الأمن المعلوماتي للحكومة الإلكترونية

أ. عبد الوهاب ملياني

جامعة الأغواط

ملخص:

أصبحت حتمية على الدولة في ظل الظروف الراهنة أن تتطور خاصة و أنها تستعمل المعلومات ذات الطابع الإلكتروني ، وهو ما أدى إلى تسمية أعمال الدولة في هذا الإطار بمصطلح قانوني جديد يعرف بالحكومة الإلكترونية نظرا لكون أعمالها أصبحت تظهر بصفة متجددة ودائمة عن طريق تقنية وسائل الاتصال الحديثة التي يميزها الانترنت . ولهذا أضحي من الضروري معرفة مفهوم الحكومة الإلكترونية ومدى تامين المعلومات الصادرة عن الدولة في هذا الإطار ، وهذا ما أدى بنا إلى بحث امن المعلومات للحكومة الإلكترونية .

Résumé :

dans les circonstances actuelles l'état doit être développer avec la nature électronique de l'information , dans ce cadre un nouveau terme juridique connu par le gouvernement électronique ,en raison du fait son travail est devenu un spectacle renouvelé et durable à travers les moyens modernes de technologie de la l'information et de la communication qui distingue l' Internet . Mais se la est devenu nécessaire de connaître le concept de gouvernement électronique et comment l'information délivré par l'État dans ce context et sécurisé , et nous conduit à examiner la sécurité de l'information de gouvernement électronique .

مقدمة :

لم يعد أمام أي دولة ان تواكب العصر ولا تتخلف عن الركب خيارا سوى الاتجاه نحو المجتمع الإلكتروني والتكنولوجيا الرقمية فقد جعلت وسائل الإتصال الحديثة العالم يشبه المدينة الواحدة في تقارب أجزائه.

ولقد أدت التقنيات الحديثة للمعلومات والاتصالات إلى إحداث تطورات هائلة في الحياة العامة سواء على مستوى الأفراد الذين يرغبون في الحصول على خدماتهم بصورة أكثر تطورا وسرعة ودقة عالية، أو على مستوى الهيئات والمؤسسات القائمة على تقديم تلك الخدمات.

الأمن المعلوماتي للحكومة الإلكترونية

ولقد أصبح إدخال تكنولوجيا المعلومات في كافة الأعمال الحكومية هو هدف العديد من الدول التي تسعى للتقدم والرقي والتي منها الجزائر بحيث سعت إلى إستخدام تكنولوجيا المعلومات في الأجهزة الحكومية .

أدى إرتباط إستخدام تكنولوجيا المعلومات في الأجهزة الحكومية لظهور مصطلح جديد أطلق عليه الحكومة الإلكترونية الذي من خلاله تسعى الإدارة إلى تبسيط وتسهيل التعاون بينها وبين الأفراد وتوفير المعلومات بشكل متكامل وسريع للجميع لتحسين أداء الإدارة وتسهيل حصول المواطن على الخدمة بأقل تكلفة وفي هذا الشأن يمكننا طرح التساؤل التالي:

كيف يمكن التعامل مع ما يعرف بالحكومة الإلكترونية؟ وكيف يمكن حمايتها؟

ونسعى من خلال هذا البحث إلى الإجابة عن التساؤل السابق من خلال إلقاء الضوء على نظام الحكومة الإلكترونية من خلال المبحث الأول ومن ثم نتطرق إلى الوقاية من الجرائم المتصلة بالحكومة الإلكترونية في المبحث الثاني وفق ما يلي:

المبحث الأول: مفهوم الحكومة الإلكترونية

في وقتنا هذا طرح في ميدان الفكر مصطلح الحكومة الإلكترونية¹ الذي يشد الإنتباه باعتباره مصطلح حديث مرتبط بالمعلوماتية وتقنياتها المرتبطة بتكنولوجيا المعلومات.

فمع تطور تكنولوجيا المعلوماتية سارعت الحكومات الرشيدة إلى بحث تنفيذ نظام يغير من أسلوب تقديم وكيفية الحصول على الخدمات التي تقدمها الإدارات الحكومية والمجالس البلدية والإقليمية وأجهزة الحكم عموما بصورة أمثل تحتصر الوقت والجهد والمال أيضا مع تحسين الأداء والكفاءة و الفعالية.

هذا ما يستلزم التطرق إلى دراسة مفهوم الحكومة الإلكترونية من خلال العناصر التالية:

المطلب الأول: مدلول الحكومة الإلكترونية:

¹لفظ الحكومة الإلكترونية متعلق بالصفات و المعاني التي توصف بها من حيث كونها سلطة عامة وركن في الدولة او الوزارة أو الهيئة التي تقوم بتنفيذ القوانين وإدارة المرافق العامة وغير ذلك.

الأمن المعلوماتي للحكومة الإلكترونية

من خلال البحوث التي تطرقت لدراسة الحكومة الإلكترونية نجد ثلاث اتجاهات متصلة بالتعريف على أساس الإتصال الإلكتروني تفتح الباب واسعا أمام استخدامات متعددة للمصطلح وسنوضح تلك الإتجاهات وفق:

الفرع الأول: مدلولها العام:

بحيث يرى أنصار هذا الإتجاه أن الحكومة الإلكترونية تعني إستخدام وسائل الإتصال التكنولوجية المتنوعة والمعلومات في تسيير سبل أداء الإدارات الحكومية خدماتها العامة الإلكترونية ذات القيمة، والتواصل مع طالبي إستخدام وسائل الإتصال الإلكترونية عبر بوابة واحدة وكذلك إستخدام المعلومات بطرق تعتمد على الآلية الإلكترونية.

وبعبارة أخرى فإن الحكومة الإلكترونية تشير إلى استخدام المعلومات ووسائل اتصال التكنولوجي كالشبكات المتكاملة بعيدة المدى، والانترنت والكمبيوتر من قبل الإدارات الحكومية.

وهذا يعني أن الحكومة الإلكترونية تتبنى التغيير أو التعديل في العلاقات الأساسية بين الحكومة من ناحية، ولجمهور المواطنين ورجال الأعمال من ناحية أخرى من خلال طريقتين:

أ- تقديم الخدمات بطريقة مختلفة عن طرق التقليدية بواسطة نتكامل المعلومات وتميز الأفراد من الوصول إليها عن طريق الأنترنت.

ب- التحول في طبيعة ممارسة السلطة عن طريق العمل على تحسين العلاقات وإقامة جسور الثقة بين الدولة ومواطنيها التي تعمل على الإستفادة من إمكانيات تكنولوجيا الإتصال لتطوير الأداء الإداري والحكومي، وتحسين علاقة القائمين على المرفق العام بجمهور المتعاملين معه، وتحقيق الديمقراطية الإدارية بإتاحة الفرصة للجمهور لإبداء رأيه في مستوى أداء المرفق لخدماته وأخذه في حسابان القائمين على إدارة المرفق.¹

الفرع الثاني: مدلولها بمعنيين:

أنصار هذا الإتجاه أن الحكومة الإلكترونية في مدلولها بمعنيين أحدهما ضيق والأخر أوسع:

¹ ماجد الحلو، الحكومة الإلكترونية والمرافق العامة، بحث مقدم إلى المؤتمر العلمي الأول الذي نظمته أكاديمية شرطة دبي حول " الجوانب القانونية والأمنية لعمليات الإلكترونية من 26-28 أبريل 2003. ص 6-10.

أولاً: المعنى الواسع للحكومة الإلكترونية:

وفقاً له فإن الحكومة الإلكترونية تعني الاستخدام الأوسع للتكنولوجيا الحديثة فعادة تنظيم الأدرج الحكومية وتطوير البنية التحتية المحلية لازمة لذلك، بشكل يؤدي إلى إستفادة الحكومة من الإنترنت والمعلومات واتصالات التكنولوجيا لإنجاز معاملات الأفراد بسهولة وسرعة، وتبعاً لهذا المعنى الحكومة الإلكترونية ليست مقصورة على بتوفير الخدمات للمواطنين عن طريق الأنترنت فحسب بل تشمل المحاولة الدائمة للحصول على أجود الخدمات الحكومية في العلاقات الداخلية والخارجية من خلال الطرق الإلكترونية دون إعتبار للمكان والزمان أو تمييز أو إخلال تكافؤ الفرص.

ثانياً: المعنى الضيق للحكومة الإلكترونية:

الذي يعني مجموعة الأنشطة الحكومية التي تعتمد على الأنترنت والإنصالات الإلكترونية عبر مجموع طبقات ومستويات الحكومة لتقديم الخدمات والمعاملات للأفراد والحصول على المعلومات في شتى المجالات بيسر وسهولة. ويمكن أن يطلق على الأنشطة الإجرايات الإدارية الإلكترونية وهي بحسب التعريف الفرنسي لها التبادل غير المادي للبيانات بين المرافق العامة والجمهور هذا التبادل يتطلب عدم الإقتصار على وضع نماذج الإجراءات الإدارية على شبكة الأنترنت وإنما يجب أن يسمح بإمكانية القيام بجميع المراحل اللازمة لإنهاء الإجراء الإداري من خلال إستخدام نظم معلومات تؤدي إلى إنشاء مواقع تفاعلية تتيح للمستخدم وتلقي جواب على طلبه¹.

الفرع الثالث: المدلول الجامع بين الحكومة الإلكترونية والإدارة على إطلاقها:

ذهب أنصار هذا الإتجاه إلى أن مفهوم الحكومة الإلكترونية يجب أن يراعى فيها:

أولاً: تحول أعمال القطاع العام إلى الإدارة الإلكترونية خصوصاً وأن التجارة الإلكترونية كانت الأصل الذي تفرعت منه الحكومة الإلكترونية.

¹ محمد حسين النيلى، العلاقة بين القانون والحكومة الإلكترونية، ورقة عمل قدمت لمؤتمر الكويت حول الحكومة الألكترونية في الفترة 13-15 أكتوبر 2003. ص 25-30.

الأمن المعلوماتي للحكومة الإلكترونية

ثانياً: أن يستوعب الخدمات التقليدية للحكومة بصرف النظر عن السلطة التي تقدمها سواء كانت السلطة التشريعية أو التنفيذية أو القضائية.

وفي هذا الإتجاه تعرف الحكومة الإلكترونية بأنها قدرة القطاعات الحكومية على تبادل المعلومات وتقديم الخدمات فيما بينها وبين المواطنين وبين القطاعات الأعمال بسرعة ودقة عالية، وبأقل تكلفة عبر شبكة الأنترنت أو وسائل الإتصال الأخرى مع ضمان سرية وأمن المعلومات المتناقلة في أي وقت أو أي مكان.

وفي هذا الإتجاه نلمس أن المعنى فضفاض للإدارة لإعتبارها جهداً جماعياً مشتركاً في منظمة عامة أو خاصة بقصد تحقيق أهداف محددة سواء هدفت المنظمات إلى تحقيق الربح أو لم تكن تهدف إلى ذلك.

أخيراً يمكن القول أن الحكومة الإلكترونية هي أداة لتطبيق نظام المعلوماتية المرتبطة بتكنولوجيا الحديثة في أعمال الحكومة لتحقيق أهدافها في تلبية احتياجات الأفراد وجعل الدولة أكثر تفاعلاً مواطنياً دون أن يجعلهم يتكبدون مشقة الذهاب بأنفسهم للإدارات الحكومية.¹

المطلب الثاني: أثر الحكومة الإلكترونية على النظام القانوني للمرفق العام وإدارته:

يعتبر المرفق العام مظهراً من مظاهر تدخل الدولة لأداء الخدمات العامة الأساسية للجمهور لهذا أصبحت نظريته ركناً أساسياً لإرساء قواعد القانون الإداري، على أساس أن إستهداف النفع العام هو غاية الغايات من المرافق العامة التي تنشأ لسد الحاجات العامة للجمهور التي تنقضي الصالح العام بضرورة توفيرها بصفة مستمرة ومنتظمة.

ومن هنات يثار التساؤل في أثر نظام الحكومة الإلكترونية على المرفق العام والنظام القانوني الذي يحكمه من خلال المبادئ التي يتضمنها سيره وكيفية إدارته؟

وهذا ما سنوضحه من خلال عرضنا للنقاط المتضمنة بالفروع التالية:

الفرع الأول: اثر الحكومة الإلكترونية على مبدأ سيرة المرفق العام بإطراء وانتظام:

¹ داود عبد الرزاق، الإدارة العامة للحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام وأعمال موظفيه، مجلس النشر العلمي، جامعة الكويت، 2004 . ص 86-91.

الأمن المعلوماتي للحكومة الإلكترونية

من المبادئ التي تحكم وتضبط المرفق العام دوام سيرة بصفة منتظمة ومطرودة تحقيقا للصالح العام الذي يرمي إلى توفير الحاجات الأساسية التي ينشأ المرفق العام لسدها بطريقة مستمرة ومنظمة إلا في العطل الرسمية وحالة القوة القاهرة، هذا ما يؤدي إلى أن الناس يرتبون أمور حياتهم المعيشية على أساس استمرار المرافق العامة ويظهر ذلك بوضوح في الخدمات الجوهرية المقدمة من مرافق الكهرباء والغاز أو مرفق توريد المياه أو مرفق النقل أو مرفق الطرق والاتصالات... إلخ.

فإذا ما فوجئ الناس بتوقف أو تعطيل في المرافق العامة أو إضراب موظفيها أدى ذلك إلى إضراب أحوال المجتمع ويلحق بأفراده المشقة والضرب مما يعرض النظام العام للخطر.¹ ويتجلى اثر تطبيق الحكومة الإلكترونية على سير المرافق العام بدوام مطرد ومنتظم من خلال الآتي تفصيله:

أولاً: التطبيق المحكم للمبدأ:

من شأن الإدارة العامة الإلكترونية أن تجعل مبدأ ودوام سير المرفق العام يتجه في تطبيقه إلى الإحكام حيث لا تحديد لمواعيد فتح مكاتب الموظفين أو إغلاقهم وإنما يعمل المرفق على مدار الساعة ولا يتوقف إلا إذا حدث عطل في التقنية اللازمة للإستفادة من خدماته سيقبل من خطورة إضراب الموظفين كما سيعمل على التقليل من التعرض لوجود الموظف الفعلي في الظروف العادية الذي يتولى الوظيفة دون إستيفاء شروطها القانونية حيث يمكن كشف أمره من خلال قواعد البيانات والمعلومات التي تزود بها الإدارات الحكومية.

كما سيؤدي هذا النظام إلى تعامل المنتفعين مع المرفق وهم مطمئنون لعدم سماعهم لمقولة " خلاص مواعيد العمل انتهت أو أن الموظف لم يحضر اليوم أو أنه في إجازة أو أرجع غدا" فالفرد يمكنه الدخول إلى شبكة المعلومات ولو في منتصف الليل لم عرفة الإجراءات والمعلومات الخاصة بإنجاز معاملته أو قضاء مصلحة لدى المرفق العام.

هذا النظام سيؤدي إلى التطبيق المحكم لمبدأ دوام سير المرفق العام بشكل شبكة تامة من خلال توفير البوابات الإلكترونية التي تقدم للخدمات على شبكة الأنترنت على مدار 24 ساعة ويومياً دون إجازات أو عطلات ودون إرتباط بساعات دوام العمل.

¹ عبد الغني بسيوني، أصول علم الإدارة، الدار الجامعية للطباعة والنشر، 1993. ص 402.

ثانيا: راحة الجمهور:

من شأن هذا النظام أن يريح الجمهور من عناء الوقوف في طوابير أو صفوف أو السفر لمسافات متباعدة للحصول على المعلومة أو إنجاز معاملة أو كم من مرة إنتهى الوقت الرسمي للدوام قبل أن يصل الواقف في الطوابير إلى شبك الموظف، وفي كثير من الحالات تعرض الطالب الخدمة من المرفق إلى عقوبات وغرامات بسبب عدم إنجازه للمعاملة أو الحصول على خدمة لأنه لم يصل إلى شبك الموظف قبل إنتهاء المواعيد الرسمية للعمل.

لهذا فالحكومات في مختلف دول العالم بدأت تعتمد على وسائل الإلكترونية لتقديم خدمة للجمهور وتلبية حاجيتهم وطلباتهم في حصول دائم على الخدمات أحسن في المرونة والجودة العالية.¹

الفرع الثاني: أثر الحكومة الإلكترونية على مبدأ المساواة أمام المرفق العام.

المقصود بهذا المبدأ بوجود معاملة المرفق العام لطالبي الإنتفاع بخدمة على قدم المساواة، إذ كانت مراكزهم القانونية التي يتواجدون فيها متماثلة وهنا يمكن القول أن التعامل الإلكتروني مع المرفق العام يحقق الفوائد التالية :

أولاً: تحقيق حياد المرفق العام إلكترونياً:

وذلك بالمنع أو التقليل من تمييز بين أفراد على أساس العلاقات الشخصية أو القرابة والطائفة على مشكلة الوساطة والمحسوبية والفساد الإداري وما هو مرتبط من الرشوة والتنفع بإمتيازات الوظيفية الإدارية.

ثانياً: مساعدة الدولة على كفاءة المساواة :

في سبيل تفعيل المساواة ينبغي أن تعمل الدولة على مساعدة الفقراء الذين لا يملكون جهاز الحاسوب

- يمكن استخدامه للإستفادة بالخدمات المرفقية عن طريق توفير أماكن أو الفروع أو مراكز الخدمة في المناطق السكنية تتوافر بها خطوط الأنترنت وأجهزة الحاسوب التي يستخدمها من لا يملك جهاز خاصا به حتى لا يكون الحكومة الإلكترونية حكرا على الأغنياء فقط وتؤدي إلى الإخلال بمبدأ المساواة في الإستفادة من خدمات المرفق العام.

¹ داود عبد الرزاق، المرجع السابق. ص 131 - 144 .

الأمن المعلوماتي للحكومة الإلكترونية

- ظهور تطبيقات جديدة للمساواة: إن الأثر المهم للإدارة الإلكترونية على مبدأ المساواة هو ما تتضمنه من قواعد تنظيمية من شروط يتم بموجبها توفير خدمات الإتصال الإلكتروني أهما عدم التفرقة بين العملاء وتحديد رسم الإستخدام التي يتطلبها إنشاء بوابات إلكترونية للحصول على خدمات المرفق العام.

- الفرع الثالث: المطابقة مع مبدأ القابلية المرفق للتغيير والتعديل في أي وقت:

إن العلاقة القائمة بين المنفعة العامة المرفق العام تفرض تكيفه المستمر مع الظروف المتغيرة ولاسيما الحاجات المتطورة للجمهور ومن ثم أن يكون المرفق العام دائما لديه القدرة على التكيف والتهيؤ مع المتغيرات التي يقتضيها الصالح العام وتطور الحاجات الجماعية، ويفترض هذا المبدأ عدم وجود موانع قانونية مع تنفيذ أو إجراء ذلك التغيير ولا يؤثر في إستعمال الإدارة لهذا الحق أي إعتبار آخر غير مراعاة المصلحة العامة.

ولقد فرض الوسائل الإلكترونية ونيته الحثيثة على الأفراد والإدارات مواكبة علوم العصر وتقنياته حيث لم يعد مقبولا التخلف عن ركب المعرفة التكنولوجية وهو أمر يبين أثر الإدارة العامة الإلكترونية في التطابق مع هذا المبدأ إن من حق الإدارات القائمة على سير المرافق العامة أن تتطلب من أشخاص القانون الخاص المتعاقد معها لأداء عمل حكومي لها، أن تستخدم أحدث الوسائل العلمية والإبتكارات التكنولوجية في تطوير خدمة المرافق وإلا أنهت عقودها بإدارة منفردة.

وتكون اللامركزية التي يطلق عليها في فرنسا اللامركزية الفنية هي الأكثر تجاوبا مع متطلبات مشروع نظام الحكومة الإلكترونية من خلال إنشاء متخصصة وتخضع لمجلس الوزراء ومن خلال هذا المبدأ سيسمح بتحويل إدارة المرفق العام من النظام التقليدي إلى الإلكتروني بصرف النظر عن طريقة الإدارة سواء أكانت مباشرة او غير مباشرة كون ضرورة التعامل الإلكتروني مع المرافق العامة سيزيد من أسلوب الترخيص الإداري ويجعلها أدلة لإسناد إدارة المرفق العام إلى شخص قانوني خاص.¹

المبحث الثاني: الوقاية من الجرائم المتصلة بالحكومة الإلكترونية

نظرا للدور الكبير الذي تمثله الحكومة الإلكترونية في حياتنا المعاصرة حيث أصبحت تقريبا تساهم في كافة المجالات الإدارية والخدمات العمومية وكذا المجالات الاقتصادية ومن ثم إنه أصبح من الضروري حماية الهيكل الحكومي

¹ نفس المرجع السابق، ص 158-166

الأمن المعلوماتي للحكومة الإلكترونية

الإلكتروني من المتعطلين وجماعات التخريب والحفاظ على خصوصية المواطن بحيث انه تتعدد التقنيات والأساليب التي من الممكن أن يعتمدها المهاجمون من أجل إلحاق الأذى بالحكومة الإلكترونية وأنظمتها ولهذا سنتطرق إلى دراسة الوقاية من الجرائم المتصلة بالحكومة الإلكترونية وفق ما يلي:

المطلب الأول: الجرائم المستحدثة في مجال المعلوماتية المرتبطة بالحكومة الإلكترونية

أدى ربط الحاسبات الآلية بعضها ببعض عن طريق شبكات المعلومات إلى سرعة انتقال المعلومات من جهة، وإلى سهولة التطفل عليها من جهة أخرى عن طريق استخدام "المودم" حيث يسمح هذا الجهاز للمتطفلين من أي مسافة يتواجدون فيها بالولوج إلى الحاسبات الآلية المستهدفة، ودون أي مساس مادي بحق ملكية الغير أو ترك أي أثر يدل على إنتهاك المعلومات أو نسخها.

وتتمثل مختلف التقسيمات لجرائم الكمبيوتر المرتبطة بالحكومة الإلكترونية وفق ما يلي:

الفرع الأول: جريمة إختراق الحاسب الآلي والبقاء غير المشروع :

يعد الاختراق ظاهرة إجرامية جديدة ذات خطورة خاصة بإعتبارها تعبير عن قوة حدث تكنولوجيا المعلومات، ويقصد به الدخول غير المصرح به أو بشكل غير مشروع إلى نظام معالجة ألية للبيانات باستخدام الحاسوب وتمثل أركانها في :

أولاً: الركن المادي ويأخذ صورتين:

1- الدخول: ويعني الولوج إلى الحاسب الآلي بصورة غير مشروعة تتحقق عدم المشروعية في عدم صلاحية

القيام بالدخول إلى نظام الحاسوب وبصورة يبرز فيها الجانب كما لو كان ممن لا تتحقق فيهم شروط الدخول إلى نظام حاسوبي وفي هذا نصت المادة 394 مكرر من قانون العقوبات " ... كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من ومنظومة للمعالجة الألية للمعطيات أو يحاول ذلك..."

2- البقاء: ويقصد به المشاركة ذات سيطرة من المخترق على تفاعل الحاسوب مع حركة الدخول والخروج

بغرض البقاء دون أن يقوم بأي نشاط أو حركة سواء إيجابية تفيد الحاسوب أو سلبية تضر به تكلمت عن البقاء نفس المادة سابقة الذكر.

ثانياً: الركن المعنوي:

تعتبر جريمة الدخول والبقاء غير المشروع على الحاسب الآلي جريمة عمدية ومن ثم يجب أن يعلم المخترق بعدم مشروعيته الدخول أو البقاء وأن تنصرف إرادته إلى إرتكاب أفعال الدخول أو البقاء وهذا مرتبط بوجود نظام حماية أو

الأمن المعلوماتي للحكومة الإلكترونية

أمن للمعلومات من عدمه فإذا كانت هناك تشفير للمعلومات يعتبر الدخول إلى هذه المعلومات باي وسيلة والبقاء فيها يعتبر جريمة ويستأهل فاعلها العقاب ولقد حدد المشرع عقوبة هذه الجريمة بالحبس من ثلاثة أشهر إلى سنة وبغرامة من خمسين ألف 50.000 دج إلى مائة ألف 100.000 دج وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

الفرع الثاني: جريمة الإتلاف المعلوماتي: ولهذه الجريمة ركنان

أولا : الركن المادي: الذي يأخذ إحدى الصور التالية:

1- الإعتداء بإتلاف المواد المادية للمعلوماتية كإتلاف الأجهزة أو تكسيرها أو إحراقها أو تعطيلها، وكذلك

الإعتداء على الدعامة المسجلة عليها المعلومات بالكسر أو الحرق أو التشويه مما يجعلها غير صالحة للإستعمال، وكذلك الإعتداء على مشغلات الجهاز من كابلات وشاشات مما يؤدي إلى إيقافها عن العمل وعم صلاحيتها.

2- الإعتداء بإتلاف الدعامات والبرامج المنسوخة عليها المعلومات والأوراق المستعملة في عمل الحاسوب

والشرائط المغنطة مما يؤدي إلى إتلاف المعلومات ويجعلها غير صالحة للاستعمال.

3- كما يمكن أن يكون الإعتداء بطريقة تقنية وفنية لمستخدمي المعلوماتية مثل الإعتداء عن طريق البرامج إما

داخل الشبكة المعلوماتية أو داخل الجهاز المعلوماتي نفسه كبرامج الفيروس والقنابل الموقوتة وبرنامج الدودة وحصان طروادة التي تستهدف تخريب وتدمير ومحو البيانات والمعلومات.

وفي هذا نصت المادة 394 مكرر الفقرة 02 من قانون العقوبات " ...تخريب نظام إشتغال المنظومة تكون العقوبة ... "

ثانيا: الركن المعنوي:

هذه الجريمة عمدية ومن ثم يتوافر فيها القصد الجنائي العام حيث يعلم الجاني بأن الأموال التي يعتدي عليها بالإتلاف هي ملك الغير وأن فعله من شأنه أن يتلف الشيء أو يجعله معطل أو يجعله غير صالح للإستعمال. كما يجب أن تتجه إرادة الجاني إلى إحداث إتلاف أو تخريب أو تعطيل وينتج عن فعله الضرر المترتب على جرمته مع علمه بأن فعله غير شرعي.¹

¹ عصام عبد الفتاح مطر، الحكومة الإلكترونية بين النظرية والتطبيق، دار الجامعة الجديدة للنشر، الإسكندرية، 2013، ص 125-132.

الأمن المعلوماتي للحكومة الإلكترونية

وفي هذا الإطار جعل المشرع العقوبة مشددة من ستة أشهر إلى سنتين والغرامة من 50.000 إلى 150.000 دج .

الفرع الثالث: الجرائم الأخرى:

أولاً: جريمة الإدخال بطريقة الغش للمعطيات:

هو ما نصت عليه المادة 394 مكرر 01 يتمثل الركن المادي فيها في:

- الإدخال بطريقة الغش في نظام المعالجة الآلية أو إزالة أو تعديل بطريقة الغش للمعطيات المتضمنة في النظام

ويتمثل الركن المعنوي في هذه الجريمة بالقصد الجنائي العام فهي جريمة عمدية كونت الجاني يعلم أنه بصدد الإدخال أو الإزالة أو التعديل عن طريق الغش وإرادته متجهة نحو إحداث الضرر المترتب عن الغش .

ثانياً: جريمة التصميم أو البحث أو التجميع أو توفير أو النشر أو الإتجار في المعطيات:

نصا عليها المادة 394 مكرر 2 للفقرة 01 فكل من يقوم عمداً أو عن طريق الغش التصميم أو البحث أو التجميع أو توفير أو النشر أو الإتجار في المعطيات المخزنة أو المعالجة أو المرسله عن طريق منظومة معلوماتية يعاقب الحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج .

ثالثاً: جريمة حيازة أو إفشاء أو نشر أو إستعمال للمعطيات:

نصت عليها المادة 394 مكرر 2 فقرة 02 بحيث ان حيازة أو إفشاء أو نشر أو إستعمال للمعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها سابقا وحددت لها نفس العقوبة السابقة.

المطلب الثاني: التحديات الأمنية للحد من جرائم المعلوماتية

يمتد الجدل والنقاش إلى التساؤل عن مدى كفاية آليات مكافحة الجرائم الجديدة سواء من حيث التقنية العلمية المستخدمة، أو من حيث تأهيل العناصر البشرية القادرة على اكتشاف الجريمة ذات الطبيعة التقنية المعقدة، والتحقيق فيها. والقدرة على التعامل مع مختلف القرائن والأدلة الرقمية Digital evidence أحياناً، ناهيك عن قصور التشريعات الدولية والوطنية في معظم الدول.

والمشكلة التي تواجه مجتمعات اليوم - والأجهزة الأمنية تحديداً - أن الجريمة في مظهرها القديم لم تختلف بل زادت، وظهرت علاوة عليها أنماط من الجرائم المستحدثة زادت من حجم الضحايا والخسائر على كافة المستويات. وفي تحسب لهذه الظاهرة؛ وإدراكاً لحجم خطورتها يمكن الإشارة هنا إلى أن الرئيس الأمريكي السابق "Clinton" طلب في يناير 2000م من الكونغرس تخصيص مبلغ 2 بليون دولار كميزانية لأمن الحاسبات وحدها.

وفقاً للمفهوم الحديث للأمن الذي يرى بأن هذا المدلول لا يقتصر على الجانب الجنائي الذي تقوم عليه الأجهزة الأمنية التنفيذية، يمكن أن نحدد العديد من التحديات الأمنية المصاحبة لشبكة الإنترنت. ولكن قبل هذا ربما يحق لنا القول بأن النظرة التقليدية لمفهوم الأمن الذي تحتزله في الأجهزة الرسمية تحل بأهمية أدوار المؤسسات الاجتماعية

الأخرى التي تقوم بمهام كبيرة ضمن مفهوم أرحب، ومنظمة متكاملة تدرج كلها تحت مفهوم الأمن الشامل الذي يشمل كافة الصور المختلفة التي تسهم مجتمعة في تحقيق الأمن في صورته المتكاملة للجميع.

الفرع الأول: تحدي الأمن الوطني :

ظهرت شبكة الإنترنت بميزاتها الكثيرة عابرة للحدود الجغرافية، والثقافية، والسياسية، وحتى الدينية، وعلى منطديات الإنترنت، ومن خلال واقعها، وتطبيقاتها بات مفهوم السيادة الوطنية محل تساؤل. فعن طريق هذه الوسيلة بات ممكناً تنظيم الاجتماعات بين المجموعات الإجرامية لتنسيق المواقف، وتبادل المعلومات، والخدمات. كما بات ممكناً مع الإنترنت تزايد حالات الاختراق للأمن الوطني مثل قضايا التجسس المعلوماتي والاقتصادي، وتهديد الكثير من مقومات الأمن الوطني عن طريق بث الشائعات والأخبار المكذوبة، لإحداث البلبلة بين أفراد المجتمع. ومع انتشار التقنيات الحديثة ظهرت موجة جديدة من الجرائم غاية في التشابه، والتعقيد، تطلبت تعاطياً مهنيّاً، وأمنياً، على نفس درجة التحدي. وحتى يمكن وضع تصور عام للبيئة الإجرامية التي تتم فيها جريمة الحاسبات، والإنترنت، نجد أن من الضروري تحليل خصائص هذا النمط من الجرائم التي يتضح أنها تتم وفق ظروف موضوعية مختلفة تتمثل في الآتي:

- ضعف سبل المقاومة ضعف الإعداد الفني والبشري.
 - صعوبة وضع وسائل التحقيق الروتين، وعدم أجهزة الأمن، ويصعب عملية التدريب.
 - التكلفة العالية لأساليب المكافحة الأجهزة، والتعليم والتدريب.
 - التقنية، واستخداماتها السلبية أسرع من التشريعات.
 - مخترعات، ووسائل المكافحة غالباً ما تأتي متأخرة الفعل ورد الفعل.
 - تدني مستوى الوعي الإداري، والاجتماعي بخطورة المشكلة.
 - قلة الاستثمار في مجالات البحث العلمي للمساهمة في مكافحة جرائم التقنية.
- وفي ضوء ذلك كله يمكن تمييز بعض الخصائص الرئيسة للجريمة على شبكة الإنترنت منها:
- يسهل نظرياً ارتكاب الجريمة ذات الطابع التقني.
 - يسهل إخفاء معالم الجريمة، وصعوبة تتبع مرتكبيها.

- الحرفية الفنية العالية التي تتطلبها سواء عند ارتكابها أو مقاومتها.
 - تعدد الأطراف المرتبطة بها حيث يلعب البعد الزمني اختلاف المواقف بين الدول، والمكاني الجريمة، وهو يعكس بطبيعة الحال اتساع نشاطها.
 - أن جريمة الإنترنت تتطلب قدراً كبيراً من الذكاء والمعرفة من مرتكبيها وفريق المكافحة.
 - تتم الجريمة بشكل سريع، وحاسم أحياناً في دقائق معدودة.
 - ترتكب الجرائم عبر الإنترنت بدقة بالغة نتيجة دقة أدوات الجريمة (برامج).
 - التخفي عبر دروب الإنترنت هو أهم ما يميز مرتكبي هذه الجرائم، بحيث يمكن أن يختفون تحت قناع فني يظهرهم من دولة إلى أخرى.
 - جرائم الإنترنت تتسم بالغموض حيث يصعب إثباتها، والتحقيق بها، كما هو الحال في الجرائم التقليدية.
 - الصورة الذهنية لمرتكب جرائم الإنترنت غالباً هي صورة البطل، والذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يتوجب محاكمته.
 - في أغلب الأحوال لا تستخدم أساليب عنيفة من قبل مرتكبي جرائم الإنترنت.
 - كثير من جرائم الإنترنت لا يتم الإبلاغ عنها.
- تستدعي جرائم التقنية نخبة متميزة من المحققين من ذوي التأهيل، واستعداد جيد حيث يتطلب التحقيق في الجرائم ذات الطبيعة التقنية قدراً كبيراً من التخطيط، والمهارة أنظر أكاديمية نايف العربية، 1999: البشري، 1421هـ، موسى 2001 حتى يمكن أن تكتمل عناصر القضية بشكل دقيق يتفق وطبيعة هذه الجرائم. وتأسيساً على ذلك فإن بعض الخبراء يرى أن من الضروري وضع حدود فاصلة، وواضحة لإجراءات المكافحة، والتفريق بين إجراءات الوقاية، ومسائل الضبط، والمتابعة، وإجراءات مباشرة جرائم الحاسب. Golmann، 1999 وإجمالاً يمكن الإشارة إلى بعض النقاط الأساسية التي ربما يحسن للمحقق أخذها في الاعتبار ومنها :
- تحليل المشكلة (الجريمة).

الأمن المعلوماتي للحكومة الإلكترونية

- ينبغي على المحقق المبادرة بالتحقيق فور تلقي التقرير بوجود نشاط إجرامي، أو جريمة ذات طابع تقني، واستغلال عامل الوقت.
 - يحتاج المحقق بعد تحليل العناصر الأساسية للقضية إلى النظر في الموضوع في ضوء الأسئلة التالية :
 - هل هناك قضية وبالتالي عمل جنائي يتطلب التحقيق؟
 - هل كان جهاز الحاسب ذاته هدفاً للدخول على المحتويات بقصد التعديل أو سرقة معلومات أو تخريبها سواء كان الجهاز شخصياً، أو متصلاً بالشبكة.
 - ما مدى الأضرار على الإدارة أو الشخص الذي كان ضحية لجريمة ذات بعد تقني، وكيف يمكن تحجيمها؟
 - هل اكتملت عناصر الموضوع بصفة واضحة، وجلية؟
 - هل يمكن إشراك عنصر، أو عناصر موثوقة من منسوبي المكان الذي ارتكبت فيه المخالفة لتسرع الإجراءات، وفهم طبيعة النظام الإلكتروني بشكل سريع؟
 - هل يوجد لدى المحقق ما يكفي من المهارة الفنية لمواجهة المتهم إن وجد بالحقائق ومناقشته بشيء من الندية في كافة التفاصيل.
 - هل يمكن تقديم نصيحة أمنية من خلال التحقيقات لتساعد الإدارة، أو الشخص في تجنب تكرار ما حصل.
- وبشكل عام فإن أهم وسائل المكافحة تبدأ بالاستعداد الجيد سواء من حيث إعداد الكفاءات البشرية المؤهلة، أو إنشاء الوحدات المتخصصة للتحقيق في جرائم الحاسب، والإنترنت، ويتوافق مع هذا ضرورة توفير الموارد المالية اللازمة لهذه الوحدات التي ترصد، وتضبط ظواهر إجرامية تتسم بالتغير، والسرعة تحتاج معه إلى مرونة في القرار الأمني، والقرار المالي.
- الفرع الثاني: دور الشرطة في البحث والتفتيش والضبط.**
- صدر القانون رقم 04/09 المؤرخ في 05 أوجست 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي وضع قواعد خاصة للوقاية منها وحدد المفاهيم العامة لما هو متصل بتكنولوجيات الإعلام والاتصال ومجالات التطبيق ومراقبة الاتصال خاصة المادة 04 وكذا القواعد الإجرائية المتعلقة بالتفتيش المادة 05 أما في المادة 06 فتكلمت عن حجز المعطيات وكذا إلزام مقدمي الخدمات المادة 10.

الأمن المعلوماتي للحكومة الإلكترونية

بحيث تختص وحدات متخصصة من أجهزة الشرطة بمكافحة جرائم الإنترنت بعد تلقي التعليم والتدريب الكافيين على استخدام شبكات المعلومات واستخدام الأجهزة الفنية الحديثة والمعرفة الكافية باللغات الأجنبية، ما يسمح لها القيام بإجراءات التفتيش والضبط والتحفظ على الأدلة التي تساعد على إثبات الجريمة. وعلى الرغم من عدم اختصاص هذه الوحدات، بملاحقة بقية الجرائم التي ترتكب بواسطة الإنترنت مثل مكافحة المخدرات وغسيل الأموال والإرهاب والدعارة واستخدام الكروت الإلكترونية وجرائم التجارة الإلكترونية، إلا أنها تلعب دوراً هاماً في معاونة الأجهزة القائمة على مكافحة هذه الجرائم باعتبارها متخصصة في مجال الحاسبات الإلكترونية. فهي تقدم لباقي الوحدات دعماً فنياً في مجال البحث والتفتيش وتحليل المعلومات التي يحصلون عليها وتحضير الوثائق الرسمية بالنسبة لما حصلوا عليه من وثائق والمثول أمام المحاكم للشهادة.

أولاً : البحث الجنائي في مجال جرائم الحاسب :

يعتقد البعض أن الإنترنت وشبكات المعلومات كمجالات فضائية يصعب فيها تطبيق القانون وذلك لمداه الدولي وغياب نقاط المراقبة على الشبكات، وتقنيات إرسال الرسائل، وعدم ذكر الأسماء أو التحقق من هويتهم، وتشفير التوقيعات الكتابة السرية Cryptographies وهي خصائص يتميز بها الإنترنت تجعل من الصعب تحديد شخصية وملاحقة مرتكب الأفعال المجرمة. مما يعقد عمل الشرطة والعدالة وربما تبقى في الكثير من الأحوال مكتوفة الأيدي.

** إلا أن هذا التحليل غير صحيح للأسباب التالية :

● أولاً: يجب العلم بأن الأفعال المجرمة التي ترتكب في داخل حدود الدولة، دون أن يمتد أثرها إلى خارجها، يستطيع المحققون أن يتصرفوا حيالها دون مصاعب أو تعقيدات.

● ثانياً: إن عدم معرفة شخصية الفاعل التي يتستر ورائها مرسل الرسالة غير المشروعة هو أمر نسبي إذ لا يوجد "تجهيل" بالمعنى الصحيح بالنسبة لشبكة المعلومات حيث يترك الفاعل "آثاراً" أثناء تنقله في طرقات شبكة المعلومات تسمح للمحققين الوصول إليه.

وأخيراً فإن الطابع الدولي للجريمة لا يمثل عقبة تمنع إجراء التحقيق والملاحقة وإلا ستساعد على خلق (جنات افتراضية) تمثل خطراً على الأمن العام الدولي.

ثانياً : مراحل تتبع الجريمة

التأكيد على تحديد هوية مرتكب الجريمة

إذا كان تحديد هوية الفاعل بالنسبة لشبكات المعلومات لم يعد وهماً، فإن الكشف عن الشخصية الحقيقية للشخص الطبيعي الذي ارتكب الجريمة ما زال يواجه الكثير من الصعاب.

الأمن المعلوماتي للحكومة الإلكترونية

لذلك من الضروري تحسين أسلوب تتبع "آثار الرسائل" وتحديد هوية المستخدمين حتى يمكن تحريك دعوى المسؤولية. وهنا يظهر أهمية دور مؤدي الخدمة كهمزة وصل ضرورية بالنسبة لنقل المعلومات. ويوجد العديد من المقترحات في هذا الصدد.

- تحديد شخصية المشتركين بشبكات المعلومات

من الضروري تحديد هوية المشتركين بشبكات المعلومات لتسهيل عمل الشرطة في حال وقوع أي مخالفة، حيث يجب على مؤدي الخدمة أن يكون قادراً على تقديم بيانات شخصية عن زبائنه، في إطار التحقيقات التي تتم بواسطة الشرطة أو رجال النيابة عندما يطلب منه ذلك. هذا الأمر يقتضي من مؤدي الخدمة أن يطلب البيانات الشخصية لكل عميل يطلب الاشتراك عبر شبكته.

وهنا تثار مشكلة جديدة بالنسبة للاشتراكات المجانية التي تتم دون تحديد هوية المشترك. هذه الاشتراكات هي التي تسهل ارتكاب الجرائم في ظل غياب أي تحديد لهوية أو مكان المستخدم وهو ما يصعب منعه أو إلغاؤه.

- حفظ البيانات المتعلقة بالاتصال بواسطة مؤدي الخدمة :

البيانات التي تتعلق بالاتصالات التي يقوم مؤدي الخدمة بتجميعها أتوماتيكياً عند توصيل المستخدم بالشبكة، تعد ذات قيمة معلوماتية كبرى لرجال التحقيق. ويظهر فيها المستخدم، ووقت بداية ونهاية الاتصال، والرقم الكودي للمتصل، والمواقع التي زارها، والمعلومات التي طلبها والبيانات التي حصل عليها هذه المعلومات وغيرها تعد بمثابة الآثار التي يتركها المستخدم.

وتحفظ هذه البيانات بواسطة مؤدي الخدمة لفترات متغيرة حسب أهمية وكثافة تردد العملاء ومن المهم الاحتفاظ بهذه المعلومات لفترة كافية، حتى يمكن تسهيل عمل رجال البحث في متابعة وإقامة الدليل على المخالفات التي ترتكب.

وتعد هذه البيانات الهدف الرئيسي والمهم لعمل رجال الشرطة، أنظر لشدة وكثافة ارتكاب هذه المخالفة. إلا أن تلك البيانات لا تحفظ إلا لمدة يومين فقط، بينما مدة حفظ المعلومات المتعلقة بالاتصالات التليفونية بواسطة Alcatel هي عام كامل.

لذلك يجب مد مدة حفظ البيانات بالنسبة لشبكات المعلومات لمدة لا تقل عن ثلاثة أشهر وتوقيع جزاء على المخالف. وبالرغم من ذلك فإن هذا الإجراء يبدو غير واقعي بالنسبة للرسائل الإلكترونية، حيث يتم مسحها بانتظام بواسطة مؤدي الخدمة نظراً لكثافة عددها والاجتماعات والمناقشات التي تتم كل لحظة. وتكون بعض الأدلة قاطعة الدلالة، أحياناً، أكثر من شهادة الشهود ويلزم أن ننوه هنا بأن المحاضر الأولية في هذا الصدد تتمتع بقيمة وأهمية خاصة حيث أنه لا يمكن عملها إلا بواسطة ضباط الشرطة أو الأشخاص المحلفين أو من لهم صفة الضبطية القضائية بموجب نصوص خاصة.

الأمن المعلوماتي للحكومة الإلكترونية

والدليل القانوني هو ما يستمد من أعمال التحقيق الذي يختلف بطبيعته عن أعمال الاستدلال التي لا يتولد عنها أدلة بالمعنى القانوني، ولا يجوز أن يكون سند القاضي في الحكم أدلة وردت في محضر الاستدلال. ولكن يمد النيابة العامة بما يسمح برفع الدعوى الجنائية بناء على هذه الأدلة كأساس للتحقيق الذي يستخلص منه الدليل في معناه القانوني.¹

التفتيش والضبط :

يتم التفتيش في مكان معين بهدف الكشف عن أشياء أو تجميع أدلة خاصة بجريمة ما حتى يمكن استخدامها في ملاحقة المجرمين. وأما الضبط يحدث عند الحصول على تلك الأشياء أثناء التفتيش ويطلق عليها مضبوطات أشياء لغرض التحقيق أو إثبات أدلة تتعلق بالجريمة.

ويجب على ضباط الشرطة القضائية إجراء المعاينات من خلال الانتقال إلى مكان الواقعة وإثبات حالة الأشياء والتحفظ على الأدلة والقرائن المادية التي تنفي في إثبات وقوع الجريمة ونسبتها إلى مرتكبيها. الفكرة الأساسية لهذين التعريفين هو إجراء تحقيق معمق في نفس المكان وهو إجراء جنائي.

والسلطة المنوط بها البحث عن المعلومات وإجراء التحقيق والقيام بالضبط تقوم بفحص الأماكن بواسطة الضابط المختص عندما يكون لديها الأسباب المعقولة للاعتقاد بأن الجريمة قد وقعت أو ستقع لتقوم بالبحث عن الأدلة المتعلقة بهذه الجريمة وتقوم بالفحص الدقيق بهدف منع وقوع الجريمة أو معاقبة فاعلها.

ويسمح إذن التفتيش للشخص المكلف بتنفيذه سلطة تفتيش المكان للبحث عن الأشياء وأيضاً البحث في داخل النظام المعلوماتي الموجود في المكان المحدد للحصول على معلومات يمكن أن تستخدم كدليل على ارتكاب الجريمة وضبط وحفظ هذه المعلومات.

وهناك اعتباران يجب أخذهما في الحسبان بخصوص إذن التفتيش :

أولاً: إن من يرخص بالتفتيش سواء القاضي أو النيابة يجب أن يلتزم بالحياد وعدم الانحياز بين الطرفين المعنيين، المصلحة العامة والمصلحة الخاصة.

ثانياً: إن من يطلب الإذن بالتفتيش يجب أن يقسم بأن لديه من الأسباب المعقولة (وليس فقط وساوس أو شكوك) تحمله على الاعتقاد أن هناك جريمة قد ارتكبت وأن هناك أدلة موجودة في المكان المطلوب تفتيشه.

أسلوب التفتيش عن البيانات على شبكة المعلومات :

¹ تشمل الأدلة الجنائية الإلكترونية على عملية العثور على المعلومات وفلك كلمات المرور التي تحميها، وفحص المعلومات المختزلة، وتعقب مصدر البريد الإلكتروني، وقرصنة البرمجيات، واسترجاع البيانات المحذوفة، وربط المعلومات والأقراص المرنة بالحسابات التي تم تكوينها بواسطتها ومراقبة الحاسبات الآلية عن بعد، وكذلك الاحتفاظ بالأدلة الإلكترونية من أجل تقديمها في المحكمة.

يتم التفتيش عن البيانات بإحدى طريقتين :

إما معرفة رقم الاتصال الذي تم من مسرح الأحداث، أي على نفس الحاسب المستخدم في ارتكاب الجريمة. أو نقل محتويات الاسطوانة الصلبة الخاصة بالجهاز وتفتيش المكان.

ويجب على ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة.

ولكي ينجح المحققون في عملهم يجب أن يقتنفوا أثر الاتصالات منذ الحاسب المصدر إلى الحاسب أو المعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل ودولة. ولكي تحدد سلطات الشرطة مكان الجريمة ترتكن عادة إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات. من أين صدرت؟ ومن الذي يحتمل إجراؤها؟ كما يجب على رجال الشرطة، في حالات أخرى، متابعة الاتصال لحظة إجرائه. الأمر الذي يستلزم دائماً تعاون ومساندة زملائهم في الدول الأخرى.

خاتمة:

ناقشنا في هذا البحث إطار الحكومة الإلكترونية من خلال التطبيق لمفهومها الذي حددنا فيه مدلولها القانوني وأثارها التطبيقية على الخدمة العامة للجمهور ومن ثم إتجهنا إلى تحديد مختلف الجرائم التي يمكن أن تتصل بتطبيقات الحكومة الإلكترونية كخدمة من خدمات المعلوماتية ورأينا أن ما يصيب شبكة المعلوماتية من جرائم يمكن أن يصيب الحكومة الإلكترونية ثم تطرقنا إلى آليات الوقاية من تلك الجرائم.

ونظراً لكون المعلومات أصولاً ذات قيمة بالنسبة لهيئة ما مثلها في ذلك مثل الأصول الأخرى الخاصة بالأعمال، وبالتبعية فهي تحتاج أن تتوافر لها الحماية المناسبة .

إن تأمين المعلومات يوفر الحماية من الكثير مما يهددها، وذلك بهدف التأكد من استمرارية العلم، ولتقليل احتمالات الخسارة في الأعمال ولرفع العائد من الإستثمارات وفرص العمل.

يوصف مبدأ تأمين المعلومات بأنه للمحافظة على:

- السرية: وذلك من خلال التأكد من أن المعلومات متاحة فقط لمن هم مصرح لهم بالوصول إليها.

- التكامل: يتمثل في حماية ودقة المعلومات وتماها وحماية طرق معالجتها.

- التوافر: التأكد من ان المستخدمين المصرح لهم يمكنهم الوصول إلى المعلومات وإلى الأصول المضمنة وقت

حاجتهم لها.

الأمن المعلوماتي للحكومة الإلكترونية

لهذا ينبغي أن تكون هناك منظومة تشريعية تنظيمية وكذا حماية توفر لما يعرف بالحكومة الإلكترونية (الإدارة الإلكترونية) التأمين اللازم والضامن لإستمرارية نشاط الإدارة.

قائمة المراجع

- 1) ماجد الحلو، الحكومة الإلكترونية والمرافق العامة، بحث مقدم إلى المؤتمر العلمي الأول الذي نظّمته أكاديمية شرطة دبي حول " الجوانب القانونية والأمنية لعلميات الإلكترونية من 26-28 أبريل .
- 2) محمد حسين النيلي، العلاقة بين القانون والحكومة الإلكترونية، ورقة عمل قدمت لمؤتمر الكويت حول الحكومة الإلكترونية في الفترة 13-15 أكتوبر 2003.
- 3) داود عبد الرزاق، الإدارة العامة للحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام وأعمال موظفيه، مجلس النشر العلمي، جامعة الكويت، 2004 .
- 4) عبد الغني بسيوني، أصول علم الإدارة، الدار الجامعية للطباعة والنشر، 1993.
- 5) عصام عبد الفتاح مطر، الحكومة الإلكترونية بين النظرية والتطبيق، دار الجامعة الجديدة للنشر، الإسكندرية، 2013.
- 6) قانون العقوبات الصادر بموجب الأمر 159/66 المعدل والمتمم .