العلاقة بين الجريمة المعلوماتية وتطور الإدارة الالكترونية

د/ عباس زواوي
جامعة بسكرة

الملخص :

سنقوم من خلال هذه الدراسة بمحاولة تسليط الضوء على مفهومين من المفاهيم المستحدثة التي أفرزها التطور التكنولوجي الذي اجتاح العالم المعاصر في مجال الاتصال وتداول المعلومات، وهما الجريمة المعلوماتية والإدارة الالكترونية بمحاولة تحديد العلاقة بينهما، فرغم توجه الإدارة إلى بلورة فكرة تداول العمل الإداري معلوماتيا لمحاولة الاستفادة من التطور في تسيير المرافق العامة لخدمة و إشباع حاجات الأفراد بتقريب الإدارة من المواطن في أي مكان وأي وقت من جهة، و تمكينه من الحصول على الوثائق التي يحتاجها بعيدا عن الماديات و الأوراق من جهة أخرى، يبقى دائما مرتبط بتخوف كل من الإدارة أو الأفراد من التعامل الالكتروني نتيجة استفحال الجرائم المعلوماتية التي أصبحت تمس المعلومات الإدارية المخزنة في أجهزة الحاسوب أو المتداولة عبر شبكة الانترنت إما بالتزوير أو الإتلاف و غيرها من صور التلاعب التي تتم من طرف أشخاص على درجة من الذكاء و التحكم في التعاملات التقنية، هذا ما يزيد من خطورة الجريمة المعلوماتية و يجعلها عائق أمام تطور الإدارة الالكترونية، و أكبر خطر من المخاطر المهددة لها.

Résumé :

Nous tenteront à travers la présente étude de faire la lumière sur deux des concepts innovants apportés par le développement technologique qui a envahi le monde moderne dans le domaine de la communication et de circulation de l'information ; à savoir: la cybercriminalité et l'administration électronique et ce, en tentant de déterminer la relation entre les deux.

Bien que l'administration tend à diriger essentiellement l'idée de circulation du travail administratif informatiquement afin d'essayer de profiter de l'évolution dans la gestion des utilités publiques pour servir et satisfaire les besoins des individus en rapprochant l'administration du citoyen en tout lieu et temps, d'une part, et lui permettre d'obtenir les documents nécessaires, loin du matérialisme et des feuilles, d'autre part, il demeurera toujours une crainte de l'administration et des individus des transactions électroniques en raison de la propagation de la cybercriminalité qui touches, de nos jours, les informations administratives stockées sur les ordinateurs ou en circulation dans les réseaux d'internet; soit par la falsification, l'endommagement ou par d'autres actes de manipulation faites par des personnes d'un certain degré d'intelligence et de maitrise dans les domaines des moyens techniques, ce qui augmente le risque de la cybercriminalité, la rendant en tant qu'obstacle devant le développement de l'administration électronique et un des plus grands risques menaçant son existence

مقدمـــة

إن انفجار الثورة المعلوماتية بتوسع استخدام الشبكة العنكبوتية "الانترنت" في جميع مجالات الحياة اليومية من معاملات تجارية واجتماعية واقتصادية، أدى إلى تفاعل جميع فئات المجتمع وتهافتها السريع على وسائل الاتصال الحديثة، انبهارا بما توفره من سرعة في التعامل وتقريب للمسافات فضلا عن ما تتمتع به من سرية بالنسبة للمستخدمين وعدم الكشف عن هويتهم الحقيقية.

إلا أن هذا التطور الهائل في التعاملات الفردية رغم ما حققه من إيجابيات في التواصل عن بعد وإلغاء للمسافات، والتحول من التواصل المادي للأفراد إلى تواصل افتراضي في عالم افتراضي بحت يخلو من الماديات قد لا يرى فيه المستخدمين بعضهم البعض إطلاقا ان أرادوا ذلك، إلا أن وجهه السلبي كان أكبر بكثير من الإيجابيات التي حققها، حيث بدأت تظهر صورة جديدة من الجرائم متخذة من التواصل المعلوماتي وشبكة الانترنت وسيلة مثالية للإيقاع بالمستخدمين وارتكاب عدة صور وأشكال من الجرائم التي يصعب فيها الإثبات المادي وتحديد مسرح الجريمة الذي أصبح افتراضيا، واصطلح على تسميتها "بالجرائم المعلوماتية".

هذه الجرائم المستحدثة وصعوبة المتابعة فيها والكشف عنها جعلت الكثير من المستخدمين يعيدون النظر في فكرة التواصل المعلوماتي، وعلى رأسهم الإدارة التي أصبحت في حيرة من أمرها بين سعيها للاستفادة من التطور التكنولوجي وما يوفره من سرعة وتقريب الإدارة من المواطن والإرتقاء بالأعمال الإدارية وتحريرها من الأوراق والماديات المتعود عليها في إدارة المرافق العامة لإشباع حاجات الأفراد من خلال ما يعرف" بالإدارة الالكترونية"، وبين تخوفها من المخاطر والتهديدات الجسيمة للجرائم المعلوماتية والخبرات والتقنيات التي يتمتع بها المجرم المعلوماتي في عمليات القرصنة، لذلك ارتأيت تخصيص هذه الدراسة لمحاولة الإيجابة على الإشكال الآتي:

كيف يمكن مواجهة الجريمة المعلوماتية من طرف الإدارة حتى لا تكون عقبة من العقبات المهددة لتطور الإدارة الالكترونية؟

قبل الخوض في دراسة العلاقة بين الجريمة المعلوماتية والإدارة الالكترونية، كان لزاما الوقوف على تحديد مفهوم المصطلحين بصفة موجزة، وذلك لنتمكن من تحديد نطاق ومجال الدراسة، خصوصا أمام تعدد التعاريف الفقهية المقدمة لهم وعدم وضوح المعايير المعتمدة في ذلك نتيجة الاهتمام الدولي والداخلي بهذه المصطلحات التي تعتبر من إفرازات التطور التكنولوجي الذي يجتاح العالم المعاصر.

المطلب الأول: مفهوم الجريمة المعلوماتية

قبل تعريف الجريمة المعلوماتية لا بد من الإشارة إلى تعدد تسميات هذه الجريمة فهناك من يطلق عليها الجريمة الالكترونية أو الجريمة السيبرانية، لكن أفضل تسميتها بالجرائم المعلوماتية في موضوع دراستنا لنحصر المجال أكثر، فالجريمة في موضوعنا تنصب على المعلومات التي تستخدمها الإدارة في أعمالها الإدارية في سبيل تجسيد فكرة الإدارة الالكترونية.

فهناك من يعرف الجريمة المعلوماتية بأنها:" نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أوهدف لتنفيذ الفعل الإجرامي المقصود."

كما عرفت أيضا بأنها:" كل جريمة تقع في محيط أجهزة الكميوتر" ، وعرفت بأنها:" الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا".

فهذه التعريفات تعتمد على المعيار التقني في تعريفها للجريمة المعلوماتية حيث يركز على الوسيلة المستخدمة في ارتكابها وهي جهاز الحاسوب بما ينطوي عليه من مكونات مادية كالشاشة والمفتاح والأجهزة التي تتصل به من طابعات وأجهزة الماسح الضوئي، ومكونات معنوية من معلومات وبيانات واتصالات عبر شبكة الانترنت.

هناك أيضا من عرفها بأنها:" كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل".

هذا التعريف يعتبر تعريف قانونيا يركز على أركان الجريمة كالركن المعنوي والمادي فضلا عن النتيجة والمتمثلة في الخسارة التي تلحق المجني عليه.

فمن خلال التعريفات السابقة لا يمكن وضع تعريف مانع جامع للجريمة المعلوماتية بالتركيز على المعيار التقني فقط لأنه توجد جرائم تستخدم جهاز الحاسوب ولا تعتبر معلوماتية كجريمة تزوير النقود، كما لا يمكن الاعتماد على الأركان المتعود عليها في القواعد العامة وإهمال خصائص وميزات الجريمة المعلوماتية التي تعتبر جريمة عابرة للحدود، فضلا عن الفاعل القائم بهذه الجريمة وهو ما اصطلح على تسميته بالمجرم المعلوماتي الذي يتمتع بقدرات تقنية هائلة وذكاء يمكننه من طمس معالم الجريمة بسهولة في العالم الافتراضي.

لذلك يمكن تعريفها بأنها:" نوع جديد من النشاط الإجرامي المتعمد الذي يقوم باستغلال جهاز الحاسوب وشبكات الاتصال من خلال الاعتداء على الأشخاص أو الأموال أو البيانات المعالجة آليا".

المطلب الثاني: مفهوم الإدارة الالكترونية

إن رغبة الإدارة في استغلال التكنولوجيا الحديثة في إدارة المرافق العامة وإشباع حاجات الأفراد أدى إلى ظهور تقنية المعلومة الإدارية واستخدامها في التوجه من الإدارة التقليدية التي تقوم على الماديات والأوراق الإدارية إلى تجسيد مصطلح تقني حديث هو الإدارة الالكترونية، الذي يقوم

على أساس تسهيل العمل الإداري وتقريبه أكثر من المواطن.

فمصطلح الإدارة الالكترونية كغيره من المفاهيم الحديثة استقطب اهتمام الدارسين لمحاولة تعريف هو بيان معالمه الأساسية، فهناك من عرفه بأنه:" استخدام الوسائل والتقنيات الالكترونية بكل ما تقتضيه الممارسة، أو التنظيم أو الإجراءات أو التجارة أو الإعلان." ، فهذا التعريف يرتكز على الوسيلة وهو تعريف واسع لا يخص المجال الإداري بل يشمل عدة مجالات أخرى كالتجارة مثلا.

عرفت أيضا بأنها:" استخدام وسائل الاتصال التكنولوجية المتنوعة والمعلومات في تسيير سبل آداء الإدارات الحكومية لخدماتها العامة الالكترونية، والتواصل مع من يطلب الانتفاع من خدمات المرفق العام من خلال تمكينهم من استخدام وسائل الاتصال الالكترونية عبر بوابة واحدة".

هذا التعريف تعريف ضيق أكثر من التعريف الأول وبالتالي فهو يعبر عن مضمون الإدارة الالكترونية ويركز على معيار المرفق العام والمصلحة العامة، هذا ما يجعله مرجح لتعريفها، فمن خلال ما تقدم يمكن القول أن الإدارة الالكترونية هي استفادة الإدارة من وسائل الاتصال التكنولوجية في إدارة المرفق العام وإشباع حاجات الأفراد بالتخلي عن الماديات والأوراق والأوقات وتقريب الإدارة من المواطن".

يتضح من خلال التعريفات السابقة أن الإدارة الالكترونية تقوم على جملة من الخصائص هي:

-إدارة بدون أوراق بل تعتمد على الوسائط والدعامات الالكترونية.

-تعتمد على المؤتمرات الالكترونية عبر شبكة الانترنت .

-تعتمد على المؤسسات الشبكية والمؤسسات الذكية في العالم الافتراضي.

-إدارة متواصلة حيث تعمل لمدة 24 ساعة.

فالإدارة الالكترونية تحاول قدر الإمكان تجنب عقبات الإدارة التقليدية والمتمثلة في كثرة الأوراق والتنقلات المستمرة من طرف المواطنين للحصول على الخدمات وغيرها، فهي إدارة تقوم على تقنية المعلومات لكنها اصطدمت في ذات الوقت بالانتشار السريع والمدهش للجرائم المعلوماتية.

المبحث الثاني:الجرائم المعلوماتية الماسة بالإدارة الالكترونية

إن فكرة الإدارة الالكترونية ترتكز بالأساس على المعلومات التي يتم تدوالها بين الأفراد والإدارة الكترونيا من خلال جهاز الحاسوب واتصاله بشبكة الانترنت، من خلال إتاحة الفرصة للمواطن في الحصول على الوثائق التي يحتاجها في أي وقت ومن أي مكان، حيث تغير مفهوم الوثائق من الدعامة الورقية إلى الدعامة الاللكترونية، وبما أن الإدارة الالكترونية ترتبط بعدة مجالات حساسة داخل الدولة كالبنوك والبريد والتأمينات فقد كانت محل نظر من طرف أصحاب النوايا السيئة للحصول على أرباح وأموال غير مشروعة من خلال التلاعب و الاعتداء على المعلومات الخاصة

بها، مما أدى إلى ظهور عدة صور من الجرائم المعلوماتية في مجال التعامل الاداري الالكتروني، نذكر منها:

المطلب الأول: تزوير المعلومات الخاصة بالإدارة الالكترونية

بما أن الإدارة الالكترونية تقوم على فكرة تداول البيانات المعالجة آليا عبر شبكة الانترنت من جهاز إلى آخر، فالوصول إليها من طرف المحترفين والقراصنة بغرض الاختراق والتلاعب أمر في غاية السهولة، حيث يسهل استخراج المحررات الالكترونية على دعائم مادية كالأقراص المضغوطة وتحويلها إلى محررات ورقية من خلال استخدام الطابعات.

فهذه التقنيات تسهل تزوير المحررات وتحميلها بالبيانات المزورة وترجمتها على الدعامة الورقية لاستخدامها في أغراض غير مشروعة، فجريمة التزوير المعلوماتي هنا تتوفر على نفس أركان جريمة التزوير التقليدية المنظمة في قانون العقوبات، لكنها تتميز من حيث الوسيلة التي تتم بها وهي جهاز الحاسوب وشبكة الانترنت، وأمام التطور التكنولوجي أصبحت الحاجة ملحة لضرورة وضع نصوص قانونية تتميز والجريمة المعلوماتية خصوصا فيما يتعلق بالدليل الالكتروني الغير ملموس ومسرح الجريمة الذي يصعب الوصول إليه في أغلب الأحيان كونه يتم في عالم افتراضي بحت.

فمن المشرعين من قام بتعديل قواعده وتطويعها أو إضافة نصوص خاصة على نحو يستوعب جريمة التزوير سواء المعلوماتية والتقليدية كالمشرع الجزائري في قانون العقوبات في المواد 394 مكرر وما بعدها، وأيضا المشرع الفرنسي الذي نص على التزوير في قانون المعلوماتي في قانون العقوبات لسنة 1994 :"" يعاقب على التزوير الذي يتم عن طريق الوسائط الالكترونية، وسواء تم في محرر رسمي أو محرر عرفي".

حيث يتضح أن المشرع الفرنسي يؤخذ بقيام بأركان قيام جريمة التزوير التقليدية ويضيف شرط الوسيلة المستخدمة والتي تتم من خلال الوسائط الالكترونية، كما أنه يساوي بين المحررات من حيث قوته، فالعبرة بتوافر السلوك الإجرامي وتحقق النتيجة واتجاه الإرادة إلى إحداثها.

ومن التشريعات من خصت الجرائم المعلوماتية بقوانين خاصة كالمشرع التونسي والإمارتي، حيث عاقبا على جريمة التزوير المعلوماتي ضمن قوانين التجارة الالكترونية .

المطلب الثاني:الجرائم المعلوماتية الواقعة على أموال التجارة الالكترونية

إن الاعتداءات الالكترونية على الأموال المتداولة في التجارة الالكترونية تعتبر من المخاطر المهددة للإدارة الالكترونية، من خلال انتشار سرقة المعلومات بالتلاعب في البطاقات الممغنطة واستعمالها استعمالات غير مشروعة، فضلا عن التلاعب في الحسابات البنكية والقيام بتحويلات وهمية.

فهذه الاختراقات من شأنها المساس بالثقة والائتمان اللذان يعتبران أساس التجارة الالكترونية، مما يؤدي إلى تشكل مخاوف لدى الأفراد من اللجوء للتعامل الالكتروني سواء التجاري أو الإداري، لتكون بذلك هذه الجرائم المعلوماتية عقبة تقف أمام تطور كل من التجارة والإدارة الالكترونيين.

المطلب الثالث: جريمة الإتلاف المعلوماتي

تعتبر جريمة الإتلاف المعلوماتي من الجرائم المعلوماتية الخطيرة كونها تنصب على المعلومات المتداولة الكترونيا عبر شبكات التواصل بغرض إتلافها ومحو آثارها لتحقيق أغراض خاصة، من طرف أشخاص أذكياء قادرين على التعامل التقني مع جهاز الحاسوب والتلاعب بكل معطياتها وبرامجه، هذا ما يجعل لها انعكاسات خطيرة على الإدارة الالكترونية نظرا لطبيعة المعلومات التي تحتويها ومساسها بالمصالح الشخصية للأفراد.

والسلوك الإجرامي لجريمة الإتلاف يتكون من عنصرين الأول مادي عندما ينصب على إتلاف الجهاز وما يحتويه من دعامات الكترونية تتضمن معلومات متعلقة بالأعمال الإدارية، والثاني معنوي يستهدف البرامج والشبكات الرابطة بين مختلف مواقع الإدارة الالكترونية من خلال زرع فيروسات مدمرة للمعلومات.

من مميزات هذه الجريمة أن الدافع وراء ارتكابها قد لا يكون دائما إجرامي، بل قد يرتكبها المجرم المعلوماتي بهدف التباهي بقدراته الذهنية في التحكم بجهاز الحاسوب عن بعد من خلال التلاعب بالمعلومات عبر شبكة الانترنت والوصول إلى مختلف برامج الإدارة الالكترونية بزرع الفيروسات والاطلاع على المعلومات التي يفترض فيها السرية.

حيث يمكن مواجهة جريمة الإتلاف ومحاولة الحد منها قدر الإمكان من خلال ما يعرف بالأمن المعلوماتي الذي يعتبر وسيلة من وسائل الحماية الفنية من الجرائم المعلوماتية، حيث ينصب على حماية أصول وموارد النظام المعلوماتي بطرق مشروعة، بوضع برامج ضد الفيروسات وأخذ الحيطة قدر الإمكان.

المطلب الرابع: الجرائم الماسة بالمعلومات الخاصة بالإدارة الالكترونية

إن المعلومات الخاصة بالإدارة الالكترونية مثلها مثل كل المعلومات المعالجة والمتداولة آليا تتعرض للجرائم المعلوماتية بمختلف صورها كالدخول الغير المشروع والغير المصرح به لمواقع الحكومة الالكترونية وانتهاك سرية البيانات وتزوير التوقيع الالكتروني وغيرها من أشكال الجرائم في العالم الافتراضي.

فكل فعل يشكل صورة من الصور السابقة يعتبر جريمة معلوماتية ماسة بالإدارة الالكترونية ومهددة لها في تحقيق الأغراض التي وجدت من أجلها، وحتى تتحقق الجرائم السابقة لابد أن تكون المواقع محل الإعتداء والخاصة بالإدارة سرية غير متاحة للجمهور ، لأن السرية هنا هي

شرط لارتكاب الجريمة ولتحقق السلوك الإجرامي المتعلق بالجريمة سواء اقتصر على الدخول غير مشروع أو غير المصرح به أو امتد إلى المحو أو التغيير.

فالجريمة المعلوماتية الماسة بمعلومات الإدارة الالكترونية قد تقتصر على مجرد الاطلاع عليها أو تمتد لأكثر من ذلك لتصل للتعييب والإفساد باستخدام عدة وسائل معلوماتية كالقنبلة أو برنامج حصان طراودة.

قد يتبادر لذهن المطلع على هذا الموضوع أن الجريمة المعلوماتية يتم أرتكابها فقط من طرف أشخاص بعيدين كل البعد عن الإدارة الالكترونية، لكن الحقيقة خلاف ذلك فقد تتم من طرف القائمين على المحاسبة أو الإشراف على المعلومات نتيجة تمتعه بموضع يخوله القيام بها أكثر من غيرها.

المبحث الثالث: وسائل الإدارة الالكترونية في مكافحة الجريمة المعلوماتية

مما لا جدال فيه أن الجرائم المعلوماتية السابق بيانها تؤثر على تطبيق نظام الإدارة الالكترونية، وتقف حجرة عقبة أمام تطورها وازدهارها، نتيجة تخوف الإدارة والأفراد المتعاملين معها من الوقوع ضحية اعتداء من الاعتداءات السابقة وصعوبة إثباته في العالم الافتراضي، خصوصا وأن محل الجريمة هنا ينصب على المعلومات الخاصة والتي لا يتاح كشفها للعامة، سواء كانت خاصة بالإدارة وعملها أو بالحياة الخاصة للأفراد، لذلك كان لزاما محاولة الحد من مخاطر المعلوماتية بإقرار وسائل تحقق ذلك للإدارة نوردها فيما يلي:

المطلب الأول: تقرير المسؤولية في الإدارة الالكترونية

بما أن الإدارة هي صاحبة الاختيار في التوجه نحو تبني الإدارة الالكترونية وتطوير خدماتها اليومية في شتى مجالات الحياة الإدارية والخدمات المتعلقة بالتليفون والكهرباء والغاز، فإنها منطقيا تتحمل المسؤولية عن منتجات هذه التصرفات من وثائق ومحررات سواء كانت على الدعامة الالكترونية أو الورقية.

لكن المسألة من الناحية القانونية يشوبها الغموض نتيجة عدم وجود نصوص قانونية خاصة بتنظيم مجالات التعامل الالكتروني، وإن كانت موجودة فهي عامة تنظم الجرائم المعلوماتية والتجارة الالكترونية، أما مسألة الإدارة الالكترونية فهي مازالت تحتاج للتنظيم القانوني الدقيق لسد الثغرات أمام أصحاب النوايا السيئة .

لذلك فقد اهتم الفقه القانوني بدراسة المسؤولية عن الأعمال الإدارية الالكترونية بشقيها الجزائي عندما يشكل السلوك المرتكب جريمة، والمدني عندما يشكل خطأ مدنيا، فأخطاء الإدارة الالكترونية قد تثير المسؤولية بأنواعها المختلفة.

لقد توصلت الدراسات الفقهية القانونية للمسؤولية الإدارية في نظام الإدارة الالكترونية إلى عدم امكانية حصر الأخطاء التي قد ترتكب في المجال المعلوماتي خصوصا وأنها لا تتصل فقد

بالجوانب المادية بل ترتبط بعدة جوانب افتراضية لا يمكن حصرها أمام التطور المستمر للأجهزة والشبكات وحتى البرامج، فإذا نظمت وسيلة من وسائل العمل الإداري قد تظهر وسائل أخرى عدة في وقت قصير لا يمكن حتى توقعه.

ومن النتائج المتوصل إليها أنه يتعين على الإدارة الالكترونية الالتزام بحسن استخدام المعلومات الخاصة بالعملاء والحفاظ على سريتها لما لها من قيم اقتصادية وإدارية، اصطلح على تسميتها ب"القيم المادة المستحدثة".

ففي مجال الإدارة الالكترونية يجب إعمال المسؤولية أيا كان وصفها مدنية أو جنائية دون اشتراط تحقق كل فروضها، فبمجرد ارتكاب الخطأ تتحقق المسؤولية وهذا بهدف الحد قدر الإمكان بالجريمة المعلوماتية والإلمام بكل صورها التي ظهرت والتي قد تظهر، فمثلا في جريمة اختراق حساب عميل من العملاء وتحويل الأموال إلى حساب آخر داخل الدولة أو خارجها فهذا وحده كافي لترتيب المسؤولية الجنائية للفاعل، فضلا عن المسؤولية المدنية لموظف البنك عن عدم اتخاذ وسائل الحماية الفنية اللازمة.

كما قد تقوم المسؤولية الإدارية للجهة القائمة بالإدارة الالكترونية في حال الخطأ في البيانات والمعلومات الخاصة بالحالة المدنية للأفراد كشهادات الميلاد مثلا، ودون أن ننسى المسؤولية الإدارية للموظف الذي يخطأ نتيجة الإهمال في القيام بوظيفته أو يستغلها استغلالا لمصلحته الخاصة، على أساس أن جهاز الحاسوب وشبكة الانترنت تبقى مجرد وسائل وهو المسير لها والقائم عليها.

يتضح من خلال ما تقدم أن المسؤولية في نظام الإدارة الالكترونية لا بد أن تتخذ مفهوم موسع مقارنة بالمسؤولية التقليدية وذلك لمحاولة تجاوز عقبة الجريمة المعلوماتية التي تبعث على عدم الثقة في هذا النظام الجديد، فإقرارها يعتبر وسيلة من وسائل تطور هذا النظام كونه يحد ولو بنسبة بسيطة من استفحال هذه الجرائم، ولابد من التأكيد على البلورة التشريعية لهذه المسؤولية ليكون إعماله تحت غطاء مبدأ المشروعية.

المطلب الثاني: اللجوء للأمن المعلوماتي

يتعين على جهات الإدارة عند التحول للنظام الالكتروني في تسيير المرافق العامة أن تتخذ الحيطة اللازمة لحماية بياناتها من التعرض للجرائم المعلوماتية بأنواعها، وذلك بتطبيق الوسائل الفنية الكفيلة بذلك في إطار ما اصطلح على تسميته بالأمن المعلوماتي.

ووسائل الأمن المعلوماتي متعددة نذكر منها:

أولا: الجدار الناري:

الجدار الناري عبارة مجموعة من الأنظمة والبرامج تهدف لتشكيل سياجات أمنية بين شبكة الانترنت والإدارة الالكترونية، وهذا ما يمنع الاختراقات والاعتداءات.

ثانيا:مكافحة الفيروسات المعلوماتية:

إن الفيروسات تعتبر من أخطر المهددات للمعلومات الخاصة بالإدارة الالكترونية حيث يمكن لها إتلافها عن بعد والتلاعب بها متى كان جهاز الحاسوب متصل بالشبكة العنكبوتية، ولتجنب الفيروسات لا بد من وضع برامج ضد الفيروسات لمنعها من الانتشار وتدمير المعلومات.

الخـــاتمـــة

من خلال ما تقدم تتضح العلاقة بين نظام الإدارة الالكترونية والجريمة المعلوماتية التي تعتبر عقبة من عقبات تطور الإدارة واستفادتها من معالم التطور التكنولوجي ووسائل الاتصال اللذين اجتاحا العالم المعاصر وتسخيرها لخدمة الأفراد وإشباع حاجاتهم بالتخلص من ماديات التعامل الإداري وما يفرزه من كثرة للأوراق وضياع للوقت وتعقيدات تنظيمية كثيرة.

فيجب اتخاذ الإدارة كل الوسائل اللازمة لحماية بياناتها من الجرائم المعلوماتية والقضاء على مخاطرها قدر الإمكان، وذلك للاستفادة من إيجابيات العمل الإداري الالكتروني المتمثلة في الارتقاء بالإدارة وتحقيق السرعة في الإنجاز دون اعتراف بالأماكن والأوقات.

ولتنجح الإدارة في التوجه للعالم الافتراضي لا بد من محاولة وضع نصوص قانونية خاصة بالإدارة الالكترونية تنظم فيه كل المسائل الفنية والتقنية تنظيما قانونيا قادرا على التغلب على مخاطر الجريمة المعلوماتية وسد الثغرات أمام المجرم المعلوماتي، من خلال تحديد الجرائم الماسة بها والعقوبات المقررة لها فضلا عن إقرار قواعد المسؤولية بكل صورها سواء كانت مدنية أو جزائية أو إدارية، وتفعيل وسائل الحماية الفنية في الأنظمة المعلوماتية بهدف بعث الثقة في هذا النظام الجديد وتشجيعه قدر الإمكان.

الهوامش:

[1]محمد الأمين البشيري، **التحقيق في جرائم الحاسب الآلي**، بحث مقدم إلى مؤتمر القانون والكومبيوتر والانترنت، كلية الشريعة و القانون، جامعة الإمارات، 2000، ص6.

[2] علي عبد القادر القهواجي، **الحماية الجنائية لبرامج الحاسب**، دار الجامعة الجديدة للنشر، الاسكندرية، 1997ص2.

[3] هشام فريد رستم، **الجرائم المعلوماتية-أصول التحقيق الجنائي و اقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي**، بحث مقدم لمؤتمر القانون و الكمبيوتر والانترنت لجامعة الإمارات،2000، ص8.

[4]تعريف قدمه BRKER مأخوذ من محمد سامي الشوا**ثورة المعلومات وانعكاساتها على قانون العقوبات**، دار النهضة العربية، القاهرة، ط1، 1994، ص6.

[5]محمد محمود الطعامنة-شريف العلوش، **الحكومة الالكترونية و تطبيقاتها في الوطن العربي**، الأردن، المنظمة العربية للتنمية الإدارية،2004، ص10.

[6]هيثم الفيلكاوي، **الحكومة الالكترونية**، مجلة الحرس الوطني الكويتي، العدد 19، 2002ص50.

[7] عبد الفتاح بيومي حجازي، **علم الجريمة و المجرم المعلوماتي**، منشأة المعارف، الاسكندرية، 2009، ص316.

[8] عبد الفتاح بيومي حجازي، **مكافحة جرائم لكمبيوتر والانترنت في القانون العربي النموذجي**، دار الفكر الجامعي، الاسكندرية، ط1، 2004، ص350.

[9]عبد الفتاح بيومي حجازي، **التجارة عبر الانترنت**، دار الفكر الجامعي، الاسكندرية، ط1، 2007، ص15.

[10] عبد الفتاح بيومي حجازي، **علم الجريمة و المجرم المعلوماتي، مرجع سابق**، ص317.

[11]**المرجع السابق**، ص 318.

[12]عبد الفتاح بيومي حجازي، **التجارة الالكترونية، المجلد الثاني**، دار النهضة العربية، القاهرة، 2009، ص 27.

[13]محمد سعيد خشبة، **نظم المعلومات – المفاهيم و التكنولوجيا**، (د.د.ن)،1990، ص101.

[14]محمد سامي الشوا، **قانون لعقوبات و انعكاساته على ثورة المعلومات**، دار النهضة العربية، القاهرة، 2000، ص71.

[15]علي عبد القادر القهواجي، **مرجع سابق**، ص10.

[16]عبد الفتاح بيومي حجازي، **علم الجريمة و المجرم المعلوماتي، مرجع سابق**، ص335.

[17]محمد محمد عبد اللطيف، **التطورات الحديثة في مسؤولية الإدارة**، مكتبة الجلاء الجديدة، 2000، ص9.

[18]عبد الفتاح بيومي حجازي، **مرجع سابق**، ص329.