مخاطر القرصنة المعلوماتية على الحكومة الالكترونية

الأستاذ يحياوي محمد
كليةالعلوم الاقتصادية والعلوم التجارية وعلوم التسيير
جامعة البويرة
Gom182 hotmail.com

Résumé

Le progrès dans le domaine des technologies de l'information et de la communication a abouti à l'émergence de plusieurs applications positives, ce qui a aidé à la transition vers la société de l'information, et le plus important de ces applications ; le soi-disant gouvernement électronique. Celui-ci est destiné à fournir des renseignements gouvernementaux et des services par Internet.

En parallèle à cette évolution, il y a une utilisation négative de la technologie moderne comme la destruction des sites du gouvernement ou l'utilisation à des fins de l'infraction et le vol d'informations de nature confidentielle, c'est ce qu'on appelle le piratage d'informations

Ainsi, il est devenu nécessaire de construire un système de sécurité électronique compatible avec ce nouveau type de crime pour la protection des sites gouvernementaux.

الملخص

لقد أدى التطور الحاصل في ميدان تكنولوجيا المعلومات والاتصالات إلى بروز عدة تطبيقات ايجابية ساعدت في الانتقال نحو مجتمع المعلومات، ومن أهم هذه التطبيقات ما يعرف بالحكومة الالكترونية، والمقصود بهذه الأخيرة تقديم مختلف المعلومات والخدمات الحكومية عن طريق شبكة الانترنت. وبالتوازي مع هذا التطور، ظهر الاستخدام السلبي لهذه التكنولوجيا الحديثة كاختراق المواقع الحكومية بغرض تدميرها أو لغرض التعدي وسرقة المعلومات ذات الطابع السري، أو ما يعرف بالقرصنة المعلوماتية.

وبالتالي، أصبح من اللازم بناء أنظمة أمنية الكترونية تتوافق والنوع الجديد من الجرائم لحماية المواقع الحكومية

مقدمة

في 20 سبتمبر من عام 2001 أصيب ميناء هيستن الأمريكي، وهو من الموانئ الرئيسية في الولايات المتحدة الأمريكية، ويعد تاسع أكبر ميناء في العالم، بالشلل، نتيجة هجوم فيروس إليكتروني سبب تعطل أنظمة الكومبيوتر في الميناء. وقد قام القرصان الذي لا يتجاوز التاسعة عشر عاماً من العمر بتعطيل الكمبيوتر المخدم الرئيسي للميناء، باستعمال سلاح الإيميل، وأمطره بآلاف الرسائل الإلكترونية مما أصابه بالشلل. ما هو هذا العصر الذي يصبح فيه شاب، قد يكون ضعيف البنية هزيلاً،

ذا نظارات، لا يتجاوز العشرين من العمر، أقوى من جميع قراصنة البحار، ويستطيع بمفرده أن يوقف العمل في تاسع أكبر ميناء في العالم؟! إنّه عصر الثورة المعلوماتية.**(1)** ويعد مفهوم الحكومة الالكترونية من أبرز المفاهيم التي أدخلتها الثورة المعلوماتية وشبكة الانترنت إلى الحياة اليومية للمواطنين، والتي ظهرت نتيجة لتطورات تقنية متفاعلة مع الإنسان على مستوى جغرافي واسع، حيث تعد فكرة الحكومة الالكترونية من الأفكار الجديدة في تطبيقاتها، تهدف إلى إحداث تطوير جذري

في الأداء الحكومي، ومن بين الأساليب الفاعلة في تطوير تقنية الحكومة الالكترونية هي تبني أنظمة أمنية لحماية المعلومات الحكومية من مختلف التهديدات والاستعمالات غير المشروعة.

أولا: تعريف الحكومة الالكترونية

تعني الحكومة الالكترونية " قدرة الأجهزة والهيئات الحكومية على إتاحة المعلومات وتقديم الخدمات الحكومية فيما بينها وبين المواطنين ومنظمات الأعمال والجهات الأخرى التي تتم التعامل معها بأسلوب سهل وسريع وأكثر مرونة وفي أي وقت 24 ساعة يوميا طوال أيام الأسبوع.**(2)** الحكومة الالكترونية هي "قدرة القطاعات الحكومية المختلفة على توفير الخدمات الحكومية المختلفة والتقليدية للمواطنين وإنجاز المعاملات عبر شبكة الانترنت بسرعة ودقة متناهيتين، وبتكاليف ومجهودات أقل، من خلال موقع واحد على الشبكة.**(3)**

الحكومة الالكترونية هي " قدرة الأجهزة الحكومية على تبادل المعلومات فيما بينها من جهة، وتقديم الخدمات للمواطنين وقطاع الأعمال من جهة أخرى، وذلك بسرعة عالية وتكلفة منخفضة عبر شبكة الانترنت، مع ضمان سرية وأمن المعلومات المتناقلة في أي وقت وأي مكان.**(4)**

من خلال هذه التعاريف يمكننا تقديم التعريف التالي للحكومة الالكترونية: هي قدرة القطاعات والأجهزة الحكومية المختلفة على تقديم الخدمات والمعلومات للمستفيدين منها إلكترونيا، وبشفافية، ومساواة، وبسرعة متناهية ودقة عالية في أي وقت وأي مكان باستخدام التقنيات الحديثة المتطورة مع ضمان سرية وأمن المعلومات.

ثانيا: أهداف الحكومة الالكترونية

يعد تطبيق الحكومة الالكترونية وسيلة وليست غاية في حد ذاتها، ذلك أن التحول لنظام الحكومة الالكترونية من قبل الجهات الحكومية وجهات القطاع الخاص سيؤدي إلى تحقيق أهداف تتفق مع ثورة المعلومات وتكنولوجيا الاتصالات، الأمر الذي سينعكس على شكل الأداء العام ومدى تقديم الخدمات للجمهور بسهولة ويسر وتكلفة أقل. ويمكن إيجاز أهداف الحكومة الالكترونية فيما يلي:

1. استخدام التكنولوجيا المتطورة للوصول إلى حكومة الكترونية تعزز مجالات الحياة الالكترونية وبالتالي في تحقيق النقلة النوعية بالانتقال إلى عالم التكنولوجيا وعصر المعلوماتية؛

2. انخفاض الإنفاق الحكومي وذلك من خلال انخفاض تكلفة الخدمات الحكومية المقدمة نتيجة لتغيير طريقة تقديم وتنفيذ الخدمات وآليات توصيلها من الشكل التقليدي إلى الشكل الالكتروني وهذا ما سيؤدي إلى وفرة في ميزانية الدولة؛**(5)**

3. تحسين مستوى أداء الخدمات لتفادي الأخطاء اليدوية التي قد تحدث عند تأدية الخدمة بالطريقة التقليدية، وبالتالي فإن تدفق بيانات المعاملات تتم بسهولة وآمان لوجود شفافية لتتبع الأداء لكل معاملة في أي وقت، مما يوفر لمتخذ القرار معرفة مسببات التأخير؛

4. تحسين فعالية وكفاءة الإدارة العامة، تحسين مستوى المعرفة واستعمال التكنولوجيا الحديثة؛

5. إعادة هندسة إدارة الموارد البشرية، وبناء القدرة على إدارة التغيير وإيجاد ثقافة مؤسسية جديدة؛

6. ترشيد العمليات الحكومية وتقليص الازدواجية في الإجراءات؛

7. حماية المواطنين من متاهات البيروقراطية، وذلك من خلال تبسيط واختصار الإجراءات، تقديم الخدمات الحكومية بتكلفة أقل وجودة أعلى وفي كل وقت؛

8. دعم الشفافية ومحاسبة المسؤولين والثقة في عمليات الحكومة.**(6)**

ثالثا: متطلبات بناء الحكومة الالكترونية

تعتمد توفير تلك المتطلبات بتقنية الحكومة الالكترونية من حيث تقديم الخدمات ووسائل نقل المعلومات وطلب الخدمات من قبل المستفيدين على مايلي:

1. تأهيل الكوادر البشرية: تتطلب الحكومة الالكترونية تغييرات جذرية في نوعية العناصر البشرية الملائمة لها، وهذا يعني ضرورة إعادة النظر بنظم التعليم والتدريب لمواكبة متطلبات التحول الجديد بما في ذلك الخطط والبرامج والأساليب التعليمية، والتدريبية على المستويات كافة، وإلى توعية اجتماعية بثقافة الحكومة الالكترونية وبطبيعة هذا التحول والاستعداد النفسي والسلوكي والفني والمادي، وغير ذلك من متطلبات التكيف، ويعد وجود المجتمع المعلوماتي مطلبا مهما لتحقيق مشروع الحكومة الالكترونية، ولذلك فإنه ينبغي سرعة تحويل فئات وشرائح المجتمع إلى الاهتمامات المعلوماتية مما يعجل بدخول المجتمع ضمن مظلة المعلوماتية.**(7)**

2. توفر قاعدة وطنية لتكنولوجيا المعلومات والاتصالات: يقصد بتكنولوجيا المعلومات والاتصالات تلك المعدات التكنولوجية التي يعتمد عليها في معالجة المعلومات الحكومية ونقلها إلى المواطنين، وأهم الوسائل المعول عليها في تقديم الخدمات الحكومية نذكر ما يلي:

أ. أجهزة الحاسب الآلي: الحاسب الآلي هو ترجمة حرفية للكلمة اللاتينية Computer كمبيوتر وهي مشتقة من الفعل Compute بمعنى حسب، لذلك يطلق على الكمبيوتر في اللغة العربية الحاسب الآلي أو الحاسوب. وهو جهاز إلكتروني سريع ودقيق وقادر على معالجة البيانات، صمم ونظم لقبول وتخزين

ومعالجة البيانات أوتوماتيكيا لإنتاج مخرجات باستخدام خطوات مطولة تمثل مجموعة من التعليمات.(8) وتتمثل أهم خصائصه في السرعة، الدقة، سعة كبيرة لتخزين البيانات، المرونة، القابلية للتوسع.

ب. البرمجيات: تتكون البرامج من عدة أنواع، فبرامج نظم التشغيل Operating System هي مجموعة من البرمجيات Software المعقدة يتواجد بعضها في الذاكرة بشكل دائم أثناء عمل الحاسب الآلي ليراقب كل ما يقوم به من عمليات ويعرف ببرنامج المشرف Supervisor، وعند البدء بتشغيل الحاسب الآلي لأول مرة يتم تحميل نظام التشغيل إلى الذاكرة سواء من القرص الصلب أو القرص المرن وتسمى System Initialization.

أما البرامج التطبيقية Application Software فتقوم بتوجيه الحاسب الآلي لتنفيذ المهام التي يتطلبها عمل المستخدم مثل معالجة طلب المبيعات، أو إجراء عمليات الحجز في رحلات الطيران، أو معالجة النصوص أو إعداد وطباعة الفواتير أو غيرها. وتسمى مثل هذه المهام التي ينفذها الحاسب الآلي بالتطبيقات، أما البرامج التي توجه الحاسب الآلي فتسمى بالبرمجيات التطبيقية.(9)

ج.شبكة الإنترنت: الإنترنت Internet كلمة إنجليزية تتكون من جزأين، الجزء الأول (Inter) يعني **بين،** والجزء الثاني (Net) يعني **شبكة،** وترجمتها الحرفية تعني : الشبكة البينية ومدلولها يعني الترابط بين عدد كبير جدا من شبكات الحاسب الآلي في جميع أنحاء العالم.(10)

وهناك من يعرفها بأنها شبكة عالمية تربط الحواسيب، والشبكات الصغيرة ببعضها عبر العالم، وذلك من خلال تكنولوجيا الاتصال بهدف تأمين الخدمات الحاسوبية الحديثة بشكل مبسط وجذاب.(11)

ومن أبرز الخدمات التي تقدمها شبكة الإنترنت للمستخدم ما يلي:(12)

- خدمة البريد الإلكتروني Electronic Mail
- خدمة برتوكول نقل الملفات File Transfer Protocol
- خدمة الشبكة العنكبوتية العالمية للمعلومات
- خدمة الربط عن بعد Telnet
- المجموعات الإخبارية (News Groups)
- المحادثات الشخصية والدردشة الجماعية (Chatting)
- الأرشيف الإلكتروني
- الاستعلامات واسعة النطاق (Wais)

د. شبكة الإنترانت Intranet: تطلق تسمية الإنترانت على التطبيق العملي لاستخدام تقنيات الإنترنت في الشبكة الداخلية للمؤسسة، بغرض رفع كفاءة العمل الإداري وتحسين آليات تشارك الموارد والمعلومات والاستفادة من التقنيات المشتركة. كما تقدم شبكة الإنترانت خدمة الدخول إلى الإنترنت، بحيث لا يمكن لغير المسجلين في شبكة الإنترانت الدخول إليها عن طريق الإنترنت، وبذلك تؤمن الإنترانت صورا منيعا حول محتوياتها مع المحافظة على حق وصول العاملين عليها إلى مصادر المعلومات الخارجية على

الإنترنت. وتقدم شبكة الإنترانت خدمات كالبريد الإلكتروني E. mail وتقنية الملفات الإلكترونية المحمولة وخدمة نقل الأخبار وخدمة مؤتمرات الفيديو Conference Video.**(13)**

هـ. شبكة الإكسترانت Extranet: أنشأت شبكات الإكسترانت استجابة لما يتطلبه قطاع الأعمال من تشارك وتحالفات وما يقتضيه من أمن على المعلومات المتبادلة مع العناية الشديدة بالمصالح المشتركة عن طريق الشبكات.

وشبكة الإكسترانت تعتمد على قطاع الأعمال الذي يقسمها إلى أنواع منها شبكات إكسترانت التزويد Supplier Extranets، شبكات الإكسترانت التوزيع Distributor Extranets وشبكات الإكسترانت التنافسية Peer Extranets.**(14)**

3. وجود خطط التطبيق والرؤية الإستراتيجية: ويتطلب تحقيق ذلك العديد من الخطوات التفصيلية، هي:**(15)**

- تشكيل إدارة أو هيئة أو نظام وطني لتخطيط ومتابعة وتنفيذ مشروع الحكومة الالكترونية؛
- وضع الخطط لمشروع الحكومة الالكترونية؛
- الاستعانة بالجهات الاستشارية والبحثية للدراسة؛
- وضع المواصفات العامة والمقاييس للحكومة الالكترونية؛
- التكامل والتوافق بين المعلومات المرتبطة بأكثر من جهة حكومية؛
- تحديد منافذ الحكومة الالكترونية Portals أي البوابة الحكومية على شبكة الانترنت؛
- الاستعانة بالقطاع الخاص لتنفيذ بعض مراحل المشروع، أو المشاركة في بعضها بما يتمتع به من إمكانية وحرية إجراءات، حيث يعد أحد الأطراف المشاركة في الحكومة الالكترونية.

4. إعادة هندسة الإجراءات الحكومية لتتناسب مع تطبيقات الحكومة_الالكترونية: إن إعادة هندسة للإجراءات الحكومية للحصول على جودة الإدارة وسرعة الإنجاز، وانخفاض التكلفة، وتحقيقا لرضا العملاء يعد أمرا ملحا إلا أن إعادة هندسة الإجراءات الحكومية لا تقتصر على تطوير وتبسيط الإجراءات وأنماط التعامل مع الجمهور، بل تمتد كذلك إلى تطوير أنماط تلك العلاقات داخل أجهزة المنظمة ذاتها، إضافة إلى تطوير تلك العلاقات بين المنظمات العامة الالكترونية بعضها البعض.**(16)**

5. استحداث إدارات جديدة: إذا كانت إعادة هندسة الإجراءات أمرا ضروريا كما سبق ذكره، فإنه سيتبع ذلك استحداث إدارات جديدة أو إلغاء أو دمج لبعض الإدارات مع بعضها بما يكفل تفعيلا نحو حكومة الكترونية تتميز بالكفاءة والفعالية وسرعة الإنجاز، بحيث أن يتم هذا التحول في إطار زمني متدرج من المراحل التطويرية.**(17)**

6. تهيئة أطر التشريعات القانونية يتوجب على الحكومات أن تقوم بمسح تشريعي شامل للقوانين والأنظمة واللوائح والتعليمات، لمعرفة مدى مواكبتها إجراءات الحكومة الإلكترونية أو تناقضها معها، بغرض تحقيق عدد من الأهداف، وهي:**(18)**

- إعطاء مشروعية للأعمال الالكترونية الخاصة بالحكومة الإلكترونية وتحديد ما هو مسموح وما هو ممنوع، والعقوبات على جرائمها؛
- إلزام الإدارات والأجهزة الحكومية بأن تضع معلوماتها وتعليماتها وإجراءاتها على الانترنت، لتحقيق سهولة الوصول إلى المعلومات، ووضع الإجراءات التي تحكم هذه العملية؛
- تحديد شروط الوصول إلى سجلات المستفيدين، وطريقة استعمالها وذلك لتحقيق الأمن الوثائقي، وخصوصية وسرعة المعلومات؛
- وضع معايير ثابتة وشفافة للإجراءات والمتطلبات الحكومية، بهدف الحد من الحاجة لتدخل المسؤولين؛
- إعطاء مشروعية لاستعمال الوثائق الالكترونية واعتمادها، كإثبات الشخصية الالكترونية، واستخدام التوقيع الالكتروني والبصمة الالكترونية...إلخ؛
- تسهيل المعاملات الالكترونية، كالسماح بالتوقيع الالكتروني، واعتماد البريد الالكتروني، وإعطاء شرعية للتجارة الالكترونية، وفي كل التعاملات الأخرى التي تتعلق بتطبيقات الحكومة الإلكترونية.

رابعا: إيجابيات وسلبيات تطبيقات الحكومة الالكترونية

تعد تطبيقات الحكومة الالكترونية مثلها مثل أي أسلوب أو ظاهرة مثيرة لها جوانبها الإيجابية كما أن لها جوانبها السلبية التي لا تؤثر على التوجه نحو تفعيل تطبيقات الحكومة الالكترونية وإحلالها بدلا من تطبيقات الحكومة التقليدية مع الأخذ في الاعتبار تفعيل الايجابيات والتغلب على السلبيات وتقدير حجم التحديات.

1. **ايجابيات تطبيق الحكومة الالكترونية:** يحقق تطبيق الحكومة الالكترونية مجموعة فوائد للجهات التي تتبنى تطبيقها في إطار خدماتها، ومن الفوائد التي لها أثر ايجابي ما يلي:**(19)**
   - توفير الوقت والجهد والمال؛
   - القضاء على التزاحم بالمصالح الحكومية؛
   - الطابع الدولي أو العالمي للخدمات الالكترونية؛
   - الشفافية في معرفة المواطن والمقيم بحقوقهم وواجباتهم؛
   - التخلص من البيروقراطية؛
   - تقليل تكاليف إدارة مؤسسات الدولة؛
   - زيادة كفاءة وفعالية الحكومة؛
2. **سلبيات تطبيق الحكومة الالكترونية:** إن مشروع الحكومة الالكترونية سيتعرض لانتقادات كثيرة، شأنه شأن النظريات والأنظمة الإدارية السابقة، وعلى الرغم من أهمية المأخذ على الحكومة الالكترونية إلا أنها لم ترق لتكون عائقا وسببا للتخلي عن خيار الأخذ بتطبيقات الحكومة الالكترونية وهي: **(20)**
   - مشكلة البطالة؛
   - مشكلة التفكك الاجتماعي؛

- ضعف النواحي الأمنية لتطبيقات الحكومة الالكترونية؛
- فقدان الخصوصية؛
- التأثير على معدلات التوظيف؛
- التكلفة الباهظة لبناء مثل هذه البيئات الالكترونية؛

كما يضاف أيضا إلى المخاطر التي قد تظهر نتيجة التحول إلى خدمات الحكومة الالكترونية تسرب المعلومات، الوصول غير المشروع، تعديل أو إلغاء المعلومات، توقيف الخدمة، ويعد ضعف الأمن في مجال العمل الكترونيا ضعفا للثقة مما يتطلب توفيرها ضمن الأنظمة الالكترونية ومستخدميها وفي البيئة الالكترونية لها أيضا، إن الضرورة تستدعي البحث عن وسائل للحماية والحفاظ على المعلومات عند تبادلها عبر الشبكات.

خامسا: تحديات أمن المعلومات في ظل تطبيق الحكومة الالكترونية

أمن المعلومات هي قضية تبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنية، هي الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن زاوية قانونية ، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت).

يعرف خبراء القانون الجرائم الإلكترونية بأنها: كل من ضبط داخل نظام المعالجة الآلية للبيانات أو جزء منه وترتب على هذه الطريقة أحد العناصر التالية: محو بيانات أو تعديل بيانات أو تعطيل تشغيل النظام.**(21)**

كما يعرف أمن المعلومات بأنه " توفير الوسائل والإجراءات التي تحقق الحماية من الأحداث المستقبلية غير المرغوب فيها، وهذه جزئيات النظام".**(22)**

وعلى غرار الجرائم التقليدية، تتميز الجرائم الالكترونية بخصائص منفردة على النحو التالي:

- الحاسب الآلي هو أداة الجريمة؛
- ترتكب هذه الجرائم عبر شبكة الانترنت؛
- مرتكب الجريمة هو الإنسان (شخص طبيعي)؛
- التخصص في استعمال الأجهزة الالكترونية وبالتالي التخصص في الجرائم الالكترونية؛
- تعتبر هذه الجريمة عابرة للحدود.

1. **أنواع الجرائم الالكترونية:** هناك عدد من الجرائم التي تتم عبر الانترنت وهي على الشكل التالي:**(23)**

أ. **صناعة نشر الفيروسات:** فقد اشتهر في السنوات الخمس الأخيرة نشر الفيروسات(*) والهدف من ذلك تغيير المعلومات في جهاز الضحية أو حذفها أو سرقتها ونقلها إلى أجهزة أخرى؛

ب. **القرصنة المعلوماتية:** ويقصد بها سرقة المعلومات من برامج وبيانات بصورة غير شرعية، وهي مخزنة في دائرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية، وتتم هذه العملية إما بالحصول على كلمة السر أو بواسطة التقاط الموجات الكهرومغناطيسية بحاسبة خاصة، ويمكن وضعها في عجلة صغيرة أو في مكان قريب من مركز إرسال هذه الموجات؛

ج. **تعطيل الأجهزة:** وقد كثرة هذه الجرائم مؤخرا حيث تتم دون عملية اختراق فعلية بل يكون بإرسال كم هائل من الرسائل بطرق فنية معينة فيؤدي ذلك إلى تعطيل الأجهزة أو الشبكات وإعاقتها عن عملها؛

د. **انتحال الشخصية:** هي جريمة الألفية الجديدة حسب تسمية المختصين في أمن المعلومات وتتمثل باستخدام شخصية أخرى بطرق غير شرعية وذلك بهدف الاستفادة من المكانة الاجتماعية لإخفاء هوية مجرم، وقد بدأ اليوم الاعتماد على توثيق شديد لهوية الشخص كالتوقيع الرقمي والتي يصعب ارتكابها؛

هـ. **المضايقة والملاحقة:** المضايقة والملاحقة تكون إما بالبريد الالكتروني أو بوسائل الحوارات الآنية وذلك بإرسال رسائل تهديد وتخويف ومضايقة، وتتميز المضايقة على الانترنت بسهولة إخفاء شخصية المجرم وقد انتشرت هذه الجريمة بالآونة الأخيرة؛

---

* – الفيروس في حقيقته هو برنامج من برامج الحاسب ولكن تم تصميمه بهدف إلحاق الضرر بنظام الحاسب، وحتى يتحقق ذلك يلزم أن تكون لهذا البرنامج القدرة على ربط نفسه بالبرامج الأخرى وكذلك القدرة على إعادة تكرار نفسه بحيث يتوالد ويتكاثر مما يتيح له فرصة الانتشار داخل جهاز الحاسب في أكثر من مكان في الذاكرة ليدمر البرامج والبيانات الموجودة في ذاكرة الجهاز. ومن أنواع الفيروسات نذكر ما يلي:

القنابل المنطقية: القنبلة المنطقية هي أحد أنواع حصان طروادة وتصمم بحيث تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين, فقد تصمم بحيث تعمل عند بلوغ عدد الموظفين في الشركة عددا معينا من الموظفين مثلا أو إذا تم رفع اسم المخرب (واضع القنبلة) من كشوف الراتب، وتؤدي القنبلة في هذه الحالة إلى تخريب بعض النظم أو إلى مسح بعض البيانات أو تعطيل النظام عن العمل.

القنابل الموقوتة: القنبلة الموقوتة هي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة أو في يوم معين كأن تحدث مثلا عندما يوافق اليوم الثالث عشر من الشهر يوم الجمعة.

باب المصيدة: يتم زرع هذا الكود Code عند تركيب النظام بحيث يعطي المخرب حرية تحديد الوقت الذي يشاء لتخريب النظام فهو يظل كامنا غير مؤذ حتى يقرر المخرب استخدامه.

الديدان: الدودة هي عبارة عن كود يسبب أذى للنظام عند استدعائه، وتتميز الدودة بقدرتها على إعادة توليد نفسها، بمعنى أن أي ملف أو جهاز متصل بالشبكة تصل إليه الدودة يتلوث، وتنتقل هذه الدودة إلى ملف آخر أو جهاز آخر في الشبكة وهكذا تنتشر الدودة وتتوالد.

و. **التغرير والاستدراج:** وغالبا ما يكون الضحية من هذا النوع هم صغار السن حيث يوهم المجرم الضحية بأنه يقيم علاقة صداقة على الانترنت والتي قد تتطور إلى لقاء مادي بين الطرفين. والمجرمون على الانترنت يتجاوزون الحدود الجغرافية؛

ز. **التشهير وتشويه السمعة:** حيث يقوم المجرم بتسوية سمعة الضحية سواء كان فردا أو جماعة أو مؤسسة تجارية وغيرها، والوسيلة الأهم لهذه الجريمة هو إنشاء موقع على الانترنت يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين؛

ح. **صناعة نشر الإباحية:** لقد وفرت الانترنت الإباحية بشتى وسائل عرضها سواء صور أو فيديو أو حوارات وهذا الجانب من أخطر الجرائم وخاصة لمجتمعات محافظة دينيا كمجتمعات العربية او الإسلامية. ولقد تم إدانة مئات المجرمين في جرائم تم فيها تغرير بالأطفال لعرض أعمال إباحية تعرض مشاهد إباحية للأطفال؛

ط. **النصب والاحتيال:** حيث أن الانترنت مجالا رحبا لعرض المنتجات التجارية فإنه أصبح بإمكان المحتالين والنصابين عرض منتجات وهمية. وميزة هذه الجريمة سهولة اختفاء وتلاشي المجرم.

2. **دوافع ارتكاب الجرائم الالكترونية:** توجد عدة دوافع لارتكاب هذه الجرائم، نذكر منها ما يلي:

أ. **الدافع السياسي والعسكري:** مما لا شك فيه أن التطور العلمي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية. فمنذ نهاية الحرب الباردة والصراع المعلوماتي بين الاتحاد السوفياتي – سابقا – والولايات المتحدة الأمريكية، ومع بروز مناطق جديدة للصراع في العالم وتغير الطبيعة المعلوماتية للأنظمة والدول، أصبح الاعتماد كليا على الحاسب الآلي وبذلك أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية؛

ب. **الدافع التجاري:** من المعروف أن الشركات التجارية الكبرى تعيش هي أيضا فيما بينها حربا مستعرة. وإن عددا من كبريات الشركات التجارية يجري عليها كثيرا من محاولات الاختراق لشبكاتها كل يوم؛

ج. **الدافع الفردي:** بدأت أولى محاولات الاختراق الفردية بين طلبة الجامعات بالولايات المتحدة الأمريكية كنوع من التباهي بالنجاح في اختراق أجهزة شخصية لأصدقائهم ومعارفهم وما لبثت أن تحولت تلك الظاهرة إلى تحدي فيما بينهم في اختراق الأنظمة بالشركات ثم بمواقع الانترنت. ولا يقتصر الدافع على الأفراد فقط بل توجد مجموعات ونقابات أشبه ما تكون بالأندية وليست بذات أهداف تجارية.

د. **الدافع الوطني:** وهو أن يقوم القرصان المعلوماتي (الهاكرز Hackers [*]) بالهجوم على مواقع معادية تختلف مع قيم وعادات مجتمع ما، ويقوم الهاكرز بتدمير أو تغيير هذه المواقع مما يؤدي إلى منعها من

---

*– أطلقت هذه الكلمة أول مرة في الستينات لتشير إلى المبرمج الذي يقوم بتصميم أسرع البرامج والخالي في ذات الوقت من المشاكل والعيوب التي تعيق البرنامج عن القيام بدوره المطلوب منه، وكان لهم بهذا الوصف مدلولات إيجابية إلى حين ظهور فئة أخرى استعملت خبرتها في مجال تصميم البرامج في السطو عنوة على البرامج ويكسرون رموزها بسبب امتلاكهم لمهارة الهاكرز الشرفاء. ليتغير اسم الفئة الثانية من الهاكرز إلى الكراكرز **Crackers** وهم الأفراد الذين يدخلون إلى

تهديد فكر وسلوك أفراد ذلك المجتمع، وكذلك يمكن أن تكون مواقع لدولة معادية وهذا ما قامت به جماعة "Umix Guard" (**)

3. **التهديدات التي تواجه الحكومة الالكترونية في ظل البيئة الرقمية:** بالنظر إلى أن نظام الحكومة الالكترونية يعتمد على قاعدة بيانات مخزنة في شبكات الحاسب الآلي أو تنساب خلالها عند التفاعل مل بين الأفراد وجهات الحكومة الالكترونية والتي يدخل فيها كافة قطاعات الدولة وغيرها، فإن نظام الحكومة الالكترونية معرض لتهديدات جسيمة تتفق وطبيعة هذا النظام المعلوماتي، وتخلص هذه المخاطر في الآتي: (25)

أ. تزوير البيانات أو المعلومات الخاصة بالحكومة الالكترونية:

ذلك أن هذه الحكومة تعتمد في نظامها وتسيير أعمالها على شبكة من الحواسيب المرتبطة فيما بينها – انترانت – وتتصل لاحقا بشبكة المعلومات العالمية – الانترنت

وبالطبع يمكن للقراصنة الحصول على البيانات أو المعلومات الخاصة بعمل الحكومة الالكترونية في صورة أوراق مطبوعة من أية طريقة متصلة بالحاسب الآلي – طابعة، أو عن طريق نسخها على شريط مرن، أو قرص مدمج ...إلخ-. وبالتالي يمكن استخدام واستكمال المعلومات المزورة بعد نقلها من الوسيط الالكتروني إلى الوسيط الورقي.

ب.جرائم الأموال في نطاق التجارة الالكترونية:

وهي من المخاطر الجسيمة التي تواجه هذه الحكومة، ومن الجرائم التي يمكن أن تتم في هذا النطاق هي:

- سرقة المعلومات من طرف القراصنة والتجسس على حسابات العملاء في البنوك؛
- العبث بالبطاقات الممغنطة واستعمالها في التلاعب بحسابات العملاء أو تحويل مبالغ من أموالهم إلى حسابات القراصنة أنفسهم؛
- إتلاف الشبكات أو الأجهزة الالكترونية إما بطريقة مادية كسكب سوائل باردة أو ساخنة على الدعامات الالكترونية المخزن عليها البيانات أو المعلومات، أو من خلال زرع فيروسات (القنابل المنطقية، القنابل الموقوتة، باب المصيدة، الدودة الالكترونية، أحصنة طروادة) تعمل على التعطيل الكلي أو الجزئي لعمل الشبكات أو لتشويه المعلومات التي تقدمها الحكومة الالكترونية للأفراد.

ج.مسؤولية مقدمي الخدمات الوسيطية في نطاق شبكة الانترنت والانترانت: يعتبر مقدمي الخدمات الوسيطية الأشخاص الذين يساعدون الأفراد في الوصول إلى شبكة الانترنت للاستفادة من خدمات

الأنظمة بقصد التطفل أو التخريب وأطلق عليم إسم الكراكرز لقيامهم بأعمال التخريب والكسر والإضرار. وهي كلمة مأخوذة من الفعل Crack بالإنجليزية وتعني الكسر أو التحطيم وهي الصفة التي يتميزون بها.

** – "Umix Guard": هي جماعة قراصنة عرب قاموا بالهجوم على مواقع إسرائيلية وأمريكية وبريطانية ودمروها وذلك بسبب استمرار الاعتداء على الشعب الفلسطيني والشعب العراقي.

الحكومة الالكترونية وهم: متعهد الوصول، متعهد الإيواء، المنتج، ناقل المعلومات، متعهد الخدمات، مورد المعلومات، مؤلف الرسالة.

د. جرائم الاعتداء على بيانات الحكومة الالكترونية: تقوم هذه الجريمة في حق القراصنة الذين يخترقون المواقع التي تؤدى من خلالها خدمات الحكومة الالكترونية إي تلك الأنظمة المخصصة لمعالجة البيانات، وذلك بإدخال بيانات خاطئة لتشويه صورة المعلومات المقدمة من طرف الحكومة، أو تعديل بيانات مخزنة من قبل، أو إزالة جزء أو كل البيانات المخزنة في مختلف الوسائط الالكترونية.

خامسا: الإجراءات والتدابير الواجب اتخاذها لحماية المعلومات الحكومية

هناك مجموعة من الإجراءات الإدارية والفنية التي يمكن استعمالها في هذا الصدد لتحقيق أمن المعلومات، وهي كالآتي:

1. **الإجراءات الإدارية لأمن المعلومات:** على الحكومات التي تتبنى تقديم خدماتها الكترونية للمواطنين القيام بعدة مهام تجاه أمن المعلومات كالرقابة والإشراف على أمن المعلومات، وسوف يتم استعراض مهام رئيسية يجب عليها القيام بها، وهي كالتالي:

أ. **توفير أمن الأجهزة:** لتأمين الأجهزة لابد من تأمين المبنى كعدم السماح لغير المصرح لهم بالدخول إلى غرفة الحاسب الآلي، ومخزن وسائط التخزين. ويفضل استخدام التكنولوجيا الحديثة للدخول على الأنظمة (بصمة الأصبع، بصمة العين، البطاقة الممغنطة ... إلخ).(26)

ب. **توفير أمن البيانات:** يتوجب على الإدارة توزيع الصلاحيات والمسؤوليات حسب الهيكل التنظيمي بما يضمن رفع المستوى الأمني، وتقليص الجرائم، ووضع آلية يتم تنفيذها للقيام بالنسخ الاحتياطي وتأمين وسائط الحفظ الخارجية بما يكفل أمنها وتحديثها، ويجب صياغة الضوابط المنظمة لعمليات التشغيل، ولمبرمجي قواعد البيانات ومدرائها، ولإدارة الشبكات وخطوط الاتصال، ولعمليات الإدخال والإخراج، والضوابط الأمنية لبناء وتشغيل البرامج التطبيقية.

ج.**توفير أمن الأفراد:** عندما تريد الإدارة حماية معلوماتها عليها إتباع الإجراءات الإدارية في مجال أمن الأفراد على النحو التالي: (27)

- منع التوظيف المؤقت نهائيا، ومراعاة إجراءات إنهاء خدمة الموظف بطلب تسليم كل ما كان بحوزته كالمفاتيح والبطاقات الممغنطة، وتغيير كلمة المرور قبل مغادرته؛
- متابعة العاملين ونقلهم إجباريا بين الأقسام المختلفة في الإدارة، وملاحظة الذين لا يطلبون إجازة بإجبارهم على الإجازة ومراقبة النظام بعد ذلك للتأكد من عدم وجود خلل كانوا يتفادونه بوجودهم؛
- عقد ندوات ومؤتمرات ومحاضرات بشكل دوري في مجال أمن المعلومات، وعرض النشرات الداخلية وتعليمات الإدارة التي تتضمن إطلاع الأفراد على المعلومات المهمة في مجال الأمن، لإلزام العاملين بالنظم الإدارية المحددة؛

-دفع العاملين لحضور المعارض العالمية للأجهزة والبرامج، وإرسالهم إلى الدورات المتخصصة بأمن المعلومات، ليكون لديهم خلفية قوية بما يكفل تحقيق أمن المعلومات؛

- منح الحوافز وربط الترقية والدورات بمدى التقيد بأمن المعلومات.

د. **توفير قسم متخصص بأمن المعلومات:** تقوم المؤسسة الكبيرة بتعيين مدير أمن نظم المعلومات يرتبط بالإدارة العليا مباشرة لأهمية التقارير التي يعدها. ويرأس مدير الأمن قسما مستقلا من المتخصصين في مجال أمن المعلومات ومن ذوي الخبرة الفنية والأمنية في معالجة البيانات والبرمجة حسب نظم التشغيل ولغات البرمجة وقواعد البيانات المستخدمة في المؤسسة، ومدربين على التنسيق الأمني ولديهم المقدرة الكافية للتعامل مع جرائم نظم المعلومات والحالات الطارئة.

2. **الإجراءات الفنية لأمن المعلومات:** هناك مجموعة من الإجراءات الفنية التي ينبغي على المؤسسات توفيرها لحماية معلوماتها، نذكر منها:

أ. **توفير الحماية الإلكترونية:** تخضع الحماية الإلكترونية للإعدادات الخاصة بالحاسب الآلي، والأجهزة الملحقة به، ويمكن بيانها على النحو التالي:**(28)**

- حذف الملفات غير الهامة ولو كانت المعلومات التي تحويها ضئيلة وعديمة الفائدة، والتأكد من عدم إبقائها في سلة المحذوفات Recycle Bin؛
- الكشف على الحاسب الآلي بعد الغياب عن طريق المستكشف، وتركيب برامج تمنع مسح المعلومات من المستكشف، أو استخدام برامج تحتفظ بالعمليات التي تم إجراؤها؛
- استغلال برنامج Win Zip كنظام حماية مرور Password لعدد كثير من الملفات المراد حمايتها. وضغط الملفات وحمايتها بكلمة مرور؛
- عدم استخدام الأسماء التي تجذب انتباه مخترقي أجهزة الحاسب الآلي، فمن الأسلم إعطاء أسماء لا تلفت الانتباه كالحفظ باسم Calendar.xls بدلا من Budget.xls؛
- التأكد من عدم وجود برامج تجسس من فئة أحصنة طروادة في حالة الارتباط بشبكات في الحاسب الآلي؛
- عند استخدام الإنترنت يجب عدم حفظ كلمة المرور الخاصة بالمستخدم وقت الدخول للإنترنت، وغلق المتصفح حال الابتعاد عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح، وعدم استخدام خاصية تذكر اسم المستخدم وكلمة المرور؛
- عند استخدام البريد الإلكتروني يجب عدم فتح الملفات المرفقة إلا بعد التأكد منها؛
- من الضروري تركيب البرامج المضادة للفيروسات على الجهاز وتشغيلها طوال فترة استخدام الجهاز، ومن الضروري أيضا تحديث برامج مستكشف الفيروسات بصورة دورية.

ب. **تأمين جميع مكونات الشبكة:** في حالة استخدام الشبكات، فإن الحماية في هذه الحالة تعتمد على التحقق من الشخصية، للدخول إلى الشبكة، وعلى وسائل أمن الشبكة والتي يجب فحصها بالكامل وتقييم إمكانية اختراق نظام الحماية وتحديد تلك المخاطر المتعلقة بالتصميم والإدارة.

ولحماية الشبكات يلزم استخدام برامج حماية، كبرنامج Look Down 2000 الذي تنتجه Harbor Telco Security corp. وهو من أشهر البرامج المستخدمة للحماية، ويعمل كجدار ناري يقوم بفحص الجهاز عند بدء التشغيل للبحث عن أحصنة طروادة ومن ثم إلغاء الملف مباشرة مع ترك رسالة تعلم المستخدم بذلك كما يمنع كذلك المخترقين ويسجل محاولات الدخول في تقرير مختصر يشمل وقت الدخول كما أنه يعطي معلومات عن جهة الاتصال، من عيوبه أنها تنطلق صفارة التحذير عند كل تغيير يحذف بملف Registry وعند استقبال Cookies غير مضرة للمواقع التي تتم زيارتها.

ج. **استخدام التشفير:** إرسال البيانات عبر الشبكة يجعل من السهل التصنت عليها، والطريقة الوحيدة لمنع هذا التصنت هي استخدام التشفير. يعرف التشفير Encryption بأنه عملية تحويل المعلومات إلى شفرات غير مفهومة تبدو غير ذات معنى لمنع الأشخاص غير المرخص لهم من الإطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة. وتشكل الإنترنت الوسط الأضخم لنقل المعلومات الحساسة، وقصد الحفاظ على سلامتها وأمنها فلابد من تشفيرها.

ويمكن استخدام ثلاث طرق للتشفير كالتالي:**(29)**

- **الشهادات الرقمية:** تصدر الشهادات الرقمية Digital Certificates عن الجهات المانحة الموثوق بها التي توقع عليها وتستخدم هذه الشهادات للتحقق من موثوقية المفاتيح العامة التي أصدرت؛
- **البصمة الإلكترونية:** وهي بصمة رقمية يتم اشتقاقها وفقا لخوارزميات معينة تدعى دوال أو اقتران التمويه. وتدعى البيانات الناتجة البصمة الإلكترونية للرسالة Message Digest، وتستطيع هذه البصمة تمييز الرسالة الأصلية والتعرف عليها بدقة، حتى أي تغيير بالرسالة سيفضي إلى بصمة مختلفة؛
- **التوقيع الرقمي:** يستخدم التوقيع الرقمي Digital Signature للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل ويمكن للمرسل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونيا. أما في طرف المستقبل فيتم التحقق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب. وباستخدام التوقيع الرقمي يتم تأمين سلامة الرسالة والتحقق من صحتها، ومن فوائد هذا التوقيع أنه يمنع المرسل من التنكر للمعلومات التي أرسلها.

د-استخدام كلمات المرور: يتطلب أمان نظم المعلومات استخدام كلمات مرور معقدة لتسجيل الدخول إلى شبكة أو حاسب الآلي، ويمكن أن تكون كلمة المرور الارتباط الأضعف في النظام، وتكون كلمات المرور القوية هامة على اعتبار أن أدوات اكتشاف كلمات المرور مستمرة في التحسن وعلى اعتبار أن أجهزة الحاسب الآلي المستخدمة لاكتشافها أصبحت أكثر فعالية من ذي قبل، وأصبح بالإمكان الآن كسر كلمات مرور الشبكة في ساعات بعد أن كان ذلك يستغرق أسابيع ولجعل كلمات المرور قوية يجب أن تكون ذات المواصفات التالية:**(30)**

- أن يكون طولها سبعة (07) أحرف على الأقل فإن أكثر كلمات المرور أمانا تكون بطول سبعة (07) أحرف إلى خمسة عشر (15) حرفا.
- أن تحتوي على أحرف من مجموعة الأحرف (A,B,C…a,b,c) ومجموعة الأرقام (0،1، 2،…، 9) ومجموعة رموز ({} + − " & > () / * . [] 14 \ | ~ ْ ؟ ....).
- أن يكون فيها على الأقل حرف رمز واحد في الموضع الثاني حتى السادس.
- استخدم كلمات مرور مختلفة لتسجيل الدخول إلى شبكة الاتصال وإلى حاسب المسؤول الحاسب الآلي الخاص بك.

د. **استخدام الجدار الناري_Firewall:** يعرف الجدار الناري(*) بأنه أداة ترشح أو تحجز البيانات بين الشبكة الداخلية والشبكة الخارجية والتي يخشى منها، والهدف هو حجز كل ما هو غير مرغوب فيه من خارج البيئة المحمية. ويستطيع المستخدم من خلال الجدار الناري الخروج إلى عالم الانترنت ولكن لا يستطيع من في الخارج الدخول إلى الجهاز من خلاله. وهناك عدة أنواع للجدار الناري، نذكر أهمها فيما يلي:

- **الموجه الحاجب Screening Router:** هو أبسط أنواع حوائط النار وفي بعض المواقف يكون أكثر فاعلية ومهمته هي استقبال حزم الرسائل Packets ويقوم بتمريرها إلى أحد المنافذ التي تتولى بدورها إيصال كل حزمة إلى جهتها، وهذا النمط من الجدار الناري يستخدم للحاسبات المضيفة Host والتي ليس من المستحب توصيلها بالشبكات الكبيرة Wan ولكنها تتصل من خلال موجه Router. ويعمل الموجه في كلا الاتجاهين فيستقبل الحزم الواردة ويرسلها إلى الداخل كما يرسل الحزم الصادرة من الشبكة الداخلية إلى الخارج؛
- **الوسيط Proxy:** يمتاز الوسيط أو البروكسي عن الموجه الحاجب بأنه لا يقرأ فقط مقدمة البيانات الخارجية بل يستطيع أن يفهم ويفسر البروتوكول المستخدم وذلك بهدف التصرفات المسموح بها من خلال حائط النار بناء على بعض محددات البروتوكول. ويمكن القول بأن الوسيط هو كالعملة ذو وجهين فالذي من الداخل يراه وكأنه من الخارج والذي من الخارج يراه يواجه الجهة الخارجية تماما كما يجب أن يفعل المتصل الداخلي ويبدو لمن في الخارج بأنه هو الذي يستقبل. ويمكن للبروكسي أن يسمح لمن يريد الإطلاع على أسعار المؤسسة أو الشركة ولا يسمح لهم بتغيير وتعديل الأسعار وكذلك بيانات المواطنين في المؤسسات الحكومية أو كذلك درجات الطلبة في المدارس والجامعات؛
- **الحارس Guard:** الحارس يشبه البروكسي في عمله إلا أنه على درجة كبيرة من التعقيد فهو يعتمد في قراره على قراءته وتفسيره للمعلومات إما يسمح لها أو يمنعها من الوصول. وبناءا على المعلومات المتاحة

---

* – سمي الجدار الناري بهذا الاسم نسبة لجدران الحصون التي كانت تشيد في القديم لحماية القلاع، وتسمى هذه الجدران بالجدران النارية بحيث أن رماة الدفاع من الداخل يستطيعون أن يطلقوا النار إلى الخارج من فتحات بجدران الحصن وهذه الفتحات لا تمكن الغزاة من إرسال نيرانهم إلى الداخل.

يقرر ماذا يعمل نيابة عن المستفيد، ويستخدم الحارس في أمور لحصر عمليات الاتصال، مثلا المدارس التي تسمح لطلابها بالدخول على الانترنت فلا تسمح لهم بإرسال إلا عدد من الرسائل أو تمنع ميزة تنزيل الرسوم المعقدة والرسوم المتحركة والقطع الموسيقية.

خاتمة

يتسم الإجرام الالكتروني بالذكاء الخارق مقارنة بالإجرام التقليدي الذي يتسم بالعنف، لهذا يطلق عليه بإجرام الأذكياء، لأنه يعتمد على وسائل تكنولوجية متطورة في تدمير أو اختراق المواقع الحكومية أو قرصنة المعلومات الخاصة بالأفراد والاعتداء على خصوصياتهم. ولا يستخدم هذه البرامج إلا مجرما يتسم بالذكاء الحاد، وباعتباره كائن اجتماعي، فقد يلجأ إلى ارتكاب هذه الجرائم بدافع اللهو والمباهاة بين زملائه، أو لتحقيق نفع مادي كالاستيلاء على أموال الغير، الانخراط في عصابة قراصنة لتدمير مواقع حكومة معينة ...الخ.

وبالتالي، نستطيع أن نؤكد أن نجاح الحكومة الالكترونية يعتمد كثيرا على نجاح نظام الحماية الذي تعتمده هذه الحكومة والذي يجب أن تكون حماية مدنية، جنائية ومعلوماتية على نحو ذا فاعلية.

وتتحقق الحماية المعلوماتية عن طريق تطوير الأبحاث العلمية للنظم الأمنية الالكترونية التي تعمل بها هذه الحكومات لكي تؤمن بياناتها ومعلوماتها من القرصنة وإساءة استعمالها، واكتشاف حالات القرصنة إن حدث ذلك.

أما بالنسبة للحماية المدنية والجنائية فتكون بسن قوانين تحمي حقوق وخصوصيات المواطنين في ظل تطبيق الحكومة الالكترونية، وتعاقب كل المجرمين الذين يتجرؤون على التجسس والتلاعب وكشف هذه البيانات الخاصة بالأفراد.

قائمة المراجع

1. شاهر أحمد نصر، عصر المعلوماتية، مجلة الحوار المتمدن (مجلة إلكترونية)، العدد 673، نشرت بتاريخ 2003/12/11 على الموقع: http://www.rezgar.com/help.htm
2. د. العلاق أبو سديرة، الخدمات الالكترونية بين النظرية والتطبيق، دار الشرق للنشر والتوزيع، الأردن، 2004، ص 02.
3. د. العبود فهد بن ناصر بن دهام، الحكومة الالكترونية بين التخطيط والتنفيذ، مكتبة الملك فهد الوطنية، الرياض، المملكة العربية السعودية (دون ذكر سنة النشر)، ص 26
4. Zhou Hongren, Global Perspectives on E. government, The united nations department of economic and social affairs, 2002, P 04
5. د. العلاق أبو سديرة، مرجع سبق ذكره، ص 03
6. د. حجازي عبد الفتاح بيومي، النظام القانوني لحماية الحكومة الالكترونية، ط 01، دار الفكر الجامعي، الإسكندرية، جمهورية مصر العربية، 2003، ص 99.

7. الحمادي بسام، مفاهيم ومتطلبات الحكومة الالكترونية، مداخلة ضمن فعاليات الملتقى الوطني حول " الحكومة الالكترونية: الواقع والتطلعات "، معهد الإدارة العامة، الرياض، المملكة العربية السعودية، يومي 12 و13 جانفي 2002، ص 03.

8. JAMES, A. Senn, Information System in Management, 04 Edition, Belmont, California, Wadsworth Publishing Co, USA, 1992, P 19

9. د. غراب كامل، حجازي فادية، نظم المعلومات الإدارية، المنتزه: مكتبة ومطبعة الإشعاع الفنية، 1999، ص 119.

10. إسماعيل الغريب زاهر، شبكة الإنترنت، المركز العربي للبحوث التربوية لدول الخليج، الموسم الثقافي التربوي، الدورة 75، 2000، ص 17.

11. د. شفا عمري معتصم، تعرف على الإنترنت، دار الرضا للنشر، دمشق، سوريا، 2000، ص 21.

12. بختي إبراهيم، دور الإنترنيت وتطبيقاته في المؤسسة، أطروحة دكتوراه دولة في العلوم الاقتصادية، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر، الجزائر، 2002، ص 51.

13. Itep, B, Available,http://www.Itep.Co.Ae/Itportal/Arabic/Content/ Educationalcenter/Internetconcepts/Intranet.Asp, 23/10/2002

14. Itep, C, Available,http://www.Itep.Co.Ae/Itportal/Arabic/Content /Educationalcenter/ Internetconcepts/Extranet.Asp, 24/10/2002

15. الحمادي بسام، مرجع سبق ذكره، ص 04.

16. *د. الباز علي*، الحكومة الالكترونية والإدارة المحلية، مداخلة ضمن فعاليات المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الالكترونية، دبي، دولة الإمارات العربية المتحدة، 2003، ص 10.

17. العمري سعيد بن معلا، المتطلبات الإدارية والأمنية لتطبيق الإدارة الالكترونية، رسالة ماجستير (غير منشورة)، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2003، ص 20.

18. الروابدة عبد الرؤوف، الحكومة الالكترونية والتشريع، مداخلة ضمن فعاليات مؤتمر " الحكومة الالكترونية: الواقع والتحديات " مسقط، سلطنة عمان، 2003، ص 04.

19. الحسن نوبي، منظومة الحكومة الالكترونية، مداخلة ضمن فعاليات مؤتمر " الحكومة الالكترونية: الواقع والتحديات " مسقط، سلطنة عمان، 2003، ص 10.

20. نفس المرجع، ص 11.

21. د. مكاوي محمد محمود ، البيئة الرقمية بين سلبيات الواقع وآمال المستقبل، مجلة Cybrarians journal (مجلة إلكترونية)، عدد 3، سبتمبر 2004، متاحة على الموقع: http://www.cybrarians.info/journal/no9/info-secuirty.htm

22. د. ديريه سعيد، أمن المعلومات، 2004، متاح على الموقع: http://www.saidder.jeeran.com/amn.htm

23. د. الهاجري إياس بن سمير ، أمن المعلومات على شبكة الإنترنت، مدينة الملك عبد العزيز، الرياض، المملكة العربية السعودية، 2002، ص ص 07 – 11

24. د.عبد الفتاح البيومي حجازي، الحكومة الالكترونية بين الواقع والطموح، دار الفكر الجامعي، الاسكندرية، مصر، 2008، ص 208.

25. *د. داود حسن، الحاسب وأمن المعلومات، معهد الإدارة، الرياض، المملكة العربية السعودية، 2000، ص 226*

26. *د. الشدي طارق عبد الله، الآلية البناء الأمني لنظم المعلومات، دار الوطن للطباعة والنشر، الرياض، المملكة العربية السعودية، 2000، ص 182.*

- *أمن الإنترنيت، مجلة الأمن الإلكترونية، متوفر على الموقع* *http://Safola.com/Security.chtml* *بتاريخ 2001/12/10.*
- *BARMAN S, Writing Information Security Policies, New Riders Publishing, Available* *http://Safari.informit.com* *November 2001*
- *NOR 2000, Available: http://www.Nor 2000.com/Netwrk.html. 19/06/2002*