيعة الرسالة تسمح بأن تكون وعاء للأسرار مما يجعل الاطلاع على مضمونها أمرا يعرض هده الأسرار لخطر الإفشاء.

1- تعريف البريد الاكتروني:

الاطلاع على مضمون الرسائل التي تصدر عبر نظومها الالكترونية وعبر العديد من الموظفين إثر ذلك عن عدم رضائهم واعتبروا أن مراقبة البري الالكتروني والمكالمات الهاتفية ليست سوى تدخل في خصوصياتهم وفي المقابل يقول المسؤولون أن الشركات تعلن عن سياستها بهذا الشأن بشكل خطي يلتزم به الموظفون. عن محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية الإسكندرية، 2004، ص 139.

[1] هناك جرائم أخرى محلها البريد الالكتروني ولكن ليست بهدف انتهاك السرية على وجه الخصوص وإنما للتعطيل مثلا أولأهداف أخرى متعددة منها جريمة تضخم البريد الالكتروني وجريمة تزوير البريد الالكتروني .

[2] خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008، ص 91.

يقصد بالرسائل العادية كافة الخطابات المكتوبة والمرسلة بطريق البريد وكذا كافة لبرقيات ويستوي أن تكون الرسالة داخل مظروف مغلق أو مفتوح أو تكون بطاقة مكشوفة طالما من الواضح أن المرسل يقصد عدم إطلاع الغير عليها بغير تمييز[1].

أما الرسائل الإلكترونية فهي التي ترسل عن طريق الإنترنت وهي قد تكون رسائل عامة يمكن لأي شخص الإطلاع عليها كما في صفحات الويب فهي شبه مفتوحة بطبيعتها أو الرسائل التي توجه إلى أشخاص كثيرين بغير تمييز، وقد تكون رسائل خاصة إذا كانت موجه إلى شخص أو أشخاص محددين أو إلى موقع يكون الدخول إليه مقيدا[2].

فالبريد الالكتروني هو عملية تبادل رسائل تم تخزينها بأجهزة الكمبيوتر سواء كانت على شبكة الإنترنت العالمية أو على نوع من الشبكات سواء كانت المحلية أو الشبكات الأكبر وتتم بواسطة وسائل الاتصال التلفونية وهي العملية التي تفهمها جميع أجهزة الكمبيوتر مهما كان نوع صنعها ونظام تشغيلها، ومع ذلك يمكننا إرسال ملفات من أي نوع آخر غير ملفات النصوص مثل الصور وملفات الصوت وذلك كملفات ملحقة، فالبريد الإلكتروني ببساطة عبارة عن نص، وهو عمل تقوم به باستخدام الكمبيوتر.

وعن تعريفه في المجال التشريعي، فقد عرفه القانون الفرنسي بشأن الثقة في الاقتصاد الرقمي الصادر في 22 يونيه 2004 بأنه" كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صور أو أصوات ويتم إرسالها عبر شبكة اتصالات عامة وتخزن عند أحد خوادم تلك الشبكة أوفي المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها"[3] وعرفه المشرع الجزائري في المادة الثانية من المرسوم 98-257 المتعلق بضبط شروط وكيفيات إقامة خدمت" الأنترنت" واستغلالها أنه" خدمة تبادل رسائل إلكترونية بين المستعملين" والملاحظ على المشرع أنه عند تعديله للمرسوم بموجب المرسوم التنفيذي 2000-307 عدل نص المادة الثانية حيث تراجع فيها عن التعريف السالف الذكر.

2- تجريم الاعتراض غير القانوني للبريد الالكتروني:

وأما عن تجريم[4] اعتراض البريد الالكتروني فإن العديد من الدول من اعتبرت هذا السلوك سلوكا مجرما ونصت على ذلك في نصوص صريحة وواضحة[5]، وبالنسبة للمشرع

---

[1] - علاء عبد الباسط خلاف، الحماية الجنائية لوسائل الاتصال الحديثة، بدون ناشر، بدون طبعة، 2004، ص 161.

[2] علاء عبد الباسط خلاف، المرجع السابق، ص 162.

[3] اسعد فاضل منديل الجياشي ، البريد الالكتروني دراسة قانونية ،مقال منشور على الموقع الالكتروني http://profasaad.info/

[4] تجدر الإشارة أنه إلى جانب الحماية الجزائية هناك الحماية الفنية للبريد الالكتروني وتتم عن طريق أساليب تعتمد على تقنيات التشفير والتوقيعات الرقمية، ويعتبر التشفير من أهم وسائل تأمين البريد الالكتروني على الإطلاق.

[5] كقانون العقوبات الكندي في المادة 1/430و نظام مكافحة جرائم المعلومات السعودي إذ عاقبت المادة 3 منه على التصنت على المكالمات الصوتية التي تتم عبر البريد الالكتروني سواء كان طرفيها يستخدما نظامين معلوماتيين لجهازين من أجهزة الحاسوب أون أجهزة الهاتف ، وكذلك تعاقب المادة على التقاط أي من الرسائل المرسلة عبر هذا البريد أو اعتراضه

الجزائري رغم أنه لم يعتبره جريمة ضمن نص صريح سوى ما هو منصوص عليه في المادة 303 من قانون العقوبات ومن خلال النص قد يعتبر البريد الالكتروني من ضمن المراسلات المقصودة في نص المادة، إضافة إلى ذلك هناك نص المادة 394 مكرر2 الذي جرم التعامل في معلومات تم الحصول عليها من اعتراض المراسلات الالكترونية وكما سبقت الإشارة رغم أنه لم يشير إلى تجريم الاعتراض غير القانوني إلا أنه جرم التعامل في تلك المعلومات المتحصل عليها من الاعتراض بدلك الشكل.

فالمشرع الجزائري اعتبر اعتراض المراسلات الالكترونية ووتسجيل الأصوات والتقاط الصور فعل غير مشروع من خلال المواد من 65 مكرر 5 إلى 65 مكرر 10 من قانون الإجراءات الجزائية التي سمحت به استثناء كإجراء تحقيق إذا ما دعت ذلك مقتضيات البحث والتحري والتحقيق الابتدائي في الجرائم المتلبس بها وكذا الجرائم الآتية: جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية؛ الجرائم الماسة بأنظمة ممارسة المعالجة الآلية للمعطيات؛ جرائم تبييض الأموال؛ جرائم الموصوفة بأفعال الإرهاب أو التخريب؛ الجرائم المتعلقة بالتشريع الخاص بالصرف؛ جرائم الفساد)، جاز لوكيل الجمهورية أن يأمر ضابط الشرطة القضائية باعتراض المناسبات التي تجري عن طريق وسائل الاتصال السلكية واللاسلكية، ووضع الترتيبات اللازمة لالتقاط الصور وتسجيل المكالمات في الأمان العامة والخاصة وتنفيذ هذه العمليات تحت إشراف ورقابة وكيل الجمهورية في مرحلة البحث والتحري، أما في مرحلة التحقيق الابتدائي فتكون تحت إشراف قاضي التحقيق الذي أمر بها) المادة 65 مكرر 5 ويسلم الإذن بهذه العملية لمدة أقصاها أربعة 04 أشهر قابلة للتجديد حسب المقتضيات التحري والتحقيق (المادة 65 مكرر 7 ، وعلى ضابط الشرطة القضائية المكلف تحرير محضر عن كل عملية اعتراض أو تسجيل أو التقاط مع ذكر زمن بداية هذه العملية وكذا تاريخ انتهائها.

كذلك المادة 3 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حيث نصت على الآتي" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام، أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هدا القانون وضع الترتيبات التقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها....".

لاسيما أن هذه الأفعال تعد انتهاك واضح لحمة الحياة الخاصة لمستخدم البريد الالكتروني.، أنظر في ذلك طارق عفيفي صادق أحمد، مرجع سابق، ص 134.

وبالنسبة للمشرع الفرنسي قد عرفت المادة 23 من قانون البريد والاتصال، الاتصال عن بعد بأنه" كل نقل أو بث أو تلقي لعلامات أو إشارات أو كتابات أو أصوات من أي نوع كانت بواسطة كابل أو راديوكهربائي أوبواسطة أي نظام كهرومغناطيسي وعلى ذلك فإن الاتصال عن بعد يشمل الاتصالات التي تتم عبر الإنترنت ومن ثم فإنها تخضع لقانون البريد والاتصال"[1].

كذلك تنص المادة 2/2 من القانون الفرنسي رقم 86-1067 الصادر في 30 سبتمبر 1986 والخاص بحرية الاتصالات السمعية البصرية على أن الاتصالات في كل وضع تحت تصرف الجمهور أو طائفة من الجمهور، بأي وسيلة للاتصال عن بعد لعلامات أو إشارات أو كتابات أو صور أو أصوات أو أي رسائل من أي طبيعة كانت والتي ليس لها طابع المراسلة الخاصة "، وهو ما ينطبق على شبكة الانترنت التي تقوم بإرسال رسائل إلى أشخاص غير محددين ويمكن الإطلاع عليها ومعرفة محتواها.

أما المراسلات الخاصة فيتم حمايتها عن طريق قانون العقوبات الفرنسي الجديد إذ تنص المادة 226-15 على أن يعاقب بالحبس لمدة سنة وبغرامة مقدارها 300000 فرنك من " فتح أو أخفى أو اختلس – بسوء نية – المراسلات المبعوثة للغير، أو الاطلاع عليها بطريق الغش" ويعاقب بنفس العقوبات " من احتجز أو اختلس أو استعمل أو أفشى بسوء نية المراسلات المبعوثة أو المنقولة أو تم تلقيها بطريق الاتصال عن بعد[2] أو أجري تركيب أجهزة مصممة لمثل هذه الإعاقات[3] .

هذا النص شأنه شأن المادة 303 من قانون العقوبات الجزائري بنصها على الآتي:"كل من يفض أويتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137 يعاقب ...."، فالمشرع في هذه المادة توسع في نطاق الحماية القانونية المكفولة لسرية المراسلات.كما نجد أيضا أن قانون البريد والمواصلات السلكية واللاسلكية في المادة 4/105 تنص على أنه لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات.

ثانيا: المحادثات الالكترونية الشخصية

[1] - جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية،2001 ، ص52.

[2] رغم أن النص لم يشر صراحة إلى المراسلة عن طريق الانترنت إلا أن البريد الالكتروني يدخل في مفهوم المراسلة المذكورة في النص.

[3] - يرى البعض أنه يمكن تطبيقه على البريد الالكتروني لأنه يدخل في مفهوم المراسلة.

من المحتمل جدا أن تحمل المحادثات الشخصية بعض الأسرار الخاصة بالفرد والتي لا يود أن يطلع عليها غيره سوى المتحدث معه، والأصل أنها محادثة خاصة وبالتالي سرية مع العلم أن التصنت على المحادثات الشخصية التي تكون عن طريق شبكة الانترنت فيه مساس بالحياة الخاصة للأفراد، وسبق وأن أشرنا أن ذلك فيه مساس بالسرية ولهذا سنحاول التطرق للموضوع على النحو التالي:

1- تعريف خدمة المحادثة الالكترونية:

هي من الخدمات التي تقدمها شبكة الانترنت، وهي نظام يمكن مستخدمه من الحديث مع المستخدمين الآخرين في وقت حقيقي كتابة وصوتا كما يمكن أن ترى الصورة باستخدام الكاميرا.

فالدردشة أو المحادثة واحدة من أكبر الخدمات شعبية وشهرة وإثارة على شبكة الانترنت، طورت في فلندا في عام 1988، وهي تسمح لعدد غير محدود من مستخدمي الانترنت، في أي مكان من العالم من الدخول في حوارات حية مباشرة، بواسطة لوحة مفاتيح أو أدوات صوت عن طريق الدخول إلى بعض المواقع التي توفر خدمات الدردشة .ولكنها تحتاج لبرنامج لكي تتمكن من الدردشة أو الدخول في غرف الحوار لكن هذا ليس إجباريا وهو يعتمد على المواقع كما أن بعض المواقع تتطلب ضرورة التسجيل في تلك المواقع قبل أن تبدأ في الدردشة [1]. وقد تتعرض هذه المحادثات للاعتراض مما يمكن المعترض الاطلاع والتعرف على كل ما يدور بين المتحدثين ويتم انتهاك هذه المحادثة وهو الأمر المجرم قانونا.

2- الحماية الجزائية للمحادثات الشخصية عبر شبكة الانترنت:

تعاقب كثير من التشريعات المقارنة على اعتراض الاتصالات السلكية واللاسلكية الخاصة، بدون إذن بذلك باعتبار أن هذا السلوك يتضمن انتهاكا لحرمة الحياة الخاصة، وثار الخلاف حول هل يعتبر اعتراض المحادثات الشخصية عبر الانترنت من قبيل التجريم أم لا؟.

هناك من تصدى لاعتراض المحادثات الشخصية عبر الانترنت بالتجريم، وذلك بإضافة نص عقابي مناسب كما فعل المشرع الجزائري بموجب نص المادة 303 مكرر من قانون العقوبات التي نصت على أنه:"يعاقب بالحبس...بأية تقنية كانت:.....بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أوسرية.....صورة لشخص ..".

[1] http://www.al-jazirah.com.sa/digimag/13062004/co27.htm يوم الاطلاع على الموقع2015/11/06 .

كما كفل المشرع السعودي صراحة سرية وحرمة المكالمات والمعلومات المتبادلة عبر شبكات الاتصال العامة، بحيث أنه لا يجيز الاطلاع عليها أو الاستماع إليها أو تسجيلها إلا في الحالات المحددة في القانون بموجب المادة 309 مكرر قانون عقوبات.

وخلاصة لما سبق ذكره فجريمة التجسس المعلوماتي الهدف منها هو الحصول على المعلومة و السؤال المطروح هو الغرض منها هل هو الإفشاء أم ماذا، في حين أن إفشاء المعلومة المتحصل عليها من جريمة التجسس هو جريمة تختلف عن جريمة إفشاء المعلومة المؤتمن عليها من قبل فئة معينة من الأشخاص لذلك كان لزوما علينا التفرقة بين الأمرين.

المطلب الخامس

جريمة إفشاء الأسرار المعلوماتية المهنية

نتيجة الانتشار المذهل للثورة المعلوماتية أن تخللت الحاسبات الآلية كل نشاط من الأنشطة الوظيفية والمهنية، حتى أن أرباب المهن والوظائف بل والأشخاص العاديين أصبحوا يعتمدون على جهاز الحاسب الآلي في تخزين كل ما يرد إليهم أو توارد في أذهان هؤلاء الأشخاص من أسرار، ويدور جوهر الإفشاء بالنسبة للسر حول إذاعته أو نقله واطلاع الغير عليه، مما يعني خروج المعلومة من دائرة الكتمان، وبالتالي تكون قد تخطت نطاق العلم بها إلى غير صاحبها أو المؤتمن عليها بحكم وظيفته، مما يشكل اعتداءا على إرادة صاحب المعلومات في أن تظل هذه المعلومات مغلقة بطابع السرية والكتمان.

فالإنسان قد يبوح لشخص ما بحكم وظيفته أو مهنته بمعلومات سرية تخصه ولا يهم أهمية تلك المعلومات المهم أن تكون تلك المعلومات خاصة بصاحبها، وأن تتجه إرادته إلى الحفاظ على سريتها.[1]

فنجد المحامي، الطبيب، المهندس والخبير وغيرهم من المؤتمنين على الأسرار يرتكن إلى الحاسب الآلي كي يفرغ في ذاكرته ما يتوصل إليه من أسرار فنص قانون العقوبات في جل بلدان العالم على معاقبة كل من الأطباء أو الجراحين أو الصيادلة أو غيرهم من كان مودعا إليه بمقتضى صناعته أو وظيفته سر خصوصي فأفشاه في غير الأحوال التي نص عليها القانون يعاقب تطبيقا لنص المادة 310 من قانون العقوبات المصري و301 من قانون العقوبات الجزائري والمادة 418 من قانون العقوبات الفرنسي، وغيرها من النصوص العقابية المختلفة على حسب كل دولة تشريع كل دولة والتي جاءت عموما في نفس السياق والصياغة[2].

[1] عمر أبوالفتوح عبد العظيم الحمامي، مرجع سابق، ص 457.

[2]- سبق لنا وأن فرقنا بين هذه الجريمة وهي جريمة إفشاء الأسرار المهنية وبين جريمة إفشاء الأسرار التي تم الحصول عليها من الاختراق لأنظمة معلوماتية أوتم الحصول عليها من عمليات استراق السمع والتصنت المعلوماتي وكل الوسائل الحديثة لانتهاك السرية المعلوماتية.

ونشير إلى أن النصوص السالفة الذكر لم تحدد ذوي المهن المؤتمنون على الأسرار المعلوماتية أو الشخصية على سبيل الحصر وإنما على سبيل الأمثلة وبالتالي فإن النص يشمل كل من يودع لديه بمقتضى صناعته أو وظيفته أي من أسرار الأشخاص الخاص كالمستخدم في الشركات والمؤسسات والهيئات والإدارات التي تعتمد على الأنظمة المعلوماتية التي تقوم بالحفاظ وتخزين المعلومات الخاصة بالعملاء في أوعية تخصص لهذا الغرض، وتمنع المساس بخصوصيتها وسريتها أو الوصول إليها بأي شكل كان[1].

وأيضا يمتد النص ليشمل طائفة المبرمجين ومحللي الأنظمة المعلوماتية ومشرفي الصيانة وغير ممن يمتهنون تقنية الحاسبات الآلية، ويمكن أن تصل إليهم معلومات وأسرار غاية في الأهمية نتيجة ممارسة هذه المهنة أوالوظيفة الملحق بها لدى أي من الجهات والهيئات والمرافق العامة[2].

إضافة إلى ذلك كل شخص يمتهن تقنية الحاسبات الآلية حتى ولو كان لا يلحق لمرفق عام لابد من أن يشمله النص، فعلى سبيل المثال قد يعرض الحاسب الشخصي وما يمكن أن يحمله من أسرار خاصة على مصلح الحاسوب في حالة العطل، والأكيد أنه سيصل إلى علمه كل ما يحمله الحاسوب من أسرار معلوماتية لابد وأن يجرم إفشاؤها من صاحب هذه المهنة.

فالإشكال الذي يطرح نفسه في هذه الجريمة وعلى أساسه تمت معالجتها وهو هل لابد أن يتم إفشاء السر من المؤتمن عليه شخصيا كما هو الحال في جريمة إفشاء الأسرار المهنية التقليدية أو أن مجرد التهاون في تأمين تلك الأسرار على حاسوب المؤتمن على السر ليصل بذلك إلى غيره هو في حد ذاته سلوك مجرم ؟ هذا من جهة ومن جهة أخرى هل نطبق النص العقابي التقليدي أم لابد من استحداث نص يتعلق بإفشاء الأسرار المهنية المعلوماتية في حالتين.

أولهما حالة إفشاء المؤتمن على السر شخصيا السر المهني المعلوماتي، وثانيهما حالة إفشاء السر المعلوماتي لتهاون المؤتمن على السر كأن لا يقوم بوسائل الحماية الفنية للحاسوب الخاص بمكتبه مثلا، أو القيام بالاحتياطات اللازمة لتأمينه من الاطلاع عليه من غير المصرح لهم بذلك. كأن يحكم الإقفال عليه معناه يبدل عناية الرجل الحريص هي تساؤلات سيتم الإجابة عنها بعدما نتعرض لأركان جريمة إفشاء الأسرار المهنية المعلوماتية وفقا للنصوص السالفة الذكر.

الفرع الأول
الركن المادي في جريمة إفشاء الأسرار المعلوماتية المهنية

[1]- بلال أمين زين الدين، مرجع سابق، ص 286.

[2]- بلال أمين زين الدين، المرجع نفسه، ص 286.

الفعل المادي في جريمة إفشاء الأسرار المعلوماتية هو قيام الجاني بإفشاء ما توصل إليه من أسرار ومعلومات بمقتضى وظيفته أو مهنته.

وبمعنى أكثر تحديدا قيام الجاني بإذاعة الخبر أو النبأ المعلوماتي بأي من طرق الإفشاء الكتابية أو الشفوية أو عن طريق النشر أو بالتحدث به في محاضرة أو بين الناس أو بالتصريح به أو بجزء منه لآخر من غير العالمين بالسر ولو كان وطيد الصلة بالشخص الأمين عليه.

ونتيجة لما وصلت إليه المعلوماتية من انتشار شمل كافة الهيئات والإدارات والشركات والمؤسسات الاقتصادية والسياسية والاجتماعية والتكنولوجية والمرفقية العامة والخاصة ولدى الأشخاص فإن السر المعلوماتي قد أصبح وفقا لمتطلبات العصر الحاضر دفين النظم المعلوماتية التي هي في حوزة شخص أمين عليها قد يكون موظف عام أو مستخدم لدى المرافق العامة التي تديره الدولة بالطريق المباشر أو أحد العاملين بالمصانع التابعة للدولة أو للقطاع الخاص أو أي من المبرمجين أو المستخدمين أو محللي النظم المعلوماتية أو مندوبي الصيانة التابعين لإحدى الشركات أو الإدارات أو المؤسسات الاستثمارية أو المحاسبية أو التي تعمل في مجال تكنولوجيا الحاسب الآلي والبرمجيات أو أي من العاملين في البنوك المعلوماتية المتخصصة في الحفظ والائتمان على الأسرار المعلوماتية .

وعلى ذلك إذا ما قام أي من المؤتمنين على الأسرار المعلوماتية كالموظف العام بإحدى المستشفيات الحكومية بإفشاء التقارير الطبية الخاصة بالمرضى نزلاء هذه المستشفيات فإنه يكون مرتكبا للجريمة المنصوص عليها في المادة 301 من قانون العقوبات الجزائري .

كذلك إذا ما قام المحاسب التابع لأي من المصالح الحكومية بإفشاء التقارير المحاسبية التي تتعلق بالموازنة والصادر والوارد وبنود الصرف والخصومات والعلاوات والحوافز والمرتبات والبدلات وغيرها فإنه يكون قد خالف القانون ويتعرض للعقوبة المنصوص عليها في المادة السالفة الذكر.

وأيضا يعد مرتكبا لجريمة إفشاء الأسرار المعلوماتية الشخص الذي يودع لديه السر بمقتضى مهنته إذا ما قام بالإفشاء. فالطبيب والجراح والصيدلي والقابلة والمحامي والقاضي وغيرهم ممن يؤتمن على الأسرار بمقتضى مهنته إذا ما قام أي من هؤلاء بإذاعة أي من الأسرار التي توصلوا إليها أثناء ممارسة مهنتهم فإنهم يكونوا قد ارتكبوا جريمة إفشاء الأسرار المنصوص عليها في المادة301 من قانون العقوبات الجزائري . فالطبيب الذي يتوصل إلى معلومات خاصة بالمريض المشرف على علاجه ويقوم بإعداد ذلك في تقارير يتضمنها الحاسب الآلي الخاص به في ذاكرته لمتابعة حالته المرضية والجراح الذي يقوم بالاحتفاظ بأسرار وتفاصيل العملية الجراحية في اسطوانات ممغنطة والقابلة التي تطلع على أسرار خاصة بمرضاها والصيدلي الذي يقوم بصرف أدوية قد يكون لها من الصفة السرية والمحامي الذي يطلع على اعترافات غاية في الأهمية والسرية الخاصة بموكله المتهم

والقاضي الذي في عهدته أوراق التحقيق والاعترافات والدفوع والاتهامات والدلائل والقرائن الخاصة بالوقائع المنظورة أمامه وبالخصوم أطراف الدعوى ... وغيرهم ممن يؤتمنون على الأسرار بمقتضى مهنتهم الغير محددين بسياق المادة إذا ما قام أي من هؤلاء بإفشاء الأسرار المعلوماتية التي يتصلون إليها عبر ممارسة مهنتهم فإنهم يكونوا قد وقعوا تحت طائلة العقاب المنصوص عليه في المادة 301 من قانون العقوبات الجزائري المتعلقة بإفشاء الأسرار.

ولم تحدد المادة المذكورة ذوي المهن على سبيل الحصر وبالتالي فمن الممكن أن يمتد سياق المادة ليشمل كل من يقوم بمزاولة مهنة من المهن والتي من خلالها يستطيع الاطلاع على أسرار المتعاملين معه كما أن هناك قوانين كثيرة أوردت طوائف مختلفة يحظر عليها إفشاء أي من الأسرار التي تصل إليهم بمقتضى أعمال وظائفهم، وبمقتضى هذه المهنة كالعاملين في المصانع إذا ما قاموا بإفشاء الأسرار المتعلقة بالمصنع والمستخدمين الذي يعملون في شركات الحاسبات الآلية والمبرمجين ومحللي النظم ومشرفي الصيانة الذين يعملون في المؤسسات والإدارات والشركات التي تعتمد على الأنظمة المعلوماتية في إدارة شئونها وأنشطتها الاستثمارية ولذلك فقد نصت المادة 418 من قانون العقوبات الفرنسي على أن كل مدير أو ممثل أو عامل يطلع أوي حاول اطلاع الأجانب أوالفرنسيين المقيمين في الخارج على أسرار المصنع الذي يعمل فيه سيعاقب بالسجن لمدة تتراوح بين سنتين وخمس سنوات وبالغرامة ثمانية عشر ألف فرنك إلى مائة وعشرون ألف فرنسي ولو كان المطلع على هذه الأسرار هم فرنسيين مقيمين على الأراضي الفرنسية ستكون العقوبة هي الحبس من ثلاثة أشهر إلى سنة.

ومن الواضح أن النص لم يشر إلى ماهية المقصود بأسرار المصنع الأمر الذي جعل الفقه يتوسع في مفهوم سر المصنع.

الأمر ذاته بموجب المادة 302 من قانون العقوبات الجزائري فإنها تجرم الإدلاء أو الشروع في ذلك بأسرار المؤسسة التي يعمل فيها العامل الذي يقوم بذلك دون أن يكون مخلا له القيام بدلك الفعل إلى أجانب أوجزائريين يقيمون في بلاد أجنبية، كذلك يجرم ذات السلوك إذا قام به العامل وأدلى بتلك الأسرار إلى جزائريين يقيمون بالجزائر والعقوبة المقررة في الحالتين مختلفة.

وتشدد العقوبة في الحالتين إذا تعلقت الأسرار بصناعة أسلحة أو ذخائر حربية مملوكة للدولة.

الفرع الثاني
الركن المعنوي في جريمة إفشاء الأسرار المعلوماتية

تعد جريمة إفشاء الأسرار من الجرائم العمدية التي تتطلب القصد الجنائي بعنصرية العلم والإرادة. علم الجاني بأنه يقوم بإذاعة ما أؤتمن عليه من الأسرار التي توصل إليها عن طريق وظيفته أو مهنته أو صنعته وإرادته الحرة المختارة لهذا السلوك. وقد أثير الخلاف الفقهي حول ما إذا كانت جريمة إفشاء الأسرار تطلب قصدا خاصا يتمثل في نية الأضرار بالمجني عليه أم لا تتطلب هذا القصد الخاص.

فقد ذهب جانب من الفقه الفرنسي إلى القول بأن نية الإضرار تعد شرطا لا غنى عنه لقيام هذه الجريمة استناد إلى أن المشرع لم يهدف إلى العقاب على إفشاء الأسرار بنية خدمة صاحب السر وإنما يحميه من الأضرار التي يمكن أن تصيبه جراء إفشاء هذا السر.

كما أنه إذا ما اختفت نية الإضرار لما كنا بصدد سر من الإسرار وإنما يعد نبأ قد يعلمه الكافة دون أضرار. وأيضا استند هذا الرأي إلى أن جريمة الإفشاء تعد من طبيعة البلاغ الكاذب وجرائم القذف التي تتطلب نية الإضرار بالمجني عليه. وقد أيد القضاء الفرنسي هذا الاتجاه حينا من الزمن إلى أن عدل عنه منحازا إلى الاتجاه الفقهي السائد سواء في مصر أوفي فرنسا اللذان لا يتطلبان اشتراط نية الإضرار لوجود جريمة الإفشاء حيث أن السر بطبيعته وفقا لمتطلبات صاحبه في كتمانه والاحتفاظ به لدى آخر أمين عليه يحمل بين طياته الأضرار الأدبية والمادية التي يمكن أن تصيب المجني عليه نتيجة الإفشاء.

وأخيرا لا عبرة بالباعث على إفشاء السر المعلوماتي الذي قد يكون لقاء رشوة أو بدافع الكره والضغينة أواللهو و الاستهانة بصاحب السر أو الربح المالي أو لهدف آخر.

و خلاصة لما سبق فإنه يعتبر جريمة إفشاء أسرار معلوماتية مهنية إذا أفشى المؤتمن على سر إلى الغير وبأي طريقة كانت في غير الأحوال التي يسمح بها القانون، بينما إهمال هذا الأخير تأمين الحاسوب الخاص به والذي يحمل أسرار خاصة بعملائه أو زبائنه، وتركه دون حماية فنية أو نوع من أنواع الحماية حيث يعتبر حريصا على كتمان ما يحمله الحاسوب من أسرار، هي الحالة التي لم يتناولها النص العقابي السالف الذكر ولا النصوص المتفرقة الخاصة بالمهن والوظائف وغيرها والتي جرمت إفشاء الأسرار إضافة إلى قانون العقوبات.

إذن يعتبر ذلك الإهمال كأن يترك الحاسوب الخاص بمهنته في متناول الأيدي، أو تركه دون حماية فنية أوعلى الأقل يضع له كودا سريا مانعا الغير من الاطلاع على ما به من أسرار خاصة بالأفراد، وبالتالي نحن نقترح إضافة هذا السلوك إلى النص العقابي في فقرة ثانية كالتالي: " وكل الفئات المذكورة أعلاه وغيرها من كل ممتهن أوحرفي أو موظف تهاون في حماية حاسبه الآلي الذي يحمل أسرار معلوماتية وصلت إلى علمه بموجب وظيفته أومهنته أو حرفته بكل الطرق المسموح بها قانونا يعاقب بنفس العقوبة في الفقرة الأولى"[1].

[1]- حيث أن نص المادة 301 قانون العقوبات جزائري تنص على الآتي : "يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من500إلى 5000دج الأطباء والجراحون و .....على أسرار أدلى بها.....بالسر المهني ".

والجدير بالذكر أن جريمة إفشاء الأسرار المهنية المعلوماتية تختلف عن جريمة إفشاء المعلومات المتحصل عليها بطرق غير مشروعة والتي نعبر عنها بجريمة إفشاء الأسرار المعلوماتية المتحصل عليها بطريق غير مشروع، حيث أنه عند حديثنا عن جريمة إفشاء الأسرار بالضرورة سنكون نعني إفشـــاء الأسرار المهنية ذلك أنـــها من الجرائم المعروفة في القانون الجنائي، في حين عندما نقول إفشـــاء الأسرار المعلوماتية فلا يعني ذلك إفشاء الأسرار المعلوماتية المهنية فقط بل تولد لدينا صورة أخرى من الإفشاء و هي إفشاء معلومات إلكترونية سرية تم التوصل إليها عن طريق جريمة من جرائم المساس بالأنظمة المعلوماتية و هما ليستا ذات الجرم، حيث أن إفشاء الأسرار المهنية المعلوماتية يطبق عليها النص التقليدي لإفشاء الأسرار وهو نص المادة 301 من قانون العقوبات الجزائري والشيء الجديد فيها هو أنها أصبحت يطلق عليها معلوماتية نظرا لاكتساح جهاز الحاسب الآلي جميع المجالات بما فيها المهنية، في حين الجرم المستحدث وهو إفشاء المعلومات المتحصل عليها من جريمة تطبيقا لنص المادة 394 مكرر2 الفقرة الثانية من قانون العقوبات الجزائري.

وكما أشرنا أنه كان للاعتداء على الأسرار المعلوماتية حماية بموجب قانون العقوبات والقوانين المكملة له من جهة بموجب الاتفاقيات الدولية ، ومن جهة أخرى أيضا سنحاول التفصيل في حماية تلك الأسرار بموجب نصوص الملكية الفكرية.

المبحث الثاني

مواجهة الجرائم الواقعة على الأسرار المعلوماتية من خلال نصوص الملكية الفكرية

الملكية الفكرية مصطلح قانوني يقصد به حق الإنسان فيما ينتجه من اختراعات علمية و إبداعات فنية وأدبية وتقنية وتجارية،...وغيرها من نتاج الفكر الإنساني، إذ يخول لصاحبه سلطات تنبع من حق الملكية الوارد على شيئ غير مادي، فله أن يتصرف فيه باستثماره أو التنازل عنه كحق المؤلف في التأليف و الناشر في حقوق النشر و المهندس في المخططات والخرائط و المخترع فيما اخترعه بعد تسجيله و الحصول على براءة الاختراع.كما له سلطة الاستعمال على نتاج الفكر و يمنع الغير من الاستيلاء عليه أو استعماله دون إذن صاحبه[1].

[1] نرجس صفو، الحماية القانونية للملكية الفكرية في البيئة الرقمية، مداخلة بالمؤتمر الدولي الحادي عشر لمركز جيل البحث العلمي حول التعلم بعصر التكنولوجيا الرقمية، في طرابلس لبنان من 22إلى 24 أبريل 2016، ص 1، منشور على الموقع الالكتروني **http://jilrc.com/** أطلع عليه بتاريخ 01 مارس 2017.

فعرف البعض حق الملكية الفكرية بأنها هي القواعد القانونية المقررة لحماية الإبداع الفكري المفرغ ضمن مصنفات مدركة(الملكية الفنية و الأدبية)، أو حماية العناصر المعنوية للمشاريع الصناعية و التجارية(الملكية الصناعية)[1]، وعرفه آخرون بأنه حق الشخص على شيء غير مادي هو نتاج ذهنه أو ثمرة فكره وخياله مثل حق المؤلف في مؤلفاته وحق المخترع في اختراعه وحق الفنان في مبتكراته الفنية[2]، و عرفتها المنظمة العالمية للملكية الفكرية(الويبو) بقولها:" تشير الملكية الفكرية إلى أعمال الفكر الإبداعية، أي الاختراعات والمصنفات الأدبية والفنية والرموز والأسماء والصور والنماذج والرسوم الصناعية.[3]

ومنه تشمل الملكية الفكرية، الملكية الأدبية والفنية[4] والحقوق المجاورة والملكية الصناعية للنماذج والرسوم الصناعية وبراءات الاختراع وملكية العلامة التجارية والرسم التجاري وغيرها.

وحيث أن الملكية الفكرية تأثرت بالتطور في المجال المعلوماتي وظهور البيئة الرقمية تولد لدينا المصنفات الرقمية، والتي لا تختلف كثيرا عن التقليدية فقط في الحامل فبدلا عن الورقي أصبح الكترونيا ولكنها أثارت العديد من المشاكل والصعوبات القانونية .

ونظرا للأهمية التي تحظى بها الملكية الفكرية أحاطتها النصوص القانونية على المستويين الدولي والداخلي بالحماية، وزادت هذه الحماية و على المستويين مع ظهور شبكة الانترنت وإدراكا من المشرعين بخطورة الجريمة المعلوماتية حيث سارعوا في سد الفراغات القانونية في القوانين و الاتفاقيات و المعاهدات فيما يتعلق بارتكاب انتهاك حقوق الملكية الفكرية بوسائل معلوماتية.

فعلى المستولى الدولي كانت اتفاقية برن من أول الاتفاقيات في مجال تأصيل الملكية الفكرية والتي طالها التعديل لأكثر من مرة و،إضافة إلى اتفاقية تربس للتدابير المتعلقة بأثر التجارة على الملكية الفكرية[5] والتي تضمنت إضافات في مجال الملكية الفكرية أهمها إضافة قواعد جديدة في مجال حماية المصنفات الرقمية وإحداث مركز لإدارة الملكية الفكرية إلى جانب المنظمة العالمية للملكية الفكرية "الويبو"[6] ومنظمة التجارة العالمية [1] ، حيث انضمت

---

[1] يونس عرب، موسوعة القانون وتقنية المعلومات، الكتاب الأول، قانون الكمبيوتر، الطبعة الأولى، منشورات اتحاد المصارف العربية، بيروت، 2001، ص 298.

[2] طارق عفيفي صادق احمد، مرجع سابق، ص 114.

[3] نرجس صفو، المرجع نفسه، ص2.

[4] كالملكية الأدبية والفنية للمصنفات كالروايات والقصائد والأفلام والألحان الموسيقية بينما الحقوق المجاورة لحق المؤلف مثل حقوق فناني الأداء ومنتجي التسجيلات الصوتية .

[5] أبرمت هذه الاتفاقية سنة 1994 لتحرير التجارة الدولية المشروعة آخذة بعين الاعتبار رورة ضمان عدم وقوف التدابير المتخذة لحماية الملكية الفكرية عائقا أمام التجارة الدولية.

[6] المنظمة العالمية للملكية الفكرية أو اتفاقية الويبو التي دخلت حيز التنفيذ في سنة 1970 و عدلت سنة 1979 لتصبح احدى وكالات الأمم المتحدة المتخصصة في ديسمبر 1976، أنظر نرجس صفو، مرجع سابق، ص 4.

الجزائر إلى هذه الأخيرة سنة 1996. أما على المستوى الداخلي فخضعت تشريعات الملكية الفكرية إلى العديد من التعديلات للتلاؤم مع متغيرات عصر المعلوماتية[2].

فورد في اتفاقية بودابست المتعلقة بالجرائم المعلوماتية تأكيد على حظر الاعتداء على حقوق الملكية الفكرية عبر الأنظمة المعلوماتية بموجب المادة 10 منها[3]، كما أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات جرمت بعض صور الاعتداء على حقوق الملكية الفكرية بواسطة إحدى وسائل تقنية المعلومات في المادة 17 منها .

ويستهدف المشرع الجزائري من خلال نصوص الملكية الفكرية إلى حماية حق الإنسان في الفكر والإبداع والابتكار، وطالما كان هذا هوا لهدف من تقرير هذه النصوص، فإن ذلك يدعو للتساؤل والقول أليست المكونات غير المادية للحاسب الآلي أي الكيان المنطقي، أي برامجه وبياناته تعتبر نتاج فكر وجهد ذهني للإنسان فإذا كان الأمر كذلك، فما المانع من خضوع برامج وبيانات الحاسب للحماية التي يقررها المشرع بمقتضى هذه النصوص[4].

ومن أهم المسائل القانونية في هذا الإطار هو تحديد الطبيعة القانونية للبرامج المعلوماتية فهل هي مصنفات تدخل تحت إطار قانون حق المؤلف أم اختراع يمكن حمايته في إطار قانون الملكية الصناعية، فتحمى بقوانين براءة الاختراع ؟ أم سلعة يمكن حمايتها وفقا لأحكام العلامات التجارية ؟ انقسم الفقه في هذا الصدد إلى اتجاهين. الاتجاه الأول، يذهب فريق من الفقه إلى أن المنتجات المعلوماتية لا تتعلق بأشياء مادية في الغالب فهي أقرب إلى عالم المجردات حيث تمثل إنتاجا فكريا إبداعيا، مما يمكن معه إدراجه ضمن قانون الملكية الصناعية.أما الاتجاه الثاني يذهب إلى اعتبار البرامج المعلوماتية مصنفات ويمكن حمايتها بحق المؤلف.

وللإجابة على هذه التساؤلات سنحاول التفصيل في حماية المكونات غير المادية للحاسب الآلي والتي تتصف بالسرية باعتبارها معلومات إلكترونية سرية خلال نصوص

---

[1] وداد أحمد العيدوني، حماية الملكية الفكرية في البيئة الرقمية (برامج الحاسوب وقواعد البيانات نموذجا)، مداخلة ألقيت في المؤتمر السادس لجمعية المكتبات والمعلومات السعودية الموسوم"البيئة المعلومات الآمنة، المفاهيم والتشريعات والتطبيقات، المنعقد بمدينة الرياض خلال الفترة بين 06-07 أفريل 2010، ص 08.

[2] مثلا بالنسبة للمشرع الجزائري ألغى الأمر رقم 97-10 بالأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة.

[3] أوجبت الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية بودابست لسنة 2001 في المادة 10 منها بفقرتيها الأولى والثانية، الأولى خاصة بحق المؤلف والثانية بالحقوق المجاورة، وجوب اتخاذ تدابير تشريعية تجرم الإخلال أوالاعتداء على حق المؤلف أوالحقوق المجاورة وفقا لما تحدده القوانين الوطنية للدول الأعضاء مع اتفاقية برن لحماية المصنفات الأدبية والفنية واتفاقية تربس.

[4] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دار الثقافة للطباعة والنشر، 1999، ص 78.

الملكية الصناعية (مطلب أول) ومواجهة الجريمة المعلوماتية من خلال نصوص الملكية الأدبية والفنية (مطلب ثان) .

المطلب الأول

مواجهة الجريمة المعلوماتية من خلال قانون الملكية الصناعية

نصت المادة الأولى من اتفاقية باريس لحماية الملكية الصناعية[1] " تشمل حماية الملكية الصناعية براءات الاختراع ونماذج المنفعة والرسوم[2] و النماذج الصناعية والعلامات الصناعية أو التجارية وعلامات الخدمة والاسم التجاري وبيانات المصدر أو تسميات المنشأ وكذلك قمع المنافسة غير المشروعة..."[3]، وسنحاول التفصيل في أوجه الحماية الجزائية من خلال أحكام العلامة التجارية (فرع أول)،ثم من خلال أحكام براءة الاختراع (فرع ثان)وبعدها من خلال أحكام حماية التصاميم الشكلية للدوائر المتكاملة (فرع ثالث)كالتالي:

الفرع الأول

مواجهة الجريمة المعلوماتية من خلال أحكام العلامات التجارية[4]

[1] اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 20 مارس 1883 و المعدلة ببروكسل في 14 ديسمبر 1900 وواشنطن في 20 يونيو 1911 ولاهاي في 6 نوفمبر 1925 ولندن في 2 يونيو 1934 ولشبونة في 31 أكتوبر 1958 واستوكهولم في 14 يوليو 1967 والمنقحة في 28 سبتمبر 1989، فحوى الاتفاقية عن الموقع الالكتروني http://www.wipo.int/wipolex/ar/treaties/text.jsp?file_id=287555 تاريخ الدخول على الموقع 2017/03/02.

[2] عرفهما المشرع الجزائري بموجب الأمر 66-86 في مادته الأولى في فقرتها الأولى: "يعتبر رسما كل تركيب لخطوط أو ألوان يقصد به إعطاء مظهر خاص لشيء صناعي أو خاص بالصناعة التقليدية، ويعتبر نموذجا كل شكل قابل للتشكيل ومركب بالألوان أو بدونها، أو كل شيء صناعي أو خاص بالصناعة التقليدية يمكن استعماله لصنع وحدات أخرى، ويمتاز عن النماذج الأخرى بشكله الخارجي"، الأمر رقم 66-86 المؤرخ في 28 أفريل 1966 ، جريدة رسمية عدد 35 مؤرخة في 3 ماي 1966 ، ص 406.

[3] انضمت الجزائر إلى اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 20 مارس 1883 بموجب الأمر رقم 66-48 المؤرخ في 25 فبراير 1966 ، جريدة رسمية عدد 16 ، ص 198 ، كما صادقت الجزائر على نفس الاتفاقية بعد تعديلها لسنة 1976 في شهر يوليو بموجب الأمر رقم 75-02 المؤرخ في 9 يناير 1975 ، جريدة رسمية عدد ، ص .

[4] العلامة التجارية أو الصناعية وسيلة من وسائل المنافسة المشروعة بين المنتجين والتجار شانها شان بقية حقوق الملكية الصناعية، بحيث إذا اتخذ أحد التجار أو المنتجتين علامة تجارية أو صناعية معينة تمييزا لبضائعه أو منتجاته، فإنه يمنع على غيره من التجار أو المنتجين استخدام نفس هذه العلامة لتمييز سلع متماثلة أي أنها تتمتع بالحماية المقررة لحقوق الملكية الصناعية.

عرف المشرع الجزائري العلامة التجارية من خلال المادة الثانية من الأمر 06/03[1] على أنها" كل الرموز القابلة للتمثيل الخطي، لاسيما الكلمات بما فيها أسماء الأشخاص والأحرف والأرقام والرسومات أوالصور والأشكال المميزة للسلع أو توضيبها والألوان بمفردها أو مركبة، التي تستعمل كلها لتمييز سلع أو خدمات شخص طبيعي أو معنوي عن سلع وخدمات غيره"، كما نصت المادة السابعة من ذات الأمر على أن العلامة كي تحظى بالحماية يتعين أن تكون مشروعة أي غير مخالفة للنظام والآداب العامة. ويقصد بالعلامة كل إشارة أو دلالة مميزة يتخذها التاجر أو الصانع أو مقدم الخدمة شعارا لتمييز بضائعه أو منتجاته أو خدماته عن التي يملكها الآخرين.[2]

إضافة إلى أنه يشترط في العلامة التجارية كي يحميها القانون ضرورة تسجيلها أوإيداع طلب تسجيلها عند المصلحة المختصة وفي الجزائر هي المعهد الوطني الجزائري للملكية الصناعية، كما أنه يدرج ضمن الحماية القانونية العلامات التي تدخل ضمن التسجيلات الدولية الممتدة حمايتها إلى الجزائر في إطار الاتفاقيات الدولية التي انضمت إليها الجزائر وذلك طبقا للمادة 13 من المرسوم التنفيذي رقم 277/05 المحدد لكيفيات إيداع العلامات وتسجيلها[3].والسؤال المطروح هل تستفيد برامج الحاسب الآلي من الحماية الجنائية للعلامات التجارية ؟

نعلم أن كل برنامج يحمل اسما خاصا به، لذلك فقد عمد أصحاب البرامج إلى تسجيل هذا الاسم كعلامة تجارية للبرنامج، ولما كانت هذه الحماية قاصرة على الاسم دون المحتوى فقد لجا أصحاب البرامج إلى وضع الاسم مقترنا به[4].

ومن خلال ما سبق يتأكد لنا بأن برنامج الحاسوب تتمتع بالحماية القانونية التي تضبطها العلامات التجارية، غير أن ما يمكن المؤاخذة عليه هو أن مجال الحماية هذه سوف يظل محدودا وسوف يتقلص أمام اتساع مجال استخدام البرمجيات باتساع رقعة التجارة الالكترونية وقد رتب القانون جزاءات مدنية وجنائية في حالة المساس بالعلامة لسيما في جريمة التقليد للعلامة المسجلة أوكل ما من شأنه المساس بالحقوق الإستئثارية لصاحب

[1] الأمر 06/03 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات، جريدة رسمية عدد مؤرخة في 23 جويلية 200344، ص 22.

[2] http://www.startimes.com/?t=16525602 يوم الاطلاع على الموقع 2017/03/03.

[3] المرسوم التنفيذي رقم 05-277 المؤرخ في 2 أوت 2005 المحدد لكيفيات ايداع العلامات و تسجيلها، جريدة رسمية عدد 54 مؤرخة في 7 أوت 2005، ص 11.

[4] http://www.startimes.com/f.aspx?t=34350161 يوم الاطلاع على الموقع 2017/03/03.

العلامة وذلك من خلال المواد[1] من 26 إلى 33 من الأمر 03- 06 وهو ذات الأمر المنصوص عليه أيضا في اتفاقية تربس[2].

كما أنه يجدر بنا الإشارة إلى أن المشرع الجزائري اعتبر قاعدة البيانات ضمن المصنفات الفكرية التي تتمتع بالحماية القانونية وذلك وفقا للمادة 5 في فقرتها الثانية من الأمر رقم 03-05 والمتعلق بحقوق المؤلف والحقوق المجاورة[3]، وحيث أن قاعدة البيانات لا تدخل في نطاق المادة2 إذن لا تستفيد من الحماية القانونية بموجب أحكام العلامة التجارية من خلال الأمر 03-06.

الفرع الثاني

مواجهة الجريمة المعلوماتية من خلال نصوص براءة الاختراع [4]

عرفت المادة 02 من الأمر 07/03[5] الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية، وبشأن الشروط التي يجب توافرها في الاختراع فتتمثل

[1] تنص المادة 26 من الأملر 06/03 على أنه:" ....يعد جنحة تقليد لعلامة مسجلة كل عمل يمس بالحقوق الاستئثارية لعلامة قام به الغير خرقا لحقوق صاحب العلامة . يعد التقليد جريمة يعاقب عليها بالعقوبات المحددة في المواد من 27 إلى 33 أدناه".

[2] ربيحة زيدان، مرجع سابق، ص 97.

[3] الأمر رقم 05/03 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، جريدة رسمية عدد 44 المؤرخة في 23 جويلية 2003، ص 3.

[4] عرفت براءة الاختراع طبقا المادة الثانية من الأمر رقم 07/03 والمتعلق ببراءات الاختراع على:" وثيقة تسلم لحماية الاختراع " و بالتالي هي أنها شهادة تمنحها الدولة ويتمتع صاحبها بحق احتكار واستغلال اختراعه لمدة معينة وبمعايير معينة.

[5] الأمر 07/03 المؤرخ في 19 جويلية 2003 المتعلق ببراءة الاختراع، جريدة رسمية عدد 44 مؤرخة في 23 جويلية 2033، ص 27.

في شرط الابتكار،شرط الجدة، القابلية للتطبيق الصناعي والمشروعية[1]، وفي حال توافر هذه الشروط يتحصل المخترع على براءة الاختراع وهي الوثيقة التي تمنحها الدولة للمخترع فتخول له حق استغلال اختراعه والتمتع بالحماية القانونية المقررة لهذا الغرض وذلك لمدة محدودة وبشروط معينة والجهاز المانح لهذه الشهادة هو المعهد الجزائري لحماية الملكية الصناعية .

والسؤال المطروح هل تستفيد برامج الحاسب من الحماية الجزائية بواسطة براءات الاختراع ؟

إن التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءات الاختراع ومنهم المشرع الجزائري في المادة السابعة[2] في فقرتها السادسة من الأمر 07/03 ،حيث نص على ذلك صراحة في النص المذكور، وتم استبعاد برامج الحاسب الآلي من مجال الحماية بواسطة براءة الاختراع لأحد السببين هما[3] إما تجرد البرامج من أي طابع صناعي، أو صعوبة البحث في مدى جدة البرنامج لتقدير مدى استحقاق البرنامج للبراءة فليس من الهين توافر شرط الجدة في البرمجيات وليس من الهين إثبات توافر هذا الشرط، إذ يجب أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لتقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا، الأمر يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال الذي تتولى بحثه.

والجهة المكلفة بتقرير توافر شرط الجدة في الجزائر هي المعهد الجزائري لحماية الملكية الصناعية إذ يأخذ المشرع الجزائري بمبدأ الجدة المطلقة الذي يتنافى مع وجود أية سابقة دون تحديد زماني أو مكاني إنما يشرط أن تتوافر علانية هذه السابقة .

إضافة إلى التحفظ العملي لمنتجي برامج الحاسب على استعمال قوانين براءة الاختراع ، ويتمثل هذا التحفظ في الإجراءات المعقدة للحصول على البراءة والتكلفة العالية والمدد الطويلة التي يستغرقها هذا التسجيل، فعمر البرنامج قصير نسبيا لا يتعدى ثلاثة سنوات بينما قد تمتد إجراءات تسجيل البراءة مثل ذلك أو أكثر وعليه يمكن للغير الوصول إلى سر

---

[1] وذلك تطبيقا للمادة 3 من الأمر 07/03 و التي تنص على :" يمكن أن تحمى بواسطة براءة الاختراع، الاختراعات الجديدة والناتجة عن نشاط اختراعي والقابلة للتطبيق الصاناعي ...".وفصلت المواد من 4 إلى 6 في كل شرط من الشروط المذكورة في المادة 3.

[2] المادة 07 من الأمر 07/03 المتضمن براءة الاختراع " لا تعد من قبيل الاختراعات في مفهوم هذا الأمر ....-مجرد تقديم المعلومات - برامج الحاسوب ".

[3] http://www.startimes.com/f.aspx?t=34350161 يوم الاطلاع على الموقع 2015/11/15 .

البرنامج واستغلاله قبل صدور البراءة[1]، وفي هذه الحالة يعتبر الحصول عليه سرقة معلوماتية.

أما عن الحماية الجزائية لبراءة الاختراع فإن المادة 11 من الأمر 03-07 في الفقرة الثانية تعتبر سر التصنيع من الحقوق الاستئثارية ومنه ووفقا للمادة 56 من نفس الأمر فإن الاطلاع على سر التصنيع وتقليده من دون رضا صاحبه يعتبر جنحة تقليد و يعاقب عليه بموجب نص المادة 61 من نفس الأمر، فقط تجدر الإشارة أن هته الحماية يتمتع بها الاختراع هما هو الشأن بالنسبة لسر التصنيع بعد تسجيله وذلك وفقا للمادة 57 من ذات الأمر.معنى ذلك أن الحصول على معلومات سر التصنيع قبل التسجيل تعتبر جريمة سرقة معلوماتية أو تجسس معلوماتي أو أي جريمة من الجرائم المعلوماتي الماسة بالسر المعلوماتي حسب السلوك المادي المكون للجريمة و لا نطبق بشأنها الأمر03-07 السالف الذكر ونفس الشيء بالنسبة للاختراعات السرية المنصوص علها في المادة 19 من نفس الأمر[2].

الفرع الثالث

مواجهة الجريمة المعلوماتية من خلال قانون حماية التصاميم الشكلية للدوائر المتكاملة

عالج المشرع الجزائري أحكام الحماية القانونية للتصاميم الشكلية للدوائر المتكاملة من خلال الأمر 03-08 [3] حيث يقصد في مفهوم هذا الأمر بموجب المادة الثانية منه بالدائرة المتكاملة " منتوج في شكله النهائي أو في شكله الانتقالي يكون أحد عناصره على الأقل عنصرا نشيطا وكل الارتباطات أو جزءا منها هي جزء متكامل من جسم و/أو سطح لقطعة من مادة، ويكون مخصصا لأداء وظيفة إلكترونية"، أما عن التصميم الشكلي نظير الطبوغرافيا هو" كل ترتيب ثلاثي الأبعاد، مهما كانت الصيغة التي يظهر فيها، لعناصر

[1] http://www.droit-dz.com/forum/showthread.php?t=5955 يوم الاطلاع على الموقع 2015/11/15

[2] تنص المادة 19 من الأمر 03-07 المتعلق ببراءة الاختراع:" يمكن أن تعتبر سرية الاختراعات التي تهم الأمن الوطني والاختراعات ذات الأثر.....".

[3] الأمر رقم 03-08 المتعلق بحماية التصاميم الشكلية للدوائرالمتكاملة،مؤرخ في 19 يوليو 2003 ، جريدة رسمية عدد 44 مؤرخة في 23 يوليو 2003، ص 35.

يكون أحدها على الأقل عنصرا نشيطا ولكل وصلات دائرة متكاملة أو للبعض منها أو لمثل ذلك الترتيب الثلاثي الأبعاد المعد لدائرة متكاملة بغرض التصنيع"، و تطبيقا للمادة الرابعة من نفس الأمر فإن الحماية لا تمتد للمعلومات المشفرة، كل تصور أو طريقة أو تقنية ترتبط بالتصميم الشكلي ومنه فإن المعلومات السرية الالكترونية المرتبطة لا يحميها القانون بموجب الأمر 03-08.

كما أن المادة 35 من الأمر السالف الذكر تعتبر النسخ غير المشروع للتصميم الشكلي محل الحماية القانونية بموجب الأمر 03-08 جنحة تقليد و تترتب علها المسؤولية المدنية والجزائية، ويعاقب مرتكب جريمة التقليد بموجب المادة 36و 37 من الأمر 03-08.

المطلب الثاني

مواجهة الجريمة المعلوماتية من خلال قانون الملكية الأدبية والفنية

نصت المادة الثانية من اتفاقية برن على أنه "تشمل عبارة المصنفات "الأدبية و الفنية "كل انتاج في المجال الأدبي والعلمي والفني أيا كانت طريقة أو شكل التعبير عنه مثل الكتب وغيرها من المحررات....". فموضوع حق المؤلف هو" المصنف الأدبي والفني" وقد عرف المشرع الجزائري المصنف في المادة الأولى من الأمر 73-14[1] بأنه:" كل انتاج فكري مهما كان نوعه ونمطه وصورة تعبيره، ومهما كانت قيمته ومقصده وأن يخول لصاحبه حقا يسمى حق المؤلف يجري تحديده وحمايته طبقا لأحكام هذا الأمر"، ولم يعرفه في الأمر

03-05 السالف الذكر وإنما حدد في المادة الرابعة منه ما يعتبر على الخصوص مصنفا أدبيا أو فنيا كما اعتبر الأعمال المحددة في المادة الخامسة من نفس الأمر مصنفات محمية[2]، حيث حدد تلك المصنفات على سبيل المثال لا الحصر و ذلك من خلال صياغة نصي المادتين الرابعة و الخامسة خاصة بذكره مصطلح "على الخصوص".

[1] الأمر 73-14 المؤرخ في 03 أبريل 1973 المتضمن حق المؤلف ، الجريدة الرسمية عدد 29 المؤرخة في 10 أبريل 1973 ، ص 434.

[2] تنص المادة 4 من الأمر 03-05 على أنه :" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي :...." ، و المادة 5 منه تنص على أنه :" تعتبر أيضا مصنفا محميا الأعمال الآتية ....".

أما عن المصنف الرقمي فلم يعرفه المشرع الجزائري ولكن ذهبت بعض الآراء إلى تعريف المصنف الرقمى بأنه "أي عمل إبداعي من بيئة تكنولوجيا المعلومات"[1] وعرفه البعض الآخر أنه" مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات".[2]

ولتحديد مدى خضوع برامج الحاسب الآلي للحماية المقررة بمقتضى قانون حق المؤلف الجزائري وجب مناقشة نقطتين أساسيتين هما مدى اعتبار البرامج المعلوماتية كموضوع من موضوعات حق المؤلف(فرع أول)، ومدى إمكانية حماية البرامج المعلوماتية وفق نصوص جريمة التقليد(فرع ثان).

الفرع الأول

مدى اعتبار البرامج كموضوع من موضوعات حق المؤلف

قد ننظر للبرنامج المعلوماتي على أنه اختراع يحميه القانون بموجب قواعد حماية براءة الاختراع و عليه ظهر اتجاهان اتجاه يرى أن البرنامج ليس مصنفا مبتكرا لأنه من الصعب البحث عن الطابع الإبتكاري الشخصي للمؤلف، و اتجاه يرى أن برنامج الحاسب الآلي يتميز بالطابع الابتكاري[3]، ولكن جل التشريعات و من بينها المشرع الجزائري اعتبرت البرنامج مصنفا يحميه القانون بموجب قواعد حقوق المؤلف وعليه سنحاول فيما يلي التفصيل في أوجه الحماية بموجب النصوص التقليدية (أولا) والحديثة(ثانيا) لحق المؤلف.

أولا: الحماية بالنصوص التقليدية لحقوق المؤلف

نصت المادة الثانية من الأمر 73-14 [4] على المؤلفات التي تشملها حماية حقوق المؤلف بموجب الأمر السالف الذكر ، فعموم النص يفيد بأنها تشمل حماية المصنفات الجديدة التي لم

---

[1] عبد الرحمان ألطاف، تحديات حماية الملكية الفكرية للمصنفات الرقمية، عن الموقع الالكتروني http://www.shaimaaatalla.com/vb/showthread.php?t=3948، تاريخ الاطلاع على الموقع 2017/03/03.

[2] راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل حق المؤلف، مجلة التواصل لكلية الحقوق، جامعة 08 ماي 45، قالمة، عدد 34، جوان 2013، ص 137، منشور PDF على الموقع الالكتروني http://dpubma.univ-annaba.dz/?p=2766 يوم الاطلاع عليه 2017/03/04.

[3] أنظر خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء حماية الملكية الفكرية، دار الجامعة الجديدة للنشر، الأسكندرية، 2005، ص 94.

[4] نصت المادة 2 من الأمر 14/73 على أن:" المؤلفات التي تشملها حماية حق المؤلف هي ما يلي:
1- الكتب والمنشورات وغيرها من المؤلفات الأدبية والعلمية والفنية
2- المحاضرات والخطب والمواعظ والمؤلفات الأخرى المماثلة
3- مؤلفات الدراما والدراما الموسيقية
4- مؤلفات الألحان الإيقاعية والمسرحيات الإيمائية المعبر عنها كتابة أوبطريقة أخرى
5- القطع الموسيقية الصامتة أوالناطقة

تكن موجودة وقت صدور تلك النصوص، وهي لهذا السبب تسري على البرامج ، وإن كان يفضل بطبيعة الحال أن يتدخل المشرع وذلك بالنص صراحة على حماية مصنفات الحاسب الآلي من خلال حق المؤلف منعا لأي لبس.

فالمشرع الجزائري لم ينص صراحة على حماية البرامج المعلوماتية في إطار حق المؤلف آنذاك لكن رغم ذلك فإن بعض المختصين يرون إمكانية الحماية، بدليل الصياغة المرنة عند ذكر المصنفات المشمولة بالحماية.

فنص المادة 2 وإن كان لم يذكر صراحة برامج الحاسوب ضمن المصنفات المحمية لحماية حق المؤلف إلا أن صياغتها قد جاءت في صورة عامة، هذا التعداد ورد على سبيل المثال لا الحصر أي يمكن إسباغ الحماية على برامج الحاسوب كمصنفات فكرية ضمن عمومية نص المادة 2 الواردة في شأن المصنفات التقليدية المحمية.

وما يؤكد ذلك هو نص المادة 07 من الأمر 16/96 تخضع للإيداع القانوني للوثائق المطبوعة والصوتية والسمعية والبصرية أو التصويرية وبرامج الحاسوب بكل أنواعها أو قواعد المعطيات وذلك مهما تكن الدعامة التي تحملها وتقنية الإنتاج والنشر والتوزيع[1].

ثانيا: الحماية بالنصوص المعدلة لقوانين التأليف

بالنسبة للجزائر فقد اعترفت صراحة باعتبار برامج الحاسوب مصنفات أدبية وذلك من خلال الأمر 97-10[2] والذي تم تعديله حيث تعددت أسباب التعديل[3] وكان أهمها هو الانضمام إلى المنظمة العالمية للتجارة والمصادقة على اتفاقية برن وهو ما فعلته الجزائر بموجب المرسوم الرئاسي 97/ 341[4] إضافة إلى تبني أحكام اتفاق جوانب الملكية الفكرية

6- الأفلام السينمائية أو الأفلام المتحصل عليها بطريقة تشابه

7-أعمال التصوير والرسم والهندسة والنحت والنقش والطباعة الحجرية

8- مؤلفات الفنون التطبيقية

9- مؤلفات التصوير الشمسي والمؤلفات المتحصل عليها بطريقة مشابهة للتصوير الشمسي.

10- الصور والخرائط الجغرافية والتصميمات والرسوم والأعمال التشكيلية الخاصة بالجغرافيا والهندسة المعمارية أوالعلوم.

11- المؤلفات الفلكلورية وبصفة عامة المؤلفات التي هي جزء من التراث الثقافي التقليدي الجزائري ".

[1] الأمر 16/96 المؤرخ في 1996/07/02 الجريدة الرسمية رقم 341 في 1996/07/03.

[2] الأمر رقم 97-10 المؤرخ في 6 مارس 1997 المتعلق بحقوق المؤلف والحقوق المجاورة، جريدة رسمية عدد 13 مؤرخة في 12 مارس 1997 ص3.

[3] http://www.startimes.com/f.aspx?t=34350161 يوم 2015/11/15 .

[4] المرسوم الرئاسي رقم 97-341 المؤرخ في 13 سبتمبر 1997، و المتضمن انضمام الجمهورية الجزائرية الديمقراطية الشعبية، مع التحفظ، إلى اتفاقية برن لحماية المصنفات الأدبية والفنية المؤرخة في 9 سبتمبر 1886 والمتممة بباريس في 4 مايو 1896 و المعدلة ببرلين في 13 نوفمبر 1908 والمتممة ببرن في 20 مارس 1914 و المعدلة بروما في 2 يونيو 1928 وبروكسل في 26 يونيو 1949 واستوكهولم في 14 يوليو 1967 وباريس في 24 يوليو 1971 و المعدلة في 28 سبتمبر 1979، جريدة رسمية عدد 61 مؤرخة في 16 سبتمبر 1997، ص 8.

المتعلق بالتجارة وذلك نظرا لانعكاسات حقوق المؤلف على المستوى الاقتصادي ولضمان حماية المؤلفات الأجنبية في الخارج وقد ورد في نص المادة 8 من الاتفاق أن على الدول الأعضاء عند تعديل أو تبني قوانين اتخاذ التدابير المناسبة بشرط أن تكون متوافقة مع الاتفاق لتفادي الاستعمال المتعسف لحقوق الملكية الفكرية من طرف حائزي الحقوق واللجوء إلى تصرفات تمس بالتجارة أوتضر بعقود نقل التكنولوجيا .

ومن أهم ما ورد في اتفاق جوانب الملكية الفكرية المتعلقة بالتجارة هو ما ورد في نص المادة العاشرة من اتفاقية بودابست أن البرامج المعلوماتية سواء كانت في صورة برنامج مصدر أو الصورة المنقوشة فهي محمية على أساس أنها مصنفات أدبية.كما نصت على تجريم الاعتداءات على حق المؤلف والحقوق المجاورة إذا ارتكبت هذه الاعتداءات عن طريق نظام معلوماتي في نطاق تجاري، واستبعدت انتهاكات حقوق براءة الاختراع والعلامة التجارية.كما أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 جرمت الانتهاكات المتعلقة بحقوق المؤلف و الحقوق المجاورة من خلال المادة17 منها.

أما عن المشرع الجزائري[1] فبموجب المادة 4 من الأمر 05/03 اعتبر البرنامج مصنف أدبي حيث نصت على الآتي: " تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يلي: المصنفات الأدبية المكتوبة مثل المحاولات الأدبية، البحوث العلمية والتقنية، الروايات والقصص، القصائد الشعرية، برامج الحاسوب، المصنفات الشفوية مثل المحاضرات والخطب والمواعظ وباقي المصنفات التي ثماثلها...."

وأما عن العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية كانت مشددة بموجب المادة 151 الأمر 10/97، فإذ كان في السابق التعدي على الملكية الفكرية يخضع للمواد 394/390 من قانون العقوبات لكنها أخرجت بموجب الأمر 10/97 من مظلة قانون العقوبات وأصبح لها تجريم خاص إذ أن قانون العقوبات كان يقرر بموجب المادة 390 الغرامة كعقوبة للاعتداء على حق المؤلف بينما الأمر 10/97 يقرر عقوبتي الحبس والغرامة مع العلم أن هذا الأمر ألغي بموجب الأمر 05/03 والنص الساري المفعول هو المادة 151 من الأمر 05/03 والتي سيرد في سياق النص الأفعال التي تعتبر تقليدا ووصفه بالجنحة كما سيتم التفصيل أدناه.

كما أنه يجدر بنا الإشارة إلى أن المشرع الجزائري اعتبر قاعدة البيانات ضمن المصنفات الفكرية التي تتمتع بالحماية القانونية وذلك وفقا للمادة 5 في فقرتها الثانية من الأمر رقم 03-05 والمتعلق بحقوق المؤلف والحقوق المجاورة بالقول:" تعتبر أيضا

[1] أما بخصوص المشرع الفرنسي فهو كالعادة سباق في سن التشريعات حيث أنه أصدر القانون رقم 2009-1311 المؤرخ بتاريخ 28 أكتوبر 2009 المتعلق بالحماية الجنائية للملكية الأدبية والفنية على شبكة الأنترنت، والقانون 2012-278 المؤرخ في 01 مارس 2012 المتعلق بالاستغلال الرقمي للكتب غير المتوفرة الصادرة في القرن العشرين وغيرها من التشريعات ذات العلاقة.

مصنفات محمية الأعمال الآتية:....وقواعد البيانات"، وتعتبر قاعدة البيانات مصنف فكري ذو أهمية بالغة في الوقت الراهن نظرا لتطور الاستخدامات التكنولوجية المتعددة الأوجه، وأضفى عليه المشرع حماية قانونية مجاراة للتشريعات العالمية والاتفاقيات[1] الدولية.[2]

وتعرف قواعد البيانات من الناحية الفقهية بأنها" تجميع لكمية من المعلومات أو البيانات وعرضها بطريقة أو بأكثر تسهل عملية الاستفادة منها، لكونها موضوعة بطريقة منظمة بحيث يمكن الوصول إليها بسهولة وإجراء العمليات المختلفة عليها.[3]

وباعتبار أن البرامج المعلوماتية و قواعد البيانات هي مصنفات أدبية يحميها القانون بموجب الأمر 03-05فسنحاول فيما يلي التعرض للحماية الجزائية للبرامج بموجب قانون الملكية الأدبية دون الحديث عن قواعد البيانات و الحديث يقاس عليه باعتبارهما يقتضيان نفس الحماية.

الفرع الثاني

مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي لجرائم التقليد

للمؤلف على مصنفه حقان حق أدبي وحق مالي، فحقوق المؤلف المالية تتركز حول حق المؤلف في استغلال مصنفه بأي صورة من الصور، وحقوقه الأدبية تتركز حول ما يسمى بحق الأبوة بمعنى حق المؤلف في نسبة المصنف إليه. وهكذا يجرم الاعتداء على أي حق من الحقوق المؤلف السابقة، ويكفي الاعتداء على حق من هذه الحقوق لقيام جريمة التقليد، كما يجرم الاعتداء أيا كانت صورته وأيا كانت جسامته.

أولا: الاعتداء على الحق الأدبي لمؤلف البرنامج

الحق الأدبي للمؤلف يتمحور حول الحق في الأبوة ويقصد به " الحق في أن يذكر اسم المؤلف على كل نسخة عند وعه للتداول"[4]، ويتفرع عن هدا الأخير الحق في تقرير الكشف عن مصنفاته بالطريقة التي يراها مناسبة والحق الاستئثاري في تعديل مصنفه.و تتمثل الاعتداءات الواردة على هاذين الحقين في الكشف غير المشروع عن المصنف الأدبي والمساس بسلامة المصنف ، وسنحاول التطرق للكشف غير المشروع دون المساس بسلامة المصنف ذلك أننا نعالج هاته الجرائم باعتبارها ماسة بالسرية المعلوماتية .

---

[1] أوردت اتفاقية تربس الحماية القانونية لقاعدة البيانات في المادة 10 منها، في حين اتفاقية الويبو أي المنظمة العامية للملكية الفكرية في أوردت نفس الحماية في المادة 5 منها لقاعدة البيانات.

[2] زبيحة زيدان، مرجع سابق، ص 98.

[3] محمد حماد مهرج الهيثي، نطاق الحماية الجنائية للمصنفات الرقمية، دراسة مقارنة في القوانين العربية لحماية حق المؤلف، مجلة الشريعة والقانون، العدد 48، كلية الحقوق جامعة مملكة البحرين، أكتوبر 2011، ص 405.

[4] شحاتة غريب شلقامي، الملكية الفكرية في القوانين العربية، دار الجامعة الجدية الأسكندرية، 2009، ص 188.

فجريمة الكشف غير المشروع عن المصنف هي من الجرائم الماسة بسرية المصنف حيث أنه لمؤلف البرنامج الحق في اختيار الوقت والطريقة التي يتم بها إذاعة أو نشر برنامجه ، وعليه فالاعتداء يتمثل في أن يذاع أو ينشر هذا البرنامج في وقت غير الوقت الذي يراه مؤلفه مناسب وملائما أو بطريقة غير تلك التي يراها مناسبة له.

حتى أنه إذا اشترك في إعداد البرنامج المبتكر عدة أشخاص، فإن الحق في تقرير في البرنامج فإنه لا يجوز لأحدهم مباشرة حقوق إذاعة هذا البرنامج ويختلف هذا الأمر حسب حالات، فإذا كان لا يمكن الفصل بين نصيب كل من المشتركين في المؤلف منفردا فإن الكشف عنه يجب أن يتم ذلك بناءا على اتفاقهم جميعا فإن تصرف بمفرده يعد مرتكبا لجريمة التقليد.

أما إذا أمكن الفصل بين نصيب كل شريك، جاز لكل منهم أن يقرر إذاعة أو نشر نصيبه منفردا دون أن يعد معتديا على حقوق الشركاء الآخرين بشرط ألا يضر ذلك باستغلال المصنف المشترك.

ثانيا: الاعتداء على الحق المالي لمؤلف البرنامج

الحق المالي للمؤلف يتمحور حول الحق في استغلال المصنف، ويتخذ الاستغلال إحدى الصور التالية: النسخ، الاستعمال، الترجمة وذلك وفقا للمادة 27 من الأمر 03-05، والجدير بالذكر أننا نفصل في جريمة النسخ غير المشروع دون البقية للسبب نفسه المذكور أعلاه وهو أنها تعني مساسا بالسرية المعلوماتية.

فالنسخ غير المشروع يقع كاعتداء على حق مؤلف البرنامج في استغلال مصنفه في الحالة التي يقوم فيها الجاني بنسخ هذا البرنامج دون إذن مؤلفه أو نسخ عدد من النسخ أكثر مما هو متفق عليه بينهما.

والعبرة في تقدير وجود التقليد بأوجه الشبه لا بأوجه الاختلاف أي بنقاط التشابه بين البرنامجين وليس نقاط الاختلاف بينها ويدخل ذلك في نطاق السلطة التقديرية لمحكمة الموضوع دون رقابة عليها من محكمة النقض.

ويستثنى من صور النسخ المجرمة السابقة حالة النسخ للاستعمال الشخصي لمستأجر البرنامج أو مستعيره فيجوز مثلا أن ينسخ منه نسخة واحدة قبل رده إلى مؤلفه بعد انتهاء مدة الإيجار أو العارية بشرط أن يقتصر استخدام هذه النسخة على الاستعمال الشخصي فقط، فإذا لم يتوقف عند هذا الحد بأن كان الغرض من النسخ هو الاستغلال التجاري بأي صورة من الصور فإنه يكون مرتكبا لجريمة التقليد لاعتدائه على حق المؤلف في الاستغلال المالي لبرنامجه[1].

[1] محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الآلي،دار الثقافة للطباعة والنشر، بدون طبعة، سنة النشر 1987، ص142

وبعد اعتبار سلوكات انتهاك السرية المعلوماتية والجزم على اعتبارها ضمن نطاق التجريم لابد وأن تكون لهته الأفعال جزاءات مقررة لمرتكبيها تتمثل أساسا في العقوبات.

المبحث الثالث

العقوبات المقررة للجرائم الماسة بالسرية المعلوماتية في القانون الجزائري

تمثل العقوبات الآلية القانونية الوقائية والردعية التي من خلالها استطاعت التشريعات الجزائية الوقاية من حدوث جرائم تمس بالأسرار المعالجة آليا والتي سيعود الكشف عنها بأضرار قد تستهدف الفرد أو الاقتصاد أو حتى الأمن القومي وغيرها، والتي يحاول من خلالها – أي العقوبات – المشرع الجزائي تقرير الحماية لهته الأسرار، ولكن هل ستكون كافية أم لا ؟ وهل وحدها كافية لتحقيق الهدف المنشود ؟.

ربما تقرير العقوبات الجزائية لمختلف السلوكات الواقعة على الأسرار المعلوماتية وحده غير كاف ولكنه لا يمكن إنكار الدور الهام جدا الذي تلعبه النصوص العقابية السالفة الذكر والتي كرست عقوبات رادعة جعلت التفكير بالاعتداء على تلك الأسرار أمر في غاية الصعوبة، إضافة إلى أن الكثير من المشرعين ومنهم الجزائري من أعادوا النظر حتى في المسألة الإجرائية حيث استحدثت نصوص إجرائية تصديا لوقوع الجرائم المعلوماتية خاصة الماسة بالأنظمة المعلوماتية.

فالمشرع الجزائري كغيره من المشرعين الذين تيقضوا لإشكالية التصدي للجرائم المعلوماتية بنصوص عقابية مستحدثة نظرا لطبيعة الجرائم المعلوماتية ووجود العالم الافتراضي الذي سهل من ارتكابها وصعب المهمة على رجال القانون حتى لا يفلت أي مجرم من العقاب وكان مضمون العقوبات المتعلقة بالجرائم الماسة بالسرية المعلوماتية كالتالي :

المطلب الأول

العقوبات المقررة للجرائم الواقعة على الأسرار المعلوماتية في نطاق قانون العقوبات

تعتبر العقوبة الصيغة الأولى للجزاء الجنائي، وتعرف بأنها إنقاص أو حرمان من كل أو بعض الحقوق الشخصية يتضمن إيلاما يصيب مرتكب السلوك الإجرامي كنتيجة قانونية،

ويتم توقيعها بمعرفة جهة قضائية جزائية وفق إجراءات خاصة.[1] وأخذ المشرع الجزائري إلى تقسيم العقوبات إلى عقوبات أصلية وعقوبات تكميلية.

وضمن قانون العقوبات حدد المشرع الجزائري لكل سلوك تم تجريمه عقوبة خاصة به حسب درجة الجريمة من جناية إلى جنحة أو مخالفة، وهو نفس الأمر بالنسبة للجرائم الماسة بالأسرار المعلوماتية التي اعتبرها المشرع الجزائري في مجملها جنح.

الفرع الأول

العقوبات المقررة للشخص الطبيعي

نصت المادة الرابعة من قانون العقوبات في فقرتها الأولى على "يكون جزاء الجرائم بتطبيق العقوبات وتكون الوقاية منها باتخاد تدابير الأمن"، ومن خلال النص نستنتج أن ثمة نوعين من الجزاءات تطبق على الشخص الطبيعي هي العقوبات كجزاء حقيقي وتدبير الأمن ذات الهدف الوقائي من الخطورة الاجرامية.

وبالنظر إلى النصوص العقابية المقررة للجرائم الواقعة على الأسرار المعلوماتية فهي تتضمن مجموعة من العقوبات ذات الصنفين الأصلية والتكميلية .

أولا: العقوبات الأصلية

وهي كل عقوبة لا توقع إلا إذا نطق بها القاضي وحدها وحدد نوعها ومقدارها وهي السجن أو الحبس أو الغرامة المالية [2]وممكن أن تكون موقوفة النفاذ تطبيقا للمادة 592 من قانون الإجراءات الجزائية فضلا عن إمكانية تطبيق العمل للنفع العام بدلا من الحبس طبقا للمادة 5 مكرر من قانون العقوبات.

ويكون للقاي سلطة تقديرية بين الحكم بين الحد الأدنى والأقصى للعقوبة، كما لا يوجد ما يمنع القاضي عن رغبته في منح أقصى ظروف التخفيف بأن يجعل عقوبة الحبس يوم واحد طبقا للمادة 53 من قانون العقوبات، وتتمثل العقوبات الأصلية في العقوبة السالبة للحرية والمالية[3] وعقوبة العمل للنفع العام[4].

---

[1] عبد القادر عدو، مبادئ قانون العقوبات الجزائري، القسم العام، الطبعة الثانية، دار هومة للطباعة والنشر والتوزيع، 2013، ص 363.

[2] عبد الله سليمان، شرح قانون العقوبات الجزائري، الجزء الأزل، دار الهدى للنشر، عين ميلة، الجزائر، دون سنة طبع، ص 429.

[3] يقصد بالعقوبة المالية الحكم قضائيا على الجاني بدفع المبالغ المحكوم بها عليه وهي تصيب ذمته المالية كجزاء على الإعتداء على مصالح قدر لها المشرع الحماية وحظر العدوان عليها، عن محمود نجيب حسني، شرح قانون العقوبات، القسم العام، دار النهضة العربية،مصر، بند 823، 1989، ص 708.

[4] استحدث المشرع الجزائري بموجب القانون 09-01المؤرخ في 2009/05/25 المعدل والمتمم لقانون العقوبات عقوبة العمل للنفع العام ووضع لها شروطا بموجب أحكام المادة 5 مكرر1 حيث يمكن للجهة القضائية أن تستبدل عقوبة الحبس المنطوق بها بقيام المحكوم عليه بعمل للنفع العام بدون أجر، لمدة تتراوح بين أربعين ساعة وستمائة ساعة بحساب ساعتين عن كل يوم حبس، في أجل أقصاه 18 شهرا حسب الشروط المذكورة في النص .

وسنحاول فيما يلي التفصيل في العقوبات **البسيطة** المقررة للاعتداء على الجرائم الماسة بالأسرار المعلوماتية حيث سنتطرق في هذا المقام إلى العقوبات المقررة لمختلف السلوكات التجريمية التي كانت محلها الأسرار المعلوماتية طبقا لقانون الجزائري كالتالي :

1-عقوبة الدخول أو البقاء غير المصرح بهما :

العقوبة المقررة لهذه الأفعال بموجب المادة 394 مكرر من قانون العقوبات هي الحبس من (3) أشهر إلى سنة والغرامة من 50000 دج إلى 100000 دج .

وتجدر الإشارة أن المشرع الجزائري اعتبر أنها العقوبة الأنسب لهذه الأفعال وما لها من خطورة كبيرة على سرية المعلومات المعالجة آليا، الأمر الذي جعل الدخول إليها وانتهاك سريتها أمر يعرض أصحابها للأضرار فادحة، خاصة إذا تعلقت بشركات أو إدارات تعتمد في تسير شؤونها على نظم المعالجة الآلية.

2-العقوبات المقررة لجريمة التعامل في معلومات غير مشروعة :

هي الحبس من شهرين (2) إلى ثلاث سنوات والغرامة من 1000000 دج5000000 دج وذلك بموجب المادة 394 مكرر 2 في الفقرة (1) وهي كالتالي : " يعاب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1000000 دج إلى 5000000 دج كل من ..." .

3-العقوبات المقررة للاعتراض غير القانوني للبيانات (التجسس المعلوماتي)

عاقب المشرع الجزائري على التجسس المعلوماتي العسكري بالإعدام فقط من خلال نص المادة 63 من قانون العقوبات، وما على المشرع الجزائري فعله وهو تخصيص نص خاص باعتراض البيانات المعالجة آليا بجميع أنواعها مع تعديل المادة 63 لتتماشى مع النص الجديد والنص على العقوبات المقررة .

4-العقوبات المقررة لمنتهك البريد الالكتروني :

يعاقب من شهر واحد(1) إلى سنة(1) وبغرامة من 25000 دج إلى 100000 دج أو بإحدى هاتين العقوبتين، ودلك وفقا لنص المادة 303 من قانون العقوبات.

5-العقوبات المقررة لمنتهك المحادثات الشخصية الالكترونية:

العقوبة هي الحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 50000 دج إلى 300000 دج ودلك من خلال المادة 303 مكرر من قانون العقوبات.

6- إفشاء الأسرار المعلوماتية:

يعاقب الطبيب والجراح و.... مفشي السر المهني في غير الحالات المسموح بدلك قانونا والمصرح لهم بدلك بالحبس من شهر إلى ستة أشهر وبغرامة من 20000 دج إلى

100000 دج، وذلك وفقا للمادة 301 من قانون العقوبات.كما يعاقب العامل في المؤسسة مفشي السر أوحتى الشروع في ذلك كالتالي:

أ- إلى جزائريين أوأجانب يقيمون في بلد أجنبي: بالحبس من سنتين إلى خمس سنوات وبغرامة من 20000 دج إلى 100000 دج. الفقرة الأولى من المادة 302 من قانون العقوبات .

ب- إلى جزائريين يقيمون بالجزائر الحبس من ثلاثة أشهر إلى سنتين وبغرامة من 20000 دج إلى 100000 دج.الفقرة الثانية من المادة 302 من قانون العقوبات .

ت- ويجب لحكم بالحد الأقصى للعقوبتين في الفقرتين 1 و2 إذا تعلقت الأسرار بصناعة أسلحة أوذخائر حربية مملوكة للدولة الجزائرية.

ث- وفي جميع الحالات المنصوص عليها في المادة 302 السابق ذكرها في الفقرات أ ، ب ، ت يجوز علاوة على تلك العقوبات الحكم على الجاني بالحرمان من حق أوأكثر من الحقوق الواردة في المادة 14 من قانون العقوبات الجزائري لمدة سنة على الأقل وخمس سنوات على الأكثر.[1]

3-السرقة المعلوماتية:

المادة 350 من قانون العقوبات بنصها كل من اختلس شيئا مملوكا للغير هي لم تحدد صراحة أي نوع من الأشياء وفي غياب النص الخاص بالسرقة المعلوماتية وجدنا أنفسنا مضطرين باعتبارها تقصد حتى المعلومات الالكترونية ومنه يعاقب سارقها بما تنص عليه المادة وهوالحبس من سنة إلى خمس سنوات وبغرامة من 100000 دج إلى 500000 دج.

ويجوز أن يحكم على الجاني علاوة على ذلك بالحرمان من حق أوأكثر من الحقوق الواردة في المادة 9 مكرر 1 لمدة سنة على الأقل وخمس سنوات على الأكثر، وبالمنع من الإقامة طبقا للشروط المنصوص عليها في المادتين 12 و13 من قانون العقوبات.

وبعد التطرق للعقوبات البسيطة، سنحاول التطرق **لظروف التشديد** فيما يتعلق بالجرائم ضد الواقعة على الأسرار المعلوماتية، حيث يقع على عاتق المشرع عند تحديده لشق الجزاء الجنائي من القاعدة الجنائية، عدة واجبات منها ضرورة أن يراعي المشرع عند إنشاءه للجزاء تدرجه بحسب ظروف كل جاني. فيفترض تطبيق نص معين عقوبته أشد أو أخف من العقوبة العادية المقررة لنفس الفعل إذا وقع في ظروف معينة، أومن جناة محددين مثل ظروف لتشديد، وأعذار التخفيف، والأعذار المعفية من العقاب، ويتمثل التفريد التشريعي أن يدخل المشرع في اعتباره عند وضع الجزاءات المقررة للجرائم المختلفة؛ ظروف الجريمة المرتكبة من ناحية، وظروف الجاني من ناحية أخرى أو تدخل المشرع

[1] المادة 14 من قانون العقوبات الجزائري تنص على الآتي :" يجوز للمحكمة ....حق أوأكثر من الحقوق الوطنية المذكورة في المادة 9 مكرر 1 ...." والمادة 9 مكرر 1 تنص على الآتي: " يتمثل الحران من ممارسة الحقوق الوطنية والمدنية والعائلية في : العزل أوالإقصاء من جميع الوظائف .....".

بغية تنظيم تفريد العقوبة[1]، ويعرف التفريد التشريعي بأنه التفريد الذي يتولاه المشرع ذاته محاولاً به أن يجعل من العقوبة جزاءاً متناسباً ومتلائماً مع الخطورة المادية للجريمة من ناحية، بما تتضمنه الجريمة من خطر على المجتمع، أو ما يمكن أن تحدث به من ضررٍ مع الظروف الشخصية للجاني الذي يمكن له أن يتوقعها أو يتنبأ بها وقت تحديده للجريمة والعقوبة، أي لحظة وضع نص التجريم والعقاب، وذلك من ناحية ثانية، فالمشرع هو الذي يحدد مبدئيا العقوبة تطبيقا لمبدأ شرعية الجرائم والعقوبات، إلا أنه في كثير من الحالات لا يستطيع القيام بذلك بشكل حصري ومحدد، فإذا كان وقت وضع النص التشريعي يقدر خطورة الجريمة؛ ويحدد تبعاً لها العقوبة الملائمة، إلا أنه على يقين بأن مرتكب هذه الجريمة ليس دائماً على هذه الدرجة من الخطورة الإجرامية، حيث أن ظروف وملابسات ارتكاب الجريمة تختلف من مجرم إلى مجرم أخر ارتكب نفس الجرم، وغالبا ما يضع المشرع عقوبتين للفعل كالإعدام أوالسجن المؤبد في بعض الجنايات، والحبس أو الغرامة أوكليهما في بعض الجنح، كما يضع المشرع عقوبة متراوحة بين حدين أدنى وأقصى، ويترك للقاضي سلطة تقديرية تتناسب ووقائع الدعوى وحيث يرى المشرع في بعض الحالات أن العقوبة التي رصدها للجريمة لا تتلاءم مع ظروف ارتكابها، سواءً ما تعلق منها بالجريمة ذاتها أو بمرتكبها، ويرى أن هذه الظروف تستدعي إما تخفيف العقاب؛ وإما تشديده. فينص على ذلك وقد يكون التخفيف أو التشديد وجوبا؛ أي يلتزم القاضي به دون أن يكون له أي سلطة تقديرية في هذا الشأن، وقد يكون اختياريا للقاضي. ونكون أمام التفريد التشريعي في الحالة الأولى التي يكون التشديد والتخفيف وجوبيا[2].

ظروف التشديد محددة في القانون على سبيل الحصر، وبالنسبة لجرائم معينة (جنايات وجنح)، بحيث يؤدي توافرها إلى تشديد عقوبتها ورفعها عن الحد الأقصى المقرر لها قانوناً، وهي عبارة عن ملابسات رافقت ارتكاب الجريمة قدر المشرع أن توافرها يوجب مبدئيا رفع العقوبة المقررة للجريمة التي ارتكبت في ظروف عادية[3]، وهو الأمر الذي رآه المشرع في جرائم نظم المعالجة الآلية للمعلومات والتشديد فيها كان إما بالنظر إلى صفة المجني عليه أو بالنظر للنتيجة المترتبة كالتالي :

1-التشديد على أساس صفة المجني عليه :

تتعلق الأسرار محل الحماية بالأفراد أو بالدولة وتولى هذه الأخيرة اهتماما كبيرا عند أغلب التشريعات إضافة إلى أن هناك من المشرعين من يجرم الاعتداء على المعلومات

[1] هناك نوع آخر من تفريد العقاب هوتفريد العقاب القضائي والمقصود منه هوإعطاء القاضي سلطة تقديرية واسعة عند تسليط العقاب لاختيار العقوبة المناسبة في نوعها ومقدارها للحالة الماثلة أمامه، ومن هذا المنطلق فإن القاضي يلعب دوراً هاماً في تفريد العقوبة بموجب سلطته التقديرية الواسعة والآليات التي منحهما له المشرع، عن ايهاب محمد الروسان، التفريد القضائي للعقوبة في 24 سبتمبر 2010، عن http://ar.jurispedia.org/ بتاريخ 2014/20/24.

[2] http://www.startimes.com/. يوم 2014/10/24

[3] http://www.startimes.com/ يوم 2014/10/24.

الإلكترونية السرية المتعلقة بمصالح الدولة فقط [1]، بينما المشرع الجزائري أخذ بحماية المعلومات الإلكترونية السرية بمختلف أنواعها بغض النظر عن الجهات التي تنتمي إليها، ولكنه شدد العقوبة إذا ما تم العدوان على المعلومات التي تتعلق بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام نظرا للخطورة البالغة التي تنجم عن تلك الاعتداءات وهذا ما نصت عليه المادة 394 مكرر كالتالي : ‹‹ تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ودون الإخلال بتطبيق عقوبات أشد ›› .والملاحظ من النص أن المشرع الجزائري اعتبر صفة المجني عليه ظرفا مشددا، إذ تشدد العقوبة لتصبح ضعف العقوبة المقررة لجرائم الاعتداء على النظم التابعة للأفراد العاديين وأشخاص القانون الخاص، إضافة إلى ذلك تضاعف الغرامة مرتين إذا ارتكبت الجرائم السالفة الذكر إذا ما ارتكبت من شخص معنوي على إحدى الجهات العامة، إذ تضاعف إلى خمس مرات كما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من طرف شخص معنوي ومن تم يضاعف ذلك لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فجموع ذلك هو مضاعفة الغرامة إلى عشر أضعاف كما هو مقرر على الشخص العادي.

2-التشديد على أساس النتيجة المترتبة :

وهما النتيجتين المنصوص عليهما في الفقرتين 2 و3 من المادة 394 مكرر والتي تنص على أنه : ‹‹ تضاعف العقوبة إذا ترتب على ذلك حذف أوتغيير لمعطيات المنظومة ››.

" وإذا ترتب على الأفعال المذكورة أعلاه تخريب اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر سنتين والغرامة من 50000دج إلى 150000دج"

والجدير بالذكر في هذه المسألة أنه كان لابد على المشرع أن يعتبر وجود الحماية الفنية للنظام المعلوماتي كظرف تشديد.

ثانيا: العقوبات التكميلية

يقدر المشرع في العديد من الحالات عدم كفاية العقوبة الأصلية التي قررها كجزاء على اقتراف الجريمة في ردع الجاني أو في حماية المصلحة التي قرر حمايتها، فيأتي بالعديد من العقوبات الفرعية لتدعيم الحماية المقررة للمصلحة المعنية[2]، فالعقوبات التكميلية هي عقوبات تضاف إلى العقوبات الأصلية، وقد حددها المشرع في نص المادة 09 المعدلة بموجب القانون 06-23 المعدل والمتمم لقانون العقوبات، وإن كانت هذه العقوبات مرتبطة

[1] كالقانون الفدرالي الأمريكي في المادة 1030 (أ) (3) منه والأمر نفسه في قانون استخدام الحاسبات الآلية في اليابان وغيرها.

[2] حنان طلعت أبو العز، الحماية الجنائية لحقوق المؤلف، الطبعة الأولى، دراسة مقارنة، دار النهضة العربية، مصر، 2007، ص 147.

بالعقوبة الأصلية ، إلا أنها لا يحكم بها على المحكوم عليه بقوة القانون،إذ لا توقع إلا بالنطق بها، وتتمثل هذه العقوبات في المصادرة والغلق ونشر الحكم وستتم مناقشتها كالتالي :

أ-المصادرة : يقصد بالمصادرة تجريد الشخص من ملكية مال أومن حيازة شيء معين له صلة بجريمة وقعت أو يخشى وقوعها، ثم إضافتها إلى جانب الدولة بلا مقابل بناء على حكم من القضاء الجنائي[1]كما عرفها المشرع الجزائري من خلال المادة 15 من قانون العقوبات[2] .فأحيانا العقوبات الأصلية لا تكون كافية كما هو الشأن بالنسبة للجرائم الماسة بالسرية المعلوماتية، إذ أنه من الممكن أن يرتكب الجاني في هاته الجرائم جرائم أخرى بحيازته لبعض الوسائل التي ارتكب بها جرائمه ومنه يعاود ارتكاب جرائم أخرى تمس السرية أو سلامة أو وفرة المعلومات لهذا يكون بالنسبة لهؤلاء من الضروري اتخاذ تدابير عملية لمنع وقع جريمة أخرى من نفس الشخص ويتحقق ذلك بمصادرة تلك الوسائل وهذا ما نصت عليه المادة 394 مكرر6 كالتالي: ‹‹ مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة ››والملاحظ على النص أن المشرع أخذ بعين الاعتبار حسن النية وبذلك يكون قد انسجم مع مبدأ الشرعية .

ب-الغلق:فإلى جانب عقوبة المصادرة نص المشرع على عقوبة تكميلية وجوبية أخرى هي الغلق وذلك بموجب المادة 394 مكرر6 كما يلي : ‹‹...مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها››، ويكون بذلك المشرع جعل لعقوبة الغلق محلين هما المواقع محل ارتكاب الجريمة ومحل أو مكان الاستغلال.

ولكن المادة لم تنص على مدة الغلق وبالتالي فإننا نرجع إلى القواعد العامة لقانون العقوبات حيث تكون مؤبدة أو مؤقتة وذلك وفقا للمادة 16 مكرر1 في فقرتها الأولى بقولها: " يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي ارتكبت الجريمة بمناسبته ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة لا تزيد عن عشر سنوات في حالة الإدانة لارتكاب جناية أو خمس سنوات في حالة الإدانة لارتكاب جنحة ...".

الفرع الثاني
العقوبات المقررة للشخص المعنوي

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، 2006، ص 230.

[2] تنص المادة 15 على أن " المصادرة هي الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو ما يعادل قيمتها عند الإقتضاء.

تبنى قانون العقوبات الجزائري مبدأ المسؤولية الجزائية للأشخاص المعنوية بموجب القانون 04-15 في نص المادة 18 مكرر ليعزز ذلك بالقانون رقم 23 لسنة 2006 بنص المادة 51 مكرر وفي مضمون هذا النص استثنى المشرع الأشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية وعلى رأسها الدولة، ومن خلال استقراء المادة 18 مكرر فالعقوبات التي تطبق على الشخص المعنوي في الجنايات والجنح كالتالي :

1-الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة[1].

2-واحدة أو أكثر من العقوبات التكميلية الآتية:حل الشخص المعنوي، غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات، الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات،المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس سنوات، مصادرة الشيء الذي استعمل في ارتكاب الجريمة أونتج عنها، نشر وتعليق حكم الإدانة،الوضع تحت التصرف لمدة لا تتجاوز خمس سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى جريمة أو الذي ارتكبت الجريمة بمناسبته.

ومما تجدر الإشارة إليه في هذا المقام أن هذه العقوبات ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية فحسب، بل تقع على كل الجرائم التي يرتكبها الشخص المعنوي، بينما ما يتعلق بالجرائم ضد الأنظمة المعلوماتية المحددة في المواد من 394 مكرر وما بعدها فإن الغرامة المطابقة على هذا الأخير هي 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وذلك تطبيقا للمادة 394 مكرر 4 من قانون العقوبات الجزائري.

حيث أن المشرع الجزائري شدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية وهي الطائفة التي تنتمي إليها جل جرائم الدراسة، إذ نصت المادة 394 مكرر 4 بمضاعفة قيمة الغرامة 5 أضعاف ما قررته للشخص الطبيعي ونصت على الآتي : "... بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة فتضاعف الغرامة في التشريع الجزائري مرتين، إذ تضاعف إلى خمس (5) مرات عما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من شخص معنوي ، وثم يضاعف ذلك إلى ضعفين لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة إلى عشر (10) أضعاف عما هو مقرر على الشخص العادي.

[1] نص المشرع الجزائري على نوعين من العقوبات المطبقة على الشخص المعنوي هي الغرامة كعقوبة أصلية و العقوبات التكميلية.

الفرع الثالث

عقوبة الاتفاق الجنائي والشروع

تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي[1] بنص المادة 394 مكرر 5 ، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار، حيث تنص المادة 394 مكرر 5 من قانون العقوبات:" كل من شارك في مجموعة أوفي اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية يعاقب بالعقوبات المقررة بالجريمة ذاتها ".

إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أوفي اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات كما أن المشرع ورغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إطار اتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

وشروط المعاقبة على الاتفاق الجنائي بمن استخلاصها من نص المادة 394 مكرر5 من قانون العقوبات والتي هي، مجموعة أو اتفاق، بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية، وتجسيد هذا التحضير بفعل مادي، مع فعل المشاركة في هذا الاتفاق، إضافة إلى القصد الجنائي.

وبالنسبة للمجموعة أو الاتفاق، يستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي كما يستوي. أن يعرف أشخاص الاتفاق بعضهم بعضا كما في العصابة أم تكون مجرد مجموعة من الأشخاص، لا يعرف أحدهم الأخر من قبل ولكن اتفقوا فيما بينهم على القيام بالنشاط الإجرامي،المهم أن يتم الاتفاق بين شخصين على الأقل، فإذا ارتكب الشخص العمل التحضيري المادي شخص واحد بمفرده أو بمعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر.

وتكاثف الجهود لا يكفي بل يجب أن يكون بهذه تحضير جريمة من جرائم الماسة بالأنظمة المعلوماتية بمعنى أن الاتفاق يجب أن يكون له هدف إجرامي منذ البداية فعليه فإنشاء نادي للمعلوماتية بهدف التكوين أو التسلية العلمية يحول نشاطه لأهداف إجرامية لا يقع تحت طائلة المادة 394 مكرر 5 من قانون العقوبات .

[1] نصت عليه المادة 11 من الاتفاقية الدولية للإجرام ألمعلوماتي

فالجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي الجنح الماسة بالأنظمة المعلوماتية وعليه لا يعاقب استنادا لهذا النص الاتفاق بهدف ارتكاب جنحة تقليد البرامج المعاقب عليها بنصوص حق المؤلف وحقوق المجاورة.

والتحضير لا يكفي بل يتم تجسيده بفعل مادي، الأمر يتعلق بأعمال تحضيرية مثل تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان على كلمة مرور أو رمز الدخول وغيرها.

ففعل المشاركة في الاتفاق إذ أن المجرم بنص المادة 394 مكرر5 ليس الاتفاق وإنما المشاركة من طرف شخص طبيعي أو معنوي فبمجرد الانضمام إلى الاتفاق غير كافي بل يجب توافر فعل إيجابي للمشاركة.

وتوافر القصد الجنائي لدى أعضاء الجماعة والمتمثل في توافر العلم لدى كل منهم بأنه عضو في الجماعة الإجرامية وأن تتجه إرادة كل عضو أي تحقيق نشاط إجرامي معين وهو العمل التحضيري.

بينما عن **عقوبة الشروع** في الجريمة فالشروع يراد به في الجريمة ذلك السلوك الذي يهدف به صاحبه إلى ارتكاب جريمة معينة كانت لتقع بالفعل لولا تدخل عامل خارج عن إرادة الفاعل في اللحظة الأخيرة دون وقوعها[1].

تبناه المشرع الجزائري في المادة 394 مكرر 7 من قانون العقوبات، فالجرائم الماسة بالأنظمة المعلوماتية لها وصف جنحي ولا عقاب على الشروع في الجنح إلا بنص، حيث أنه نصت المادة 394 مكرر7 قانون العقوبات:" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "[2].

ويبدو من خلال هذا النص أن رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في أحد الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر5 من قانون العقوبات أيضا مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي أيضا.

المطلب الثاني

العقوبات المقررة للجرائم الواقعة على الأسرار المعلوماتية

[1] رمسيس بهنام، النظرية العامة للقانون الجنائي، منشأة المعارف، الإسكندرية، بدون طبعة، سنة النشر 1995، ص 583.

[2] اتفاقية بودابست لسنة 2001 المتعلقة بالجريمة المعلوماتية تبنت الشروع أيضا في المادة 11 في الفقرة الثانية من الفصل الخامس منها والمعنون بأشكال أخرى للمسؤولية والجزاءات.

خارج نطاق قانون العقوبات[1]

سنحاول التطرق إلى العقوبات المقررة للمعتدي على المعلومات تطبيقا للأمر المتعلق بحقوق المؤلف والحقوق المجاورة الأمر رقم 05/03 ،الأمر 03-06 المتعلق بالعلامات والأمر 03-07 المتعلق ببراءات الاختراع .

بداية تنص المادة 151 من الأمر 05/03 على أنه:"يعد مرتكبا لجنحة التقليد كل من يرتكب الأعمال التالية: الكشف غير المشروع للمصنف.....استنساخ مصنف.....". كما نصت المادة 152 من ذات الأمر على أنه :" يعد مرتكبا لجنحة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر...من يبلغ المصنف أو الأداء عن طريق التمثيل أو الأداء العلني أو البث الإذاعي السمعي أو البصري أو التوزيع بواسطة الكابل أو أية وسيلة نقل أخرى للإشارات تحمل أصواتا أو صورا و أصواتا وبأية منظومة معالجة معلوماتية."

وأما عن العقوبة المقررة لهذه الجرائم منصوص عليها في المادة 153 من نفس الأمر حيث أنه للقاضي أن يطبق كعقوبة أصلية الحبس من 06 أشهر إلى 03 سنوات وغرامة قدرها 500 ألف دينار جزائري إلى 01 مليون دينار جزائري سواء تمت عملية النشر في الجزائر أوفي الخارج.إضافة إلى أنه بموجب المادة 154 من نفس الأمر يعد مرتكبا للجنحة المنصوص عليه في المادة 151 أعلاه كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف و يعاقب بالعقوبة المحددة في 152.

وللقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لإقساط الإيرادات المحصلة من الاستغلال غير المشروع للمصنف (البرنامج) وكل النسخ المقلدة والمصادرة تدبير تكميلي[2] ، وتأمر الجهة القضائية بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك وكذلك الإيرادات موضوع المصادرة للمؤلف أو أي مالك حقوق أخر لتكون عند الحاجة بمثابة تعويض.[3]

و يمكن للقاضي إن يضاعف العقوبات المقررة وذلك في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى 06 أشهر، وإذا اقتضى الحال تقرير الغلق النهائي[4]، كما يمكن للجهة القضائية بناء على طلب الرف المدني أن تأمر بنشر حكم الإدانة[5] .

---

[1] المقصود بالعقوبات المقررة للجرائم الماسة بالأسرار خارج نطاق قانون العقوبات هو العقوبات المقررة لجريمتي الكشف والنسخ غير المشروع وفقا لقوانين الملكية الأدبية والفكرية.

[2] تطبيقا للمادة 157 من الأمر 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة السالف الذكر.

[3] وفقا للمادة 159 من الأمر 03-05.

[4] وذلك وفقا للمادة 156 من الأمر 03-05.

[5] وفقا للمادة 158 من الأمر 03-05.

وتجدر الإشارة إلى إجراء هام يتم أثره اكتشاف جريمة التقليد وهو ما يسمى بالحجز الناتج عن التقليد يمكن بواسطته لمؤلف البرنامج المحمي أو ذوي حقوقه المطالبة بحجز الوثائق والنسخ الناتجة عن الاستنساخ غير المشروع أو التقليد، وذلك حتى في غياب ترخيص قضائي أو أنه إيقاف لأية عملة جارية ترمي إلى الاستنساخ غير المشروع للبرنامج أو حجز الدعائم المقلدة والإيرادات المتولدة عن الاستغلال غير المشروع للمصنفات .

كما نصت المادة 154 من نفس الأمر على أن المشاركة في ارتكاب جرائم التقليد المنصوص عليها في المواد 151 و152 هي نفسها المقررة للفاعل الأصلي.

بينما تنص المادة 32 من الأمر 03-06 المتعلق بالعلامات " كل شخص ارتكب جنحة تقليد يعاقب بالحبس من ستة أشهر إلى سنتين و بغرامة من مليونين وخمسمائة ألف دينار إلى عشرة ملايين دينار أو بإحدى هاتين العقوبتين فقط مع: الغلق المؤقت أو النهائي للمؤسسة، مصادرة الأشياء والوسائل والأدوات التي استعملت في المخالفة، إتلاف الأشياء محل المخالفة".

و تنص المادة 61 من الأمر 03-07 المتعلق ببراءات الاختراع على أنه يعاقب مرتكب جنحة التقليد بالحبس من ستة أشهر إلى سنتين وبغرامة من مليونين وخمسمائة ألف دينار إلى عشرة ملايين دينار أو بإحدى هاتين العقوبتين فقط".

الفصل الثاني

المواجهة الإجرائية و الأمنية للجرائم ضد الأسرار المعلوماتية

يعتبر تجريم سلوكات الاعتداء على الأسرار المعلوماتية عن طريق إصدار النصوص التشريعية مكافحة موضوعية لهذا النوع من الجرائم، وإلى جانب هذه الآليات من المكافحة هناك آليات إجرائية تمثلت في إجراءات التحقيق الجنائي وإجراءات أمنية تمثلت في التعاون الدولي في مجال مكافحة هذا النوع من الجرائم.

المبحث الأول

التحقيق الجنائي في الجرائم الماسة بالأسرار المعلوماتية

تعتبر مسألة إثبات الجرائم المعلوماتية من أهم المواضيع القانونية ذلك بالنظر إلى المشكلات الإجرائية التي أثارتها هذه الجرائم المستحدثة والمتمثلة في سرعة ودقة تنفيذ الجريمة وإمكانية نفاذ المجرمين المتمرسين إلى الأجهزة وتخريب أو إخفاء الملفات التي

تدينهم أو تجرمهم وهو ما يصعب عملية جمع الأدلة. كما أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من طبيعتها.

فنظرا للطابع الخاص الذي تتميز به هذه الجرائم، فإن إثباتها يحيط به الكثير من الصعاب والتي تتمثل في صعوبة اكتشاف هذه الجرائم لأنها لا تترك أثرا خارجيا[1]، فلا يوجد جثث قتلى وأثار للدماء، وإذا اكتشفت الجريمة غالبا يكون ذلك بمحض الصدفة[2].ناهيك عن ارتكاب الجريمة يتم غالبا من مسافات بعيدة باستخدام وحدات طرفية أو بأساليب أخرى مشابهة.

عموما بالنسبة لهذا النوع من الجرائم فإن رجال التحقيق يواجهون صعوبات شديدة في ضبط وتوصيف الجرائم المعلوماتية وأيضا لتعقب مرتكبيها، ويعود ذلك بالطبع إلى كونها جرائم ترتكب في فضاء الكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

وهذه الصعوبات تعود عموما لما تتميز به الجريمة المعلوماتية من مميزات سبق التفصيل فيها كسهولة إخفاء الجريمة، غياب الدليل المرئي، صعوبة الاهتداء إلى مرتكب الجريمة، إعاقة الوصول إلى الدليل بواسطة الحماية الفنية[3]، سهولة محو الدليل، الضخامة البالغة لكم البيانات المتعين فحصها، نقص خبرة رجال التحقيق.

فصعوبة الاهتداء إلى مرتكبي الجرائم الواقعة في ذلك السياق فإذا أراد شخص إلحاق الضرر بشخص لآخر وقام باختراق جهازه الحاسب الآلي وتمكن من الحصول على بعض البيانات والمعلومات الشخصية الخاصة بالمجني عليه، فإنه وإن أمكن تحديد الحاسب الذي اخترق تلك البيانات فإنه يصعب تحديد شخص المستخدم لذلك الحاسب في ذلك الوقت .

ولا شك أن التعامل في مسرح الجريمة سواء أكان مسرحا ماديا أو الكترونيا يتطلب، إجراءات روتينية معينة متفق عليها لحماية الدليل وإبراز قيمته الاستدلالية إلا أن طرق حفظ الأدلة واستخلاصها تختلف من مسرح الجريمة المادي إلى مسرح الجريمة الالكتروني.

---

[1] ومرد ذلك إلى مجموعة من العوامل تتمثل في:عدم وجود أثر كتابي، إذ يتم نقل المعلومات بالنبضات الإلكترونية، يستطيع الجاني تدمير دليل الإدانة في زمن متناه القصر، إعاقة الوصول إلى الدليل بوسائل الحماية الفنية، حيث أنه في كبرى المواقع العالمية على شبكة تحاط البيانات المخزنة على صفحاته بسياج من الحماية الفنية لإعاقة المحاولات الرامية للوصول غير المشروع إليها لتدميرها أوتبديلها أوالإطلاع عليها أونسخها، فإذا تمكن الجاني من اختراق تلك المواقع وقام بالعبث بها، فإنه قد يقوم بوضع وسائل حماية فنية خاصة به لكي يمنع الغير من الدخول على ذلك الموقع الذي قام بالعبث به ومن ثم يصعب الوصول إليه كما يصعب الكشف عن دليل يدينه. مثل قيام الجاني باستخدام كلمات مرور بعد تخريب الموقع مثلا، ويشكل استخدام تقنيات التشفير أحد اكبر العقبات التي تعوق جهات التحري.

[2] غالبا ما تكتشف تلك الجرائم بمحض الصدفة وذلك للإحجام عن الإبلاغ من طرف المجني عليهم يحاولون درء الأثر السلبي للإبلاغ عما وقع خاصة إذا كان المجني عليه من المؤسسات التي لديها عملاء.

[3] - منى فتحي أحم، مرجع سابق، ص 143 والدكتور عبد الفتاح بيومي حجازي، الجوانب الإجرائية، الأعمال الإجرائية لإعمال التحقيق الابتدائي في الجرائم المعلوماتية، ص57

وباعتبار أن الجرائم محل الدراسة هي من الجرائم المعلوماتية فالتحقيق فيها والإثبات هو نفسه التحقيق والإثبات في الجرائم المعلوماتية ولهذا سيتم تخصيص هذا الفصل لكل ما يتعلق بالتحقيق في هذه الأخيرة على الوجه الذي سيأتي أدناه، وذلك لتسليط الضوء على الجانب الإجرائي المتعلق بالجرائم محل الدراسة على النحو التالي:

المطلب الأول

ماهية التحقيق في الجرائم الماسة بسرية المعلومات الالكترونية

إن ظهور الجريمة المعلوماتية فرض على جهات التحقيق تحديات عظيمة لم يسبق لها مثيل، فما تتميز به هاته الجرائم من حيث السهولة والسرعة الفائقة في تنفيذ الجريمة، وانعدام الآثار المادية للجريمة، وغياب الدليل المرئي، وصعوبة الوصول إلى الدليل بالوسائل الفنية التقليدية، وكذلك سهولة إتلاف الدليل المادي وتدميره في زمن قياسي، كل ذلك استوجب إعادة النظر بوسائل المكافحة التقليدية للجريمة وأساليبها وطرق الوقاية منها، وأصبح من الضرورة بمكان وضع الخطط والبرامج الإستراتيجية لتحديث أجهزة العدالة الجنائية وتطويرها من حيث بنيتها المؤسسية وكوادرها البشرية لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم ومواجهة مرتكبيها وضبطهم وتقديمهم للعدالة، فضلا عن إشكالية توفر المعرفة القانونية لدى الجهات المختصة بمواجهة هذا النوع من الجرائم، ومنه تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطوراً ملموساً يواكب حركة الجريمة وتطور أساليب ارتكابها.

معنى ذلك أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة من السابق ونحن لا نزال في بداية عصر الانفجار المعلوماتي ويمكن أن نتوقع ظهور المزيد والمزيد من هذه الأنماط الجديدة، كان يتوجب معها تحديث الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة ، وهو ما يستتبع تطوير أسلوب التحقيق فيها.

كما أن الطبيعة الفنية والتقنية الناجمة عن الجرائم المعلوماتية نتج عنها في مجال الإثبات الجنائي نوع جديد من الأدلة يطلق عليه الدليل الرقمي أو الدليل الإلكتروني، وقد اعتدت به المحاكم في بعض النظم القانونية المقارنة، سواء من حيث قيمته القانونية أي الدليل الرقمي وبين حجيته في الإثبات حيث ساوت هذه الأنظمة القانونية في الإثبات الدليل التقليدي والدليل الإلكتروني لهما نفس الحجية في الإثبات، ويعرف الدليل الإلكتروني بأنه "هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي

لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون[1].

الفرع الأول: مفهوم التحقيق الجنائي الابتدائي في المجال الالكتروني[2]

فالتحقيقات الجنائية هي علوم تطبيقية تنطوي على دراسة الحقائق، وتستخدم للتحقق من وجود جريمة وإثبات ذنب المجرم.[3]

فالتحقيق الجنائي صراع بين المحقق والمجرم، الأول ينشد الحقيقة عن الجريمة والثاني يحاول التضليل وطمس الحقائق حتى يفلت من العقاب ولكن بقدر ما يكون للمحقق الجنائي من خبرة وفراسة وإلمام بالعلوم الجنائية والنفسية وبقدر ما يتمتع به من كفاءة ومقدرة وسيطرة على المواقف التي يواجهها بقدر ما تكون النتيجة في صالح التحقيق إرساءً لقواعد الحق والعدل.[4]

ومع تزايد الجرائم الماسة بسرية المعلومات الالكترونية (الجرائم الالكترونية)أصبح من الواجب معرفة كيفية إثباتها في سبيل الحصول على دليل رقمي يمكن الاستناد عليه في عملية الإثبات.

ففي كثير من الأحيان نسمع بأن جهات حكومية قامت باقتحام منزل هاكر واعتقاله وأخذ جميع الأدوات والأمور التقنية الموجودة في منزل الهاكر.. بالتأكيد لم يأخذوها فقط لكي يثبتوا التهمه عليه ! فهل قاموا بمصادرة وحجز جميع الأدوات لكي يقوموا بتحليلها واستخراج أدلة قاطعة بأن العملية تمت بالإضافة لكي يستفيدوا من هذه الأدوات الموجود في فهم الاختراقات الموجهة كتهم لهذا الهاكر... لذلك بكل بساطة عملية التحليل الجنائي الرقمي تعرف على أنها عملية استخراج ومعرفة وجمع أكبر قدر من الأدلة من أماكن الاختراقات وأيضاً من نفس أجهزة هذا الهاكر لكي يتم إثبات التهم الموجهة عليه وأيضاً كما ذكرت معرفة الأمور والأدوات التي تم استخدامها في هذه العملية لكي تكون المحاكمة لمثل هذه الأشخاص سليمة وعادلة وتثبيت جميع الأمور بالأدلة القاطعة، فعملية التحقيق الجنائي الرقمي ليست مقتصرة فقط على الأجهزه الإلكترونية أو أدلة ملموسة، بل من الممكن أن تكون أيضاً عملية تتبع لبعض الأدلة والأمور التي تم إجرائها إثناء عملية الاختراق أو بعد

---

[1] http://www.f-law.net/law/threads يوم 2014/10/20

[2] باعتبار أن الجرائم الواقعة على الأسرار المعلوماتية هي جرائم واقعة في بيئة الكترونية فالتحقيق فيها يكون مختلف عن التحقيق في الجرائم الالكترونية ، وذلك للاختلاف بين الصنفين من الجريمة، حيث أن المشرع الجزائري وغيره من التشريعات المقارنة استحدثت إجراءات خاصة بالجريمة المعلوماتية.

[3] http://ar.wikipedia.org/wiki يوم الاطلاع على الموقع 2014/10/20

[4] http://www.startimes.com/ يوم الاطلاع على الموقع 2014/10/21

عملية الاختراق من خلال تحليل ملفات النظام وتتبع أثراه والحركات التي قام بها أو يقوم بها في نفس اللحظة وهذه الأمور جميعها تفيد في عملية التحقيق الجنائي الالكتروني ليس فقط لمعرفة الجاني بل لمعرفة نقاط ضعف الموقع لديك من خلال تحليل الحركات التي قام بها المخترق أثناء عملية الاختراق[1].

حيث تمكنت العديد من التشريعات من إرساء قواعد إجرائية تتوافق وطبيعة الجريمة الإلكترونية ومن ضمنها المشرع الجزائري من خلال القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، إذ تضمن الفصل الثالث من هذا القانون القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك وفقا للمعايير العالمية المعمول بها في هذا الشأن، إذ خول هذا القانون لأجهزة إنفاذ القانون الدخول والتفتيش ولوعن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة من أجل الحصول على المعطيات المبحوث عنها في منظومة معلوماتية تقع في بلد أجنبي في المادة الخامسة ، كما سمح القانون المذكور باستنساخ المعطيات محل البحث في حال تبين جدوى المعلومات المخزنة في الكشف عن الجرائم أومرتكبيها في المادة السادسة بالإضافة إلى الالتزامات التي ألقاها هذا القانون على مقدمي الخدمات وذلك بمساعدة السلطات العمومية في مواجهة هذه الجرائم والكشف عن مرتكبيها وذلك من خلال الفصل الرابع من نفس القانون[2]، كما ألزم المشرع الجزائري من خلال المادتين 10و 11من القانون 04/09المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على مقدمي الخدمات حفظ المعطيات بشكل يسمح بالتعرف على الأشخاص المساهمين في إنشاء المحتويات على الانترنيت وذلك من أجل التبليغات المحتملة للسلطات القضائية أوفي حال طلب هذه الأخيرة لأجل التحريات أو المعاينات أو المتابعات القضائية للجرائم المرتكبة والقيام بحفظ المعطيات المتعلقة بحركة السير، منها المعطيات التي تسمح بالتعرف على مستعملي الخدمة وكذا الخصائص التقنية وتاريخ ووقت ومدة الاتصال[3] .

كما عالج هذا القانون مسألة الاختصاص من خلال مقتضيات المادة 15حيث نصت هذه المادة " على أنه زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات

[1] مقال لمحمد عسكر، بعنوان تعريف لعملية التحقيق الجنائي الرقمي، في 16 ماي 2013، عن http://www.isecur1ty.org

[2] يوسف صغير، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو،الجزائر، سنة 2013 ، ص 114.

[3] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، جامعة قاصدي مرباح ورقلة - الجزائر، سنة 2013، ص 100.

الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني، »علاوة على هذه الآليات الإجرائية التي تضمنها القانون 04/09، فقد تضمن قانون الإجراءات الجزائية الجزائري مجموعة من الآليات الخاصة بالتحريات والتحقيقات في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مثل الآلية المتعلقة باعتراض المراسلات (المواد من 65 مكرر 5 إلى المادة 65 مكرر 10من قانون الإجراءات الجزائري) ، كما سمح بامتداد اختصاص الأجهزة المكلفة بالبحث والتحري إلى كامل الإقليم الوطني إذا تعلق الأمر بجريمة إلكترونية من خلال المادة 16 من قانون الإجراءات الجزائري على امتداد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني إذا تعلق الأمر ببحث ومعاينة لجرائم ماسة بأنظمة المعالجة الآلية للمعطيات، وكذا من خلال ما نصت عليه المادة 37 على جواز امتداد الاختصاص المحلي للنيابة العامة إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والجدير بالذكر في هذا المقام هوأنه سيتم التفصيل في النصوص القانونية أعلاه بمناسبة التفصيل في إجراءات التحقيق أدناه[1].

أولا: تعريف التحقيق الجنائي الالكتروني

التحقيق الجنائي الالكتروني هو استخدام الطرق المثبتة علمياً لحفظ, جمع، عرض، تحديد، تحليل ترجمة، توثيق، والتحقق من صحة الأدلة الرقمية المستخرجة من المصادر الرقمية بهدف تسهيل أو تعزيز بناء الأحداث الجنائية, أو المساعدة في إحباط العمليات غير الشرعية المرتقبة.[2]

ويعرف أنه "عمل قانوني يقوم به مأمور الضبط القضائي المختص والمتخصص لضبط الجرائم الالكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل"[3].

ثانيا:تعريف المحقق الجنائي

المحقق الجنائي هو كل من عهد إليه القانون بتحري الحقيقة في الحوادث الجنائية وتحقيقها ويسهم بدور في كشف غموضها وصولاً لمعرفة حقيقة الحوادث وضبط الفاعل[4].

---

[1] بالنسبة للتشريع الفرنسي فإن المشرع سعى إلى ملاءمة قانون الإجراءات الجزائية مع الآليات والقواعد الإجرائية التي جاءت بها اتفاقية بودابست في مجال البحث عن الجريمة الإلكترونية باعتبار أن فرنسا كانت من الدول السباقة للتوقيع على اتفاقية بودابست وذلك بتاريخ 23 نوفنبر 2001.

هذه إذن كانت نظرة على بعض القوانين المقارنة وحدود ملاءمتها مع مختلف الآليات الإجرائية التي أرساها المنتظم الدولي .

[2] محمد عسكر، مقال بعنوان مقدمة لمراحل التحقيق الجنائي وخطواته، في 7 ديسمبر 2013،عن http://www.isecur1ty.org/.

[3] مصطفى محمد موسى، المرجع السابق، ص 166.

[4] http://www.startimes.com/ يوم الاطلاع على الموقع 2015/08/10

وفي تعريف آخر هو المكلف بالبحث عن الحقيقة في الجرائم الالكترونية لكشف مرتكبيها وتجميع أدلة الإدانة أو البراءة ضدهم لإحالتهم إلى القضاء، فالمحقق هو المكلف بتنفيذ إجراءات القانون المطبق كل حسب اختصاصه.[1]

كما تم تعريفه أيضا أنه من يتولى التحقيق من رجال الضبط القضائي أو أعضاء النيابة أو رجال القضاء[2]، كما عرفه البعض أيضا أنه هو ذلك الشخص الذي عهد إليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل إلى علمه من جرائم يهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة[3]، وعرف أيضا أنه" من يقوم بمباشرة التحقيق بمعناه القانوني أي أعضاء النيابة العامة أو قضاة التحقيق فلا ينصرف هذا اللفظ إلى الذين يباشرون جمع الاستدلالات[4].

فالمحقق الجنائي بصفة عامة هو الشخص القائم بأعمال إجراءات التحقيق الجنائي ولا يختلف تعريف المحقق في الجرائم الالكترونية عنه في الجرائم التقليدية فالفرق في نوعية الجريمة وليس في المحقق.

ثالثا:الصفات والمؤهلات التي يتطلبها المحقق الجنائي في الجرائم الالكترونية

يتطلب المحقق الجنائي في الجرائم المعلوماتية تقريبا ذات الصفات الواجب توافرها في أي محقق جنائي وهي كالتالي:

1- أن يكون هدفه هو الوصول إلى الحقيقة ولديه موهبة فن التحقيق ذلك أن المحقق يكون مؤمناً برسالته في استظهار الحقيقة، واتخاذ كل الوسائل الكاشفة عنها، وأن يكون لديه اعتقاد أن الوصول إلى الحقيقة وتحقيق العدالة هما هدفه وغايته المنشودة.

فينبغي عليه أن يكون مؤمنا بأنه يؤدي رسالة إنسانية مؤتمن عليها أمام الله وأمام المجتمع، فلا تؤثر فيه أي روايات يستمع إليها خارج إطار التحقيق الذي يجريه، ولا تؤثر فيه أيضا كتابات يطلع عليها في الصحف، وإنما يجب عليه أن يجرد نفسه من كل تأثير يقع عليه من جراء الحادث الذي يقوم عليه تحقيقه فيباشر إجراءاته على أساس أنه خالي الدهن ومجرد من أي علم سابق على أول إجراء يبدأ به[5].

---

[1] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية،مطابع الشرطة القاهرة، الطبعة الأولى، 2008، ص 253.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي،الإسكندرية، 2009، ص 87، مشار إليه لدى محمود عبد الرحيم،التحقيق الجنائي، بدون ناشر، 1963، ص 16

[3] خالد ممدوح إبراهيم، مرجع سابق، ص 87.

[4] خالد ممدوح إبراهيم، مرجع سابق، ص 87.

[5] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة والنشر، الجزائر، 2008، ص 13، مشار إليه لدى عبد الفتاح مراد، التحقيق الجنائي التطبيقي، ص 78.

ويعتبر فن التحقيق هو الإبداع والتمكن والقدرة على الاستنتاج والتحليل من أمور معطاة وتحويلها إلى الوقائع الناتجة، أوبمعنى آخر رفع الستار عن الحقيقة والغموض[1].

2-أن يكون سريع التصرف بمعنى أنه يقع على عاتقه تسير إجراءات التحقيق بالسرعة الواجبة لإنجازه دفعة واحدة, أوفي جلسات قريبة متلاحقة، وعدم التباطؤ في جمع الأدلة، وألا يتردد في مباشرة الإجراء الذي يراه سليماً، حتى لا تضيع الفائدة من اتخاذه في وقته المناسب. كذلك يجب أن تكون لديه قوة الملاحظة وسرعة البديهة،وهي تعني القدرة على حفظ المعلومات والمشاهدات التي تقع تحت أحد حواسه واستدعائها عند الحاجة وهي ما يمكنه من ربط الحوادث بعضها مع بعض الآخر، إذن يتعين عليه أن يتصف بقوة الملاحظة فيركز انتباهه إلى كل ما يتعلق بالتحقيق من أشخاص ووقائع، ويلاحظ مكان الجريمة حتى المعاينة لاكتشاف بعض الآثار المادية التي تفيد في استظهار كيفية وقوع الجريمة وتعرف الحقيقة.

3- أن يكون محايد أثناء التحقيق وملتزم الهدوء وضبط النفس، وذلك يعني عدم تحيزه وتحري الحق أينما كان سواء أدى إلى إقامة الدليل قبل المتهم أو إلى نفي التهام عنه، فبقدر ما يحاصر المتهم بوسائل الإثبات، فإنه أيضا يجب عليه أن يأخذ بعين الاعتبار وسائل إثبات البراءة التي تظهر له من التحقيق[2]، وكما يصغي باهتمام لأقوال الضحايا والشهود فإنه يفسح المجال أيضا للمتهم لتقديم ما لديه، ويناقشه في جو من الهدوء والمعاملة الحسنة دون استعمال أساليب الإكراه المادية والمعنوية أو وسائل الخداع للحصول على إفادات مغايرة من شأنها أن تؤدي إلى إلصاق تهمة باطلة بشخص بريء[3].

وينبغي عليه أيضا أن يعامل جميع أطراف القضية على قدم مساواة فلا تفرقة بينهم بسبب الجنس أو الطبقة أو الثروة أو بسبب وظيفتهم الاجتماعية أو الاقتصادية أو المهنية في المجتمع.

كما يجب أن يلتزم المحقق بضبط النفس، ولا يستسلم للغضب أو لسيطرة الميول والغرائز، وأن يتحلى بالصبر والمثابرة في الكشف عما يدق أو يغمض من أمور التحقيق، وأن يتأتى في الحكم على قيمة الدليل، مقلباً الرأي على مختلف وجوهه حتى يتيقن من مطابقته لمقتضى الحال دون التزام بالتأثير الأول الذي يتبادل إلى ذهنه عن الحادث.

4- عدم التأثر باتجاهات الرأي العام،إذ يجب على المحقق أن يبتعد عن أي مؤثرات من شأنها التأثير على سير العدالة، فتأثر المحقق قد يجعله قاسيا عنيف أو متعاطفا ودود، فلابد أن لا يتأثر مثلا بإعجاب المحيطين به لأن الغرور من الصفات القاتلة التي من شأنها أن تؤخر ولا تقدم في التحقيق، كما يلتزم بحفظ أسرار التحقيق.

---

[1] خالد ممدوح ابراهيم، المرجع السابق،ص 98.

[2] محمد حزيط، مرجع سابق، 14، عن معجب بن معدي الحويقل، المرشد للتحقيق والبحث الجنائي، ص 72.

[3] محمد حزيط، المرجع نفسه، ص 14، عن مقراني حمادي، دروس في قانون الإجراءات الجزائية، غير منشورة.

5- العلم التام بالقوانين الجنائية حيث، يجب أن المحقق يكون على علم تام بأحكام القانون الجنائي، وبعلم الإجرام وبعلم العقاب، وأن يكون على دراسة بمبادئ الطب الشرعي وعلم النفس الجنائي، وأن يكون ملماً بمختلف الظروف المحيطة بالمجتمع وبالمعلومات العامة التي تتصل بالوقائع التي يتولى تحقيقها، كما يجب أن يكون على جانب كبير من الثقافة العامة متنوع الإطلاع والمعارف التي تتصل بالحياة البشرية على مختلف صورها وطبائعها.

إضافة إلى بعض الأمور الواجب توفرها فيه كالاستقامة في حياته الشخصية، العمل بروح الفريق، قوة الذاكرة، علاقته بزملائه وأن يكون قدوة لمرؤوسيه، البعد عن الصغائر والشبهات، وغيرها، أي يجب أن يتصف المحقق بجمال الخلق، واحترام الذات، وقوة الشخصية وحسن المظهر وسمو الشعور والإدراك, حتى يكتسب ثقة الخصوم ويرسخ اعتقاد الناس في سلامة إجراءات التحقيق.

وكل المهارات التي سبقت الإشارة إليها والتي يجب أن تتوفر في المحقق الجنائي إنما هي لازمة بالنسبة لكل محقق في حين لابد من توفر بعض المهارات الإضافية في المحقق في الجرائم المعلوماتية وليتمكن من التعامل مع هذه الأخيرة ليتمكن لابد له من التعرف على علوم أخرى والإلمام بها وهي علم الكمبيوتر والأدلة الرقمية، أي الاستخدام الأمثل للحاسب الآلي ونظمه وبرامجه ووسائل الاتصال الالكترونية الرقمية، ويجب أن يتحقق لديه التوازن الفكري الالكتروني باستمرار القراءة في مجال التقنية الالكترونية الرقمية وشبكة الانترنت والتعليم والتدريب والخبرة، لأنها تحقق لصاحبها التفوق ومن ثم ينخفض لديه القلق وبدلك يستطيع تحديد أهدافه وتحقيقها[1]، ويمكننا التفصيل فيها على النحو التالي:

أولا: التعرف على المكونات المادية للحاسوب وآلية عمل الشبكات

يجب التعرف على مكونات الحاسوب، لأن التحقيق وجمع الأدلة في الجرائم المتعلقة بالحاسوب والإنترنت، يتطلب مهارات فنية وتقنية من أجل التعامل مع كافة الجوانب والمكونات المادية والمعنوية للحاسوب، ومعرفة كيفية التعامل مع مكونات هذه الأجهزة ومعطياتها وطريقة عملها، وكيفية تخزين هذه المعطيات ووسائط تخزينها.

وإن معرفة أجهزة الحاسوب المختلفة وأجهزة الاتصال التي تشكل الشبكة الدولية للمعلومات المرتبطة بالانترنت وطرق تخزين البيانات الرقمية، يساعد المحقق عند وصوله إلى مسرح الجريمة، ومعاينة هذه الأجهزة من سرعة تحديد كيفية وقوع الجريمة وارتباطها بالأنظمة المعلوماتية (الحاسوب والانترنت) وسهولة التعرف على مكوناتها، والأقراص الصلبة وما حوته من بيانات ذات الصلة بارتكاب الجريمة.

[1] مصطفى محمد موسى، مرجع سابق،ص 257.

ولابد من أن يعلم المحقق بجميع أشكال الحاسوب وملحقاتها ووسائط التخزين بصفتها أدلة محتملة، وهذا ما تهدف إليه الدورات التدريبية لرجال التحقيق، حتى يتم الإلمام بالمعرفة اللازمة لمكونات الحاسوب واكتساب المهارات الفنية اللازمة[1]، والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة أو المدمجة، لأية مؤثرات خارجية كالقوى المغناطيسية أو موجات الميكروويف حتى لا تتلف محتوياتها.

وكذلك يتوجب على المحقق معرفة آلية عمل شبكات الحاسوب والإنترنت، لأن الشبكة الدولية للمعلومات تربط ملايين أجهزة الحاسوب ببعضها البعض، مما ساهم بشكل كبير في نشوء أنماط إجرامية لم تكن معروفة، حيث أتاحت هذه الشبكات لمحترفي الإجرام إلى تطوير أساليب الإجرام، وارتكاب جرائمهم بعيدا عن مسرح الجريمة.

إن الكثير من الجرائم المعلوماتية يتم ارتكابها من خلال شبكة الإنترنت، ولذا وجب على محقق أن يلم بمبادئ الاتصال وأنواعها، وكيفية انتقال البيانات من جهاز لآخر على شكل حزم عن طريق الشبكات.

وتبرز أهمية فهم المحقق لمبادئ عمل الشبكات في كونها ضرورة لتصوير كيفية ارتكاب الفعل الإجرامي في الفضاء السيبراني من اختراق للشبكات والحواسيب، واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويل مسارها، كما أنها تعطي المحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الاعتداء على الشبكة والمعوقات التي تحول دون ذلك[2].

ثانيا : تمييز أنظمة تشغيل الحاسوب المختلفة ومعرفة صيغ معطيات الحاسوب

يتوجب على المحقق أن يستطيع التمييز بين الأنظمة المختلفة لتشغيل الحاسوب، وأن يلم المحقق بجميع الأنظمة التشغيلية لأجهزة الحاسوب وما تتسم به من خصائص ومميزات لكل نظام على حدة، لأنه ملزم بالتعامل معها، وكذلك أنظمة الملفات التي يعتمدها كل نظام، حتى يتمكن من إجراء التحقيق في جرائم الحاسوب والانترنت في كشف الجناة، ومعاينة مسرح الجريمة، وإجراء التفتيش والتمكن من ضبط الأدلة الجرمية[3].

إن التعامل المباشر مع هذه الأنظمة، والقيام بفحصها ورفع الأدلة الجنائية الرقمية الموجودة فيها، يعتبر مهمة الخبير الجنائي في الحاسوب والشبكات الموجودة ضمن فريق التحقيق، إلا أن معرفة المحقق الجنائي الأولية بهذه الأنظمة ضرورية لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة، وأحيانا يجد قائد الفريق نفسه أمام قرار فني صعب يجب أن

---

[1]- د. حسين سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، من موقع قوانين الشرق على شبكة الانترنت www.eastlaws.com ، ص 2.

[2]- د. حسين الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، مرجع سابق، ص 2.

[3]- من موقع معهد دراسات الأمن التكنولوجي على شبكة الانترنت www.istsdartmouth.eud

يتخذه بالتشاور مع خبير الحاسوب، ودون توافر الحد الأدنى من المعرفة التقنية لهذا القائد فإن القرار سيكون للخبير وحده، مثال ذلك وجود حواسيب ضمن مسرح الجريمة وهي في وضع التشغيل، ويكون القرار الواجب اتخاذه هو هل سيتم إيقاف عملها حتى لا يكون بداخلها برامج تعمل على محو أدلة الإدانة أوعلى استمرارية تنفيذ جريمة ما، أم يتم الإبقاء عليها في حالة عمل خشية أن يتسبب بقفلها عن العمل، ضياع بعض الأدلة الموجودة في ذاكرة الحاسوب أوفي نظام الملفات على القرص الصلب، وربما يتسبب في تشغيل أداة خفية لتدمير كافة محتويات القرص الصلب، تم إعدادها من قبل المجرم وذلك دون أن ينتبه خبراء الحاسوب لوجودها.[1]

ويتعين على المحقق كذلك التعرف على معطيات الحاسوب المختلفة ليصبح قادرا على معرفة صيغ الملفات وما يمكن أن تحتويه من معطيات، ومعرفته لأهم التطبيقات التي يمكنه من خلالها قراءة أو مشاهدة محتوى هذه الملفات يعد أمرا في غاية الأهمية، لأن هذه الملفات هي الوعاء الحقيقي لأدلة الإدانة في الكثير من القضايا ذات الصلة بالحاسوب والانترنت بما تحتويه من معلومات، علما بأنه يتم حفظ البيانات الرقمية داخل الحاسوب على شكل مجموعات أو كتل من البيانات، تمثل وحدة واحدة تسمى الملفات، حيث يتميز كل ملف ببنية وصيغة خاصة تميزه عن غيره، وغالبا ما ترتبط كل صيغة بنوع محدد من المحتوى، كأن يحتوي الملف على بيانات تمثل صورة أو صوتا أو فيديو أو مستندا خطيا منسقا أو غير منسق أو غير ذلك[2].

ويلعب الانترنت دورا رئيسا كمصدر للمعلومات، حيث يتيح الاطلاع على كم هائل منها من جميع أنحاء العالم بسرعة وسهولة، وهي بالنسبة للمحقق تمثل أداة جمع تحريات مناسبة فقد خلقت الانترنت مجتمعا افتراضيا شبيها إلى حد ما بالمجتمعات الحقيقية، ويدور في مجتمع الانترنت هذا الكثير من الحديث الذي قد يفيد المحقق في توضيح غموض بعض الجرائم[3].

ومن الضروري أن يستخدم رجال التحقيق الحاسوب والإنترنت، حتى يستطيعوا التصدي لجرائم الحاسوب والانترنت والنظم المعلوماتية، بما لديهم من معرفة بالبرمجيات المستخدمة في المواقع الالكترونية، وتبادل الرسائل البريدية ونقل الملفات وكافة الخدمات التي تتيحها شبكة الانترنت، حيث من الممكن استخدامها كأداة تعليمية للاطلاع على جرائم الحاسوب والانترنت وطرق التصدي لها[4].

---

[1]- محمد السرحاني، مرجع سابق، ص 96.

[2]- حسين الغافري،، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب ، مرجع سابق، ص2.

[3]- محمد السرحاني، المرجع نفسه، ص 98.

[4]- حسين الغافري، المرجع نفسه، ص 3.

ثالثا : معرفة الأساليب المستخدمة في ارتكاب جرائم الحاسوب وتقنيات الأمن المعلوماتية

إن معرفة رجال التحقيق بالأساليب المستخدمة في ارتكاب جرائم الحاسوب والانترنت والإلمام بكيفية استخدامها، من الأمور المهمة التي تساعدهم في معرفة الجناة وموقع ارتكاب الجريمة، ومن أي طرفية إلكترونية صدر السلوك الجرمي، وكذلك في مناقشة الشهود واستجواب المتهمين ومحاصرتهم بالأسئلة التي تتعلق بكيفية ارتكاب الجريمة وطرق ارتكابها والتفاهم مع خبراء الحاسوب عند التوصل إلى الأدلة عن طريق ارتكاب الجريمة وعن الأدوات التي ساعدت في ارتكابها[1].

ولأن جرائم الحاسوب والانترنت كثيرة ومتعددة، يستخدم مرتكبها أساليب مستجدة وأدوات تجريمية متطورة لتساعدهم على ارتكاب هذه الجرائم، وهذه الوسائل وتلك الأدوات من التجدد وسرعة التطور بحيث إنه لا يمكن أن يحيط بها أي برنامج تدريبي يستهدف رجال التحقيق، ولا حل إلا بالمتابعة المستمرة والاطلاع على النشرات الأمنية التي تصدرها منظمات رسمية وغير رسمية ذات مصداقية من خلال الانترنت.

إن الإلمام بتقنيات الأمن المعلوماتية والحاسوبية من الأمور المهمة التي لابد للمحقق في جرائم الحاسوب والانترنت من معرفتها واستيعابها، لأنها تساعده في معرفة مجريات التحقيق لأن المحقق عندما يباشر التحقيق في جريمة اختراق شبكة الحاسوب التابعة لمؤسسة ما يسأل القائمين على الشبكة عن نوع برامج الحماية المستخدمة وكيفية إعدادها، والكيفية التي تفاعلت بها مع الحدث محل التحقيق.

وهناك الكثير من التقنيات التي تستخدم في أمن الحاسوب والشبكات، والتي تكون وثيقة الصلة بالتحقيق، ويكون فهم المحقق لوظائفها وأسلوب عملها وطرق استخدامها عاملا مساعدا له عند قراءته للتقارير الجنائية التي يعدها خبير الحاسوب، والتي تعتبر من أهم الوثائق التي يرجع إليها المحقق ويعتمد عليها في تحقيقه، والتي ترفق بمحاضر التحقيق ويرتكز عليها توجيه الاتهام عند اللزوم[2].

ومن أهم هذه التقنيات الجدار الناري وأنظمة كشف الاختراق وأنظمة الخادم الوكيل وأدوات تتبع مصدر الاتصال الشبكي، وأدوات ومراجعة العمليات الحاسوبية، والتي بالرغم من أن استخدامها يتم من قبل خبير الحاسوب الجنائي، إلا أنه من الضروري أن يمتلك المحقق فهما جيدا لأساسيات عملها، ليكون قادرا على التحقيق في القضية والتواصل مع الخبير في ما يختص بعلاقة هذه التقنيات بها[3].

الفرع الثاني

[1]- خالد عياد الحلبي، مرجع سابق، ص 188 و189.

[2]- خالد عياد الحلبي ، المرجع نفسه، ص 189 و190.

[3]- محمد السرحاني، مرجع سابق، ص 100.

عناصر التحقيق الجنائي الالكتروني

يجب علي المحقق أن يستظهر الركن المادي والمعنوي للجريمة محل التحقيق، وتحديد وقت ومكان ارتكاب الجريمة المعلوماتية بالإضافة إلي علانية التحقيق .

أولا: إظهار الركن المادي للجرائم المعلوماتية

إن النشاط أو السلوك المادي في الجرائم الالكترونية يتطلب وجود بيئة رقمية واتصال بالانترنت ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته.[1]

ثانيا: إظهار الركن المعنوي للجرائم المعلوماتية

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني[2].

ثالثا: تحديد وقت ومكان ارتكاب الجريمة المعلوماتية

تثير مسألة النتيجة الإجرامية في جرائم الالكترونية مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلوقام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم Server أحد البنوك في الإمارات، وهذا الخادم موجود في الصين فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين، وهذا بالتالي يثير مشكلة أخري وهي مكان ارتكاب الجريمة المعلوماتية، ويثور أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن. حيث أن هناك بعد دولي في هذا المجال ذلك أن الجريمة المعلوماتية جريمة عابرة للحدود[3].

رابعا: علانية التحقيق

إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولهذا قيل إن العلانية في مرحلة المحاكمة لا يقصر فيها الأمر علي وضع الاطمئنان في قلب المتهم، بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلا للشك أو الخضوع تحت التأثير، كما أن فيها اطمئنانا للجمهور على أن الإجراءات تسير في طريق طبيعية[4].

والعلانية المقررة للتحقيق في الإجراءات الجنائية هي من بين الضمانات الخاصة به، وهي تختلف في التحقيق الابتدائي عنها في مرحلة المحاكمة. ففي الابتدائي تعتبر العلانية نسبية أي قاصرة علي الخصوم في الدعوى الجنائية. والعلانية في التحقيق النهائي أو مرحلة

---

[1] محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الالكترونية، الفكر الشرطي ، المجلد الحادي والعشرون ، العدد 81 2012، ص 36.

[2] محمد حسن السراء، المرجع نفسه، ص 36.

[3] محمد حسن السراء، مرجع سابق ، ص 37.

[4] محمد حسن السراء، المرجع نفسه ، ص 37.

المحاكمة هي علانية مطلقة، بمعني أنه يجوز لأي فرد من أفراد الجمهور الدخول إلى قاعة الجلسة وحضور المحاكمة، كما أنه يجوز في المرحلتين، في التحقيق الابتدائي والتحقيق النهائي مباشرة الإجراءات في غير علانية، فيصدر القرار بجعله سرياً. ولما كان هذا استثناء يأتي على قاعدة عامة أصلية، كان لابد من أن يتم تحديد الأحوال التي يجوز فيها جعل التحقيق سرياً، وهي رخصة لا يستحسن الالتجاء إليها إلا عند الضرورة.

الفرع الثالث
تعريف الدليل الالكتروني[1]

تعددت التعريفات التي قيلت بشأن الدليل الإلكتروني حيث يتجه البعض إلى التوسع في تعريف الدليل الإلكتروني أو التقني أو الرقمي، فهو في نظره كل بيانات يمكن إمدادها أو تخزينها في شكل رقمي (لغة الحاسب) بحيث تمكن الحاسب الآلي من إنجاز مهمة ما، على أن ربط الدليل التقني بفكرة المعلومة يجعل موضوع الدليل التقني يؤدي دوره في إطار عملية استرجاع أو استرداد المعلومات فقط وبحيث لا يكون دليلا سوى كل ما يمكن استرجاعه أو استرداده من معلومات، لذلك يمكن تعريف الدليل التقني بأنه " الدليل الذي يجد له أساسا في العالم الافتراضي ويقود على الجريمة "، فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات، والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الإنترنت، فكلما كان هناك مزج في موضوع الدليل بالمعالجة الآلية للمعلومات فإنه يعد هنا دليلا تقنيا.[2]

[1] في جميع أطوار هذه الدراسة كنا نفضل مصطلح المعلوماتية مثلا بخصوص الجريمة الالكترونية نحن كنا مع تسميتها بالجريمة المعلوماتية بينما فيما يتعلق بالدليل المستخرج من البيئة الرقمية من جهتنا نفضل اصطلاح الدليل الالكتروني بدلا من معلوماتي لأنه في الحقيقة دليل ذو طبيعة الكترونية، ولا يمكن الاصطلاح عليه بالمعلوماتي مع العلم أنه يمكن أيضا تسميته بالدليل الرقمي وهو صحيح ذلك لأنه مستخرج من بيئة رقمية.

[2]- منى فتحي أحمد عبد الكريم، مرجع سابق، ص 162.

وهو أيضا "الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة "[1].**و**يعرف الدليل الجنائي أيضا بأنه" هو الوسيلة التي يستعين بها القاضي للوصول إلى اليقين القضائي الذي يقيم عليه حكمه في ثبوت الاتهام المعروض عليه"[2] .

وهناك من يعرفه على أنه "كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث يمكن الحاسوب من انجاز مهمة ما"[3]، ويعرف أيضا أنه " معلومات يقبلها المنطق والعقل ويعتمدها العلم يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه"[4].

والملاحظ على جميع هذه التعاريف أنها حصرت الدليل التقني في تلك المستخرجة من الحاسوب فقط، مع العلم أن الرأي الغالب أن في دلك حصر للدليل التقني وهو يمتد لأكثر من ذلك على أساس أن يمكن أن يستمد من أي وسيلة تقنية أخرى غير الحاسوب.

ومن وجهة نظرنا يمكن تعريفه أنه "الدليل المتحصل عليه من جهاز الحاسوب بمكوناته المادية والمعنوية أومن أي نظام معلوماتي آخر، وذلك لاعتماده أمام سلطات التحقيق والمحاكمة".

وللدليل الإلكتروني خصائص تميزه عن غيره هي:

1.هو دليل علمي أي يتكون من معلومات ذات هيئة إلكترونية غير ملموسة لا تدرك بالحواس العادية بل يتطلب إدراكها الاستعانة بأجهزة ومعدات، وهو يحتاج إلى مجال تقني يتعامل معه لكونه من طبيعة تقنية، فلا يمكن الاطلاع على الدليل الالكتروني سوى باستخدام الأساليب العلمية كما أن تعامل رجال الضبط القضائي والتحقيق والمحاكمة يجب أن يكون بطريقة علمية، سواء في حالة حفظه أو تقديمه كدليل إثبات حتى لا تسقط حجيته.[5]

2. يتميز الدليل الرقمي بصعوبة محوه أو تحطيمه، حيث انه حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوى ذلك الدليل .

---

[1]ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، بدون طبعة، سنة النشر 2006، ص 88.

[2]- أحمد فتحي سرور ، الوسيط في الإجراءات الجنائية، دار النهضة العربية، طبعة ع م 1996، ص 492.

[3] رشيدة بوكر، مرجع سابق، ص 382و383.

[4]رشيدة بوكر، المرجع نفسه، ص 383.

[5] وليد المعداوي، دور الشرطة في حماية الحياة الخاصة من أخطار المعلوماتية، رسالة دكتوراه، بدون ناشر، 2011، ص 352.

3 .إن محاولة الجاني لمحو الدليل الرقمي بذاتها تسجل عليه كدليل، حيث إن قيامه بذلك يتم تسجيله في ذاكرة الآلة وهو ما يمكن استخراجه واستخدامه كدليل ضده.

4. إن الطبيعة الفنية للدليل الرقمي تمكِّن من إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للعبث والتحريف أم لا لإمكانية مقارنته بالأصل .

4 . الدليل الإلكتروني متطور ومتنوع وذلك تبعا للمصدر المستمد منه، فأما عن التطور فإنها خاصية تكاد تكون تلقائية نظرا لارتباطه بطبيعة حركة الاتصال عبر الأنترنت و العالم الافتراضي اللذان لا يزالان في تطور، و أما عن خاصية التنوع فالدليل الالكتروني قد يكون في عدة أشكال فقد يكون بيانات مقروءة أو أفلام رقمية و غيرها.

الفرع الرابع

مدى اقتناع القاضي الجنائي بالدليل الإلكتروني

مبدأ حرية الإثبات الجنائي معناه أنه يجوز إثبات الجرائم بكل طرق الإثبات الجائزة قانونا وذلك لأنها واقعة حدثت في الماضي وإثباتها بكل الطرق يفتح المجال أمام القاضي لكي يتمكن من إعادة حتى أحداث الجريمة أمامه من خلال هذا المبدأ الهام، ويجيز للقاضي الاعتماد على كل الوسائل المقدمة إليه بما فيها الدليل الالكتروني حيث نص المشرع الجزائري في المادة 212 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم على أنه" :يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص" .

وغاية المشرع من إعطاء القاضي الجزائي هذه الحرية الواسعة لتشكيل قناعته وتقدير الأدلة المطروحة أمامه هو تمكينه من معرفة الحقيقة وكشف غموض كل واقعة جرمية لتأمين العدالة وضمان حرية الأفراد وصون كرامتهم، لذا أسند المشرع لوجدان القاضي الجزائي وضميره وشرفه مسألة تقدير الأدلة وحرية الاقتناع بها كإنسان مسؤول أمام الله والمجتمع لتطبيق العدالة، واعتبره أفضل ضمانة لتطبيق القانون وبسط العدالة.

مبدأ حرية الإثبات هو مبدأ هام جاء في الإثبات الجنائي كما سبق وأشرنا ولكنه ليس مطلقا بالشكل الذي يتصوره البعض بل هو مبدأ ترد عليه مجموعة من القيود[1]، والمهم في هذه المسألة هو مبدأ المشروعية. والمقصود منه هو الحصول على الأدلة بطرق مشروعة إذ لا يجوز أن يعتمد القاضي في حكمه على دليل تم الحصول عليه بطرق غير مشروعة، لهذا كفل المشرع تنظيم إجراءات الحصول على الدليل الجنائي في قانون الإجراءات الجزائية، والجدير بالذكر أن المشرع الجزائري عدل قانون الإجراءات الجزائية ليتناسب مع التحقيق

[1] القيود الواردة على حرية القاضي الجنائي في قبول الدليل هوقيد مشروعية الحصول على الدليل الالكتروني وقيود مستمدة من نصوص قانونية كقيد تحديد الأدلة في بعض الجرائم كالزنا .

في الجرائم المستحدثة والتي من بينها جرائم الدراسة، وفي هذا الشأن سنحاول أن ندرس هذا المطلب من خلال نقطتين هما مشروعية الدليل الالكتروني وحجيته في الإثبات.

أولا: مشروعية الدليل الالكتروني

من المسلم به في القانون الجنائي سلطة القاضي الجنائي في تقدير الأدلة والتي يحكمها مبدأ الاقتناع الشخصي للقاضي الجنائي أو حريته في تكوين قناعته، الأمر الذي فتح الباب أمام القاضي إذ يجوز له تقدير كل الأدلة المطروحة أمامه ولكن بشروط على القاضي التقيد بها في تكوينه اقتناعه بالأدلة ويشترط في الدليل هنا أن يكون معترف به قانونا.

إن مسألة تقدير الأدلة مسألة موضوعية لأن الأدلة جميعها لا تحظى أمام القاضي الجنائي بالقوة الحاسمة في الإثبات بل تخضع لاقتناعه بها، ولكن الأمر يصعب تطبيقه على الدليل الالكتروني وذلك يجعل لا محالة إلى الطبيعة الفنية لهذا الأخير، حيث أنه يسهل العبث بمضمونه كما أن القاضي الجنائي هورجل قانون قد يفتقد الثقافة المعلوماتية ما يحتم عليه في أغلب الأحوال الاستعانة بالخبرة الفنية التي قد تعطي للدليل الالكتروني قيمته في الإثبات مع وجود احتمالات الخطأ الواردة علميا وفنيا.

في كل الأحوال ومع احتمال الخطأ الوارد من قبل الخبير في المجال المعلوماتي ونقص الثقافة المعلوماتية لدى القاضي الجنائي، هل سيكون للدليل الالكتروني تأثيره على قناعة القاضي ليعتمده في إصدار حكمه أم لا؟

يعتبر المشرع الجزائري من ضمن المشرعين الذين اعتمدوا مبدأ الاقتناع الشخصي للقاضي الجنائي كأهم مبادئ الإثبات الجنائي، وهو ما كرسته صراحة المادة 212 من قانون الإجراءات الجزائية، حيث أنه يجوز للقاضي أن يستمد قناعته من أي دليل تطمئن إليه نفسه ويسكن إليه وجدانه بشرط أن يتناسب ذلك مع ما تقتضيه العدالة والمنطق والعقل.

فمن خلال قانون الإجراءات الجزائية الجزائري والتعديلات الواردة عليه وصلنا إلى نتيجة حتمية وهي أن ظهور الدليل الالكتروني لم يغير شيئا في مبدأ الاقتناع الشخصي للقاضي الجنائي وإنما هو مجرد دليل لا تزيد قيمته ولا حجيته عن غيره ويخضع كغيره لقناعة القاضي الشخصية والوجدانية وعليه يصح للقاضي إذا اطمئن إليه يعتمده كدليل ويؤسس عليه حكمه والعكس فإذا توغل إليه الشك بشأنه جاز له طرحه وعدم الأخذ به.

إذا ترك للقاضي الجنائي الحرية في أن يستمد قناعته من أي دليل وبأية وسيلة يراها موصلة إلى الحقيقة، إلا أن هذه الحرية لا تعني أنه غير مقيد بضوابط قانونية لابد له وأن يحترمها في هذا المجال وهو ما يعبر عنه بحرية القاضي في تكوين عقيدته أو حرية تقدير الأدلة ولكن بشروط إذا توفرت في الدليل جاز للقاضي اعتماده في إصداره الحكم القضائي، تتلخص في الآتي:

1 - :يجب الحصول على الدليل بصورة مشروعة أوما يعبر عنه بصحة الدليل

لا يجوز للقاضي الجزائي أن يستند في حكمه إلى أي دليل تم الحصول عليه بطرق غير مشروعة، مثل الإكراه أو إفشاء سر مهني في غير الأحوال المقررة قانونا أو خيانة أمانة وغيرها من الطرق غير المشروعة، ولابد أن يكون الدليل صحيحا لا يشوبه بطلان يتقرر بمخالفة إجراءات القانون، لأن مشروعية الأدلة تعتبر حدا لا يمكن للقاضي أن يتجاوزه نظرا لما تقوم عليه الخصومة الجنائية من مبدأ حرية المتهم وتعزيز قرينة براءته وليس فقط إطلاق حرية القاضي في الإثبات ممثلا سلطة الدولة في العقاب[1].

2 - طرح الدليل في الجلسة للمناقشة:

وقد أرست هذا الضابط الفقرة الثانية من المادة 212 من قانون الإجراءات الجزائية الجزائري[2]، فلا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه، وتكون الأدلة كذلك متى كان لكل منها أصل في ملف الدعوى، ولكن لا يلزم أن يناقشه الخصوم فعلا وإنما يكفي بتمكين الخصوم من ذلك ما دام الدليل كان مطروحا على بساط البحث[3].

ويحول هذا الشرط دون أن يحكم القاضي بمعلوماته الشخصية، إذ يتعين عليه أن يستمد اقتناعه مما دار في التحقيقات لا من خارجها وإلا يستند إلى أوراق لم يطلع عليها الخصوم ولم يتمكنوا من مناقشتها[4]، ولا تعد من قبيل المعلومات الشخصية الثقافة المعلوماتية للقاضي[5].

والجدير بالذكر أيضا أنه يجوز للقاضي أن يستعين بالخبراء وأن يأخذ برأي الخبير متى ارتاح ضميره إلى التقرير المحرر من طرفه، بحيث أن القرار الذي سيتوصل إليه القاضي لحسم الدعوى يكون قد استمده من عقيدته وليس من تقرير الخبير.[6] حيث أن القاضي سيكون مضطرا إلى الاستعانة بخبير في المجال المعلوماتي إذا كانت معارفه لا تؤهله من فهم الأدلة المطروحة أمامه وهي القاعدة العامة في تعيين الخبير مع احترام القواعد القانونية والإجرائية في ذلك، ويمكنه الاستغناء عن الاستعانة بالخبير إن أمكن إذا كان القاضي الجزائي مؤهلا التأهيل الفني والتقني على كيفية التعامل مع الدليل التقني لهذا أقترح أن

---

[1] http://www.startimes.com.2015/06/25 / يوم

[2] تقابلها المادة 2/427 من قانون الإجراءات الجزائية الفرنسي، والمادة 176 من قانون أصول المحاكمات الجزائية السوري، عن رشيدة بوكر، مرجع سابق، ص 511.

[3] أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، الجزء الثاني، الطبعة الخامسة، 2010، ص 443.

[4] احمد شوقي اللقاني، المرجع نفسه، ص 443.

[5] رشيدة بوكر، مرجع سابق، ص 514.

[6] رشيدة بوكر، المرجع نفسه، ص 515.

يدرس للقضاة مثل هذه المسائل أثناء التكوين إذ هوأمر ضروري وأكيد، أو خضوعهم للتدريب على كافة مستوياتهم ودرجاتهم على تقنية المعلومات.

فإذا كان القاضي مؤهلا في المجال المعلوماتي تمكن من السيطرة الفعلية على الجلسة وتمكن من المناقشة العلمية والفنية للأدلة العلمية المطروحة أمامه، ذلك أنه قد توفرت فيه المعارف الحسية والعقلية والمعلوماتية.

3 – استساغة الدليل عقلا: القاضي حر في اقتناعه بالدليل وله أن يؤسس حكمه عليه بالإدانة أو البراءة، ولا يخضع في ذلك لأية رقابة قضائية حيث أنه لا وجود لآلة مثلا تقيس لنا مدى اقتناع القاضي أو ما شابه، المهم في ذلك أن يسبب حكمه تسبيبا كافيا ويجب أن تكون الأسباب التي بنى عليها هذا الاقتناع يقبلها العقل والمنطق[1].

ثانيا: حجية الدليل الالكتروني في الإثبات

إن مجرد الحصول على الدليل الرقمي وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ الطبيعة الفنية الخاصة للدليل الرقمي تُمكِّن من العبث بمضمونه على نحو يحرّف الحقيقة دون أن يكون في قدرة غير المتخصص إدراك ذلك العبث، فضلاً عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة ، ولذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي[2]؟

لقد اختلفت أنظمة الإثبات في حجية الخرجات الالكترونية ولكن في القوانين ذات الصياغة اللاتينية فإنها لا تثير أي إشكال مثلما هو الشأن في القانون الفرنسي، الجزائري، الأردني وغيرهم، لمدى حرية تقديم هده الأدلة لإثبات الجرائم المعلوماتية، ولمدى حرية القاضي الجنائي في تقدير هذه الأدلة، أمام المحاكم أمام المحاكم الجنائية لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، والأدلة الجنائية الإلكترونية من هذا القبيل لكونها معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آليًا بأسلوب علمي[3].

المطلب الثاني

إجراءات التحقيق الجنائي

هناك بعض إجراءات التحقيق التي تعد منابع للأدلة وهي الانتقال والمعاينة، نذب الخبراء، سماع الشهود والتفتيش وليس لها أي ترتيب يجب إتباعه، بل يبدأ المحقق بما يراه ملائما

[1] نستثني أحكام محكمة الجنايات لأنها لا تسبب وتؤسس على الإجابات نعم أم لا على الأسئلة المطروحة، بواسطة الرئيس.

[2] طارق محمد الجملي ، الدليل الرقمي في مجال الإثبات الجنائي، عن http://www.startimes.com، يوم 2015/06/21.

[3] علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمد من التفتيش، دراسة مقارنة، 2009، ص13، عن الموقع الالكتروني: www.maljasem.com/ *يوم 2015/06/25.*

لظروف كل جريمة. إضافة إلى بعض الإجراءات المستحدثة لجمع الأدلة في مجال الجريمة المعلوماتية بوجه عام.وسيتضمن هذا المطلب إجراءات التحقيق الجنائي في الجريمة المعلوماتية باعتبار أن الجرائم ضد الأسرار المعلوماتية هي في الأصل جرائم معلوماتية.

الفرع الأول

الخبـــــرة الفنية وتدريب الكوادر

حاولت الجمع بين الخبرة وتدريب الكوادر في جزئية واحدة رغم أن الخبرة إجراء تحقيق بينما تدريب الكوادر هو آلية لمكافحة الجريمة بما يتناسب و الجريمة المستحدثة، ويخضع الكوادر إلى دورات التدريب وتبادل الخبرات على المستوى الإقليمي والدولي كآلية من آليات التعاون، في حين فضلت الجمع بينهما لسبب أن الكوادر في الأصل قد يستعينون بالخبراء وبعد تدريبهم على المجال المعلوماتي يمكننا اعتبارهم كالخبراء في عملهم.

أولا: الخبرة

إن إثبات الجريمة المعلوماتية عن طريق الأدلة الرقمية التي يتطلب اشتقاقها و كشف أنماطها أمر يتطلب أصحاب الخبرة و التخصص في هذا المجال الفني و التقني، ولطالما تم ندب هؤلاء الخبراء من طرف القضاة للاستعانة بهم في أمور فنية تتطلب خبرة خاصة.

الخبرة هي وسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية، وهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو المادي، وإنما هي تقييم لهذا الدليل[1].

قد تعتمد الخبرة من أجل كشف الجريمة المعلوماتية وهذا ما تحاول تطويره بعض الدول التي سنت تشريعات لمكافحة الجريمة المعلوماتية، والخبرة المطلوبة من أجل إثبات هذه الجريمة يجب أن تكون من نوع خاص يتماشى وخصوصية الجريمة المعلوماتية وقد تعمل بعض البلدان على إعادة تأهيل بعض ما يسمى بالمجرمين المعلوماتيين من أجل الاستفادة من خبراتهم في الاختراق، ويجب أن يتوفر الخبير على مؤهلات عالية ومقدرة فنية وخصوصا المعرفة التامة بتركيب الكمبيوتر، معرفة شاملة لشبكة الانترنت، التعامل مع الجريمة التي خلفتها التقنية الحديثة، كيفية عزل النظام المعلوماتي والحفاظ على الأدلة دون تلف[2].

ويشير الفقه الجنائي إلى أهمية الخبرة في التحقيق في الجريمة المعلوماتية والكشف عنها إذ تستعين أجهزة العدالة الجنائية الشرطة وسلطات التحقيق والمحاكمة بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الالكتروني، وذلك بغرض كشف غموض الجريمة أو تجميع أدلتها والمحافظة عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات

[1] أحمد فتحي سرور، الوسيط في شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السابعة، 1996 ص 588.

[2] أسامة أبوالحجاج، دليلك الشخصي إلى الانترنت، دار النهضة العربية، القاهرة ،1998 ، ص20.

الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق[1]، حيث تكتسب أهمية بالغة في مجال الجريمة المعلوماتية نظرا لأن الحاسبات وشبكات الاتصال أنواع ونماذج متعددة، كذلك فان علوم التقنيات المتصلة بها تنتمي إلى تخصصات علمية وفنية دقيقة ومتنوعة والتطورات في مجالها سريعة ومتلاحقة لدرجة قد يصعب معها على المتخصص تتبعها واستيعابها، ويمكن القول بصفة عامة بأنه لا يوجد حتى الآن خبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرامجها وشبكاتها وكذلك لا يوجد خبير قادر على التعامل مع كافة أنماط الجرائم التي تقع عليها أو ترتكب بواسطتها[2]، ربما للتطور المتجدد والسريع في هذا المجال.

فالمشرع الجزائري[3] أجاز للمحقق الاستعانة بالخبرة ومنه ندب خبير في أي وقت إلى أن ينتهي التحقيق وذلك ليتوصل إلى كشف الحقيقة بالسرعة اللازمة، فندب خبير في المسائل الفنية البحتة التي تتجاوز معارف جهة التحقيق والقاضي واجبة في مجال الجرائم المعلوماتية، حيث أنها تتعلق بمسائل غاية التعقيد إضافة إلى أن محل الجريمة المعلوماتية غير مادي والتطور في أساليب ارتكابها سريع ومتلاحق ولا يكشف غموضها إلا المتخصصون و اللذين هم على درجة كبيرة من التميز في تخصصهم فإجرام الذكاء والفن لا يكشفه إلا دكاء وفن مماثلين.

حيث أن المشرع الجزائري أجاز الاستعانة بالخبرة في الجريمة المعلوماتية من خلال نص المادة 05 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها إذ أشار من خلال النص إلى أنه يمكن للسطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخدة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

والجدير بالذكر أن المشرع الجزائري قرر الحماية اللازمة للخبير إذا ما سببت له المعلومات التي أفاد بها القضاء أي خطر حول حياته أو سلامته الجسدية أو سلامة أفراد

---

[1] رامي متولي القاضي، مرجع سابق، ص 112.

[2] علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، الناشر المكتب الجامعي الحديث، 2012 بدون طبعة، ص 26.

[3] هناك العديد من التشريعات من أوردت تعديلات لنصوص قانون الإجراءات الجزائية والذي يتضمن تنظيما لأعمال الخبرة في الجرائم المعلوماتية كالقانون البلجيكي الصادر في 2000/11/23 الذي يتضمن قانون تحقيق الجنايات بموجب نص المادة 88 منه حيث تضمن النص جواز استعانة مأمور الضبط وقاضي التحقيق بخبير ليقدم المعلومات والأدلة التي تعيين المحقق في إثبات وقوع الجريمة، كما يجيز لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أوعمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحولة أو المنقولة، في حين أن هناك بعض التشريعات تجيز الاستعانة بالخبير في التحقيق في الجريمة المعلوماتية كباقي الجرائم ولم تتصدى لتلك النصوص بالتعديل ومن بينها المشرع الجزائري في المادة ... من قانون الإجراءات الجزائية، ولنا رأي في ذلك حيث أنه باعتبار الجريمة المعلوماتية كباقي الجرائم وفي الأصل يمكن للخبير القيام بجميع الأعمال التي يحددها له القاضي في الأمر القاضي بتعيين خبير فلا داعي لتعديل النص وسرد بعض الأعمال التي تتعلق بالمجال المعلوماتي فيه.

عائلته أو أقاربه أو مصالحه الأساسية وذلك بموجب الأمر[1] 02/15 المعدل والمتمم لقانون الاجراءات الجزائية بموجب المواد 65 مكرر19 إلى 65مرر28.

ثانيا: تـــــدريب الكوادر.

طبيعة الجرائم الواقعة على الأسرار المعلوماتية تقتضي معرفة متميزة بنظم المعلوماتية وكيفية تشغيلها ووسائل إساءة استعمالها من قبل مستخدميها، ولا تتحقق هذه المعرفة التقنية إلا بتدريب القائمين على أعمال التحري، والمباشرين للتحقيق في مجال الجرائم المعلوماتية بصفة عامة، إلى الحد الذي دعا البعض إلى القول بضرورة وجود شرطة متخصصة، ونيابة متخصصة في هذا المجال، ففي الجزائر وعلى مستوى جهاز الشرطة أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بالجزائر العاصمة ومخبرين جهويين في كل من قسنطينة ووهران، أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.

ويجب أن يشتمل التدريب على كيفية تشغيل الحاسبات وكل الوسائل الالكترونية التي في حكمها، بعد التعرف على أنواعها ونظمها المختلفة، لاكتساب مهارات ومعارف تتعلق ببرمجة الحاسبات، والمعالجة الإلكترونية للبيانات والجرائم التي تقع على الأنظمة المعلوماتية، أو تستخدم الحاسبات وسيلة لارتكابها، وأساليب ارتكاب هذا النوع من الجرائم، فضلا عن أمن المعلومات ووسائل اختراقها، مع دراسة حالات تطبيقه لجرائم وقعت سلفا وكيف تم مواجهتها، وفي كثير من بلدان العالم تعقد الدورات التدريبية المتخصصة لرجال الشرطة وأعضاء النيابة العامة، والتحقيق سواء في مراكز تابعة لوزارة الداخلية أوفي المراكز المتخصصة التابعة لوزارة العدل.

ليس هذا فحسب بل لا بد وأن تسعى الأجهزة الأمنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات في المجال المعلوماتي وضمهم إليها ليكونوا ضمن كوادرها والاستفادة منهم ومن أجل ذلك ينبغي على كليات الشرطة من جهة أن تعمل جاهدة لقبول دفعات من الجامعين من خريجي كليات الحاسبات الآلية لتخرجهم ضباطاً مؤهلين قانونيا وتقنيا، كذلك يتعين على الكليات المعينة بتدريس القانون أن تسعى جاهدة إلى تدريس الحاسبات الآلية وكل ما يتعلق به إلى الطلبة، وأن تكون مادة الحاسب الآلي وتقنية المعلومات إحدى المواد الأساسية، لأن من شأن ذلك أن تتكون لدي خريجي هذه الكليات ثقافة قانونية وثقافة حاسوبية[2].

---

[1] الأمر رقم 02/15 المؤرخ في 23 يوليو سنة 2015 يعدل ويتمم الأمر رقم 155/66 المتضمن قانون الاجراءات الجزائية، الجريدة الرسمية العدد 40، ص 28.

[2] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مكافحة جرائم الانترنت، ص 44، عن *www.minshawi.com* يوم الاطلاع على الموقع 2015/06/22.

وكان للإتحاد الأوروبي[1] تجربة في مجال التدريب على مكافحة الجرائم المعلوماتية حيث يعتبر هذا الأخير من أهم الجهات التي قامت بالمشروعات والبرامج التدريبية الهادفة لمكافحة الجرائم عالية التقنية من خلال أحد مؤسساتها وهو مركز التدريب الوطني عن الجرائم التقنية NSLEC وقد أعد هذا المركز العديد من المشروعات والبرامج التي تتعامل مع مكافحة هذه الجرائم ولعل أهمها مشروع[2] فالكون 2001 وأيضا برنامج[3] أجيس 2004/2003.[4]

والتعاون الدولي في مجال تدريب رجال العدالة على مواجهة الجرائم المعلوماتية قد يكون بين الدول وأجهزة العدالة الجزائية لديها، فنجد في بعض الدول أنه مثلا يتم إرسال أعضاء النيابة العامة من مختلف الدرجات في برامج خارجية وذلك بالتعاون مع أجهزة النيابة العامة في الدول الأخرى والهيئات الدولية بهدف الإطلاع على أحدث النظم المقارنة.

وقد يتم التعاون الدولي في مجال تدريب الكوادر من خلال عقد ندوات ومؤتمرات أو ورش العمل الجماعي، متخصصة في مواجهة تلك الجرائم تعقد على المستوى الدولي أو الإقليمي، حيث تقدم هذه الفعاليات العلمية من أبحاثها ودراستها وموضوعات محاورها الضوء على المستجدات المتعلقة بالجرائم المستحدثة من خلال تحليل ومناقشة أبعادها بعقلية ناجحة مما يمكن المعنيين بالوقاية ومكافحة هذه الجرائم من التعرف على أساليب ارتكابها وأخطارها ووسائل الوقاية بأساليب تتناسب وتفوق أساليب ووسائل مرتكبيها، وعلى هامش هذه المؤتمرات أو الندوات أو ورش العمل الجماعي تعقد اللقاءات وتبادل الآراء والخبرات[5].

وباعتبار أن التعاون الدولي في يتحقق مجال تدريب الكوادر العاملين في أجهزة العدالة الجزائية والمعنيين بمكافحة الجريمة على المستوى الدولي، ومنه يمكننا القول أن هذه الصورة تعد الأكثر تطورا للتعاون الدولي، الذي يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين المشاركين في مكافحة الجريمة في الدول المختلفة من خلال تبادل الخبرة، والتعرف على أحدث التطورات في مجال الجريمة المعلوماتية وأساليب مكافحتها، وغالبا ما يجري مثل هذا التدريب من خلال المنظمات أو الدول[6].

---

[1] على مستوى الاتحاد الأوروبي تم انشاء الشرطة الأوروبية أو الأوروبول ومقره في مدينة لاهاي بهولندا وذلك في سنة 1992 وهو حلقة الوصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال عدة جرائم من بينها الجريمة المعلوماتية.أنظر في ذلك سعيداني نعيم، مرجع سابق، ص 108.

[2] ينظم هذا المشروع العديد من الدورات التدريبية في إطار الاتحاد الأوروبي تختص بمواجهة الجرائم المعلوماتية.

[3] يقوم المشروع على تطوير وتقديم برنامج تدريبي تعاوني حول الجريمة المعلوماتية للعاملين في أجهزة إنفاذ القانون الأوروبية، وتوفير إطار ابتكاري ومستديم في دول الاتحاد الأوروبي والدول المرشحة للانضمام إليه.

[4] رامي متولي القاضي، مرجع سابق، ص 167.

[5] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص 685 و686.

[6] استفادت اطارات من الشرطة الجزائرية بمعهد الشرطة الجنائية بالسحاولة الجزائر من دورة تكوينية لمكافحة الجريمة المعلوماتية، و التي دامت مدة خمسة أيام يشرف عليها وفد من الشرطة الايرانية لتبادل الخبرات عن أفضل والمساعدة التقنية والتعاون الدولي بغية تعزيز سبل مكافحة الجريمة المعلوماتية، هذا ما أفاد به بيان للمديرية العامة للأمن الوطني بالجزائر، للتفاصيل أكثر أنظر

الفرع الثاني
الانتقال ومعاينة مسرح الجريمة المعلوماتية

يقصد بالانتقال ذهاب مأموري الضبط القضائي أو المحقق الجنائي إلى المكان الذي ارتكبت فيه الجريمة، حيث توجد آثارها وأدلتها[1].

أما المعاينة يقصد بها فحص مكان أو شيء أو شخص له علاقة بالجريمة وإثبات حالته كمعاينة مكان ارتكاب الجريمة أو أداة المعاينة قد تكون إجراء تحقيق لإثبات ما بالجسم من جراح وما على الثياب من دماء أو ما بها من مزق أو ثقوب[2]. والمعاينة بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو إلى أي محل آخر توجد به أشياء أو آثار يرى المحقق أن لها صلة بالجريمة غير أن المحقق قد ينتقل لغرض آخر غير المعاينة كالتفتيش مثلا[3]، وفي الجريمة المعلوماتية يقصد بها معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت، وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من

---

http://www.elkhabar.com/press/article/87512/ يوم لاطلاع على الموقع 2017/03/12. كما أشرف خبراء من الاستخبارات المركزية الأمريكية وعملاء من مكتب التحقيقات الفدرالي، على ورشة تكوينية حول مكافحة الجريمة المعلوماتية لفائدة ضباط الشرطة القضائية والقضاة تهدف إلى إطلاعهم على آخر التكنولوجيات لمحاربة الجريمة وكيفية استخدام الأدلة الإلكترونية في التحقيق والمقاضاة وذلك في نوفمبر 2010.شارك في الإشراف على الورشة التدريبية ، خبراء من مكتب التدريب والمساعدة لتطوير المقاضاة عبر البحار قسم الجرائم الحاسوبية والملكية الفكرية، قسم الجريمة المنظمة وابتزاز الأموال التابعة لوزارة العدل الأمريكية، حسبما أفاد به بيان للسفارة الأمريكية بالجزائر.
استفاد من هذه الورشة التدريبية 10 ضباط من الشرطة القضائية و60 قاضيا متخصصا في الجريمة المنظمة في الجزائر، تلقوا تدريبات نظرية وتطبيقية عبر التعرف على تقنيات إجراءات التحري وإقامة الدليل على الجرائم المعلوماتية، وعلاقة الجريمة المعلوماتية بالجريمة المنظمة وأمن المعلومات والمعطيات وكيفية استغلال الانترنت والبريد الالكتروني وكذا التعاون الدولي في هذا المجال.وقال المدير العام للشؤون القضائية والقانونية لوزارة العدل، محمد عمارة، أن التعاون الدولي في مجال مكافحة الجريمة المنظمة بات أكثر من ضروي، وأشار في نهاية الدورة التدريبية إلى أن "أي دولة مهما بلغت من التطورلا يمكنها أن تكافح لوحدها أشكال الجرائم المتطورة التي يستخدم مقترفوها وسائل تكنولوجية حديثة ومتطورة". وأضاف بأن التعاون القضائي بين الجزائر والولايات المتحدة الأمريكية تدعّم أكثر بعد إمضاء اتفاقية التعاون في المجال الجزائي بين البلدين خلال زيارة وزير العدل الأمريكي إيريك هولدر إلى الجزائر في أفريل 2010 ، والتي تهدف إلى تحسين التعاون في مجال مكافحة الجرائم والتبادل الجيد للأدلة التي بإمكان المسؤولين في كلا البلدين استعمالها في سياق التحقيق ومقاضاة النشاط الإجرامي.ومن جانبه، قال سفير الولايات المتحدة الأمريكية بالجزائر، دافيد بيرس خلال هذه المناسبة، أن واشنطن مهتمة بإرساء ''شراكة أكثر فعالية بين الجزائر وبلاده في مجال مكافحة الجريمة المعلوماتية، حيث أنه من المفيد معرفة سلوك مقترف هذه الجريمة في الدول المختلفة''. مشيرا أنه من الضروري تشجيع الدول على تأسيس شراكة للتعاون الناجع والفعال بين وزارة العدل ومصالح الشرطة في مكافحة الجريمة المعلوماتية التي تشهد تطورا مستمرا ولا تحترم أية حدود أو تشريعات. ويسعى المجرمون للاستفادة من التكنولوجيات الجديدة والحدود القضائية للإفلات من العقاب واضطهاد الضعفاء من الأفراد والشركات. وأضاف السفير بيرس أن ''مقترفي الجريمة المعلوماتية يقومون يوميا بالاعتداء على أمن الخواص والمؤسسات والحكومات'' قبل أن يضيف أن هذه الجرائم تتخذ عدة أشكال. للتفاصيل أكثر أنظر http://www.algeriachannel.net/2010/11/ يوم الاطلاع على الموقع 2017/03/12.

[1] رامي متولي القاضي، مرجع سابق، ص 106.

[2] http://www.startimes.com/ يوم الاطلاع على الموقع 2015/08/02.

[3] خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012، ص 59.

خلال الكمبيوتر والشبكة العالمية[1].

والمعاينة جوازية للمحقق، شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم أولم يطلبوها. ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية، ومرد ذلك إلى اعتبارين:

1. الجرائم التي تقع على نظم المعلومات والشبكات قلما يترتب على ارتكابها آثار مادية.
2. أن عدد كبيرا من الأشخاص قد يتردد على مكان أو مسرح الجريمة خلال الفترة الزمنية التي تتوسط عادة ارتكاب الجريمة واكتشافها مما يهيئ الفرصة لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو زوال بعضها وهو ما يثير الشك في الدليل المستمد من المعانية وحتى تصبح معاينة مسرح الجريمة المعلوماتية لها فائدة في كشف الحقيقة عنها وعن مرتكبها فإنه ينبغي مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي[2]:

* تصوير الحاسب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته ويراعي تسجيل وقت وتاريخ ومكان التقاط كل صورة.
* العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام والآثار الإلكترونية وبوجه خاص السجلات الإلكترونية التي تتزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقة الولوج إلى النظام أو الموقع أوالدخول معه في حوار.
* ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن أجراء عملية المقارنة والتحليل حين عرض الأمر فيما بعد على القضاء.
*عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختيارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجالات لقوى مغناطيسية يمكن أن تتسبب في محو البيانات المسجلة.
*التحفظ على محتويات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة وغير السليمة أو المحطمة وفحصها ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.
*التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليه من بصمات.

---

[1] خالد ممدوح ، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي،الإسكندرية، 2009، ص

[2] هشام فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، بدون طبعة، 1994، ص 59، أ،ظر أيضا علي عدنان الفيل، مرجع سابق، ص 33- 35.

ويلاحظ أن الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الكمبيوتر من الممكن أن تكون ثرية جداً فيما تحتويه من معلومات مثل صفحات المواقع المختلفة والبريد الإلكتروني، الفيديو الرقمي الصوت الرقمي، غرف الدردشة والمحادثة، الملفات المخزنة في الكمبيوتر الشخصي ، الصورة المرئية الدخول للخدمة والاتصال بالإنترنت والشبكة عن طريق مزود الخدمات[1]، وللفهم الدقيق للمعاينة لابد من التعرف على المقصود من مسرح الجريمة في الجريمة الالكترونية.

عموما لم تهتم معظم التشريعات الجنائية المعاصرة بتعريف مسرح الجريمة أو وضع معايير ثابتة لتحديد نطاقه المكاني كما هو الشأن بالنسبة للتفتيش بل أن هذا التحديد لم يحظ كثيراً باهتمام الفقه والقضاء الجنائي على نفس النحو الذي حظي به التفتيش فمعظم التشريعات تعبر عن مسرح الجريمة بمحل الواقعة، وتتفق معظم تعريفات رجال الفقه على أن مسرح الجريمة هو المكان الذي وقعت فيه الجريمة كلها أو بعضها بحيث يتخلف فيه آثار ارتكابها[2]، ويرجع عدم الاهتمام التشريعي بتعريف مسرح الجريمة وتحديد معالمه المكانية على وجه مفصل إلى اعتبارين[3]. **الأول** يتمثل في أن معظم القوانين الجنائية لا ترتب عادة آثار قانونية بالبطلان أو الانعدام على تجاوز الحدود المكانية لما هو معروف بمصطلح " **مسرح الجريمة** " عند إجراء المعاينة تاركاً للمحقق أو القائم بالمعاينة تقدير دائرة نشاطه الإجرائي في المعاينة داخل محيط اختصاصه الوظيفي حسبما يراه وفقاً لما تقتضيه مصلحة التحقيق طالما أن التوسع الميداني في هذا الإجراء ليس فيه مساس بخرق مستودع سر الغير في مسكنه أو محله الخاص وليس فيه خروج على قواعد الاختصاص .

بينما يتمثل **الثاني** في أنه لا تثور عادة بشأن تحديد المجال الميداني لمسرح الجريمة منازعة أو جدل بين الخصوم في الدعوى الجنائية (الدفاع أو الاتهام) أو طلب بطلان الإجراء تأسيساً على تجاوز هذا النطاق المكاني وذلك فيما لم تتناوله التشريعات بتفصيل أو تحديد كما هو الشأن بالنسبة للتفتيش الذي يمثل مساساً بحرمة الأفراد ومستودع أسرارهم ومن ناحية أخرى فالمعاينة إجراء واجب من إجراءات التحقيق تفرضه القوانين على رجال الضبط والتحقيق بمجرد علمهم بوقوع الجريمة أو تبليغها إليهم وبالتالي فلا يجوز لأي خصم أو طرف أن يعترض على إجراء معاينة مسرح الجريمة أو على طريقة أو أسلوب تنفيذها أو مجالها الميداني إذ أن المعاينة تستهدف التعرف على أبعاد الجريمة وأركانها وظروفها وكشف الحقيقة بشأنها وليست إجراء موجه ضد شخص معين ماساً بحرمة مستودع سره حتى ينشأ له حق الطعن فيه بالبطلان .

---

[1] http://www.kenanaolinecom وأيضا http://www.th3professional.com/.2014/10/24 يوم

[2] خالد ممدوح ابراهيم، المرجع السابق، ص 166.

[3] خالد ممدوح ابراهيم، المرجع نفسه، ص 166 وما بعدها .

ومن جانب آخر، فقد تكون معاينة مسرح الجريمة أول إجراء يقوم به المحقق بعد تلقي البلاغ أو إخطاره به. وذلك في ظروف قد لا يكون فيها عنصر الخصوم أو المتهمين قد ظهر بعد بهذه الصفة على ساحة التحقيق وذلك بخلاف التفتيش، الذي لا يجري إلا في مواجهة شخصية وجه إليها الاتهام وإذا تناول التفتيش مكاناً فهو مستودع السر الذي يلزم أن يكون معيناً على وجه التحديد التعين النافي للجهالة ، وهو ما اهتمت به التشريعات والفقه والقضاء وأحاطته بضمانات كافية .

ويمكن تعريف مسرح الجريمة بأنه " هو كل محل أو وحدة من منشأة أو رقعة من الأرض تضم بؤرة الجريمة ومركزها بحيث تكون ميداناً لأنشطة الجاني أو الجناة من الفاعلين الأصليين عند ارتكاب الأفعال المؤثمة جنائياً والتي تدخل في عداد الأعمال التنفيذية المكونة للجريمة أو الشروع فيها ".

ويدخل في عداد ذلك الملحقات المتصلة التي تكون مع المكان وحدة واحدة وهذا النطاق المكاني يكتسب صفة مسرح ارتكاب الجريمة من واقع احتوائه على مركز وقوعها بداخله ووجود آثار ومخلفات ارتكابها أواحتمال وجود ذلك .

ويجب أن تكون هذه المواقع ميداناً لأنشطة الجاني الذي ارتكب الجريمة وحده" أو الجناة من الفاعلين الأصليين عند تعددهم "ومارسوا أفعالاً تضفي عليهم هذه الصفة وذلك بارتكاب كل أو بعض الأعمال التنفيذية للجريمة أو الشروع فيها .

الفرع الثالث
التفتيش في مجال الجريمة المعلوماتية

التفتيش في قانون الإجراءات الجزائية هو البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة[1]، وقد أحاط القانون هذا التفتيش بضمانات عديدة ومحل التفتيش إما أن يكون مسكنا أو شخصا، وهو بنوعية قد يكون متعلقا بالمتهم أو بغيره وهو في كل أحواله جائز مع الاختلاف في بعض الشروط.

[1] الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار الفكر الجامعي الإسكندرية، الطبعة الأولى، 2011، ص 196.

فالتفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة بينما البيانات الالكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي، ومع ذلك يمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الالكترونية لحفظها وتخزينها كالأسطوانات الممغنطة، ومخرجات الحاسبات الالكترونية، لهذا فقد أجاز الفقه والتشريعات التي صدرت في هذا المجال إمكانية أن يكون محل للتفتيش البيانات المعالجة الكترونيا والمخزنة بالحاسب الآلي، ثم ضبطها والتحفظ عليها أو ضبط الوسائط الالكترونية التي سجلت عليها هذه البيانات، والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام[1].

فالتفتيش أو البحث في الشبكات الالكترونية يسمح باستخدام الوسائل الالكترونية للبحث في أي مكان عن البيانات أو الأدلة المطلوبة[2]، وقد عرف المجلس الأوروبي هذا النوع من التفتيش بأنه إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني[3]. وفي هدا السياق سوف نفصل في هذا الإجراء من خلال النقاط التالية:

أولا:مدى قابلية مكونات وشبكات الحاسب الآلي للتفتيش

يتكون الحاسب الآلي من مكونات مادية ومكونات معنوية كما أن له شبكات اتصالات بعدية سلكية ولا سلكية سواء على المستوى المحلي أو المستوى الدولي فهل تخضع هذه المكونات للتفتيش؟.

1- مدى خضوع مكونات الحاسب المادية للتفتيش

إن التفتيش الواقع على المكونات المادية للنظام المعلوماتي لا إشكال فيه حيث أن نص المادة 44 من قانون الإجراءات الجزائية الجزائري ورد فيه بأن التفتيش يرد على الأشياء، وهي كلمة تنصرف على الأرجح على المكونات المادية، مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها.

يخضع الولوج في المكونات المادية للحاسب بحثا عن شيء يتصل بجريمة معلوماتية وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، للإجراءات القانونية الخاصة بالتفتيش وبعبارة أخرى فإن جواز تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو مكان عام أم مكان خاص، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش فإذا كانت

[1] علي عدنان الفيل، مرجع سابق، ص 39.

[2] علي عدنان الفيل، المرجع نفسه، ص 39.

[3] conseil de l eurpe , problemes de procedure penale lies a la technologie de l information , recommendation n .r(95) 13 et expose des motif . ed. conceil de l europe 1996 , p 28.

موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونيا في التشريعات المختلفة[1]، كالقانون الجزائري حيث نصت المادة 64 من قانون الإجراءات الجزائية والتي قيدت ممارسة هذا الإجراء بالشروط التالية:

- الحصول على إذن للتفتيش من وكيل الجمهورية واستظهار هذه المذكرة قبل بدء العملية، وتتضمن مذكرة التفتيش البيانات التالية: وصف الجريمة محل البحث والتحري، عنوان الأماكن التي سيتم تفتيشها، عدم ذكر هذه البيانات تؤدي إلى بطلان إجراء التفتيش.

- أن يجرى التفتيش بحضور صاحب المسكن وإن تعذر وجب تعيين ممثل له وإن تعذر الأمر كذلك يقوم ضابط الشرطة القضائية بتعيين شاهدين لا علاقة لهما(المادة45 من ق ا ج).

- أن يجري التفتيش بعد الساعة الخامسة 05 صباحا وقبل الساعة 08 مساءا غير أنه يجوز التفتيش في أي وقت إذا طلب صاحب المسكن ذلك أو إذا سمعت نداءات من داخل المسكن كما يجوز تفتيش الفنادق والمحلات والنوادي والمقاهي وأماكن المشاهدة العامة (المسرح، السينما) وكل مكان مفتوح للجمهور في أي ساعة ليلا ونهارا.

هذا وقد استثنى عن القاعدة العامة في المادة 64 السالفة الذكر بموجب الفقرة 3 من نفس المادة تطبيق هذه الضمانات على بعض الجرائم محيلا ذلك إلى المادة 47 في الفقرة 3 حيث أجازت أن يتم التفتيش والمعاينة في المساكن في كل ساعة ليلا ونهارا ودون التقيد لشرط حضور صاحب المسكن أو ممثيله إذا تعلق الأمر بالجرائم التالية":..... الجرائم الماسة بأنظمة ممارسة المعالجة الآلية للمعطيات".

ويجب التمييز داخل المكان الخاص بين ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحاسبات الأخرى أم أنها متصلة بحاسب أو بنهاية طرفية في مكان آخر كمسكن لا يخص مسكن المتهم، فإذا كانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيش هذه الأماكن، أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب الآلي المادية أو كان مسيطرا عليها أو حائزا لها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص بنفس الضمانات والقيود المنصوص عليها في هذا المجال[2] .

2- مدى خضوع مكونات الحاسب المعنوية للتفتيش:

أثار تفتيش المكونات المنطقية للحاسب الآلي خلافا كبيرا في الفقه بشأن جواز تفتيشها من عدمه فصلاحية المكونات المعنوية للتفتيش هي محل جدلبين موقفين، **فالرأي الأول**

[1] علي عدنان الفيل، مرجع سابق، ص 41.

[2] علي عدنان الفيل، مرجع سابق،ص 41.

يذهب إلى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فإن هذا المفهوم المادي لا ينطبق على بيانات الحاسب الآلي غير المحسوسة أو الملموسة ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي)، وبذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب . ويرى بعض الفقهاء في فرنسا أن النبضات الإلكترونية أو الإشارات الإلكترونية الممغنطة لا تعد من قبيل الأشياء المحسوسة وبالتالي لا تعتبر شيئا ماديا بالمعنى المألوف للمصطلح ولذا لا يمكن ضبطه[1].

وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم 34 من القواعد الفيدرالية الخاصة بالإجراءات الجنائية عام 1970 لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول وعن طريق الفاكس[2].

أما الرأي الثاني فهو على النقيض من الرأي الأول فهو يرى على أنه يسمح بضبط بيانات الحاسب غير المحسوسة أي يجوز ضبط البيانات الالكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك على القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أي شيء) وبذلك يمكن تفسيره أنه يشمل بيانات الحاسب الآلي المحسوسة وغير المحسوسة، لأن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن المفهوم يمتد ليشمل البيانات الالكترونية بمختلف أشكالها[3] .

وفي هذا المعنى نجد المادة 251 من قانون الإجراءات الجنائي اليوناني تعطي سلطات التحقيق إمكانية القيام (بأي شيء يكون ضروريا لجمع وحماية الدليل) ويفسر الفقه اليوناني عبارة أي شيء بأنها تشتمل بالضبط البيانات المخزنة أو المعالجة إليكترونيا، ولذلك فإن ضبط البيانات المخزنة في الذاكرة الداخلية للحاسب الآلي لا تشكل أية مشكلة في اليونان إذ بمقدور المحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية، وتمنح المادة 487 من القانون الجنائي الكندي سلطة إصدار إذن لضبط أي شيء طالما تتوفر أسس معقولة للاعتقاد بأن الجريمة ارتكبت أو يشتبه في ارتكابها أو أن هناك نية في أن يستخدم في ارتكاب الجريمة أو أنه سوف ينتج دليلا على وقوع الجريمة[4].

أما عن المشرع الجزائري فإنه استجاب للرأي القائل –أي الثاني- بأن طبيعة المعلومات المعالجة تتطلب قواعد خاصة وعلى هذا الأساس أجاز تفتيش المعطيات ولكن

---

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 653.

[2] عبد الفتاح بيومي حجازي، المرجع نفسه، ص 657.

[3] علي عدنان الفيل، المرجع السابق،ص 42.

[4] علي عدنان الفيل، المرجع نفسه، ص 42.

بموجب نص جديد وهو المادة 5 من القانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث سمح لضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 من هذا القانون ومن بين هذه الحالات توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام أوالدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وللوقاية من الجرائم الماسة بأمن الدولة، الدخول بغرض التفتيش ولوعن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها وكذا منظومة تخزين معلوماتية[1].

وبالنسبة للتشريع الفرنسي فإنه أرسى القواعد التي تسمح بالتفتيش في البيئة الإلكترونية حيث نصت المادة 56على أنه " في حالة ما إذا كانت الجريمة المرتكبة مما يمكن إثباته بواسطة معطيات أو وثائق معلوماتية توجد في حوزة الغير، فإنه يمكن لضابط الشرطة القضائية أن ينتقل إلى مقر هذا الأخير لإجراء تفتيش وتحرير محضر في الموضوع "، كما نصت الفقرتين الخامسة والسادسة من المادة 56أيضا على أنه " يتم حجز المعطيات والبرامج المعلوماتية الضرورية لإظهار الحقيقة بوضع الدعامات المادية المتضمنة لهذه المعلومات رهن إشارة العدالة أوبأخذ نسخ منها بحضور الأشخاص الذين حضروا التفتيش ".

ثانيا: التفتيش عن بعد

التفتيش عن بعد هو نتيجة لطبيعة التكنولوجيا الرقمية، وهنا نميز بين ثلاث احتمالات:

آ-الاحتمال الأول: اتصال حاسب المتهم بحاسب أو نهاية طرفيه موجودة في مكان آخر داخل الدولة، فهناك من الدول من وجدت حلا للإشكالية المتعلقة بمدى جواز امتداد التفتيش إلى الأجهزة الأخرى المتصلة بجهاز المتهم أو المشتبه فيه، أم يقتصر على جهازه فقط؟، ومنها المشرع الجزائري حيث نصت المادة 05 في الفقرة 2 من القانون رقم 04/09 بأنه " في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذا كانت هناك أسباب تدعوا للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك ..." وكذلك المشرع الفرنسي حيث أضاف المادة 1/57 من قانون الإجراءات الجزائية. ويرى الفقه الألماني أيضا بشأن مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو طرفية في مكان آخر مملوك لشخص غير المتهم، أنه يمكن أن يمتد التفتيش

[1] رشيدة بوكر، المرجع السابق، ص 398.

في هذه الحالة إلى سجلات البيانات التي تكون في موقع أخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجنائية الألماني.

كما نص مشروع قانون جرائم الحاسب الآلي في هولندا على جواز أن يمتد التفتيش إلى نظم المعلومات الموجودة في موقع آخر بشرط أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس من المادة 125) وذلك بمراعاة بعض القيود[1].

كما نصت المادة 17 فقرة (أ) من القانون الفرنسي رقم 2003/239 بشأن الأمن الداخلي المؤرخ في مارس 2003 بأنه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي على البيانات التي تهم عملية البحث و التحري، فتنص المادة 17 منه على أنه :" يجوز لرجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتم فيها التفتيش على البيانات التي تهم التحقيق و المخزنة في النظام المذكور أو في أي نظام معلوماتي آخر مادامت هذه البيانات متصلة في شبكة واحدة مع النظام الرئيسي أو يتم الدخول إليها أو تكون متاحة ابتداءا من النظام الرئيسي"[2].

وتسمح الاتفاقية الأوروبية لجرائم تقنية المعلومات لعام 2001 للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز حاسب آلي معين إلى غيره، من الأجهزة المرتبطة به في حالة الاستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش، فتنص الفقرة الثانية من المادة 19 من القسم الرابع على أنه من حق السلطة القائمة بتفتيش الحاسوب المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمد التفتيش إلى جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الحاسب الآلي محل التفتيش[3].

ب-الاحتمال الثاني: اتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة، لأن من المتصور طبقا لهذا الاحتمال أن يقوم مرتكبوا الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصال البعيدة بهدف عرقلة سلطات الإدعاء في جميع الأدلة[4].

ووفقا لما جاء بتقرير المجلس الأوروبي فإن الاختراق المباشر يعتبر انتهاكا لسيادة دولة أخرى ما لم توجد اتفاقية دولية في هذا الشأن ويؤيد الفقه الألماني ما جاء بتقرير المجلس الأوروبي حيث أن السماح باسترجاع البيانات التي تم تخزينها بالخارج يعتبر انتهاكا لحقوق السيادة لدولة أخرى وخرقا للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون في

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص 655 ، عن هلالي عبد الله، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 1998، ص 375.

[2] عاشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الأزاريطة، 2010، ص 93 -94.

[3] رشيدة بوكر، المرجع السابق، ص403.

[4] عبد الفتاح بيومي حجازي، المرجع نفسه، ص 655.

مجال العدالة القضائية[1]، وقد أيد القضاء الألماني هذا الاتجاه حيث أسفر البحث في إحدى جرائم الغش المعلوماتي عن وجود طرفية حاسب في ألمانيا متصلة بشبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها وعندما أرادت سلطات التحقيق الألمانية الحصول على هذه البيانات لم يتحقق لها ذلك إلا من خلال طلب المساعدة المتبادلة، وقد ساور الاعتقاد الشرطة اليابانية بأن مجموعة من المخربين قد استخدمت أجهزة كمبيوتر في الصين والولايات المتحدة في مهاجمة العديد من المواقع الخاصة للحكومة اليابانية على الشبكة وقد طالبت الشرطة اليابانية كل من بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الكمبيوتر في كل من هاتين الدولتين حتى تتمكن من الوصول إلى جذور هذه العملية الإرهابية[2].

فضلاً عن ذلك فإن الجريمة قد ترتكب في إقليم دولة ما وتمتد آثارها إلى إقليم دولة أخرى، فإذا كانت هذه الدولة مختصة بالتحقيق في هذه الجريمة لأن قانون عقوباتها واجب التطبيق، فإن التساؤل يثور حول مدى إمكانية تفتيش تلك الآلة الموجودة خارج الإقليم بواسطة السلطات التابعة لهذه الدولـة ؟

إن اختصاص الدولة بالتحقيق في جريمة ما وإن كان يخولها تطبيق قانون إجراءاتها بشأن هذا التحقيق بصرف النظر عن مكان وقوع الجريمة مادامت خاضعة لقانون العقوبات الخـاص بها، إلا أن ذلك لا يعني أن تباشر الدولة هذه الإجراءات خارج إقليمها، إذ يتعذر على الدولة مباشرة اختصاصاتها بالتحقيق خارج إقليمها،لأن ذلك من مظاهر سيادتها فلا يسمح لها بممارسته على إقليم دولة أخرى ولذا فمن المتعذر قانوناً مباشرة الدولة المختصة بالتحقيق لأي إجراء خارج إقليمها بشأن الجريمة رغم انعقاد اختصاصها بالتحقيق فيها، ولذا تبدو مشكلة الحصول على دليل بشأن بعض الجرائم إذا كان الدليل المراد الحصول عليه يوجد في جهاز موجود في دولة أخرى في إطار الإشكالية المعروضة، إذ لن تتمكن سلطات التحقيق من الحصول عليه، ولذا تبدو اتفاقيات الإنابة القضائية هي السبيل لتحصيل هذا الدليل بحيث تُقوَّض الدولة الأخرى في جمع هذا الدليل وإرساله لدولة التحقيق، وقد نصت المادة 25 /أ من قانون الحاسوب الهولندي على الاعتداد بالدليل المتحصل عليه في إقليم دولة أخرى إذا تم ذلك تنفيذاً لاتفاقيات التعاون الأمني والقضائي، وأحياناً تكون تلك الدولة مختصة هي الأخرى بالتحقيق في هذه الجريمة، ولذا فإن هي لم ترغب في مباشرة التحقيق بشأنها قد تتطوع بتزويد دولة التحقيق بالبيانات التي تم ضبطها وفقاً لما يعرف بنظام تبادل المعلومات أو المساعدات ، وقد نصت اتفاقية بودابست على هذا النظام في المادة 1/25 بقولها " تقوم الدول الأطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض إلى أقصى حد ممكن، وذلك للإغراض الخاصة بعمليات التحقيق أو الإجراءات المتعلقة

[1] عبد الفتاح بيومي حجازي، المرجع نفسه، ص 656.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 656 -657 .

بالجرائم التي لها علاقة بنظم وبيانات الكومبيوتر، أو بالنسبة لتجميع الأدلة الخاصة بالجريمة في شكل الكتروني".

أيضا المشرع الفرنسي في المادة**1/57** من قانون الإجراءات الجزائية والتي سمحت صراحة بمباشرة بعض إجراءات البحث عن الجريمة الإلكترونية خارج الحدود الإقليمية كإمكانية تفتيش الأنظمة المعلوماتية المتصلة حتى ولوكانت متواجدة خارج إقليم الدولية، حيث سمحت المادة المذكورة لضباط الشرطة القضائية بأن يقوموا بتفتيش الأنظمة المتصلة حتى ولو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية.

وكذلك المشرع الجزائري قام بإجازة تفتيش الأنظمة حتى ولو كانت خارج إقليم الدولة وذلك بموجب المادة 5 في الفقرة 3 منها من القانون 04/09 حيث أجاز النص الحصول على المعطيات المبحوث عنها والمخزنة في الأنظمة المتصلة الواقعة خارج الإقليم الوطني والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى وذلك بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل. وكذلك أكد بموجب نص المادة 16 من ذات القانون على أنه وفي إطار التحقيقات والتحريات القضائية التي تمت مباشرتها، وتتبع الجرائم المنصوص عليها في ذات القانون والكشف عن مرتكبيها، فإن السلطات المختصة بإمكانها تبادل المساعدات القضائية على المستوى الدولي.

ونصت المادة 2/16 أيضا من ذات القانون أنه من واجب سلطات التحقيق الجزائرية أن تقدم جميع التسهيلات لمراقبة الاتصالات وتفتيش المنظومات المعلوماتية الموجودة على التراب الوطني متى طلب منها ذلك مع مراعاة مبدأ المعاملة بالمثل والاتفاقيات الدولية.

وفي نص المادة 18 من نفس القانون أي القانون 04/09 حيث أورد المشرع استثناءات على طلب المساعدة القضائية، وهي الحالة التي يمكن أن تؤدي إلى المساس بالسيدة الوطنية أو النظام العام، كما اشترط المشرع الجزائري قبول المساعدة القضائية بضرورة الالتزام بالمحافظة على سرية المعلومات المبلغة، وبشرط عدم استعمالها في غير الأغراض التي أدت إلى تجميعها.

كذلك الشأن بالنسبة للمشرع الفرنسي حيث أجاز بموجب الفقرة 2 من المادة 57-1 من قانون الإجراءات الجزائية المضاف بموجب المادة 17 الفقرة 2 من قانون الأمن الداخلي رقم 239- 2003.

ج-الاحتمال الثالث: التصنت والمراقبة الإلكترونية لشبكات الحاسب الآلي، فالتصنت والأشكال الأخرى للمراقبة الالكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريبا، مثلما هو الأمر بالنسبة للمشرع الجزائري في المادة

04 في الفقرة "ج" من القانون 04/09 أجاز النص استثناء المراقبة الالكترونية للوصول إلى الحقيقة واشترط أن تكون هي الحل الوحيد للوصول إلى الحقيقة.

وبالنسبة للمشرع الفرنسي نجد حالتين أجاز فيهما إمكانية مراقبة الاتصالات وهما الحالة المنصوص عليها في قانون الإجراءات الجزائية في المادة 100 وهي الحالة المتعلقة بالمراقبة بغرض تحقيق قضائي، وكان التحقيق في الجرائم التي هي على درجة من الخطورة[1]، والحالة الثانية هي الحالة الواردة في نص المادة 03 من القانون رقم 669/2004 المعدل للقانون 91/ 646الخاص بحماية المراسلات التي تتم عن طريق وسائل الاتصال عن بعد، حيث أجازت المادة بصفة استثنائية على النحو المنصوص عليه في المادة الرابعة من ذات القانون التي تنص على حماية الاتصالات الالكترونية أن يتم الترخيص باعتراض المراسلات الالكترونية بالوسائل الفنية، لأغراض البحث عن المعلومات التي تمس الأمن القومي والمحافظة على العناصر الأساسية للمكون العلمي والاقتصادي للبلاد، والوقاية من الإرهاب ومنع الجريمة المنظمة.

وأما عن السلطة المختصة بالتفتيش فيختص قاضي التحقيق أصلا بإجراء التفتيش تساعده النيابة العامة بتوليها تتبع الجرائم واتخاذ الإجراءات الملائمة بصددها ثم يخطر قاضي التحقيق الذي يتولى مباشرة التحقيق، فالنيابة توجه الاتهام والتحقيق يباشر إجراءات التحقيق.

ولقد نصت المادتين 81 و82 من قانون الإجراءات الجزائية على أنه يجوز لقاضي التحقيق القيام بإجراء التفتيش في أي مسكن يرى أنه توجد به أشياء يفيد اكتشافها في إظهار الحقيقة ولقد أجازت المادة 83 قانون الإجراءات الجزائية لقاضي التحقيق القيام بنفسه بالتفتيش في أي مكان آخر وبالتالي أي مسكن آخر غير مسكن المتهم ليضبط أدوات الجريمة أو ما نتج عن ارتكابها وكل شيء آخر يفيد في كشف الحقيقة، كما منحته المادة84 قانون الإجراءات الجزائية حق إنابة احد ضباط الشرطة القضائية للقيام بهذا التفتيش إذا استحال على قاضي التحقيق تنفيذ هذا التفتيش بنفسه وطبقا للشروط التي نصت عليها المواد 138 إلى 142 قانون الإجراءات الجزائية إذ أن المشرع الجزائري قيد سلطة قاضي التحقيق في منح الإنابة بشرط استحالة قيامه بالإجراء بنفسه نظرا لخطورة السلطات التي يملكها قاضي التحقيق ومنها التفتيش.

[1] حد تلك الخطورة بأن تكون العقوبة المقررة لها الحبس من سنتين أوأكثر على أن لا تزيد المراقبة على أربعة أشهر في جميع الأحوال.

وبالنسبة لضباط الشرطة القضائية فإن من الممكن أيضا أن يقوم بعملية التفتيش حيث يتم التفتيش بمعرفة ضباط الشرطة القضائية في الجرائم المتلبس بها ولقد نصت المادة 15 ق.إ.ج على أعضاء الضبطية القضائية الذين لهم صفة ضابط الشرطة القضائية، إذ نص القانون على ضرورة إجراء التفتيش من طرف ضابط يساعده أعوان ولكن يتم الإجراء بحضوره وتحت إشرافه وإلا وقع باطلا.

ثالثا: ضوابط تفتيش نظم الحاسب الآلي الإجرائية

سنحاول أن نسرد بعض التفصيل في الضوابط الموضوعية والشكلية لعملية التفتيش وسنقصرها على المشرع الجزائري، حيث أننا نخص التفتيش داخل منظومة معلوماتية وهي كالتالي:

1 - الضوابط الموضوعية لإجراء التفتيش:

يقصد بالضوابط الموضوعية الشروط اللازمة لإجراء تفتيش صحيح وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاثة شروط أساسية هي: السبب والمحل والسلطة المختصة بالقيام بالتفتيش وسنتم التفصيل فيها كالتالي:

آ- سبب التفتيش: سبب التفتيش يعني السعي نحو الحصول على الدليل في تحقيق قائم، من أجل الوصول إلى حقيقة الحدث[1]، و لابد لتحقق السبب أولا وقوع جريمة من جرائم الاعتداء على نظام المعالجة الآلية للمعطيات.

حيث يقتضي المنطق العقلي و القانوني للقيام بإجراء التفتيش وقوع جريمة جناية أو جنحة و تستبعد المخالفة لضآلة خطورتها، و الملاحظ أنه لا محل لإصدار إذن بتفتيش نظم المعالجة الآلية للمعطيات إلا إذا كان المشرع قد نص على الجرائم التي تشكل اعتداءا عليها في شكل نصوص التجريم و العقاب تطبيقا لمبدأ شرعية الجرائم و العقوبات، و ذلك ما قامت به الكثير التشريعات المقارنة و قام به المشرع الجزائري ن خلال القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 حيث أدرج فصلا خاصا بجرائم الاعتداء على نظم المعالجة الآلية للمعطيات(الفصل السابع) و عزز هذه الحماية بموجب القانون رقم 04/09 المؤرخ في 5 أوت في 2009 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحته.

ولابد كذلك من وجود شخص أو أشخاص معينين وجه لهم الاتهام بالجريمة أو المشاركة أو الشروع فيها، حيث ينبغي أن تتوافر في حق الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية تدعوا إلى الاعتقاد المعقول بأنه قد ساهم في ارتكاب الجريمة المعلوماتية بوصفه

[1] قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري و المقارن، منشأة المعارف بالأسكندرية، 2005، ص 53.

فاعلا أصليا أو شريكا فيها مما يستوجب اتهامه بها، وحيث أن قوانين الإجراءات الجزائية لم تعرف الدلائل بينما عرفها الفقه بالنسبة لجرائم الاعتداء على المعالجة الآلية للمعطيات أنها مجموعة من المظاهر أو الأمرات التي تكفي وفق السياق العقلي و المنطقي أن ترجح جريمة من جرائم نظم المعالجة الآلية إلى شخص معين سواء بوصفه فاعلا أو شريكا[1].

وكشرط أخير من شروط السبب أن تتوافر أمارات قوية أو قرائن وأشياء أو أجهزة أو معدات تفيد في كشف الحقيقة، لدى المتهم المعلوماتي وغيره، حيث يجب أن تتوافر لدى سلطات التحقيق أسباب كافية أنه يوجد في المكان أو لدى الشخص المراد تفتيشه هو أو غيره أدوات استخدمت في جريمة من جرائم الاعتداء على نظم المعالجة الآلية أو أشياء متحصلة منها.

ب- محل التفتيش:

يقصد بالمحل المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة[2]، ومحل التفتيش في النظام المعلوماتي هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به بالإضافة إلى الأشخاص الذين يستخدمون الحاسوب محل التفتيش[3].

ج - السلطة المختصة بالتفتيش :

باعتبار أن إجراء التفتيش من إجراءات التحقيق الابتدائي والتي تمس بالحرية الشخصية وانتهاك حرمة الحياة الخاصة للأفراد، حرص المشرع الجزائي على العموم على إسناد مهمة التفتيش لجهة قضائية تكفل تلك الحقوق والحريات وتضمنها، وحدد الجهة المختصة بالتفتيش في قاضي التحقيق حيث يختص بإجراء التفتيش وتساعده النيابة العامة بتوليها تتبع الجرائم واتخاذ الإجراءات الملائمة بصددها.

2 -الضوابط الشكلية لإجراء التفتيش:

[1] هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي، المرجع السابق، ص 121.

[2] قدري عبد الفتاح الشهاوي، مرجع سابق، ص 110.

[3] خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر و التوزيع، عمان الأردن، الطبعة الأولى، 2011، ص 154، أشار إليه صالح البريري، دور الشرطة في مكافحة جرائم الانترنت، مؤتمر الجوانب القانونية و الأمنية، للعمليات الالكترونية، دبي 2003، ص 392.

سنحاول أن نسرد بعض التفصيل في الضوابط الشكلية لعملية التفتيش وسنقصرها على المشرع الجزائري، كالتالي:

أ-الحضور الضروري لبعض الأشخاص

يستوجب إجراء التفتيش عند مباشرته سواء تم بمعرفة سلطة التحقيق أم بمعرفة الشرطة القضائية وجوب حضور أشخاص عند مباشرته، وأول من يتعين حضوره هو المتهم، ويعتبر هذا شرطا مفترضا إذا ما تعلق الأمر بتفتيش شخصه، وذلك على خلاف تفتيش المساكن إذ من المتصور إجراء التفتيش بغير حضور المشتبه فيه متى كان حضوره غير ممكن، وبخلاف المتهم الذي يتعين حضوره قد يتطلب الأمر حضور بعض الشهود لأجراء التفتيش.

فلقد نصت المادة 45 من قانون الإجراءات الجزائية في فقرتها الأولى على ضرورة حضور صاحب المسكن عملية التفتيش، فاذا تعذر عليه الحضور لسبب ما مثل السفر فإنه يتعين عليه تعيين ممثل له بناءا على أمر مكتوب من ضابط الشرطة القضائية المكلف بالتفتيش وينوه عن ذلك في محضر التفتيش، فإذا أمتنع صاحب المسكن أوكان هاربا فإن ضابط الشرطة القضائية المكلف بإجراء التفتيش يستدعى شاهدين شريطة أن لا يكونا من الموظفين الخاضعين لسلطته، ويجب أن يتضمن محضر التفتيش اسمهما ولقبهما وكل البيانات المتعلقة بالتفتيش، ويتم تسخير الشاهدين بواسطة محضر يوقعه الشاهدين مع ضابط الشرطة القضائية. هذا إذا كان القائم بالتفتيش هو ضابط الشرطة القضائية بناءا على أمر من قاضي التحقيق (ندب) أما إذا حصل التفتيش بمعرفة قاضي التحقيق فلقد نص المشرع على نفس الأحكام، إذا أحال في نص المادة 82 من قانون الإجراءات الجزائية على نص المواد من 45 إلى 47 .

أما إذا حصل التفتيش أثناء التحقيق الابتدائي فلقد نصت المادة 64 من قانون الإجراءات الجزائية على أنه لا يجوز تفتيش المسكن إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، وحددت المادة شكل الرضا الذي يكون مكتوبا بخط يد صاحب الشأن فإذا كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه وينوه عن ذلك في المحضر كما أحالت نفس المادة على المواد 44 إلى 47 من نفس القانون.

تضبط الأشياء والأوراق التي يعثر عليها جراء عملية التفتيش والتي تكون مفيدة لإظهار الحقيقة أو التي يمكن أن تشكل دلائل أو أدلة مادية في القضية كما يقوم ضابط الشرطة القضائية بجرد كل المضبوطات ويرقمها ويصنفها في أحراز مختومة بعد تقديمها للمشتبه فيه أو الشهود للتعرف عليها[1].

[1] http://www.djelfa.info يوم لاطلاع على الموقع 2015/06/21.

إذن يشترط حضور صاحب المسكن[1] في عملية التفتيش أو شخصين عدا أعضاء التابعين للمحقق وهذا يعتبر كضمانة شكلية للتفتيش مما يحقق الاطمئنان على سلامة الإجراءات وصحة الضبط وهذا فيما يتعلق بالتفتيش في الجرائم التقليدية، في حين بالنسبة للجرائم المعلوماتية أو المستحدثة بما فيها جرائم الدراسة فإنه يختلف عنه في أن عملية التفتيش فيها تكون إما بالانتقال إلى مسكن المتهم أو إلى المكان الموجودة به الأجهزة المراد تفتيشها أو أن يتم دلك عن بعد. فالنسبة للطريقة الأولى أحالها المشرع إلى القواعد العامة في التفتيش الواردة في قانون الإجراءات الجزائية كغيرها من الجرائم التقليدية وفي هذا تطبق إجراءات التفتيش المنصوص عليها في المادة 44 من قانون الإجراءات الجزائية.

بينما حالة التفتيش عن بعد فقد تكون المنظومة داخل الجزائر أو خارجها، وفي الحالة الأخيرة فإن ذلك مرهون بمساعدة السلطات الأجنبية المختصة التي توجد بها المنظومة، ويتم دلك في نطاق الاتفاقيات التي تم إبرامها في مجال ملاحقة الجرائم المعلوماتية وطبقا لمبدأ المعاملة بالمثل[2].

وطبقا لنص المادتين 04 و05 من القانون 04/09 فلا يجوز إجراء عملية التفتيش إلا بإذن مكتوب من السلطة القضائية المختصة.

2- طريقة التعامل مع الأدلة التقنية المضبوطة

حدد المشرع الجزائري من خلال القانون 04/09 في المواد السادسة والسابعة والثامنة، حيث تنص الثامنة على المحافظة على سرية المعلومات التي تم ضبطها، وهو التزام يقع السلطة التي تباشر التحقيق حيث لابد لها من اتخاذ كل الإجراءات اللازمة التي من شأنها منع الأشخاص غير المسموح لهم قانونا بالاطلاع عليها، وتكليف شخص مؤهل للقيام بدلك.

كما يعاقب كل من يستعمل تلك المعلومات المتحصل عليها من التفتيش في غير الأغراض التي ضبطت من أجلها وهذا تطبيقا للمادة 09 من القانون 04/09 وذلك لما قد تتضمنه من أسرار خاصة بأشخاص آخرين.

[1] أورد المشرع الجزائري تعريف المسكن في نص المادة 355 من قانون العقوبات: "يعد منزلا مسكونا كل مبنى أودار أوغرفة أوخيمة أوكشك ولومتنقل متى كان معدا للسكن وإن لم يكن مسكونا ووقتذاك وكافة توابعه مثل الأحواش وحظائر الدواجن ومخازن الغلال والإسطبلات والمباني التي توجد بداخلها مهما كان استعمالها حتى لوكانت محاطة بسياج خاص داخل السياج أو السور."

[2] المسوس عتو، مرجع سابق، ص 309.

3- محضر التفتيش

القاعدة المسلم بها أن أعمال التحقيق جميعا ينبغي كتابتها، والكتابة تشمل جميع إجراءات التحقيق سواء كانت معاينة، سماع شهود أو إجراءات التفتيش وتنص المادة 68 فقرة 2 من ق إ ج "وتحرر نسخة عن هذه الإجراءات وكذلك جميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل".

وبقصد حماية الحريات الفردية والمنع من التعسف، ألزم المشرع الجزائري ضباط الشرطة القضائية المنتدبين للتحقيق تحرير المحاضر المثبتة لما قاموا به من إجراءات مبينين فيها الإجراءات والمحضر بشكل عام له مجموعة من البيانات الواجب توافرها إضافة إلى الأشخاص المؤهلين لتحريره[1].

4-وقت أوميعاد إجراء التفتيش

حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن، تحرص التشريعات الإجرائية على تحديد وقت معين يتم فيه إجراء التفتيش في حين تترك بعض التشريعات الإجرائية أمر تحديد دلك الوقت للقائم بالتفتيش.[2]

المقصود به هو الوقت من الزمن الذي يسمح فيه بتنفيذ التفتيش فلقد حظر المشرع الجزائري القيام بتفتيش المساكن في أوقات معينة، إذ نصت المادة47 فقرة 01 ق إ ج "لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة صباحا ولا بعد الثامنة مساءا"، ويستفاد من هذا النص أن المشرع الجزائري اعتبر وقت الليل الفترة الواقعة قبل الساعة الخامسة صباحا أو بعد الساعة الثامنة مساءا وهذا يعني أن المشرع حظر التفتيش ليلا، وتبعا لذاك فإن الأصل في النظام الإجرائي الجزائري هو عدم دخول المساكن وتفتيشها أثناء الليل، ولا يجوز الخروج عن هذا الأصل مبدئيا، فإن كان من الضروري عدم الانتظار إلى وقت النهار خشية هروب المتهم أو تهريب الأدلة الجريمة المطلوب ضبطها وجب الاكتفاء بمحاصرة المسكن ومراقبته من الخارج حتى وصول الوقت الجائز قانونا مباشرة التفتيش فيه وهذا ما أكدت عليه المادة 122 في فقرتيها الأولى والثانية من قانون الإجراءات الجزائية على أنه: "لا يجوز للمكلف بتنفيذ أمر القبض أن يدخل مسكن أي مواطن قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساءا وله أن يصطحب معه قوة كافية لكي لا يتمكن المتهم من الإفلات من سلطة القانون".

إذن القاعدة أنه لا يجوز مباشرة التفتيش خارج الأوقات المسموح بها قانونا، لكن استثناءا حدد المشرع الجزائري بعض الحالات على سبيل الحصر، أجاز فيها لضابط

[1] http://www.djelfa.info يوم الاطلاع على الموقع 2015/06/26.
[2] رشيدة بوكر، مرجع سابق ، ص 415.

الشرطة القضائية الخروج عن القاعدة ومنه يجوز لهم التفتيش في أي وقت حتى ليلا وتتمثل في عدة حالات منها الجرائم المستحدثة حيث نصت المادة 47 بعد تعديلها بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006على" :عندما يتعلق الأمر بجرائم المخدرات أو جريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال أو الإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص"[1].

وبعد القيام باجراء التفتيش طبقا لما هو مقرر قانونا تتبعه النتيجة الطبيعية التي ينتهي إليها التفتيش و هي ضبط الأدلة وسنحاول التفصيل فيها على النحو الوارد أدناه.

الفرع الرابع
ضبط الأدلـــــــــة

ضبط الأدلة هو نتيجة للتفتيش فالغاية من التفتيش هو ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أومن إجراءات التحقيق[2].

فإذا كان معنى الضبط هو وضع اليد على كل ما يُفيد في كشف حقيقة الجريمة[3]، وإذا كانت الأشياء المضبوطة في الجرائم التقليدية تتصف بالمادية، فما هي طبيعة المضبوطات في الجرائم الالكترونية علما أن مجالها عموما العالم الافتراضي؟.

أولا: نطاق الضبط الالكتروني

فالضبط بحسب الأصل يرد على أشياء مادية، فلا وجود للصعوبة في ضبط الأدلة في الجرائم الواقعة على المكونات المادية للنظام المعلوماتي كرفع البصمات مثلا، ولكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في الجريمة وذلك لعدم وجود دليل مرئي في هذه الحالة ولسهولة تدمير هذا الأخير في ثوان معدودة[4]، فهل يصلح هذا النوع من الأدلة أن يكون محلا للضبط؟.

انقسم الفقه إلى اتجاهين عند الإجابة عن هذا التساؤل[5]، فيرى البعض أن بيانات الحاسب لا تصلح لأن تكون محلا للضبط، لانتفاء الكيان المادي عنها، ولا سبيل لضبطها

---

[1] http://www.djelfa.info يوم الاطلاع على الموقع 2015/06/26.

[2] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية،مرجع سابق، ص 669.

[3] http://www.th3professional.com / يوم الاطلاع على الموقع 2014/10/24.

[4] خالد ممدوح إبراهيم، مرجع سابق، ص 284

[5] علي عدنان الفيل، مرجع سابق، ص 57 .

إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية. ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط محل تطبيقها الأشياء المادية الملموسة.

ويرى الاتجاه الثاني أن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره.

وهذا الخلاف دعا المشرعين[1] في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط ليشمل فضلا عن الأشياء المادية المحسوسة، البيانات المعالجة إلكترونيا، أو إصدار تشريعات تتعلق بجرائم الحاسب الآلي، تتضمن القواعد الإجرائية المناسبة لهذه الصورة من البيانات.

فأما عن المشرع الجزائري فهو أيضا من جهته تدخل وحل هذه المسألة والتي كان من الضروري الحسم فيها، إذ نص في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 6 منه والتي تنص على:" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهما على دعامة تخزين الكترونية تكون قابلة للحجز، والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية...".

فكما يعتبر الضبط هو عملية تتبع التفتيش فيعتبر أيضا تحريز المضبوطات عملية تلي إجراء الضبط وعليه فان المشرع الجزائري قضى بضرورة إتباع بعض الإجراءات الخاصة للمحافظة على سلامة المضبوطات من العبث وذلك كالتالي:

1- منع المشرع من خلال المادة 7 من القانون 04/09 السالف الذكر الوصول إلى المعلومات المتحصل عليها والتي تم ضبطها وذلك عن طريق ترميزها أو تقييدها عن طريق أي وسيلة إلكترونية أخرى تمنع الدخول إلى هذه المعلومات وهو ما نصت عليه أيضا المادة 19 في فقرتها الثالثة من اتفاقية بودابست، غير أنه وفقا لهذه الأخيرة يتم اللجوء إلى هذا الإجراء في حالة ما إذا المعطيات تتضمن خطرا أو ضررا بالمجتمع.

2- ضبط الدعائم الأصلية للمعلومات وعدم الاقتصار على ضبط نسخها.

3- عدم ثني القرص لأن ذلك قد يؤدي إلى تلفه وفقدان المعلومات المسجلة عليه.

---

[1] مثلا المادة 39 من قانون تحقيق الجنايات البلجيكي المدخلة في القانون الصادر في 2000/11/23 حيث يشمل الحجز وفقا لهذا النص على الأشياء المادية وعلى البيانات المعالجة الكترونيا،عن علي عدنان الفيل، مرجع سابق، ص 58. وأيضا المادة 487 من القانون الكندي تمنح سلطة إصدار إذن الضبط لأي شيء طالما توافرت أسس معقولة للاعتقاد بأن الجريمة التي وقعت أويشتبه في وقوعها أوأن هناك نية في ارتكاب الجريمة بواسطته أوسوف ينتج دليلا على وقوع الجريمة، أي أن النص يسمح بطريقة جلية بضبط بيانات الحاسب الآلي غير المحسوسة، عن عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية ، مرجع سابق، ص 653.

4-عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا الرطوبة.

ثانيا: مدى إمكان إحراز المضبوطات الالكترونية

إن إحراز المضبوطات المادية كأجهزة الكمبيوتر وملحقاتها من طابعات وماسحات ضوئية وغيرها لا يثير ما يذكر من مشاكل، حيث تنطبق عليه جميع القواعد التقليدية المنصوص عليها في القانون، كما ويتم إحرازها وفق الطرق التقليدية المنصوص عليها في القانون[1].ولكن المشكلة تدق في إحراز المضبوطات الإلكترونية لا يكون بالإمكان إحراز هذه المضبوطات وفق القواعد التقليدية للضبط والإحراز، بل يلزم لإحرازها اللجوء إلى الطرق ووسائل تقنية تتفق مع الطبيعة الالكترونية لهذه البيانات وبعدها الجغرافي عن متناول أيدي أجهزة الضبط، ومن هذه الطرق والوسائل نذكر على سبيل المثال لا الحصر ما يلي :

1-**طريق النسخ :** وتتم من خلال نسخ المضبوطات الالكترونية باستخدام برامج معدة خصيصا لهذا الغرض مثلا كبرنامج (Laplink)[2]، حيث يتم أخذ نسخة من تلك البيانات أو المضبوطات الالكترونية ومن تم يتم لصقها وخزنها باسم معين على إحدى وسائط النقل (FLASH MEMORY , CD,DVD) الخاصة بالجهة القائمة بالضبط، وتبقى بعهدتها إلى حين انتهاء التحقيق أو المحاكمة، على أنه يفضل على رأي البعض حفظ نسخة أخرى من تلك المضبوطات لدى المحضرين بالمحكمة، كي تكون بديلا للأولى في حالة تلفها أو ضياعها[3].

وينصح باللجوء إلى هذه الطريقة لإحراز المضبوطات الالكترونية المشفرة بغية فك شفرتها فيما بعد من دون الخوف عليها من خطر الإتلاف أو المحو أو التعديل عن بعد، وكذلك عندما يتخوف من أن يكون الكمبيوتر أو النظام المعلوماتي الذي يحوي تلك المضبوطات مبرمجا ببرنامج القنبلة الالكترونية الزمنية على التفجير الذاتي[4]. فمثلا أجاز قانون الإجراءات الجزائية الجزائري في نص المادة 65 مكرر 10 نسخ المكالمات المفيدة في التحقيق بما فيها الالكترونية.

2-**طريق التجميد :** وتتم من خلال تجميد التعامل بالكمبيوتر أو النظام المعلوماتي الذي تتواجد بداخله المضبوطات الالكترونية، أو على الأقل تجميد القسم الصلب الذي يحمل

---

[1]- فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية و الاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007، ص 288.

[2]- عائشة بن قارة مصطفى، مرجع سابق، ص 116.

[3]- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، 2010، ص 158.

[4]- فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية والاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي، مرجع سابق، ص 288 -289.

تلك المضبوطات[1]، وذلك من خلال برامج معدة خصيصا لهذا الغرض، ومن تم يتم ضغط الملفات أو المضبوطات الإلكترونية من خلال برامج الضغط[2]، حيث تقوم هذه الأخيرة بتقليص حجم تلك الملفات أو المضبوطات وتضغطها بداخل ملف أوعدة ملفات صغيرة الحجم بصيغة (ZIP) أو(Rar) ومن دون أن يؤثر ذلك في سلامة تلك الملفات، بحيث تبقى محتفظة بكامل خواصها الأصلية، ومن تم يتم حفظ تلك الملفات المضغوطة على أقراص ليزرية (CD DVD)[3] ، أو على الفلاش ميموري، ومن ثم يتم فتح الملفات المضغوطة على أي كمبيوتر آخر من خلال برامج خاصة من مثل برنامج (winrar) أو(zip- 7). وينصح باللجوء إلى هذه الطريقة في إحراز المضبوطات الالكترونية، عندما يراد ضبط الخوادم المعلوماتية التي تحوي مواقع للدعارة أو مواقع للهكرز أو الكراكرز، أوفي حالة وجود خطر على تلك المضبوطات[4]. وكذلك في الأحوال التي يراد فيها حفظ الغير من مضار الموقع الذي يحوي ملفات ضارة.

وقد نصت الفقرات (3/ب، ج، د) من المادة (19) من الاتفاقية الأوروبية لمكافحة الجرائم الإلكترونية على ضرورة أخذ الدول الموقعة عليها بهاتين الطريقتين في تشريعاتها، لذا يلحظ بأن المشرع الفرنسي قد أخذ وبالنص الصريح بهاتين الطريقتين.[5] فيما لم يجد في القانونين الأمريكي والمصري أي نص قانوني ينظم هذه المسألة بالرغم أن الولايات المتحدة الأمريكية هي الأخرى من الدول الموقعة على الاتفاقية المذكورة أعلاه. وأما فيما يتعلق بالقانون الجزائري لم نجد نص يتحدث عن هده الطريقة كما هو الشأن بالنسبة للنسخ.

الفرع الخامس

التسرب

على ضوء التغيرات والتطورات التي طالت الجريمة حيث تولدت لدينا الجريمة المستحدثة المسماة الجريمة المعلوماتية أو ما سماها المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تتضمن في طياتها الجرائم الماسة بالأسرار

[1]- عائشة بن قارة مصطفى، مصدر سابق، ص 116.

[2]- فتحي محمد أنور عزت، المرجع نفسه، ص 288 -289

[3]- ينبغي حفظ هذه الأقراص في أماكن خاصة بعيدة عن الرطوبة، ذلك أن العلماء قد اكتشفوا في الآونة الأخيرة وجود نوع من الفطريات التي تتغذى على بعض المكونات الأساسية (طبقة الأليمنيوم الرقيقة العاكسة وطبقة الراتنج التي تغفلها) لهذه الأقراص وبحيث تدمر وتزيل البيانات المسجلة على هذه الأقراص في زمن قصير، وللمزيد من التفصيل أنظر مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، مرجع سابق، ص 361 -362.

[4]فتحي محمد أنور عزت، الحماية الجنائية الموضوعية والإجرائية والاعتداء على المصنفات والحق في الخصوصية والكمبيوتر والانترنت في نطاق التشريعات الوطنية والتعاون الدولي، مرجع سابق، ص 288 و289، وأيضا أنظر عائشة بن قارة مصطفى، مرجع سابق، ص 289.

[5] أنظر المادة (97) من قانون الإجراءات الجنائية الفرنسي.

المعلوماتية يسعى المشرع لوضع سياسة جزائية فعالة للحد من انتشار هذا النوع من الجرائم ومن بين آليات مواجهتها ميدانيا أسلوب التسرب[1].

اعتمد المشرع الجزائري أسلوب التسرب في ميدان التحقيق بموجب القانون 22/06 المعدل لقانون الإجراءات الجزائية حيث خصص له الفصل الخامس من الباب الثاني تحت عنوان " في التسرب" فأصبح لوكيل الجمهورية ولقاضي التحقيق بعد إخطار وكيل الجمهورية صلاحية منح الإذن بإجراء عملية التسرب لأجل مراقبة الأشخاص لإيهامهم من قبل المتسرب بأنه فاعل معهم أو شريك، وذلك بموجب المواد من 65 مكرر11 إلى المادة 65 مكرر18 وتناول أيضا من خلال هذه المواد مفهوم عملية التسرب وشروطها وإجراءاتها.

أولا: تعريف التسرب

التسرب لغة مشتق من الفعل تسرب تسربا أي دخل وانتقل خفية وهي الولوج والدخول بطريقة أوبأخرى إلى مكان أو جماعة[2].

عرفه المشرع الجزائري من خلال المادة في المادة 65 مكرر 12 بقوله:"يقصد بالتسرب قيام ضباط أوعون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

ومن خلال التعريف السابق يتضح أن التسرب هو عبارة عن عملية ميدانية تستخدم أسلوب التحري لجمع الوقائع المادية والأدلة من داخل العملية الإجرامية وكذا الاحتكاك شخصيا بالمشتبه بهم والمتهمين وهذا ينطوي على خطورة بالغة تحتاج إلى دقة وتركيز وتخطيط سليم، من ثم يمكن القول أن التسرب هو أكثر الوسائل تعقيدا وخطورة، لأنه يتطلب من ضابط الشرطة القضائية وأعوانه القيام بمناورات وتصرفات توحي بأن القائم بها مساهم في ارتكاب الجريمة مع بقية أفراد العصابة، لكنه في حقيقة الأمر يخدعهم ويتحايل عليهم فقط، حتى يطلع على أسرارهم من الداخل ويجمع ما يستطيع من أدلة إثبات، ويبلغ السلطات بذلك فتتمكن من ضبط المجرمين ووضع حد للجريمة[3].

---

[1] حدد المشرع الجزائري نطاق عملية التسرب بالجرائم المذكورة في المادة 65 مكرر5 من قانون الإجراءات الجزائية وقد ورد تعدادها على سبيل الحصر وتعتبر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إحداها.

[2] سهيل حسيب سماحة، معجم اللغة العربية، الطبعة الأولى، مكتبة سمير ، 1984، ص 130.

[3] زوزو هدى، الترسب التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مقال منشور بمجلة السياسة والقانون، العدد الحادي عشر ، جوان 2014، ص 117، عن الموقع الالكتروني http://revues.univ-ouargla.dz/index.php/numero-11-2014-dafatir/1991-2014-06-16-08-20-50 يوم الاطلاع على الموقع 2016/09/18.

ويمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي واشتراكه مثلا في محادثات غرف الدردشة أو حلقات النقاش والاتصال المباشر في كيفية قيام أحدهم باختراق شبكات أو بث الفيروسات، مستخدما في ذلك أسماء وصفات هيئات مستعارة ووهمية ظاهرا فيها بمظهر طبيعي كما لو كان فاعل مثلهم سعيا منه الاستفادة منهم حول كيفية اقتحام الهاكر لموقع مثلا[1].

ثانيا: شروط وإجراءات التسرب

نظرا لما قد يحيط بعملية التسرب من انتهاك للحرمة الحياة الخاصة للمتهم أحاطها المشرع بمجموعة من الشروط والإجراءات الشكلية والموضوعية لضمان السير القانوني للعملية وهذا ما سنتناوله من خلال ما يلي:

1- شروط عملية التسرب:

اشترط المشرع من خلال المادة 65 مكرر 11 من قانون الإجراءات الجزائية وجوب أن تقتضي ضرورات التحري أو التحقيق إجراء عملية التسرب، معنى ذلك أن وجود أدلة كافية تعزز الاشتباه أو تدعم الاتهام فإنه لا داعي للمخاطرة بإجراء عمليات تسرب وعليه فإن هذه الأخيرة تجرى عند الضرورة فقط والمتمثلة في قلة أوصعوبة الحصول على أدلة وبراهين كافية لتحريك دعاوى عمومية.

كما اشترط المشرع في اللجوء إلى هذا الأسلوب ضرورة ارتكاب أنواع محددة من الجرائم التي تتسم بالخطورة والتعقيد، من ثم فإن الأمر بإجراء عمليات التسرب ليس مفتوحا لكل الجرائم بل هو خاص بمجموعة محددة من الجرائم المذكورة في المادة 65 مكرر 5 من قانون الإجراءات الجزائية والتي تعتبر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من ضمنها، ومنه فيما عدا الجرائم المذكورة على سبيل الحصر لا يجوز استخدام هذا الأسلوب.

2- شروط صحة عملية التسرب:

هناك عدة إجراءات تطلبها المشرع لصحة عمليات التسرب، وهذا لإضفاء طابع الشرعية في الحصول على الدليل تطبيقا لمبدأ المشروعية الذي يمثل أساسا لكل إجراء

[1] رشيدة بوكر، مرجع سابق، ص 434.

صحيح، سواء من حيث الجهات صاحبة السلطة في الإذن بإجراء عمليات تسرب أومن حيث الجهات المختصة بمباشرة هذا الإجراء وسنحاول التفصيل فيها على النحو التالي:

أ – صدور إذن قضائي:

من خلال المادة 65 مكرر 11 اشترط المشرع ضرورة حصول المتسرب على إذن من وكيل الجمهورية المختص وأن تتم عملية التسرب تحت إشرافه ومراقبته أومن قاضي التحقيق وليمكن له منح الإذن بهذا الإجراء وجب عليه أولا إخطار وكيل الجمهورية بذلك، ثم يقوم بمنح إذن مكتوب لضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، على أن يتم ذكر هويته فيه.[1]

ب – أن يكون الإذن مكتوبا:

وهذا ما نصت عليه المادة 65 مكرر 15 حيث يجب أن يكون الإذن مكتوبا ومسببا، حيث يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ولا بد أن يحدد الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر.

ويمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية، غير أنه يجوز للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة، وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب، حيث أنه لابد من إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى غاية الانتهاء من العملية حفاظا على السرية المطلوبة التي حصرها المشرع بين القاضي الآمر بها(وكيل الجمهورية أو قاضي التحقيق)، وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب.

يحرر ضابط الشرطة القضائية المكلف بالتنسيق تقريرا يتضمن العناصر الضرورية لمعاينة الجرائم غير تلك التي قد تعرض للخطر أمن الضابط العون المتسرب، وكذا الأشخاص المسخرين لهذا الغرض وهذا ما تناولته المادة 65 مكرر 13.

فإذا تقرر وقف العملية أوعند انقضاء المهلة المحددة في رخصة التسرب وفي حالة عدم تمديدها يمكن للعون المتسرب مواصلة المهمة للوقت الضروري الباقي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا على أن يتجاوز ذلك مدة

[1] أما عن الجهات المخولة بإجراء عمليات تسرب فهم ضباط الشرطة القضائية المذكورون في المادة 15 من قانون الإجراءات الجزائية، ويستثنى من هؤلاء لاعتبارات ميدانية الولاة ورؤساء المجالس الشعبية البلدية بالإضافة إلى مساعدي ضباط الشرطة القضائية وهم الأعوان الذين جاء ذكرهم في المادة 19 من نفس القانون، فالأعوان يمارسون مهامهم تحت مسؤولية ضباط الشرطة القضائية المكلفين بتنسيق العملية وتصدر باسمهم، كما أضافت المادة 65 مكرر 13 مصطلح المسخرين ويقصد بهم كل الأشخاص من الجنسين يراه ضابط الشرطة القضائية القائم بتنسيق عملية التسرب مفيدا لإنجاز مهمته، وهذا دائما تحت رقابة القضاء.

أربعة 04 أشهر وإذا انقضت مدة أربعة أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه يجب إخبار القاضي المرخص الذي يستطيع أن يرخص بتمديدها لمدة أربعة أشهر أخرى على الأكثر[1]، وللإشارة فإنه يجوز سماع ضابط الشرطة القضائية الذي تجري العملية تحت مسؤوليته دون سواه لوضعه شاهد على العملية كما يرتب القانون عقوبات جزائية على كل من يكشف هوية ضابط أوأعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات.[2]

ثالثا: آثار التسرب

بعد صدور الإذن بالتسرب من طرف القضاء يباشر العون المتسرب عمله حسب المقتضيات المطلوبة منه ومن تم هناك آثار ستترتب عن ذلك منها تسخير الوسائل المادية والقانونية وذلك تطبيقا للمادة 65 مكرر 14 من قانون الإجراءات الجزائية يمكن اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها[3]، وكذا استعمال أو وضع تحت تصرف مرتكبي الجرائم المذكورة في نص المادة 65 مكرر5 الوسائل ذات الطابع القانوني والمالي وكذا وسائل النقل والتخزين أو الإيواء أو الحفظ أو الاتصال، وبالتالي يمكن للعون المتسرب تسخير الوسائل المادية لفائدة الخلية الإجرامية، أما عن الوسائل القانونية فالمقصود منها الوثائق الرسمية كاستخراج بطاقة تعريف أو رخصة سياقة وبالتالي يحتاج إلى جهاز خاص لتزوير الوثائق الرسمية دون المرور على الإدارة المختصة لإبقاء أعماله ضمن السرية المطلوبة[4].

كما أنه بعد انتهاء عملية التسرب، تتمكن جهات البحث والتحري وعلى رأسها وكيل الجمهورية وقاضي التحقيق من الوقوف على التفاصيل الأساسية لارتكاب الجرائم. وكذا تحرير محاضر تشكل أدلة تخدم الدعوى وتعطي نظرة عميقة لحقيقة ما يحدث في بؤر الإجرام وداخل العصابات، كما تطرح أمام جهات الحكم بما لها من حرية في تقدير ما يعرض عليها من أدلة مختلف المحاضر المحررة بطرق احترمت فيها الشروط الشكلية والموضوعية، وكل مخالفة تهدر ما يترتب عنها، كما تقدم للقاضي الفاصل في الدعوى شهادات لشهود عيان خاطروا بأنفسهم للحصول على الدليل، وهذا كله لتحقيق الهدف

---

[1] المادة 65 مكرر 17 من قانون الإجراءات الجزائية.

[2] المادة 65 مكرر 16 من قانون الإجراءات الجزائية.

[3] هناك من يرى في هذه الأعمال خروجا عن مبدأ النزاهة ومشروعية الدليل الجنائي ولكن ذلك للوصول لغاية أسمى هي ضرورة حماية المجتمع عندما تعجز الأساليب التقليدية للتحري والتحقيق عن مواجهة بعض الجرائم.

[4] رشيدة بوكر، مرجع سابق، ص 438.

الأساسي من الدعوى العمومية تحديدا والإثبات الجنائي عموما المتمثل في البحث عن الحقيقة والكشف عنها.

في هذا الإطار تجدر الإشارة إلى المخاطر الجسيمة التي يمكن أن يتعرض لها المتسرب بعد انتهاء عملية التسرب في حياته والتي يمكن أن تمتد إلى أفراد أسرته، وهنا وفر المشرع حماية لهؤلاء من خلال العقوبات المنصوص عليها في المادة 65 مكرر 16 من قانون الإجراءات الجزائية التي تنص على معاقبة كل شخص يكشف هوية ضباط الشرطة القضائية بالحبس من سنتين إلى 5 سنوات وبغرامة من 50.000 دج إلى 200.000 دج، وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أصولهم المباشرين تكون العقوبة بالحبس من 05 إلى 10 سنوات وغرامة من 200.000دج إلى 500.000 دج، وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص تكون العقوبة بالحبس من 10 سنوات إلى 20 سنة والغرامة من 500.000 دج إلى 1.000.000دج .

كما رتب المشرع حماية أخرى تتمثل في عدم تقديم العون المتسرب للإدلاء بشهادته شخصيا حفاظا على حياته، بل يقتصر الأمر على إدلاء ضابط الشرطة القضائية المكلف بتنسيق العملية وحده دون سواه بشهادته تحت مسؤوليته .

الفرع السادس

التزامات مزودي الخدمات اتجاه جهات التحقيق

يتسم الدليل الرقمي بسمات الجريمة المعلوماتية ومنه يمكن للمجرم المعلوماتي و بكل سهولة ويسر باستخدام أساليب التقنية الحديثة إزالته وعن بعد، لهذا رتب المشرع الجزائري على عاتق مقدمي الخدمات مجموعة من الالتزامات من ضمنها تقديم المساعدة لسلطات التحقيق بموجب أحكام المواد 10 و12 من الفصل الرابع ضمن القانون 04/09 المتعلق بتكنولوجيا الإعلام والاتصال السالف الذكر تحت عنوان " التزامات مقدمي الخدمات"، وقبل التفصيل في الالتزامات التي على مزودي الخدمات القيام بها للتعاون مع جهات التحقيق للحصول على الدليل لإثبات الجريمة المعلوماتية بصفة عامة و التي من ضمنها الجرائم الماسة بالأسرار المعلوماتية لابد وقبل ذلك التطرق لتوضيح المقصود بمزودي الخدمات.

أولا: تعريف مقدمي الخدمات.

عرفت المادة الأولى من اتفاقية بودابست في الفقرة "ج" مزود أو مدم الخدمة أنه" كل من يقوم بخذمات الإيصال أو معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامة أو خاصة وقد يدم خدماته للجمهور أو لمجموعة من المستخدمين الذين يشكلون مجموعة مغلقة"، كما عرفته الاتفاقية العربية في المادة الثانية أنه" أي شخص طبيعي أو معنوي عام

أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها"، وعرفه المشرع الجزائري بموجب المادة الثانية في فرتها السادسة من القانون 04/09 بأنه:

- كل كيان عام أو خاص يقدم لمستعملي خدماته ضمانة القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام الاتصالات.
- أي كيان آخر يوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة لمستعمليها.

ذلك بالإضافة إلى مقتضيات المرسوم التنفيذي 2000-307 المتعلق بضبط شروط وكيفيات إقامة خدمات "الانترنت" واستغلالها السالف الذكر حيث ذكر مقدمي الخدمات في المادة الرابعة[1] منه أنه أشخاص معنويين خاضعيين للقانون الجزائري دونما التطرق لتعريفهم.[2]

ثانيا: التزامات[3] مقدمي الخدمات لمساعدة جهات التحقيق

ألزمت المادة 10 من القانون 09-04 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش كما ألزمتهم أيضا بكتمان السر بخصوص العمليات التي ينجزونها بطلب من المحققين وما تحصل عن ذلك من معلومات وذلك تحت طائلة العقوبات التي يقررها القانون في حالة إفشاء أسرار التحقيق.[4]

وإلى جانب ذلك ألزمت المادة 11 من القانون 09-04 مقدمي الخدمات بحفظ المعلومات التي من شأنها تمكين جهات التحقيق من التعرف على مستعملي الخدمة و ذلك لمدة سنة واحدة وازالتها بعد ذلك لأن الحفظ إجراء وقتي، إذن هم ملزمون بتسجيل وحفظ المعطيات التي هم ملزمون بحفظها ووضعها تحت تصرف المحققين بل أن أي عمل من شأنه عرقلة حسن سير التحقيق يؤدي إلى قيام مسؤولية جزائية لهؤلاء و يعرضهم للعقوبة المنصوص عليه في المادة 11 و هي الحبس من ستة أشهر إلى خمس سنوات وبغرامة من 50000 دينار جزائري إلى 500000 دينار جزائري.

---

[1] تنص المادة الرابعة من المرسوم 2000-307 أنه" لا يخص باقامة خدمات "أنترنت" واستغلالها لأغراض تجارية ضمن الشروط المحددة أدناه، إلا للأشخاص المعنويين الخاضعين للقانون الجزائري الذين يدعون أدناه" مقدمي خدمات أنترنت .....".

[2] جاء المرسوم التنفيذي رقم 2000-307 المؤرخ في 14 أكتوبر 2000 ليعدل المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها، الجريدة الرسمية عدد 60 مؤرخة في 15 أكتوبر 2000، ص 15.

[3] ألقى المشرع الجزائري على عاتق مقدمي الخدمات مجموعة من الالتزامات خلال ممارستهم لنشاطهم منصوص عليها في المرسوم التنفيذي 98-257 في المادة 14 منه و المعدل بالمرسوم التنفيذي 200-307 مع العلم أن المادة 14 بقت كما هي بعد التعديل.

[4] زبيحة زيدان، مرجع سابق، ص 153.

وما تجدر الإشارة إليه أن المشرع الجزائري حدد المعطيات المعلوماتية الواجب على مزودي الخدمات حفظها وهي معطيات المرور و حصرها في الآتي: المعطيات التي تسمح بالتعرف على مستعملي الخدمة، المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال، الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال، المعطيات التي تسمح بالتعرف على المرسل إليه وكذا عناوين المواقع المطلع عليها[1].

المبحث الثاني
التعاون الدولي في مجال مكافحة الجرائم ضد السرية المعلوماتية

باعتبار جرائم الدراسة من الجرائم المعلوماتية سيتم التطرق في هذا الفصل للتعاون الدولي في مجال مكافحة الجريمة المعلوماتية باعتبارها عابرة للحدود، حيث أن الأمر نفسه بشأن الجرائم ضد الأسرار المعلوماتية باعتبارها جزء من الكل، وفي هذا الصدد سبقت الإشارة إلى أن تأمين المعلومات يتناول ثلاث موضوعات هامة، وهي السلامة والإتاحة والسرية في مجال المعلوماتية.

إن ما تتميز به الجرائم المعلوماتية من حداثة الأسلوب وسرعة التنفيذ وسهولة الإخفاء والقدرة على محو آثارها وتعدد صورها وأشكالها، ليس هذا فحسب بل اتصفت بالعالمية وبأنها عابرة للحدود وهذا أمر طبيعي خاصة إذا ما علمنا أن شبكة الإنترنت ذاتها لا تعرف الحدود أي أنها ذات طبيعة عالمية[2] .

وحيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم المعلوماتية، كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل أمتد إلى أكثر من إقليم، بحيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في بلد معين، ويقبل على التنفيذ في بلد آخر ويهرب إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة.

وإزاء ذلك كان، لا بد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم، التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه، بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الاتصالات والمواصلات، وتعزيز التعاون بينها واتخاذ تدابير فعّالة للحد منها والقضاء عليها

[1] عرفت المادة الأولى الفقرة د من اتفاقية بودابست هذا النوع من المعطيات بأنها" صنف من بيانات الحاسوب التي تشكل محلا لنظام قانوني محدد، حيث يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد سلك الاتصالات من مصدرها إلى الجهة المقصودة، وهي بذلك تشمل طائفة من المعطيات تتمثل في مصدر الاتصال، ووجهته المقصودة ، خط السير، وقت وزمن الاتصال، حجم الاتصال ومدته ونوع الخدمة المؤداة، أنظر في ذلك سعيداني نعيم، مرجع سابق، ص 140.

[2] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مواجهة الانترنت، مرج سابق،ص 2 .

ولمعاقبة مرتكبيها[1].

وبناء عليه سيتم التفصيل في هذا الموضوع من خلال التطرق لمفهوم التعاون الدولي في مجال مكافحة الجرائم الواقعة على الأسرار المعلوماتية، وبالأخص عندما يكون الحاسب الآلي مرتبط بشبكة الانترنت، لأنه وكما سبقت الإشارة أن استخدام هذه الشبكة هو ما جعل بها عابرة للحدود، ومنه سنتطرق لمفهوم التعاون الدولي (المطلب الأول) من جهة، ومن جهة أخرى سيتم التطرق إلى أهم الصعوبات التي واجهت هذا التعاون (المطلب الثاني).

المطلب الأول

مفهوم التعاون الدولي في مجال مكافحة جرائم الاعتداء على الأسرار المعلوماتية

في هذا المقام سوف نتطرق ببعض من التفصيل فيما يخص التعاون الدولي لمكافحة الجرائم المعلوماتية والتي تعتبر أغلب جرائم الدراسة من طائفتها، وما لهذه الجريمة من أبعاد خطيرة خاصة وأنها قد تكون عابرة للحدود. الأمر قد الذي يجعل نتائجها والقضاء عليها من الأمور الصعبة المنال، وقد فرض البعد الدولي للجريمة المعلوماتية على المجتمع الدولي البحث عن وسائل أكثر ملائمة لطبيعتها، وتضييق الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرب من العقاب ولنشر نشاطهم في مناطق مختلفة[2]. الأمر الذي دفع بالمجتمع الدولي إلى البحث عن آليات جديدة تتلاءم وطبيعتها، وتطوير الوسائل التقليدية بما يكفل تضامن جهود الدول وأجهزتها القائمة بمهمة مكافحة الجرائم عموماً، والجريمة المعلوماتية على وجه الخصوص وذلك لتحقيق خلق مؤسسات أكثر ديناميكية استجابة لسرعة ظهورها وتطورها.

والتعاون القضائي الدولي هو الآلية الرئيسية للكفاح ضد الجريمة بأبعادها المختلفة، ويقصد بالتعاون في هذا المقام ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم، وذلك من خلال تدابير وقائية تستهدف مواجهة الصيغة غير الوطنية للجريمة، وتستجمع الأدلة بمختلف الطرق، وهو ما يستغرق وقتاً، ويتطلب إمكانات لا تملكها سلطات قانونية لدولة واحدة ما لم تدعمها وتساندها جهود السلطات القانونية في الدول الأخرى[3] . ولتحديد المقصود من التعاون الدولي في مجال مكافحة الجريمة ضد السرية المعلوماتية لابد من التطرق للتعاون القضائي الدولي بشأن مكافحة جرائم السرية المعلوماتية(الفرع الأول)، والتعاون القضائي في مجال تسليم

[1] حسين بن سعيد بن سيف الغافري، المرجع نفسه، ص 2.

[2] أبوا لمعالي محمد عيسى ، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، مشاركة في المؤتمر المغاربي الأول حول المعلوماتية والقانون، ص7. عن الموقع الالكتروني iefpedia.com/.../ يوم الاطلاع على الموقع 10 /2015/10.

[3] أبو المعالي محمد عيسى، مرجع سابق، ص 2.

المجرمين(الفرع الثاني)، في حين التعاون الدولي في مجال تدريب الكوادر، فإنه تجدر الإشارة أنه بمناسبة التطرق لإجراءات التحقيق تم تناول الخبرة وتم ادراج تدريب الكوادر على المستويين الإقليمي والدولي على أساس أن الكوادر يندرجون ضمن الخبراء، وطبيعة الحال ليس الخبراء بالمفهوم القانوني للخبير وإنما يمكن اعتبار الكوادر الموكول لهم مهمة التحقيق والبحث والتحري لابد لهم من الخبرة في المجال التقني والفني المعلوماتي. وتفاديا للتكرار حول تدريب الكوادر تم التعمد في إدراج الدولي مع الإقليمي في موضوع واحد.

الفرع الأول

التعاون القضائي الدولي[1]في مكافحة جرائم السرية المعلوماتية.

ليس التشريع هو الأداة المنفردة للتعاون بين الدول في مكافحة الجريمة المعلوماتية، ولكن السلطة القضائية أيضا يمكن أن تقوم بدور فعال في هذا الصدد. والتعاون القضائي ينبع من الضرورة ذاتها التي ينبع منها التعاون التشريعي وفعالية التحقيق والملاحقة القضائية في الجرائم المتعلقة بالانترنت[2]، فغالبا ما تقتضي تتبع أثر النشاط الإجرامي من خلال مقدمي خدمات الانترنت أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالانترنت. وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدرية والجهاز الخاص بالضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات وسطاء في بلدان مختلفة.

ولتحديد مصدر الجريمة غالبا ما يتعين على أجهزة إنفاذ القانون الاعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها.

وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه، وقد يكون ذلك خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى بمعنى أن هناك حاجة إلى التعاون

---

[1] عقدت الجمعية المصرية للقانون الجنائي مؤتمرها السادس في القاهرة في الفترة بين 25 إلى 28 أكتوبر 1993 وناقشت موضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات من خلال الأبحاث والدراسات المقدمة من الباحثين وقد بينت هذه الأخيرة صعوبة اكتشاف جرائم نظم المعلومات وإثباتها وفي نهاية المؤتمر تم تقديم عدة توصيات توصل إليها المؤتمرون كان من ضمنها حث الدول على التعاون فيما بينها خاصة في مجال المساعدات والإنابة القضائية للكشف عن تلك الجرائم وجمع الأدلة لإثباتها وتسليم المجرمين المقترفين لها وتنفيذ الأحكام الأجنبية الصادرة بالإدانة، كما قدمت لجنة الكمبيوتر بالتحاد الأوروبي توصيات تتعلق بجرائم الكمبيوتر تمحورت في عدة نقاط من بينها أهمية الاستجابة الدقيقة والسريعة للتحدي الجديد للجرائم المتصلة بالكمبيوتر والأخذ في الحسبان أنها ذات خاصية تحويلية، مع ضرورة الوعي بالحاجة الناجمة للتناغم بين القانون والتطبيق وتحسين التعاون الدولي القانوني، عن عبد العال الديربي، محمد صادق اسماعيل، الجرائم الالكترونية، دراسة قانونية وقضائية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، الطبعة الأولى، 2012، ص 354-355-358.

[2] تجدر الإشارة أنه لابد من استخدام مصطلح جرائم الانترنت في هذا المقام ذلك أنه لولا الانترنت لما أخذت البعد الدولي.

القضائي، فالدول لا يمكن لها أن تتجاوز حدود سلطاتها ويمتنع عليها القيام بأي عمل قضائي أو إجراء جزئي في دولة أخرى إذن لابد من التعاون الدولي.

وحيث أنه قد يكون للجرائم الواقعة على الأسرار المعلوماتية بعد دولي، حيث أنه يستخدم في الاعتداء عليها شبكة الانترنت وما لهذه الشبكة من أبعاد دولية، وقد تكون الدولة التي تود متابعة المعتدي بحاجة إلى طلب المساعدة من جميع البلدان التي مرت الهجمة من خلالها، ذلك أنها لا يجوز لها تخطي حدودها الإقليمية وعليها احترام سيادة تلك الدول، وبالتالي فالتعاون هو المنفد الوحيد للتمكن من متابعة الجاني .

ويقصد بالتعاون القضائي ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم، وذلك من خلال تدابير وقائية تستهدف مواجهة الصيغة غير الوطنية للجريمة. وتستجمع الأدلة بمختلف الطرق، وهو ما يستغرق وقتاً ويتطلب إمكانات لا تملكها سلطات قانونية لدولة واحدة ما لم تدعمها وتساندها جهود السلطات القانونية في الدول الأخرى[1]. ويقصد به أيضا تعاون السلطات القضائية في الدول لمكافحة الجريمة المعلوماتية[2] بهدف إجراء العمل القضائي فوق أراضيها.

ومن أهم صور التعاون القضائي، التعاون الأمني الدولي (أولا) والمساعدة القضائية الدولية(ثانيا).

أولا: التعاون الأمني على المستوى الدولي

في مواجهة الجريمة المعلوماتية عموما، غالبا ما تقف السلطات القضائية وقوات الشرطة عاجزة عن التحكم في هذا الإجرام الجديد وذلك لعوامل عديدة يأتي في مقدمتها الحدود الطبيعية بين الدول، بيد أنها تقف حاجزا في وجه المكلفين بمكافحة الإجرام المعلوماتي والتي تتوقف صلاحيتها عند حدود دولتهم، وفي حالة اتصال شبكة معلومات الكمبيوتر بين دولتين أو أكثر، نكون بحاجة إلى التعاون لتخطي هذا الإشكال.

آ- ضرورة التعاون الأمني الدولي:

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول، فإنها تحتاج إلى قدرٍ من الأمن والنظام وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بال الحكومات والمختصين والأفراد على حد سواء. ولقد أثبت الواقع العملي أن الدولة – أي

[1] أبو المعالي محمد عيسى، مرجع سابق، ص 2.

[2] هدى حامد قشقوش، الجريمة المنظمة، القواعد الموضوعية والإجرائية والتعاون الدولي ، دار النهضة العربية، 2000، ص 85.

دولة – لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة. فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت والانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بشبكة الإنترنت وهي نوعٌ من الجرائم المعلوماتية، التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة[1]، ومع تميزها بالعالمية وبكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي، على المستوى الإجرائي الجنائي بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها[2].

والإشكال المحتم بالنسبة لهذه الجرائم هو أن تقف مشاكل الحدود والولايات القضائية عقبة أمام اكتشافها ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المتصلة بالحاسب الآلي وملاحقتها قضائيا تؤكد على أهمية المساعدة القانونية المتبادلة بين الدول، حيث يستحيل على الدولة بمفردها القضاء على هذه الجرائم الدولية العابرة للحدود، لأن جهاز الشرطة في هذه الدولة أو تلك لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها بمعنى آخر أنه متى ما فرّ المجرم خارج حدود الدولة يقف الجهاز الشرطي عاجزا[3].

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة بالإضافة إلى تعقب المجرمين الفارين من العدالة [4]، وللتعاون الدولي الأمني صور من أهمها:

1 - تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة[5] :

تتعرض كافة دول العالم لاحتمالات وقوع كوارث ضخمة وأحداث مفاجئة بشكل لا يمكن توقعه أو يستحيل التنبؤ بتوقيت حدوثه، أو يصعب معه مواجهته بالإمكانيات القومية للدولة التي تعرضت للكارثة بمفردها .

---

[1] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ، دار النهضة العربية القاهرة، 2009، ص 636 ، مشار إليه في ورقة عمل بعنوان تدابير مكافحة الجرائم المتصلة بالحواسيب – مقدمة في مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية- المنعقد في بانكوك في الفترة 18-2005/4/25م – وثيقة رقم A/CONF.203/14 .

[2] حسين بن سعيد الغافري، المرجع نفسه، ص 636 ، كذلك أنظر جميل عبد الباقي الصغير ، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة ، 1998م ص 75.

[3] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص 637.

[4] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص 637.

[5] حسين بن سعيد الغافري، ،المرجع نفسه، ص 641.

ومع وقوع مثل هذه الكوارث أو الأزمات أو المواقف الحرجة غالبا ما يكون عنصر الوقت من الأمور الحاسمة في المواجهة، الأمر الذي يحتاج إلى تكثيف خاص للجهود والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتضافر الجهود الدولية.

وهذه الصورة من صور التعاون الأمني تعد من أهم الصور في مجال مكافحة جرائم الإنترنت لاسيما وأن أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية في جميع الدول، وإنما هناك تفاوت فيما بينها فبعض الدول متقدمة تقنيا وتكنولوجيا ولها نصيب كبير في مواجهة الجرائم المعلوماتية تشريعيا وفنيا، والبعض الأخر تفتقد ذلك من هنا كان لابد من التعاون بين الدول.

2- القيام ببعض العمليات الشرطية والأمنية المشتركة[1]:

تعقب مجرمي المعلوماتية عامة وشبكة الإنترنت خاصة، وتعقب الأدلة الرقمية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية، كلها أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، وهي من شأنها صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم، وبالتالي وضع حد لها.

ب- جهود المنظمة الدولية للشرطة الجنائية" الأنتربول:

أسس الأنتربول، الذي هو أكبر منظمة شرطية في العالم، عام 1923 ، ومهمته تتمثل في تقديم المساعدة إلى أجهزة إنفاذ القانون في بلدانه الأعضاء الـ 186 لمكافحة جميع أشكال الإجرام عبر الوطن للأنتربول بنى تحتية متطورة للإسناد الفني والميداني تمكين قوى الشرطة في سائر أنحاء العالم من مواجهة التحديات الإجرامية المتنامية في القرن الحادي والعشرين. وتركز المنظمة اهتمامها على ستة مجالات إجرامية أعطتها الأولوية هي الفساد؛ المخدرات والإجرام المنظم؛ الإجرام المالي والمرتبط بالتكنولوجيا المتقدمة؛ المجرمون الفارون؛ تهديد السلامة العامة والإرهاب؛ والاتجار في البشر[2].

وتقع الأمانة العامة للأنتربول في ليون بفرنسا، وهي تعمل على مدار الساعة وطوال أيام السنة وللأنتربول ستة مكاتب إقليمية في مختلف أرجاء العالم، ومكتب لتمثيله في مقر الأمم المتحدة في نيويورك، ولكل بلد عضو في الأنتربول مكتب مركزي وطني يعمل فيه موظفو شرطة وطنيون مؤهلون أفضل تأهيل[3].

---

[1] سليمان أحمد فضل، المواجهة التشريعية والأمنية الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2008، ص 415.

[2] http://www.startimes.com يوم الاطلاع على الموقع 2015/06/20.

[3] http://www.startimes.com يوم الاطلاع على الموقع 2015/06/20.

تعد منظمة الانتربول[1]، من الأجهزة التابعة لمنظمة الأمم المتحدة وتعمل تحت رعايتها وإشرافها،كونها قد أنشأت بقرار صادر عن الجمعية العامة للمنظمة الدولية "الأمم المتحدة" . وتسعى الانتربول إلى تعزيز وتشجيع التعاون الأمني الدولي الشرطي، أي مساعدة أجهزة في الدول الأعضاء على التعاون مع بعضها البعض، والعمل معاً على مكافحة الإجرام، ولاسيما العابر للحدود والمنظم حيث يتم تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها، وتتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجرائم المتشعبة في عدة دول ومنها جرائم الإنترنت[2].

بمعنى أن الدور الأساسي للإنتربول هو تفعيل التعاون بين أجهزة الشرطة التابعة للدول الأعضاء عن طريق تنسيق العمل الشرطي وتبادل المعلومات، أي أنها تقوم بدور الوسيط للدول المشتركة فيها بالمعاونة في التصدي للجريمة بكافة أشكالها وتبادل البيانات والمعلومات وإعداد الإحصاءات التي تحدد معدلات الجريمة في العالم وأهم دور تؤديه في مجال التسليم أنها تقوم بإرسال النشرة الدولية.[3]

وعلى غرار هذه المنظمة، أنشأ المجلس الأوربي في لكسمبورج عام 1991م شرطة أوربية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة ولملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت. أما على المستوى

---

[1] فالبدايات الأولية للتعاون الدولي الشرطي ترجع إلى عام 1904م عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ 1904/5/18م والتي نصت في مادتها الأولى على "" تتعهد كل الحكومات المتعاقدة بإنشاء أوتعين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج، ولهذه السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة. ""، بعد ذلك أخذ التعاون الشرطي الدولي يأخذ صورة المؤتمرات الدولية أولها وأسبقها تاريخيا كان مؤتمر موناكو(18-1914/4/14م) والذي ضم رجال الشرطة والقضاء والقانون من 14 دولة، وذلك لمناقشة ووضع أسس التعاون الدولي في بعض المسائل الشرطية، خاصة ما يتعلق بمدى إمكانية إنشاء مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين، إلا أنه ونتيجة لقيام الحرب العالمية الأولى لم يحقق المؤتمر أي نتائج عملية تذكر، وبعد انتهاء الحرب العالمية الأولي وتحديدا عام 1919م حاول الكولونيل "فان هوتين" أحد ضباط الشرطة الهولندية إحياء فكرة التعاون الدولي الشرطي وذلك بالدعوة لعقد مؤتمر دولي لمناقشة هذا الموضوع، غير أنه لم يوفق في مسعاه.

وبنهاية عام 1923م نجح الدكتور" جوهانوسويرا" مدير شرطة فينا في عقد مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية وذلك في الفترة 3-1923/9/7م، ضم مندوبي تسعة عشر دولة. وتمخض عنه ولادة اللجنة الدولية للشرطة الجنائية و يكون مقرها فينا، وتعمل على التنسيق بين أجهزة الشرطة من أجل التعاون في مكافحة الجريمة.

إلا أنه وباندلاع الحرب العالمية الثانية توقفت اللجنة عن أعمالها، حتى وضعت الحرب أوزارها عام 1946م، حيث عقد في بروكسل ببلجيكا في الفترة6-9-1946/6/9م مؤتمر دولي بهدف إحياء مبادئ التعاون الأمني ووضعها موضع التنفيذ بدعوة من المفتش العام للشرطة البلجيكية (Louvage)،وانتهى الاجتماع إلى إحياء اللجنة الدولية للشرطة الجنائية (ICPO) ونقل مقرها إلى باريس بفرنسا، وغيّر اسمها ليصبح المنظمة الدولية للشرطة الجنائية، عن حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ، مرجع سابق، ص 639.

[2] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، مرجع سابق، ص 639 و640

[3]- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، جامعة عين شمس القاهرة، 2012، ص 519.

العربي، نجد أن مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية[1] ، بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء[2].

وأما عن علاقة الجزائر بالمنظمة الدولية للشرطة الجنائية فالجزائر انخرطت مباشرة بعد الاستقلال أي في سنة 1963 وشاركت في عدة ملتقيات وكانت عنصرا نشيطا بها، وقد أقام المشرع الجزائري علاقة قانونية بين أعمال المنظمة وما يتطلبه تحويل المتهمين عبر نقاط الحدود والسفارات المعتمدة لدى الدولة فجاء في قانون الإجراءات الجزائية مفهوم إجراءات التسليم وآثاره وحركة العبور سواء طبقا لاتفاقية أو بطريقة دبلوماسية وهذا بعد انجاز الطلبات الواردة في شكل استمارات من الانتربول أو بضمانات دولية[3].

ثانيا: المساعدة القضائية الدولية[4]

تعّرف المساعدة القضائية الدولية بأنها"" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم" [5]، وتتخذ المساعدة القضائية في المجال الجنائي صور عدة كما أنه قد تكون هده المساعدة رسمية أو غير رسمية .

ولقد نص المشرع الجزائري في القانون04/09 على مبدأ المساعدة القضائية في المادة 16منه معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني، وتتخذ المساعدة القضائية الدولية عدة صور أهمها:

---

[1] هذا المكتب هوأحد المكاتب الخمسة التابعة للأمانة العامة لمجلس وزراء الداخلية العرب ومقره دمشق بالجمهورية العربية السورية، عن فهد عبد الله العبيد العازمي، مرجع سابق، 509 و510.

[2] فهد عبد الله العبيد العازمي، مرجع سابق، ص 509 و510.

[3] قادري أعمر، أطر التحقيق، دار هومة للنشر والتوزيع، الجزائر، 2013 ؛ ص 302-303.

[4] أبرمت الجزائر العديد من الاتفاقيات القضائية بشأن المساعدة القضائية في المجال الجزائي مع العديد من الدول نأخذ على سبيل المثال: اتفاقية قضائية بين الجزائر وبلغاريا بموجب مرسوم رئاسي رقم 77-191 المؤرخ في 24 ديسمبر 1977 ، الجزائر وإسبانيا مرسوم رئاسي رقم 04-23 المؤرخ في 07 فبراير 2004 ، الجزائر وفرنسا أمر رقم 65-194 المؤرخ في 29 يوليو1965، الجزائر وإيران مرسوم رئاسي رقم 2006-113 المؤرخ في 11 مارس 2006، الجزائر وتركيا مرسوم رئاسي رقم 2000-370 المؤرخ في 16 نوفمبر 2000، الجزائر ومصر أمر رقم 65-195 المؤرخ في 29 يوليو1965، عن فريدة شبري، تحديد نظام تسليم المجرمين، مذكرة ماجستير، جامعة أمحمد بوقرة بومرداس، السنة الجامعية 2007- 2008، ص 33-35.

[5] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ،المرجع نفسه ص 644، أشار إليه سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية رسالة دكتوراه، كلية الحقوق جامعة عين شمس، 1997، ص 425.

آ-.تبادل المعلومات :

يولي المجتمع الدولي تبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموماً والجريمة المعلوماتية خصوصاً، لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القوانين في كافة المجالات، بما في ذلك متابعة نشاط المنظمات الإجرامية، ومصادر الأموال في كافة المجالات، لذلك أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، بتطوير التبادل المنهجي للمعلومات بوصفه عنصراً رئيسياً من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها، وأوصى بأنه على منظمة الأمم المتحدة أن تنشئ قاعدة معلوماتية للإعلام الدول الأطراف بالاتجاهات العالمية في مجال الجريمة وهكذا ينبغي للتعاون في المسائل المتعلقة بالجريمة المعلوماتية أن يدعم بتوظيف نظم تبادل المعلومات بين الدول الأعضاء، وتقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء، باستخدام التدريب على تنفيذ القوانين والمعاهدة المتعلقة بالعدالة الجنائية على الصعيد الدولي[1].

وهو يشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة[2].

وحيث أنه يعتبر تبادل المعلومات وتبادل الخبرات من أهم العناصر المتعلقة بالوقاية من الجريمة إذ أن تقاسم المعلومات وسرعة الحصول عليها يعمل على تسهيل مهمة الأجهزة الوطنية في التحرك لمواجهة الجريمة[3].

ولهذه الصورة من صور المساعدة القضائية الدولية صدى كبيراً في كثير من الاتفاقيات ما يشير إلى أن معظم الدول بدأت تولي اهتماما كبيرا لقضية تبادل المعلومات كالبند "و" والبند"ز" من الفقرة الثانية من المادة الأولى من معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[4]، وذات الصورة نجدها في المادة الأولى من اتفاقية

---

[1] أبو المعالي محمد عيسى، مرجع سابق ص8، عن علي والي، أصداء مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، مجلة العدالة، س 8 ، ع 27 تصدر عن وزارة العدل،1981 ، ص147 .

[2] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ،مرجع سابق، ص 644.

[3] سناء خليل، الجريمة المنظمة والعبر وطنية، الجهود الدولية ومشكلات الملاحقة القضائية، المجلة الجنائية القومية القاهرة، المجلد التاسع والثلاثون، العدد الثاني، يوليو1996، ص 100.

[4] صدرت هذه المعاهدة في 1990/12/14 في الجلسة العامة 68 للجمعية العامة للأمم المتحدة . وتقضي باتفاق أطرافها على أن يقدم كل منهم للأخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات، أوإجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية في الدولة الطالبة للمساعدة، عن حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ،المرجع نفسه، ص 645.

الرياض العربية للتعاون القضائي[1]، ويوجد لها تطبيق كذلك في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000 في البنود الثالث والرابع والخامس من المادة الثامنة منها[2]. وكذلك حرصت المادة 26 من اتفاقية بودابست على التأكيد على واجب الدولة التي تمتلك معلومات هامة مساعدة دولة أخرى في معرض التحقيقات أو تداول الدعاوى الجنائية في الحالات التي لا يدرك فيها الفريق الذي يجري التحقيقات أوالملاحقة وجود هده المعلومات.

ويصدق الأمر أيضا على ما قضت به المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية[3].

وعلى المستوى التشريعي الوطني فقد نصت المادة 17 من القانون 04/09 على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الاتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل.

وقامت الجزائر بإنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا المعلومات تدعى "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته" ، تشكلت من خبراء ومتخصصين على أن يكون دور هذه الهيئة مواجهة جرائم الانترنت بكل الطرق، وتبادل المعلومات مع الدول في إطار اتفاقيات التعاون التي توقعها الجزائر ومبدأ المعاملة بالمثل. تم إنشاء هذه الهيئة بموجب المادة 13 من القانون 04/09 حيث تنص المادة 13 على أنه:" تتولى الهيئة على وجه الخصوص:...تبادل المعلومات مع نظيراتها في الخارج كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم".

ب- نقل الإجراءات:

ويقصد به قيام دولة ما بناء على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة، من أهمها التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب إليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة. وأيضا من الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تؤدى دورا مهما في الوصول إلى الحقيقة[4].

---

[1] صدرت هذه الاتفاقية في 1993/4/6م بمدينة الرياض بالمملكة العربية السعودية، أنظر المادة الخامسة منها.

[2] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ،المرجع نفسه، ص 645.

[3] سعيداني نعيم، مرجع سابق، ص 90 .

[4] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ،المرجع نفسه، ص 646.

وأقرت العديد من الاتفاقيات الدولية والإقليمية هذه الصورة كإحدى صور المساعدة القضائية الدولية.

ج-الإنابة القضائية الدولية:

ويقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها[1]. وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش وغيره[2]. والإنابة القضائية تجد أساسها في القوانين الوطنية وفي الاتفاقيات الدولية وفي مبدأ المعاملة بالمثل.

وعادة وكما هو معهود يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية، فمثلا طلب الحصول على دليل إثبات وهو عادة من شأن النيابة العامة تقوم بتوثيقه المحكمة الوطنية المختصة في الدولة الطالبة ثم يمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب. وما أن يتم تلبية الطلب ينعكس الاتجاه الوارد في سلسلة العمليات، إلا أنه وسعيا وراء الحد من الروتين والتعقيد والبطء التي تتميز بها الإجراءات الدبلوماسية يحدث وبدرجة متزايدة أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية – عادة ما تكون وزارة العدل- ترسل إليها الطلبات مباشرة بدلا من الولوج إلى القنوات الدبلوماسية والتي من شأنه تسريع الإجراءات التي قد تأخذ وقتا طويلا فيما لوتم عبر تلك القنوات.[3]

ولقد تناولت المادة 28 من اتفاقية بودابست في فقراتها الثانية والخامسة والسادسة والسابعة على الإجراءات المتعلقة بطلبات المساعدة القضائية المتبادلة بين الأطراف. وينتج عن الإنابات القضائية مجموعة من النتائج والآثار القانونية يمكن أن نوجزها في الآتي:

أولها أن الدولة التي توجه إنابة قضائية، لا تتخلى بذلك عن سلطاتها للقاضي الأجنبي الذي يقوم بتنفيذها ولا تنبيه في الحقيقة عنها في ممارسة اختصاصاتها، رغم أن تنفيذ الإنابة القضائية يجري وفق الصيغ والأشكال والقواعد المنصوص عليها في تشريعات الدولة التي

[1] عبد الرؤوف مهدى، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، ، 2000، ص 102، أنظر أيضا حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ،المرجع نفسه، ص 646، جميل عبد الباقي الصغير، الجوانب الإجرائية المتعلقة بالانترنت، دار النهضة العربية ، القاهرة، ص83، وأيضا حازم الحارون، الإنابة القضائية، المجلة الجنائية القومية، القاهرة، العدد 2، يوليو1998، ص 20.

[2] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ، مرجع سابق، ص 647.

[3] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ،مرجع سابق، ص 647.

تقوم بالتنفيذ، ولا يجوز أن يجري وفق الصيغ والأشكال والقواعد المنصوص عليها في تشريعات الدولة التي وجهت الإنابة .

وثانيا يتجلى في كفالة أفضل الشروط الموضوعية لحسن التنفيذ، وبالتالي يكون من الأفضل لتنفيذ الإنابة القضائية أن تأمر الدولة المطلوب إليها التنفيذ، أن تطلب الأشخاص المقيمين في أراضيها للمثول أمام محاكم الدولة الطالبة التي تدعوهم للإدلاء بشهاداتهم حضوريا وبصورة شفاهية، وبذلك نكون قد نقلنا من الصعيد الوطني إلى الصعيد الدولي واجب المثول أمام القضاء تلبية لمذكرات الدعوة بالحضور.

لكن ماذا لو عكست المسألة بحيث يمكن انتداب القاضي الذي يضع يده على الدعوى للانتقال إلى الدولة الأجنبية، التي يقيم فيها الشهود والاستماع إلى أقوالهم وضبط شهاداتهم عوضا عن إجبارهم على الحضور من بلادهم إلى الدول التي يقيم فيها هذا القاضي للإدلاء بشهاداتهم ولمثل هذا الحل فائدتان.

الأولى أنه يتيح للقاضي المنتدب أن يقوم بتحقيق أشمل وأدق وأجدى مما لو كان هذا التحقيق قد أنيب به قاضي أجنبي يجهل كل ملابسات الدعوى وظروف القضية، وليس في وسعه أن يجيب على الأسئلة الموجهة إليه بالقدر الأوفى طالما أنه لم يحط بالقضية إحاطة شاملة. والثانية التحقيق الذي يقوم به القاضي المنتدب يطبق فيه قوانينه الوطنية في الحدود التي لا تتعارض مع أحكام القانون العام لهذه الدولة الأجنبية، ولا شك في أن تضييق تلك القواعد يجعل إجراءات القاضي المنتدب أكثر جدوى، وأعم فائدة وأعمق أثر للوصول عند الفصل في الدعوى إلى قرار عادل .

د- التنسيق القضائي والتقني:

حيث يشكل التنسيق القضائي حد ذاته القاعدة اللازمة لإقامة تعاون دولي فعال، القوانين الإجرائية الفعالة تجعل عملية التعاون تسير بشكل آلي وسهل، حتى أنه من المفضل بالطبع اتخاذ إجراءات أخرى لتسهيل عملية بناء هذا التعاون، وتعتبر عملية تجريم الفعل من كلا الطرفين الأساس القانوني الذي يتحدد بناء عليه قبول أورفض التعاون بين الطرفين، فقد يحدث الخلاف عندما يكون قانون العقوبات للدولة متلقية الطلب بتسليم الجناة لا يعاقب على مثل هذه الأفعال المرتكبة والتي دفعت بالدولة مقدمة الطلب إلى التقدم بطلب التسليم، فمن الضروري تنسيق عملية التجريم[1].

وبشأن التنسيق التقني ينبغي تبادل العناصر الإدارية، والتقنيات الفنية، وتعزيز القدرات لأجهزة العدالة وتحليل ونشر البيانات والمعلومات المتاحة حول الجريمة والسبل والآليات المبتكرة لمكافحة ما هو تقليدي وغير تقليدي منها، ويجب التركيز على الأساليب الجديدة كدعم للتعاون الفني، وتقديم الخدمات الاستشارية الواسعة لتشمل كافة المجالات بهدف

[1] فهد عبد الله العبيد العازمي ، مرجع سابق، ص 546.

حرمان المجرم من عائدات الجرائم، لأن السياسة الوقائية ستظل قاصرة، ما لم تضبط كافة عناصر السلوك الإجرامي المفترض.[1] ويمكن تقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء، باستخدام التدريب وبرامج التبادل الدولي والتدريب على إنفاذ القوانين والمعاهدات المعنية بالعدالة الجنائية على الصعيد الدولي. بيد أنه في هذه الحالة يتوجب على السلطات التشريعية لأي دولة إحداث تعديل في قانون الإجراءات الجزائية لإضفاء الشرعية على هذه الإجراءات بما يتلائم وطبيعة الجريمة بأبعادها الجديدة المختلفة.

ه:الاعتراف بالأحكام الأجنبية

حسب القاعدة الكلاسيكية، أن كل دولة لا تعترف إلا بأحكام قانونها الجنائي ولا تعتد إلا بالأحكام الجنائية الصادرة عن محاكمها الوطنية، ولهاته القاعدة ما يبررها فهي من ناحية تعبير عن سيادة الدولة، ومن ناحية أخرى فإن قواعد القانون الجنائي تتعلق في جملتها بالنظام العام، وهذا ما يحول دون إمكانية تطبيق قانون أجنبي.

لكن مع استفحال ظاهرة الإجرام الدولي، وضرورة تعاون الدول فيما بينها لمكافحة الجرائم عبر الوطنية وحتى لا يفلت الجناة من العقاب لمجرد أنهم أقاموا في دولة غير تلك التي صدر ضدهم فيها حكم جنائي بالإدانة صار ممكنا الاعتراف بحجية الأحكام الأجنبية استنادا على معاهدات تبرم بين الدول[2].

إذن من المفاهيم التي يجب تجاوزها لدعم أواصر التعاون الدولي عدم قابلية الحكم الأجنبي للتنفيذ بحجة أنه مظهر لسيادة الدولة ولحقها في العقاب، حيث أنه لا ينبغي أن يقتصر الأمر على ما يرتبه الحكم الأجنبي من آثار سلبية تتعلق بعد جواز محاكمة الشخص مرتين، حيث يدعوا الفقه الجنائي إلى ضرورة الاعتداد بالسوابق القضائية للحيلولة دون إفلات الجناة من العقاب اتفاقا مع متطلبات العدالة[3].

الفرع الثاني
التعاون الدولي في مجال تسليم المجرمين

استقر فقه القانون الدولي على اعتبار تسليم المجرمين شكلا من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها واستقرارها وحتى لا يبقى أولئك العابثين بمنأى عن العقاب يعيشون في الأرض فسادا[4]، وحيث أن الأجهزة

---

[1] فهد عبد الله العبيد العازمي، المرجع نفسه، ص 548.

[2] http://www.startimes.com/f.aspx?t=33290431 يوم الاطلاع على الموقع 2015/11/01.

[3] Denis Flory,Union europeenne programme,d action tri1/2/ 1997, pp ,criminlitc organisee, Revinter d dr p, vol 68, 338- 339.

[4] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ،المرجع نفسه، ص 649.

المختصة بتطبيق القانون وتنفيذه تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين، كان لابد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية على إقليمها ، ولتفعيل التعاون الدولي في مجال تحقيق العدالة كان من اللازم تنظيم هذا النوع من التعاون الدولي.

يجب على الدول أن تتعاون بعضها مع البعض ومن خلال تطبيق المواثيق الدولية ذات الصلة بشأن التعاون الدولي في المسائل الجنائية، وعلى وجه الخصوص في مجال تسليم المجرم المعلوماتي حيث يجب تسليم مرتكبيها وذلك وفقا لمعيار معين لتكييف الجريمة كجريمة يجوز تسليم مرتكبيها، وفي هذا مثلا يجب أن يكون الدخول إلى النظام أو البيانات قد تم بدون وجه حق وبنية الإخلال بسرية البيانات[1].

وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافات المجالات ومنها مجال الاتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزاً أمام مرتكبي الجرائم كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل أمتد إلى أكثر من إقليم، بحيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في بلد معين ويقبل على التنفيذ في بلد آخر ويرتكب الفرار إلى بلد ثالث للابتعاد عن أيدي أجهزة العدالة . فالجريمة إذاً أصبح لها طابع دولي والمجرم ذاته أصبح مجرما دوليا، وهذا بالفعل ما ينطبق على الجرائم المتعلقة بالإنترنت[2]، وهو ذات الأمر بشأن جرائم الدراسة.

ويمكن القول أن نظام تسليم المجرمين يقوم على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب أحد الجرائم العابرة للحدود ومنها الجرائم المتعلقة الماسة بالأسرار المعلوماتية العابرة للحدود، عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك. وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة. فهو إذاً يحقق مصالح الدولتين الأطراف في عملية التسليم، فهو يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وتشريعاتها، ويحقق في ذات الوقت مصلحة للدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون ومن شأن بقائه فيها تهديد أمنها واستقرارها[3] .

ولهذا فقد حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين، بالإضافة إلى عقد العديد من الاتفاقيات الإقليمية والدولية والثنائية التي تعنى بعملية التسليم.

وللتفصيل أكثر حول موضوع تسليم المجرمين كمظهر من مظاهر التعاون الدولي القضائي في مجال مكافحة جرائم الأسرار المعلوماتية، يقتضي الأمر بيان تعريفه(أولا) ثم

[1] http://www.accronline.com يوم الاطلاع على الموقع16 /2015/05 .

[2] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة، مرجع سابق، ص 649.

[3] حسين بن سعيد الغافري، المرجع نفسه، ص 650.

التطرق لمبرراته (ثانيا).

أولا: تعريف نظام تسليم المجرمين

وهو مجموعة من الإجراءات القانونية التي تهدف إلى قيام دولة بتسليم شخص متهم أو محكوم عليه إلى دولة أخرى لكي يحاكم بها، أو ينفد فيه الحكم الصادر عليه من محاكمها[1].

ويعني قيام دولة ما (الدولة المطلوب منها التسليم) بتسليم شخصا موجودا في إقليمها إلى دولة أخرى(الدولة طالبة التسليم) بناءا على طلبها بغرض محاكمته عن جريمة نسب إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمها، بمعنى آخر تسليم دولة لدولة أخرى شخصا منسوبا إليه اقتراف جريمة ما أو صدر ضده حكما بالعقاب كي تتولى محاكمته أو تنفيذ العقاب عليه[2].

وعرفه البعض بأنه " عمل تقوم بمقتضاه الدولة التي لجأ أرضها شخص متهم أو محكوم عليه في جريمة بتسليمه إلى الدولة المختصة بمحاكمته أو تنفيذ العقوبة عليه"، و عرفه آخرون أنه "أحد مظاهر التضامن الدولي لمكافحة الجريمة تقوم بموجبه دولة ما بتسليم شخص مقيم في إقليمها إلى دولة أخرى تطلبه لتحاكمه عن جريمة انتهك بها حرمة قوانينها أو لتنفيذ فيه حكما صادرا عليه من إحدى محاكمها.[3]

ولقد عرفه أيضا النظام الأساسي للمحكمة الجنائية الدولية في المادة 102 تحت عنوان المصطلحات: " يعني التسليم نقل دولة ما شخصا إلى دولة أخرى، بموجب معاهدة أو اتفاقية أو تشريع وطني"[4].

والتعريف الذي يحظى بتأييد الأغلبية هو أن" تسليم المجرمين هو أن تسلم دولة شخصا موجودا في إقليمها إلى دولة أخرى بناء على طلبها لتحاكمه عن جريمة يعاقب عليها قانونها، أو لتنفيذ فيه حكما صادرا عليه من محاكمها"[5].

والواضح مما سبق أن فكرة نظام التسليم تقوم من جهة على وجود علاقة بين دولتين: الأولى تطالب بأن يسلم إليها مرتكب الجريمة لتتخذ بحقه الإجراءات اللازمة لإيقاع العقوبة اللازمة عليه. والثانية يوجه إليها طلب التسليم لتقرر بعد ذلك إما الاستجابة له إذا كان متوافقا مع تشريع نافذ المفعول فيها أو معاهدة أو اتفاق يربط بينها وبين الدولة الطالبة، وإما الرفض

---

[1] ابراهيم العناني، النظام الدولي الأمني، المطبعة التجارية الحديثة، 1998، ص 23.

[2] حسين بن سعيد الغافري، ،المرجع نفسه، ص 651.

[3] http://www.startimes.com/f.aspx?t=32309948 يوم الاطلاع على الموقع الإلكتروني 2015/11/28.

[4] النظام الأساسي للمحكمة الجنائية الدولية 1998 عن الموقع الإلكتروني www.ara.amnesty.org .

[5] لحمر فافة، إجراءات تسليم المجرمين في التشريع الجزائري على ضوء الاتفاقيات الدولية، جامعة وهران، السنة الجامعية 2013- 2014، ص 9، أشار إليه محمد فاضل، التعاون الدولي في مكافحة الإجرام، مديرية الكتب الجامعية، 1967، ص 57.

لعدم وجود ذاك التشريع أو تلك الاتفاقية. ومن جهة أخري نجده يشمل طائفتين من الأشخاص طائفة الأشخاص المتهمين الذين تسند إليهم ارتكاب جرائم إلا أنه لم يصدر بحقهم أحكام بعد، والفرض هنا أن شخصا ما اقترف جريمة ما في دولة معينة، وقبل أن يلقى القبض عليه يفر هاربا إلى دولة أخرى، عندها تطلب الدولة المرتكب على إقليمها الفعل الإجرامي من الدولة التي فر المتهم هاربا إليها أن تسلمه لها لمحاكمته عما ارتكب من جرم.

وطائفة الأشخاص المحكوم عليهم الذين صدر بحقهم حكمٌ بالإدانة إلا أنه لم ينفذ بعد نتيجة لفرارهم إلى دولة أخرى، والفرض هنا أن الشخص المتهم بارتكاب جريمة ما قد لوحق جزائيا من قبل قضاء الدولة التي ارتكب فيها الفعل الإجرامي، وصدر بحقه حكما قضائيا إلا أنه وقبل البدء في التنفيذ يفر هاربا إلى دولة أخرى فتطلب الدولة التي ارتكب فيها الجريمة استلامه من الدولة التي فر إليها[1].

فمصادر نظام تسليم المجرمين ليست واحدة في كافة التشريعات وإنما تختلف باختلاف الظروف التشريعية لكل دولة، إلا أنه وبشكل عام يمكن ردها وكما استقر الرأي إلى ثلاثة مصادر وهي القوانين الداخلية التي تنظم تسليم المجرمين فمثلا المشرع الجزائري أخذ بإجراء تسليم المجرمين كمظهر من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الإجراءات الجزائية في المواد 694 وما يليها، والعرف الدولي[2] الذي يطبق في حالة عدم وجود اتفاقيات أو قوانين داخلية[3]، والمعاهدات والاتفاقيات بين الدول وهى تنقسم بدورها إلى ثلاثة أنواع كالتالي:

1 - اتفاقيات التسليم الثنائية: وهي تتم بين دولتين وفقا للشروط والضوابط الموضوعة من قبلهما.

2 -اتفاقيات التسليم المتعددة الأطراف: وهي اتفاقيات يكون أطرافها عدة دول.

3 - الاتفاقيات الدولية: وهي اتفاقيات دولية تتضمن أحكاما متصلة بتسليم المجرمين دون أن تكون بحد ذاتها اتفاقيات تسليم[4].

---

[1] حسين بن سعيد الغافري، المرجع نفسه، ص 656.

[2] يكتسب العرف الدولي أهمية كونه المصدر الثاني من مصادر القانون الدولي التي قررتها المادة 38 من النظام الأساسي لمحكمة العدل الدولية، عن محمد بوسلطان، مبادئ القانون الدولي العام، الجزء الأول، ديوان المطبوعات الجامعية، الجزائر، بدون طبعة، 1994، ص 59.

[3] لا يوجد تأثير مباشر للعرف الدولي في مجال تسليم المجرمين ورغم دلك يمكن استخلاص بعض القواعد العرفية الناجمة من تواتر اعتراف الدول بها وصياغتها في الاتفاقيات ومنها شرط التجريم المزدوج، استثناء تسليم الرعايا، حظر تسليم اللاجئ، عدم التسليم في الجرائم السايسية، عن لحمر فافة، مرجع سابق، ص 19، عن محمد أمحمد عبد الرحمان طه، النظام القانوني لتسليم المجرمين مصادره وأنواعه، دورية فصلية تصدر عن مركز البصيرة للبحوث والاستشارات والخدمات التعليمية، فيفري 2010، ص 96 و97.

[4] حسين بن سعيد الغافري، مرجع سابق، ص 653.

ثانيا: مبررات نظام تسليم المجرمين.[1]

أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة العابرة للحدود، حيث أنها قد تقف بمفردها عاجزة عن التصدي لهذا النوع من الجرائم، خاصة مع التطور الملموس والمذهل في الاتصالات وتكنولوجيات المعلومات ما جعل الدول تلم شملها وتوحد جهودها في مواجهة هذا الإجرام في عدة مظاهر من أهمها نظام تسليم المجرمين[2]، خاصة وأن الأجهزة المختصة بتطبيق القانون وتنفيذه لا يمكنها تجاوز حدودها الإقليمية لممارسة الأعمال القضائية على المجرمين الفارين كان لابد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية على إقليمها ولتفعيل التعاون الدولي في مجال تحقيق العدالة كان من اللازم تنظيم هذا النوع من التعاون الدولي وتجدر الإشارة في هدا المقام أنه من المتفق عليه أن نظام تسليم المجرمين إذا كان جائزا في كل جرائم القانون العام فإنه يكون خلاف ذلك فيما يتعلق بالجرائم السياسية[3].

يقوم نظام تسليم المجرمين على أساس أن الدولة التي يتواجد على إقليمها المتهم بارتكاب أحد الجرائم العابرة للحدود ومنها الجرائم المتعلقة بالإنترنت وعليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة[4]. فهو إذاً يحقق مصالح الدولتين الأطراف في عملية التسليم، فهو يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وتشريعاتها، ويحقق في ذات الوقت مصلحة للدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون ومن شأن بقائه فيها لتهديد أمنها واستقرارها، ولهذا فقد حرصت

---

[1] فريدة شبري، تحديد نظام تسليم المجرمين، مذكرة لنيل شهادة الماجستير قانون عام، جامعة امحمد بوقرة، بومرداس، السنة الجامعية 2007-2008، ص 21 و22.

[2] استقر فقه القانون الدولي على اعتبار تسليم المجرمين شكلا من أشكال التعاون الدولي في مكافحة الجريمة والمجرمين وحماية المجتمعات من المخلين بأمنها واستقرارها.

[3] قد يعتبر تعقب المجرم السياسي اعتداءا على القيم القانونية ومفاهيم العدالة السائدة في الدولة المطلوب منها التسليم، فقد تنظر الدولة الطالبة للمطلوب تسليمه أنه من أخطر المجرمين في حين يعتبر ذات الشخص من الأبطال من وجهة نظر الآخرين، ودلت الحوادث التاريخية أن المجرمين السياسيين ليسوا بالضرورة من الأشقياء بل على العكس هم في الغالب من ذوي الشرف وأصحاب المبادئ الوطنية، فمثلا المشرع الفرنسي فرق بين جرائم القانون العام والجرائم السياسية من حيث العقوبة في حين أن المشرع الجزائري رغم أنه أردها في الباب الأول من الكتاب الثالث الجزء الثاني من قانون العقوبات المعدل والمتمم بالقانون رقم 01/09 تحت عنوان الجنايات والجنح ضد الشيء العمومي، والملاحظ من خلال التفصيل في تلك الجرائم أن المشرع الجزائري لا يقيم وزنا للتفرقة بين الجرائم السياسية والجرائم العادية كما أنه لم يفرد لها إجراءات خاصة بها، ولم يحدد لها نوعا من الاختصاص يختلف عن الجرائم العادية. ولكن المشرع الجزائري لم يغفل الإشارة إلى الجرائم السياسية بصورة مطلقة بل أشار إليها في موضوعين، الأول في الدستور في المادة 66 والثاني في المادة 689 من قانون الإجراءات الجزائية حيث أنه لا يقبل التسليم إدا اتصفت الجناية أوالجنحة بالصبغة السياسية، أوتبين من الظروف أن المطلوب تسليمه لغرض سياسي.

[4] محمد ذكي أبوعامر، الإجراءات الجنائية القسم العام، دار المطبوعات الجامعية بالإسكندرية، 1984، ص 109.

معظم الدول على سن التشريعات الخاصة بتسليم المجرمين بالإضافة إلى عقد العديد من الاتفاقيات الإقليمية والدولية والثنائية التي تعنى بعملية التسليم.

و يمكن إجمال مبررات التسليم فيما يلي:

1 – يعتبر التسليم حقا وطنيا تمارسه الدولة وفق لما يمثله هذا الإجراء من أهمية قصوى لتحقيق مصالحها وفقا لمصادر التسليم التي تعتمد عليها الدولة في علاقاتها مع غيرها من الدول الأخرى.

2 – يقوم التسليم على أساس العلاقات الدولية أيا كانت نوع وطبيعة الجريمة المرتكبة، ولا يوجد أي نظام دولي أووطني يلزم أي دولة بإجراء التسليم خروجا على مقتضيات السيادة التي تمارسها على إقليمها ومن يقيم عليها، وهذا المبرر يدعم فكرة السيادة التي ترتكز عليها بعض الاتجاهات لتحديد طبيعة نظام التسليم.

3 - يحقق الإجراء مصلحة المجتمع الدولي في عدم إتاحة الفرصة للمجرم بإفلاته من قبضة العدالة.

4 – إن مثول المتهم أمام القاضي موقع الجريمة يحقق أفضل الضمانات لمحاكمة الشخص المطلوب وإجراء تحقيقات بصورة أكثر فعالية.

5 – ينبني التسليم أيضا على حق الدولة الطالبة في معاقبة منتهك قوانينها، وذلك إعمالا لمبدأ الإقليمية في شقيه الموضوعي والإجرائي، ويمكن أن يعتبر المبرر الأساسي للتسليم يكمن في ضمان معاقبة المتهم على سلوكه الإجرامي، وذلك في إطار مبادئ العدالة الجنائية التي تعتمد عليها الدول عند صياغة ملامح هذا التعاون.

الفرع الثالث

مكافحة الجزائر للجريمة المعلوماتية من خلال تسليم المجرمين

تسليم المجرمين هو إجراء من إجراءات التعاون القضائي الدولي والذي اعتمدته غالبية الدول في تشريعاتها الداخلية، خاصة في ظل التطورات التكنولوجية الحديثة كالقانون الفرنسي الصادر في مارس 1927 والذي عدل في 2004 وأدمج في قانون الإجراءات الجزائية، وكذلك الجزائر نصت على تسليم المجرمين في الأمر رقم 66- 155 المتضمن قانون الإجراءات الجزائية الصادر في 8 جوان 1966 في الكتاب السابع تحت عنوان" العلاقات بين السلطات القضائية الأجنبية"، حيث خصص الباب الأول لتسليم المجرمين. وسعت الجزائر إلى الانضمام إلى العديد من الاتفاقيات الدولية والإقليمية وعقد مجموعة من الاتفاقيات الثنائية لتسليم المجرمين، على أساس أن أي الدولة مهما كانت أجهزتها القضائية فعالة لا يمكنها لوحدها القبض على المجرمين الفارين خاصة المعلوماتيين

للأسباب السالف ذكرها، ومنه سنتطرق للتفصيل في ذلك إلى بعض الاتفاقيات التي أبرمتها الجزائر بخصوص تسليم المجرمين (أولا)ثم سنحاول التطرق لاعتماد نظام تسليم المجرمين وفق قانون الإجراءات الجزائية (ثانيا).

أولا: الجزائر واتفاقيات تسليم المجرمين

فالدولة ما دامت عضوا في المجتمع الدولي لا بد لها من الإيفاء بالالتزامات المترتبة على هذه العضوية ومن ضمنها الارتباط بعلاقات دولية وثنائية تتعلق باستلام وتسليم المجرمين لمكافحة الجريمة عموما وخاصة ذات البعد الدولي كالجريمة المعلوماتية مع العلم أن الجزائر صادقت على العديد من الاتفاقيات في مجال مكافحة الجريمة المعلوماتية ونأخذ على سبيل المثال الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة في21 ديسمبر 2010 والتي نصت في المادة 31 منها على تسليم المجرمين فيما يتعلق بالجرائم المعلوماتية[1].

والجزائر كغيرها[2]من الدول أبرمت العديد من اتفاقيات التعاون القضائي مع معظم الدول تناولت مواضيع عدة ويأتي موضوع تسليم المجرمين من بين المواضيع الهامة التي أدرجت في صلب هذه الاتفاقيات[3]، ومن بينها:

1 – اتفاقية قضائية بين الجزائر والأردن:

مرسوم رئاسي رقم 03-139مؤرخ في 25 مارس 2003 يتضمن التصديق على الاتفاقية المتعلقة بالتعاون القانوني والقضائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وبين حكومة المملكة الأردنية الهاشمية الموقعة بالجزائر في 25 يونيو2001 والتي نشرت في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 22 ليوم 30 مارس 2003.

---

[1] صدر بشأنها مرسوم رئاسي رقم 252/14 المؤرخ في 08 سبتمبر 2014 يتضمن التصديق على الاتفاقية العربية المحررة بالقاهرة 21 ديسمبر 2010 في الجريدة الرسمية العدد 57 بتاريخ 28 سبتمبر 2014.

[2] أبرمت الجزائر اتفاقيات فيما يتعلق بتسليم المجرمين أيضا مع باكستان والموقعة بالجزائر يوم 25 مارس 2003، أيضا مع جمهورية إفريقيا الجنوبية والموقعة ببريتوريا يوم 19 أكتوبر 2001، أيضا مع نيجيريا والموقعة بالجزائري يوم 12 مارس 2003 عن فريدة شبري، تحديد نظام تسليم المجرمين، مذكرة ماجستير، جامعة أمحمد بوقرة بومرداس، السنة الجامعية 2007- 2008، ص 34 و35.

[3] فريدة شبري، تحديد نظام تسليم المجرمين، مذكرة ماجستير، جامعة أمحمد بوقرة بومرداس، السنة الجامعية 2007-2008، ص 31.

2 - اتفاقية لتسليم المجرمين بين الجزائر وايطاليا:

مرسوم رئاسي رقم 74/05 المؤرخ في 13 فبراير 2005 يتضمن التصديق على الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وبين حكومة الجمهورية الإيطالية الموقعة بالجزائر في 22 يوليو2003 والتي نشرت في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 13 ليوم 16 فبراير 2005.

3 - اتفاقية لتسليم المجرمين بين الجزائر وجمهورية الصين الشعبية

مرسوم رئاسي رقم 176/07 المؤرخ في 06 يونيو2007 يتضمن التصديق على الاتفاقية المتعلقة بتسليم المجرمين بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وبين حكومة جمهورية الصين الشعبية الموقعة والتي ببكين في 06 نوفمبر 2006 نشرت في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 38 ليوم 10جوان 2007.

ثانيا: تسليم المجرمين في قانون الإجراءات الجزائية الجزائري

يخضع تسليم المجرمين إلى الاتفاقية الثنائية بين الدولة الطالبة، والدولة المطلوب منها التسليم والمتعلقة بالتعاون القضائي، ولكن في حالة عدم وجود هذه الاتفاقية الثنائية فيمكن تطبيق الاتفاقيات المتعددة الأطراف واعتبارها الأساس القانوني للتسليم وهو ما نصت عليه المادة 16 فقرة 4 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية .[1]

وبالإطلاع على مختلف المواثيق الدولية والثنائية نجدها أنها تنص على أن تسليم المجرمين حيث يخضع في شروطه وإجراءاته إلى القانون الداخلي لكل دولة وذلك وفقا لنصوص الاتفاقيات .

1- شروط تسليم المجرمين في قانون الإجراءات الجزائية الجزائري:

نصوص قانون الإجراءات الجزائية تناولت الشروط التي يتعين توافرها لقيام الجزائر بتسليم شخص إلى دولة أجنبية أخرى مع العلم أن شروط تسليم المجرمين وإجراءاته وآثاره تحدد وفقا لقانون الإجراءات الجزائية وذلك ما لم تنص المعاهدات والاتفاقيات السياسية على خلاف ذلك، وهذا ما نصت عليه المادة 694 من قانون الإجراءات الجزائية، ومن تم ومن خلال هذه المادة فإن الاتفاقيات الدولية الثنائية أو المتعددة الأطراف هي التي تطبق على تسليم المجرمين في حالة ما إذا كانت مقتضيات الاتفاقيات المصادق عليها تتعارض مع قانون الإجراءات الجزائية، وذلك تطبيقا لمبدأ سمو المعاهدات على القانون الداخلي طبقا للمادة 132 من الدستور 1996، وشروط التسليم تتعلق بالشخص الذي هو موضوع التسليم

[1] http://www.startimes.com يوم الاطلاع على الموقع الإلكتروني 2015/06/21.

وبالأحداث المسندة إليه[1]. وطبقا لنصوص الإجراءات الجزائية يجوز التسليم في الحالات الآتية:

أ- أن تكون الجريمة المتابع بشأنها أو المحكوم عليه من أجلها الشخص المطلوب تسليمه من الجرائم المنصوص عليها في هذا الباب تطبيقا للمادة 695 وهو ما يعني أن المشرع الجزائري يأخذ بشرط ازدواج التجريم[2] إذ لا يمكن أن يتابع شخص أو تقوم الجزائر بتسليمه إذا كان الفعل مباحا وفقا للقانون الجزائري.

ب- تطبيقا للمادة697 من قانون الإجراءات الجزائية إن تسليم شخص غير جزائري إلى حكومة أجنبية بناءا على طلبها إذا وجد في أراضي الجمهورية وكانت قد اتخذت في شأنه إجراءات متابعة باسم الدولة الطالبة أوصدر حكم ضده من محاكمها، لا يجوز التسليم إلا إذا كانت الجريمة موضوع الطلب قد ارتكبت:

*إما في أراضي الدولة الطالبة من أحد رعاياها أومن أحد الأجانب.

*إما خارج أراضيها من أحد رعايا هذه الدولة.

*إما خارج أراضيها من أحد الأجانب عن هذه الدولة إذا كانت الجريمة من عداد الجرائم التي يجيز القانون الجزائري المتابعة فيها في الجزائر حتى ولو ارتكبت من أجنبي في الخارج.

وعليه فإنه للجزائر تسليم غير الجزائري في حالات وهي أن يكون أحد رعايا الدولة الطالبة أوأن تكون الجريمة قد اقترفت في أراضي الدولة الطالبة ومن أجنبي عنها إلا أن الجريمة تدخل ضمن الجرائم المعاقب عليها وفقا للقانون الجزائري، كذلك أن يشكل الفعل المقترف من طرف الشخص المطلوب تسليمه جناية في قانون الدولة الطالبة، أو أن يشكل جنحة إذا كان الحد الأقصى للعقوبة المطبق سنتين أو أقل، أو إذا تعلق الأمر بمتهم قضي بها من الجهة القضائية للدولة الطالبة تساوي أو تجاوز الحبس لمدة شهرين، وأن يكون الفعل المطلوب من أجله التسليم يكون جناية أو جنحة في التشريع الجزائري وهذا وفقا للمادة 697من قانون الإجراءات الجزائية. كما أنه تخضع الأفعال المكونة للشروع والاشتراك للقواعد السابقة بشرط أن تكون معاقبا عليها طبقا لقانون كل من الدولة الطالبة والمطلوب إليها التسليم ذلك تطبيقا أيضا لنص المادة 697 الفقرة الثانية من قانون الإجراءات الجزائية.

والملاحظ أن المشرع الجزائري[3] أثناء سنه لقانون الإجراءات الجزائية فرق بين ما إذا كان الغرض من طلب التسليم هو محاكمة الشخص المطلوب تسليمه، فاشترط أن يكون الفعل المطالب التسليم من أجله معاقب عليه بعقوبة سالبة للحرية لمدة سنتين أو أقل، وبين ما إذا

---

[1] André-Huet et Renée Koering –joulin, Droit pénal intérnational, p .343.

[2] العبرة في التجريم المزدوج بالتجريم فقط دون الوصف القانوني للفعل، لأنه من الممكن أن يختلف التكييف القانوني لفعل معين في دولة عن أخرى حسب تشريع كل منهما.

[3] دليلة مباركي، غسيل الأموال، أطروحة دكتوراه، الجزائر، جامعة باتنة، 2007، ص 291.

كان الغرض من التسليم هو تنفيذ العقوبة المحكوم بها على الشخص المطلوب تسليمه، فاشترط أن يكون قد صدر عليه حكم بعقوبة الحبس تساوي أو تجاوز الحبس لمدة شهرين. وهذه التفرقة لها ما يبررها من الناحية العملية لضمان أهمية الفعل لمرتكب من طرف الشخص المطلوب تسليمه لمحاكمته أو لتنفيذ العقوبة المحكوم بها عليه لأنه لو لم يشترط أن تكون العقوبة السالبة للحرية لمدة سنتين أو أقل، أو أن يكون الحكم الذي صدر عليه هو مدة الحبس التي تساوي أو تجاوز مدة الشهرين، لوجب قبول التسليم حتى ولو كانت المحكمة التي حاكمت الشخص المطلوب تسليمه قد حكمت عليه بعقوبة بسيطة نزلت بها عن الحد الأدنى المسموح به طبقا لظروف خاصة مختلفة، قدرتها المحكمة ويسمح بها قانونها قد تصل إلى الحبس لمدة شهر واحد على سبيل المثال وهي عقوبة لا تتطلب اتخاذ إجراءات التسليم عن فعل ليست له أهمية كبيرة من الناحية الواقعية، كما يرى بعض الفقهاء أن هذه العقوبة البسيطة لا تستحق اتخاذ إجراءات التسليم وما يصاحبها من مشقة وتكاليف في واقعة غير مهمة.

وفي حالة تعدد الجرائم المقترفة من طرف الشخص المطلوب تسليمه يجب أن يكون الحد الأقصى للعقوبة المطبقة لقانون الدولة الطالبة لمجموع هذه الجرائم يساوي أو يجاوز الحبس لمدة سنتين حتى تقوم الجزائر بتسليمه.

ج - أن التسليم لا يقبل في بعض الحالات وهي المحددة في نص المادة 698 وهي كالتالي:

*يجب أن لا يكون الشخص المطلوب تسليمه جزائري الجنسية[1]، والعبرة بتقدير هذه الصفة بوقت وقوع الجريمة المطلوب التسليم من أجله[2]، ولم يحدد المشرع الجزائري في قانون الإجراءات الجزائية حالة رفض الجزائر تسليم أحد مواطنيها أنه هذا لا يمنعها من متابعته ومحاكمته رغم أنه تم النص على ذلك في الاتفاقيات الدولية وعلى سبيل المثال الاتفاقية بين الجزائر وتونس في المادة 27، الجزائر ومصر المادة 24، الجزائر وبلجيكا المادة 3، الجزائر وفرنسا في المادة 12 وغيرها من الاتفاقيات التي نصت على ذات الأمر.

* يجب أن لا تكون للجناية أوالجنحة صبغة سياسية.

* يجب أن لا تكون قد تمت متابعة الجناية أوالجنحة وصدر فيها حكم نهائي في الأراضي الجزائرية حتى ولوكانت قد ارتكبت خارجها.

* يجب أن لا تكون الدعوى العمومية قد سقطت بالتقادم قبل تقديم الطلب وأن لا تكون العقوبة

[1] تعتبر الجنسية رابطة قانونية وسياسية بين الفرد والدولة، عن زروتي الطيب، الوسيط في الجنسية الجزائرية، مطبعة الفسيلة الدويرة الجزائر، الطبعة الثانية، 2010، ص 19.

[2] عدم جواز تسليم الرعايا من المبادئ السائدة والمستقر عليها في المجتمع الدولي، والتي نصت عليها معظم التشريعات الوطنية والاتفاقيات، عن أحمد سعد الحسيني، الجوانب الإجرائية الناشئة عن استخدام الشبكات الالكترونية، رسالة دكتوراه، كلية الحقوق، قسم القانون الجنائي، جامعة عين شمس، 2012، ص 284.

قد انقضت بالتقادم قبل القبض على الشخص المطلوب تسليمه.

*أن لا يكون قد صدر عفوفي حق الشخص المطلوب تسليمه من طرف الدولة الطالبة والدولة المطلوب إليها التسليم، ويشترط في الحالة الأخيرة أن تكون الجريمة من عداد تلك التي كان من الجائز أن تكون موضوع متابعة في هذه الدولة إذا ارتكبت خارج إقليمها من شخص أجنبي عنها.

د - لا يقبل التسليم إلا بشرط أن لا يكون الشخص المسلم موضوع متابعة إلا بعد الانتهاء من تلك المتابعة أوبعد تنفيذ العقوبة في حالة الحكم عليه، كما لا يقبل التسليم إلا بشرط أن يحكم عليه إلا في الجريمة التي سلم من أجلها، وهذا تطبيقا لنص المادة 700.

ولم يتحدث المشرع الجزائري عن حالة الشخص المطلوب تسليمه من حيث سنه وصحته وما يجب تطبيقه في هذا الشأن في قانون الإجراءات الجزائية بينما هناك من الاتفاقيات التي أبرمتها الجزائر ووضعت فيها حلا لما هو واجب تطبيقه ويمكننا أن نورد دلك كالتالي:

– الحدث: يجوز تسليم الحدث، إذا لم يكن من الجزائريين، وإذا لم تكن هناك اتفاقية تمنع التسليم[1]، وإذا توافرت فيه شروط التسليم، والعبرة بتقدير السن وقت ارتكاب الجريمة.

– الحالة الصحية للمطلوب تسليمه: يمكن رفض طلب التسليم على أساسها، ومثال ذلك الاتفاقية القضائية الخاصة بالتعاون القضائي في المجال الجزائي وتسليم المجرمين بين الجزائر والصين، حيث نصت المادة الرابعة منها تحت عنوان الأسباب التقديرية للرفض على أنه يجوز رفض التسليم إذا كان يتنافى مع اعتبارات إنسانية بسبب الشخص أو حالته الصحية أو لظروف أخرى للشخص المطلوب.

وبما أن المشرع لم ينص في قانون الإجراءات الجزائية على حالة تسليم المطلوب تسليمه لحالته الصحية أوسنه، ومنه فإن الجزائر يجوز لها أن ترفض تسليم الشخص المطلوب إذا كان حدثا أو لأن حالته الصحية لا تسمح بتسليمه إلى الدولة التي ترتبط معها باتفاقية تسليم تنص على ذلك، أو طبقا لمبدأ المعاملة بالمثل، وإذا كانت الاتفاقية لا تنص على ذلك فللدولة السلطة التقديرية في قبول أو رفض التسليم.

– رفض التسليم بسبب العرق أوالدين أ الجنس أو العقيدة: إذا كان أن المطلوب تسليمه سيحاكم بسبب أصله أو جنسه أو عقيدته أو جنسيته يمكن للدولة المطلوب منها التسليم أن ترفض ذلك، مثلا اتفاقية تسليم المجرمين بين الجزائر وبريطانيا في المادة 4/ه، وهو نفس الحكم التي نصت عليه الجزائر في اتفاقيتها مع البرتغال ومع جنوب إفريقيا، كما لا يجوز تسليم اللاجئ السياسي والأشخاص المتمتعين بالحصانة.

[1] اتفاقية تسليم المجرمين بين الجزائر وايطاليا ترفض التسليم إذا كان الشخص المطلوب تسليمه وقت ارتكاب الجريمة حدثا حسب قانون الطرف المطلوب منه التسليم، في المادة الثالثة منها.

كما أن المشرع الجزائري من خلال قانون الإجراءات الجزائية لم يوضح موقفه من تسليم الشخص الذي يحمل جنسية دولة ثالثة أي لا يحمل لا جنسية الدولة الطالبة ولا المطلوب منها التسليم فهناك رأي قائل أنه باعتبار أن هده المسألة من الأمور التي لها علاقة بالمعاملة بالمثل والمجاملات والأخلاق الدولية، فإنه للدولة المطلوب منها التسليم أن تستشير الدولة التي يحمل المطلوب تسليمه جنسيتها لدولة أخرى ثالثة طالبة التسليم، وذلك إعمالا بقواعد المجاملات الدولية، وضمانا لمبدأ المعاملة بالمثل.

في حين أن الرأي السابق يرى البعض أنه يسبب عرقلة وبطء لإجراءات التسليم خاصة أنه أحيانا ترفض الدولة في حين تستشيرها دولة أخرى مطلوب منها التسليم تسليم رعاياها لذلك لا داعي من تلك الاستشارة خاصة إذا كانت هناك اتفاقية تربط الدولتين الطالبة والمطلوب منها التسليم.

ثالثا: إجراءات تسليم المجرمين في التشريع الجزائري[1]

رسم المشرع الجزائري والاتفاقيات الدولية التي ترتبط بها الجزائر عددا من القواعد والإجراءات التي يجب إتباعها سواء كانت الجزائر هي التي تطلب التسليم أو المطلوب منها التسليم، وما تجدر الإشارة إليه أنه من خلال قانون الإجراءات الجزائية يتضح أن الإجراءات المعمول بها فقط في حين تكون الجزائر مطلوب منها التسليم، في حين شروط التسليم التي تطبق عندما تكون الجزائر هي طالبة التسليم تكون بالضرورة محددة في الاتفاقيات التي تبرمها الجزائر مع غيرها من الدول بشأن تسليم المجرمين، ومنه يتعين على الحكومة الجزائرية اتخاذ الإجراءات التالية إذا طلب منها تسليم أجنبي نسبت إليه جريمة ما استنادا لما يلي:

1 - بينت المادة 702 من قانون الإجراءات الجزائية الإجراءات التي يتعين إتباعها من طرف الدولة الطالبة في حالة تقديمها طلبها إلى الجزائر فنصت على أنه:" يوجه طلب التسليم إلى الحكومة الجزائرية بالطريق الدبلوماسي ويرفق به إما الحكم الصادر بالعقوبة حتى ولو كان غيابيا وإما أوراق الإجراءات الجزائية التي صدر بها الأمر رسميا بإحالة

[1] يقصد بإجراءات التسليم تلك القواعد ذات الطبيعة الإجرائية التي تتخذها الدول الأطراف في عملية التسليم وفقا لقوانينها الوطنية وتعهداتها لأجل إتمام عملية التسليم، بهدف التوفيق بين المحافظة على حقوق الإنسان وحريته وبين تأمين الصالح لعام الناشئ عن ضرورات التعاون الدولي في مكافحة الجريمة، بحيث لا يفلت أي مجرم من العقاب، وهذه الإجراءات تتقاسمها الدولتان الطالبة والمطالبة بالتسلي، كما أنها ليست مطلقة بل مقيدة ببعض الالتزامات الدولية والتعاهدية، عن أحمد سعد الحسيني، مرجع سابق، ص 284.

المتهم إلى جهة القضاء الجزائي أو التي تؤدي إلى ذلك بقوة القانون وإما أمر القبض أو أية ورقة صادرة من السلطة القضائية ولها ذات القوة على أن تتضمن هذه الأوراق الأخيرة بيانا دقيقا للفعل الذي صدرت من أجله وتاريخ هذا الفعل، ويجب أن تقدم أصول الأوراق المبينة أعلاه أو نسخ رسمية فيها، وذلك يعني أن طلب التسليم يكون مكتوبا وهذا من خلال نص المادة 702 كذلك هذا ما أكدت عليه جل الاتفاقيات في مجال تسليم المجرمين.

2 - كما يجب على الحكومة الطالبة أن تقدم في الوقت ذاته نسخة من النصوص المطبقة على الفعل المكون للجريمة وأن ترفق بيانا بوقائع الدعوى، ثم بعد فحص المستندات يتولى وزير الخارجية تحويل طلب التسليم إلى وزير العدل الذي يعطيه خط السير الذي يتطلبه القانون بعد التحقق من سلامة الطلب (المادة 703 من قانون الإجراءات الجزائية)، بعدها يستجوب الأجنبي من طرف النائب العام للتحقق من شخصيته حيث يبلغه المستند الذي قبض عليه، ويحرر محضر بهذه الإجراءات(المادة 704 من قانون الإجراءات الجزائية)، وبعدها ينقل الأجنبي في أقصر أجل ويحبس في سجن العاصمة.

وفي الوقت ذاته تحول المستندات المقدمة تأييدا لطلب التسليم إلى النائب العام لدى المحكمة العليا الذي يقوم باستجواب الأجنبي ويحرر بذلك محضرا خلال 24 ساعة، ثم ترفع المحاضر وكافة المستندات الأخرى إلى الغرفة الجنائية بالمحكمة العليا ويمثل الأجنبي أمامها في ميعاد أقصاه 08 أيام تبدأ من تاريخ تبليغ المستندات، ويجوز أن يمنح مدة 08 أيام قبل المرافعات وذلك بناءا على طلب النيابة العامة أو الأجنبي ثم يجري بعد ذلك استجوابه، ويحرر محضرا بهذا الاستجواب وتكون الجلسة علنية ما لم يتقرر خلاف ذلك بناءا على طلب النيابة العامة، وتسمع أقوال النيابة العامة وصاحب الشأن وهنا تبدو لنا حالتين:

1 - إذا قرر صاحب الشأن عند مثوله قبول طلب تسليمه رسميا إلى سلطات الدولة الطالبة، فهنا تثبت المحكمة هذا الإقرار وتحول نسخة منه بغير تأخير بواسطة النائب العام إلى وزير العدل لاتخاذ ما يلزم بشأنها.

2- وفي الحالة العكسية تقوم المحكمة العليا بإبداء رأيها وتتجلى لنا هنا حالتين:

أ- إذا كان الرد برفض طلب التسليم نظرا لوجود خطأ أوأن الشروط القانونية غير مستوفاة وهنا يجب إعادة الملف إلى وزير العدل خلال 08 أيام تبدأ من انقضاء المواعيد المنصوص عليها في المادة 707 من قانون الإجراءات الجزائية، وهنا إذا أصدرت المحكمة العليا رأيا مسببا برفض طلب التسليم فإن هذا الرأي يكون نهائيا ولا يجوز قبول التسليم.

ب - أما في الحالة العكسية أي إذا كان الرد بقبول الطلب فيعرض على وزير العدل للتوقيع إذا كان هناك محل لذلك مرسوما بالإذن بالتسليم وإذا انقضى ميعاد شهر من تاريخ تبليغ هذا المرسوم إلى حكومة الدولة الطالبة دون أن يقوم ممثلوا تلك الدولة باستلام الشخص المقرر تسليمه فيفرج عنه، ولا يجوز المطالبة به بعد ذلك لنفس السبب، وتجدر الإشارة هنا إلى أن هناك إجراء مهم يجوز لوكيل الجمهورية لدى المجلس القضائي في حالة الاستعجال اتخاذه

وذلك بناء على طلب مباشر من السلطات القضائية للدولة الطالبة أن يأمر بالقبض المؤقت على الأجنبي وذلك إذا أرسل إليه مجرد إخطار سواء بالبريد أوبأي طريق من طرق الإرسال الأكثر سرعة التي يكون لها أثر مكتوب. ويجب على النائب العام أن يحيط وزير العدل والنائب العام لدى المحكمة العليا علما بهذا القبض ولكن يجوز أن يفرج عن الشخص الذي قبض عليه مؤقتا وفقا للشروط المنصوص عليها بالمادة 705 من قانون الإجراءات الجزائية إذا لم تتلق الحكومة الجزائرية المستندات الواردة في المادة 702 خلال 45 يوما من تاريخ القبض عليه.

ويتقرر الإفراج بناءا على عريضة توجه إلى المحكمة العليا التي تفصل فيها خلال ثمانية أيام بقرار لا يقبل الطعن فيه، وإذا وصلت المستندات المشار إليها أعلاه بعد ذلك إلى الحكومة الجزائرية فتستأنف الإجراءات طبقا للمواد 703 وما بعدها.

رابعا: آثار التسليم وبطلانه

تترتب على التسليم مجموعة من الآثار يمكننا أن نجملها في التالي:

1- بعد الموافقة على طلب التسليم، يتم الاتصال بين الدولتين الطالبة والمطلوب منها التسليم للاتفاق على طريقة التسليم.[1]

2 - بالنسبة لنفقات التسليم فالرأي الراجع أنها تقع على عاتق الدولة طالبة التسليم، غير أنه هناك مصاريف تتحملها الدولة المطلوب منها التسليم تتمثل في نفقات إجراء التسليم التي تتم في نطاق ولايتها القضائية، وإجراءات الحجز التحفظي والحبس الاحتياطي وغيرها.[2]

3- إعادة تسليم الشخص المسلم من دولة إلى دولة أخرى في العموم لا يجوز دلك إلا بالرجوع إلى الدولة التي سلمت الشخص في الأول، فمثلا الجزائر في اتفاقيتها مع مصر لسنة 1964 في المادة 37 من الاتفاقية نصت على أنه لا يجوز للدولة المسلم إليها الشخص تسليمه إلى دولة ثالثة إلا بناء على موافقة الدولة التي سلمته.

ويبطل التسليم وفقا للقانون الجزائري كالتالي:

1- يبطل التسليم إذا لم يستوفي الشروط والإجراءات السابقة الذكر، ويصدر الحكم بالبطلان إما من الجهة القضائية الخاصة بالتحقيق أوبالحكم والتي يتبعها الشخص المسلم من تلقاء نفسه، وفي حالة ما إذا أصدرت هذه الجهة قبولها التسليم، يتعين على الغرفة الجزائية بالمحكمة العليا القضاء ببطلان التسليم.

2- للشخص المسلم حق في تعيين محام عنه، كما له حق طلب البطلان الذي يجب تقديمه خلال ثلاثة أيام تبدأ من تاريخ إنذاره الذي وجهه إليه النائب العام.

---

[1] عبد الرحيم صدقي، تسليم المجرمين في القانون الدولي، دراسة مقارنة للقوانين الفرنسية والكندية والسويسرية والرواندية، المجلة المصرية للقانون الدولي، المجلد 39 لسنة 1983 ، ص 112.

[2] فريدة شبري، مرجع سابق، ص 122.

3- يفرج على الشخص المسلم في حالة إبطال التسليم إذا لم تطالب به الحكومة لتي سلمته كما لا يجوز إعادة القبض عليه مرة أخرى سواء عن تلك الأفعال لمذكورة في طلب التسليم أوعن أفعال أخرى سابقة على طلب التسليم إلا في حالة واحدة وهي عدم مغادرة الشخص الذي أفرج عنه أراضي الجمهورية الجزائرية في مدة 30 يوم من تاريخ الإفراج عليه وتم إلقاء القبض عليه (المادة 716 من قانون الإجراءات الجزائية).

4-كما يخضع الشخص المفرج عنه لقوانين الدولة الطالبة إذا لم يغادر أراضي تلك الدولة في مدة أقصاها ثلاثين يوما من الإفراج عنه يبدأ سريانها من يوم الإفراج عنه، عن الأفعال التي ارتكبها هذا الشخص من قبل التسليم شريطة أن تكون مختلفة عن الأفعال المطلوب التسليم من أجلها (المادة 716 من قانون الإجراءات الجزائية).

الفرع الرابع
القانون الواجب التطبيق على تسليم المجرمين

إن تسليم المجرمين يخضع إلى الاتفاقية الثنائية بين الدولة الطالبة، والدولة المطلوب منها التسليم والمتعلقة بالتعاون القضائي، ولكن في حالة عدم وجود هذه الاتفاقية الثنائية فيمكن تطبيق الاتفاقيات المتعددة الأطراف واعتبارها الأساس القانوني للتسليم وهو ما نصت عليه م 16 فقرة 4 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية .[1]

وبالإطلاع على مختلف المواثيق الدولية والثنائية نجدها تنص على أن تسليم المجرمين يخضع شروطه، وإجراءاته إلى القانون الداخلي لكل دولة وذلك وفقا لنصوص الاتفاقيات .

وتطبيقا لذلك نجد أن المادة 694 من قانون الإجراءات الجزائية تنص على أن شروط تسليم المجرمين وإجراءاته وآثاره تحدد وفقا لقانون الإجراءات الجزائية وذلك ما لم تنص المعاهدات والإتفاقيات السياسية على خلاف ذلك، ومن تم ومن خلال هذه المادة فإن الاتفاقيات الدولية الثنائية أو المتعددة الأطراف هي التي تطبق على تسليم المجرمين في حالة ما إذا كانت مقتضيات الاتفاقيات المصادق عليها تتعارض مع قانون الإجراءات الجزائية، وذلك تطبيقا لمبدأ سمو المعاهدات على القانون الداخلي طبقا للمادة 132 من الدستور 1996.

ولكن الإشكال المطروح، هل يمكن للقاضي تطبيق بنود الاتفاقية الخاصة بالإجراءات مباشرة رغم أن نص الاتفاقية المصادق عليها يتعارض مع القانون الداخلي ولم تتخذ الدولة التدابير التشريعية اللازمة لإدماجه ؟

إن حل هذا الإشكال يتطلب منا التفرقة بين ما إذا كانت البنود المراد تطبيقها ـ مباشرة دون إدماج ـ دقيقة وواضحة وقابلة للتطبيق المباشر أم غامضة مبهمة تحتاج إلى تدابير تشريعية داخلية من أجل جعلها قابلة للتطبيق، ومن ثم إذا كانت الإجراءات المنصوص عليها

[1] http://www.startimes.com يوم الاطلاع على الموقع 2015/06/21 .

في الاتفاقية والمخالفة لقانون الإجراءات الجزائية، واضحة ودقيقة فيمكن للقاضي عندئذ من تطبيقها مباشرة بمجرد المصادقة على الاتفاقية، أما إذا كانت الإجراءات غامضة فلا يمكن للقاضي تطبيقها إلا بعد إدماجها في القانون الداخلي.[1]

وتطبيقا للمادة 695 من قانون الإجراءات الجزائية أنه لا يمكن للدولة الجزائرية تسليم المجرم الأجنبي ما لم يكن قد اتخذت في شأنه إجراءات متابعة عن جريمة منصوص عليها في المادة 697 من ذات القانون.

المطلب الثاني

الصعوبات التي تواجه التعاون الدولي

مع ضرورة التعاون الدولي والمناداة به، إلا أنه ثمة صعوبات تقف دون تحققه وتجعله صعب المنال لذلك سيتم التفصيل بشيء من الإيجاز في بعض تلك الصعوبات والمعوقات التي جعلته ليس بالأمر اليسير .

الفرع الأول

عدم وجود نموذج موحد للنشاط الاجرامي
واختلاف النظم القانونية الإجرائية

يعتبر عدم وجود نموذج موحد للنشاط الإجرامي وتنوع واختلاف النظم القانونية الإجرائية، من أهم الصعوبات التي تعترض التعاون الدولي في مجال مكافحة الجريمة المعلوماتية وسنحاول التفصيل فيه على النحو التالي:

أولا: عدم وجود نموذج موحد للنشاط الإجرامي

من خلال هذه الدراسة والمرور ببعض التشريعات في مجال تجريم السلوكات ضد الأسرار المعلوماتية بصفة خاصة والجريمة المعلوماتية بصفة عامة، تم التوصل إلى نتيجة وهي عدم وجود اتفاق مشترك بين جميع الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها، إذ أن بعض التشريعات جرمتها وبصور مختلفة والبعض الآخر لم يجرمها بعد.

فعدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي المعلوماتي، صعب التعاون الدولي في مجال مكافحة هذا الإجرام حيث أن الأنظمة القانونية في بلدان العالم قاطبة لم تتفق على صور محددة يندرج في إطارها الجرائم المعلوماتية، ما ينتج عنه قصور التشريع ذاته في كافة بلدان العالم.

[1] http://www.startimes.com يوم 2015/06/21 .

فلنا أن نتصور مثلا أنه حتى الآن لم يصدر قانون في دولة معينة يتعلق بالجريمة المعلوماتية سواء ارتكبت عن طريق الحاسب الآلي أو عن طريق شبكة الانترنت مثلما هو الحال في مصر.

فكيف يمكن التصور أنه حتى اليوم هناك من لم يتصدى لانتهاك سرية المعلومات وما لهذه الأخيرة من خطورة وأهمية بالغة رغم تعدد وسائل التقنية الحديثة التي جعلت انتهاكها بالأمر اليسير.

ثانيا: تنوع واختلاف النظم القانونية الإجرائية

بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليته في دولة ما قد تكون عديمة الفائدة في دولة أخرى أوقد لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الإلكترونية وغيرها، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى، وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنفاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى جمعه بطرق ترى هذه الدولة أنها طرق غير مشروعة، حتى وإن كان هذا الدليل تم الحصول عليه في اختصاص قضائي وبشكل مشروع.

الفرع الثاني
مشكلة الاختصاص[1]

ينعقد الاختصاص[2] القضائي أو ما يعرف بالاختصاص المكاني أو المحلي للمحاكم الجزائية من خلال القاعدة الثلاثية ، حيث يرجع الاختصاص إما لمحكمة مكان ارتكاب الجريمة أو محكمة مكان إلقاء القبض على المجرم أو أحد مشاركيه أو محكمة موطن إقامة المجرم[3] وهي القاعدة التي عموما تأخذ بها جل التشريعات.

---

[1] المقصود بمشكلة الاختصاص مدى خضوع الجرائم التي ترتكب في الخارج عبر الشبكة الدولية للمعلومات للقانون والقضاء الوطني .

[2] الاختصاص هومباشرة المحكمة ولايتها القضائية في نظر الدعوى في الحدود التي رسمها القانون، أنظر حازم حسن الجمل، الحماية الجنائية للأمن الإلكتروني، دار الفكر والقانون، المنصورة، الطبعة الأولى، 2015، ص 77.

[3] صغير يوسف، مرجع سابق، ص 142، عن غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة أعدت لنيل شهادة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص 518.

فتطبيق القواعد التقليدية التي تحدد معايير الاختصاص لا يتلاءم مع طبيعة الجريمة الإلكترونية العابرة للحدود، حيث يصعب تحديد مكان وقوع الفعل الجرمي في هذه الجرائم، لأن الطبيعة الخاصة لهذا الصنف من الجرائم المستحدثة تتطلب تجاوز المعايير التقليدية، الشيء يجعل من الصعب تطبيقها على الجرائم الإلكترونية على اعتبار أنها لا تتلاءم مع تحديد محل وقوع الجرم في العالم الافتراضي، فهذه الجرائم لا تعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، بحيث فقدت الحدود الجغرافية كل إثر لها في هذا الفضاء المتشعب العلاقات، وأصبحنا بالتالي أمام جرائم عابرة للحدود تتم في فضاء إلكتروني معقد عبارة عن شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأي سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي، له وجود حقيقي وواقعي لكنه غير محدد المكان، وعليه يمكن القول أن قواعد الاختصاص القضائي المنصوص عليها في قانون الإجراءات الجزائية صيغت لكي تحدد الاختصاص المتعلق بجرائم قابلة للتحديد المكاني وبالتالي لا ينبغي إعمالها بشأن الجريمة الإلكترونية والتي ترتكب في فضاء تنعدم فيه الحدود الجغرافية يبقى معها أمر تحديد مكان ارتكاب الجريمة في غاية الصعوبة مما ينبغي معه إيجاد قواعد إجرائية تحكم مسألة الاختصاص في هذه الفئة من الجرائم بما يتناسب مع طبيعتها الخاصة[1].

وعليه يمكن القول أن الجريمة الإلكترونية لا تحدها حدود خلافا للجرائم التقليدية الأخرى، الأمر الذي يجعلها في كثير من الأحيان تستعصي على الخضوع للقوالب القانونية التي تحكم مسألة الاختصاص المكاني، ومن تم فإن الطبيعة الخاصة لهذا الصنف من الجرائم تتطلب تجاوز المعايير التقليدية قصد التغلب على مشكلة تعدد الاختصاص والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها والتخلص من أثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها، وتجعل من التعاون الدولي آلية مهمة لا مجال لغض الطرف عنها ، فمن الضروري تعزيز التعاون بين الدول في المجال القضائي لضمان الفعالية في محاربة هذا النوع من الجرائم حيث أن ما من دولة يمكنها النجاح في مواجهة هذه الأنماط المستحدثة بمفردها دون تعاون وتنسيق مع غيرها من الدول، ما يفرض حتمية التعاون الدولي لتوحيد التشريعات أوعلى الأقل لتقليص الفوارق بينها ومحاولة تعزيز هذه الآليات حتى لا يستفيد المجرمون من عجز وقصور التشريعات الداخلية من جهة وغياب التنسيق الدولي الذي يعالج سبل التصدي لهذه الجرائم من جهة أخرى، حيث لا تستطيع أية دولة مجابهة الجريمة الإلكترونية وإشكالية الاختصاص التي تطرحها والتي تتخطى إمكانياتها القضائية بمنأى وبمعزل دون وضع نظام تعاون دولي فعال من أجل إزالة مختلف هذه الإشكاليات، الأمر الذي أصبح يفرض على المجتمع الدولي

[1] يوسف قجاج، إشكالية الاختصاص في الجريمة المعلوماتية، مقال منشور في مارس 2015 على الموقع الالكتروني http://www.hespress.com يوم 2015/06/22.

البحث عن وسائل أكثر ملائمة لطبيعتها وتضييق الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرب من العقاب ولنشر نشاطهم في مناطق مختلفة من أنحاء العالم[1].

إذن مشكلة الاختصاص في جرائم الانترنت أصبحت الحاجة فيها ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية، يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت، بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات.[2]

وهو ما قام به المشرع الجزائري عندما تخطى كغيره من المشرعين مشكلة امتداد التفتيش خارج إقليم الدولة الجزائرية بموجب ما أرساه القانون 04/09 من أحكام كما سبق وأن فصلنا فيه، أيضا عندما توصل إلى حل إشكالات الاختصاص بالنسبة لبعض الجرائم مثل جرائم المخدرات والجرائم الماسة بالأنظمة المعلوماتية وغيرها بالنسبة للعديد من التشريعات حيث تم تمديد الاختصاص الإقليمي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم، مثلما هو الأمر بالنسبة للمشرع الجزائري حينما عدل نص المادة 329 من قانون الإجراءات الجزائية وأيضا تم تمديد الاختصاص الإقليمي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق ليتجسد فعليا بموجب المادة الأولى من المرسوم التنفيذي رقم 348/06 المؤرخ في 2006/10/05 .

وبالنسبة لإشكالية الاختصاص القضائي فيما يتعلق بالجرائم المعلوماتية بالنسبة للاختصاص القضائي للمحاكم الجزائرية، ونحن نعلم أن أغلب جرائم هذه الدراسة تنتمي إلى هده الطائفة من الجرائم، لمعالجتها طرحنا تساؤل، هل يمتد اختصاص المحاكم الجزائرية إلى الجرائم التي ارتكبت من خارج أرض الوطن ؟.

أوجد المشرع الجزائري حل أيضا لهذه النقطة حيث نص في المادة 15 من القانون 04/09 بأنه وبالإضافة إلى قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية فإن المحاكم الجزائرية ينعقد لها الاختصاص أيضا في الجرائم التي لها صلة بتكنولوجيا الإعلام والاتصال والتي يرتكبها شخص أجنبي وخارج أرض الوطن عندما يكون غرضها مستهدفا مؤسسات الدولة الجزائرية، هيئات الدفاع الوطني، المصالح الإستراتيجية للاقتصاد الوطني، ومن خلال استقراء المادة 15 نستنتج أنه فيما عدا الجرائم المخصصة فيه تطبق الاتفاقيات الدولية فيما يتعلق بالاختصاص القضائي.

---

[1] يوسف قجاج، المرجع نفسه.

[2] حسين بن سعيد بن سيف الغافري، الجهود الدولية في مكافحة جرائم الانترنت، ص 60، عن www.minshawi.com *يوم الدخول على الموقع 2015/06/22.*

الفرع الثالث

الصعوبات الخاصة بالمساعدات القضائية الدولية وتدريب الكوادر

تتعدد الصعوبات التي تواجه الدول في مجال مكافحة الجريمة المعلوماتية ذات البعد الدولي، في المجالين ما تعلق منها بالمساعدات القضائية وكذلك ما تعلق بتدريب الكوادر وسنحاول إيراد البعض منها على النحو التالي:

أولا: الصعوبات الخاصة بالمساعدات القضائية الدولية

تعتبر الإنابة الدولية من أهم صور المساعدات القضائية الدولية في المجال الجنائي والتي تتم عموما عن طريق الطرق الدبلوماسية وهو ما يتسم بالبطء أحيانا وذلك لا يتناسب بالطبع مع طبيعة جرائم الانترنت التي تتميز بالسرعة.

كذلك من الصعوبات في مجال المساعدة القضائية أحيانا هو البطء في الرد حيث أن الدولة المتلقية طلب المساعدة تكون متباطئة في الرد وهو أيضا ما لا يتناسب وخصوصيات تلك الجرائم.

ثانيا: الصعوبات الخاصة بالتعاون الدولي في مجال التدريب

تتمثل الصعوبات الخاصة بالتعاون الدولي في مجال التدريب في عدم رغبة بعض القيادات الإدارية في بعض الدول في التدريب لإنقاذهم بدوره السلبي في تطوير العمل من خلال تطبيق ما تلمه المتدربون في الدورات التدريبية وما اكتسبوه من خبرات، ومن الصعوبات أيضا والتي قد تهدد التعاون في مجال التدريب ما يتعلق بالفوارق الفردية بين المتدربين وتأثيرها على عملية الاكتساب للمهارات المستهدفة بقوة تامة ومتكافئة لدى مختلف الأفراد المتدربين، سيما في مجال تكنولوجيا المعلومات وشبكات الاتصال حيث أنه يوجد بعض الأشخاص ممن لا يعي في هذا المجال شيء، وعلى النظير يوجد أناس على قدرة

كبيرة من المعرفة والثقافة في هذا المجال، بالإضافة إلى أن نظرة المتدرب إلى الدورة التدريبية على أنها مرحلة تدريبية أو عبء لا طائل منه تهدد العملية التدريبية برمتها وبالطبع نسف التعاون الدولي في هذا المجال.[1]

[1] حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، مرجع سابق، ص 695.

خاتمة

تعتبر السرية المعلوماتية من الأوليات التي يحرص عليها الفرد بشكل خاص والدولة بشكل عام، فهي تمتد لتشمل كافة ميادين الحياة الشخصية والاجتماعية والاقتصادية والسياسية وغيرها. فمراعاة للمصالح الفردية والجماعية تحاول الجهات المعنية القائمة على أمن الحياة البشرية على كافة الأصعدة، ومن خلال تطبيق القوانين الوضعية لمواكبة مستجدات ما تولده التكنولوجيا من آثار سلبية تهدد الأمن العام أو الخاص. ذلك أن الاستخدام غير المشروع للتكنولوجيا هدد وبالفعل الحياة العامة والخاصة للأشخاص من خلال جرائم مستحدثة مست عماد الشخص وهو الحفاظ على أسراره، والتي لا يرغب في أن يعلم بها غيره أو غير المسموح لهم العلم بها. ورغم أنه توالت التعديلات القانونية اللازمة لمواجهة تلك الجرائم المستحدثة، إلا أنه ربما لابد أيضا من إضافة البعض من النصوص المستحدثة لمواجهة كل أشكال الاعتداء على المعلومات.

وللإحاطة بصور الاعتداء على الأسرار في عصرنا هذا ،تم التطرق لموضوع الأسرار المعلوماتية وحمايتها الجزائية، وذلك من خلال تحديد المقصود بالسرية المعلوماتية باعتبارها مصطلح جديد أفرزه الاعتماد المطرد على الأنظمة المعلوماتية في كل ميادين الحياة. وهو الأمر الذي جعل الحصول على الأسرار المعلوماتية بالأمر اليسير مع إمكانية تدمير كل ما يدل على ارتكاب أي سلوك يمس بها، كما تمت الإحاطة بأغلب أشكال السلوكات التي تعتبر تهديدا للأسرار المعلوماتية وكيفية الحد منها، على الصعيدين الدولي والوطني لأنها قد تكون جرائم ذات بعد دولي، إن لم تكن في الغالب كذلك. ومن خلال هذه الدراسة والمرور بعدة محطات تم الإمكان من الوصول إلى النتائج التالية:

المعلوماتية هي علم معالجة البيانات آليا، والأسرار المعلوماتية هي البيانات السرية المعالجة آليا ويمكن التعبير عنها بالمعلومات الالكترونية السرية. وتم التوصل إلى هذه النتيجة على أساس أننا اليوم نعالج كل بيان كل فكرة كل قرار كل تفصيلة خاصة معالجة آلية، بواسطة الآلة الالكترونية الأكثر شيوعا وهي الحاسب الآلي. وبينما كانت الأسرار تحافظ عليها الصدور فهي الآن تحتويحها ويتم التحفظ عليها في ذاكرة الحواسيب، لهذا فالأسرار اليوم هي أسرار معلوماتية أي معالجة آليا.

في مجال دراسة الحماية الجزائية "للمعلومات الالكترونية السرية"، يمكن اقتصار المصطلح على "المعلومات" فقط دون البقية لأن الدراسة التي تشمل البيئة الرقمية أو المعلوماتية فالمعلومات فيها بالضرورة إلكترونية.

في مجال الحماية الجزائية للمعلومات تطال هذه الحماية، سرية المعلومة وإتاحتها وسلامتها وفي هذه الدراسة تم الاقتصار على مجال الحماية الجزائية للأسرار المعلوماتية، بمعنى أن الدراسة اقتصرت على جانب حماية سرية المعلومة دون الإتاحة والسلامة لعدم ارتباطهم بموضوع الدراسة.

الأسرار المعلوماتية مصطلح وليد اكتساح الأنظمة المعلوماتية مجالات الحياة وعلى كافة الأصعدة، ذلك أن البيانات اليوم تعالج وتنتقل عن طريق وسائل الكترونية كلها تكون لنا ما يسمى بالنظام المعلوماتي مع العلم أن النظام المعلوماتي الذي يعتبر جهاز الحاسب الآلي جزء منه هو الغالب في العصر الحالي. ما جعل مصطلح الجريمة المعلوماتية يرتبط بمصطلح الحاسب الآلي حيث سميت في الأغلب باسمه" جرائم الحاسب الآلي"أو "جرائم الحاسب الآلي والانترنت"، مع العلم أنه في ختام هذه الدراسة تم ترجيح تسمية الجرائم المستحدثة الواردة في عصرنا هذا بالجريمة المعلوماتية كاختصار لجرائم نظم المعالجة الآلية للمعطيات.

الجرائم المعلوماتية هي التي تستهدف المعلومات، فهي أنماط السلوك الإجرامي التي تطال المعلومات المخزنة أوالمعالجة في نظام الحاسب الآلي أو المتبادلة عبر الشبكات، أو أي جهاز الكتروني آخر في حكم الحاسوب كالهاتف الذكي مثلا.

الجريمة المعلوماتية هي " كل فعل غير مشروع وغير قانوني يتم باستعمال الحاسب الآلي أو أي وسيلة معالجة آلية للمعطيات، قام به شخص ما مستخدما معرفته وقدراته بالحاسب الآلي أو أي وسيلة من وسائل المعالجة الآلية للمعطيات، واستخدم فيها الجهاز كأداة أو موضوع للجريمة، سواء كان الجهاز مربوط بشبكات الاتصال أم لا".

نقصد بالأسرار المعلوماتية الأسرار المعالجة آليا، أي تتناول المعالجة الآلية للمعلومات السرية بشكل منظم وفعال بحيث لا تكون هذه المعلومات في مجموعها أوفي الشكل والتجميع الدقيقين لمكوناتها معروفة عادة أوسهلة الحصول عليها من قبل الأشخاص خاصة الذين يتعاملون في نوع تلك المعلومات.

الخصوصية من الناحية اللغوية تقترب من مفهوم السرية، لكنها ليست مرادفة له ذلك لأن السرية تفترض الكتمان والتخفي في حين أن الخصوصية وإن كانت تفرض قدرا من الكتمان والتخفي، لكنها قد تتوفر رغم انعدام السرية.

هناك ضرورة للتفرقة بين السرية المعلوماتية والخصوصية المعلوماتية على هذا الأساس كانت هذه الدراسة شاملة لكل ما هو سري سواء ما تعلق بالحياة الخاصة للفرد أو غير ذلك.

الجرائم الواقعة على الأسرار المعلوماتية قد تقع بواسطة الحاسوب والانترنت، وقد تقع بواسطة أي جهاز في حكم الحاسوب كالهاتف الذكي ولكن لها نفس الوصف القانوني كلها

جرائم معلوماتية، وذات الأمر بالنسبة للتخصيص بشأن الجرائم الواقعة على الأسرار المعلوماتية رغم أن هناك بعض الجرائم يكون ارتكابها أسهل بواسطة الهاتف كالتقاط صور خاصة للأفراد لا يحبذون أن يراها غيرهم .

تعددت سلوكات الاعتداء على سرية المعلومات الالكترونية" الأسرار المعلوماتية"، وحيث تم تجريم تلك السلوكات على الصعيدين الدولي والداخلي بينما نظرة كل مشرع لهذه الأخيرة قد تختلف عن الثاني على النحو الوارد أدناه:

جريمة الدخول غير المصرح به جريمة تهتك فعلا بسرية المعلومات، حيث تم النظر إليها بأنها سلوك يؤدي إلى الاطلاع غير المسموح به على المعلومات المعالجة بواسطة النظام المعلوماتي. لأن مجرد الاطلاع يعتبر جريمة بشرط توفر أركان الجريمة، مع العلم أن المشرع الجزائري اعتبر الحصول على المعلومات بواسطة الدخول غير المصرح به للنظام المعلوماتي واستخدامها لغرض غير مشروع يعتبر جريمة من نوع آخر، وهو ما سماها بالتعامل في معطيات غير مشروعة. وبالنسبة للمشرع الفرنسي اعتبر جريمة الدخول للنظام المعلوماتي غير المصرح به والحصول على المعلومات بالتصنت والاطلاع وغيرها هو نفس الشيء بينما نحن نفرق بين الجرمين.

وفق المشرع الجزائري حينما نص على الجريمة المعلوماتية وسماها جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، ولم يسمها تسمية أخرى لأنه باعتبار أن محل الجرائم المعلوماتية هو المعلومات لا يمكن اعتبار أن تكون المعالجة الآلية بواسطة النظام المعلوماتي للحاسب الآلي وفقط، بينما أيضا أي جهاز آخر في حكمه إذن لهذا كانت التسمية موفقة جدا.

جريمة التعامل في معطيات غير مشروعة من الجرائم التي تمس بالسرية المعلوماتية، حيث أن بعض المعلومات تكون في طي الكتمان وتصبح غير ذلك بعد لحصول عليها من غير المصرح لهم بمعرفتها، فيتم نشرها أو إفشائها للغير أو تهديد أصحابها بذلك. وهي جريمة نص عليها المشرع الجزائري وأعطاها تسمية واحدة وتعددت أشكال الركن المادي فيها، بينما البعض الآخر من المشرعين نظروا إليها بنفس عين التجريم في حين اختلفوا مع المشرع الجزائري من حيث وصف الجرم.

ربما الكثير من يختلف مع المشرع الجزائري في وصفه للسلوك الإجرامي المعلوماتي، ورغم الاتفاق معه في أغلب ما قضى به، بينما لابد له أن يضيف النصوص التالية لكي يمكن اعتباره قد سد الفراغ في إطار التجريم في مجال السرية المعلوماتية ليصبح أفضل كالتالي:

إضافة نص تجريم قرصنة المعلومات، مع استثناء البرامج لوجود نصوص التجريم فيما يتعلق بقانون حماية الملكية الفكرية والأدبية، في حدود ما ينص عليه القانون. بمعنى أن الاعتداء على سرية البرنامج التي لا ينطبق عليها نص حماية الملكية الفكرية نطبق عليها نص قرصنة المعلومات.

التجسس المعلوماتي يختلف عن الدخول غير المصرح به للنظام المعلوماتي، بمعنى أن الدخول غير المصرح به جريمة والبقاء جريمة في حين الدخول بهدف التجسس والتصنت جريمة من نوع آخر والفرق بينهما هو السلوك المترتب بعد الدخول. لهذا لابد على المشرع إضافة نص صريح يتعلق بالتجسس المعلوماتي يجرم بشكل مباشر اعتراض البيانات المعالجة آليا والتصنت والتلصص على المعلومات بمختلف الأشكال وفي جميع المجالات، وبدون استثناء حبذا لو اعتبر التلصص على المعلومات الماسة بأمن الدولة ظرف تشديد، والمبرر في ذلك أن الدخول والاطلاع والحصول على المعلومات غير الترصد للمعلومات والتجسس عليها لغاية في نفس يعقوب.

إفشاء الأسرار المعلوماتية ليس هو إفشاء الأسرار المعلوماتية المهنية هناك فرق كبير بين الجرمين، والملاحظ أن الأغلبية يخلطون بينهما والبعض يدرجهم في ذات السياق والأصح هما مختلفين. فالمشرع الجزائري نص على الأولى في جريمة التعامل في معطيات غير مشروعة في سلوك الإفشاء بينما الثانية تعرض إليها في جريمة إفشاء الأسرار المهنية ولابد له من تعديل النص ليشمل المعلومات الالكترونية وتحديد أركان الجريمة خاصة الركن المعنوي.

تختلف جريمة التجسس المعلوماتي عن جريمة السرقة المعلوماتية، حيث أن الأولى هي الحصول على المعلومات السرية عن طريق اعتراض البيانات المنتقلة عبر النظام المعلوماتي أي المتحركة بينما الثانية هي الحصول على المعلومات عن طريق اختلاس المعلومات المختزنة في ذاكرة الحاسوب أو الهاتف.

التصنت المنصوص عليه في المادة 303 من قانون العقوبات الجزائري ينطبق على التجسس المعلوماتي، وإنما كان من باب أولى النص عليه بموجب نص مستحدث على أساس أن المشرع صادق على الاتفاقية العربية رغم أنه ملزم بها ولكن ما المانع من استحداث نص صريح .

الالتقاط الذهني والسمعي في جريمة السرقة المعلوماتية، يكون محله المعلومات المختزنة في النظام ليس كما هو الشأن بالنسبة للمعلومات المنتقلة عبر النظام، والتي تعتبر اعتراضا لمسار المعلومات وحينها تعتبر تجسسا وليس سرقة.

قائمة المراجع

أولا: المراجع باللغة العربية

I-المصادر والقواميس

أ- المصادر:

القرآن الكريم

ب - القواميس:

1-ابن منظور، محمد بن مكرم، لسان العرب، تحقيق، عبد الله علي الكبير وآخرون، دار المعارف القاهرة.

2-الرازي محمد بن أبي بكر، مختار الصحاح، دار الكتب العلمية، بيروت، 1983.

3-الفيروز أبادي، محمد بن يعقوب، القاموس المحيط، الطبعة السادسة ، مؤسسة الرسالة، بيروت، 1999

4- القاموس القانوني الثلاثي، قاموس قانوني موسوعي، شامل و مفصل عربي- فرنسي- انجليزي، موريس نخلة وآخرون، منشورات الحلبي الحقوقية، سوريا ، 1992.

5- المعجم الوسيط، مجمع اللغة العربية، القاهرة، دار إيحاء الترات العربي، بيروت.

6- جورج متني عبد المسيح، لغة العرب، الجزء الأول، مكتبة لبنان، بدون سنة نشر.

جمال الدين أبي الفضل -محمد بن مكرم ابن منظور الأنصاري الإفريقي المصري، راجعه عبد المنعم خليل إبراهيم، المجلد الثالث، الطبعة الأولى دار الكتب العلمية بيروت لبنان، 2005.

7- قاموس المصطلحات الصادرة عن المنظمة العربية للعلوم الإدارية (انجليزي، فرنسي، عربي)، 1980.

8- عبد المحسن الحسيني، المعجم الكامل عن المعلوماتية، الطبعة الأولى، دار القلم بيروت لبنان، 1987.

9- مفتاح محمد ديب، معجم مصطلحات نظم و تكنولوجيا المعلومات و الاتصالات:انجليزي-عربي ، الدار الدولية للنشر،القاهرة،1995.

II- الكتب العامة:

1- إبراهيم العناني، النظام الدولي الأمني، المطبعة التجارية الحديثة،القاهرة، 1998.

2-أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، 2006.

3- أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الطبعة الخامسة، ديوان المطبوعات الجامعية، الجزائر، الجزء الثاني، 2010.

4- أحمد فتحي سرور،الوسيط في الإجراءات الجنائية، دار النهضة العربية، بدون طبعة، سنة النشر 1996.

5- شحاتة غريب شلقامي:

- الملكية الفكرية في القوانين العربية، دار الجامعة الجدية الإسكندرية، 2009.
- شرح قانون العقوبات قسم عام، دار النهضة العربية، القاهرة، بند1989،823.
6- عبد الرؤوف مهدي، شرح القواعد العامة للإجراءات الجنائية، دار النهضة العربية، القاهرة، 2000.
7- عبد الله سليمان، شرح قانون العقوبات الجزائري، الجزء الأول، دار الهدى للنشر، عين ميلة، الجزائر.
8- علي صادق أبو هيف، القانون الدولي العام، الطبعة السابعة، منشأة المعارف الإسكندرية، 1965.
9- قادري أحمد، أطر التحقيق، دار هومة للنشر و التوزيع، الجزائر، 2013.
10- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة للطباعة و النشر، الجزائر، 2008.
11- محمود نجيب حسيني، دروس في القانون الدولي الجنائي، دار النهضة العربية، القاهرة، 1960.
12-نبيل صقر، الوسيط في شرح جرائم الأموال، دار الهدى، الجزائر، 2012.

III- الكتب المتخصصة:

1-احمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.
2- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع الجزائري والمصري، الطبعة الأولى، دار النهضة العربية، القاهرة، 2010.
3- أسامة المناعسة، جرائم الحاسب الآلي و الانترنت، دراسة مقارنة، الطبعة الأولى، دار وائل للنشر و التوزيع عمان، 2001.
4-أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة و النشر و التوزيع، الجزائر،الطبعة الثانية، 2006.
5- السيد عتيق، جرائم الانترنت، دار النهضة العربية، القاهرة، 2000.
6- الشحات إبراهيم محمد منصور، الجرائم الالكترونية في الشريعة الإسلامية و القوانين الوضعية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011 .
7- أمير فرج يوسف، الجرائم المعلوماتية عبر شبكة الانترنت، دار المطبوعات الجامعية الإسكندرية، 2008
8- انتصار نوري الغريب، أمن الكمبيوتر و القانون، دار الراتب الجامعية، بيروت لبنان، بدون طبعة، 1994.
9- أيمن إبراهيم العشماوي، المسؤولية المدنية عن المعلومات،دار النهضة العربية، القاهرة، بدون طبعة، 2004 .

10- بريستزن جرالا، مرشد الأذكياء الكامل إلى حماية جهازك أثناء التواجد على الانترنت، ترجمة خالد العامري، مروة السيد، دار الفروق، القاهرة، 1999.
11- بشرى حسين الحمداني، القرصنة الالكترونية أسلحة الحرب الحديثة، الطبعة الأولى، دار أسامة للنشر والتوزيع عمان، الأردن، 2014.
12- بلال أمين زين الدين، جرائم نظم المعاجة الآلية للبيانات في التشريع المقارن و الشريعة الإسلامية، دار الفكر الجامعي، الإسكندرية، 2008.
13- جابر وسف المراغي، جرائم انتهاك أسرار الدفاع عن البلاد، دار النهضة العربية، القاهرة، 1998.
14- جلال محمد الزغبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية، دراسة مقارنة ، الطبعة الأولى دار الثقافة للنشر والتوزيع ، عمان الأردن ، 2010.
15-جميل عبد الباقي الصغير:
- الانترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، القاهرة، 2001.
- القانون الجنائي والتكنولوجيا الحديثة، الجرائم الناتجة عن استخدام الحاسب الآلي
16-حازم حسن الجمل، الحماية الجنائية للأمن الالكتروني، الطبعة الأولى، دار الفكر و القانون، المنصورة، 2015.
17-حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، دراسة مقارنة ، دار النهضة العربية،القاهرة، 2009.
18-حنان طلعت أبو العز، الحماية الجنائية لحقوق المؤلف، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007.
19-خالد بن سليمان الغثير و محمد بن عبد الله القحططاني، أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، جامعة الملك سعود ، الطبعة الأولى، 2009.
20-خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت ، دار الثقافة للنشر والتوزيع عمان الأردن ، الطبعة لأولى، 2015.
21-خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء حماية الملكية الفكرية، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.
22-خالد ممدوح إبراهيم:
- الجرائم المعلوماتية، الطبعة الأولى،دار الفكر الجامعي، الإسكندرية، 2009.
-فن التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، دار الفكر الجامعي،الإسكندرية، 2009.
23-خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى للطباعة و النشر عين ميلة الجزائر، 2010.

24-خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012.
25-رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة و في ضوء الاتفاقيات و المواثيق الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011.
26-رشا علي الدين،النظام القانوني لحماية البرمجيات، دار الجامعة الجديدة الإسكندرية، 2007.
27-رشا مصطفى أبو الغيط، تطور الحماية القانونية للكيانات المنطقية،دار الفكر الجامعي الإسكندرية،2006
28-رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الإنترنت، دار النهضة العربية، القاهرة، 2013.
29-رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الالية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية بيروت، لبنان، 2012.
30-زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى للطباعة و النشر الجزائر، 2011.
31-سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دراسة تحليلية ، دار شتات للنشر و البرمجيات، مصر، 2011.
32-سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي الإسكندرية، 2007 .
33-سليمان أحمد فضل، المواجهة التشريعية و الأمنية الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2008.
34-سهيل محمد العزام، الوجيز في جرائم الإنترنت، الطبعة الأولى، دائرة مكتبة الجامعة الأردنية، 2009.
35- شلباية مراد وفاروق علي، مقدمة إلى الانترنت، الطبعة الأولى، دار الميسرة للنشر والتوزيع، عمان، 2001.
36-شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة الإسكندرية، 2007 .
37- صليحة علي صداقة، الابعاد القانوني و الأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية، الأسكندرية، 2017.
38-طارق عفيفي، صادق أحمد، الجرائم الالكترونية، جرائم الهاتف المحمول، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015.
39-عامر محمود الكسواني، التجارة عبر الحاسوب، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2008.

40-عبد الله الشيخ عصمت، دور النظم وتكنولوجيا المعلومات في تيسير وفعالية العمل الإداري، دار النهضة العربية، القاهرة، 1998.
41- عبد الصبور عبد القوي علي مصري، الجريمة الالكترونية، دار العلوم للنشر و التوزيع، القاهرة، الطبعة الأولى، 2008
42-عبد الفتاح بيومي حجازي:
- مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، الطبعة الأولى، دار النهضة العربية الإسكندرية، 2009. دار الفكر الجامعي، الإسكندرية، 2006.
-نحو صياغة عامة في علم الجريمة والمجرم المعلوماتي، الطبعة الأولى، منشأة المعارف الإسكندرية،2009.
-الأحداث و الانترنت، الطبعة الأولى،دار الفكر الجامعي، الإسكندرية، 2002.
43-عبد الله الشخ عصمت، دور النظم وتكنولوجيا المعلومات ف تسيير وفعالية العمل الإداري، دار النهضة العربة، القاهرة، 1998.
44-عبد الله ذيب محمود، حماية المستهلك في التعاقد الالكتروني دراسة مقارنة، دار الثقافة للتوزيع والنشر عمان الأردن، الطبعة الأولى، 2012.
45-عصام أحمد البهجي، حماية الحق في الحياة الخاصة،في ضوء حقوق الإنسان و المسؤولية المدنية،دار الجامعة الجديدة للنشر الإسكندرية، 2005.
46-عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة و القانون، دراسة مقارنة، الطبعة الثانية، منشورات الحلبي الحقوقية، لبنان، 2007.
47-علي أحمد عبد الزغبي، حق الخصوصية في القانون الجنائي، دراسة مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2006.
48-علي جبار الحسناوي، جرائم الحاسوب والانترنت، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، الطبعة العربية 2009 .
49-علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للنشر والتوزيع الإسكندرية، 1992.
50-علي عدنان الفيل:
إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، 2012 .
الإجرام الالكتروني، الطبعة الأولى، منشورات زين الحقوقية، 2011.
51-عماد مجدي عبد المالك، جرائم الكمبيوتر و الانترنت، دار المطبوعات الجامعية، الإسكندرية، 2011.
52-عماد محمد سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، الطبعة الأولى، دار وائل للنشر الأردن ، 2005 .

53- عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة، 2004 .
54- عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتعلقة بالحاسب الآلي و أبعادها الدولية، القاهرة
1992.
55-عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات، دراسة مقارنة، دار النهضة العربية، القاهرة، 2000.
56-عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والإنترنت في مصر والدول العربية، المكتب الجامعي الحديث، بدون طبعة وبدون سنة نشر.
57-فتوح الشادلي و عفيفي كامل عفيفي،جرائم الكمبيوتر،منشورات الحلبي الحقوقية،بيروت لبنان، 2003.
58-فريد منعم جبور، حماية المستهلك عبر الانترنت ومكافحة الجرائم المعلوماتية (دراسة مقارنة)، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت، لبنان، 2010.
59- فريد هكيت، الخصوصية في عصر المعلومات، ترجمة محمد محمود شهاب، مركز الأهرام للترجمة والنشر القاهرة، الطبعة الأولى ، 1999.
60- فهد سيف بن راشد الحوسني، جرائم التجارة الالكترونية، دراسة مقارنة،السحاب للنشر والتوزيع سلطنة عمان، 2010
61- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، جامعة عين شمس القاهرة 2012.
62- ماجد أحمد عبد الرحيم الحياري، مسؤولية الصحفي المدنية، دراسة مقارنة بين القانونين الأردني والمصري
الطبعة الأولى، دار يافا العلمية للنشر والتوزيع، 2008.
63- محمد احمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن ، 2009.
64- محمد أحمد فكيرين، أساسيات الحاسب الآلي، دار الجامعة الجديدة، بيروت، 1993.
65- محمد أمين الرومي، جرائم الكمبيوتر و الانترنت، دار المطبوعات الجامعية الإسكندرية،2004.
66- محمد أمين الشوابكة، جرائم الحاسوب والأنترنت الجريمة المعلوماتية، الطبعة الرابعة، دار الثقافة للنشر والتوزيع، عمان الأردن، 2012.
67- محمد أمين الشوابكة، جرائم الحاسوب و الانترنت، الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، عمان الأردن، الطبعة الرابعة، 2011.

68- محمد حسام محمود لطفي، الحماية القانونية لبرامج الحاسب الآلي، دار الثقافة للطباعة والنشر، 1987.
69- محمد حماد الهيتي، جرائم الحاسوب، الطبعة الأولى، دار المناهج للنشر و التوزيع، عمان الأردن، 2006.
70- محمد حماد مرهج الهيتي، جرائم الحاسوب، الطبعة الأولى دار المنهاج للنشر والتوزيع، عمان الأردن، 2006.
71- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي ، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.
72- محمد سامي الشوا، ثورة المعلومات و انعكاساتها على قانون العقوبات، دار النهضة العربية القاهرة، 1994.
73- محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والانترنت، ، منشأة المعارف الإسكندرية، 2006.
74- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، دراسة مقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، 2009.
75- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر الإسكندرية، بدون طبعة، 2004.
76- محمد محمد الهادي، التطورات الحديثة لنظم المعلومات المبنية على الكمبيوتر، الدور الثقافي و التنموي للكتب والمكتبات في عالم متغير، الدار الشرقية القاهرة، 1993.
77- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، للنشر، الإسكندرية، 2001.
78- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، الطبعة الأولى المكتبة العصرية للنشر والتوزيع، مصر، 2010.
79- محمد مصطفى الشقيري، السرية المعلوماتية ، ضوابطها و أحكامها الشرعية، الطبعة الأولى، دار النشر الإسلامية، بيروت لبنان، 2008.
80- مدحت محمد عبد العزيز ابراهيم، الجرائم المعلوماتية على النظام المعلوماتي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2015.
81- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة القاهرة، 2008.
82- ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في حرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر، 2006.
83- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية ، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005.

84- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2007.
85- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف الإسكندرية، 2008.
86- نعيم مغبغب، حماية برامج الكمبيوتر، دراسة في القانون المقارن، منشورات الحلبي الحقوقية، بيروت،الطبعة الثانية 2009.
87- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة عمان، الأردن، 2008.
88- هدى حامد قشقوش، الجريمة المنظمة، القواعد الموضوعية و الإجرائية و التعاون الدولي ، دار النهضة العربية، 2000.
89- هلالي عبد الله أحمد:
- الجوانب الإجرائية والموضوعية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، القاهرة، 2003.
-تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، القاهرة، 1998.
90- وليد الزيدي، القرصنة على الانترنت والحاسوب، الطبعة الأولى دار أسامة للنشر والتوزيع الأردن عمان، 2003.
91- يوسف أبو الحجاج، أشهر جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الكتاب العربي، القاهرة 2010.
92- يونس عرب، موسوعة القانون وتقنية المعلومات، الكتاب الأول، قانون الكمبيوتر، الطبعة الأولى، منشورات اتحاد المصارف العربية، بيروت، 2001.

IV- الأطروحات ومذكرات الماجستير:

أ- الأطروحات:

1- أحمد سعد الحسيني، الجوانب الإجرائية الناشئة عن استخدام الشبكات الالكترونية، رسالة دكتوراه، كلية الحقوق، قسم القانون الجنائي، جامعة عين شمس، 2012.
2- ايهاب عبد السميع روبي محمد، الجريمة عبر الانترنت، صورها ومشاكل إثباتها، أطروحة دكتوراه،جامعة حلوان، 2012.
3- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، رسالة دكتوراه ، جامعة القاهرة، بدون سنة.
4- منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات صورها ومشاكل إثباتها، رسالة دكتوراه جامعة القاهرة ، كلية الحقوق، سنة 2013.

5- الموسوس عتو، حماية الحق في الخصوصية في القانون الجزائري في ظل التطور العلمي والتكنولوجي، دراسة مقارنة رسالة دكتوراه جامعة سيدي بلعباس، السنة الجامعية2014-2015.

ب- مذكرات الماجستير:

1- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري المقارن، جامعة منتوري قسنطينة، رسالة ماجستير 2013.

2- سالم محمد بني مصطفى، جريمة السرقة المعلوماتية، ماجستير قانون عام، جامعة جدارا، الأردن، سنة 2011.

3- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، جامعة الحاج لخضر، باتنة، السنة الجامعية 2012-2013.

4- ماجد بن عبد الرحمان الكعيد، الحماية الجنائية للمعلومات الرقمية البنكية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض 2011.

Vالمقالات:

1- ايهاب محمد الروسان، التفريد القضائي للعقوبة ، عن الموقع الالكتروني /http://ar.jurispedia.org

2- العربي بن حجار ميلود، تشريعات الملكية الفكرية في حقل حماية البرمجيات بالجزائر ، العدد 26، سبتمبر 2011 ، عن الموقع الالكتروني http://journal.cybrarians.info/in

3- راضية مشري، الحماية الجزائية للمصنفات الرقمية في ظل حق المؤلف، مجلة التواصل لكلية الحقوق، جامعة 08 ماي 45، قالمة، عدد 34، جوان 2013، ص 137، منشور PDF على الموقع الالكتروني http://dpubma.univ-annaba.dz/?p=2766

4- زوزو هدى، الترسب التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مقال منشور بمجلة السياسة والقانون، العدد الحادي عشر ، جوان 2014، ص 117، عن الموقع الالكتروني http://revues.univ- ouargla.dz/index.php/numero-11-2014-dafatir/1991-2014-06-16-08-50-20 -

5- عبد الرحمان ألطاف، تحديات حماية الملكية الفكرية للمصنفات الرقمية، عن الموقع الالكتروني http://www.shaimaaatalla.com/vb/showthread.php?t=3948 http://www.hespress.com

5- حسين بن سعيد بن سيف الغافري ،جريمة الاعتراض، عن /http://www.omanlegal.net

6-محمد الألفي،دور المجتمع المدني في مكافحة مظاهر العدوان الإجرامي عبر الانترنت، عن الموقع الالكتروني http://www.minshawi.com
7-محمد حماد مهرج الهيثي، نطاق الحماية الجنائية للمصنفات الرقمية، دراسة مقارنة في القوانين العربية لحماية حق المؤلف، مجلة الشريعة والقانون، العدد 48، كلية الحقوق جامعة مملكة البحرين، أكتوبر 2011.
8- محمد عبد الرحيم سلطان العلماء، جرائم الأنترنت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث الطبعة الثالثة 2004
09- محمد عبد المحسن المقاطع، نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر، بحث مقدم لمؤتمر الكويت الأول للقانون والحاسب الآلي ، كلية الحقوق ، جامعة الكويت ، الطبعة الأولى 1994.
10- مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد 21 جوان 2012.
11-نرجس صفو، الحماية القانونية للملكية الفكرية في البيئة الرقمية، مداخلة بالمؤتمر الدولي الحادي عشر لمركز جيل البحث العلمي حول التعلم بعصر التكنولوجيا الرقمية، في طرابلس لبنان من 22إلى 24 أبريل 2016، ص 1، منشور على الموقع الالكتروني http://jilrc.com/
12-نادية محمد معوض، أثر المعلوماتية على الحق في سرية الأعمال، ص 15، منشور على الموقع الالكتروني www.flaw.bu.edu.eg/flaw/images/part1.pdf
13-وداد أحمد العيدوني، حماية الملكية الفكرية في البيئة الرقمية (برامج الحاسوب وقواعد البيانات نموذجا)، مداخلة ألقيت في المؤتمر السادس لجمعية المكتبات والمعلومات السعودية الموسوم"البيئة المعلومات الآمنة، المفاهيم والتشريعات والتطبيقات، المنعقد بمدينة الرياض خلال الفترة بين 06-07 أفريل 2010، ص 08.
14- يونس عرب دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، ورقة عمل مقدمة إلى ندوة أخلاق المعلومات - نادي المعلومات العربي 16-17 أكتوبر 2002 – عمان – الأردن.
15-يونس عرب، الخصوصية وحماية البيانات، منشور على شبكة الإنترنت من خلال الموقع الالكتروني www.arablaw.net

VIالنصوص التشريعية:

آ- المعاهدات و الاتفاقيات الدولية

1-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010.

2- اتفاقية بودابست (الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية) بتاريخ 2001/11/08.
3- معاهدة الويبو بشأن حق المؤلف كما اعتمدها المؤتمر الدبلوماسي في 20 ديسمبر 1996.
4-اتفاقية باريس لحماية الملكية الصناعية المؤرخة في 20 مارس 1883 و المعدلة ببروكسل في 14 ديسمبر 1900 وواشنطن في 20 يونيو 1911 ولاهاي في 6 نوفمبر 1925 ولندن في 2 يونيو 1934 ولشبونة في 31 أكتوبر 1958 واستوكهولم في 14 يوليو 1967 والمنقحة في 28 سبتمبر 1989
5-إتفاقية برن لحماية المصنفات الأدبية والفنية وثيقة باريس المؤرخة 24 يوليو 1971 والمعدلة في 28 سبتمبر 1979.
6-اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية (تربس).

ب - التشريعات الداخلية العربية:

1-مرســـوم ســـلطاني رقـم 12/2011 بإصدار قانون مكافحة جرائم تقنية المعلومات، لسلطنة عمان، جريدة رسمية عدد 929.
2- القانون الأردني لجرائم أنظمة المعلومات رقم 30 لسنة 2010، الجريدة الرسمية عدد 5056 المؤرخة في 2010/09/16، ص 5334
-القانون رقم 15 لسنة 2015، الجريدة الرسمية مؤرخة في 2015/05/19، ص 5292
-قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001، جريدة رسمية 2001/4524 المؤرخة في 2001/12/31 رقم الصفحة 6010
6-قانون العقوبات الأردني رقم 16/ 1960، جريدة رسمية مؤرخة في 1960/01/01 و المعدل بالقانون رقم 2011/8 في الجريدة الرسمية رقم 5090 بتاريخ 2011/05/02.

ج- التشريعات الجزائرية:

1- القوانين الأوامر:

-الدستور الجزائري لسنة 2016 بموجب القانون رقم 01/16 المؤرخ في 6 مارس 2016 ، جريدة رسمية رقم 14 مؤرخة في 7 مارس 2016، ص 3.
-القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،جريدة رسمية العدد 47 بتاريخ 16 أوت 2009.
- القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 156/66 المؤرخ في 08/06/1966 المتضمن قانون العقوبات، جريدة رسمية العدد71لسنة2004 المعدل والمتمم.
-الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، الصادر بالجريدة الرسمية عدد 44 بتاريخ 23 يوليو 2003.

-الأمر 06/03 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات، جريدة رسمية عدد مؤرخة في 23 جويلية 200344، ص 22.
-الأمر 07/03 المؤرخ في 19 جويلية 2003 المتعلق ببراءة الاختراع، جريدة رسمية عدد 44 مؤرخة في 23 جويلية 2033، ص 27.
- الأمر رقم 03-08 المؤرخ في 19 يوليو 2003 يتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، الصادر بالجريدة الرسمية عدد 44 بتاريخ 23 يوليو 2003.
- الأمر رقم 97-10 المؤرخ في 6 مارس 1997 المتعلق بحقوق المؤلف والحقوق المجاورة، جريدة رسمية عدد 13 مؤرخة في 12 مارس 1997 ص3.
-الأمر رقم 73-14 المؤرخ في 03 ابريل 1973 المتضمن حق المؤلف، الجريدة الرسمية عدد 29 بتاريخ 10 ابريل 1973.
-الأمر 73- 26 المؤرخ في 05 يونيو 1973 يتعلق بإنظمام الجزائر للاتفاقية العالمية لسنة 1952 حول حق المؤلف المراجعة بباريس في 24 يوليو 1971، جريدة رسمية عدد 53 بتاريخ 03 يوليو 1973.

2- المراسيم و القرارات:

- مرسوم رئاسي رقم 288/15 المتعلق بالقواعد العامة المتعلقة بالنظام الوطني للمراقبة بواسطة الفيديو، المؤرخ في 22 غشت 2015، جريدة رسمية عدد 45،ص 3.
- مرسوم رئاسيّ رقم 252-14 مؤرّخ في 8 سبتمبر يتضمّن التّصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر سنة 2010، جريدة رسمية عدد 57 بتاريخ 28 سبتمبر 2014.
-المرسوم التنفيذي رقم 07-162 المؤرخ في 30 ماي 2007 يعدل و يتمم المرسوم رقم 2001-123 المتعلق بنظام استغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية، و على مختلق خدمات المواصلات السلكية و اللاسلكية، جريدة رسمية عدد 37 لسنة 2007.
- المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فبراير 2002، يتضمن مصادقة الجزائر بتحفظ على إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، جريدة رسمية رقم 09 بتاريخ 10 فبراير 2002.
-المرسوم التنفيذي رقم 02-141 المؤرخ في 16 أبريل 2002 يحدد القواعد التي يطبقها متعاملوا الشبكات العمومية للمواصلات السلكية و اللاسلكية من أجل تحديد تعريفة الخدمات المقدمة للجمهور، جريدة رسمية عدد 28 لسنة 2002.
-المرسوم التنفيذي رقم 2001-123 المؤرخ في 09 ماي 2001 يتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف المواصلات السلكية و اللاسلكية، جريدة رسمية عدد 27 لسنة 2001.

-المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 يتعلق بضبط شروط وكيفيات إقامة خدمات الانترنت و استغلالها، المعدل بموجب المرسوم التنفيذي رقم 2000-307 المؤرخ في 14 أكتوبر 2000، جريدة رسمية عدد 60 بتاريخ 15 أكتوبر 2000.
- المرسوم الرئاسي رقم 97-341 المؤرخ في 13/09/1997 المتضمن انضمام الجزائر بتحفظ إلى الاتفاقية برن لحماية المصنفات الأدبية والفنية المعدلة و المتممة ،جريدة رسمية عدد61 بتاريخ 14 سبتمبر 1997 .
-قرار وزاري مشترك مؤرخ في 30 أكتوبر سنة 2014 يحدد كيفيات تطبيق النظام المعلوماتي لمحاسبة التسيير في المؤسسات العمومية للصحة وكذا قائمة المؤسسات المعنية بتنفيذ هذا النظام، جريدة رسمية العدد 01، مؤرخة في 07 يناير 2015.

ثانيا:المراجع باللغة الأجنبية

أ- الكتب:

1. PIERRE CATALA, Ebauche d’une Theorie juridique de l’information,D.1984, chron
2. PIERRE CATALA, Les transformations de droit par l’informatique, in Emergence du droit de l’informatique, éd Parque, 1983
3. PIERRE CATALA, Ebouche D’une Theorie juridique de l’information,D.1984 .
4. AlAIN Houande. .LINANT de Bellefant Xavier, Pratique du droit de l’informatique, edition Delmas (5eédition) avril 2002, (France) .
5. JéROME HUET«droit prive et informatique Herbert,L emergence du droit de l’informatique, 1983
6. Kenneth C Lauden , Jane Lauden , Management Information Systemmanaging The Digital Firm” , seventh edition, prentice-bhall,inc,new jersey,USA, 2004.
7. Laure Zicry, Enjeux et maitrise des cyber-risques, édition Largus , France,2014
8. Lucas André , jean DEVRéZE, jean frayssinet, Droit de l’informatique et l’internet ,éditions dalloz, collection thémis (droit privé) 2001 (France).

9. Michael JAMES Privacy and Human Rights: An international and comparative study wide special reference to developments in information technology, Dartmouth publishing compary.(1994)
10. RoSALIND Resnick, exploring the world of services ,sybex inc 1993.
11. ZICRY Laure, Enjeux et maitrise des cyber-risques,largus , edition,2014, France.
12. BENSOUSSAN ALAIN, Le vol des programmes et des fichier, un grand malentendu expertisés, février1981.

2- القوانين الفرنسية :

1. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978.
2. Loi n°88-19 du 05 janvier 1988 relative à la fraude informatique, JORF du 06 janvier 1988.(LOI GODFRAIN).
3. Loi n° 92-683 du 22 juillet 1992, portant réforme du code pénal, texte origine au 01 mars 1994.
4. Loi n° 2004-575 du juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 200.
5. Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF 10 mars 2004 en vigueur le 1er octobre 2004.
6. Loi n° 2004-575 du juin 2004 pour la confiance dans l'économie numérique, JORF n°0143 du 22 juin 2004
7. Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF n°182 du 7 août 2004 page 14063, texte n° 2.

8. Loi n° 2009-1311 du 28 octobre 2009 relative à la protetion pénale de la propriété littéraire et artistique sur internet, JORF Du 29 Octobre 2009, texte 1 sur 183.
9. Loi n° 2012-287 Du 1er mars 2012 relative à l'exploitation numérique des livres indisponibles du XXe siècle, JORF Du 2 mars 2012, texte 1 sur 133.
10. Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, JOPF n°0075 du 28 mars 2012, texte n°2, P5604,(art 9 modifie les articles 323-1,323-2,323-3 de code pénal français).
11. loi n° 2013¬-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n°0294 du 19 décembre 2013 page 20570 texte n° 1
12. Loi n°2014-¬1353 du 13 novembre 2014 renforçant les dispositions relatives à la lute contre le terrorisme, art. 16, JOPF n° 0263 du 14 novembre 2014.

ثالثا:مواقع الانترنت

http://ar.jurispedia.org /
http://ar.wikipedia.org/wiki
http://journal.cybrarians.info/in
http://www.accronline.com
http://www.al-jazirah.com.sa/digimag/13062004/co27.htm
http://www.arablaw.org/arablaw.net
http://www.djazairess.com
http://www.djelfa.info
http://www.f-law.net/law/threads/
http://www.ita.gov.om /
http://www.kenanaolinecom
http://www.lebarmy.gov.
http://www.maljasem.com /
http://www.omanlegal.net/
http://www.press-maroc.com

http://www.shaimaaatalla.com/vb/showthread.php?t=3948
http://www.startimes.com
http://www.startimes.com/?t=16525602
http://www.startimes.com/f.aspx?t=33290431
http://www.startimes.com/f.aspx?t=34350161
http://www.th3professional.com /
http://www.wipo.int/wipolex/ar/profile.jsp?code=DZ

فهرس

الملخص باللغة العربية:

تمثل الأسرار المعلوماتية في البيانات السرية المعالجة آليا وهي ما نعبر عنه بالمعلومات، ولا يدخل في نطاق المعلومات بالمفهوم الحديث كل ما يمكن أن يطلق عليه مجازا معلومات. فالمعلومة محل الحماية القانونية الجزائية، لابد من أن تتصف بالسرية. وبالتالي، فإن موضوع الحماية الجزائية للأسرار المعلوماتية يشمل حماية كل الأسرار المعالجة آليا من كل أنواع الاعتداءات ما تعلق منها بالاطلاع المجرد أو استعمالها لأغراض غير مشروعة كالإفشاء والسرقة أو اعتراض طريقها وغير ذلك من السلوكات المستحدثة الماسة بحق صاحب المعلومة في الحفاظ على سريتها، طبعا بالوسائل الفنية ذات الحدين التي تعتبر من جهة أهم وسائل المعالجة والتخزين والإرسال ومن جهة أخرى هي ذاتها الوسائل التي سهلت انتهاك سرية المعلومات.

الكلمات المفتاحية: أسرار، معلومات، أنترنت، حماية، عقوبات.

الملخص باللغة الفرنسية:

La confidentialité informatique est un ensemble des données confidentielles traitées automatiquement , ce qu'on appelle des informations, Ce terme dans le concept moderne ne peut pas comprendre tout ce qu'on peut appeler métaphoriquement informations car l'information qui est protégé par la loi dans la matière pénale, doit être caractérisée par la confidentialité. Ainsi, en matière de protection pénale de confidentialité informatique, les données automatisées doit être protégées de toute atteinte tel que la consultation abstraite , utilisation illégale , vol ou d'autres faits développés , portant atteinte au droit de son propriétaire de garder sa confidentialité, et cela avec des moyens techniques décrites binomiales, qui sont d'un part des moyens de traitement ,de stockage et de la transmission, et d'autre part, sont des méthodes qui facilitent la violation de la confidentialité des informations.

Mots-clés: secrets, informations, Internet, protection , sanctions.

الملخص باللغة الانجليزية:

The computer confidentiality is a set of secret data processing automatically, what is called information. The latter is a modern concept protected by the criminal law. Therefore, the topic of the legal protection of information includes the protection of infromation from any illegal uses such as revealing these secrets, fraud, theft, cybercrimes. As a result, it is crucial to protect the individuals information confidentiality by two edged swords means, i,emeans of data processing, stocking, and transmission are both useful and at the same time tools used to violate the information confidentiality.

Key words: information, confidentiality, protection, criminal law.