جامعة أكلي محند اولحاج – البويرة
كلية الحقوق والعلوم السياسية
قسم القانون العام

الجريمة المعلوماتية في ظل التشريع الجزائري

مذكرة لنيل شهادة الماستر في القانون العام
تخصص: القانون الجنائي والعلوم الجنائية

إعداد الطالبة:
لعاقل فريال

إشراف الأستاذ:
بوديسة كريم

لجنة المناقشة

الأستاذ: حمودي ناصر.....رئيسًا
الأستاذ: بوديسة كريم.....مشْرِفًا ومقرّرًا
الأستاذ: خليفي سمير.....ممتحنا

السنة الجامعية:

2015/2014

القوانين مرآة المجتمع ومقياس الحضارة ورقي الدولة، فهي النور الذي يهدي إلى الصواب دون إرهاق، وبقدر ما تكون متطورة بقدر ما تتحقق الغايات التي وجدت لأجلها، وقد رافق التطور الكبير الذي شهده العالم منذ منتصف القرن الماضي تطورات وتبدلات بسائر جوانب الحياة في المجتمع، مما أدى إلى ظهور عدة إشكالات.

وهو ما حذا إلى التفكير بوسيلة يتم من خلالها تجاوز هذه المشكلات، وأفضى إلى ظهور الكمبيوتر بكفاءته العالية في تجميع وتركيب وترتيب واسترجاع المعلومات في ثوان معدودة وبدقة متناهية لينطلق بذلك عصر جديد وهو ما يحلو للكثير أن يطلق عليه **عصر المعلوماتية** نظرا لما اكتسبته المعلومات فيه من أهمية فائقة ولما أصبح لها من تأثير هائل على البشر والحكومات، فأصبحت المعلومة قوة لا يستهان بها في يد الفرد أو في يد الدولة بل أصبحت المعلومات سلاحا في يد المجرمين.

ومن هنا نشأ ما يسمى جرائم المعلوماتية والتي يستخدم فيها الكمبيوتر لأغراض غير شرعية، مثل سرقة الأموال عن طريق اختراق نظام الكمبيوتر الخاص بمؤسسة أو مصرف معين أو سرقة المعلومات عن طريق اختراق شبكة اتصالات معلوماتية أو يكون الاختراق لأهداف سياسية أو عسكرية أو دينية أو غير ذلك.

وقد كثرت هذه الجرائم في الآونة الأخيرة بازدياد استخدام الكمبيوتر من قبل عدد كبير من الناس في معظم دول العالم وازداد عدد شبكة الاتصالات المعلوماتية وتوسعها، ويصعب تحديد حجم الخسارة الفعلية التي تنجم عن جرائم الكمبيوتر حيث أن بعض هذه الجرائم لا يتم اكتشافها والبعض الآخر يتم اكتشافها ولكن لا يعلن عنها من قبل الشركات والمؤسسات التي تتعرض لها حتى لا يؤثر ذلك على سمعتها وثقة المتعاملين معها.

وغالبا تكون البنوك والمصارف ومراكز المعلومات المهمة هدفا لتلك الجرائم كما أن نسبة كبيرة من مرتكبي تلك الجرائم تكون من موظفي المصارف والمنشآت نفسها حيث يسهل عليهم معرفة الرموز المستخدمة للدخول إلى النظام او المستخدمة في عملية تحويل الأموال وبالتالي استخدامها في ارتكاب الجريمة.

أهمية موضوع البحث:

يرجع سبب اختيار الموضوع التعريف بظاهرة جديدة هي الجريمة المعلوماتية التي بدأت في الظهور والانتشار وارتبطت بتكنولوجيا الحاسبات الآلية مما أسفر عن تميزها بمجموعة من الخصائص تختلف عن غيرها من الجرائم مما يستتبع ضرورة التعامل معها بما يتلاءم من هذه الخصوصية.

ولما كانت هذه الجرائم ترتبط بتقدم المجتمعات فكلما ازداد اعتماد المجتمع على الحاسبات الآلية كلما كان ذلك إيذانا بزيادة معدل جرائم المعلوماتية كان لزاما أن يواكب هذا التقدم فهما كاملا للجريمة المعلوماتية وكيفية مواجهتها سواء من الناحية التقنية وهو عمل المتخصصين في مجال تكنولوجيا المعلومات أو من الناحية القانونية وهي مهمة المشتغلين بالقانون.

لقد زاد من أهمية البحث صعوبة تطبيق النصوص التقليدية على هذه الجرائم وهو ما دفع العديد من الدول إلى التدخل التشريعي لمواجهة الجريمة المعلوماتية لذا فإن إدراك ماهية هذه الجريمة واستظهار خصائصها وسمات مرتكبيها ودوافعهم وجزاءاتها يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة.

ثم ما يزيد من أهمية هذا الموضوع صدور القانون رقم 15/04 المعدل والمتمم للأمر رقم 156/66 المتضمن قانون العقوبات الذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية.

وبهذا سنحاول إبراز من خلال طرح الإشكال التالي:

هل الترسانة القانونية للمشرع الجزائريكفاية للتصدياللجريمة المعلوماتية وردع مرتكبيها، أم لابد من إعادة النظر في فحوها لتواكب خصوصيات الجريمة المعلوماتية؟

للإجابة عن هذا التساؤل ارتأينا تقسيم هذا البحث إلى فصلين نتناول في أوله الأحكام العامة للجريمة المعلوماتية بتبيان مفهومها على ضوء التشريعات المقارنة بالإضافة إلى التطرق إلى خصوصيات الجريمة المعلوماتية إلى أن نفضي إلى تحديد أركانها.

أما في الفصل الثاني سنضفي عليه جانبا تطبيقيا بالتطرق إلى مكافحة الجريمة المعلوماتية في ظل الترسانة القانونية الجزائرية.

الفصل الأول

الفصل الأول

أحكام الجريمة المعلوماتية.

إن الحديث عن الجرائم الناشئة عن الاستخدام غير المشروع للكمبيوتر كأداة لارتكاب الأفعال غير المشروعة وشبكة الانترنت المرتبطة به التي ساهمت إلى حد كبير إلى انتشار الجريمة بمختلف أشكالها لنذهب بالقول أننا أمام عولمة الجريمة، وإن كان في نطاق تطبيق نصوص القانون الجنائي، إلا أنه يجب أن نعترف أننا بصدد ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، سواء من حيث محل الجريمة أو أسباب ارتكابها أوصفات المجرم المعلوماتي فالجريمة هنا جريمة معلوماتية تتعلق بالتقنية المعتمدة على المعالجة الالكترونية للمعلومات والبيانات وقبل الدخول في الحديث عن مختلف الإشكالات التي ثارت في خصوص هذا الموضوع من خلال إخضاعها لقانون العقوبات وبعض القوانين التقليدية والخاصة، سنتعرف من خلال هذا الفصل إلى المفاهيم العامة للجريمة المعلوماتية من خلال مبحثين، نتطرق في المبحث الأول إلى مفهوم الجريمة المعلوماتية وفي المبحث الثاني إلى أركان الجريمة المعلوماتية.

المبحث الأول

مفهوم الجريمة المعلوماتية

لقد ترتب على الاستخدام المتزايد لنظم المعلومات إلى نشوء ما يعرف بالجريمة المعلوماتية، ولقد استخدمت عدة مصطلحات للدلالة على هذه الظاهرة الإجرامية فمنهم من يطلق عليها: **الغش المعلوماتي**، والبعض الآخر يطلق عليها اسم **جرائم الحاسب الآلي**، والآخر **جرائم الكمبيوتر والانترنت** أو **الجريمة الالكترونية** أما في الدول الأوربية فيطلق عليه اسم:**cybercriminalité**.[1]

إن الجريمة المعلوماتية جريمة مستحدثة يعتمد مرتكبها على وسائل تقنية ويكون ذا دراية كافية باستخدام النظم المعلوماتية لذا فإن الإحاطة بمفهومها الدقيق لا يزال محل خلاف فقهي، فهي ظاهرة إجرامية مستحدثة تتميز عن الجريمة التقليدية، وتختلف عنها من حيث المفهوم، ولإزالة اللبس سنتعرض في هذا المبحث إلى مطلبين:

نتعرض لتعريف الجريمة المعلوماتية من خلال(المطلب الأول).

ونخصص (المطلب الثاني) إلى خصائص ودوافع الجريمة المعلوماتية.

المطلب الأول

تعريف الجريمة المعلوماتية

تعددت التعريفات التي تناولت الجريمة المعلوماتية، ويرجع ذلك إلي الخلاف الذي أثير بشأن تعريف هذه الجريمة، فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين انتقلوا بالجريمة من صورتها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها، لأن الجريمة المعلوماتية هي من الظواهر الحديثة، وذلك لارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات

[1] قربوز حليمة، الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006_2009، ص1.

والاتصالات. وقد أحاط بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها.

الفرع الأول

التعاريف الفقهية

على الرغم من تنامي جهود التصدي لظاهرة الإجرام المعلوماتي إلا أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف على نحو ضيق وجانب أخر عرفها على نحو موسع.

أولا :التعريف الضيق للجريمة المعلوماتية.

يعرف الفقيه الفرنسي (Mass) جريمة الكمبيوتر بأنها:" ***الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح***"[1] وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال استخدم لهذا التعريف معيارين هما: الوسيلة، وتحقيق الربح المستمد من معيار محل الجريمة المتمثل في المال.

ويعرفها الفقيهان الفرنسيان (Vivant وLe Stant) بأنها: "***مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب***"[2] هذا التعريف مستند من بين معيارية على احتمال جدارة الفعل بالعقاب وهو معيار غير منضبط ولا يستقيم مع تعريف قانوني وان كان يصلح هذا التعريف في نطاق علوم الاجتماع وغيرها.

ذهب الفقيه (Merwe) إلى أن الجريمة المعلوماتية هي:**"الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي – أو هو الفعل الاجرامى الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية".**

[1] -ابرهيمي سهام،مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2004، 2007، ص7.

[2] Vivant et autres: Informatique et droit pénal. Les biens informatiques objets de fraude. Lamy informatique.1991.n°3445.p1511.

كما عرفها الفقيه (Ros Blat) بأنها:**"كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الالى والى تحويل طريقه".**

وعرفها (كلاوس تايدومان) بأنها:**"كافة أشكال السلوك غير المشروع الذي يرتكب باسم الحاسب الآلي".**

ويرى البعض أن تعريف كلا من (Marwe)و(Ros Blat) جاءا مقصورين على الإحاطة بالظاهرة الإجرامية أما تعريف كلاوس تايدومان فيؤخذ عليه أنه بالغ في العمومية والاتساع، لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع.[1]

ويدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة، تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها: **"الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا".**[2]

ثانيا :التعريف الموسع للجريمة المعلوماتية.

ذهب الفقيهان (Michel وCredo) إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته.[3]

---

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت،الطبعة الأولى، دار الفكر الجامعي، مصر، 2006،ص98.

[2] المرجع نفسه،ص99.

[3] طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر1، كلية الحقوق، 2011،2012، ص6.

وذهب رأى أخر من الفقه إلى تعريف الجريمة المعلوماتية بأنها:"**عمل أو امتناع يأتيه الإنسان، إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب".**

ويرى جانب من الفقه من أنصار هذا الاتجاه الموسع بأنها:"**كل سلوك اجرامى يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر".**

ويعرفهاTièdement بأنها ":**كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب** "

من خلال هذه التعريفات يتبين لنا أن هذا الاتجاه يوسع من مفهوم الجريمة المعلوماتية، حيث أن مجرد مشاركة الحاسب الآلي في السلوك الإجرامي يضفي عليه وصف الجريمة المعلوماتية.[1]

ويعرفها (David Tompson):"**جريمة يكون متطلبا لاقترافها أن يتوفر لدى فاعلها معرفة تقنية الحاسب".**[2]

والدكتور هلالي عبد الله أحمد يرى أنها:"**عمل أو امتناع يأتيه إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا".**

الفرع الثاني

التعاريف على ضوء الاتفاقيات الدولية

يعرف خبراء منظمة التعاون الاقتصادي والتنمية جريمة الكمبيوتر بأنها:" **كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها".**[3] ويتبنى هذا التعريف الفقيه الألماني (Ulrich Siehr) يعتمد هذا التعريف على معيارين هما: وصف السلوك، واتصال السلوك بالمعالجة الآلية للبيانات أو نقلها.

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص30.

[2] عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمن العربي،2002،ص4

[3] موقع منظمة التعاون الاقتصادي والتنمية، WWW.Oecd.Org

عرف جريمة الكمبيوتر خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية (OECD)[1]بأنها:"**كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية**".[2]

قدمت المادة الأولى من الاتفاقية الدولية للإجرام المعلوماتي تعريف للنظام المعلوماتي على النحو التالي:"***يقصد بمنظومة الكمبيوتر أي جهاز أو مجموعة من الأجهزة المتصلة ببعضها البعض أو ذات صلة بذلك ويقوم إحداهما أو أكثر من واحد منها تبعا للبرنامج بعمل معالجة آلية للبيانات ويقصد ببيانات الكمبيوتر أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل مناسب لعملية المعالجة داخل منظومة الكمبيوتر بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدي وظائفها***".

عرف المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاقبة المجرمين الجريمة المعلوماتية بأنها:"**أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية**".[3]

عرفت اتفاقية بودابست في المادة الأولى منها بعنوان تعريف خاص بأغراض هذه الاتفاقية منظومة معلوماتية ومعطيات معلوماتية:

أ/منظومة معلوماتية: "أي جهاز أو مجموعة من الأجهزة المتصلة يبعضها أو ذات صلة بذلك ويقوم أحدها أو أكثر من واحد منها تتبعا للبرنامج بعمل معالج آلية للمعطيات"

[1]Organisations Economique de commerce et développement

[2] موقع منظمة التعاون الاقتصادي والتنمية .www. Ocd. Org

[3] عقد هذا المؤتمر في فيينا في الفـــترة ما بين (10-17) افريل 2000.

ب/معطيات معلوماتية:"أية عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل معين جاهز لعملية المعالجة داخل منظومة معلوماتية بما في ذلك البرامج الماسة لجعل منظومة معلوماتية تطبق وظيفة".[1]

يذهب البعض إلى أنة عند وضع تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة اعتبارات مهمة منها:

1- أن يكون هذا التعريف مقبول ومفهوم على المستوى العالمي.

2- أن يراعى هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.

3- أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الاجرامى.

4- أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية.[2]

الفرع الثالث

موقف المشرع الجزائري.

تدارك المشرع الجزائري مؤخرا ولو نسبيا الفراغ القانوني في مجال الجرائم المعلوماتية وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون15/04المؤرخ في 2004.11.10 المتضمن تعديل قانون العقوبات[3]، ولكن المشرع تناول في النصوص المستحدثة الاعتداءات الماسة بالأنظمة المعلوماتية وأغفل الاعتداءات الماسة بمنتجات الإعلام الآلي وسنبين بصفة موجزة الأفعال التي جرمها المشرع الجزائري بموجب القانون السالف الذكر:

---

[1] الاتفاقية الدولية حول الإجرام السيبيري التي أبرمت بتاريخ 2001/11/08 من طرف المجلس الأوروبي وتم وضعها للتوقيع منذ تاريخ 2001/11/23.

[2] أمير فرج يوسف، الجرائم المعلوماتية، ص58.

[3] القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات (ج ر 71 بتاريخ 2004/11/10).

1-جريمة التوصل أو الدخول غير المصرح به: نصت عليه المادة 394 مكرر من قانون العقوبات بقولها "**يعاقب بالحبس و الغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو ترتب عن الأفعال المذكورة تخريب نظام اشتغال المنظومة** ."فقد أورد المشرع ظرفي تشديد لعقوبة الدخول غير المشروع وهما: في حالة ما إذا ترتب عن الدخول غير المشروع حذف أو تغيير المعطيات، أو تخريب نظام اشتغال المنظومة. وقد نص المشرع في المادة المذكورة على تجريم فعل الشروع في جريمة الدخول غير المصرح به وذلك بقوله" أو يحاول ذلك[1]."

2-جريمة التزوير المعلوماتي: نص عليها المشرع في نص المادة 394 مكرر 1 بقوله "**يعاقب بالحبس وبالغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها**[2]."

3-جريمة الاستيلاء على المعطيات: نصت عليها المادة 394 مكرر 2 بقولها" **كل من يقوم عمدا و بطريق الغش تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.**"

4-جريمة إتلاف وتدمير المعطيات: نص عليها المشرع الجزائري بالمادة 394 مكرر 1 من قانون العقوبات" **يعاقب بالحبس والغرامة كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي تتضمنها** ."وجريمة الإتلاف حسب نص المادة المذكورة تتمثل في إزالة معطيات نظام المعالجة الآلية عن طريق الفيروسات.

---

[1] أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري،الطبعة الأولى، دار هومة، ص99.

[2] تنص المادة 394مكرر2 من قانون العقوبات:"يعاقب بالحبس والغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

ـ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم."

5جريمة الاحتيال المعلوماتي: وهو ما نصت عليه المادة 394 مكرر 1/2 بقولها" **يعاقب بالحبس وبالغرامة كل من قام بطريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية "...** أي أن يهدف مرتكبها إلى جني فوائد مالية من جراء ذلك.

6-أنشطة الانترنت المجسدة لجرائم المحتوى الضار والتصرف غير القانوني: نصت مواد القسم السابع مكرر من قانون العقوبات وخاصة المادة 394 مكرر2/2 على تجريم أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق، وجميع الأفعال غير المشروعة، وقد نصت المواد على توقيع عقوبتي الحبس والغرامة إضافة إلى ما نصت عليه المادة 394 مكرر6[1] بتوقيع عقوبة تكميلية تتمثل في غلق المواقع(sites les)التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات[2].

أما الجزاءات المقررة بموجب الفصل السابع مكرر فتتمثل في العقوبات ***الأصلية*** وهي عقوبة الحبس والغرامة. وعقوبات ***تكميلية*** بموجب نص المادة 394 مكرر 6 والمتمثلة في: مصادرة الأجهزة والبرامج والوسائل المستخدمة وإغلاق المواقع (les sites) والمحل أو أماكن الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ومثال ذلك إغلاق مقهى الانترنت (cybercafé)الذي ترتكب فيه هذه الجرائم بشرط علم مالكه. وقد أورد المشرع ظروفا تشدد بها عقوبة الجريمة وهي: في حالة الدخول والبقاء غير المشروع إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة أو تخريب للنظام، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام. ونص أيضا بموجب المادة 394 مكرر5 على تجريم الاشتراك(سواء شخص طبيعي أو معنوي) في

[1] تنص المادة 394 من قانون العقوبات:"مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة 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"

[2] أمال قارة، المرجع السابق، ص 20.

مجموعة أو اتفاق بغرض الإعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية - بعقوبة الجريمة -وكان التحضير لهذه الجرائم مجسدا بفعل أو بعدة أفعال مادية. أي بمعنى آخر فإن المشرع استثنى من العقاب الأعمال التحضيرية للجرائم المعلوماتية المرتكبة من طرف شخص منفرد[1].

نصت المادة 394 مكرر4 [2] على توقيع العقوبة على الشخص المعنوي الذي يرتكب إحدى الجرائم الواردة في الفصل السابع مكرر بغرامة تعادل 05 مرات الحد الأقصى للغرامة المحددة للشخص الطبيعي. غير أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة. والشروع في الجريمة المعلوماتية يعاقب عليه بالعقوبة المقررة للجريمة ذاتها وهو ما نصت عليه المادة 394 مكرر7[3] من قانون العقوبات.

إلى جانب قانون العقوبات التي جاءت نصوصه المستحدثة مجرمة لبعض الاعتداءات على المعلوماتية فإن المشرع الجزائري وبموجب الأمر05/03 المؤرخ في 2003.07.19المتعلق بحقوق المؤلف والحقوق المجاورة قد عمد إلى توفير الحماية لبرامج الحاسب الآلي وإخضاعها لقوانين الملكية الفكرية وأقر عقوبة الحبس والغرامة على كل من يعتدي على هذه المصنفات.[4]

المطلب الثاني

خصائص ودوافع الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية،

[1] تنص المادة 394مكرر5من قانون العقوبات:"كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية يعاقب بالعقوبة المقررة للجريمة ذاتها."

[2] تنص المادة 394مكرر4من قانون العقوبات:"يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل 5مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

[3] تنص المادة 394مكرر7من قانون العقوبات:"يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

[4] أمال قارة، المرجع السابق،ص20.

وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي، وقد كان لظهور شبكة المعلومات وتطورها إلى الصورة التي أصبحت عليها الآن فيما يعرف بالانترنت أثره في إعطاء شكل جديد للجريمة المعلوماتية، ولعل أهم ما أضفته شبكة المعلومات على الجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود.

وسوف نحاول فيما يلي التطرق إلى بعض السمات الخاصة بالجريمة المعلوماتية والمجرم المعلوماتي ثم سنتناول بالدراسة الدوافع التي أدت به إلى ارتكاب هذه الجرائم.[1]

الفرع الأول

خصائص الجريمة المعلوماتية.

تتميز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية ببعض السمات والخصائص والتي نوجزها فيما يلي:

أولا:السمات الخاصة بالجريمة المعلوماتية

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية في عدة نواح،سواء كان هذا التمييز في السمات العامة لها أو كان في الباعث على تنفيذها أو في طريقة هذا التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة.

أ/ خصوصية الجريمة المعلوماتية: تتسم الجريمة المعلوماتية بصعوبة اكتشافها وإثباتها، ويرجع ذلك إلى عدة أسباب من بينها:

وسيلة تنفيذها التي تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد، بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجني

[1] قربوز حليمة، المرجع السابق،ص6.

عليهم من فقد ثقة عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة قد تقل عن الثانية الواحدة.

فعلى سبيل المثال أحصت وزارة الداخلية في فرنسا عام 1986 حوالي 1200 جريمة معلوماتية في حين كان هناك حوالي 53600 جريمة ضد الأشخاص و18900 جريمة تندرج تحت وصف جرائم الآداب و3 مليون جريمة ضد الأموال، وفي أحدث تقارير مركز شكاوى احتيال الانترنت الأمريكي أظهر التحليل الشامل للشكاوى التي قدمت للمركز خلال سنة 2004 قد بلغت 6348 شكوى من ضمنها 5273 حالة تتعلق باختراق الكمبيوتر عبر الانترنت و814 تتعلق بوسائل الدخول والاقتحام الأخرى كالدخول عبر الهاتف أو الدخول المباشر إلى النظام بشكل مادي مع الإشارة إلى أن هذه الحالات هي فقط التي تم الإبلاغ عنها ولا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي.[1]

وفي مقابل انخفاض نسبة جرائم المعلوماتية في مواجهة الجرائم التقليدية، ترتفع الخسارة الناجمة عن الجرائم المعلوماتية بصورة كبيرة بالمقارنة بغيرها من الجرائم، فعلى سبيل المثال كانت الخسارة الناجمة عن 8000 حالة سرقة بالإكراه في فرنسا عام 1986 حوالي 561 مليون فرنك الفرنسي، في حين يتضاعف هذا الرقم في حالة الجرائم المعلوماتية على الرغم من انخفاضها نسبة 8 مرات عن حالات السرقة بالإكراه.

وفي المقابل فانه، وعلى غرار الآراء التي تتجه إلى القول بأن الجريمة المعلوماتية لا يوجد شعور حقيقي بعدم الأمان في مواجهتها، أو أنه لا يوجد شعور عام بعدم أخلاقية هذه الأفعال، فإنه من الفقهاء من لا يتفقون مع هذه الآراء إذ أن الجريمة المعلوماتية لا تختلف عن غيرها من الجرائم من حيث اعتدائها على مصالح لها أهميتها لدى أفراد المجتمع، ومن ثم تستحق الحماية القانونية كون أن مساس هذه الأفعال بهذه المصالح هو الذي يبرر تجريمها.

[1] نائلة عادل محمد فريد قورة -جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية- منشورات الحاتي الحقوقية 2005، ص49.

ب/ دولية الجريمة المعلوماتية: يمكن القول أن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن اكتسابها طبيعة دولية، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد.

كما أن السرعة الهائلة التي يتم من خلالها تنفيذ الجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة المعلوماتية عن الجريمة التقليدية بصورة كبيرة.[1]

وقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة، فهل هي الدولة التي وقع بها النشاط الإجرامي، أم تلك التي توجد بها المعلومات محل الجريمة، أم تلك التي أضرت مصالحها نتيجة لهذا التلاعب، كما أثارت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة[2].

ولذلك فلقد بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضا تبادل المعلومات بين الدول المختلفة، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو "**إبرام الاتفاقيات الدولية**".

---

[1] نائلة عادل محمد فريد قورة المرجع السابق ص50.

[2] - المرجع نفسه، ص54.

تعد الاتفاقيات الخاصة بتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية، إلا أن الوصول إلى إبرام هذه الاتفاقيات يقتضي التنسيق بين قوانين الدول المختلفة لضمان تحقق **"مبدأ ازدواجية التجريم"** فيما يتعلق بجرائم المعلوماتية.

ونجد أن هذا المبدأ يقف عقبة رئيسية طالما أن كثيرا من القوانين لم يتم تعديلها بحيث تتلاءم مع هذه الجرائم. وإن كان المشرع قد خطى خطوة إلى الأمام في هذا المجال بصدور القانون 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات. والذي استحدث نصوصا خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد من المادة 394 مكرر إلى غاية المادة 394 مكرر 7 من القسم السابع مكرر الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

ونخلص مما سبق إلى أنه في سبيل مكافحة الجريمة المعلوماتية يجب أن تتحرك الدول المختلفة في محورين:

الأول: داخلي بحيث تتلاءم تشريعاتها الداخلية مع هذا النمط الجديد من الجرائم.

الثاني: دولي عن طريق عقد الاتفاقيات الدولية، حيث لا يستفيد مجرموا المعلوماتية عن عجز التشريعات الداخلية من ناحية، وغياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم من ناحية أخرى.

ثانيا/ السمات الخاصة بالمجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره من المجرمين، وقد اختلف الباحثون في تحديد هذه السمات، ويعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة

عامة، بالمجرم المعلوماتي بصفة خاصة. إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه.[1]

فالمجرم المعلوماتي من ناحية ينتمي في أكثر الحالات إلى وسط اجتماعي متميز كما أنه على درجة من العلم و المعرفة، وإن لم يكن من الضروري أن ينتمي إلى مهنة يرتكب من خلالها الفعل الإجرامي.[2].

ويتميز المجرم المعلوماتي كذلك بمجموعة من الخصائص التي تميزه بصفة عامة عن غيره من المجرمين و يرمز إليها الأستاذ Parker بكلمة S.K.R.A.M و هي تعني :

المهارة Skill

المعرفة Knowledge

الوسيلة Resources

السلطة Anthority

و أخيرا الباعث Motives.[1]

تعد المهارة: المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين. إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا

[1] حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2005_2006. ص9

[2] Suthreland (Eduin H) "White collar criminality " Gers (Gilbert) in white collar criminal The offender in business the professions atherton press 1968

[1] Parker (Donn B) Figding computer crime A neur Framework for protecting information 1998/P 114

المجال. بل إن الواقع العملي قد أثبت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما المعرفة: فتتلخص في التعرف على كافة الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أن المجرم المعلوماتي باستطاعته أن يكون تصورا كاملا لجريمته. كون المسرح الذي تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلي. فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذ جريمته.

أما الوسيلة: فيراد بها الإمكانيات التي يتزود بها الفاعل لإتمام جريمته ففيما يتعلق بالمجرم المعلوماتي فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسبات الآلية هي في أغلب الحالات تتميز نسبيا بالبساطة وبسهولة الحصول عليها.

أما السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها. وقد تتمثل هذه السلطة في الحق في استعمال الحاسب الآلي أو إجراء بعض التعاملات، وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

و أخيرا يأتي الباعث وراء ارتكاب الجريمة، الذي قد لا تختلف في كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية،[1]ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الانتقام من رب العمل أو أحد الزملاء، حيث يفرق مرتكبي هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية لأخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم، وبناء على ما تقدم يمكن أن نقسم مجرمي

[1]précédent p142 Parker (DonnB)ouvrage

المعلوماتية Cyber criminals إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية ويمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة وتتمثل هده الطوائف فيما يأتي:[1]

- تضم الطائفة الأولى: Pranksters الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث).
- أما الطائفة الثانية "Hackers" فهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.
- وتتضمن الطائفة الثالثة "Malicious Hackers" هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترقي فيروسات الحاسبات الآلية وموزعيها.
- أما الطائفة الرابعة "Personnel Problem Solvers" فهم الطائفة الأكثر شيوعا بين مجرمي المعلوماتية، فهم يقومون بارتكاب جرائم المعلوماتية التي تلحق بالمجني عليهم خسائر ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.
- وتتضمن الطائفة الخامسة "Career Criminals" مجرمي المعلوماتية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، بحيث ينطبق على أفعالهم وصف الجريمة المنظمة، أوعلى الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل، ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.[2]

[1] نائلة عادل محمد فريد قورة- المرجع السابق- ص 58

[2] Parker (DonnB) l'ouvrage precedent P144-146

- أما الطائفة السادسة "Extreme Advocates" فتدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات و أفكار اجتماعية أو سياسية أو دينية ويرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، ويركز نشاطهم بصفة عامة في استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه، وان اعتماد المؤسسة المختلفة داخل الدول على أنظمة الحاسبات الآلية في إنجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات.[1]
- وأخيرا تأتي الطائفة السابعة "The Criminally Negligent" والتي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية، ألا وهي الإهمال الذي يترتب عليه في مجال الحاسبات الآلية وفي أغلب الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح.

الفرع الثاني

دوافع الجريمة المعلوماتية

يقول الدكتور(ADAM GRAYCAR)مدير المعهد الأسترالي لعلم الإجرام، بأن الجريمة تحتاج إلى أربعة عناصر رئيسية لتشجيع المجرم على ارتكابها وهي:

أولا: دافع معين لارتكاب العمل.

ثانيا: هدف ضحية محاسبة.

ثالثا: الفرصة المواتية

رابعا: غياب عيون الأمن[2]

إذا فالدافع والقصد يشكل أحد الركائز في جميع الجرائم. وبالنسبة لجرائم الحاسب الآلي والإنترنت فهي لا تختلف في وضعها العام عن أسباب أي جريمة أخرى تقليدية.[1]

---

[1]الدكتور نائلة عادل محمد فريد قورة – المرجع السابق- ص63

[2]_ فايز بن عبد الله الشهري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنيت، الدليل الإلكتروني للقانون العربي arablawinf ،ص 9.

فثمة دوافع عديدة تحرك العينات لارتكاب أفعال الاعتداء المختلفة المنضوية تحت هذا المفهوم، ويمكن تلخيص هذه الدوافع فيما يلي:

أولا: الدوافع الشخصية.

أ/الدوافع المادية:

يعتبر السعي إلى تحقيق الكسب المالي في الحقيقة غاية الفاعل، وهو من بين أكثر الدوافع تحريكا للجناة لاقتراف الجرائم المعلوماتية. ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الحاسوب أو الاحتيال المرتبط بالحاسوب الذي يتيح تعزيز هذا الدافع بما تحققه من ثراء فاحش، والدليل على ذلك ما حدث في فرنسا سنة 1986 حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو 70000 فرنك فرنسي في حين أن جريمة الغش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 670.000 فرنك فرنسي أي ما يعادل أكثر من 38 مرة[2].

ومنذ بداية الظاهرة فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر وفيما بعد احتيال الإنترنت هو تحقيق الكسب المالي، ففي دراسة الفقيه Parker الصادرة في إحدى مجلات المتخصصة بخصوص موضوع الأمن المعلوماتي تبين أن:

- 34% من جرائم الغش المعلوماتي من أجل اختلاس الأموال.
- 23% من أجل سرقة المعلومات.[3]
- 19% من أجل الإتلاف.
- 15% من أجل سرقة وقت الحاسوب لأغراض شخصية.

وإذا انتقلنا للدراسات الحديثة، فسنجد أن هذا الدافع يسود على غيره ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية، وفي مقدمة هذه الدراسات

---

[1]_ فايز بن عبد الله الشهري، نفس المرجع، ص 10.

[2]Rose philippe la criminalité informatique que sais je 1er édition PU 1988 P 490

[3]_ G.Delmare, sécurité informatique Ressource informatique N° 1 juill

المسحية والإحصائية الدراسات والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية.

وهناك فئة من مرتكبي الجرائم المعلوماتية يرجع ارتكابهم لها إلى الديون الناتجة من المشاكل العائلية والخسائر الضخمة من ألعاب القمار أو إدمان المخدرات، فقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه الحالات، فالغاية تبرر الوسيلة.

ب/ الدوافع الذهنية أو النمطية:

الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنيت غالبا هي صورة البطل والذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب محاكمته، فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة، فيحاولون إيجاد الوسيلة إلى تحطيمها، أو التفوق عليها.

ثانيا: الدوافع الخارجية

أ/ دافع الانتقام و إلحاق الضرر برب العمل

قد يكون الانتقام مؤثرا في ارتكاب تلك الجرائم، ومثال ذلك قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشآت بحيث بعد رحيله من المنشأة بعدة أشهر يتم تدمير البيانات الخاصة بحسابات و ديون المنشأة.[1]

ولقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفردة في حالات معنية، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح، لكنها في حالات كثيرة، مثلت قوة محركة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها الانتقام من المنشأة أو رب العمل.

[1]comment se protéger contre le crime informatique. temps réels P264-1984

وربما تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيسي والغالب للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك لارتكاب الجريمة.[1]

ب/ الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية.

يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجادها وغالبا ما يجدون الوسيلة التي تحيطها، ويتزايد شيوع هذا الدافع لدى فئة صغار السن من مرتكبي الجرائم المعلوماتية الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات لإظهار تفوقهم على الوسائل التقنية.

إن هذا الدافع هو أكثر الدوافع التي يجري استغلالها قبل المنظمات الإجرامية (مجموعات الجريمة المنظمة) لأجل استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة.هذا وإن كان الفعل الواحد قد يعكس دوافع متعددة وخاصة، فمحرك أنشطة الإرهاب الالكتروني وحروب المعلومات دوافعه سياسية وإيديولوجية، في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، وقد تتداخل وتشترك هذه الدوافع في الفعل الواحد فتتمازج دون إمكانية التفرقة بينها.[2]

[1] حاجب هيام، المرجع السابق، ص14.

[2] حاجب هيام، المرجع السابق، ص 15.

المبحث الثاني

أركان الجريمة المعلوماتية

إن الجريمة المعلوماتية ليست واحدة، إنما تتخذ عدة أشكال مما يقتضي دراسة أركانها بالتفصيل ، وهذا من خلال المطلبين التاليين:

الركن المفترض (نظام المعالجة الآلية للمعطيات) في المطلب الأول.

الأركان الأساسية في المطلب الثاني.

المطلب الأول

الركن المفترض

يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان جريمة من جرائم الاعتداء على هذا النظام.

ويؤدي توافر هذا الشرط إلى الانتقال للمرحلة التالية، إذ أن هذا الشرط يعتبر عنصرا لازما، ولذلك يكون من الضروري تعريف نظام المعالجة الآلية للمعطيات ومدى خضوع هذا النظام لحماية فنية.

الفرع الأول

تعريف نظام المعالجة الآلية للمعطيات

هو تعبير فنِّي تقني متطوِّر، يخضع للتطوُّرات السَّريعة والمتلاحقة في مجال الإعلام الآلي، ولذلك لم يعرِّف المشرِّع الجزائري على غرار المشرِّع الفرنسي نظام المعالجة الآلية للمعطيات، فأوكل بذلك مهمّة تعريفه لكل من الفقه و القضاء.

حيث قدَّمت المادة الأولى من الاتّفاقية الدولية للإجرام المعلوماتي تعريفا للنّظام المعلوماتي على النّحو التالي:[1]

[1] أمال قارة المرجع السابق، ص102.

"يقصد بمنظومة الكمبيوتر أيُّ جهاز أو مجموعة من الأجهزة المتّصلة ببعضها البعض أو ذات صلة بذلك، ويقوم إحداهما أو أكثر من واحد منها، تبعا للبرنامج بعمل معالجة آلية للبيانات". ويقصد بـ "بيانات الكمبيوتر" أيَّة عملية عرض للوقائع، أوالمعلومات أو المفاهيم في شكل مناسب لعمليّة المعالجة داخل منظومة الكمبيوتر، بما في ذلك البرنامج المناسب لجعل منظومة الكمبيوتر تؤدِّي وظائفها".

أماّ الفقه الفرنسي، فقد عرَّفهُ من خلال الأعمال التّحضيرية للمادة 323-1 من قانون العقوبات الفرنسي، الذي تبنّى التّعريف الوارد في القانون الخاص بالمعلوماتية وحماية الحرّيات لسنة 1978، بأنَّه **"كلُّ مركّب من وحدة أو مجموعة وحدات للمعالجة، والتي تتكوَّن كل منها من الذّاكرة و البرامج والمعطيات وأجهزة الإدخال والإخراج، وأجهزة الرَّبط التي تربط بين العناصر المختلفة للنظام، كالشّاشة ولوحة المفاتيح والطّابعة والبطاقات المغناطيسية التي تشكِّل وسيلة للدخول، والتي تربط بينها مجموعة من العلاقات التي عن طريقها تتحقّق نتيجة معيّنة، وهي معالجة المعطيات، على أن يكون هذا المركَّب خاضع لنظام الحماية الفنية".**[1]

وهذه العناصر المادية والمعنوية التي يتكوّن منها المركَّب، واردة على سبيل المثال لا الحصر، فيمكن إضافة عناصر جديدة أو حذف بعضها حسب ما يفرزه التطوُّر التِّقني في هذا المجال. فإذا تمَّ الاعتداء على أحد هذه العناصر بمعزل عن النّظام، فلا تقوم الجريمة، فلا بدّ من الاتّصال بينها.

ويكون نظام المعالجة الآلية للمعطيات في طور التّشغيل عند إرسال إشارة كهربائية نحو وحدة المعالجة المركزية، والتي تقوم بدورها بإرسال البرنامج المسؤول عن تشغيل ذاكرة القراءة، هذه الأخيرة تقوم بالبحث عن المعطيات التي تسمح بتشغيل النِّظام المسؤول عن البحث، ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة التي تقوم بمتابعة المراحل اللاّحقة .[2]

[1] نائلة عادل، المرجع السابق، ص331.

[2] المرجع نفسه، ص331.

الفرع الثاني

الحماية الفنّية لأنظمة المعالجة الآلية للمعطيات

تكفل بعض القواعد الأمنيّة الحماية لنظم المعالجة الآلية للمعطيات، كوضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من الأجهزة المختلفة، والتي يمكن عن طريقها معرفة محتوى المعلومات التي يتمُّ نقلها، ويتأتّى ذلك عن طريق حماية الكابلات والوصلات الكهربائية لارتباطها بالأجهزة، ومن بين هذه القواعد، أُسلوب يعتمد على توزيع العمليّات التي يقوم بها نظام المعالجة الآلية للمعطيات ونقلها إلى نظام احتياطي (مركز للمساعدة) عند الضّرورة، ويلجــأ إلى هذا الأســلوب عادة البنــوك وشركات التّــأمين، ويظلّ هــذا الموقع سرًّا ويخضع لدرجة عالية من الحماية، ومن الأساليب المستعمــلة كذلك، الاعتماد على الاختبــارات الفيــزيولوجيــة للدخــول إلى النِّظام عن طريــق التحــقّق من شخصــيّة القائــم بعمليــة الدخول عن طريق بصمة الأصبع أو نبرة الصّوت أو شكل الأذن أو شبكيّة العين .[1]

لكن يبقى نظام التّشفير لحماية المعلومات هو الأسلوب الواسع الانتشار، خاصّة البيانات المتناقلة عبر الشّبكات، كشبكات الإنترنت، لما تنطوي عليه من سريّة البيانات الشخصية كالرّسائل الإلكترونية وكذا البيانات الخاصّة بالأعمال التجارية الرّقمية.[2]

ويقوم نظام التّشفير على تحويل المعلومات والبيانات إلى شكل رمزي غير مفهوم بدون مفتــاح لحلِّ رموزه، يعرفــه عادةً مرسل المعلومات والمرسل إليه، وفي داخل جهاز الكمبيوتر توجد أجهزة مهمّتها التّحقُّق من شخصيّة القائم بعملية الدخول عن طريق الشّفرة.

وقد ثار التّساؤل حول ضرورة وجود أو عدم وجود حماية للنّظام كشرط للتمتّع بالحماية الجنائية ؟

---

[1] نائلة عادل، المرجع السابق، ص353.

[2] أمال قارة، المرجع السابق، ص 103.

فبالرّجـــوع إلى نص المادة 394 مكرر[3] من قانون العقوبـــات، لا نجد إشـــارة إلى ضرورة خضوع النِّظام للحماية الفنية حتى يتمتع بالحماية الجنـــائية، وكذلك الشّأن بالنّسبة للمـــادة 323-1 من قانون العقوبات الفرنسي، و يظهر من خلال الأعمال التّحضيرية لقانون 1988، المتعلِّق بالمعلوماتية والمقتبسة منه المادة 323-1 ، أنه كان من المقترح ضرورة شمول النّص بهذا الشرط، ولكن اشتراط وجـــود حمـــاية أمنيّة في نظام المعالجة الآليـــة للمعطيـــات لم يتم الاتّفاق عليه في المناقشات الأخيرة في البرلمـــان الفرنسي ، ولذلك جاء النّص خالياً من هذا الشَّرط، ووجد أن هذا الشّرط قد يؤدِّي إلى الحدِّ من الحماية الجنائية للنُّظم غير المشمولة بتجهيزات أمنية داخل النِّظام.

ولذلك اكتفى المشرِّع الفرنسي في النَّص النِّهائي بأن يكون التوصُّل قد تمّ "بـــطريق الغش"، وهذا التَّعبير يترك تفسيره لقاضي الموضوع.[1]

وهذا ما فتح أبواب النِّقاش حول هذه النُّقطة من خلال ظهور رأيين مختلفين:

الرأي الأول: يقول بعدم جدارة الأنظمة التي لا تحميها نظم أمنية بالحماية الجنائية، كون أنّه من غير المعقول حماية معلومات هامة تركها المسؤولون عنها دون أيِّ إجراءاتٍ تكفل لها الحماية.

ويقيس أنصار هذا الرأي جريمة الدخول غير المشروع في أنظمة المعالجة الآلية للمعطيات على جريمة انتهاك حرمة المنزل، حيث لا تقوم الجريمة لمجرد أنّ الدخول إلى المسكن قد تمّ بغير رضاء صاحبه، كترك مسكنه دون حماية بسبب عدم وجود أقفال أو أبواب أو نوافذ، فيجب أن يكون الدخول مصحوبـــاً باستعمـــال وسائل تدلّ على عدم رضا صاحب المســـكن.

ويستند أنصار هذا الرأي إلى عدّة أسباب تنصبُّ جميعها في اتجاه واحد هو ضرورة أن يكون هناك نظم أمنيَّة يتم اختراقها لامتداد الحماية الجزائية للمعلومات، وأول

---

[3] تنص المادة394مكرر من قانون العقوبات:"يعاقب بالحبس والغرامة كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

[1] صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،2003 ، ص117.

هذه الأسباب يتعلّق بالمادة 28 من القانون 78-17 لسنة 1978 الخاص بالمعلوماتية وحماية الحريات الفرنسي، حيث تتطلّب أن تكون الأنظمة مشمولة بتدابير أمنيّة لحمايتها، والسبب الثاني يكمن في إقامة الدّليل على قيام الركن المادي للجريمة وكذا التّحقُّق من توافر القصد الجنائي لدى مرتكبها، لأنّ اختـــراق الأنظـــمة الأمنيـــّة من طرف الفاعل يترك أثراً، ويؤكِّد طريق الغش والاحتيال الذي سلكه.

الرأي الثاني: فهو يذهب إلى أنَّه ينبغي حماية أنظمة المعالجة الآلية للمعطيات جزائيا بغض النّظر إن كانت تتمتّع بحماية النّظم الأمنية من عدمه، ويقيس أنصار هذا الاتِّجاه جريمة الدخول غير المشروع على جريمة السرقة، حيث أن تمتُّع المال المسروق بحمـــاية صـــاحبه أو عدم تمتُّعه بهذه الحماية لا يؤثّر في قيام جريمة السرقة، بغضِّ النّظر عن مقدار الصّعوبة التي واجهت الجاني في تنفيذها، كما أن تطلُّب مثل هذا الشّرط يضيِّق من تطبيق الحماية الجزائية، ويتجـــاهل الحالات التي يتمُّ فيها الدخـــول إلى النـــّظام نتيـــجة خـــطأٍ قام به المبرمجـــون، أو المسؤولون عن أمن النِّظام.[1]

هذا الرّأي هو الأقرب إلى الصّواب استنادا إلى المبادئ العـــامّة المستقرّة في القانون الجنائي كحَرفيَّة النّص، وعدم جواز تقييد النّص المطلق أو تخصيص النّص العـــــام، إلاّ إذا وجد نص يجيـــز ذلك، ولا يوجـــد في حالتنا نص خاص يقـــيّد إطـــلاق النّص أو يخصّص عمومه، وبالتّالي يجب التزام حرفيّة النّص في التّفسير، فعدم ذكر المشرِّع لشرط الحماية الفنّية يعني أنّ المشرّع أراد استبعاده.[2]

وأكّدت محكمة استئناف باريس في حكم صادر لها في 1994/04/05 ،على أنّه من غير الضّروري لقيام جريمة الدخول غير المصرح به أن يكون فعل الدخول قد تمّ بمخالفة التدابير الأمنيّة، وأنه يكفي أن يكون هذا الدخول قد تمّ ضدَّ إرادة المسؤول عن النِّظام.

[1] نائلة عادل، المرجع السابق، ص355.

[2] أمال قارة، المرجع السابق، ص 105.

المطلب الثاني

الأركان الأساسية للجريمة المعلوماتية

متى ثبت توفر الشرط الأولي لقيام الجريمة المعلوماتية ألا وهو نظام المعالجة الآلية للمعطيات أمكن الانتقال إلى المرحلة التالية وهي البحث في توافر أركان أية جريمة من جرائم المعلوماتية.

الفرع الأول

الركن المادي

يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات وهناك ثلاثة أشكال للاعتداء نذكرها فيما يأتي:

أولا/ الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات

نصت عليه المادة الثانية من الاتفاقية الدولية للإجرام المعلوماتي بالإضافة للمادة 394 مكرر من قانون العقوبات بقولها: " **يعاقب بالحبس من ثلاثة أشهر إلى سنة بغرامة من 50.000دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج .**"

وعليه فإن هذا الشكل من الاعتداء على نظام المعالجة الآلية للمعطيات يتكون من صورة بسيطة للجريمة وأخرى مشددة.

فأما الصورة البسيطة تقوم بمجرد الدخول أو البقاء غير المشروع.

ويقصد **بفعل الدخول** ظاهرة 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 وبالتالي لا نقصد بالدخول الدخول بمفهومه المادي[1].

وتجدر الملاحظة أن المشرع لم يحدد وسيلة الدخول أو الطريقة التي يتم الدخول بها إلى النظام، ومنه تقع الجريمة بأية وسيلة أو طريقة تمت بها الدخول، فيستوي أن يتم الدخول مباشرة أو عن طريق غير مباشر.[1]

كما أن هذه الجريمة تقع من كل إنسان أيا كانت صفته، وكفاءته المهنية والفنية، فهذه الجريمة ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة.

في حين أنه يقصد **بفعل البقاء**[2]التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.

وتجدر الإشارة إلى أنه قد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول إلى النظام، وقد يجتمعان، ويكون البقاء معاقبا عليه وحده حين يكون الدخول إلى النظام مشروعا.

وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا، في الحالة التي لا يكون فيها للجاني الحق في الدخول إلى النظام، ويدخل إليه رغم ذلك ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق الاجتماع المادي للجريمتين الدخول والبقاء غير المشروعين. [3]

إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، فإنها تحقق أيضا، وبصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها.

---

[1]علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، مصر، 1999، ص120.

[1] علي عبد القادر القهوجي، نفس المرجع، ص121.

[2] علي عبد القادر القهوجي، نفس المرجع، ص133.

[3] أمال قارة، المرجع السابق، ص110.

أما الصورة المشددة تتحقق بتوافر الظرف المشدد المتمثل في حصول نتيجة الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

وقد نصت **المادة 394 مكرر 2+3** من قانون العقوبات على أن " **تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 150000 دج.**"

وعليه نستنتج من خلال ذلك أن هناك ظرفين تشدد بهما عقوبة جريمة الدخول والبقاء داخل النظام، وتربط بين هذين الظرفين علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع والنتيجة الضارة وإن لم تكن مقصودة.

ومنه فظرف التشديد يعتبر ظرف مادي يكفي أن توجد بينه وبين الجريمة الأساسية المتمثلة في الدخول أو البقاء غير المشروع علاقة سببية للقول بتوافره، إلا إذا أثبت الجاني انتفاء تلك العلاقة ويثبت أن تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث مفاجئ.[1]

ثانيا/ الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات

نصت على هذا الشكل من الاعتداء المادتين الخامسة والثامنة من الاتفاقية الدولية للإجرام المعلوماتي، في حين أن المشرع الجزائري لم يورد نصا خاصا بالاعتداء العمدي على سير النظام واكتفى بالنص على الاعتداء على المعطيات الموجودة بداخل النظام، ويمكن رد ذلك لكون أن المشرع الجزائري قد اعتبر من خلال الفقرة ج من المادة الثانية [2]من

[1] أمال قارة، المرجع السابق، ص114.

[2] تنص الفقرة ج من المادة الثانية من القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 07 لـــ 2009.على ما يلي:"منظومة معلوماتية: أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها"

القانون 04/09 على أن برامج سير نظام المعالجة الآلية للمعطيات تدخل ضمن المعطيات المعلوماتية.

وقد وضع الفقه معيارا للتفرقة بين الاعتداء على المعطيات والاعتداء على النظام على أساس ما إذا كان الاعتداء وسيلة أم غاية، فإذا كان الاعتداء مجرد **وسيلة** فان الفعل يشكل جريمة الاعتداء العمدي على النظام، أما إذا كان الاعتداء **غاية** فان الفعل يشكل جريمة الاعتداء العمدي على المعطيات.

وتشمل صورة الاعتداء العمدي على سير النظام فعلين يتمثلان في الآتي:

يتمثل **الأول** منها في فعل **التعطيل (العرقلة)** والذي يفترض وجود عمل إيجابي، مع العلم أن المشرع لم يشترط أن يتم التعطيل بوسيلة معينة فيستوي أن يتم التعطيل بوسيلة مادية ككسر الأجهزة المادية للنظام أو تحطيم أسطوانة أو عن طريق وسيلة معنوية تتم بموجب الاعتداء على الكيانات المنطقية للنظام كالبرامج والمعطيات وذلك بإتباع إحدى التقنيات المستعملة في هذا المجال مثل إدخال برنامج فيروسي، استخدام قنابل منطقية مؤقتة، جعل النظام يتباطأ في أدائه لوظائفه كما يستوي أن يقترن التعطيل بالعنف أم لا.

أما الفعل **الثاني** يتمثل في **الإفساد** الذي يتم بكل فعل إلى تعطيل نظام المعالجة الآلية للمعطيات يؤدي إلى جعله غير صالح للاستعمال السليم وذلك من شأنه أن يعطي نتائج غير تلك التي كان من الواجب الحصول عليها[1].

ثالثا_ الاعتداءات العمدية على المعطيات

نصت عليها المواد **03،04،08**، من الاتفاقية الدولية للإجرام المعلوماتي كما نص عليها المشرع الجزائري في المادة **394 مكرر1** و**394 مكرر2** من قانون العقوبات فجرم في المادة الأولى الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي، وجرم في المادة الثانية المساس العمدي بالمعطيات الموجودة خارج النظام، ويظهر هذا فيما يلي:

أ_ جرائم الاعتداءات العمدية على المعطيات الموجودة داخل النظام المعلوماتي

باستقراء المادة **394 مكرر 1**[2] نجد أن لهذه الجريمة صورتين تتمثل الأولى في الاعتداءات العمدية على المعطيات الموجودة داخل النظام أما الصورة الثانية تتمثل في

[1] علي عبد القادر القهوجي، المرجع السابق، ص143.

المساس العمدي بالمعطيات خارج النظام نجد **الاعتداءات العمدية على المعطيات الموجودة داخل النظام** تتجسد في إحدى الأفعال الثلاثة: **الإدخال (L'intrusion)، المحو(L'effacement)، التعديل(modification La)**، ويقصد بها:

الإدخالl'intrusion: يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل ويتحقق هذا الفعل في الفرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة التي يسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه وكذلك الحامل الشرعي لبطاقة الائتمان والتي يسدد عن طريقها مبلغا (التاجر أو شخص يتعامل معه) أكثر من المبلغ المحدد له.

وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب(فيروس-حصان طروادة - قنبلة معلوماتية زمنية)يضيف معطيات جديدة .

المحوl'effacement :يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[1].

التعديل modification: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة تتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أم بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة gomme d'effacementأو برامج الفيروسات بصفة عامة، وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل

---

[2] تنص المادة394مكرر1من قانون العقوبات" أنه يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات، و بغرامة من 500.000 دج إلى 2.000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

[1] علي عبد القادر القهوجي، المرجع السابق، ص144.

الحصر فلا يقع تحت طائلة التجريم أي فعل آخر غيرها حتى ولو تضمن اعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات فلا يخضع لتلك الجريمة فعل نسخ المعطيات أو فعل نقلها أو فعل التنسيق أو التقريب فيما بينهما، لكن كل تلك الأفعال لا تنطوي لا على إدخال ولا على تعديل بالمعنى السابق.

مع الملاحظة أن المشرع لم يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يقوم الركن المادي.

كما أن أفعال الإدخال والمحو والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة أو محو أو تعديل معطيات موجودة من قبل[1].

ب_ أما صورة **المساس العمدي بالمعطيات خارج النظام** نص عليها المشرع الجزائري بموجب أحكام المادة **394 مكرر2 من قانون العقوبات[2]**، وكرس بموجبها المشرع الحماية الجزائية للمعطيات في حد ذاتها لأنه لم يشترط أن تكون المعلومات داخل نظام معالجة آلية للمعطيات أو أن يكون قد تم معالجتها آليا.

إذ نصت الفقرة الأولى من المادة **394 مكرر 2** أن محل الجريمة يتمثل في المعطيات سواء كانت مخزنة في أشرطة أو أقراص أو معالجة آليا أو مرسلة عن طريق منظومة معلوماتية ، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

في حين أن الفقرة الثانية من المادة **394 مكرر 2** جرمت أفعال الحيازة، الإفشاء، النشر، الاستعمال أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات فقد يكون الهدف من ذلك المنافسة غير المشروعة، الجوسسة، الإرهاب، أو التحريض على الفسق ...الخ

---

[1] أمال قارة، المرجع السابق، ص120.

[2] تنص المادة 394مكرر2من بقانون العقوبات:" يعاقب بالحبس وبغرامة كل من يقوم عمدا وعن طريق الغش بما يأتي:

-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات محزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

ـــــــحيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

الفرع الثاني

الركن المعنوي

إن الرّكن المعنوي في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات تتّخذ صورة القصد الجنائي.

أولا/ الركن المعنوي بالنسبة للدخول والبقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات.

إنّ الرّكن المعنوي لجريمة الدخول والبقاء غير المشروعين، يتّخذ صورة القصد الجنـــائي من علم و إرادة باعتبارها من الجرائم العمدية، وقد عبّر نص المادة 394 مكرر عن القصد الجنائي العـــام بتطلُّبـــه أن يكـــون الدخول أو البـــقاء " عن طريق الغش " ، فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخـــوله أو بقاءه في نظام المعالجة الآلية للمعطيات غير مشروع، وهو نفس ما عبّر عنه المشـــرِّع الفرنسي في نص المـــادة 323-1بعبـــارة " frauduleusement ".

يتطلّب القصد العام أن يحيط علـــم الجـــاني بكل واقـــعة ذات أهمية قانونيـــة في تكوين الجريمة، وبناء أركانها، واستكمال عناصرها، وخاصّة الركن المادي منها، وأوّل هذه العناصر هو موضوع الحق المعتدى عليه، فيتعيَّن توافر علم الجاني بأنّ فعـــله ينصبُّ على نظام المعالجة الآليـــة للمعطيـــات بما يتضـــمّنه من معلومات وبرامج، باعتباره محل الحق الذي يحميه المشرّع، فإذا اعتقد الفاعل بناءً على أسباب معقولة بأنـــّه يـــقوم على سبيل المثال بإجراء بعض العمليّات الحسابيّة عن طريق الحاسب الآلي، دون

أن يتّجه علمه إلى أنه يقوم بالدخول أو البــقاء في نظـــام المـــعالجة الآلية للمعطيات، فإنّ قصد الدخـــول أو البقاء لا يتوفّر فيه.[1]

كذلك يتعيّن أن يعلم بخطورة الفعل الذي يقوم به، فإذا كان غير ذلك ينتفي القصد الجـــنائي. ويتطلّب القصد الجنائي أيضًا أن يتوقّـــع الجاني النّتيجة الإجرامية التي ستترتّب عن القيام بفعله، فتوقّـــع النتيجة هو أساس النّفي الذي تقوم عليه إرادتـــها، فحيث لا يكـــون التّوقّـــع لا نتصوّر الإرادة، والنّتيجة التي يجب أن يتّجه إليها توقّع الفاعل هي النّتيجة التي يحدِّدها القانـــون، وهي الدخول والبقاء غير المشروع لنظام المعالجة الآلية للمعطيات .

ولا يشترط أن يتوقّع الضّرر الذي سوف يلحق النِّظام أو صاحبـــه من جرَّاء هـــذا الدخول[1]، فإذا توقّع الفاعل أنّه بصدد الدخول إلى نظام معيّن ، ثم ترتّب على فعله الدخول إلى نظام آخر، فإنّ القصد الجنائي يظلُّ متوافراً لديه .

وهناك وقائع يسأل فيها الجاني عن الجريمة دون أن يتطلّب القانون علمه بها، فحين يقرّر القانـــون لبعض الجرائم عقاباً معيناً إذا أحدث الفعل نتيجة ذات جـــسامة معنيّة، وإذا ازدادت جـــسامة هذه النّتيجـــة فأفضت إلى نتيـــجة أشدّ جسامة، شدّد الـــقانون العـــقاب، ويتطلّب المشرع انصراف القصد الجنـــائي إلى النّتيجـــة الأقـــل جـــسامة، ولكنّه لا يتطلّب انصرافه إلى النّتيجة الأشدُّ جسامة، بحيث يسأل الجاني عنـــها بالرّغم من عدم توقُّعها لها[2].

وهذا ما ينطبق على الفقرة الثّانية والثّالثة من المادة 394 مكرر من قانون العقوبات، حيث يعاقب الجاني على النّتيجة الأشد بمجرد ترتُّبها عن الدخول أو البقاء غير المشروع الذي قصده.

---

[1] نائلـــة عـــادل محمـــد فريـــــد قـــورة المرجـــع الســـــابق ص365.

[1] نائلـــة عـــادل محمـــد فريـــــد قـــورة المرجـــع الســـــابق ص366

[2] نفس المرجـــع، ص 367

ويجب أن يعلم مرتكب جريمة الدخول أو البقاء غير المشروعين داخل نظم المعالجة الآلية للمعطيات، أن دخوله إلى هذا النِّظام غير مشروع أو غير مصرّح به، فلا يتوافر القصد الجنائي إذا وقع الجاني في خطأ ،كأن يجهل وجود حظر للدخول أو البقاء، أو كان يعتقد خطأً أنّه مسموح له بالدخول أو البقاء .

أما بالنِّسبة لإرادة الجاني فيجب أن تتّجه إلى الدخول أو البقاء غير المشروعين داخل النّظام، أي أن تتّجه إرادته لتحقيق هذه النّتيجة ، ولا عبرة بعد ذلك للباعث أو الغاية من وراء هذا الدخول أو البقاء سواء كان هذا الباعث هو الفضول، أو إثبات القدرة على المهارة والانتصار على النِّظام، حتى وإن كانت الغاية نبيلة كمن يدخل إلى النِّظام غير المصرَّح له بالدخول رغبةً في الكشف عن أوجه القصور التي تعتري النِّظام الذي تمكّن من الدخول إليه، وذلك لتجنُّب هذا القصور مستقبلاً [1].

ثانيا/:الركن المعنوي للاعتداءات على سير نظام المعالجة الآلية للمعطيات والاعتداءات على المعطيات خارج وداخل النظام

إنّ الاعتداءات على سير نظام المعالجة الآلية للمعطيات بصورتيها التّعطيل أو العرقلة، وإفساد النّظام، لا تكون إلاّ عمدية هذا ما يميِّزها عن الاعتداء غير العمدي لسير النِّظام الذي يشكِّل ظرفاً مشدّداً لجريمة الدخول والبقاء غير المشروعين داخل النِّظام[2].

وهذه الاعتداءات تتطلّب القصد الجنائي العام من علم وإرادة ، شأنها شأن الاعتداءات العمدية على المعطيات، فيجب أن يعلم الفاعل بأنّه يقوم بإحدى هذه الأعمال التي أوردها النّص القانوني، والتي من شأنها إتلاف المعلومات، فيعلم بأنه يقوم بفعل الإدخال أو المحو أو التّعديل، ويعلم خطورة النّشاط الإجرامي الذي يقوم به وما يترتّب عنه من عقاب.

[1] نائلة عادل محمد فريد قورة ، المرجع السابق ص 368

[2] آمال قارة، المرجع السابق ص 124.

كما يجب أن تتّجه إرادة الفاعل إلى فعل الإدخال أو المحو أو التّعديل، فلا يسأل من قام بذلك خطأً أو عن غير قصد، بل يسأل طبقاً للمادة 394 مكرر 2/**3** التي تتناول الصّورة المشدّدة لجريمة الدخول أو البقاء غير المشروعين في نظام المعالجة الآلية للمعطيات، كونها تعاقب الفاعـــل عن الحذف والتّغيير المترتِّب عن الدخول أو البقاء غير المشروعين حتى وإن كان خطأً، كون أن نص المادة 394 مكرر 1من قانون العقوبـــــات اشترط أن ترتكب هذه الأفـــــعال " بطريق الغش ".

وهي العبارة المستعملة كذلك في نص المادة 323-3 من قانـــــون العقوبـــــات الفرنســـي "frauduleusement "، أي أن يعلم أنّه ليس له الحق في القـــيام بذلك، وأنّه يعتـــدي على صاحب الحق في السّيطرة على تلك المعطيات دون موافقته. ولا يتطلّب نص المادة 394 مكرر 1 قصداً جنائياً خاصاً، إذ لا يوجد فيه ما يشير إلى ذلك، عكس بعض التّشريعات المقارنة التي اشترطت قصدًا خاصًا إلى جانب القصد العام، يتمثّـــل في اتِّجـــاه نيّـــة المتّهم إلى الإضرار بالغير أو إلى تحقـــيق ربح غير مشروع له أو للغير، وهو ما كان عليه النّص الفـــرنسي القـــديم قبل تعديله، ويبرز ذلك في عـــبارة "ارتكاب الفـــعل دون مراعاة حقـــوق الآخرين". وقد انتُقدت هذه المادة قبل تعديلها بشدّة لتطلُّبها القصد الجنائي الخاص، كون أن اشتراط هذا القصد الخاص سوف يؤدِّي إلى اللاّعقاب في الحـــالات التي لا تتّجه فيها نيّة الفـــاعل إلى تحقيق ربح، على الرّغم من أهميّة المعلومات التي قد يتمُّ إتلافها، مثل إتلاف معلومات علمية[1].

و هو ما دعا المشرّع الفرنسي إلى استبعاد القصد الخاص من هذه الاعتداءات العمديّة، حيث اقتبس المشرِّع الجزائري نص الـــمادة 394 مكرر1 من نص المادة 323-3 المعدّلة من قانون العقوبات الفرنسي.

أما بالنسبة للاعتداءات العمديّة الماسة بالمعطيات الموجودة خارج النظام، فيجب لقيام الركن المعنوي أن يتوافر القصد الجنائي العام، وهو ما عبّرت عنه المادة 294 مكرر2 بعبارة " كل من يقوم عمداً وعن طريق الغش ".

[1] نائلـــــة عـــــادل محمـــــد فريـــد قـــورة ، المرجـــع السابـــق ص368.

وبالتّالي يجب توافر العلم والإرادة لدى الجاني لقيام الركن المعنوي، فيجب أن يكون عالما أن المعطيات المخزّنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى الاعتداءات الماسة بأنظمة المعالجة الآلية للمعـــطيات ، وذلك بتصميـــمه أو بحثه أو تجميعه أو توفيره أو نشره أو الاتّجار في هذه المعطيات، أي علمه بأن هذه المعطيات يمكن أن تكون وسيلة لارتكاب الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

ويجب أن يعلم الجاني كـــذلـــك، أن إتيـــانه أحـــد الأفـــعال الســـابقة ينصبُّ على معـــطيـــات مخـــزّنة أو معالجة أو مرسلة عن طريق منظومة معلومـــاتية، وكذلك أن يعلم بخطورة الفعل الذي يقوم به، وأن يتوقّـــع النّتـــيجة المترتِّـــبة عن القيام بأحد الأفعال السَّابقة.

الفصل الثاني

الفصل الثاني

مكافحة الجريمة المعلوماتية في ظل القانون الجزائري.

لوضع حماية جزائية للجريمة لمعلوماتية استجابت عدة دول لها، فمثلا الولايات المتحدة الأمريكية التي أصدرت قانون فيدرالي سنة 1984 متعلق بالاحتيال وإساءة استخدام الكمبيوتر، كما أصدرت فرنسا قانون رقم 19/88 الموافق لـــ1988/01/05بشان الغش المعلوماتي، والذي ادمج في قانون العقوبات الفرنسي وأصبح يشكل باب جديد هو الباب الثالث من قانون العقوبات الفرنسي، ثم صدر تعديل جديد لهذا القانون في1994/03/01.

أما عن التشريعات العربية فقد تبنى المشرع الجزائري في القسم السابع مكرر نصوص الجريمة المعلوماتية أو ما يصطلح عليه بجرائم المساس بأنظمة المعالجة الآلية للمعطيات وذلك بالقانون رقم23/06المؤرخ في 20/12/ 2006 المتضمن قانون العقوبات الجزائري.

ونجد المشرع الجزائري لم يتكلم عن الاعتداءات الماسة بمنتجات الإعلام الآلي، والتي تنطوي ضمنها التزوير المعلوماتي.

وقد شهد العالم مولد أول معاهدة دولية لمواجهة جرائم الكمبيوتر وذلك في سبتمبر 2001 في مدينة بودابست بتوقيع 26دولة من الاتحاد الأوروبي إضافة إلى كندا وجنوب إفريقيا والولايات المتحدة الأمريكية، والحقيقة أن تلك المعاهدة وإن كانت أوروبية المنشأ فهي دولية النزعة فهي مفتوحة للدول الأخرى التي تطلب الانضمام أو الترشح للانضمام لها.[1]

ولذلك سنتناول في هذا الفصل إلى الجوانب الموضوعية في نصوص الجريمة المعلوماتية (المبحث الأول) وإلى الجوانب الإجرائية في نصوص الجريمة المعلوماتية (المبحث الثاني).

[1] أمال قارة، المرجع السابق، ص27_28.

المبحث الأول

الجوانب الموضوعية في نصوص الجريمة المعلوماتية

لابد من الاعتراف أن الإسهام في اقتراح حلول للإشكالات التي يطرحها موضوع الحماية الجزائية للمعلوماتية مهمة تعترضها صعوبة منهجية كبرى مصدرها اتساع وتشعب الجوانب التي تتعلق بالمعلوماتية، لذلك سوف نتعرض في هذا المبحث للحماية الجزائية للمعلوماتية من جانبه الموضوعي، من خلال قانون العقوبات ونصوص الملكية الفكرية والصناعية باعتبار المعلوماتية نتاج فكر وإبداع.

المطلب الأول

الحماية الجزائية للجريمة المعلوماتية في ظل قانون العقوبات.

لقد نص المشرع الجزائري في قانون العقوبات على المساس بأنظمة المعالجة الآلية أو ما يعرف بالغش المعلوماتي بموجب التعديل الذي تم بالنسبة لقانون العقوبات بالقانون رقم23/06المؤرخ في 12/20/ 2006 المتضمن قانون العقوبات الجزائري في قسمه السابع مكرر، والذي شمل المواد من394مكرر الى394مكرر7،متتبعا في ذلك خطى التشريعات الغربية التي اتجهت في وقت متقدم إلى إصدار تلك النصوص المتعلقة بالجريمة المعلوماتية.

اهم تلك التشريعات نجد التشريع الفرنسي ولا ننسى أول اتفاقية حول الإجرام المعلوماتي التي أبرمت بتاريخ:2001/11/08 من طرف المجلس الأوروبي.لذلك سنتطرق في (الفرع الأول) إلى جريمة المساس بأنظمة المعالجة الآلية، أما في(الفرع الثاني) فهو مخصص للتزوير المعلوماتي الذي لم يتطرق إليه المشرع الجزائري فتمت معالجته من منظور التشريع المقارن.[1]

[1] أمال قارة، المرجع السابق، ص28.

الفرع الأول

جريمة المساس بأنظمة المعالجة الآلية للمعطيات

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي، وهو الفعل المنصوص والمعاقب عليه في المواد394 مكرر إلى المادة394مكرر7ونجد أن المشرع الجزائري لم يعرف لنا نظام المعالجة الآلية للمعطيات، بالرجوع إلى الاتفاقية الدولية الخاصة بالإجرام المعلوماتي قدمت تعريفا للنظام المعلوماتي في مادتها الثانية[1]،وكذلك عرفها الفقه الفرنسي.[2]

وبالعودة إلى قانون العقوبات الجزائري، نجد أن الغش المعلوماتي يأخذ صورتين أساسيتان وهما:

- الدخول في منظومة معلوماتية **introduction dans système informatique**.
- المساس بمنظومة معلوماتية **atteintes au système informatique.**
- صور أخرى من الغش المعلوماتي.

أولا/الدخول في منظومة معلوماتية.

ويشمل فعلين هما: الدخول والبقاء.

1_جريمة الدخول غير المشروع

تنص المادة394مكرر من قانون العقوبات الجزائري والتي تقابلها المادة1/323 قانون عقوبات فرنسي على معاقبة كل من يدخل عن طريق الغش في كل جزء من

[1] تنص المادة الثانية من الاتفاقية الخاصة بالإجرام المعلوماتي على:"

(Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données).

[2] عرف الفقه الفرنسي جريمة المساس بأنظمة المعالجة الآلية للمعطيات بأنها:"(كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها الذاكرة والبرامج والمعطيات وأجهزة الربط والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية.)

منظومة المعالجة الآلية للمعطيات أو يحاول ذلك،وتضاعف العقوبة إذ ترتب على الدخول أو البقاء أو حذف أو تغيير معطيات المنظومة أو تخريب النظام.

2_جريمة البقاء غير المشروع.

نص المشرع الجزائري على هذه الجريمة في المادة394مكرر من قانون العقوبات الجزائري. المقابلة لنص المادة 1/323من قانون العقوبات الفرنسي.ويقصد بالبقاء،الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم أتاء إتاوة.

وتقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل بعد،كما يجرم البقاء حتى ولو تم بصفة عرضية.[1]

ثانيا/المساس بمنظومة معلوماتية.

تنص المادة394مكرر1 قانون العقوبات الجزائري والذي يقابله في النص الفرنسي المادة3/323 قانون العقوبات الفرنسي عن «**كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها**».[2]

ثالثا/صور أخرى للغش المعلوماتي.

جاء نص المادة 394 مكرر 2من قانون العقوبات الجزائري بتجريم الأعمال التالية:

*تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السالفة الذكر.

*حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى جرائم الغش المعلوماتي.

كما نصت المادة6 من اتفاقية بودابست على جريمة الاستخدام غير المشروع للمعطيات على معاقبة كل من يقوم عمدا بإنتاج أو استعمال أو استيراد أو توزيع

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي،الطبعة6، دار هومة، الجزائر، ص445.

[2] مرزوق نسيمة، جرائم الانترنت مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006_2009، ص10.

برنامج حاسوب بغرض ارتكاب أو كلمة سر أو رمز وصول أو بيانات مماثلة بغرض ارتكاب الجرائم المنصوص عليها في المواد2الى5، ولا يشترط اجتماع تلك الجرائم بل يكفي توافر إحدى تلك الجرائم.

الفرع الثاني

جريمة التزوير المعلوماتي.

إن التعديل أو التغيير الذي يقع على المعطيات أو البرامج من شأنه أن يشكل جريمة تزوير والتي تقوم على تغيير الحقيقة بقصد الغش تغييرا يترتب عليه إلحاق الضرر بالغير، ويلاحظ أن المشرع الفرنسي بعد تعديل قانون العقوبات لسنة1988 وصدور قانون العقوبات لسنة1994 عدل المادة1/441لكي تستوعب بجانب التزوير العادي جريمة التزوير المعلوماتي، حيث نصت بعد تعديلها على :

«**إن كل تغيير للحقيقة بطريق الغش ....في محرر مكتوب أو في أي دعامة أخرى تحتوي تعبير عن الفكر**»فالمشرع فصل بذلك بين التزوير في البيانات المسجلة في ذاكرة الكمبيوتر وبين التزوير في محررات نظام المعالجة الآلية للمعلومات، حيث أفرد نص خاص، للصورة الأولى بينما احتوى الصورة الثانية في النص العام لجريمة التزوير.[1]

وقد تناولت المادة7 من اتفاقية بودابست جريمة التزوير المتصلة بالحاسوب واعتبرت أن الواقعة تعتبر تزويرا إذا تضمنت خلق أو تعديل لبيانات أو برامج غير مرخص بإنشائها أو تعديلها، حيث تصبح لها قيمة مختلفة في الإثبات فيما يتعلق بالمعاملات القانونية التي تقوم على الثقة في المعلومات القائمة على تلك البيانات التي تعرضت للتزوير.

ونجد المشرع الجزائري لم ينص عن التزوير المعلوماتي لذلك سنتطرق إلى تحديد جريمة التزوير المعلوماتي(الفقرة الأولى) وموقف المشرع الجزائري من التزوير المعلوماتي(الفقرة الثانية).[2]

[1] أمال قارة، المرجع السابق، ص47.

[2] أمال قارة، المرجع السابق، ص48.

أولا/تحديد جريمة التزوير المعلوماتي

إن موضوع التزوير هو المحرر، الذي لا بد من توافر شروط فيه، تتمثل في الكتابة من قبل شخص وأن ينتج أثاره القانونية هذه من الناحية التقليدية لجريمة التزوير، لكن في مجال المعلوماتية فالأمر يختلف فجريمة التزوير المعلوماتي تقع على المستندات المعلوماتية.

كما أن الغاية من تجريم أفعال التزوير هو حماية الثقة العامة، التي تنشأ من تعامل الأفراد بالمحررات بمفهومها التقليدي، ووضع نص خاص بالتزوير المعلوماتي يحقق الحماية للنظام المعلوماتي فقط دون الحفاظ على الثقة العامة، وبذلك فإن المحررات المعلوماتية تخرج من المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها، لذلك فإن إلغاء النص يخضع المحررات المعلوماتية إلى النصوص التقليدية الخاصة بالتزوير، بالمفهوم الجديد للمحررات.

إن النشاط الإجرامي المكون لجريمة التزوير المعلوماتي يتمثل في فعل تغيير الحقيقة ويعني استبدالها بما يخالفها وإذا انتفى هذا التغيير انتفى التزوير. وإن تحوير البرنامج أو قواعد البيانات لا يعد تزويرا بل يقع تحت طائلة نصوص قانون حقوق المؤلف والحقوق المجاورة.[1]

ثانيا/موقف المشرع الجزائري من جريمة التزوير المعلوماتي

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي، الذي يعتبر من اخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسوب الآن. ونجد أن المشرع الجزائري نص على التزوير الخاص بالمحررات في القسم الثالث والرابع والخامس من الفصل السابع من الباب الأول من الكتاب الثالث من قانون العقوبات في المواد214الى229التي تشترط المحرر لتطبيق جريمة التزوير، ولم يتخذ أي موقف لتوسيع مفهوم المحرر من اجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة التزوير.

[1] أمال قارة، المرجع السابق، ص42.

لقد كان من الأفضل لو أضاف المشرع الجزائري نصا خاصا بالتزوير المعلوماتي مثلما قام به المشرع الفرنسي، ونخلص في النهاية أن المشرع الجزائري رغم تداركه من خلال القانون رقم 23/06 الفراغ القانوني في مجال الإجرام المعلوماتي وذلك بتجريم الاعتداءات الواردة على الأنظمة المعلوماتية باستحداث نصوص خاصة إلا أنه أغفل تجريم التزوير المعلوماتي، ولم يتبنى الاتجاه الذي انتهجته التشريعات الحديثة التي قامت بتوسيع مفهوم المحرر ليشمل كافة صور التزوير الحديث ليشمل المستند المعلوماتي.

المطلب الثاني

الحماية الجزائية في ظل نصوص قانون الملكية الفكرية والصناعية.

نظرا لنسبية الحماية من خلال النصوص التقليدية لجرائم الأموال نتيجة للطبيعة المميزة للمال المعلوماتي، ولما كانت الحاجة ملحة وضرورية لحماية برامج الحاسب الآلي في الوسط القانوني والتوجه الفعلي من قبل رجال القانون نحو وضع الأطر القانونية لهذه الحماية مما أدى إلى إثارة جدل حول الحماية المناسبة لبرامج الحاسب الآلي، فقد استقر الفقه القانوني مؤخرا في الدول التي ترعرعت فيها برامج الحاسب الآلي على إخضاعها لقوانين الملكية الفكرية والصناعية.[1]

الفرع الأول

الحماية الجزائية لبرامج الحاسوب من خلال نصوص قانون الملكية الفكرية

يعتبر حق المؤلف من ابرز صور الملكية الفكرية وأهمها، لذلك قامت العديد من الدول سواء عبر تشريعات داخلية أو اتفاقيات دولية بإقرار حماية قانونية لحق المؤلف وسايرها المشرع الجزائري في ذلك والذي اصدر عدة قوانين لحماية حق المؤلف أحدثها الأمررقم05/03الموافق ل19يوليو2003.

1 عبد القادر القهوجي، المرجع السابق، ص119.

ويشمل نطاق قانون حق المؤلف من حيث الموضوع المصنفات الأدبية والفنية المبتكرة أيا كان نوعها أو طريقة التعبير عنها أو أهميتها أو الغرض منها، ومن أهم هذه المصنفات: برامج الكمبيوتر، فنجد أن المشرع الجزائري من خلال نص المادة الرابعة من الأمررقم05/03 قد نص صراحة على اعتبار برامج الكمبيوتر كمصنفات أدبية محمية وكذلك القانون الفرنسي الصادر في 3يوليو1985، وفي مصر بموجب القانون رقم 38/92، أما على الصعيد الدولي فإن اتفاقية برن وتريبس اعتبرها كمصنفات محمية بموجب قانون حقوق المؤلف.

ونظرا لما تتعرض له برامج لكمبيوتر، من جرائم متعددة ومتنوعة فإن أغلب التشريعات المعاصرة الخاصة بحماية حقوق المؤلف لم تخلو من حماية جزائية لكون الحماية المدنية لا تردع هذه الاعتداءات الخطيرة، فالحماية الجزائية لما تشتمل عليه من قوة وردع زاجرة تكفل حماية أكثر فعالية لحق المؤلف حيث نص المشرع الجزائري في المواد 151الى 159من قانون رقم05/03 على جرائم وعقوبات الاعتداء على حقوق المؤلف، وهذا ما أورده كذلك المشرع الفرنسي من جرائم وعقوبات بموجب المادة2/335 من الأمررقم657/01الصادر في 14 سبتمبر2001. لذلك ستقتصر دراستنا في هذا الفرع على الاعتداءات الواردة على برامج الكمبيوتر(الفقرة الأولى)وفي(الفقرة الثانية) نخصصه للجزاءات المقررة لتلك الجرائم.[1]

أولا/الاعتداءات الواردة على برامج الكمبيوتر

حماية لحقوق المؤلف لم تخلو اغلب التشريعات الخاصة بحماية حق المؤلف من نصوص تجـــــــــــــــــريم الاعتداء على حق المؤلف، ومن تلك التشريعات التشريع الجزائري الذي جرم الاعتداء على حقوق المؤلف بما فيها حقوق مؤلفي البرامج، وذلك في المواد151،154،155،من الأمر05/03 المتعلق بحقوق المؤلف والحقوق المجاورة، أما المشرع الفرنسي فنص عليها في المادة02/335 من الامر657/01 المتعلق بحقوق المؤلف والحقوق المجاورة، أما المشرع المصري فنص عليها في نص المادة 47من القانون38/92.

[1] أمال قارة، المرجع السابق، ص44.

وأما بالنسبة للاتفاقيات الدولية كاتفاقية برن لعام 1979 فإنها أقرت مبادئ وأسس تحكم الجانب الجزائي للمساس بحق المؤلف، ولم تجرم بصفة صريحة تصرفات معينة لتترك أمر تحديد جرائم الاعتداء على حقوق المؤلف إلى التشريعات الداخلية للدول.

ويلاحظ أن المشرع أدخل جميع جرائم الاعتداء على حقوق المؤلف بما فيهم مؤلفي البرامج تحت وصف جنحة التقليد وإن كان لا يصدق عليها جميعها ذلك الوصف.[2]

1_جريمة التقليد

لم يضع المشرع في مختلف الدول تعريفا لجريمة التقليد، وكل ما فعله هو أنه بين فقط الأفعال التي تشكل جريمة التقليد، أما الفقه فقد تباين في تعريفها، ومن بينها: **هي اعتداء مباشر أو غير مباشر على حقوق المؤلف الأدبية أو المالية المحمية لقانون حق المؤلف.[2]**

ولقد نص المشرع الجزائري في المادة151من الامر05/03على أنه يعد مرتكب لجنحة التقليد كل من يقوم بالكشف غير المشروع للمصنف أو يمس بسلامته، أو يقوم باستنساخ مصنف أو يقوم باستيراد أو تصدير أو نسخ مقلدة من مصنف أو يقوم بتأجير أو وضع رهن التداول لنسخ مقلدة لمصنف، أما المادة 154منه فقد نصت على أنه يعد مرتكب لجنحة التقليد كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف، ونصت المادة155منه على أنه يعد مرتكب لجنحة التقليد كل من يرفض عمدا دفع المكافئة المستحقة للمؤلف.

والحقيقة أن كل الأفعال السابقة لا يصدق عليها وصف جنحة التقليد بل هي جرائم ملحقة بجريمة التقليد.

2_الجرائم الملحقة بجرائم التقليد:

---

[2] أسامة أمحمد المناعسة، جلال محمد الزغبي،جرائم الحاسب الآلي والانترنت،دار وائل للنشر، الأردن،2004،ص144.

[2] أسامة أمحمد المناعسة، المرجع السابق، ص144.

ولقد نصت على هذه الجرائم في التشريع الجزائري لحقوق المؤلف والحقوق المجاورة في المادة151، أما في التشريع الفرنسي فإنه نص عليها في المادة 2/335من قانون العقوبات وبالرجوع إلى التشريع الجزائري والفرنسي لحقوق المؤلف والحقوق المجاورة، نجد أن تلك الجرائم الملحقة بجريمة التقليد تتمثل في التعامل في البرامج المقلدة بالاستيراد أو التصدير أو البيع أو التأجير أو التداول، وهذا بخلاف التشريع المصري الذي أشار إلى جريمة التعامل بالبرامج المقلدة وأضاف جريمتين اخريتين وهما إدخال برامج منشورة في الخارج وجريمة التقليد في مصر لبرنامج منشور في الخارج أو التعامل فيه.[1]

ثانيا/الجزاءات المقررة لجرائم الاعتداء على برامج الكمبيوتر

نظرا لخطورة وجسامة الجرائم المرتكبة على حق المؤلف وبالأخص حقوق مؤلفي برامج الكمبيوتر، ظهرت الحاجة لوضع جزاءات رادعة،ل هذا سنتطرق إلى العقوبات الأصلية والعقوبات التكميلية المخصصة لهذا النوع من الجرائم.

لقد قرر المشرع الجزائري بموجب المواد:153،156،157،158،159من الأمر 05/03المتعلق بحقوق المؤلف والحقوق المجاورة الجزاءات المقررة على كل من يعتدي على حقوق المؤلف.

غير أن الشروع أو المحاولة الذي يمكن تصوره بالنسبة لهذه الجرائم غير معاقب عليه بنص خاص، لان العقوبة المقررة لهذه الجرائم عقوبة جنحة والقاعدة تقضي بأن لا يعاقب على الشروع في الجنح إلا بنص خاص.

1_العقوبات الأصلية

حدد المشرع الجزائري في المادة153من الامر05/03 عقوبة تتمثل في الحبس من 3اشهر الى3سنوات وغرامة من 500.000دج الى1.000.000دج سواء كان النشر قد حصل في الجزائر أو خارجها.

[1]أسامة أمحمد المناعسة، المرجع السابق، ص145.

ويلاحظ أن قيمة الغرامة التي جاءت في التشريع الجزائري غير رادعة مثل ماهو الحال في التشريع الفرنسي، الذي قد تصل قيمة الغرامة إلى مليون فرنك فرنسي فضلا عن تعويض للطرف المتضرر من عملية القرصنة، فالمكاسب التي يحققها سارقي حقوق الملكية الفكرية من جراء الاعتداء على حقوق مؤلفي البرامج كبيرة جدا، لذلك في الغرامة يجب أن تكون على قدر الجرائم.

وفي هذا الصدد قال عصام الكردي الخبير القانوني في مجال حماية الملكية الفكرية إن القانون لا يجب أن يتضمن الحد الأقصى وأن يتم تحديد حد أدنى للغرامة ويترك للقاضي تحديد الحد الأقصى للغرامة، كما يرى أنه على القانون جعل الحبس جوازا مع مضاعفة الغرامة وذلك في المرة الأولى وجعله وجوبي مع مضاعفة الغرامة في حالة العود.

ونص المشرع الجزائري على تشديد العقوبة في حالة العود بموجب المادة156من الامر05/03،فالجاني يكفي أن يرتكب مرة ثانية جريمة من الجرائم المنصوص عليها في

المواد151،154،155من الامر03/.05[1]

2_ العقوبات التكميلية وتدابير الأمن

تتمثل العقوبات التكميلية في التشريع الجزائري في المصادرة ونشر الحكم حيث نص على المصادرة في المادة157من الامر05/03 التي نصت على انه تقرر الجهة القضائية المختصة مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي للمصنف ومصادرة العتاد المخصص لمباشرة النشاط أو المشروع والنسخ.

ويلاحظ أن المشرع الجزائري أوجب على الجهة القضائية المختصة في المادة159من الامر05/03 أن تأمر في جميع الحالات المنصوص عليها في المواد 151،152بتسليم العتاد أو النسخ المقلدة أو قيمة ذلك كله وكذلك الإيرادات موضوع

[1] أمال قارة، المرجع السابق، ص50.

المصادرة للمؤلف أو لأي مالك حقوق أخرى أو ذي حقوقهما لتكـــــــــــون عند الحاجة بمثابة تعويض عن الضرر اللاحق بهم. وقد جعل المشرع الجزائري المصـــادرة جوازية، فالجهة القضائية أن تقرر الحكم بالمصادرة. على خلاف التشريع المصري الذي يقضي أنه في جميع الأحوال تقضي المحكمة بمصادرة النسخ المقلدة والأدوات المستخدمة في التقليد، والمصادرة وجوبية يتعين على القاضي أن يحكم بها، وإن لم يفعل كان حكمه معيبا مستوجبا نقضه للخطأ في تطبيق القانون.[2]

أما عن عقوبة نشر الحكم فنص عليها المشرع الجزائري في المادة158من الأمر رقم05/03 والتي تقضي أنه يمكن للجهة القاضية المختصة بطلب من الطرف المدني، أن تأمر بنشر أحكام الإدانة كاملة أو مجزئة في الصحف التي تعينها وتعليق هذه الأحكام في الأماكن التي تحددها ومن ضمن ذلك على باب المسكن الخاص بالمحكوم عليه وكل مؤسسة أو قاعة حفلات يملكها على أن يكون ذلك على نفقة هذا الأخير شريطة أن لا تتعدى هذه المصاريف الغرامة المحكوم بها.

ويقصد بهذه العقوبة التشهير بالمحكوم عليه والتأثير على شخصيته الأدبية والمالية، وهي بذلك عقوبة ماسة بشرف الاعتبار.

ونجد مرة أخرى أن المشرع المصري قد جعل نشر الحكم أمر وجوبي يتعين على الجهة القضائية الفاصلة في الموضوع أن تقرره، على خلاف المشرع الجزائري الذي جعله جوازي، إذ يمكن للجهة القضائية بناء على طلب من الطرف المدني أن تأمر بنشر الحكم أما عن تدابير الأمن فقد نص المشرع الجزائري بموجب المادة2/156عن عقوبة الغلق، حيث نصت أنه يمكن للجهة القضائية المختصة أن تقرر الغلق المؤقت مدة لا تتعدى 6اشهر التي يستغلها المقلد أوشريكه أو أن تقرر الغلق النهائي عند الاقتضاء، ويستفاد من هذا النص أن عقوبة الغلق جوازية يجوز للقاضي أن يحكم بها، على خلاف التشريع المصري الذي اعتبرها وجوبية في حالة العود وجوازية في حالة الجرائم البسيطة.

[2] عبد القادر القهوجي، المرجع السابق، ص46.

وتجدر الإشارة إلى أن المشرع المصري اعتبر عقوبة الغلق عقوبة تكميلية على خلاف المشرع الجزائري الذي اعتبرها تدابير امن.

وبعد عرض جوانب الحماية الجزائية لبرامج الكمبيوتر من خلال حق المؤلف يمكن القول انه لكي تتمتع البرامج بتلك الحماية يجب أن تتوفر شروط المصنف المحمي وأهمها شرط الابتكار، وأن يتحقق الاعتداء عليها بإحدى النماذج الإجرامية، فإذا تخلف شرط الابتكار أو إذا لم تتوفر أحد أركان الجرائم السابقة تفتقد البرامج للحماية الجنائية من خلال نصوص حقوق المؤلف.[1]

الفرع الثاني

الحماية الجزائية لبرامج الحاسوب في ظل نصوص الملكية الصناعية

إن قانون الملكية الفكرية يشمل عدة مجالات منها: العلامات التجارية براءة الاختراع، الرسوم والنماذج، تسمية المنشأ، وما يهمنا بصدد حماية برامج الكمبيوتر هو حمايتها من خلال براءة الاختراع.

أولا/الشروط الواجب توافرها في براءة الاختراع

بصدور الأمر 07/03 المؤرخ في: 2003/07/19 المتضمن براءة الاختراع وبالعودة إلى نصوصه نجد المادة الثانية منه عرفت الاختراع بأنه:«**فكرة المخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال التقنية**»، وبشأن الشروط الواجب توافرها في الاختراع كي تطبق عليه أحكام المادة الثالثة من ذات الأمر التي تنص على مايلي: «**يمكن إن تقع تحت براءة الاختراع الجديدة الناتجة عن نشاط الاختراعي والقابلة للتطبيق صناعيا**»

ومن خلال نصوص الملكية الفكرية نجد أنه يضفي حماية جنائية عن طريق براءة الاختراع، حيث لابد من توافر شروط معينة في الاختراع تتمثل فيما يلي:

*الابتكار.

[1] عبد القادر القهوجي، المرجع السابق، ص47.

*الجدية.

*القابلية للتطبيق الصناعي.

*المشروعية.

إن الفقه التجاري الذي تناول موضوع براءة الاختراع كموضوع من موضوعاته على كون الاختراع ذو صفة مادية، وذلك يتضح من الشروط الواجب توفرها في الاختراع حتى يتمتع بالحماية القانونية التي تقررها النصوص قانون براءة الاختراع التي لا تطبق إلا على الأشياء المادية الملموسة سواء كان منتجا أو وسيلة خاصة إذ لاحظنا أن كل ذلك في إطار شرط القابلية للاستغلال الصناعي، ليتبين أنه يحتوي على بعد مادي، وهذا ما يفرق على أساسه الفقه التجاري بين الابتكار الصناعي والمصنفات الأدبية، وعلى هذا يمكن القول بأن الفقه التجاري وإن كان قد اختلف في ترتيب شروط الاختراع التي تؤهله للحصول على البراءة، فإنه متفق على الطابع المادي لهذا الاختراع أو الابتكار الجديد القابل للاستغلال الصناعي.[1]

وبناءا على ذلك فان أحكام قانون براءة الاختراع يمكن أن تطبق على المكونات المادية للكمبيوتر متى توافرت فيها الشروط التي يتطلبها هذا القانون أما مكونات الكمبيوتر غير مادية فلا يمكن أن نطبق النصوص الخاصة بقانون براءة الاختراع وذلك لانتفاء الطابع المادي لها.

ثانيا/مدى تطبيق نصوص براءة الاختراع على برامج الكمبيوتر.

يرى الدكتور محمد حسنين إن الحماية بقوانين براءة الاختراع أن برامج الكمبيوتر ولأنها تستعمل للتعامل مع آلات الكمبيوتر، وإدارتها فهي بذلك تصبح جزء منها، ولما كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الكمبيوتر فهي من هذه الزاوية تصبح قابلة للبراءة.[2]

[1] أمال قارة، المرجع السابق، ص65.

[2] محمد حسنين، الوجيز في الملكية الفكرية، المؤسسة الوطنية للكتاب، الجزائر، 1985، ص125.

أما المنتقدون فيقولون على الرغم من مزايا الحماية التي توفرها قوانين براءة الاختراع إلا أنه توجد عدة أسباب تحول دون امتداد نصوص براءة الاختراع إلى المكونات غير المادية الكمبيوتر.

حسبما يراه المختصون في الميدان فأنه من الصعب توفير حماية ناجحة للبرمجيات بالرجوع إلى قانون الملكية الصناعية، ويتعلق الأمر خاصة بشرطين لابد من توفرهما في العمل الإبداعي لكي يظفر صاحبه بالبراءة:

*الجدية.

*القابلية لاستغلال الصناعي.

هذان الشرطان تتفق حولهما التشريعات المقارنة مع التشريع الجزائري فيما يضيف هذا الأخير شرطا آخر هو إن يكون الاختراع نشاطا خلاقا(**une activité inventive**).[1]

أولا/شرط الجدية.

طبقا للمادة 09من الأمر 07/03:«**يعتبر الاختراع ناتجا عن نشاط اختراعي إذا لم يكن ناجما بداهة عن الحالة التقنية**».

ويرى الفقهاء أن هذا لا يمكن تحققه في البرمجيات، ولا من الهين إثباته، إذ يجب للتقرير بتوافر هذا الشرط أن يكون لدى الجهة التي تقوم بفحص طلبات البراءة قدرا معقولا من الدراية لكي تقرر ما إذا كان قد سبق تقديم اختراعات مشابهة للاختراع المقدم الطلب بشأنه أم لا. الأمر الذي يتطلب أن تكون هذه الجهة على درجة عالية من الكفاءة والتمييز في المجال الذي تتولى بحثه.

وتقرير جدة الاختراع في معظم الأحيان يكون أمر جزافيا، لما تتميز به من طابع ذهني بحت، قد يكون صعبا على المبرمجين ذاتهم، فكيف يكون الوضع بالنسبة للقاضي عند عرض هذه المسألة عليه.

[1] عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي، لبنان، 2003، ص45.

إن صعوبة تقييم طابع الجدة بالنسبة للكيانات غير المادية ليس مرده لاعتبارات قانونية، بل مرجع ذلك عدم توافر الكفاءات اللازمة التي يمكنها بحث وفحص الكيان المعنوي، والنظر في مدى توافر شرط الجدة بالنسبة له من عدمه.

ثانيا/صعوبة الاستغلال الصناعي بالنسبة للكيان المعنوي

يجب أن يكون الاختراع قابلا للاستغلال الصناعي لكي يتمتع بنصوص الحماية الخاصة ببراءة الاختراع، هذا الشرط يفترض أن يكون الاختراع ذا صفة مادية، ويجب أن يؤدي استغلاله إلى منتج صناعي، أو يمكن الوصول إلى نتيجة صناعية، وكل هذه الأمور تتناقض مع الكيان المعنوي.

ويقول البعض انه مع تقديرنا للحجج التي قالت بعدم انطباق صفة الوسائل الصناعية على البرامج لانعدام طبيعتها المادية، إلا أن ذلك يعد تفسيرا فقهيا إذ أن التشريعات المعاصرة لم تتطلب صراحة مادية الاختراع أو وسائله.[1]

فالنظريات العلمية وهي مجرد أفكار لكن إذا تم استخدامها في غرض صناعي معين، اكتسبت براءة الاختراع، كذلك الحال بالنسبة للبرامج أو الكيان المعنوي إذا ما تم استثمارها، وعليه هناك إمكانية تطبيق وصف الوسائل المستحدثة على البرامج وبالتالي يمكن أن تحظى بالحماية القانونية المقررة للاختراعات، ويمكن تصور ذلك في البرامج المعلوماتية المتطورة التي تعتبر من أحدث الوسائل التي تستخدم في الصناعة وفي تطويرها.

التشريعات المعاصرة بصفة عامة تستبعد البرامج المعلوماتية من مجال الحماية بواسطة براءة الاختراع وذلك راجع لأحد السببين التاليين:

1/ تجرد برامج المعلوماتية من أي طابع صناعي، وهذا ما أثبتته الإحصائية التي أجرتها المنظمة العالمية للملكية الفكرية عام1978التي جاء فيها أن 1% فقط من البرامج يستوفي شرط قابلية الاستغلال الصناعي.

[1] أمال قارة المرجع السابق،ص67.

2/صعوبة البحث في مدى جدة البرامج، لتقدير مدى استحقاقها، لبراءة الاختراع.

ويمكن استثناء الحصول على براءة الاختراع بخصوص برامج الإعلام الآلي في حالتين هما:

–أن يكون البرنامج جزء من ذاكرة الكمبيوتر.

–أن يكون طلب براءة الاختراع ينصب على وسيلة صناعية جديدة يستخدم البرنامج في تحقيق إحدى مراحلها.

وتجدر الإشارة إلى أن المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءة الاختراع وذلك طبقا للمادة 07من الأمر07/03 المتضمن براءة الاختراع «**لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب**».

فنظرا لاستبعاد نظام براءة الاختراع في حماية البرامج الكمبيوتر، ونظرا لصعوبة استحداث تشريع خاص بالبرمجيات، تبنى المشرع الجزائري نظام الحماية وفقا لحقوق المؤلف والحقوق المجاورة وهو ما سارت عليه غالبية التشريعات والاتفاقيات الدولية.[1]

المبحث الثاني

الجوانب الإجرائية في نصوص الجريمة المعلوماتية

إضافة إلى الجوانب الموضوعية التي تمت دراستها في المبحث الأول نخصص المبحث الثاني للجوانب الإجرائية في نصوص الجريمة المعلوماتية حيث يأتي المطلب الأول بعنوان قواعد الاختصاص المحلي وإجراءات التحقيق الابتدائي أما المطلب الثاني جاء بعنوان المكافحة الإجرائية في القانون الجزائري.

المطلب الأول

قواعد الاختصاص المحلي وإجراءات التحقيق الابتدائي

[1] أمال قارة، المرجع السابق، ص68.

إن الطبيعة الخاصة للجرائم المعلوماتية لابد أن تنعكس على قانون الإجراءات الجزائية، فيلزم على المجتمع المعلوماتي في مجال قانون الإجراءات الجزائية أن تنشأ قواعد إجرائية حديثة إلى جانب القواعد الموضوعية، كانت هذه الجرائم المعلوماتية تتميز بصعوبة اكتشافها وإثباتها وتحتاج إلى خبرة فنية عالية للتعامل معها، فإن ذلك أثار العديد من المشكلات العملية الإجرائية التي جعلت القواعد الإجرائية التقليدية قاصرة عن مواجهة تلك المشاكل، ولهذا اتجهت بعض التشريعات كالتشريع الانجليزي والأمريكي والجزائري إلى تعديل بعض قواعدها الإجرائية لجعلها قادرة على مواجهة تلك المشاكل الإجرائية كتلك المتعلقة بالاختصاص المحلي، وإجراءات التحقيق الابتدائي خاصة التي تهدف إلى جمع الأدلة.

وسوف نتناول في هذا المطلب إلى قواعد الاختصاص المحلي(الفرع الأول)، وإجراءات التحقيق الابتدائي(الفرع الثاني).[1]

الفرع الأول

قواعد الاختصاص المحلي

عالج المشرع الاختصاص المحلي للجهات القضائية وذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه،وقد اعتمد على عناصر معينة تربط بين اختصاص الجهات القضائية بالنظر في الخصومة الجزائية، وهذا المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه، لكن لما كانت الجريمة المعلوماتية جرائم عابرة للإقليم، إذ غالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر كما قد يكون الضرر الحاصل في بلد ثالث في الوقت نفسه، لهذا فان المشرع الجزائري أجرى بعض التعديلات المتعلقة بالاختصاص المحلي في الجريمة المعلوماتية بموجب القانون 22/06المؤرخفي 20ديسمبر2006المعدل والمتمم للأمر رقم155/66الموافق ل08يونيو1966والمتضمن قانون الإجراءات الجزائية، لهذا سنتطرق لتلك القواعد على النحو التالي:

[1] أمال قارة، المرجع السابق، ص55.

أولا/الاختصاص المحلي للنيابة العامة

يتحدد الاختصاص المحلي للنيابة العامة وفقا للمادة37من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة ومحل إقامة احد الأشخاص المشتبه في مساهمتهم في الجريمة أو بالمكان الذي في دائرته القبض على هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر.

وبالتالي فإن اختصاص وكيل الجمهورية يجب أن لا يتعدى مكان وقوع الجريمة أو محل إقامة احد الأشخاص المشتبه في مساهمتهم في الجريمة أو بمكان القبض على هؤلاء الأشخاص حتى ولو تم لسبب أخر لكن لما كانت الجريمة المعلوماتية جريمة قد ترتكب في مكان معين وتكون أثارها في مكان أخر فإن المشرع الجزائري بموجب المادة 37فقرة2 من قانون الإجراءات الجزائية[1] أجاز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة الاختصاص المحاكم الأخرى إلا أنه ترك كيفية تطبيق ذلك عن طريق التنظيم الذي سيحدد المحاكم التي يمتد إليها الاختصاص.[2]

ويتعين على ضابط الشرطة القضائية طبقا للمادة40مكرر1من قانون الإجراءات الجزائية الجزائري[3] أن يبلغوا وكيل الجمهورية لدى المحكمة الكائن لها الجريمة بأصل ونسختين من إجراءات البحث ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة.

والذي يطالب طبقا للمادة40مكرر2من هذا القانون بالإجراءات فورا إذ اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة40مكرر من هذا القانون،وهذه الإجراءات تتعلق ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام

---

[1] تنص المادة 2/37 من قانون الإجراءات الجزائية الجزائري على ما يلي:" يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف"

[2] أمال قارة، المرجع السابق، ص 56.

[3] تنص المادة 40مكرر1 من قانون الإجراءات الجزائية الجزائري على ما يلي:"يخبر ضباط الشرطة القضائية فورا وكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة ويبلغونه بأصل وبنسختين من إجراءات التحقيق ويرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة"

لدى المجلس القضائي التابعة له المحكمة المختصة،والذي يطالب طبقا للمادة40مكرر2من هذا القانون بالإجراءات فورا إذ اعتبر أن الجريمة تدخل ضمن اختصاص المحكمة المذكورة في المادة40مكرر من هذا القانون، وهذه الإجراءات تتعلق بتحريك الدعوى العمومية أو مباشرتها أو رفعها مجرد أن يتبين للنائب العام أن الجريمة تدخل ضمن المحكمة المختصة التابعة لها وهذا مانصت عليه المادة40مكرر.3[1]

ثانيا/الاختصاص المحلي لقاضي التحقيق ومحاكم الجنح

1_الاختصاص المحلي لقاضي التحقيق

يقصد بالاختصاص المحلي لقاضي التحقيق المجال الذي يباشر فيه قاضي التحـــــــقيق، ويتحدد الاختصاص المحلي لقاضي التحقيق طبقا للمادة40 من قانون الإجراءات الجزائية[2] لمكان وقوع الجريمة أو محل إقامة احد هؤلاء الأشخاص المشتبه في مساهمتهم في اقترافها أو محل القبض على احد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب أخر.

إلا أن المشرع ألغى في التعديل الجديد الفقرة2و3من المادة40، وأصبحت تنص الفقرة2 على انه:" **يجوز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات"**، وبالتالي فإن المشرع أجاز إمكانية تمديد الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم أخرى لكنه ترك تحديد كيفية تطبيق تلك الإجراءات لتنظيم الذي سيصدر لاحقا.[3]

2_ الاختصاص المحلي لمحاكم الجنح.

[1] تنص المادة 40مكرر3 من قانون الإجراءات على ما يلي:"يجوز للنائب العام لدى المجلس القضائي التابعة له الجهة القضائية المختصة أن يطالب بالإجراءات في جميع مراحل الدعوى."

[2] تنص المادة 40مكرر من قانون الإجراءات على ما يلي:"يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض لسبب آخر."

[3] أمال قارة، المرجع السابق، ص57.

يتحدد الاختصاص المحلي لمحاكم الجنح طبقا للمادة329من قانون الإجراءات الجزائية الجزائري بمكان وقوع الجريمة، أو بمحل إقامة احد الأشخاص المتهمين، أو شركائهم، أو بالمكان الذي تم في دائرته القبض على احد هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر، غير أن المشرع في التعديل الصادر بموجب القانون 14/04اضاف فقرة أخرى أجاز فيها في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد الاختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم.[1]

إذن فإن المشرع أجاز في حالة ارتكاب جريمة من جرائم الماسة بأنظمة المعالجة الآلية للمعطيات تمديد اختصاص وكيل الجمهورية واختصاص قاضي التحقيق واختصاص محاكم الجنح ولكنه ترك ذلك للتنظيم الذي سيصدر لاحقا والذي يحدد تلك المحاكم التي يمتد إليها الاختصاص، وقرر في المادة40مكرر[2] أيضا تطبيق القواعد المتعلقة بالدعوى العمومية والتحقيق والمحاكم أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد37،40،329من قانون الإجراءات الجزائية.

والحقيقة أن مشكلة الاختصاص القضائي في الجريمة المعلوماتية تعد من المشكلات العويصة التي تعرقل الحصول على الدليل، ذلك أن هذه الجريمة قد ترتكب في مكان معين وتنتج أثارها في مكان أخر داخل الدولة أو خارجها وإذا كانت مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس معيار القبض على المتهم أو محل إقامته أو مكان وقوع الجريمة فأي مكان في هذه الأماكن ينعقد الاختصاص الجنائي لسلطات التحقيق والمحاكمة في الجريمة المعلوماتية.

لكن على المستوى الدولي فان الأمر بحاجة إلى اتفاقيات دولية ثنائية أو جماعية، ولقد شرعت بعض الدول في عقد اتفاقيات ثنائية لتسهيل مهمة التحقيق في جرائم الحاسوب الآلي، إلا أن ذلك لم يحقق تقدما في معالجة الاختصاص القضائي، فلذلك

[1] محمد الأمين البشري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة، دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الانترنت، الدليل الالكتروني للقانون العربي، ص372.

[2] تنص المادة40 مكرر من قانون العقوبات الجزائية الجزائري على ما يلي:" تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد37 ،40،329من هذا القانون، مع مراعاة أحكام المواد من 40مكرر1إلى 40مكرر5"

فالحاجة ماسة إلى قوانين جنائية أكثر مرونة حتى تواكب سرعة تقدم الحاسب الآلي في كل المجالات.[3]

الفرع الثانـي

إجراءات التحقيق الابتدائـي.

إجراءات التحقيق الابتدائي هي مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشان واقعة جنائية معروضة عليها وذلك بالبحث عن الأدلة المثبتة لذلك، والتحقيق مرحلة لاحقة لإجراءات جمع الاستدلال وتسبق مرحلة المحاكمة التي تقوم بها جهة الحكم، وعليه فإن التحقيق يهدف إلى تمهيد الطريق أمام قضاء الحكم باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة.

يهدف التحقيق الابتدائي إلى الكشف عن الحقيقة للوصول إلى هذا الغرض يلجا المحقق إلى مجموعة إجراءات بعضها يهدف للحصول على الدليل، وتسمى إجراءات جمع الدليل كالتفتيش والضبط والمعاينة والشهادة والخبرة، وبعضها الأخر يمهد للدليل ويؤدي إليه وتعرف بالإجراءات الاحتياطية ضد المتهم كالقبض والحبس المؤقت.[1]

وسوف تقتصر دراستنا على إجراءات جمع الأدلة المادية التي يكون منها القاضي الجزائي اقتناعه تلقائيا بحكم العقل والمنطق، فهي أقوى مفعولا في الاقتناع من الأدلة القولية على أن نخص بالدراسة التفتيش وضبط الأشياء باعتبارهما أهم التحديات الإجرائية لجرائم الكمبيوتر.

أولا/التفتيش في مجال الجريمة المعلوماتية

[3] محمد الأمين البشري، المرجع السابق،ص 373.

[1] محمد الأمين البشري، المرجع السابق، ص374.

لقد تعددت التعريفات التي أضافها الفقه على التفتيش، إلى أنها تجتمع على أن التفتيش عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في محل وذلك من اجل إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات القانونية المقررة، وقد أحاط القانون التفتيش بضمانات عديدة لأنه قد يقتضي البحث في محل له حرمة خاصة. وإذا كان التفتيش للأشياء المادية بما فيها المكونات المادية للحاسوب لا يثير إشكالية، فما مدى خضوع البرامج والمعلومات كمكونات معنوية للحاسوب للتفتيش؟وماهي ضوابط تفتيش نظم الحاسوب؟

1_مدى قابلية نظم الحاسوب للتفتيش:

يتكون الحاسوب من مكونات مادية ومكونات معنوية، ولا تثار أدنى صعوبة إذا كان محل جرائم الحاسوب الآلي مكونات مادية حيث ينطبق بصددها القواعد التقليدية دون صعوبة، فالواقع أن ولوج المكونات المادية للحاسوب بأوعيتها المختلفة بحثا عن شيء يتصل بجريمة معلوماتية قد وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وأنه يدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة، بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجود فيه وهل هو من الأماكن العامة أو الأماكن الخاصة إذ أن لصفة المكان أهمية خاصة في مجال التفتيش.

إذا كانت موجودة في مكان خاص كمسكن المتهم أو احد ملحقاته كان له حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش منزله وبنفس الضمانات المقررة قانونا في التشريعات المختلفة، وبالنسبة للاماكن العامة سواء كانت بطبيعتها كالطرق العامة والشوارع أو كانت بالتخصيص كالمقاهي والمطاعم والسيارات العامة فان الشخص إذا وجد في هذه الأماكن وهو يحمل مكونات مادية للحاسوب أو كان مسيطرا أو حائـــــــزا لها فان التفتيش لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا الصدد.[1]

[1] عبد الله هلالي، تفتيش نظام الحاسب الآلي، وضمانات متهم المعلومات، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية، مصر، ص74.

أما إذا كان محل جرائم الحاسوب الآلي مكونات غير مادية أي معنوية، كبرامج لحاسوب أو بياناته فقد ثار خلاف كبير في الفقه بين مؤيد ومعارض، حيث يذهب رأي انه إذا كانت الغاية من التفتيش هو جمع الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم يمتد ليشمل البرامج والبيانات. وقد لجأ الفقه في العديد من الدول استنادا إلى عمومية نصوص التفتيش إلى التوسع في تفسيرها وذلك بمد حكمها إلى البرامج والبيانات المخزنة في أنظمة المعالجة الآلية للمعطيات، وابرز مثال لذلك الفقه الكندي عندما وسع من تفسير المادة487من قانون العقوبات الكندي التي تنص على إمكانية إصدار أمر قضائي لتفتيش أي شيء تتوافر بشأنه أسس أو مبررات معقولة تدعو للاعتقاد بأن الجريمة قد وقعت أو يشتبه فيل وقوعها أو أن هناك نية لاستخدامه في ارتكاب جريمة أو انه سيتيح دليلا على ارتكاب الجريمة. وهكذا فإن هذا النص يفسر على أنه يسمح بضبط وبتفتيش البيانات وبرامج الحاسب الآلي.[1]

وفي هذا المعنى نجد المادة251 من قانون الإجراءات الجزائية اليوناني تعطي سلطات التحقيق إمكانية القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، ويفسر الفقه اليوناني أن عبارة أي شيء تشمل تفتيش البرامج والبيانات المعالجة الالكترونية.

وعلى النقيض يرى أنه إذا كانت الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة فإن هذا المفهوم المادي لا ينطبق على برامج وبيانات الحاسب الآلي غير محسوسة، ويقترح هذا الرأي في مواجهة هذا القصور التشريعي ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة (مواد معالجة الكترونية)،ولذلك تصبح الغاية الجديدة من التفتيش بعد هذا التطور التقني الحديث هي البحث عن الأدلة أو أي مادة معالجة بواسطة الحاسب الآلي.

والحقيقة أن الحاجة ماسة لتدخل تشريعي لتقرير الضوابط القانونية الكفيلة لتغلب على الصعوبات الإجرائية التي تثار عند تفتيش الأنظمة المعلوماتية، ففي الولايات المتحدة الأمريكية تم تعديل المادة34من قانون الإجراءات الجنائية الفيدرالية عام1970

[1] كامل عفيفي، المرجع السابق، ص366.

لتنص على السماح بتفتيش أجهزة الكمبيوتر والكشف عن الوسائط الالكترونية،كما نص المشرع الانجليزي في القسم الثاني من قانون إساءة استخدام الكمبيوتر الصادر عام 1990 على تفتيش نظم الحاسب الآلي جرائم الولوج غير المصرح به على أنظمة الحاسب الآلي، والتعديل غير المرخص به في نظام الحاسب الآلي بدون إذن طالما كان هدف هذا الدخول ارتكاب أفعال غير مشروعة عن قصد، أما إذا كان الدخول مجرد دون نية لارتكاب أفعال غير مشروعة فإن التفتيش ممكن ولكن دون إذن قضائي.[1]

كما قرر المشرع الجزائري بموجب المادة45 من القانون رقم 22/06المؤرخ في 20ديسمبر 2006، التفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقرر له بعض الضوابط والقواعد سنراها لاحقا.

زيادة على ذلك فإن المشرع في بعض الدول الأخرى لجأ إلى تقرير بعض القواعد القانونية بغية التغلب على الصعوبات التي قد تثار عند تفتيش الأنظمة المعلوماتية، وشاركه في ذلك الفقه، ومن تلك التشريعات التشريع الهولندي الذي أجاز في المادة25/أ منه للقائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيد بالحصول على إذن مسبق بذلك من قاضي التحقيق وهذا لتذليل الصعوبة الخاصة بوجود النهاية الطرفية للنظام المعلوماتي في منزل أخر غير منزل المتهم، كما أجاز بموجب المادة25منه إلزام غير المتهم كالشاهد والشخص القائم بالتشغيل القائم بتقديم كافة البيانات والمعلومات اللازمة لدخول نظام الحاسب الآلي والتعامل مع سلطة التحقيق في هذا الصدد، وأيضا اتجه المشرع الجزائري بموجب القانون السالف الذكر إلى وضع ضوابط للتفتيش في الجرائم المعلوماتية.[2]

2_ ضوابط تفتيش نظم الحاسب الآلي

[1] كامل عفيفي، المرجع السابق، ص 367.

[2] عبد الله الهلالي، المرجع السابق، ص75.

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات، بيد أن تحقيق تلك الغاية لا يكون بأي ثمن، ففي كل الحالات فإن الغاية لا تبرر الوسيلة، فالبحث عن الحقيقة القضائية لا ينبغي أن يكون طليقا من كل قيد، بل إن ذلك يخضع لضوابط معينة، ومن هذا المنطلق يجب أن يخضع التفتيش لضوابط يمكن تقسيمها إلى ضوابط موضوعية وضوابط شكلية:

أ/الضوابط الموضوعية

تنحصر هذه الضوابط فيما يلي:

1/وقوع جريمة معلوماتية: والجريمة المعلوماتية هي كما سبق القول كل فعل غير مشروع يكون الحاسوب الآلي وسيلته أو محله وذلك لتحقيق أغراض غير مشروعة، وهناك العديد من التشريعات التي حرصت على استحداث نص خاص للجريمة المعلوماتية كما هو الحال بالنسبة لإنجلترا التي أصدرت قانون إساءة استخدام الكمبيوتر في 29يونيو1990، وفي فرنسا صدر قانون رقم19/88في 5يناير1988 وهو خاص بالغش المعلوماتي الذي تم تعديله مع صدور القانون العقوبات الفرنسي الجديد الذي بدأ العمل به اعتبارا من أول مارس 1994.

2/اتهام شخص أو أشخاص معينين بارتكاب الجريمة المعلوماتية أو المشاركة فيها: فينبغي أن يتوفر في حق الشخص المراد تفتيشه دلائل كافية تدعو إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية، سواء بصفته فاعلا أو شريكا، بحيث أنه إذا لم تتوافر هذه الدلائل كان على قاضي التحقيق أن يصدر أمر بأن لا وجه للمتابعة، وهذا ما تؤكده المادة 163من قانون الإجراءات الجزائية الجزائري[1] والمادة177من قانون الإجراءات الجزائية الفرنسي.

[1]تنص المادة 163 من قانون الإجراءات الجزائية الجزائري على ما يلي:" إذا رأى قاضي التحقيق أن الوقائع لا تكون جنحة أو جناية أو مخالفة أو أنه لا توجد دلائل كافية ضد المتهم أو أن مقترف الجريمة ما يزال مجهولا، أصدر أمر بألا وجه لمتابعة المتهم.

وفي مجال المعلوماتية يمكن القول أن تعبير الدلائل الكافية يقصد به مجموعة المظاهر والدلائل التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة القائم بالتفتيش والتي تنسب الجريمة المعلوماتية إلى شخص معين سواء بصفته فاعلا أو شريكا.[2]

3/توافر قرائن على وجود أشياء لدى المتهم المعلوماتي أو غيره تفيد في كشف الحقيقة: فلا يكفي مجرد وقوع جناية أو جنحة بل يجب أن تتوافر قرائن قوية على وجود أشياء تفيد كشف الحقيقة،ويستوي أن تكون هذه الأشياء المعلوماتية موجودة في حيازة الشخص أو في منزله.

وهكذا فإن التفتيش لا يجري إلا إذا توافرت لذا المحقق أسباب كافية على أنه يوجد في المكان أو لدى الشخص المراد تفتيشه أدوات استعملت في الجريمة المعلوماتية أو أشياء المتحصلة منها أو أية أشياء أخرى أو مستندات الكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم المعلوماتي أو غيره.

4/إجراء التفتيش لنظم الحاسوب الآلي من قبل سلطة مختصة بالتحقيق:

يجب أن يقوم بتفتيش نظم الحاسوب الآلي سلطة مختصة بالتحقيق، وقد جعل المشرع المصري الاختصاص بالتفتيش كإجراء التحقيق في الجرائم التقليدية للنيابة العامة بصفة أصلية ولقاضي التحقيق في حالات خاصة وذلك على خلاف التشريع الفرنسي والجزائري الذين أناطا الاختصاص الأصيل بقاضي التحقيق، أما النيابة العامة فلا تختص بالتفتيش إلا في حالات معينة كالتلبس، أما انجلترا فإن معظم الإجراءات الجنائية منوطة بالشرطة القضائية ما عدا بعض الجرائم التي تناط بالمدعي العام.[1]

ب/الضوابط الشكلية

[2] أمال قارة، المرجع السابق، ص59.

[1] عبد الله الهلالي، المرجع السابق، ص76.

بالإضافة إلى الضمانات الموضوعية لتفتيش نظم الحاسب الآلي، توجد ضمانات شكلية يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريات الفردية من التعسف أو الانحراف من استخدام السلطة وهي كالتالي:

1/الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش الخاص بنظم الحاسوب الآلي:

والهدف من ذلك ضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط، وقد استوجب المشرع الجزائري في المادة 1/45أن يتم التفتيش في حضور صاحب المسكن الذي يجري فيه التفتيش وكذلك المشرع الفرنسي استوجب في الفقرة الأولى من المادة57من قانون الإجراءات الجنائية حضور صاحب المسكن الذي يجري فيه التفتيش وعدم حضوره يترتب عليه البطلان للتفتيش.

غير أن المشرع الجزائري بموجب المادة45من القانون رقم22/06المؤرخ في 20ديسمبر2006استثنى إجراء الحضور لبعض الأشخاص، إذا تعلق الأمر بالتفتيش في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، لكنه اوجب الحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات، لكن إذا تعلق التفتيش بمسكن موقوف صاحبه للنظر أو محبوس في مكان أخر أوجب المشرع بموجب المادة 47 حضور شاهدين مسخرين أو بحضور ممثل يعينه صاحب المسكن محل التفتيش.

2/محضر تفتيش نظم الحاسب الآلي :

فإن التفتيش من أعمال التحقيق فينبغي تحرير محضر به يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ولم يتطلب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنه لا يشترط لصحته سواء ما تستوجبه القواعد العامة في المحاضر عموما والتي تقضي بأن يكون المحضر مكتوب باللغة الرسمية وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها.[1]

[1] عبد الله الهلالي، المرجع السابق،ص77.

3/الميقات الزمني لإجراء تفتيش نظم الحاسوب الآلي:

حرصا على عدم التضييق من نطاق الاعتداء على الحرية الفردية وحرمة المسكن حرصت التشريعات الإجرائية على حضر القيام بتفتيش المنازل وما في حكمها في وقت معين، فالقانون الفرنسي ينص في المادة 59 من قانون الإجراءات الجزائية على أن التفتيش لا يمكن أن يبدأ قبل الساعة السادسة صباحا وبعد التاسعة مساءا، ولقد أخذت بعض التشريعات العربية بمبدأ عدم جواز تفتيش المنازل ليلا كقانون التونسي والجزائري، أما بالنسبة لتشريعات الدول الانجلسكسونية كالقانون الانجليزي والأمريكي فإنها لا تقيد التفتيش بوقت معين.

لكن المشرع الجزائري بموجب المادة47 من قانون الإجراءات الجزائية الجزائري قرر إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات الليل والنهار أو الليل وفي كل محل سكني وغير سكني، بناء على إذن مسبق من وكيل الجمهورية المختص، إلا أنه أوجب الحفاظ على السر المهني.

4/أن يتم التفتيش بناءا على إذن مكتوب: إذا نصت المادة 44 من قانون الإجراءات الجزائية الجزائري على ضرورة أن يكون التفتيش بناءا على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا إذن قبل الدخول إلى المكان والشروع في تفتيش نظم الحاسوب الآلي.

إن التفتيش لنظم الحاسوب الآلي يتطلب مذكرة قضائية تجيز تفتيش أنظمة الكمبيوتر، فإجراء التفتيش دون تلك المذكرة مسالة تثير الكثير من المعارضة خاصة في ظل ما يتقرر من قواعد تحمي الخصوصية وتحمي حقوق الأفراد. ويجب أن تكون المذكرة واضحة في تحديد النظام محل التفتيش.[1]

ثانيا/الضبط في مجال الجريمة المعلوماتية

[1] أمال قارة، المرجع السابق، ص62.

منح المشرع في المادة 63[2]صلاحية القيام بالتحقيقات الابتدائية لأعوان الضبطية القضائية بشرط أن تكون تحت رقابة ضباط الشرطة القضائية.

1_ فيما يخص التوقيف للنظر.

إن التحقيق الابتدائي في الجرائم الخطيرة المذكورة في المادة16 من قانون الإجراءات الجزائية أصبح عسيرا وصعبا، خاصة وأن مرتكبي هذه الجرائم أصبحوا يستعملون أساليب متعددة، وحديثة و معقدة.

وأصبحت مدة الوضع تحت النظر لا تتماشى ومتطلبات التحقيق الأولي، مما جعل المـــشرع الجزائري يعدلها بالمادة51 والتي نصت على انه:

«يمكن تمديد أجال التوقيف للنظر بإذن مكتوب من وكيل الجمهورية المختص:

-مرة واحدة عندما يتعلق الأمر بجرائم الاعتداء على أنظمة المعالجة الآلية للمعـــــــــــــــــــــــــــــــــطيات.»

نلاحظ أن المشرع ربط تجديد مدة التوقيف للنظر بطبيعة الجريمة موضوع التحري واشترط أن يكون تمديد المدة بإذن مكتوب من وكيل الجمهورية وأثناء التحقيق الابتدائي كثيرا ما يقوم ضباط الشرطة القضائية باستدعاء أشخاص لإجراء التحقيق، إلا أنهم لا يمتثلون للإستدعاءات الواردة إليهم مما يقلص من فعالية وسرعة التحقيق لذا استوجب الترخيص لرجال الضبطية القضائية استعمال القوة لإحضارهم.

2_ استعمال القوة لإحضار الأشخاص.

جاء بالمادة 65الفقرة1[1] أنه يجوز لضباط الشرطة القضائية بعد الحصول على إذن مسبق من وكيل الجمهورية المختص أن يستخدم القوة العمومية لإحضار الأشخاص الذين لم يستجيبوا لاستدعائين للمثول.

---

[2] تنص المادة 63 من قانون الإجراءات الجزائية الجزائري على ما يلي:"يقوم ضباط الشرطة القضائية وتحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الابتدائية بمجرد علمهم بوقوع الجريمة إما بناء على تعليمات وكيل الجمهورية وإما من تلقاء نفسه"

[1] تنص الماد 1/65من قانون الإجراءات الجزائية الجزائري على ما يلي:"إذا دعت مقتضيات التحقيق الابتدائي ضابط الشرطة القضائية إلى أن يوقف للنظر شخصا مدة تزيد عن 48 ساعة فإنه يتعين عليه أن يقدم ذلك الشخص قبل انقضاء هذا الأجل إلى وكيل الجمهورية"

هذه المادة تتيح استعمال القوة لإحضار الأشخاص أمام الضبطية القضائية لأخذ أقوالهم بشرط أن يكون إحضارهم بترخيص من وكيل الجمهورية المختص، ولا يمكن إبقاؤهم في حالة التوقيف إلا للمدة اللازمة لأخذ أقوالهم بشرط أن يكون قد تم استدعائهم مرتين على الأقل ولم يمتثلوا.

حتى يحقق التفتيش غايته في جمع الأدلة الإجرامية لا بد من وسيلة التقاط تلك الأدلة،وهذه الوسيلة هي الضبط،والضبط في معظم الأحيان يكون هو غرض التفتيش وإن لم يكن هو السبب الأوحد له فقد يأتي الضبط لأسباب أخرى غير التفتيش مثل المعاينة.

ويقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها وهو من حيث الطبيعة القانونية من إجراءات الاستدلال أو التحقيق، وتتحدد طبيعته بحسب الطريقة التي تم فيها وضع اليد على الشيء المضبوط، فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة استدلال.[1]

وإذا كانت الجرائم الواقعة على المكونات المادية للحاسوب الآلي لا يثير صعوبة للتقرير بصلاحية هذه الجرائم لضبط أدلتها، ذلك أن الضبط لا يرد بحسب الأصل إلا على أشياء مادية، إلا أن الأمر بالنســـــبة للجرائم الواقعة على المكونات المعنوية للحاسوب الآلي، يثير مشاكل بالنسبة لضبط أدلتها. وقد اختلف الفقهاء بين مؤيد ومعارض. ونجد المشرع الجزائري قد أجاز بموجب المادة 47الضبط أو الحجز في مجال الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في محل سكني أو غير سكني، وفي ساعة من ساعات النهار أو الليل بإذن مسبق من وكيل الجمهورية.

ومن اجل ضبط أدلة الجريمة فإن المشرع الجزائري بموجب مواد65مكررالى 65مكرر 10 أجاز اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، إذا

[1] حجازي عبد الفتاح بيومي، المرجع السابق، ص162.

اقتضت ذلك ضرورة التحقيق الابتدائي بإذن من قاضي التحقيق لمدة أربعة أشهر قابلة للتجديد، وتنفذ العمليات المأذون بها تحت مراقبة مباشرة لقاضي التحقيق، وتتم العمليات المحددة دون المساس بالسر المهني المنصوص عليه في المادة45.

ويبقى أن نتساءل عما إذ يجوز لضباط الشرطة القضائية الاطلاع على محتويات الحاسوب الآلي التي يتم ضبطها.

أجاب القسم110من قانون الإجراءات الجنائية الألماني على هذا التساؤل بقوله إن سلطة الاطلاع على مطبوعات الحاسوب الآلي وحاملات البيانات الأخرى تقتصر على المدعي العام فقط ولا يكون ضباط الشرطة القضائية الحق في قراءة البيانات عن طريق تشغيل البرامج أو الوصول إلى ملفات البيانات المخزونة دون إذن الشخص الذي له حق نقل هذه البيانات لكل ما لهم هو مجرد فحص حاملات البيانات والبرامج دون استخدام أية مساعدات فنية.[1]

وإذا كان الأمر يبدو محسوما من الناحية النظرية في بعض التشريعات التي قالت بصلاحية البرامج ومعلومات وبيانات الحاسوب الآلي للضبط، إلا أن المسالة عند التطبيق تأخذ بعد أخر، إذ لا يمكن ضبط مكونات الحاسوب الآلي المعنوية بعد تفتيشها إلا إذا نقلت من صورتها المعنوية إلى صورتها المادية، فلا بد من حصرها وجمعها في حيز مادي، ويتم ذلك بإخراجها على الورق أو بأخذ تسجيل منها أو جمعها على أقراص مرنة أو ممغنطة.

إلا أن السؤال الذي يطرح نفسه، إلى أي حد يمكن اعتبار هذه المخرجات بصورتها المختلفة مستندات تصلح أن تكون أدلة إثبات مقبولة أمام القضاء؟

القاعدة في الدعاوى الجزائية هي جواز الإثبات بكافة طرق الإثبات القانونية، والقيد على هذه القاعدة أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الالكترونية خاصة مع احتمال ظهور أنشطة إجرامية عديدة.

[1] حجازي عبد الفتاح بيومي، المرجع السابق، ص163.

والمعلومات إن كانت قيمتها تتجاوز شيئا فشيئا الموجودات والطاقة فإنها ليست من الماديات لتقبل بينة في الإثبات إلا أن الاتجاه الحديث لم يعد يقف عند المفهوم المحدود للمستندات، بل تطور بحيث أصبح يقبل بمخرجات الحاسوب الآلي سواء كانت على شكل مخرجات ورقية أو صور أو تسجيلات كدليل إثبات،إذ اعترف الفقه والقضاء الجنائيين في فرنسا بمخرجات الحاسوب الآلي سواء كانت مخرجات ورقية أو الكترونية كالأشرطة المغنطيسية وغيرها من الأشكال الالكترونية الأخرى بأن لها قيمة دلائل الإثبات،وبالتالي تصلح كأدلة إثبات أمام القضاء الجنائي،لاسيما وأن التعديل المدخل على قانون العقوبات الفرنسي بمقتضى القانون08يناير 1988لم يتضمن ما يخالف وجهة النظر هذه.[1]

المطلب الثاني

المكافحة الإجرائية في القانون الجزائري

اقتدى المشرع الجزائري بالمشرعين الذين سبقوه، فسارع لمواكبة هذا التطور الذي لحق الجريمة بمكافحتها من الناحية الإجرائية وذلك بتعديل بعض المواد في قانون الإجراءات الجزائية وإصدار قوانين خاصة وجديدة في مجال الإجراءات.

الفرع الأول

المكافحة الإجرائية في القانون 04/09

نظم المشرع الجزائري في القانون رقم 04/09 المؤرخ في 05أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، أحكاما جديدة وخاصة بمعالجة الجريمة المعلوماتية تتماشى والتطور الذي لحق بهذه الجريمة، من هذه القواعد ما نص عليه في المادة الثالثة منه التي تضمنت

[1] حجازي عبد الفتاح بيومي، المرجع السابق، ص164.

الإجراءات الجديدة التي تتطلبها التحريات والتحقيقات القضائية من ترتيبات تقنية،[2] الهدف منها هو:

- مراقبة الاتصالات الإلكترونية وتجميعها، حيث نجد أن المشرع الجزائري قد تبنى هذا الإجراء رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها بنص المادة 39 من الدستور الجزائري نظرا لخطورة بعض الجرائم المعلوماتية المحددة حصرا.
- تسجيل الاتصالات الإلكترونية في حينها.
- القيام بإجراءات التفتيش والحجز للمنظومة المعلوماتية.

كما يبين القانون 04/09 في مادته الرابعة الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية وذلك على سبيل الحصر وهذه الحالات هي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الالكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة تنص المادة16 من القانون 04/09 على إمكانية تبادل المساعدات القضائية على المستوى الدولي لنجاح عمليات التحقيق والتحريات لمكافحة الجرائم المعلوماتية.[1]

كما أن المادة18 من القانون04/09 قد بينت الحالات التي لا تجوز فيها عملية المساعدة القضائية الدولية وحددتها بالحالات التالية:

- إذا كان فيها مساس بالسيادة الوطنية.

[2] هلالي عبد الله أحمد، المرجع السابق، ص121.

[1] طرشي نورة، المرجع السابق، ص130.

- إذا كان فيها مساس بالنظام العام.

أما المادة الخامسة من القانون 04/09 فهي تبين إجراءات التفتيش للمنظومة المعلوماتية يقصد بالتفتيش في مجال الجرائم المعلوماتية هو التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وان اختلف مضمونه عن التفتيش العادي بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة45 من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

غير أن القانون 04/09 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات التي يحتوي عليه هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها.[1]

كما نص المشرع الجزائري في الفقرة الأخيرة من المادة الخامسة من القانون04/09 على إجراء أخر يسهل عملية التفتيش وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسبات لإجراء عمليات التفتيش على المنظومة المعلوماتية، وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات.

كما ألزمت المادة العاشرة من القانون04/09 مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش وحفظ المعلومات طبقا للمادة 11 من نفس القانون التي من شأنها تمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب في المادة 12 على مقدمي الخدمات التزامات خاصة هي:

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.

[1] طرشي نورة، المرجع السابق، ص131.

- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجودها.[2]

الفرع الثاني

المكافحة الإجرائية في قانون الإجراءات الجزائية

سارع المشرع الجزائري بتعديل قانون الإجراءات الجزائية تماشيا مع التطور المعلوماتي الذي لحق بالجريمة، محاولة منه الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث أنه بتعديلي 09/01 و14/04 وضع قواعد وأحكام خاصة لسلطة المتابعة والاختصاص، الغرض منها هو مواجهتها،[1] وهذه الأحكام هي:

- **جواز تمديد الاختصاص المحلي للمحكمة:** حيث نصت المادة 329من قانون الإجراءات الجزائية في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- **توسيع مجال اختصاص النيابة العامة:** حيث أنه بموجب المادة 37من قانون الإجراءات الجزائية تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخصا لها من قبل حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.
- **العمل بنظام المشروعية في تحريك الدعوى العمومية:** حيث سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، حيث يلتزم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون بحيث لا يتمتع بشأنها بسلطة الملائمة بين

[2] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي دار الهدى الجزائر، 2011،،ص155.

[1] طرشي نورة، المرجع السابق، ص134.

تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر،144مكرر1و2 من قانون العقوبات المعدل والمتمم بالقانون09/01 المؤرخ في26 يونيو 2001.

- إضافة لما سبق ودائما في إطار المكافحة الإجرائية للجرائم المعلوماتية تم توسيع مجال اختصاص النيابة العامة في مجال البحث والتحري عن هذه الجرائم بمنح الإذن بالتفتيش والقيام باعتراض المراسلات وتسجيل الأصوات والتقاط الصور حسب نص المادة 65 مكرر5 في إطار تعديل قانون الإجراءات الجزائية بالقانون 22/06 المؤرخ في 2006/12/20

- **التسرب:** إضافة لما سبق تجدر الإشارة إلى الإجراء الجديد الخاص بمكافحة الجرائم المعلوماتية والمنصوص عليه في المادة 65 مكرر11 من قانون الإجراءات الجزائية، وهو إجراء التسرب فتنص المادة 65 مكرر11 على أنه"**عندما تنقضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر5، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد 65مكرر12 و65مكرر18من قانون الإجراءات الجزائية.**"

وقد عرفت المادة 65مكرر12 التسرب على أنه "**قيام ضابط أو عون 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**"

كما سمحت الفقرة الثانية من المادة 65مكرر12 أن يستعمل لغرض إجراء التسرب هوية مستعارة أو أن يرتكب عند الضرورة الأفعال المنصوص عليها في المادة 65مكرر14 وهذه الأفعال هي:

- اقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

ويمكن للمتسرب بإتيان هذه الأفعال دون أن تترتب عليه المسؤولية الجزائية لأنه مرخص له بهذه الأفعال بهدف الوصول إلى مرتكبي الجريمة.[1]

وقد بينت المادة 65مكرر15 الشروط الواجب توفرها في الإذن بالتسرب، وهي أن يكون مكتوبا ومسببا وأن يذكر فيه الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته.

كما يجب أن يحدد في الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر كما أجازت المادة 65مكرر15 كإجراء جديد في مكافحة الجريمة المعلوماتية اعتبار ضابط الشرطة القضائية الذي جرت عملية التسرب تحت مسؤوليته كشاهد عن العملية في إجراءات التحقيق فيها.[1]

[1] طرشي نورة، المرجع السابق، ص135.

[1] طرشي نورة، المرجع السابق، ص137.

خاتمة

لقد بات من المحتم على دول العالم مواكبة التطور التكنولوجي الحاصل في العالم الافتراضي الجديد الذي صارت المعلومة فيه سيدة دون منازع ومصدرا للقوة، المعرفة، السلطة والمال، بل وأكثر من هذا صارت معيارا لتطور الشعوب ونموها.

وإزاء التطور العلمي الهائل فإن مزايا المعلوماتية جلبت معها أيضا مخاطر جمة طوعها المجرم المعلوماتي وصارت سلاحا لا يستهان به لممارسة نشاطاته الإجرامية وبهذا ظهرت طائفة جديدة من الجرائم المستحدثة، إضافة إلى إمكانية ارتكاب الجرائم التقليدية بطريقة حديثة، وباتت القوانين الجزائية، الموضوعية منها والإجرائية قاصرة عن مواجهة الجرائم المرتكبة باستخدام الحاسب الآلي.

والملاحظ من خلال بحثنا هذا نظرا لنقص المراجع في هذا الميدان، الصعوبات القانونية التي تواجه رجل القانون، خاصة القاضي في تطبيق النصوص الجزائية التقليدية خاصة فيما يتعلق بطبيعة المال المعلوماتي باعتباره مالا معنويا في حين الحماية الجزائية في أغلب الدول يقتصر على المال المادي إضافة إلى تكييف المنقول، وما تعلق بمفهوم الاختلاس كل هذا وغيره بحاجة إلى مراجعة تشريعية شاملة لسد الفراغ التشريعي بما يتناسب ومبدأ الشرعية.

ثم تبين لنا من خلال دراسة الفصل الثاني لهذا البحث قصور قواعد الإجراءات الجزائية في مواجهة الإجرام المعلوماتي، كفشلها في مجال الضبط والتحري، التحقيق، تفتيش النظام المعلوماتي استنباط الأدلة وإثبات الجريمة المعلوماتية وصعوبة إثبات الجرائم الالكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها، إذ قد يكون هذا الدليل غير مرئي وقد يسهل إخفاؤه أو تدميره، وقد يكون متصلا بدول أخرى فتكون هناك صعوبة للحصول عليه نظرا لتمسك كل دولة بسيادتها. كما وأن هذا الإثبات قد يحتاج إلى معرفة علمية وفنية قد لا تتوافر لضباط الشرطة القضائية والقضاة.

وهكذا حاولنا من خلال هذا البحث معالجة إشكالية تطبيق النصوص التقليدية والمستحدثة في مجال الجريمة المعلوماتية وصعوبة إثبات الجرائم التي تقع على العمليات الالكترونية، وقد توصل البحث بنا من خلال هذه الدراسة إلى النتائج التالية:

1. أظهر البحث أن هناك قصورا واضحا في الكثير من التشـــريعات الموضـــوعية والإجرائية في مواجهة ظاهرة الجريمة المعلوماتية، فمازال الكثير من هذه الجرائم تخضع للنصوص التقليدية وهو ما يترتب عليه الاعتداء على مبدأ الشرعية من جهـــة أو إفـــلات الكثير من الجناة من العقاب.

2. أظهر البحث كذلك أنه رغم التدخل التشريعي الموضوعي إلا أن هناك قصـــورا في التشريعات الإجرائية، ذلك أنه ما يزال يقف في حمايته للحرية الشخصـــية وحرمـــة الحياة الخاصة من الوسائل الالكترونية متجاهلا بذلك الإجراءات الضـــرورية للحصـــول على الدليل في الجريمة المعلوماتية ومعتمدا دائما على الإجراءات التقليدية، خاصة منهـــا التفتيش والخبرة.

3. أظهر البحث كذلك أن هناك صعوبة تكتنف الدليل بالنسبة للجريمـــة المعلوماتيـــة سواء من حيث طرق الحصول عليه أو من حيث طبيعته، فالحصول عليه قد يحتاج إلـــى عمليات فنية وعلمية وحسابية معقدة، كما أن طبيعته قد تكون غيـــر مرئيـــة، كالذبـــذبات والنبضات، وأنه من السهولة استخدام التقنية العلمية في إخفائه أو إتلافه وقد يتم ذلك عن طريق التشفير وكلمات المرور السرية واستخدام الفيروسات المدمرة.

4. أظهر البحث كذلك تأثر قانون الإجراءات الجزائية في إثبات المســـائل المتعلقـــة بالجريمة المعلوماتية وقوانين غير عقابية كالقانون التجاري والقـــانون المـــدني بظهـــور الشيكات الالكترونية والمحررات الالكترونية فيكون إثباتها بذلك مع الأدلة التي تتفق مـــع طبيعتها وعليه توجب تطوير هذه التشريعات الأخيرة غير العقابية كي تتســـع نصوصـــها لهذه العمليات الالكترونية وتتجاوب مع الثورة الرقمية التي نعيشها اليوم

<u>وعلى ضوء هذه النتائج فإن البحث قد توصل إلى التوصيات التالية:</u>

1. يجب أن يتلاءم تعريف الجريمة المعلوماتية مع فكرة عالميـــة المعلومـــات والاتصالات، بحيث يكون متفقا عليه على المستوى العالمي خاصـــة مراعـــاة التطـــور التكنولوجي الحاصل يوما عن يوم، ويجب توضيح الدور الذي يقوم به الحاسب الآلي في ارتكاب الجريمة.

2. ضرورة إيجاد قاعدة تعاون دولي فيما يتعلق بالجريمة المعلوماتية للتوفيق بين التشريعات الخاصة بهذه الجرائم.

3. ضرورة تدخل تشريعي لحماية المعلومات والبيانات بنصوص خاصة فلا يكفي التوسع من نطاق تطبيق النصوص التقليدية حتى لا يصطدم القاضي بمبدأ الشرعية ويجد نفسه أمام أفعال وسلوكات غير مجرمة فيفلت فاعلوها من العقاب، رغم أن العديد من الدول كفرنسا والو.م.أ وكندا أصدرت تشريعات تتعلق بمكافحة الجريمة المعلوماتية، إلا أن هذه التشريعات لا يمكن اعتبارها جامعة مانعة.

4. ضرورة التنسيق فيما يتعلق بالإجراءات الجزائية المتبعة في شأن الجريمة المعلوماتية بين الدول مختلفة خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق، سيما وأن الحصول على الدليل في مثل هذه الجرائم خارج نطاق الدولة عن طريق التفتيش في نظام معلوماتي معين هو في غاية الصعوبة، فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته.

5. تخصيص وحدات أمنية لديها الإلمام الكافي بتقنيات الحاسب، وذلك لا يتأتى إلا من خلال تكوين فرق وتعليمهم مبادئ وعلوم الحاسب الآلي وكيفية التعامل مع هذه الأجهزة في الضبط والتحري عن هذه الجرائم، وتطوير وسائل البحث.

6. ضرورة استحداث نصوص قانونية جديدة خاصة في قانون الإجراءات الجزائية، حتى تتلاءم في مجال الضبط والتحقيق لعدم ملائمة الإجراءات التقليدية في مواجهة هذه الجرائم إضافة إلى تحديث الأساليب الإجرائية المتبعة في الجرائم المعلوماتية، دون أن تتعرض حقوق الأفراد وحرياتهم للخطر عند الإثبات في مجالها.

7. تأهيل القضاة وتكوينهم في مجال الجرائم المعلوماتية حتى يتسنى له الإلمام بكافة النصوص والإجراءات المتبعة في هذا النوع من الجرائم، خاصة في الأحكام المستحدثة وتنشيط دورات تكوينية مستمرة من قبل خبراء وقانونيين باعتبار أن هذا يؤثر على العدالة بصفة مباشرة.

قائمة المراجع

أولا/الكتب.

1_أحسن بوسقيعة، الوجيز في القانون الجزائي، الطبعة السادسة، دار هومة، الجزائر،.2007.

2_أسامة احمد المناعسة،جرائم الحاسب الآلي والانترنت،دار وائل للنشر،الاردن2004.

3_أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة للطباعة والنشر، الجزائر، 2006.

4_أمير فرج يوسف، الجرائم المعلوماتية،

5_زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011.

6_صلاح سالم، تكنولوجيا المعلومات والاتصالات والأمن القومي للمجتمع، الطبعة الأولى،2003.

7_عبد الله الهلالي، تفتيش نظام الحاسب الآلي وضمانات متهم المعلومات، دراسة مقارنة، الطبعة الأولى، القاهرة، دار النهضة العربية.

8_عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي، مصر، 2006.

9_علي عبد القادر القهوجي،الحماية الجنائية لبرامج الحاسب الآلي،الدار الجامعية للطباعة والنشر،الاسكندرية، 1999.

10_كامل عفيفي، جرائم الكمبيوتر، لبنان، منشورات الحلبي، الحقوقية، 2003.

11_محمد حسنين، الوجيز في الملكية الفكرية، المؤسسة الوطنية للكتاب، الجزائر1985

ثانيا/المذكرات.

1_ إبراهيمي سهام، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2004، 2007.

2_ حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2005_2006.

3_ طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير، في القانون الجنائي، جامعة الجزائر1، كلية الحقوق، 2012،2011.

4_ قربوز حليمة، الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006_2009.

5_ مرزوق نسيمة، جرائم الانترنت، مذكرة التخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006، 2009.

ثالثا/البحوث والمقالات.

1_نائلة عادل محمد فريد قورة -جرائم الحاسب الآلي الاقتصادية دراسة نظرية و تطبيقية- منشورات الحاتي الحقوقية 2005.

2_فايز بن عبد الله الشهري، التحديات الأمنية المصاحبة لوسائل الاتصال الجديدة دراسة وصفية تأصيلية للظاهرة الإجرامية على شبكة الإنترنيت، الدليل الإلكتروني للقانون العربي.

3_عرب يونس، جرائم الكمبيوتر والانترنت،ورقة عمل مقدمة إلى مؤتمر الأمنالعربي،2002.

4_محمد الأمين البشري: التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون بجامعة.

رابعا/النصوص القانونية

1_القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 07 لـــ 2009.

2_أمر رقم 156/66 المؤرخ في 18 صفر 1386 الموافق لـــ08 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم، الجريدة الرسمية العدد 47.

3_أمر رقم 155/66 المؤرخ في 18 صفر1386 الموافق لـــ08 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم، الجريدة الرسمية العدد 47.

4_القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر 156/66 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات (ج ر 71 بتاريخ 2004/11/10).

5_أمر رقم 07/03 المؤرخ في 2003/07/19 المتعلق ببراءة الاختراع، الجريدة الرسمية العدد 44 لسنة 2003.

6_أمر رقم 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد 44 لسنة 2003.

خامسا/المراجع باللغة الأجنبية

1. G.Delmare, sécurité informatique Ressource informatique N° 1 juillet
2. Parker (Donn B) Figding computer crime A neur Framework for protecting information 1998
3. Rose Philippe la criminalité informatique que sais je 1er édition PU 1988
4. Suthreland (Eduin H) "White collar criminality» Gers (Gilbert) in white collar criminal the offender in business the professions Atherton press 1968

سادسا/المواقع الالكترونية

1_ موقع منظمة التعاون الاقتصادي والتنمية www.oecd.org

2_ موقع الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبيةwww.jordap.dz

الفهرس