

الاعتداء على المعطيات الآلية في الحكومة الالكترونية

بومعيزة جابر

أستاذ بكلية الحقوق والعلوم السياسية

جامعة البليدة -2-

ملخص

إن واقع التطور البشري وما صاحبه من تطور في التكنولوجيا والنظر إلى المستقبل بلغة المعطيات والبيانات الالكترونية كرس لدى العديد من الدول واقع ما أصبح يطلق عليه الحكومة الالكترونية، هذه الأخيرة التي لا تخلوا صورها من مختلف الاعتداءات على البيانات والمعطيات باعتبار أن كل تطور في مجالات الحياة والمعاملات يضطحبه تطور في الجريمة وصور الاعتداء، وذلك من خلال التركيز في مداخلتنا على جريمة الدخول أو البقاء غير المشروع في النظام وكذلك إعاقة أو تحريف تشغيل نظم معالجة البيانات، هذا الاعتداء الذي يقع على المعطيات والبيانات الآلية للحكومة الالكترونية، وعليه فإن هناك عدة صور للاعتداء على الحكومة الإلكترونية.

Résumé

La réalité de l'évolution humaine qui est associée à l'évolution technologique en prenant en considération les données électroniques ont obligé de nombreux pays à créer ce qu'on appelle E-gouvernement, malgré ce progrès réalisé, ce nouveau système reste toujours inefficace vue les diverses attaques sur les données ;considérant le fait que le progrès dans tous les domaines est accompagné à celui de la criminalité et de toutes sortes d'agression, c'est pour cette raison que nous allons nous concentrer dans notre communication sur le délit d'accès et le maintien frauduleux illégaux dans tout ou partie d'un système ainsi que l'altération du fonctionnement des systèmes de traitement des données. donc il y'a plusieurs aspects d'assaut sur le E-gouvernement que nous allons exposer selon le plan suivant:Chapitre 1: définition du système automatisé de traitement de données. Chapitre 2: aspects d'assaut sur le système automatisé de traitement de données.

مقدمة

أصبحت فكرة الحكومة الالكترونية (تجدر الإشارة إلى أن الدول العربية هي الأخرى على غرار باقي دول العالم منها الأوروبية والأمريكية شرعت في تطبيق الحكومة الالكترونية

وأحسن مثال يضرب في هذا الشأن هي إمارة دبي بدولة الإمارات العربية المتحدة التي تعد أول دولة عربية طبقت نظام الحكومة الالكترونية بشكل شبه كلي، وتعتبر التجربة لدى إمارة دبي تجربة رائدة وتأتي بعدها دولة مصر والعراق والجزائر التي هي الأخرى تسعى جاهدة من أجل تحقيق مفهوم الحكومة الالكترونية من خلال تنظيم تشريعاتها، فقد قامت إمارة دبي بالإمارات العربية المتحدة بإنشاء منطقة دبي الحرة للانترنت أو مدينة الانترنت، كما قامت بإطلاق الحكومة الالكترونية سنة 2001 وأصدرت قانون التجارة والمعاملات الالكترونية تحت رقم: 2 لسنة 2002. لمزيد من التفصيل انظر: د. عبد الفتاح بيومي الحجازي، سنة 2007 ص 351 وما تليها) واقعا مفروضا على المجتمعات البشرية باعتبارها من بين نتائج التطور والتغيرات الحاصلة في شتى المجالات والتي أصبحت تتصل وتترابط فيما بينها ببرامج آلية متطورة من جهة ومعقدة من جهة أخرى من خلال استعمال معدات متطورة، خاصة وأن هذا التقدم العلمي صاحبه ظهور أنماط مستحدثة من الجرائم لم تكن موجودة ولم تنص عليها التشريعات العقابية ذلك أن التشريع وليد الحاجة، ولهذا لم تتطرق التشريعات العربية إلى جرائم الحاسب الآلي، ولعل مرد ذلك أن الدول العربية جاءت متخلفة عن الركب العالمي في مجال المعلوماتية إضافة إلى أنها بدأت الاعتماد على نظام المعلوماتية منذ نهاية العقد الأخير من القرن الماضي، وعلى العكس من ذلك فالبلدان الأوروبية وكندا والولايات المتحدة الأمريكية يعتمدون على الحاسب الآلي منذ عقدين من الزمن أو أكثر، وعلى هذا الأساس بدأت الدول العربية في تقنين العمل بالمعطيات الآلية للمعلومات والنص على الجريمة المعلوماتية ضمن قوانينها العقابية وقد قنن المشرع الفرنسي ظاهرة الجرائم المعلوماتية بمقتضى تعديلات في قانون العقوبات منذ عام 1994 وبعد ذلك قننها المشرع الجزائري في قانون العقوبات لسنة 2004.

وبناء على ذلك وضعت عدة تعريفات للجريمة المعلوماتية، فمنهم من عرفها على نطاق ضيق، ومنهم من عرفها على نطاق واسع، بأنها جريمة تقوم على معيار قانوني كتعريفها بدلالة موضوع الجريمة أو السلوك محل التجريم أو الوسيلة المستخدمة أي باعتبارها من الأفعال والسلوكات المجرمة قانونا.

بينما هناك من انصب في تعريفه على عدة معايير والتي تشمل تبيان موضوع الجريمة وأنماطها وبعض العناصر المتصلة بآليات ارتكابها وصفة مرتكبيها، والتعريف الشامل لهذه الظاهرة هي أنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى

المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه (انظر في هذا الصدد مختلف التعريفات في: 3 n 1988 R.S.C. ; Champy)

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها: "الجريمة التي تلعب فيها البيانات الحاسوبية والبرامج المعلوماتية دورا رئيسيا"، كما عرفها الأستاذ: "جون كارول" وتبناه الأستاذ: "جيون قرين" من أن الجريمة المعلوماتية هي: "أي عمل ليس له في القانون أو الأعراف جزاء، يضر بالأشخاص أو الأموال، ويوجه أو يستخدم ضد التقنية المتقدمة لنظم المعلومات".

وقد عرف خبراء متخصصون في بلجيكا الجريمة المعلوماتية في معرض ردهم على منظمة التعاون الاقتصادي والتنمية بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأمواج المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية" والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين بوصفه أفضل التعريفات لأنه يعبر عن الطابع التقني الذي تنطوي تحته أبرز صور جرائم المعلوماتية (د. هشام محمد فريد رستم، سنة 1992 ص 35. مشار إليه: ابراهيمي سهام، بدون سنة ص 3). ويشمل كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب (Tiedemann , 1984 n° 7 ; p 61)

ومن ضمن التعريفات التي تعتمد أكثر من معيار، يعرف جانب من الفقه الجريمة المعلوماتية وفق معايير قانونية صرفة، أولها تحديد محل الجريمة، وثانيها وسيلة ارتكابها وهو في كلا المعيارين الحاسب الآلي لما يلعبه من الضحية ودور الوسيلة حسب الفعل المرتكب حيث يعرفه الأستاذ: "Thomas J. smedinghoff" (ورد هذا التعريف في مؤلفه تحت عنوان: "المرشد القانوني لتطوير وحماية وتسويق البرمجيات) على أنها: "أي ضرب من النشاط الموجه ضد استخدام نظام الحاسوب" وهنا تعبير "النشاط الموجه ضد" ينسحب على الكيانات المادية إضافة للكيانات المنطقية وكذلك تعريف الأستاذين: "Jack Bolgna, J. Robert Lindquist" جريمة يستخدم الحاسوب كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها

ويعرف الفقيه Masse الجريمة المعلوماتية - يستخدم اصطلاح الغش المعلوماتي (هو نفس المصطلح الذي استعمله المشرع الجزائري في تجريمه للاعتداء على نظام المعالجة الآلية للمعطيات في القسم السابع مكرر من الفصل الثالث من الباب الثاني تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات من قانون العقوبات الجزائري المعدل والمتمم. لمزيد من التفصيل انظر: د. أحسن بوسقية، ص 444 وما تليها، انظر كذلك: الدكتور: علي عبد

القادر القهوجي، سنة 1997 ص 2) بأنها: "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح" (مشار إليه: د. محمد سامي الشوا، سنة 1998 ص 3) وقد عرفها مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقة المجرمين تعريفا لجرائم الحاسب الآلي وشبكاته 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" (انعقد هذا المؤتمر في فيينا ما بين 10-17 أبريل سنة 2000).

من مجمل التعريفات يتبين لنا أن الحكومة الالكترونية تنصب عليها الجريمة المعلوماتية إذ أنها تهدف للمساس بنظام المعالجة الآلية للمعطيات من خلال الاعتداء على بيانات الحكومة الالكترونية ومعطياتها.

وإذا كانت تعريفات الجريمة عموما تقوم على أساسين: عناصر الجريمة والسلوك ووصفه، والنص القانوني على تجريم السلوك وإيقاع العقوبة، فإن الجديد في مجال جرائم الحاسوب هو إضافة عنصر ثالث يبرز محل الاعتداء في هذه الظاهرة الإجرامية المستحدثة، متمثلا بمعطيات الحاسوب فقانون العقوبات ينطوي على نصوص تحرم الاعتداء على الأشخاص، الأموال، الثقة العامة، لكن المستجد في مجال الحكومة الالكترونية هو الكيانات المعنوية الافتراضية ذات القيمة المعنوية البحتة، أو كلاهما ولولا هذه الطبيعة المستجدة في الأساس لما كنا أما ظاهرة مستجدة برمتها، لكن المستجد هو دخول الكمبيوتر عالم الجريمة والاعتداء بمختلف صوره، فما هو مفهوم الاعتداء على بيانات الحكومة الالكترونية وفيما تتمثل صور الاعتداء على المعطيات والبيانات الآلية للحكومة الالكترونية؟

وسوف نتعرض إلى ذلك وفق الخطة التالية: المبحث الأول: ماهية نظام المعالجة الآلية للمعطيات. المبحث الثاني: صور الاعتداء على نظام المعالجة الآلية للمعطيات.

المبحث الأول: ماهية نظام المعالجة الآلية للمعطيات.

إن مصطلح الحكومة الالكترونية مصطلح ظهر حديثا ويرتبط ظهوره باستعمال الحاسب الآلي (الحاسب الآلي عبارة عن آلة الكترونية تستقبل البيانات ثم يقوم بعد ذلك عن طريق الاستعانة ببرامج المعطيات الآلية بعملية تشغيل هذه البيانات للوصول إلى النتائج انظر في هذا الصدد: د. ماجد عمار، سنة 1989 ص 54، ويعرف أيضا على انه عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات ومعالجتها وتخزينها واستشارتها واسترجاعها عند الطلب. انظر الدكتور: محمد فتحي عبد الهادي، سنة 1984 ص 217). في التعدي على الحكومة الالكترونية من الجرائم المستحدثة باعتبار أن كيان

الحكومة الالكترونية كيان افتراضي خاصة وانه لا تخلوا وسائل الإعلام من الإشارة إلى جرائم المعلومات والمساس بمعطيات الحكومة الالكترونية، فالصراع مستمر بين المجرمين ومتتبعي هذه الجرائم من خلال زرع الفيروسات واختراق أنظمة المعلومات (د. محمد ناجي، العدد 342 ص 34). ولدراسة موضوع بحثنا هذا فانه لزاما علينا التطرق إلى مفهوم نظام المعالجة الآلية للمعلومات في المطلب الأول ونتناول في المطلب الثاني مدلول الحكومة الالكترونية.

المطلب الأول: مفهوم نظام المعالجة الآلية للمعطيات للحكومة الالكترونية.

إن كل نظام للحكومة الالكترونية يعتمد على وجود نظام للمعالجة الآلية للمعطيات وهي مجموع الشبكات التي يعتمد عليها لانجاز الأعمال الخاصة بالحكومة أو الإدارة الالكترونية (د. عبد الفتاح بيومي حجازي، سنة 2007 مصر ص 358). وما يلاحظ أن البدايات الأولى لظهور الحكومة الالكترونية كان في الدول الاسكندنافية بحيث تمثلت في ربط القرى البعيدة بالمركز عن طريق الشبكات وأطلق عليها تسمية القرية الالكترونية ويعتبر "لارس" من جامعة "ادونيس" في الدنمارك رائد هذه التجربة وأطلق عليها مركز الخدمة عن بعد ومن رواد هذه الفكرة "مايكل دل" صاحب شركة دل للإعلام الآلي والتي تعتبر من الشركات ذات الريادة في مجال الحلول الإلكترونية (د. علي حسون الطائي، سنة 2008) وسوف نتطرق في هذا المطلب إلى مدلول نظام المعالجة الآلية للمعطيات في الفرع الأول وفي الفرع الثاني نتطرق إلى مدلول الحكومة الالكترونية.

الفرع الأول: تعريف نظام المعالجة الآلية للمعطيات.

لقد كان مجلس الشيوخ الفرنسي قد اقترح تعريفا لنظام المعالجة الآلية للبيانات بأنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة، والتي تتكون كل منها الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية (د. عبد الفتاح بيومي حجازي، ص 358).

يمثل نظام المعالجة الآلية للمعطيات المفهوم الأولي (د. علي عبد القادر القهوجي، سنة 1999 ص 25) الذي يمكن أن يتحقق به الاعتداء والمساس بالمعطيات والبيانات ومنه توافر أركان هاته الجريمة (Gassin J.C. P1988. doct. p95) لكونها جريمة تقع في بيئة المعالجة المعلوماتية للبيانات لتصحيحها وتعديلها وتشكل محلا للاعتداء أو كوسيلة للاعتداء (د. هدى حامد قشقوش،

سنة 1992 ص 15) وما يلاحظ على هذا التعريف أنه أشار للعناصر المادية والمعنوية التي يتكون منها المركب الذي هو أساس نظام المعالجة الآلية للبيانات، وهذه العناصر وردت على سبيل المثال لا الحصر، كما عرفه القانون العربي النموذجي الموحد نظام المعالجة الآلية للمعطيات بأنه: "يقصد به كل مجموعة مركبة من وحدة أو عدة وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة".

ولقد نص على الاعتداء على المعطيات الآلية لنظام المعلوماتية في قانون حماية الملكية الفكرية باعتبار انه تعدي على الحقوق الفنية باعتبار أن الاعتداء على النظام الأمني للمعلوماتية شرط مفترض لقيام الجرائم التي تتعلق بنظم المعلوماتية، غير أن القاعدة العامة للتجريم والعقاب هو ما كرسه المشرع الجزائري في نص المادة الأولى من قانون العقوبات بقولها: " لا جريمة ولا عقوبة أو تدابير امن بغير قانون".

الفرع الثاني: تعريف الحكومة الالكترونية.

إن الكلام عن بيئة العالم الافتراضي فان كل حكومة تهدف إلى تحقيق فعالية عالية في أداء خدماتها وتبادل المعلومات والنشاطات ما بين إداراتها ودوائرها ومؤسساتها (د. محمد محمود الخالدي، سنة 2007 ص 30).

ولقد وردت عدة تعريفات للحكومة الالكترونية وتعرف عل أنها إعادة ابتكار الأعمال الحكومية بواسطة طرق جديدة لإدماج وتكامل المعلومات وتوفير فرصة إمكانية الوصول إليها من خلال موقع الكتروني (د. محمد محمود الخالدي، ص 70).

إن الحكومة الالكترونية في مدلول آخر هي قدرة القطاعات على تبادل المعلومات البينية وتقديم الخدمات فيما بينها وبين المواطنين بسرعة فائقة ودقه عالية وبأقل تكلفة ممكنة مع ضمان السرية وأمن المعطيات المتداولة فهي نظام افتراضي يمكن الأجهزة الحكومية من تأدية التزاماتها لمواطنيها والمستفيدين من خدماتها وذلك باستخدام التقنية الالكترونية المتطورة (د. محمد محمود الخالدي، ص 70 - 71. انظر كذلك: د. عبد الفتاح بيومي حجازي، ص 9 وما تليها).

ويرى جانب من الفقه أن مدلول الحكومة الإلكترونية ترتبط بتعظيم استخدام التكنولوجيا الحديثة في تحرير المعلومات والخدمات من اجل التغلب على القيود والعوائق وهذا لما يحققه من مزايا وفوائد كتبسيط الإجراءات والتنسيق ما بين مصالح الحكومة وتحسين التعاون والإدارة والتقليل من الوقت المستغل للقيام بالأعمال ومنه إفادة المواطنين وتسهيل الحصول على المعلومة (د. عبد الفتاح بيومي الحجازي، ص 20 وما تليها).

المطلب الثاني: مرتكبوا جرائم المعالجة الآلية للمعطيات.

عند تحديد مجرمي المعلوماتية ظهر عدة أصناف من المجرمين (د. علي عبد القادر القهوجي، ص 1) يختصون في الاعتداءات على نظام المعالجة الآلية للمعطيات للحكومة الالكترونية وما ينجر عنها من مساس بالبيانات والمعطيات الآلية وفي هذا الصدد اتجه الباحثون إلى الإقرار بأن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء ويعد من أفضل التصنيفات لمجرمي التقنية الذي أورده David icove, Paul serger et William Vonstouch في مؤلفهم " جرائم الكمبيوتر" الصادر عام 1995 حيث تم تصنيف مجرمي المعلوماتية إلى ثلاثة طوائف وهم: المخترقون، المحترفون والحاقدون وستناول كل صنف من هاته الأصناف في فرع مستقل.

الفرع الأول: المخترقون.

هم طائفة تقوم على اختراق المواقع ومحاولة التسلل إلى المعطيات الآلية ويندرج تحت هاته الطائفة نوعين من المخترقين أو المتطفلين:

أولاً: الهاكرز **les hackers** أو الهاكر (**hacker**) أو المتسلل هو شخص بارع في استخدام الحاسب الآلي وبرامجه ولديه فضول في استكشاف حسابات الآخرين وبطرق غير مشروعة (ورد هذا التعريف في رسالة للماجستير وبالضبط في ملحق لهذه الدراسة خصص للمفاهيم الأساسية المتداولة في جرائم الحاسوب والانترنت، هذه الدراسة قام بها الطالب: محمد بن عبد الله بن علي المنشاوي تحت عنوان: جرائم الانترنت في المجتمع السعودي، تاريخ المناقشة 29-04-2003. انظر كذلك: يعقر الطاهر - بسكري حليم، 11/10/09 مارس 2008 ص 19).

فالهاكرز وكما يدل على ذلك اسمهم، هم متطفلون يتحدون إجراءات أمن نظم الشبكات، لكن لا تتوفر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات الذات (Mohammed bozobar mars 2002, p: 45) وتتألف هذه الطائفة أساساً من مراهقين وشباب - طلبة وتلاميذ الثانويات - وشباب عاطل عن العمل (حسب دراسة قام بها مكتب التحقيقات الفدرالي الأمريكي (**federal bureau of investigation FBI**) غالبية الهاكرز الأكثر خطورة هم فئة الشباب المتراوحة أعمارهم بين 18-35 سنة).

ثانياً: طائفة الكراكرز **les crackers** الكراكر أو المقتحم وهو شخص يقوم بالتسلل إلى نظم الحاسوب والإعلام الآلي للإطلاع على المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها والقيام بأعمال من شأنها أن تعطل أداء عمل الجهاز

والمساس بالمعطيات، ولقد تم استعمال هذا المفهوم سنة 1985 من طرف الطائفة الأولى طائفة الهاكرز للرد على الاستعمال السيئ للصحفيين لمصطلح الهاكرز. (Bouchaib RMAIL, Fès, 2005, p: 82.)

وما يلاحظ على هاته الفئة أنها استفادت هذه كثيرا من التقنيات التي طورتها فئة الهاكرز وبدؤوا يستخدمونها استخداما سيئا في اعتداءات التي تنم عن ميول إجرامية لدى مقترفيها. والسمة المميزة الأخرى لهذه الطائفة هي تبادلهم للمعلومات والخبرات الفنية في مجال المعلوماتية وكيفيات الاختراق فيما بحيث وصل الأمر بهم إلى تنظيم هذه نفسها بعقد مؤتمرات لمخترقي الكمبيوتر يدعى له الخبراء منهم للتشاور حول وسائل الاختراق ووسائل تنظيم عملهم وكيفية.

الفرع الثاني: المحترفون.

يظهر لدى هذه الفئة ما يسمى بالتقنية المعلوماتية إذ أنها تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب عن طريقها، ولذلك فإن هذه الطائفة تعد الأخطر من بين مجرمي التعدي على المعطيات الآلية من خلال الكمبيوتر والانترنت حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم وللجهات التي كلفتهم وسخرتهم لارتكاب جرائم المعلوماتية (هناك من يطلق عليها جرائم الانترنت ونجد كذلك جرائم الحاسوب والجريمة المعلوماتية والغش المعلوماتي وقد نظمها ونص عليها المشرع الفرنسي في المواد من 1/323 إلى المادة: 8/323 من قانون العقوبات الفرنسي).

كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي يخدم مصالح معينة أو آراء أو اتجاهات فكرية.

وتعتبر هذه الطائفة كتومة مقارنة بالطائفة الأولى إذ أنها طائفة تهدف إلى احتراف التسلل والمساس بالمعطيات الآلية وترقية مجال التقنية والمعرفة لديها والتنظيم العالي والتخطيط المحكم للأنشطة الإجرامية التي تقوم باقترافها، فهي طائفة تنعدم تبادل المعلومات فيما بينهم بل يقومون فقط بتطوير مهاراتهم الخاصة ويحاولون قدر الإمكان عدم الكشف عن التقنية التي اعتمدها في ارتكاب الجرائم، وما يلاحظ على هذه الفئة أن الغالبية منهم تتراوح أعمارهم ما بين 25 و 40 سنة.

الفرع الثالث: الحاقدون

تعتبر هذه الطائفة مختلفة تماما عن الطائفتين السابقتين كونها طائفة لا يعرف عنها هدفها الإجرامي والأغراض التي ارتكبت الجرائم لأجلها، كونها طائفة لا تهدف إلى إثبات قدرتهم على التسلل أو الاختراق ولا يسعون إلى مكاسب مادية أو سياسية، إنما يحرك

أنشطتهم الرغبة في الانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم أو مكان عملهم عندما يطردون أو في مؤسسة لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة، أو إلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم.

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية والقدرة العالية في مجال المعلوماتية، ومع ذلك فانه يسعى الفرد منهم في الوصول إلى كافة عناصر المعرفة المتعلقة بالفعل الإجرامي الذي ينوي ارتكابه، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم أو إتلاف كل أو بعض معطياته، أو نشاط إنكار الخدمة وتعطيل النظام أو الموقع المستهدف إن كان من مواقع الإنترنت.

وما يلاحظ على هذه الفئة انه ليس لها ضوابط محددة بشأن أعمارهم، كما أنها طائفة لا يوجد علاقات وتفاعلات ما بين أعضائها، فهي طائفة تهدف إلى إخفاء أعمالها والتستر عليها لكي لا ينكشفون من طرف الجهات المتخصصة في الكشف على هذا النوع من الجرام، وبالمقابل فهم الطائفة الأسهل من حيث الكشف عليهم وعلى أنشطتهم الإجرامية لتوافر عدة عوامل مساعدة.

المبحث الثاني: صور الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

إن حرمة حماية بيانات الحكومة الالكترونية بادر إلى توجيه الأنظار إلى طائفة من الأفعال في بيئة المعالجة الآلية للبيانات تقتضي مصلحة المجتمع إدخالها في دائرة التجريم والعقاب تمثل هذا في صور الاعتداء على المعطيات الآلية للحكومة الالكترونية (د. سهير لطفي، 1990 ص 129) والذي يأخذ صورتين أساسيتين في قانون العقوبات الجزائري، وذلك على غرار ما قضى به المشرع الفرنسي وعليه سوف نتناول بالدراسة في المطلب الأول الصورة الأولى وهي الدخول في منظومة المعطيات الآلية للحكومة الالكترونية وفي مطلب ثاني نتطرق إلى المساس بالمنظومة المعطيات الآلية للحكومة الالكترونية.

المطلب الأول: الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات.

نص المشرع الجزائري على الدخول والبقاء في نظام المعالجة الآلية للمعطيات في نص المادة 394 مكرر من قانون العقوبات الجزائري وتقابلها المادة: 1/323 من قانون العقوبات الفرنسي، كما نصت عليها المادة 02 من الاتفاقية الدولية للإجرام المعلوماتية

باستثناء هاته المواد نجد أن هناك صورتين من صور الاعتداء على المعطيات الآلية للحكومة الاليكترونية، ولم يحدد المشرع الفرنسي وسيلة الدخول إلى النظام أو اختراقه فيجوز إذن الدخول إلى النظام بأي وسيلة تقنية ومن ذلك انتهاك كلمة السر الحقيقية "Passe Word" أو عن طريق فك الشيفرة متى كان الجاني غير مخول في استخدامها أو عن طريق استخدام برنامج خاص.

كما يمكن كذلك استخدام الرقم السري لشخص آخر أو الدخول من خلال شخص مسموح له بالدخول، ومن صور الدخول غير المشروع كذلك أن يكون مالك النظام قد وضع قيودا على الدخول إليه ولم يحترم الجاني هذه القيود، أو كان الأمر يتطلب سداد مبلغ من النقود لم يسدها الجاني، وتحايل وقام بالدخول غير المشروع إلى النظام.

والملاحظ أن المشرع يعاقب على الدخول المجرد إلى النظام المعلوماتي، ذلك أن مجرد الدخول إلى النظام تقوم به الجريمة حتى لو لم يترتب على دخوله ضرر أو يتحقق له من وراء الدخول فائدة، طالما أن الدخول غير مشروع، ويتحقق فعل الدخول متى دخل الجاني إلى النظام كله أو جزء منه، كالدخول إلى طرفية الحاسب أو شبكة الاتصال أو البرنامج، كما يتحقق الدخول غير المشروع متى كان مسموحا للجاني بالدخول إلى جزء معين من البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه.

ويعرف البقاء غير المشروع بأنه: "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"، ففعل البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات فقد كان الهدف من تجريمه هو تجريم البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات لمن كان دخوله إلى النظام بطريق الصدفة البحتة، وانتفى لديه القصد الجنائي ومع ذلك يبقى داخل النظام وتنصرف إرادته إلى ذلك، حيث يعاقب الجاني على الجريمة العمدية لأن إرادته انصرفت إلى البقاء داخل النظام رغم علمه بأن دخوله غير مشروع (د. جميل عبد الباقي، سنة 1992 ص 20) وذلك الحكم ينصرف إلى من هو مسموح له بالدخول إلى جزء من النظام ثم يدخل إلى جزء آخر غير مصرح له بالدخول فيه (قارة أمال، سنة 2006 الجزائر ص 110. انظر كذلك: على عبد القادر القهوجي، ص ص 53-54).

كما يعد صورة للبقاء غير المشروع أيضا أن يظل الجاني باقيا داخل النظام بعد المدة المحددة له للبقاء داخله أو في الحالة التي يطبع فيها نسخة من المعلومات، في الوقت الذي كان مسموحا له بالرؤية والاطلاع فقط

ومفهوم الدخول والبقاء غير المشروع على النحو السابق يمثل مفهوما للنشاط الإجرامي سواء في صورته البسيطة أو المشددة وهو ما سنتطرق له بحيث نتناول تحت هذا المطلب فرعين نتطرق في الفرع الأول إلى الصورة البسيطة لفعل الدخول أو البقاء غير المشروع وفي الفرع الثاني إلى الصورة المشددة للعقاب على فعل الدخول أو البقاء غير المشروع وفيها تضاعف العقوبة المقررة للجريمة في صورتها البسيطة.

الفرع الأول: الصورة البسيطة.

تتحقق الصورة البسيطة بفعل الدخول غير المشروع أو البقاء غير المشروع في النظام الذي تم اختراقه، وتعد هذه الجريمة بمثابة الصورة البسيطة لأن المشرع الفرنسي عاقب عليها بالحبس مدة سنة وغرامة مائة ألف فرنك فرنسي، وضاعف العقوبة متى اقترن بها ظرف مشدد، وهذا ما ذهب إليه كذلك المشرع الجزائري إذ نص في المادة: 1/394 مكرر من قانون العقوبات على الصورة البسيطة وفي الفقرة الثانية ضاعف العقوبة إذا اقترنت بظرف مشدد وحتى تتحقق هاته الجريمة في صورتها البسيطة يجب تحقق فعل الدخول غير المشروع أو البقاء غير المشروع كما سبق واشرنا أو أن يتحققا معا (د. احسن بوسقيعة، ص 445).

وجريمة الدخول على النظام أو البقاء فيه هي من الجرائم العمدية التي تقوم على القصد الجنائي العام الذي يتكون من عنصري العلم والإرادة، ذلك أنه يجب أن يعلم الجاني في مجال المعلوماتية بأنه لا يحق له الدخول أو البقاء داخل النظام والمساس به، وأن ذلك ضد رغبة مالك النظام أو صاحب السيطرة عليه، ومع ذلك تنصرف إرادته إلى إثبات هذا الفعل بالمخالفة للقانون وبالمخالفة لإرادة صاحب النظام أو صاحب الحق فيه.

ولهذا يرى جانب من الفقه أن الدخول يكون مشروعاً متى كان بطريق الصدفة أو السهو أو الخطأ وعلى الشخص الذي دخل بهذه الطريقة أن يقوم بالانسحاب فوراً من النظام، فإذا لم ينسحب منذ هذه اللحظة فإنه يتوافر في حقه القصد الجنائي العام لارتكاب هذه الجريمة ويعاقب عليها، بينما يرى جانب آخر من الفقه أن الدخول بطريق السهو أو الخطأ أو المصادفة هو سلوك يتسم بعدم المشروعية وهو فعل يناهز القانون لكن المشرع لا يعاقب عليه لانتفاء القصد الجنائي (علي عبد القادر القهوجي، ص 54)

فالركن المعنوي لا يتوافر متى كان دخول الجاني أو بقاءه داخل النظام مسموح به أي مشروعاً، كذلك لا يقوم القصد الجنائي إن وقع الجاني في خطأ يتعلق بحقه في الدخول أو

حقه في البقاء أو في مدى نطاق هذا الحق كأن يجهل وجود حظر للدخول أو البقاء أو كان يعتقد خطأ أنه مسموح له بالدخول (د. احسن بوسقيعة، ص 445).

ولذلك فمتى توافر القصد الجنائي بعنصرية العلم والإرادة، فإنه لا محل للاعتداد بالبائع والدافع على ارتكاب الجريمة، وبالتالي تقوم الجريمة ولو كان البائع على الدخول إلى النظام أو البقاء فيه الهدف منه محاولة الفضول أو النزهة أو إثبات القدرة على الانتصار على النظام المعلوماتي أو إثبات المهارات والذكاء في مجال المعلوماتية (قارة أمال، ص ص 112-113).

الفرع الثاني: الصورة المشددة.

تتحقق هذه الجريمة في صورتها المشددة، متى ترتب على الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام ذاته لأن يؤدي وظيفته (قارة أمال، ص 113 وما تليها).

ويكفي لتوافر هذا الظرف المشدد، أن يكون هناك علاقة سببية ما بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت، وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات، وهذه النتيجة ذاتها هي التي اعتبرها المشرع ظرفا مشددا في هذه الجريمة، وهذه الجريمة عمدية يتعين لقيامها توافر القصد الجنائي العام لدى الجاني بعنصريه العلم والإرادة، فإذا أثبت الجاني انتفاء علاقة السببية بين السلوك الإجرامي - الدخول أو البقاء غير المشروع - والنتيجة الإجرامية التي هي ذات الظرف المشدد في الجريمة، كأن يثبت تعديل أو محو المعطيات أو عدم صلاحية النظام للقيام بوظائفه يرجع إلى قوة قاهرة أو حادث فجائي انتفى السلوك الإجرامي ومنه ينتفي القصد الجنائي لدى الجاني، وإذا توافرت أركان جريمة الدخول أو البقاء غير المشروع في صورتها المشددة، أنزلت العقوبة بالجاني حسب ما هو مقرر في قانون العقوبات.

المطلب الثاني: جريمة التلاعب في بيانات نظم المعالجة الآلية للمعطيات.

نص المشرع الجزائري على هاته الصورة من التجريم (المادة 394 مكرر 2 من قانون العقوبات الجزائري وهي تقابل المادة 3/323 من قانون العقوبات الفرنسي لسنة 1994، كما تقابلها المواد 03-04-08 من الاتفاقية الدولية للإجرام المعلوماتي)، حيث عاقب كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو تلاعب بطريق الغش في المعطيات الآلية التي تضمنها.

وبناء على هذا فإن المشرع لا يحمي نظام البيانات من الناحية المادية بقدر ما يوفر الحماية للمعلومات الموجودة داخل النظام ذاته، وذلك ضد أي نشاط إجرامي وهو ما يطلق

عليه تسمية القرصنة المعلوماتية التي يهدف من ورائها الجاني إلى أن يحقق النظام المعلوماتي نتائج أو معطيات غير تلك التي كان يجب أن يحققها والنشاط الإجرامي في هذه الجريمة يتمثل في أفعال الإدخال، المحو والتعديل، ويكفي توافر إحداها لقيام الجريمة، فلا يشترط اجتماعها معا حتى يتوافر النشاط الإجرامي فيها ومن ثم قيام الركن المادي للجريمة، فهذه الجريمة تقع على بيانات نظم المعالجة الآلية للمعطيات أي البيانات المعالجة دون المعلومة ذاتها، ولذلك يخرج من نطاق هذه الجريمة المعلومات التي لم تعالج بعد ونتطرق إلى حالات هذا التلاعب من خلال ثلاث فروع نتناول في الفرع الأول فعل الإدخال وفي الفرع الثاني فعل المحو وفي الفرع الثالث فعل التعديل.

الفرع الأول: فعل الإدخال.

يتحقق فعل الإدخال بإضافة معطيات جديدة على الدعامة الخاصة به سواء كانت خالية أم يوجد عليها معطيات من قبل ومن صور إدخال المعلومات المصطنعة "اختلاس النقود عن طريق الغش المعلوماتي" ويتحقق كذلك فعل الإدخال في القرص الذي يتمكن فيه الحامل الشرعي لبطاقة السحب الممغنطة والتي تسحب النقود من البنوك وتحديدًا أجهزة السحب الآلي، وذلك حين يستخدم رقمه الخاص -السري- للدخول كي يسحب مبلغًا أكثر من ذلك المبلغ المسموح به لصاحب البطاقة، أو في حالة إدخال فيروس (الفيروس المعلوماتي هو عبارة عن برنامج له أهداف تدميرية، الغرض منه إحداث أضرار جسيمة بنظام الحاسب الآلي سواء ببرامجه أو بمكوناته، فهو أي الفيروس برنامج مكتوب بإحدى لغات البرمجة من قبل مبرمجين وهذا البرنامج قادر على التوالد والتناسخ ويستطيع الدخول إلى برامج لها إمكانية اختراق نظم التشغيل والتخزين وقد ظهر الفيروس في نهاية الأربعينيات وكان أول من فكر فيه هو اختصاصي الكمبيوتر "جون فون نيومان" وذلك خلال نشر مقاله يتعلق بالفيروسات. لمزيد من التفصيل انظر: الدكتور: علاء عبد الرزاق محمد السالمي، سنة 2005 ص 207 وما يليها، انظر كذلك: قارة آمال، ص 118). "حصان طروادة" (حصان طروادة: هو برنامج خادع يخفي ظاهره غرضًا غير مشروع، إذ أنه يظهر كبرنامج عادي يؤدي بعض المهام المفيدة والمعتادة لمستخدميه بينما يكون موجودًا بطريقة خفية داخله وهو برنامج كثير الانتشار في نظم الحاسب الآلي يهدف إلى محو البيانات من ذاكرة الحاسب أو التهديد بمحوها ويكون ذلك على البيانات والمعطيات المدخلة أو المخزونة، لمزيد من التفصيل انظر هامش: قارة آمال، ص 116). أو "قنبلة معلوماتية" أو برامج الدودة (يعتبر برنامج الدودة برنامج تشغيل تنقل من حاسب إلى آخر مغطيه شبكة بأكملها عبر الوصلات التي تربط بينها وأثناء عملية انتقالها تتكاثر كالبكتيريا بإنتاج عدة نسخ منها وتهدف إلى التقليل من كفاءات نظم الحاسب الآلي وقد تتعدى ذلك إلى التخريب الفعلي للملفات والبرامج ونظم التشغيل وتسمى باسم: "دودة موريس" وكذلك اسم "انترنت" وقد ادخل هذا البرنامج إلى نظم الحاسب الآلي بتاريخ: 1988/11/03 عن طريق إحدى وسائل الربط والاتصال، لمزيد من التفصيل انظر هامش: قارة آمال، ص 117). تؤدي إلى إضافة وإدخال معطيات جديدة (قارة آمال، ص 121).

ومن التطبيقات القضائية قضي في فرنسا بأنه يقع تحت طائلة نص المادة 3/323 من قانون العقوبات وتقابلها المادة: 394 مكرر 1 من قانون العقوبات الجزائي كل من تعمد إدخال فيروس المعلوماتية في برامج الحاسب الآلي وكذا الامتناع عن إخبار الغير عن هذا الإدخال ولو كان ذلك بصفة عرضية (د. احسن بوسقيعة، ص 446).

الفرع الثاني: فعل المحو.

يقصد به إزالة جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة ويعد هذا الفعل مساسا خطيرا بالمعطيات الآلية إذ انه يمكن أن يزيل دعامة أساسية تؤدي مهامها داخل النظام عن طريق الحاسب الآلي (قارة أمال، ص 122).

الفرع الثالث: فعل التعديل.

ويقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى وقد يتم التلاعب في المعطيات عن طريق استبدالها أو عن طريق التلاعب في البرنامج، وذلك بإمداده بمعطيات مغايرة تؤدي إلى نتائج مغايرة عن تلك التي صمم البرنامج لأجلها (قارة أمال، ص 122).
وكقاعدة عامة فإن المحو أو التعديل للمعطيات الموجودة في النظام، كصورتين للركن المادي في جريمة الاعتداء على نظام المعالجة الآلية للمعطيات، يتم عن طريق برامج خبيثة (البرامج الخبيثة هي برامج ذات أهداف مختلفة كالاغتيال والاستيلاء بواسطة الحاسبات على المال وقد ظهرت هذه البرامج بعد فترة وجيزة في الشروع في استعمال الحاسبات ومن بين اخطر هذه البرامج تلك البرامج التي ينتج عن إدخالها تحقيق أغراض إجرامية، لمزيد من التفصيل انظر هامش: قارة أمال، ص 116). تتلاعب في هذه المعطيات وذلك بمحوها كلياً أو جزئياً أو بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات سواء أكانت منطقية أو زمنية.

المطلب الثالث: العقوبات المقررة عن جرائم المساس بالمعطيات الآلية.

يقرر الجزاء (تعتبر برامج محمية بحيث أنها تبقى ساكنة وغير فعالة وغير مكتشفة لمدة زمنية تصل إلى شهر أو حتى أعوام وهذه المدة يحددها مؤشر زمني يحتويه البرنامج كتاريخ معين داخل نظام التشغيل بحيث ينشط البرنامج عند حلوله ويؤدي مهامه الهدامة وقد لا يرتبط مؤشر التفجير بالزمن، وإنما يكون بشروط منطقية معينة داخل نظام التشغيل أو داخل برنامج أو ملف وذلك حسب ما يحدده مبرمج القنبلة، فيمكن أن يكون مؤشر التفجير إدخال أو عدم إدخال بيان ما إلى نظام المعالجة الآلية للمعلومات المخزنة في الحاسب الآلي أو بمجرد الاتصال بمستخدمي الحاسب يكون لديهم القنبلة وتحقق هذه القنابل عدة أغراض أبرزها تأخير تفجير لجعل اقتفاء اثر معدي القنابل صعب وتعقبهم أكثر صعوبة أو متعذراً لما تنطوي عليه هاته التقنية على ذكاء مقترفيها، لمزيد من التفصيل انظر: قارة أمال، ص 117). لكل جريمة ارتكبت وتختلف الجزاءات المقررة لكل جريمة حسب طبيعتها ومقدار الخطورة التي تتوافر في

مرتكبيها وسوف نتناول في الفرع الأول العقوبة المقررة لكل جريمة وفي الفرع الثاني نتطرق إلى القواعد المشتركة بين كل الجرائم (د. أحسن بوسقية، ص 446).

الفرع الأول: العقوبة المقررة لكل جريمة.

نتناول بالإشارة في هذا الفرع إلى ما نص عليه المشرع الجزائي وما قرره من عقوبات على جرائم المساس بالمعطيات الآلية:

أ- الدخول في منظومة معلوماتية أو البقاء فيها: نصت عليها المادة: 394 مكرر من قانون العقوبات والتي تعاقب على هذا الفعل بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000 دج إلى 200.000 دج وتطبق العقوبات ذاتها على المحاولة.

تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة من ستة أشهر إلى سنتين والغرامة من 50.000 دج إلى 300.00 دج.

ب- المساس بمنظومة معلوماتية: نصت عليها المادة 394 مكرر 1 من قانون العقوبات وتعاقب على هذا الفعل بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 4.000.000 دج.

ج- الأعمال الأخرى: نصت عليها المادة 394 مكرر 2 وتعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 10.000.000 دج كل من يقوم عمدا وعن طريق الغش بـ:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلّة عن طريق منظومة معلوماتية يمكن أن ترتكب بها إحدى الجرائم المذكورة أعلاه.
- حيازة أو إفشاء أو استعمال لأي غرض كان المعطيات المتحصلة من إحدى الجرائم المذكورة أعلاه.

الفرع الثاني: القواعد المشتركة بين كل الجرائم (د. أحسن بوسقية، ص 447) تعتبر جرائم

المساس بالمعطيات من الجرائم ذات القواعد المشتركة

1- مضاعفة العقوبة طبقا للمادة 394 مكرر 3 والتي تضاعف العقوبة

بمقتضاها العقوبات المقررة لجرائم الحاسب الغش المعلوماتي إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات اشد.

2- المشاركة في جمعية أشرار طبقا للمادة 394 مكرر 5 من قانون العقوبات وتكون مقررة لكل من شارك في مجموعة أو في اتفاق تالف بغرض الإعداد لجريمة أو أكثر من جرائم الغش المعلوماتي وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها.

المصادرة طبقا للمادة 394 مكرر 6 من قانون العقوبات مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة والبرامج (د. علي عبد القادر القهوجي، ص ص 48-49).

3- الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من جرائم الغش المعلوماتي، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكيها.

4- الجزاء المقرر للشخص المعنوي طبقا للمادة 394 مكرر 4 من قانون العقوبات يعاقب الشخص المعنوي الذي يرتكب إحدى جرائم الغش المعلوماتي بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

5- الشروع أو المحاولة طبقا للمادة 394 مكرر 7 من قانون العقوبات بنصها يعاقب على الشروع في ارتكاب جنح الغش المعلوماتي بالعقوبة المقررة للجنحة ذاتها.

خاتمة

من خلال دراستنا هذه توصلنا إلى أن صور الاعتداء على الحكومة الالكترونية عديدة على الرغم من أنها تنحصر في صورتين أساسيتين وقد حاول المشرع الجزائري الإلمام بجوانبها من خلال وضع آليات ردعية جرمت المساس بأنظمة المساس بالمعطيات الآلية للحكومة الالكترونية خاصة وأنها نتجه نحو عالم الرقمية الذي أصبح لزاما على تشريعات الدول ومنها التشريع الجزائري إيجاد قوانين منظمة وآليات تحدد كفاءات وإجراءات تنظيم الحكومة الالكترونية وتقرير الحماية الجنائية لها سواء كانت واقعة على المعلومات في حد ذاتها أو في نظم التشغيل وعليه يتبين لنا أن حماية الحكومة الالكترونية ضرورة ملحة لمواكبة التطور العلمي الحاصل والتكنولوجية الحديثة والمضي قدما باعتبار أن البشرية في تطور وتغير مستمر والمشرع الجزائري من خلال نصه على تجريم الغش المعلوماتي يكون بذلك مواكبا للمتغيرات الحاصلة على المستوى العالمي.

إن خطورة هذه الجريمة تتمثل في خطورة صور الاعتداء على الشبكة المعلوماتية وبيانات ومعطيات الحكومة الالكترونية تحتم على تشريعات الدول ومنها التشريع الجزائري

على تكتيف التعاون والجهود الدولية بهدف السيطرة على المجرمين في مجال المعلوماتية والسيطرة على العصابات التي تهدف إلى تدمير الأنظمة والمساس بالمعطيات، ووضع آليات تنفيذية تعمل على تفكيك هذه العصابات والحيلولة دون تحقيق أهدافها ومآربها وعليه فإن المشرع الجزائري اتخذ التدابير اللازمة لمحاربة الغش المعلوماتي ولكن لا يزال ذلك في بداياته نظرا لعدم تحقق مفهوم الحكومة الالكترونية بالمعنى الحقيقي لها على غرار بعض دول العالم والمشرع الجزائري رغم انه جاء متأخرا في النص على الغش المعلوماتي ونعزي ذلك إلى تأخر الجزائر عن الدخول في المنظومة المعلوماتية العالمية إلا انه حاول جاهدا من خلال مجموع النصوص القانونية سواء في قانون الإجراءات الجزائية أو قانون العقوبات أو قانون الملكية الفكرية أن يلم بالجريمة المعلوماتية وصور الاعتداء والمساس بمعطيات الحكومة الالكترونية وينص عليها محاولا بذلك مسايرة التطورات الحاصلة في عالم الرقمية من جهة ومحاربة الأنماط المستحدثة في مجال الإجرام المعلوماتي.

وعليه من خلال دراستنا هذه توصلنا إلى وضع الاقتراحات التالية:

- 1- إيجاد مفهوم يتلاءم مع الجريمة المعلوماتية وعالميتها وشموليتها بحيث يكون مفهوما متفقا عليه في ظل تطور الاستعمال الآلي للمعطيات والبيانات الحكومية.
- 2- إيجاد تعاون دولي مفاده التنسيق ما بين المصالح الأمنية والقضائية والتوفيق ما بين التشريعات وتنظيم دورات تكوينية للقضاة في مجال المعلوماتية.
- 3- تخصيص جهات أمنية متخصصة في متابعة جرائم المساس بالمعطيات الآلية للحكومة الالكترونية تكون لديها الإلمام بالحاسب الآلي من خلال خلق فرق تقنية تقوم بالمتابعة في هذه الجريمة.
- 4- وضع تشريعات ردعية من حيث إجراءات المتابعة الجزائية والعقوبات المقررة تتلاءم مع الأنماط المستحدثة في عالم الاعتداء على بيانات ومعطيات الحكومة الالكترونية من الناحية الفنية والناحية العملية من شأنها تحقيق الأمن المعلوماتي.
- 5- توحيد التشريع الخاص بالجريمة المعلوماتية في قانون خاص بها يحدد ماهيتها وإجراءات المتابعة والجزاءات ومختلف الأحكام القانونية التي تنظمها.
- 6- خلق آلية رقابة مشددة على مقاهي الانترنت وإخضاعها للقانون المنظم للجريمة المعلوماتية في حالة ارتكاب جرائم من خلالها وإلزام أصحابها بضرورة الحماية والتبليغ في حالة الشبهة.

- 7- إنشاء لجنة متخصصة تتولى صياغة القوانين والتشريعات التي تتلاءم والمتغيرات الحاصلة في مجال البيانات على مستوى البرلمان.
- 8- إنشاء لجنة متابعة خاصة على غرار لجنة متابعة جريمة تبييض الأموال ينحصر عملها في إعداد التقارير والتنسيق بين المصالح القضائية والأمنية وإخطارهم عن وجود الشبهة في الجريمة المعلوماتية وذلك من خلال خلق مراكز متخصصة في التعقب والتحري عن الجريمة المعلوماتية.
- 9- نشر التوعية وثقافة المعلوماتية لدى مستخدمي التقنية وتعميم المناشير والتنبيه إلى المخاطر جراء الاستعمال اللاعقلاني والاعتداءات على بيانات ومعطيات الحكومة الالكترونية.
- 10- تحذير الآباء من مخاطر الانترنت المنزلي وترشيد أبنائهم من الاستعمال السيئ له.
- 11- عقد الملتقيات وندوات وطنية وجهوية ودولية بين التقنيين والخبراء في مجال المعلوماتية لتبادل المعلومات وتفعيل الدور الوقائي من الاعتداءات على الحكومة الالكترونية.

المراجع

أولاً: باللغة العربية:

أ- الكتب:

- 1- د. جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة سنة 1992.
- 2- د. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة طبعة سنة 1992.
- 3- د. هشام محمد فريد رستم، قانون العقوبات ومخاطر التقنية المعلوماتية، مكتبة الآلات الحديثة سنة 1992.
- قارة آمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه الطباعة والنشر والتوزيع الطبعة الأولى سنة 2006 الجزائر.
- 4- د. عبد الفتاح بيومي الحجازي، النظام القانوني للحكومة الالكترونية، الكتاب الأول الحكومة الالكترونية، دار الكتب القانونية، دار شات للنشر والبرمجيات، 2007.
- 5- د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب، دار الجامعة الجديدة للنشر الإسكندرية، سنة 1997.
- 6- د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت لبنان سنة 1999.

7- د. عبد الفتاح بيومي حجازي، النظام القانوني للحكومة الالكترونية، الكتاب الثاني، الحماية الجنائية والمعلوماتية للحكومة الالكترونية، دار الكتب القانونية دار شات للنشر والبرمجيات، مصر سنة 2007.

8- د. علي حسون الطائي، الحكومة الالكترونية وإمكانيات تطبيقها في العراق"، كلية الإدارة والاقتصاد، جامعة بغداد 2008.

9- د. علاء عبد الرزاق محمد السالمي، شبكات الإدارة الالكترونية، دار وائل للنشر، الطبعة الأولى سنة 2005

10- د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها من قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر سنة 1998.

11- د. محمد محمود الخالدي، التكنولوجيا الالكترونية، دار كنوز المعرفة للنشر والتوزيع، الطبعة الأولى سنة 2007.

12- د. محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة غريب، القاهرة سنة 1984.

13- د. ماجد عمار، المسؤولية القانونية الناشئة عن استخدام فيروس برامج الكمبيوتر ووسائل حمايتها، دار النهضة العربية، القاهرة طبعة 1989.

ب- المقالات والملتقيات:

14- د. محمد ناجي، أمن المعلومات، من ينتصر في النهاية، مجلة الشرطة، العدد 342.

15- د. سهير لطفي، تقرير حول ندوة الجرائم الاقتصادية المستحدثة المنعقدة في 20-21/04/2001 مجلة حق المؤلف بين الواقع والقانون، مركز الدراسات القانونية، جامعة القاهرة، دار النشر هايتي 1990.

16- يعقر الطاهر - بسكري حليم، النظام القانوني للمجتمع الالكتروني، مداخلة أقيمت في الملتقى الوطني الأول حول القانون وقضايا الساعة، معهد العلوم القانونية والإدارية، المركز الجامعي خميس مليانة، أيام: 11/10/09 مارس 2008.

ج- المذكرات والرسائل:

17- إبراهيمي سهام، الجريمة المعلوماتية، مذكرة تخرج من المدرسة العليا للقضاء، الدفعة الخامسة عشر، الجزائر.

18- محمد بن عبد الله بن علي المنشاوي، رسالة ماجستير تحت عنوان: جرائم الانترنت في المجتمع السعودي، تاريخ المناقشة 29-04-2003.

ثانيا: المراجع باللغة الفرنسية.

- 1- Bouchaib RMAIL, la criminalité informatique, criminalité a double dimension internationale, thèse pour l'obtention du grade de docteur en droit privé- option: droit des affaires, faculté des sciences juridiques, économiques et sociales- Fès, 2005.
- 2- Champy, Essai de définition de la fraude informatique ; R.S.C. 1988.n 3.
- 3- Gassin: le droit pénal de l'informatique.les systèmes de traitements automatique des données. Commentaire de la loi n°88/18 du03/01/1988 relative à la fraude informatique. J.C.P1988.doct.
- 4- Mohammed bozobar, la criminalité informatique sur l'Internet, journal of Law n 1- val 26, mars 2002.
- 5- Tiedemann ,fraude et autres délits d'affaires commis à l'aide d'ordinateurs électroniques.R.D.P.C 1984 n° 7.