خصوصية الجريمة الالكترونية
وجهود المشرع الجزائري في مواجهتها

محمد خليفة – أستاذ جامعي
الرتبة: أستاذ مساعد قسم " أ"
الاختصاص: القانون الجنائي المعلوماتي
كلية الحقوق والآداب والعلوم الاجتماعية– جامعة 08 ماي 45 قالمة

مقدمة:

لاشك أن المعلوماتية غزت كل مجال من مجالات الحياة، ، وقد عادت بالخير الكبير عليها، إذ طبعت الكثير من المعاملات بالسير والسهولة والسرعة، لكن وإن كان هذا هو الجانب المشرق للمعلوماتية فإن لها جانبا مظلما أفرزه استعمالها لأغراض غير مشروعة، فقد استغل البعض هذه المعلوماتية للاعتداء على أموال الناس وعلى مصالحهم، وهذا ما شكل ما يسمى بالجرائم المعلوماتية أو الالكترونية. وما يلاحظ على هذه الجرائم أنها تتميز بالعديد من الخصائص التي تميزها عن الجرائم التقليدية.

ويمكننا تعريف هذه الجرائم بأنها كل عدوان على المعطيات (المعلوماتية أو الالكترونية) ، في سريتها أو في موفوريتها أو في سلامتها وتكاملها، وذلك بالإطلاع غير المشروع عليها أو حذفها أو تغييرها أو إدخال معطيات أخرى عليها، أو تعطيل أنظمة معالجتها، " فالجرائم المعلوماتية أو الالكترونية إنما تقع على المعطيات أو البيانات الموجودة داخل أنظمة المعالجة الآلية للمعطيات، وقد عرف مجلس الشيوخ الفرنسي نظام المعالجة الآلية للمعطيات بأنه كل مجموع يتركب من واحدة أو أكثر من: وحدات المعالجة، من ذاكرة، برامج، معطيات، أجهزة إدخال وإخراج، روابط تؤدي إلى نتيجة محددة..."(1).

وهذا التعريف واسع لا يقتصر على الأنظمة الموجودة بالحاسبات الآلية، وإنما يشمل كل نظام يحتوي على هذه المكونات المادية وغير المادية، فيدخل فيه مثلا بطاقات الائتمان بما تحويه من معلومات لأن هذه البطاقات جزء من نظام صالح لكي يقرأ ويسجل المعلومات على شريحة عندما يوضع في اتصال معه، كذلك القرص المرن القابل للعزل والنقل والذي يحمل شريحة برامج خاصة تقرأ من جهاز قارئ خاص، هذا القرص يشكل نظاما مع هذا القارئ(2).

وسنتناول في هذا البحث خصائص الجرائم االالكترونية في المبحث الأول وجهود المشرع الجزائري في مواجهتها في المبحث الثاني.

المبحث الأول: خصائص الجرائم الالكترونية:

لا شك أن المعلوماتية عادت علي الإنسان بالخير الكثير، وطبعت مختلف جوانب حياته بطابع لم يكن ليحلم به قبل وقت قريب، فهذا التقدم العلمي الكبير في مجال المعلوماتية يسر حياة الإنسان ووفر عليه جهداً كبيراً وطبع شتى معاملاته بالسرعة الفائقة ، والتي لولا هذا التطور لاستغرقت من الوقت الكثير، كما أن هذه المعلوماتية وفرت علي الإنسان الكثير من المال الذي كان سينفقه في قضاء حاجات أصبح يمكنه أن يقضيها في بيته بكبسة زر، لكن وفي المقابل فقد ارتبط استعمال هذه الوسائل الفنية الحديثة بظهور جرائم جديدة لم تكن معروفة من قبل، كما ارتبط بزيادة في حدة بعض الجرائم التي كانت موجودة من قبل، فهذه التقنية أوجدت ألوانا جديدة من الجرائم طبعتها بطابعها وأسبغت عليها خصائص ميزتها عن غيرها من الجرائم، سواء تعلقت هذه الخصائص بالشخص الذي يقدم علي هذه الجرائم فميزته عن المجرم التقليدي أو تعلقت بالجريمة ذاتها وصعوبة اكتشافها وإثباتها أو ما يلعبه الضحية من دور فيها، أو تعلق الأمر بالنطاق المكاني لهذه الجريمة أو الخسائر التي تخلفها.

المطلب الأول: أنها ترتكب من مجرم غير تقليدي:

يختلف مجرم المعطيات كثيرا عن المجرم في الجرائم التقليدية، ذلك أن له سمات لا يوجد لها مثيل لدى غيره، كما أن له طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لارتكاب الجريمة مختلفة عنده أيضا، فبالنسبة لسمات هذا المجرم فهو إنسان اجتماعي، أي انه متوافق مع مجتمعه وغالبا ما تكون له مكانة معتبرة فيه ويحظى بالاحترام منه، كما أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة بهذه الجريمة، وهذا الاكتساب يتم عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة والاحتكاك بالآخرين، كما أن هذا المجرم إنسان ذكي، إذ أنه يستغل ذكاءه في تنفيذ جريمته، ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا، ويفسر هذا أن هذا المجرم من ذوي المستويات العلمية العالية غالبا.

وما يميز مجرم المعطيات أيضا هي الدوافع التي تدفعه لارتكاب الجريمة، فهي متعددة ومختلفة فقد تكون السعي لتحقيق الربح وقد تكون الرغبة في الانتقام من رب العمل وقد تكون الرغبة في قهر النظام والتفوق علي وسائل التقنية وتعقيدها . وقد يرتبط الدافع بحب التعلم والاستكشاف، كما قد يرتبط بالسياسة والايديولوجيا .. إلى غير ذلك من البواعث.

كما يتميز مجرم المعطيات أيضا بفئاته وأنماطه المختلفة وهو ينقسم إلى نوعين رئيسيين: الأول هم الهواة المولعون بالمعلوماتية، والثاني هم محترفو الجرائم المعلوماتية وأساس التمييز بين النوعين هو الباعث أو الدافع إلى ارتكاب الجريمة، بينما هو ساذج لدى النوع الأول لا يتعدى الرغبة في الاستطلاع والاستكشاف، فهو خبيث لدى النوع الثاني، والذي قد يكون ماليا أو سياسيا أو غيره(3).

المطلب الثاني: صعوبة اكتشاف واثبات الجرائم الالكترونية

من المفترض أن اكتشاف هذه الجرائم يتم عن طريق الفحص والتدقيق أو عن طريق الشكاوي التي يقدمها المجني عليهم، والوضع بخصوص جرائم المعطيات بالغ التعقيد في الأمرين معا، فجهات التحقيق لم تصل إلى تلك المعرفة أو الخبرة التي تملكها حيال التحقيق في الجرائم التقليدية، لأن الأمر يتطلب معرفة واسعة وإحاطة كاملة بهذه التكنولوجيا الحديثة، وتحديث هذه المعارف يوميا، هذا من جهة، ومن جهة أخرى فالضحية في هذه الجرائم تمتنع في الغالب عن التبليغ عنها وقد يسعى إلى التعتيم علي المحققين وتضليلهم حتى لا يكتشفوا هذه الجرائم.

ويفترض إثبات هذه الجرائم الكثير من الصعوبات، فطبيعة هذه الجرائم غير مرئية في الغالب لأنها تتعلق بمعطيات في شكل نبضات أو ذبذبات الكترونية، ويسهل علي الجاني محو الأدلة المتعلقة بها وتدميرها في وقت وجيز، فضلا عن العقبات التي تشكلها طبيعة هذه الجرائم العابرة للحدود.

لهذا لا نعجب إذا وجدنا أن أكثر تلك الجرائم لم تكتشف إلا بمحض الصدفة وهناك من يشير إلى أن هذه الجرائم لم يكتشف منها إلا ما نسبته 01 % فقط وما تم الإبلاغ عنه إلى السلطات المختصة لم يتعد 15 % من النسبة السابقة، وحتى ما طرح أمام القضاء من هذه الجرائم فان أدلة الإدانة فيه لم تكن كافية إلا في حدود الخمس 5/1(4).

المطلب الثالث: الجرائم الالكترونية للضحية دور مهم فيها:

كالمجرم في جرائم المعطيات، فان للضحية أيضا ما يميزها في هذه الجرائم، ذلك أنها تلعب دورا لا يستهان به في أغلبها، هذا الدور قد لا تلعبه الضحية بإرادتها، كما هو الحال عندما تكون شخصيتها غير متجلية أمام الجاني، وذلك عندما لا يرى هذا الأخير أمامه إلا

الحاسبات وما تحويه أنظمتها من معطيات دون أن يدرك قيمتها وما قد تمثله في الواقع، وكذلك الأمر عندما تلعب العلاقة بين الضحية والجاني دورها في حدوث الجريمة وذلك إذا كان الجاني يعمل لحساب الضحية، لاسيما إذا كان عارفا بخبايا أنظمة الحاسبات والثغرات الأمنية فيها، أو كان مؤتمنا علي ذلك، كأن يكون هو المسؤول عن المركز المعلوماتي فيستغل مركز الثقة الذي يجوزه والألفة التي بينه وبين هذه الأنظمة(5) وذلك ما حدث في إحدى القضايا أن كان الجاني يعمل مستشارا لدى أحد البنوك الكبرى وكان يتمتع بثقة مطلقة من جانب هذا البنك مكنته من الدخول في مفتاحين الكترونيين من أصل ثلاثة أساسية للتحكم في التحويلات الإلكترونية للنقود من بنك لآخر، وتمكن بفضل قدراته في هذا المجال من الوصول إلى المفتاح الثالث، لينقل في الحال مبلغ عشرة (10) ملايين دولار إلى حساب بنكي فتح باسمه في سويسرا وقد القى القبض عليه وصدر ضده حكم بالسجن لمدة ست (6) سنوات. وتقدم إحدى الإحصاءات الأرقام التالية: 25 % من أفعال الغش المعلوماتي يرتكبها المحللون Informaticiens و18% يرتكبها المبرمجون، و17 % يرتكبها مستخدمون لهم افكار معلوماتية تتجاوز الدخول في النهايات الطرفية و16 % يرتكبها الصرافون، 12 % يرتكبها أشخاص أجانب عن المنشأة، و11% يرتكبها المشغلون Opérateurs وفي دراسة أجراها مركز الدراسات الاجتماعية والاقتصادية بفرنسا CESE عام 1988 تبين أن حوالي 65 % من الجرائم محل الدراسة ارتكبها عاملون في المؤسسة المجني عليها وكانت النسبة 85 % في دراسة أخرى أجرتها اللجنة المحاسبية بالمملكة المتحدة دامت من عام 1993 إلى 1993 .

المطلب الرابع: الجرائم الالكترونية ناعمة مغرية للمجرمين:

إذا كانت بعض الجرائم التقليدية تحتاج من مرتكبها إلى قوة عضلية لتنفيذها فان جرائم المعطيات لا تحتاج إلى مثل تلك القوة العضلية وإنما تحتاج إلى قوة علمية وقدر من الذكاء ومهارة في توظيف ذلك، والجاني في سبيل تنفيذها لا يحتاج من الوقت إلا ثوان أو دقائق معدودات، ولا يحتاج من القوة العضلية غير تحريك الأنامل من علي وسائل الإدخال وقد يتسبب بذلك في حصول خسائر فادحة رغم أن جريمته قد لا ترى بالعين.

ونعومة هذه الجريمة وما تدره من أرباح ومن إشباع للفضول عند البعض جعلها من الجرائم المغرية والجذابة للمجرمين(6).

المطلب الخامس: الجرائم الالكترونية جرائم عابرة للحدود:

ليس هناك في عالم اليوم حدود تقف حائلا أمام نقل المعطيات بين الحاسبات الآلية الموزعة في مختلف دول العالم عبر شبكات المعلومات فيمكن في بضع دقائق نقل كم هائل من المعطيات بين حاسب وآخر يبعد عنه آلاف الكيلومترات، كما يمكن أن تقع الجريمة من جان في دولة معينة علي مجني عليه في دولة أخرى في وقت يسير جدا مكبدة أفدح الخسائر لاسيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت، خاصة في مجال التجارة الإلكترونية وازدياد اعتماد البنوك عليها.

وتثير الطبيعة الدولية لهذه الجرائم العديد من المشاكل، كمشكلة السيادة والاختصاص القضائي وقبول الأدلة المتحصلة عليها في دولة ما أمام قضاء دولة أخرى(7) وتذكر في هذا المجال قضية RN Thompson وفيها قام مبرمج انجليزي يعمل لدى بنك بالكويت بالتلاعب في معطيات بنظام الحاسب الآلي الخاص بالبنك، وذلك عن طريق الخصم من أرصدة العملاء ثم الإيداع في حسابه الخاص، وبعد عودته لانجلترا طلب من البنك تحويل

الحساب الخاص إلي عدة حسابات بنكية في انجلترا فقام البنك بذلك حوكم الفاعل بتهمة الحصول علي أموال الغير بطريق الاحتيال وحكم عليه بعقوبة السجن، طعن في الحكم استنادا إلى عدم اختصاص القضاء الإنجليزي لان فعلي السحب والإيداع قد تما في الكويت لا في إنجلترا لكن محكمة الاستئناف رفضت طعنه وردت بأن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل وما أسفر عنه من حصوله علي الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية .

تما في الكويت لا في إنجلترا لكن محكمة الاستئناف رفضت طعنه وردت بأن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل وما أسفر عنه من حصوله علي الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية. ولهذا فمكافحة هذه الجرائم تتطلب تعاونا كثيفا بين الدول وتوافقا كبيرا بين تشريعاتها .

المطلب السادس: الجرائم الالكترونية فادحة الأضرار:

أن الاعتماد المتزايد علي الحاسب الآلي في إدارة مختلف الأعمال في شتى المجالات ضاعف من الأضرار والخسائر التي تخلفها الاعتداءات علي معطيات هذا الحاسب، لاسيما إذا كانت تمثل قيما مالية، خاصة مع ازدياد اعتماد البنوك والمؤسسات المالية ومختلف الشركات علي الحاسب الآلي في تسييرها، وفي هذا الخصوص تشير الدراسات إلى أن الأضرار الناجمة عن جرائم المعطيات تفوق بكثير تلك الناجمة عن الجرائم التقليدية(8) ففي الولايات المتحدة الأمريكية وحسب مكتب التحقيقات الفيدرالي (FBI) فالجريمة المعلوماتية تكلف خسائر تقدر بمائة وخمسين (150) ضعف ما تكلفه الجريمة العادية، وان الخسائر الناجمة عن 139 عملية غش معلوماتي وقع علي البنوك، بلغت ثمانمائة ألف دولار (800000 $) عام 1981 كما أن الغش المعلوماتي كان السبب في حدوث خمسين (50)

حالة إفلاس في ثلاثمائة وأربعة وخمسين (354) بنكا بين شهري جانفي (يناير) 1985 وجوان (يونيه) 1987، وفي دراسة للمركز الوطني لجرائم الكمبيوتر والبيانات قدرت خسائر الجرائم المعلوماتية بين ثلاث (03) وخمس (05) مليارات دولار أمريكي وفي دراسة أجراها معهد أمن المعلومات بالولايات المتحدة الأمريكية عام 2001 شملت 538 مؤسسة تبين أن الخسائر قدرت بحوالي 378 مليون دولار في حين كانت عام 2000 بحدود 265 مليون دولار وان معدل الخسارة للأعوام الثلاثة السابقة علي عام 2000 بلغت 120 مليون دولار.

وفي المملكة المتحدة أجرت لجنة المراجعة المحاسبية دراسة خلال عدة سنوات تبين منها أن خسائر 64 حالة عام 1984 قدرت بـــ 1133487 جنيها إسترلينيا وفي سنة 1987 قدرت الخسائر الناجمة في 55 حالة بـــ 2561351 جنيها إسترلينيا وفي سنة 1990 بلغت الخسائر في 180 حالة 1140142 جنيها إسترلينيا وشملت الدراسة من سنة 1993 إلى 1993 حوالي537 حالة قدرت خسائرها بـــ 3196720 جنيها إسترلينيا.

وفي دراسة قامت بها مدرسة لندن الاقتصادية قدرت الخسائر بحوالي 400 مليون جنيه إسترليني بمتوسط خسارة للحالة الواحدة بحوالي 46000 جنيها إسترلينيا.

وفي فرنسا قدرت الخسائر سنة 1991 حسب ما نشرته الجمعية الفرنسية لأمن المعلومات بـــ (10.4) مليار فرنك فرنسي، في سنة 1993 قدرت الخسائر بحوالي (10.8) مليار فرنك فرنسي، وفي سنة 1996 قدرت بحوالي 12.720 مليار فرنك فرنسي.

المبحث الثاني: جهود المشرع الجزائري في مواجهة الجريمة الالكترونية

نص قانون العقوبات الجزائري على ثلاث أنواع من الجرائم المعلوماتية يمكن أن تقع في قطاع البنوك، وهي جريمة الدخول أو البقاء غير المصرح بهما في أنظمة المعالجة الآلية للمعطيات وجريمة التلاعب بالمعطيات وجريمة التعامل في معطيات غير مشروعة، وسنعرض فيما يلي لكل واحد من هذه الجرائم.

المطلب الأول: جريمة الدخول أو البقاء غير المشروع في أنظمة المعالجة الآلية للمعطيات:

هذه الجريمة من أهم الجرائم وأخطرها، إذ أنها تشكل في كثير من الأحيان مفترضا لحدوث الجرائم الأخرى، ذلك أن الجاني يحتاج إلى الدخول إلى الأنظمة المعلوماتية حتى يرتكب مختلف الجرائم الأخرى، وسنتعرض فيما يلي لأركان هذه الجريمة وعقوباتها.

الفرع الأول: أركان جريمة الدخول أو البقاء غير المصرح به:

حرص المشرع الجزائري على تجريم كل تواجد عمدي غير شروع داخل أنظمة المعالجة الآلية للمعطيات سواء أدى إلى نتيجة معينة أو لم يؤذي إلى ذلك، وفيما يلي الركن المادي والمعنوي لهذه الجريمة.

أولا: الركن المادي:

تقوم هذه الجريمة على سلوك إجرامي يتخذ إحدى صورتين، إما الدخول أو البقاء، ولم تنص المادة 394 مكرر على تعريف للدخول أو البقاء، وهناك من عرف الدخول غير المصرح به

بأنه الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام(9).

أو هو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه، للوصول إلى المعلومات والمعطيات المخزنة بداخله، للإطلاع عليها أو لمجرد التسلية، أو لإشباع الشعور بالنجاح في اختراق الحاسب الآلي(10).

أما البقاء فيعرف بأنه التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام(11). أو هو: "عدم وضع حد للتشعب داخل النظام مع الاعتقاد بأن ذلك يشكل خطأ "(12).

فالبقاء يتمثل في عدم قطع الفاعل للاتصال بالنظام عند إدراكه أن وجوده فيه غير مشروع(13). فمن صور البقاء استمرار وجود الجاني داخل النظام بعد المدة المحددة له، ومن صوره أيضا تلك الحالة التي يجد الجاني فيها نفسه داخل نظام المعالجة الآلية للمعطيات بدون قصد منه، كأن يكون الدخول قد تم عن طريق الصدفة بدون إرادة من الداخل، لكنه بعد اكتشافه بأنه داخل النظام يبقى فيه ولا يخرج منه في الوقت الذي كان يجب عليه مغادرته(14).

ولا يشترط صفة معينة فيمن يقوم بالدخول أو البقاء، وقد عبرت عن ذلك المادة 394 مكرر بقولها: "كل من يدخل أو يبقى...." كما لا يشترط أن يتم الدخول بطريقة معينة، لأن المادة السابقة جاءت شاملة وعامة(15).

هذا بالنسبة للسلوك الإجرامي في هذه الجريمة، أما بالنسبة للنتيجة الإجرامية فلا تتطلب المادة 394 مكرر تحقق نتيجة معينة حتى تقوم الجريمة، وإنما تقوم هذه الأخيرة بمجرد توافر السلوك الإجرامي أي الدخول أو البقاء، لكن إذا ترتب على الدخول أو البقاء نتائج

محددة فإن المشرع رتب على ذلك تشديد العقوبة كما سنراه فيما سيأتي(16). وهذه النتائج هي حذف أو تغيير معطيات نظام المعالجة الآلية للمعطيات أو تخريب هذا النظام.

ثانيا: الركن المعنوي:

تنص المادة 394 مكرر ق ع ج صراحة على وجوب كون جريمة الدخول أو البقاء غير المصرح بهما جريمة عمدية، ويستشف ذلك من قولها: "كل من يدخل أو يبقى عن طريق الغش".

والحقيقة أن المنطق يحتم أن تكون هذه الجريمة عمدية، لأن عمليات الدخول إلى أنظمة الحاسبات الآلية والبقاء فيها هي عمليات تتكرر بشكل مذهل في اليوم الواحد وتقع من عدد هائل من المستخدمين، لاسيما مع ارتفاع عدد مرتادي شبكة الانترنت، وليس من المستبعد في ظل كل هذه الحركة دخولا وخروجا أن تكون هناك عمليات دخول أو بقاء غير مصرح بهما لكنها غير عمدية، لهذا وجب أن تكون الجريمة غير عمدية حتى لا يقع هؤلاء تحت طائلة العقاب، وعلى هذا كان من اللازم أن تكون هذه الجريمة عمدية، وذلك من أجل الموازنة بين خصوصية الأنظمة المعلوماتية وحماية حرية الأفراد في استخدام الانترنت(17).

لكن بالنسبة للظروف المشددة لهذه الجريمة، أو النتيجة المشددة فلا بد أن تكون غير عمدية، لأنها لو كانت عمدية ستشكل جريمة أخرى هي جريمة التلاعب بالمعطيات، كما سنراه لاحقا(18).

<u>الفرع الثاني: عقوبة جريمة الدخول أو البقاء غير المصرح بهما:</u>

تتخذ جريمة الدخول أو البقاء غير المصرح بهما صورتان لكل واحدة منهما عقوبتها، الأولى بسيطة أو مجردة والثانية مشددة.

أولا: عقوبة الجريمة في صورتها المبسطة:

إذا كانت الجريمة في صورتها المشددة أو البسيطة فلم تؤد إلى إعاقة أو إفساد نظام المعالجة الآلية للمعطيات أو إزالة أو تعديل لهذه الأخيرة فإن العقوبة الأصلية تكون الحبس من ثلاثة أشهر إلى سنة والغرامة من خمسين ألف (50000) إلى مائة ألف (100000) دينار جزائري.

أما العقوبة التكميلية لهذه الجريمة فسنتكلم عنها في الأحكام المشتركة لجميع الجرائم.

ثانيا: عقوبة الجريمة في صورتها المشددة:

تشدد الفقرة الثانية والثالثة من المادة 394 مكرر ق ع ج عقوبة جريمة الدخول أو البقاء غير المصرح بهما إذا أدت إلى تخريب نظام اشتغال منظومة المعالجة الآلية للمعطيات أو حذف أو تغيير لهذه الأخيرة، تشدد إلى ضعف تلك المقررة للجريمة في صورتها المجردة أو البسيطة، سواء في حدها الأدنى الذي يتضاعف إلى (06) أشهر، أو في حدها الأقصى الذي يتضاعف إلى سنتين، أما الغرامة فيثبت حدها الأدنى عند خمسين ألف دينار جزائري (50000 دج) ويرتفع حدها الأقصى إلى مائة وخمسين ألف دينار جزائري (150000 دج)، هذا في حالة ما إذا أدى الدخول أو البقاء إلى حذف أو تغيير للمعطيات أما إذا أدى إلى تخريب النظام فالغرامة تشدد للضعف أي تتراوح بين مائة ألف (100000 دج) ومائتي ألف (200000) دينار جزائري.

<u>المطلب الثاني: جريمة التلاعب بالمعطيات:</u>

هي الجريمة الثانية من الجرائم المعلوماتية في قانون العقوبات الجزائري، نصت عليها المادة 394 مكرر 01 من ق ع ج بقولها: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات

وبغرامة من 500 ألف إلى مليوني دينار جزائري كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

وسنتناول فيما يلي أركان هذه الجريمة والعقوبة المقررة لها.

الفرع الأول: أركان جريمة التلاعب بالمعطيات:

نتناول فيما يلي الركن المادي والركن المعنوي لجريمة التلاعب بالمعطيات.

أولا: الركن المادي:

يتكون الركن المادي لجريمة التلاعب بالمعطيات من سلوك إجرامي يتمثل في إدخال أو تعديل أو إزالة المعطيات يؤدي إلى نتيجة إجرامية تتمثل في تغيير حالة المعطيات.

أ- السلوك الإجرامي:

للسلوك الإجرامي ثلاث صور في هذه الجريمة: الإدخال، التعديل والإزالة.

01- فعل الإدخال:

يشمل هذا الفعل إدخال خصائص ممغنطة جديدة على الدعامات الموجودة، سواء كانت فارغة – غير مشغولة – أو كانت تحتوي على خصائص ممغنطة قبل هذا الإدخال(19)، ففعل الإدخال هو إضافة معطيات جديدة غير مصرح بإدخالها.

02- فعل التعديل:

التعديل هو تغيير حالة المعطيات الموجودة بدون تغيير الطبيعة الممغنطة لها(20) أو هو كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف الحاسب الآلي(21).

03- فعل الإزالة:

الإزالة هي اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو عن طريق طمسها، أي ضغط خصائص أخرى فوقها (خصائص جديدة تطمس الخصائص القديمة) وكذلك عن طريق تحويل ورص خصائص مزالة في منطقة محفوظة من الذاكرة(22).

ب- النتيجة الإجرامية:

النتيجة الإجرامية في جريمة التلاعب بالمعطيات هي تغيير حالة هذه الأخيرة بالزيادة أو بالنقصان أو بالتعديل(23).

ثانيا: الركن المعنوي في جريمة التلاعب:

جريمة التلاعب بالمعطيات جريمة عمدية لابد لقيامها توافر القصد الجنائي لدى مرتكبها، وفي حال عدم وجود قصد لا يعاقب الجاني على تعديل وإزالة المعطيات غير العمديين إلا إذا كانا نتيجة دخول أو بقاء غير مصرح بهما كما سبق بيانه.

الفرع الثاني: عقوبة جريمة التلاعب:

تقرر المادة 394 مكرر 01 من ق ع ج على مرتكب جريمة التلاعب بالمعطيات عقوبة الحبس من 06 أشهر إلى 03 سنوات، والغرامة التي تتراوح من خمسمائة ألف (500000) إلى مليوني (2000000) دينار جزائري.

كما تقرر عقوبة تكميلية شأنها شأن باقي الجرائم.

المطلب الثالث: جريمة التعامل في معطيات غير مشروعة:

لاشك أن المشرع عندما يدرك أهمية مصلحة ما، يسعى لإحاطتها بالحماية من كل الجوانب، ويوصد كل باب يمكن أن يلجه من يريد الاعتداء عليها، كما يسعى إلى إيقاف العدوان عليها في مصدره، وفي حال حصل هذا العدوان يسعى المشرع على الحد من آثاره، ورغبة من المشرع في حماية أكبر للمعطيات لاسيما المعطيات الخاصة بقطاع البنوك، رغبة منه في

حماية أكبر لها من جرائم الدخول أو البقاء غير المصرح بهما وجرائم التلاعب، قام بتجريم التعامل في المعطيات الصالحة لارتكاب تلك الجرائم وتجريم التعامل في معطيات متحصلة من تلك الجرائم، وهذان هما صورتان لجريمة التعامل في معطيات غير مشروعة(24)، والتي سنتناول فيما يلي أركانها وعقوباتها.

الفرع الأول: أركان جريمة التعامل في معطيات غير مشرعة:

نتناول فيما يلي الركن المادي والركن المعنوي لجريمة التعامل في معطيات غير مشروعة.

أولا: الركن المادي:

يتكون الركن المادي من مجرد السلوك الإجرامي دون النتيجة الإجرامية.

أ- السلوك الإجرامي:

يقوم الركن المادي لجريمة التعامل في معطيات غير مشرعة على مجرد توافر السلوك الإجرامي الذي يتخذ صورتين اثنتين: أولاهما هي التعامل في معطيات صالحة لارتكاب الجريمة وثانيهما هي التعامل في معطيات متحصلة من جريمة.

1- التعامل في معطيات صالحة لارتكاب جريمة:

تجرم المادة 394 مكرر 02 في البند الأول منها مجموعة من الأفعال الخطرة التي لو تركت بدون تجريم لأدت إلى حدوث جرائم أخرى، هذه الأفعال تشمل كافة أشكال التعامل الواقعة على معطيات لاسيما المتعلقة بقطاع البنوك، والتي تسبق عملية استعمال هذه المعطيات في ارتكاب الجريمة، فالمعطيات قبل هذه المرحلة الأخيرة تمر بالعديد من المراحل حتى تصل إلى يد الجاني فيرتكب بها جريمته وهذه المراحل تبدأ من تصميم هذه المعطيات والبحث فيها وتجميعها وصولا إلى جعلها في متناول الغير وتحت تصرفه وذلك بتوفيرها أو نشرها أو الاتجار فيها.

ولا يشترط أن تقع هذه الأفعال مجتمعة لتقوم الجريمة، بل يكفي أن تقع إحداهما فقط، وهذه الأفعال هي التصميم والبحث والتجميع والتوفير (الوضع تحت التصرف أو العرض) والنشر والاتجار.

2- التعامل في معطيات متحصلة من جريمة:

هي الصورة الثانية من جريمة التعامل في معطيات غير مشروعة، وتتحقق بواحد من أربعة أفعال هي حيازة معطيات متحصلة من جريمة (دخول أو بقاء غير مصرح بهما أو التلاعب بالمعطيات) أو إفشاء هذه المعطيات أو نشرها أو استعمالها، أي أنه يكفي تحقق واحد من هذه الأفعال فقط حتى تقوم الجريمة.

ب- النتيجة الإجرامية:

جريمة التعامل في معطيات غير مشروعة هي من جرائم الخطر لا يتطلب لقيامها حدوث نتيجة معينة، فالمشرع جرم تلك الأفعال بوصفها أفعال خطرة يمكن أن تؤدي إلى ضرر فعلي(25).

ثانيا: الركن المعنوي:

جريمة التعامل في معطيات غير مشروعة جريمة عمدية، ويستفاد ذلك من عبارة المادة 394 مكرر 02 "عمدا وعن طريق الغش"

ولدينا أن الجريمة في صورتها الأولى (التعامل في معطيات صالحة لارتكاب جريمة) تتطلب قصدا خاصا هو قصد الإعداد أو التمهيد لاستعمالها في ارتكاب جريمة.

أما الجريمة في صورتها الثانية (التعامل في معطيات متحصلة من جريمة) فلدينا أنه يكفي لقيامها توافر القصد الجنائي العام(26).

الفرع الثاني: عقوبة جريمة التعامل في معطيات غير مشروعة:

تعاقب المادة 394 مكرر 2 من ق ع ج على هذه الجريمة بالحبس من شهرين إلى 03 سنوات وبالغرامة من مليون (1000000) إلى خمسة ملايين (5000000) دينار جزائري. كما يعاقب عليها بالعقوبة التكميلية المقررة على كل الجرائم السابقة.

المطلب الرابع: الأحكام المشتركة للجرائم المعلوماتية في قطاع البنوك:

هناك العديد من الأحكام القانونية التي تشترك فيها كل الجرائم المعلوماتية التي يمكن أن تقع في قطاع البنوك وهي جريمة الدخول أو البقاء غير المصرح بهما وجريمة التلاعب بالمعطيات وجريمة التعامل في معطيات غير مشروعة، وهذه الأحكام المشتركة منها ما يتعلق بالجرائم وبنيانها ومنها ما يتعلق بعقوبة تلك الجرائم.

الفرع الأول: الأحكام المتعلقة بالجرائم:

الأحكام المشتركة المتعلقة بالجرائم نصت عليها المادة 394 مكرر 05 وهي المتعلقة بالعقاب على الاتفاق الجنائي على ارتكاب أي من الجرائم السابقة إذا تجسد بأعمال مادية. كما نصت المادة 394 مكرر 07 على العقاب على الشروع في أي من تلك الجرائم(27).

أولا: الأحكام المتعلقة بالعقوبة:

تشترك جرائم المعطيات في ثلاثة أحكام تتعلق بالعقوبة(28)، أولاها تتعلق بالعقوبات التكميلية، فكل جرائم المعطيات لها نفس العقوبات التكميلية وهي المصادرة والغلق (م 394 مكرر06) والثانية تتعلق بتشديد عقوبة الشخص المعنوي، فقد نصت المادة 394 مكرر 04

على مضاعفة عقوبة الشخص المعنوي الذي يرتكب جرائم المعطيات إلى خمسة أضعاف ما هو مقرر على الشخص الطبيعي.

والثالثة هي تشديد عقوبة تلك الجرائم إلى الضعف إذا ارتكبت ضد مؤسسة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام (م394 مكرر 04).

خاتمة:

إن الجرائم المعلوماتية من أخطر الجرائم، فالشخص الذي يرتكبها هو مجرم غير تقليدي له مميزاته الخاصة، وهي جرائم يصعب اكتشافها وإذا ما اكتشفت يصعب إثباتها، وما يزيد من خطورة هذه الجرائم أن للضحية دور مهم فيها، وأنها جرائم ناغمة شديدة الإغراء للمجرمين وأنها جرائم عابرة للحدود وجرائم فادحة الأضرار.

هذا الأمر جعل المشرع الجزائري يتصدى لمحاربة هذه الجرائم، إذ نص عليها في قانون العقوبات إثر تعديل سنة 2004، وقد صنفها إلى ثلاثة أنواع: جريمة الدخول أو البقاء غير المصرح بهما وجريمة التلاعب بالمعطيات وجريمة التعامل في معطيات غير مشروعة، ورغبة من المشرع الجنائي في حماية أكبر للمعطيات ومنها ما يتعلق بقطاع البنوك فقد جرم الاتفاق الجنائي على ارتكاب إحدى الجرائم السابقة إذا تجسد بأعمال مادية، كما جرم الشروع في تلك الجرائم كما فرض عقوبات تكميلية عليها، وشدد من عقوبة الشخص المعنوي الذي يرتكبها، كما شدد العقوبة إذا طال هذا الاعتداء الجهات العامة في الدولة.

وبهذا يعتبر المشرع الجزائري قد خطى خطوة كبيرة في هذا المجال، وتشريعه هذا لا يقل شأنا عن كثير من التشريعات الأوروبية.

الهوامش:

(1) - Raymond Gassin , Fraude informatique . Daloz, 1995 p.12.

(2) Xavier Linant de bellefonds et Allan Hollande droit de l'informatique et de la telematique 2em edition . J Delmas et Cie p236.

(3) د. عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، ط 2، القاهرة 2002، ص36.

وانظر كذلك: محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998، ص30.

وانظر: د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، 2004، ص192.

وانظر: Dr. Mohammed bo Buzubar . la criminalite informatique sur l'internet . journal of law academic publication council Kuwait university . No1 vol. 26 – march 2002 pp.41.49

(4) د. سعيد عبد اللطيف حسن، اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط1، دار النهضة العربية، القاهرة، 1999، ص95.

وانظر: د: هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة بأسيوط، 1994، ص35.

Philipe Rose . La criminalite informatique a l'horizon Analyse prospective . L'harmattan 1992 p (5)2005 49.

(6) اسامة احمد المناعسة، جلال محمد الزعبي، صايل فاضل الهواوشة، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، دار وائل للنشر، عمان، الأردن، الطبعة الأولى، 2001 ص107.

(7) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، 2003، ص49.

وانظر أيضا: Sophie Revol . Terroristes et internet . memoire de DESS en droit du multimedia et de l'informatique . Universite pantheon assas Paris II Faculte de droit

(8) Philipe Rose , La criminalite infromatique edition dahlab imprimerie . Alger pp 22-30

(9) bainbridge (david) hacking the unavthorised access of computer system. The legal implication m.l.rev.march 1989.vol 52 p237.

(10) the recommendation no r(89) 9 on computer relatedcrime pp49-51

مشار إليه لدى د: نائلة قورة، ص326.

(11) د:علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت. كلية الشريعة والقانون، جامعة الإمارات، دولة الإمارات العربية المتحدة 2000، ص52.

(12) R. gassin fraude informatique. Dalloz. 1995.p 19.

(13) د:علي عبد القادر القهوجي ، الحماية الجنائية للبيانات المعالجة الكترونيا، المرجع السابق، ص52.

(14) R .gassin op. cit. p 19

(15) R .gassin op. cit. p 15

(16) محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، 2007 ص 159.

(17) المرجع نفسه، ص162-163.

(18) المرجع نفسه، ص 169.

(19) R. gassin op. cit. p 32

(20) R. gassin op. cit. p 32

(21) د نائلة قورة، المرجع السابق، ص220.

(22) R. gassin op. cit. p 32

(23) محمد خليفة، المرجع السابق، ص185.

(24) المرجع السابق، ص ص 193-195.

(25) محمد خليفة، المرجع السابق، ص210.

(26) لمزيد من التفصيل أنظر: محمد خليفة، ص213 وما بعدها.

(27) لمزيد من التفصيل أنظر: محمد خليفة، المرجع السابق، ص111 وما بعدها.

(28) المرجع نفسه، ص ص 119- 130