الحكومة الإلكترونية ومساعي إستتباب الأمن المعلوماتي: الإمارات العربية المتحدة نموذجا

E-Government and efforts to establish information security : United Arab Emirates as a model

ب. د شعيب قماز
جامعة باتنة - 1 -
chouaibguemazsp@gmail.com

ب. د عبد العزيز صحراوي
جامعة المسيلة
sahraoui_785@hotmail.com

تاريخ الإيداع:2018/12/07	تاريخ المراجعة:2019/01/15	تاريخ القبول:2019/01/21

الملخص:

في إطار مسايرة التطورات الحاصلة في المجال الإلكتروني، تعمل هذه الورقة البحثية على تمحيص سبل إحداث نقلة نوعية في الخدمات الحكومية بحيث يتم هندرة الحكومة إلكترونيا عبر اعتماد تكنلوجيا المعلومات لترقية أساليب التعامل مع المواطنين والمؤسسات، مع الحرص على إبراز استراتيجيات مواجهة التهديدات الأمنية الرقمية من خلال توليفة أمننة المعلومات، و إن البحث عن تجربة ناجعة في هذا المجال أحالنا إلى دراسة الحكومة الإلكترونية والأمن المعلوماتي في الإمارات العربية المتحدة.

الكلمات المفتاحية: الحكومة الإلكترونية، الأمن المعلوماتي، الإمارات العربية المتحدة .

Abstract:

In the context of developments in the electronic field, this paper examines the ways to make a qualitative shift in government services so that the government will be electronically managed through the adoption of information technology to upgrade the methods of dealing with citizens and institutions, while highlighting the strategies to address digital security threats through Information securitization, the search for an effective experience in this area we referred to the study of E-government and information security in the United Arab Emirates.

Keywords: E-Government, Information Security, United Arab Emirates.

مقدمة:

مع مطلع الألفية الثالثة شهد العالم طفرة إلكترونية ومعلوماتية أدت إلى تغييرات كثيرة على جميع الأصعدة والميادين، و كذلك أحدثت تطورات كبيرة في نمط الحياة البشرية، إذ برزة توليفة من المفاهيم والمقاربات الجديدة غيرت ما كان متعارف عليه من قبل، ومن هذا المنطلق دخلت الأساليب الإلكترونية إلى الأعمال الحكومية وأحدثت تغييرا جذريا في ثقافة تنفيذ العمليات الحكومية المتساندة وقائيا بمتطلبات الأمن المعلوماتي من أجل تقويض المخاطر السيبرانية.

والإمارات العربية المتحدة كغيرها من الدول تأثرت بهذه التغييرات، فعمدت على مسايرة مختف التطورات التي أفرزتها تكنولوجيا المعلومات والإتصال وربطها بمجال الحكومة الإلكترونية و ذلك من خلال اتخاذ حزمة من الإجراءات التقنية والإلكترونية من أجل توسيع نطاق الحكومة الإلكترونية فضلا على السعي إلى تقويض التهديدات الأمنية السيبرانية لها من خلال بناء جدار الأمن المعلوماتي... وفق لما سبق تطرح هذه الورقة البحثية الإشكالية التالية:

- إلى أي مدى يمكن تفعيل حكومة إلكترونية متساندة تواسقيا مع متطلبات الأمن المعلوماتي من خلال التركيز على تجربة الإمارات العربية المتحدة نموذجا؟

ويتفرع عن هذا التساؤل مجموعة من الأسئلة الفرعية:

- ما هو مفهوم الحكومة الالكترونية و الأمن المعلوماتي؟
- كيف يمكن هندرة الحكومة إلكترونيا و أمننتها معلوماتيا؟
- ماهي خطة دولة الإمارات العربية المتحدة في مجال أمن المعلومات الالكترونية ؟

و من أجل الإجابة على هذه الإشكالية تتطب الضرورة المنهجية التطرق إلى المحاور التالية:

I. **تمحيص الخطابات المعرفية بشأن الحكومة الإلكترونية و الأمن المعلوماتي.**
II. **هندرة الحكومة إلكترونيا وأمننة المعلومات ممارساتيا...المساعي والمعيقات.**
III. **تجربة الحكومة الإلكترونية في الإمارات العربية المتحدة .**

I.تمحيص الخطابات المعرفية بشأن الحكومة الإلكترونية و الأمن المعلوماتي.

أولا: الإطار المفاهيمي للحكومة الإلكترونية

من المؤكد أن تطبيق الحكومة الإلكترونية يقضي على الحواجز المكانية والزمانية التي تحد من التفاعل بين الحكومة والمواطن، وتقدم شكلاً جديدًا للخدمات الحكومية يتصف بالسهولة والمرونة والشفافية ، لذا فمن الضروري استعراض وجهات النظر المختلفة التي تناولت مفاهيم الحكومة الإلكترونية، والأطراف المشاركة في بناء الحكومة الإلكترونية وأهم مميزاتها.

1- تعريف الحكومة الإلكترونية:

الحكومة الإلكترونية كما يرى الخبراء أنها ترتبط بتعظيم استخدام التكنولوجيا الحديثة لتحرير حركة المعلومات والخدمات من أجل التغلب على القيود والعوائق المادية الموجودة في الأوراق والأنظمة التقليدية.[1]

وتعرف المنظمة العربية للتنمية الادارية الحكومة الإلكترونية بأنها: "عملية استخدام المعلومات عن طريق الانترنت والاتصال عبر الهاتف الجوال لتغيير وتحويل العلاقات مع المواطنين ورجال الأعمال ومختلف المؤسسات الحكومية،وقد قامت المنظمة في هذا الإطار بتصنيف الحكومة الإلكترونية إلى صنفين: التصنيف التفاعلي، التصنيف على أساس الخدمة".[2]

كما قدم البنك الدولي (2005) مفهوما أشمل للحكومة الإلكترونية E-government بأنها: "عملية استخدام المؤسسات الحكومية لتكنولوجيا المعلومات (مثل: شبكات المعلومات العريضة، وشبكة الإنترنت، وأساليب الاتصال عبر الهاتف المحمول) والتي لديها القدرة على تغيير وتحويل العلاقات مع المواطنين ورجال الأعمال ومختلف المؤسسات الحكومية. وهذه التكنولوجيا يمكنها أن تخدم عددًا كبيرًا من الأهداف مثل: تقديم خدمات أفضل للمواطنين، وتحسين التعامل والتفاعل مع رجال الأعمال ومجتمع الصناعة، وتمكين المواطنين من الوصول للمعلومات مما يوفر مزيدًا من الشفافية وإدارة أكثر كفاءة للمؤسسات الحكومية، كما أن نتائج هذه التطبيقات يمكن أن تؤدي إلى تحجيم الفساد، وزيادة الشفافية، وتعظيم العائد ككل، وتخفيض النفقات، وزيادة قناعة المواطن بدور المؤسسة الحكومية في حياته".[3]

وقد ركز هذا التعريف على المزايا التي يحققها تطبيق الحكومة الإلكترونية للمنظمات الحكومية وللجمهور المتعامل معها من المواطنين نتيجة للاستخدام الواسع لتكنولوجيا المعلومات والاتصالات والتي تزيد من كفاءة وفاعلية المنظمات الحكومية دون أن يتطرق إلى الأهداف السياسية للحكومة الإلكترونية.

---

1 دليلة العوي، مجتمع المعلومات في الجزائر-واقع الفجوة الرقمية-، مذكرة ماجستير غير منشورة،كلية العلوم السياسية والإعلام،جامعة الجزائر، 2007، ص 112.

2 تغريد أبو سليم، دراسة تحليلية لإبعاد التحول نحو الحكومة الإلكترونية في الدول العربية، رسالة ماجستير غير منشورة، كلية العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر،2005، ص21.

3 محمد صادق إسماعيل، الحكومة الإلكترونية وتطبقاتها في الدول العربية، القاهرة: العربي للنشر و التوزيع،2010، ص ص 78-79.

كما عرف ألكويست و آخرون Ahlekwest & et al (2004) الحكومة الإلكترونية بأنها: "نموذج أعمال مبتكر مستند للتقنيات خصوصا تقنيات الخدمة الذاتية اللاسلكية وأساليب التفاعل والشفافية والمصداقية والثقة المتبادلة مكرس وموجه بالمواطنين ومنظمات الأعمال الربحية منها وغير الربحية، ويستهدف بالدرجة الأولى تقديم خدمات عامة بأسلوب مميز يأخذ في الاعتبار خصوصيات السوق المستهدفة ويحقق لأطراف التبادل والتعامل الأهداف المشتركة بكفاءة وفعالية"[1].

ينظر هذا التعريف إلى الحكومة الإلكترونية من وجهة النظر التسويقية والتي تغير من شكل العلاقة بين الحكومة والمواطن ليتحول المواطن إلى عميل، يتم تصميم الخدمات الحكومية الإلكترونية وفقا لرغباته واحتياجاته بما يحقق درجة عالية من التفاعل والثقة بين الحكومة والمواطن.

من التعاريف السابقة للحكومة الإلكترونية يتضح أن الحكومة الإلكترونية لا تقتصر فقط على استخدام تكنولوجيا المعلومات والاتصالات لتقديم الخدمات الحكومية للمواطنين عبر شبكة الإنترنت وإنما هي فكر متطور يعيد صياغة الحكومات بشكل جديد له أبعاده السياسية والإدارية والاجتماعية.

2- المشاركون في الحكومة الالكترونية:

يعرف المشاركون في الحكومة الألكترونية بـ:

- فريق الادارة Team/Project Manager: وهم من يقومون ببناء وتصميم الحكومة الإلكترونية.
- المشغلون Operators: وهم من يقومون بالعمليات والإجراءات التي تشغل الحكومة الإلكترونية.
- الزبائن Clients: وهم المتلقون الإخيرون لمخرجات الحكومة الإلكترونية.
- الأبطال Champions: وهم الأشخاص الذين يحولون المشروع إلى التطبيق بالطريقة الصحيحة.
- الممولون Sponsors: وهم الأشخاص أو المجموعة الذين يمولون الحكومة الإلكترونية.
- Other stockholders: مجموعة أو شخص له تأثير مباشر على الحكومة الإلكترونية أو يتأثر بها.[2]

3- مزايا الحكومة الإلكترونية:

تحقق الحكومة الإلكترونية العديد من المزايا للمواطنين والإدارات الحكومية المحلية ولكافة الأطراف الأخرى التي تتعامل معها نوجزها فيما يلي[3]:

- تقليص النفقات، حيث إن استخدام الأساليب التكنولوجية يؤدي إلى تقليل عدد القائمين على حفظ ونسخ ونقل وتوزيع الأعمال الورقية الخاصة بالتعاملات، ويقلل الجهد والموارد المخصصة لكل خطوة من خطوات الإجراءات الحكومية، مما يؤدي إلى تقليص جزء كبير من تكلفة التعاملات الحكومية التقليدية.
- تحقيق الشفافية الحكومية من خلال إتاحة المعلومات عن كافة الأنشطة الحكومية وإتاحة القوانين واللوائح

1 بشير عباس العلاق، الخدمات الإلكترونية بين النظرية والتطبيق، الأردن، المنظمة العربية للتنمية الإدارية، 2004، ص 257.
2 تغريد أبو سليم،مرجع سبق ذكره،ص36.
3 رأفت رضوان، عالم التجارة الإلكترونية، القاهرة، المنظمة العربية للتنمية الإدارية، 1999، ص148.

الحكومية على شبكة الإنترنت، كما يتم إتاحة المعلومات عن المشتريات الحكومية على شبكة الإنترنت للمساواة بين الموردين.

- زيادة جودة الخدمات الحكوميةعبر شبكة الإنترنت، وهو ما يتيح للمواطنين المزايا التالية[1]:

أ- الحصول على الخدمات الحكومية في أي وقت على مدار أربع وعشرين ساعة يوميا وفي أي مكان وبأقل جهد.

ب- السرعة الفائقة للتعاملات الحكومية التي تتم إلكترونيا إذا ما قورنت بالتعامل الورقي بالأساليب التقليدية.

ت- إن تقديم الخدمات الحكومية إلكترونيا يقضي على تأثير الفروق الفردية في أداء العاملين والتي قد تؤثر سلبا على جودة الخدمات الحكومية.

وكذلك من مزاياها:

أ- إدارة علاقات أكفأ مع المواطنين، فالمواطن بالنسبة للحكومة الإلكترونية هو بمثابة العميل (الزبون) الذي تدرس احتياجاته وتلبي طلباته، وقد سهلت الإنترنت ما يسمى بالذاكرة المجتمعية للعلاقات مع المواطنين، وهي عبارة عن معلومات هائلة يتم استرجاعها بسرعة فائقة .

ب-تحقيق الكفاءة في الأداء الحكومي من خلال خفض تكاليف الأعمال الحكومية بالتحول من الأسلوب الورقي إلى الأساليب الإلكترونية في أداء الأعمال.

ت-التكامل بين الإدارات الحكومية من خلال الاتصالات الفائقة التي تربط الإدارات الحكومية بعضها البعض بحيث يتعامل المواطن معها ككيان واحد، مما يقلل الوقت والجهد ويقضي على التضارب في الاختصاصات بين الجهات الحكومية عند التعامل مع المواطنين.

ث-الحد من ظاهرة الفساد الإداري من خلال نشر كافة البيانات والمعلومات المتعلقة بالأداء الحكومي على شبكة الإنترنت وإتاحتها للمواطنين، وإعطائهم حق المساءلة عن القرارات التي يتخذها المسئولون، وبذلك تتحقق الرقابة الشعبية على الممارسات التي تمس الصالح العام.[2]

ثانيا: مفهوم أمن المعلومات.

أولا : تعريف أمن المعلومات

لقد أورد فايز جمعة تعريف أمن المعلومات نقلا عن الكيلاني وآخرون حيث عرفوا أمن المعلومات على أنها:" هي حماية التجهيزات الحاسوبية وغير الحاسوبية والتسهيلات والبيانات والمعلومات من الأخطار، فهي مجموعة الإجراءات والتدابير الوقائية التي تستخدمها المنظمة للمحافظة على المعلومات وسريتها سواء من الأخطار الداخلية أوالخارجية، كالحفاظ عليها من السرقة والتلاعب بها والاختراق أو الإتلاف غير المشروع، سواء قبل أو خلال أو بعد

1 ريتشارد هيكس، الحكومة الإلكترونية من البيروقراطية إلى الإلكترونية، كتب المدير ورجل الأعمال الناجح"، القاهرة، خلاصات شعاع، العدد 259 ،أكتوبر 2003، ص 5.

2 على عبد الوهاب، دور إدارة الموارد البشرية في دعم الحكومة الإلكترونية: ورقة عمل مقدمة لمنظمة الأمم المتحدة، صنعاء، اللجنة الاقتصادية والاجتماعية لغربي آسيا، 2003، ص 4.

إدخال المعلومات إلى الحاسب من خلال تدقيق المدخلات وحفظها في مكان آمن، وتسمية الأشخاص المخول لهم التعامل مع هذه البيانات." [1]

ويلاحظ على هذا التعريف على أنه واسع وغير محدد تحديدا دقيقا، لذلك أورد كل من يونس عرب ومحمد الألفي تعريف أمن المعلومات من خلال ثلاث زوايا:

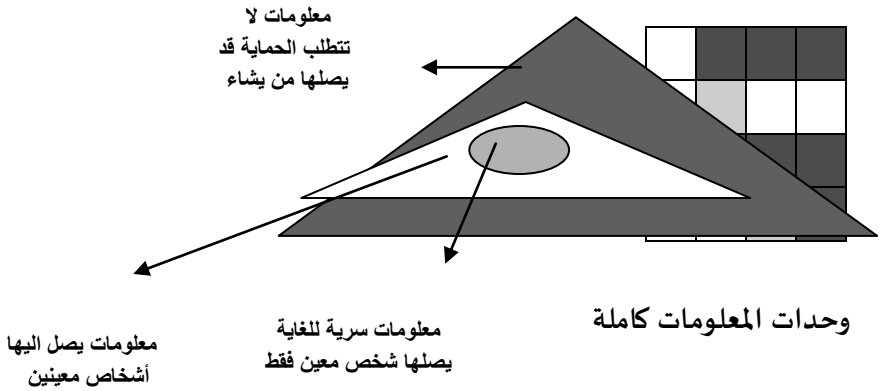
- من زاوية أكاديمية: هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.
- من زاوية تقنية: هو الوسائل والإجراءات اللازم توفيرها لضمان أمن المعلومات من الأخطار الداخلية والخارجية.
- من زاوية قانونية: هو محل دراسات وتدابير حماية سرية وسلامة المحتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة عير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها(جرائم الكمبيوتر والانترنت). [2]

والجدير بالذكر أن ضمان عناصر أمن المعلومات كلها أو بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها.

فليس كل المعلومات تتطلب سرية وضمان، وليس كل المعلومات في المنشأة الواحدة بذات الأهمية من حيث الوصول لها أو ضمان عدم العبث بها، لذا يطرح التساؤل ما الذي نريد أن نحميه؟[3]

والإجابة على هذا التساؤل تحدد تصنيف البيانات والمعلومات من حيث أهمية الحماية، إذ تصنف المعلومات تبعا لكل حالة على حده، من معلومات لا تتطلب الحماية إلى معلومات تتطلب حماية قصوى كما هو موضح في الشكل رقم (1).

الشكل (01): مدى الحماية المطلوبة لأنواع المعلومات



المصدر: يونس عرب،مرجع سبق ذكره، ص 54.

1 فايز جمعة صالح، نظم المعلومات الإدارية، ط2، عمان: دار الحامد للنشر والتوزيع، 2007م، ص235.
2 يونس عرب، أمن المعلومات" أهميتها وعناصرها واستراتيجياتها"، مجلة اتحاد المصارف العربية، بيروت، أبريل 2004، عدد 282، ص53.
3 محمد محمد الألفي، الحماية القانونية لقواعد البيانات في نظم المعلومات ، ندوة أمن وحماية نظم المعلومات في المؤسسات العربية، منشورات المنظمة العربية للتنمية الإدارية، القاهرة 3-7 يونيو 2007، ص8.

فجدار الحماية البارز في الشكل يجب أن يوضع في المكان المناسب، بحيث أن وحدات المعلومات الكاملة تكون مقسمة إلى معلومات لا تتطلب الحماية، معلومات يصل إليها أشخاص معينين، معلومات يصل إليها شخص واحد فقط، وهنا يتم فتح المجال أم المعلومات التي لا تتطلب حماية لكي يصل إليها الجميع، ووضع جدار حماية أمام معلومات يصل إليها أشخاص معينين أو شخص واحد.

II. هندرة الحكومة إلكترونيا وأمننة المعلومات ممارساتيا...المساعي والمعيقات

أولا: مساعي هندرة الحكومة إلكترونيا ومعيقاتها.

تتمثل الهندرة في إعادة النظر في الوضع القائم والتخلي التام عن كل إجراءات وأساليب العمل القديمة والبحث عما هو جديد ومختلف في كيفية التسيير، كما أنها: إحدى أنواع التغيير التنظيمي الجذري الحديث، التي يمكن أن تستخدمها جميع الإدارات والحكومات، من أجل إدخال تغييرات أساسية وجذرية على عملياتها وأساليب وطرق واجراءات العمل لديها.[1] و تهدف الهندرة إلى:

- ✓ التخلص من الروتين القديم وأسلوب الإدارة الجامد والتحول إلى الحرية والمرونة.
- ✓ تخفيض تكلفة الأداء.
- ✓ الجودة العالية في الأداء والخدمة السريعة والمتميزة.
- ✓ إحداث التكامل والترابط بين مكونات العملية الواحدة .[2]

أما مقاربة هندرة الحكومة إلكترونية هي نقلة نوعية لعملية لإعادة هندسة عمل الحكومة عبر دمج الأساليب الإلكترونية الحديثة في عملية التسيير ، بحيث يتم الانتقال من الحكومة التقليدية إلى الحكومة الإلكترونية عن طريق توفير مجموعة من الأسس كما سيتم التطرق إليه في العنصر الموالي.

1) متطلبات هندرة الحكومة إلكترونيا:

بالرغم من الاختلاف في الاستراتيجيات التي تتبعها دول العالم من أجل إرساء الحكومة الإلكترونية إلا أن هناك مجموعة من المتطلبات التي ينظر إليها كمحددات أساسية يجب أخذها في الاعتبار عند وضع استراتيجية الحكومة الإلكترونية، وتعمل كمرشد يساعد الحكومات على تقليل عنصر المخاطرة وزيادة فرص نجاح برامج ومشروعات الحكومة الإلكترونية والتي يمكن إيضاحها على النحو التالي:

أ- **دعم ومساندة النظام السياسي:**

يرتبط التخطيط الاستراتيجي في المنظمات الحكومية بصفة عامة بالنظم السياسية المطبقة على مستوى الدولة، فعادة ما يتمتع الاستراتيجيون العاملون في المجال الحكومي بقدر محدود من الحرية في تعديل رسالة منظماتهم أو إعادة توجيه الأهداف، وقد يرجع ذلك إلى أن التشريعيين والسياسيين كثيرًا ما يكون لهم سيطرة على القرارات والموارد الرئيسة سواء بشكل مباشر أو غير مباشر.

1خضير علي فيروز ،"دور إعادة هندسة عمليات الأعمال (BPR) في تحقيق الميزة التنافسية للمنظمات الصناعية"، مجلة الغري للعلوم الاقتصادية والادارية ، المجلد: 9 ، الاصدار: 26، 2013، ص99.

2 نفس المرجع، ص100.

ويتم تطبيق الحكومة الإلكترونية بموجب قرار سياسي يتم بناء عليه اعتماد الموازنات اللازمة لدعم مشروعات الحكومة الإلكترونية وتحديد الأهداف والأولويات، ويختلف مركز اتخاذ القرار تبعًا لشكل الدولة، ففي النظام الفيدرالي تنتقل سلطة اتخاذ القرار من الوحدات المركزية إلى الولايات التي تتمتع بالحرية في تنظيم أجهزتها الإدارية وتكون السلطة المركزية مقيدة وفقًا للدستور الذي يكفل حماية فعالة لاختصاصات الولاية .

ب- **البنية الأساسية التكنولوجية:**

تمثل البنية التكنولوجية حجر الأساس لبناء معمار الحكومة الإلكترونية والعنصر الحاكم الذي ترتكز عليه كافة استراتيجيات الحكومة الإلكترونية، وتشمل البنية الأساسية التكنولوجية الأجهزة والتقنيات التي يتم من خلالها نقل وتداول البيانات والمعلومات وممارسة كافة المعاملات. ويعتمد نجاح الحكومة الإلكترونية بالدرجة الأولى على القدرة التكنولوجية للدولة حيث تعتبر أهم المعوقات التي تواجه الدول النامية عند التحول إلى الحكومة الإلكترونية، ولذلك فمن المهم عن القائمين على مشاريع الحكومة الالكترونية التركيز على:

- ✓ توفير البنى التحتية والاستراتيجيات المناسبة الكفيلة ببناء المجتمعات، فبناء المجتمعات يتطلب انشاء وسيط تفاعلي على الانترنت يقوم بتفعيل التواصل بين المؤسسات الحكومية وبينها وبين المواطنين وبينها وبين مزوديها[1].
- ✓ حل المشاكل القائمة في الواقع الحقيقي قبل الانتقال إلى البيئة الالكترونية وللتمثيل على أهمية هذا المطلب كمثال، فإنه يجب على الحكومات أن تقوم بتوفير المعلومات اللازمة لمواطنيها عبر الانترنت، حيث يجب أن تتواجد سياسة يتم بموجبها تحديد جميع الوثائق والمعلومات والنماذج الحكومية مباشرة عبر الأنترنت، بحيث كلما ظهرت وثيقة حكومية جديدة أو معلومات جديدة يجب وضعها مباشرة عبر الانترنت.
- ✓ اجراء تغييرات في الجوانب التشغيلية مع بناء التكنولوجيا الممكنة وهذا لا يعني بالضرورة وصول الأنترنت إلى كل البيوت، بل يكفي أن تتوفر لهم إمكانية الولوج إلى شبكات معلومات الدولة من أماكن تواجدهم.
- ✓ العمل على زيادة انتشار تكنولوجيا المعلومات والاتصالات بين الأفراد والجماعات.
- ✓ تشجيع انشاء مراكز إلكترونية فريبة من التجمعات السكانية ومقاهي الأنترنت وتوفير المساعدة الفنية في تلك المراكز من أجل تجاوز عقبة الأمية الإلكترونية والعمل على تعزيز الثقة في تطبيقات الحكومة الالكترونية لدى الجماهير العريضة.
- ✓ الاستفادة من كل ما هو جديد في تكنولوجيا المعلومات حتى تتمكن الدولة من تقديم خدمات إلكترونية ذات جودة عالية من مختلف الجهات والمواطنين لانجاز معاملاتهم دون أي عقبات[2].

ت- **تطوير الإدارات الحكومية:**

يتطلب نجاح تطبيق استراتيجية الحكومة الإلكترونية في الواقع العملي إجراء العديد من التغيرات التنظيمية داخل الإدارات الحكومية، حيث أن نظم وأساليب الإدارة التقليدية لا تتناسب مع تطبيقات الحكومة الإلكترونية التي

1 بوزكري جيلالي، الادارة الالكترونية في المؤسسات الجزائرية واقع وآفاق، رسالة دكتوراه غير منشورة ، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر3، 2016، ص 94.

2 أحمد الشريف بسام، واقع الحكومة الالكترونية في الدول العربية-حالة الجزائر-، رسالة ماجستير غير منشورة، كلية العلوم السياسية والإعلام، جامعة الجزائر3، 2011، ص

تتطلب المرونة والسرعة في اتخاذ القرارات. وتتعدد مجالات التغيير المطلوبة حيث يتطلب الأمر تغيير الهياكل التنظيمية بالتحول إلى الهياكل الشبكية ذات الاتصالات الواسعة، ويقل التوجه نحو التخصص وتقسيم العمل، وفي المقابل يزيد التوجه نحو دمج الوظائف وتقليل المستويات الإدارية، وتقل سيطرة القيادات الإدارية الأعلى، وتقل المستويات الرقابية، ويزيد تمكين العاملين والاعتماد على فرق العمل المدارة ذاتيًا[1].

ويتطلب التحول إلى الحكومة الإلكترونية إعادة هندسة نظم وإجراءات العمل بما يتناسب مع النظم الإلكترونية، وذلك بتحليل الأعمال الحالية وتحديد الأعمال المقترح تحويلها إلى النظم الإلكترونية وتبسيط إجراءاتها وتطوير النماذج المستخدمة، ولا تقتصر إعادة الهندسة عند هذا الحد حيث يتطلب الأمر إعادة تصميم الوظائف وتطوير الواجبات والمسئوليات التي يقوم بها العاملون بما يتناسب مع العمل الإلكتروني.

وتؤثر الثقافة التنظيمية للعاملين بدرجة كبيرة في نجاح تطبيق الحكومة الإلكترونية، فكلما كانت ثقافة المنظمة إيجابية في موقفها من التكنولوجيا الرقمية ازداد رضا الأفراد عن أدوارهم في المنظمة قبل قدوم هذه التكنولوجيا وأثناءها وبعد تطويرها وتطبيقها لتحسين الإنتاجية وجودة المنتجات والخدمات المقدمة ، وبالتالي تقل مقاومة العاملين للتغيير التي تعد من أهم المعوقات التي تواجه الحكومة الإلكترونية.[2]

ث- **إعداد وتهيئة المواطن:**

يجب أن تركز استراتيجية الحكومة الإلكترونية على إعداد وتهيئة المواطن لفهم واستيعاب مزايا التعامل الإلكتروني من حيث تقليل الوقت والجهد والتكلفة. حيث تواجه بعض الدول النامية صعوبات في محاولة نقل تجارب وتطبيقات الدول المتقدمة في مجال تكنولوجيا المعلومات دون اتخاذ الإجراءات اللازمة لتكيف وتهيئة مجتمعاتها لهذه النقلة الحضارية، مما يعرض شعوبها إلى صدمة ثقافية لعدم قدرتها على مسايرة هذه التغيرات التكنولوجية والتجاوب معها. وذلك من خلال اتباع الخطوات التالية:

- ✓ تغيير الصورة الذهنية الراسخة لدى المواطنين عن الخدمات الحكومية، والتأكيد على حرص المنظمات الحكومية على راحة المواطن ورفاهيته وذلك من خلال الحملات الإعلامية المكثفة لإعادة الثقة في الحكومات.
- ✓ الإعلام عن مواقع الخدمات الحكومية الإلكترونية في وسائل الإعلام المختلفة من إذاعة وتلفاز وجرائد ومجلات، وشرح كيفية الوصول إليها والمزايا التي تحققها.
- ✓ التوسع في تدريب المواطنين على استخدام شبكة الإنترنت في المعاملات الإلكترونية مع إتاحة الفرصة لمشاركة القطاع الخاص في نشر الوعي التكنولوجي.
- ✓ العمل على زيادة انتشار تكنولوجيا الاعلام والاتصال بين الأفراد والمؤسسات واستعمالاتها، وذلك عن طريق محاربة الأمية الالكترونية في هذا المجال، بتشجيع انشاء مراكز متخصصة للولوج إلى الأنترنت داخل التجمعات السكنية وتوفير المساعدة الفنية في تلك المراكز من أجل تجاوز عقبة الأمية الالكترونية لدى الجماهير العريضة[3].

1إيمان عبد المحسن زكي، الحكومة الالكترونية –مدخل اداري متكامل، منشورات المنظمة العربية للتنمية الادارية، مصر، 2009، ص72.
2 سعد غالب ياسين، الإدارة الإلكترونية وآفاق تطبيقاتها العربية، الرياض، معهد الإدارة العامة، 2005، ص264.
3 بوراس زهرة، بوشارب أحمد، مدى نجاعة العمل الاداري في الجزائر باعتماد نظام الحكومة الالكترونية، المجلة الجزائرية للعولمة والسياسات الاقتصادية، العدد 04، 2014، ص 22.

ج **متطلبات أمنية:** تتمثل المتطلبات الأمنية للحكومة الالكترونية في ضمان أمن وحماية معلوماتها، هذه الأخيرة التي تعد ثروة ذات قيمة عالية وثمينة مما يجعلها عرضة للتهديد والتعدي والخرق من قبل العابثين وتعد ثروة ذات قيمة عالية وثمينة مما يجعلها عرضة للتهديد والتعدي والخرق من قبل العابثين والمتلصصين وقراصنة الحاسوب. ويقصد بهذا مجموعة الاجراءات والتدابير المستخدمة في المجالين الاداري والفني لحماية المصادر البيانية من أجهزة وبرمجيات وبيانات من التجاوزات والتداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا أو عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة من إدارة هذه المصادر1.

2- معوقات تطبيق الحكومة الإلكترونية.

يواجه تطبيق الحكومة الإلكترونية العديد من العوائق والتحديات التي يرتبط بعضها بالطبيعة الخاصة لمشاريع الحكومة الإلكترونية باعتبارها مشاريع طويلة الأجل تتطلب درجة عالية من التنبؤ بالتغيرات المتوقعة في الظروف المحيطة، ويرتبط البعض الآخر بغياب الدعائم الأساسية لتطبيق الحكومة الإلكترونية، لذا يجب على الحكومات أن تأخذ في الاعتبار هذه المعوقات لوضع الاستراتيجيات اللازمة للتغلب عليها بما يضمن نجاح التطبيق العملي للحكومة الإلكترونية والتي يمكن إيجازها في المحاور التالية:

1.2 المعوقات البشرية: ويمكن تحديدها في الآتي[2]:

- ✓ الأمية الالكترونية لدى العديد من شعوب الدول النامية، وصعوبة التواصل عبر التقنية الحديثة.
- ✓ غياب الدورات التكوينية ورسكلة موظفي الإدارة أو الأجهزة التنظيمية في ظل التحول للحكومة الالكترونية.
- ✓ الفقر وانخفاض الدخل الفردي يؤدي إلى صعوبة التواصل عبر شبكات الحكومة الالكترونية لعدم امتلاك وسائل التواصل من أجهزة وأنترنت...
- ✓ اشكالية البطالة التي يمكن أن تنجم عن تطبيق الحكومة الالكترونية، وحلول الآلة محل الانسان، هذا الأخير الذي يرفض ويقاومم التحول الإلكتروني خوفا عن امتيازاته ومنصبه.

2.2المعوقات الإدارية: تتمثل المعوقات الإدارية في مختلف العراقيل التي تجعل تطور الحكومة الالكترونية عملية متعثرة، ومن أهم المعوقات الإدارية مايلي[3]:

- ✓ تعقيد الإجراءات وانعدام مرونة الهياكل التنظيمية لصعوبة التخلص من الطابع التقليدي البيروقراطي على العكس تقتضي الحكومة الالكترونية منطقا تسييريا آخر يتجاوز الطابع البيروقراطي للمعاملات، مما يجعل البيروقراطية من أهم العوامل المعرقلة للإدارة الالكترونية.
- ✓ انعدام التخطيط لبرامج الحكومة الالكترونية وخاصة الجانب الاستراتيجي، إذ أن تطبيق الحكومة الالكترونية في الغالب يكون في شكل تطوير تكنولوجي ومعلوماتي يفتقر إلى التخطيط المحكم.

1 دلال صادق الجواد، حميد ناصر الفتال، أمن المعلومات، دار اليازوري العلمية للنشر والتوزيع، عمان، 2008، ص ص 11-12.

2 عشور عبد الكريم، دور الإدارة اللالكترونية في ترشيد الخدمة العمومية في الولايات المتحدة الأمريكية والجزائر، رسالة ماجستير غير منشورة، كلية الحقوق والعلووم السياسية، جامعة منتوري، قسنطينة، 2011، ص 39.

3 عصام عبد الفتاح مطر، الحكومة الالكترونية بين النظرية والتطبيق، الدار الجامعية الجديدة، القاهرة، 2008، ص 52.

- ✓ وجود مخاوف على مستوى القيادات الادارية العليا في بعض الدول من تنفيذ مشروع الحكومة الالكترونية نظرا لعناصر مهمة كالشفافية وتكافؤ الفرص والمشاركة.

3.2المعوقات التشريعية والقانونية: يعتبر وضع الأطر التشريعية والقانونية الملائمة لمبادرات الحكومة الالكترونية عاملا ملائما في نجاح هذه المبادرات ومع استبدال العمليات الورقية بمعاملات إلكترونية معترف بها قانونيا (كالدفع الالكتروني، التوقيع الالكتروني وغيرها من المعاملات الالكترونية) لا تزال في المراحل الأولى في كثير من الدول النامية خاصة العربية منها[1]، وقد أدى افتقار الدول العربية لقوانين تنظيم الانترنت خاصة، وللأطر القانونية الملائمة للخدمات الإلكترونية عموما إلى الإبطاء في طرح العديد من الخدمات الالكترونية.

4.2المعوقات الفنية(التقنية): تتمثل أهم المعوقات التقنية فيما يلي[2]:

- ✓ أول ما يواجه المؤسسات التي تسعى إلى تعميم تطبيقات التقنية على دوائرها الإدارية هو ما تحتاج إليه الأجهزة من عمليات فنية تشمل صيانة أجهزة الحاسوب وإصلاحها، وتتفاقم هذه المشكلة مع تقادم مهارات التقنية وظهور الجديد كل يوم، مما يحتاج إلى تجديدها لمواكبة التطورات، الأمر الذي يشكل صعوبة أمام إنشاء الإدارات الالكترونية واستمرارها.
- ✓ صعوبة تطوير البرمجيات في ظل الخلط الحاصل في تحديد البرمجيات المطلوبة ومواصفاتها وشروط عملها.
- ✓ عجز البنى التحتية كالشبكات مثلا لدى بعض الدول عن الوفاء بالتزامات تشغيل العمليات الالكترونية التي تؤسس وتقوم على تلك البنى التحتية التي يفترض أن تدخل ضمن المشروعات التنموية في الدولة.
- ✓ ضعف تقنية دعم اللغة العربية، حيث لا تتيح بعض التقنية تنظيم المعلومات لاستخدامات اللغة العربية.
- ✓ ضعف قطاع تقنيات المعلومات في الدول النامية لقلة الخبرات الفنية، وضعف جاهزية المؤسسات من ناحية أمن المعلومات في هذه الدول على شبكة الانترنت.
- ✓ المخاطر التي يتعرض لها الموقع على الانترنت، ومخاطر إنشاء المعلومات الخاصة بطالب الخدمة والسطو عليها عند إجراء تعامل على الشبكة المعلوماتية، وغياب المستندات الورقية في بعض الخدمات المقدمة إلكترونيا مما يثير إشكالية إثبات التعاملات والعقود وتوثيق الحقوق والالتزامات.

ثانيا: أمننة المعلومات ممارساتيا.

إن التطورات الحاصلة في مفهوم الأمن توحي بالخروج من المفهوم التقليدي للأمن (العسكري) إلى المفهوم الحديث المرتبط بالمجتمع والأفراد في سياق التفكير البنائي، إذ أن مفهوم الأمن بالنسبة لنظرية الأمننة Securitization Theory ليس شرطا موضوعيا بل هو عملية تصاغ من خلال التأسيس التاذاتاني intersubjective لتهديد وجودي كافي لانتاج آثار سياسية...تحدث هذه العملية من خلال ممارسة إستراتيجية تسعى إلى إقناع جمهور المستهدف بالقبول، استنادا للادعاء بأن تنمية معينة أوكيانا ما مهدد بما فيه الكفاية، ما يستدعي

1 أحمد الشريف بسام، مرجع سبق ذكره، ص 141.

2 بوزكري جيلالي، مرجع سبق ذكره، ص 130.

سياسة فورية لتخفيفه...[1]، بناء على ذلك يجب أن نتعامل مع أمن المعلومات باعتباره تهديد غير تقليدي، بحيث يلزمنا التعامل الفوري معه، ومنه سنتطرق إلى العناصر الأساسية لنظام أمن المعلومات، وكافة المخاطر والتهديدات، لنصل في الأخير إلى وسائل أمننة المعومات، وهذا ما سيرد في العناصر القادمة.

1- <u>العناصر الأساسية لنظام أمن المعلومات:</u>

إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات سواء من الناحية التقنية أو التدابير التشريعية هو ضمان توفر العناصر التالية لأية معلومة يراد توفير الحماية الكافية لها.

أ- **السرية أو الموثوقية:** وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين.

ب- **التكاملية وسلامة المحتوى:** وتعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص في أي مرحلة من مراحل المعالجة، أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

ت- **استمرارية توفر المعلومات أو الخدمة:** التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

ث- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به:** ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين.

ج- **ضبط الدخول:** هي تحديد السياسات والإجراءات و تحديد مناطق الاستخدام المسموحة لكل مستخدم وأوقاته، لمنع دخول من لا يملك حق شرعي للدخول إلى نظام المعلومات سواء من الداخل أو الخارج.[2]

2- <u>المخاطر والاعتداءات في بيئة المعلومات:</u>

أ. المخاطر الرئيسية في بيئة المعلومات:

تطال المخاطر والاعتداءات في بيئة المعلومات أربعة مواطن أساسية هي مكونات تقنية المعلومات في أحدث تجلياتها، ويمكن تلخيصها فيما يلي:

✓ **الأجهزة Hardware:** هي كافة المعدات والأدوات المادية التي تتكون منها النظم كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها. لذلك لا بد من إعطاء الأهمية الكبيرة لحماية مواقع منظومة الأجهزة الالكترونية وملحقاتها، والتي تحوي الأجهزة المختلفة في نظم المعلومات، واتخاذ كافة الإجراءات الاحترازية لحماية الموقع، سواء من السرقة أو الأخطار البيئية المختلفة وإدامة الطاقة الكهربائية وانتظامها، وتحديد الإجراءات المختلفة

1 سكوت واتسون،" الانسان ككيان مرجعي؟ النزعة الانسانية باعتباراتها إحدى قطاعات الأمننة" ، تر: سميرة سليمان، المجلة الجزائرية للأمن والتنمية، العدد الثاني، جانفي 2012، ص 200.

2 محمد حمد الألفي، مرجع سبق ذكره، ص ص 14-15.

للتفتيش والتحقق من هوية الداخلين إلى الموقع.

✓ **البرامج:** وهي الأوامر المرتبة في نسق معين لإنجاز الأعمال وهي إما مستقلة عن النظام أو مخزنة فيه.

✓ **المعطيات:** إنها الدم الحي للأنظمة، وتشمل كافة البيانات المدخلة و المعلومات المستخرجة عقب معالجتها، والمعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط التخزين الخاصة.

✓ **الاتصالات:** وتشمل شبكات الاتصال التي تربط أجهزة التقنية بعضها البعض محليا وإقليميا ودوليا، وتتيح فرصة اختراق النظم عبرها كما أنها بذاتها محلا للاعتداء وموطن من مواطن الخطر الحقيقي.

✓ **الإنسان:** يمثل الإنسان محل الخطر. سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بالنظام، فإدراك هذا الشخص حدود صلاحياته، وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية هي مسائل رئيسية يعنى بها نظام الأمن الشامل، خاصة في بيئة العمل المتركزة على نظم الكمبيوتر وقواعد البيانات. [1]

ب. تصنيف المخاطر:

من الناحية التقنية يتعين على أصحاب المنظمات أن تحمي البنية المادية المحيطة بالأجهزة والنظم من الاختراقات وهذا ما يعرف بالحماية المادية، وكذلك يتعين عليهم حماية المنشأة من المخاطر المتصلة بالموظفين والأشخاص وكذلك من الاعتداءات التي تتصل بالمعطيات ذاتها ونظم التوصل إليها، وأخيرا من الاعتداءات التي تتعلق بعمليات النظام ذاته.

وهذا هو التصنيف الذي قال به قطاع عريض من الخبراء التقنيين أو الباحثين في أمن المعلومات ولكن قبل الخوض في تصنيف المخاطر يجدر بنا معرفة ما هو الاختراق ومن هم المخترقون.

- يعرف **الاختراق** بأنه:" الوصول لهدف ما بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالجهاز المستهدف"

وهي بالطبع سمة سيئة يتصف بها المخترق لقدرته على الوصول إلى أجهزة الآخرين عنوة ودون رغبة منهم، وحتى دون علم منهم بغض النظر عن الأعمال التخريبية المقصودة أو غير المقصودة التي قد يحدثها سواء بأجهزتهم الشخصية أو بنفسياتهم.

- أما **المخترقون** Hackers فكانت بداية هؤلاء من المبرمجين المهرة الذين أصبحت لديهم قدرة على التعامل الفني العالي مع مشاكل الكمبيوتر والحاسب الآلي بمهارة شديدة. [2]

إذن فالهاكرز هم الملمين بالبرمجة ومقدمي خدماتهم للآخرين وليسوا كما يقال عنهم أنهم يسطون عنوة على البرامج ويكسرون رموزها.

ويعتبر الهاكرز هو المبرمج الذي يقوم بتصميم أسرع البرامج مع خلوه من المشاكل والعيوب التي تعوق البرنامج

1 نجم عبد الله الحميدي وآخرون، **نظم المعلومات الإدارية-مدخل معاصر-**،ط1(عمان: دار وائل للنشر والتوزيع، 2005)، ص269.

2 حسام شوقي، حماية وأمن المعلومات على الانترنت، القاهرة: دار الكتب العلمية، 2003، ص37.

عن القيام بدوره المطلوب منه، فهو شخص مغرم بالكمبيوتر ويملك معرفة عالية في مجال الشبكات أيضا.

وقد تم تصنيف الهاكرز إلى ثلاثة نماذج:

- ✓ الهاكرز الذين يعملون من أجل الربح المادي فقط
- ✓ الهاكرز الذين يتصرفون بعشوائية ولتحقيق رغبات نفسية
- ✓ الهاكرز الذين يعملون من أجل أغراض البحث.[1]

وعلى ضوء هذا يمكن تصنيف المخاطر والاعتداءات على النحو التالي:

اختراق الحماية المادية Breaches of physical security : وهو على أنواع منها:

❖ التفتيش في المخلفات: ويقصد به قيام المهاجم بالبحث في مخلفات المنشأة من القمامة والمواد المتروكة، بحثا عن أي شيء يساعده على اختراق النظام، كالأوراق المدون عليها كلمات السر أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة، أو أي أمر يحصل من خلاله على أية معلومة تساهم في الاختراق.

❖ الالتقاط السلكي: ويمثل التوصيل السلكي المادي مع الشبكة أو توصيلات النظام جهة استراق السمع أو الاستيلاء على المعطيات المتبادلة عبر الأسلاك، وهي أنشطة تتم بطرق سهلة أو معقدة تبعا لنوع الشبكة وطرق التوصيل المادي.

❖ استراق الأمواج: ويتم من خلال استخدام لواقط تقنية لتجميع الموجات المبعثرة من النظم باختلاف أنواعها.[2]

❖ حجب الخدمة عن المستخدمين الشرعيين: والمقصود هنا الإضرار المادي بالنظام لمنع تقديم الخدمة، حيث يقوم المهاجم في هذه الحالة باستخدام برامج تقوم بإرسال عدد هائل من حزم البيانات العبثية بهدف التحميل الزائد على خادم الويب، وبالتالي حجب الخدمة عن المستخدمين الشرعيين[3].

اختراق الحماية الشخصية: Breaches of personnal security

تعد المخاطر المتصلة بالأشخاص والموظفين وتحديدا المخاطر الداخلية منها واحدة من مناطق الاهتمام العالي لدى جهات أمن المعلومات، إذ ثمة فرصة الاختراق لأن الأشخاص من الداخل ممكن أن يحققوا ما لا يحققه أحد من الخارج وتتعلق هذه بالأخطار الداخلية والخارجية معا ويمكن تلخيصها على النحو التالي[4]:

أ- التخفي بانتحال صلاحيات شخص مفوض: والمقصود هنا الدخول غير المصرح به إلى النظام عبر استخدام وسائل التعريف الخاصة بمستخدم آخر مصرح له بالدخول والاستخدام، أي أن يستخدم شخص غير مصرح له بالدخول إلى النظام وسائل التعريف الخاصة بشخص آخر مصرح له بالدخول.

ب- الهندسة الاجتماعية: وصنف هذا الأسلوب ضمن الحماية المادية أحيانا، ويرجع إلى أنشطة الحصول على معلومات تهيئ الاقتحام من خلال علاقات اجتماعية.

---

1 **نفس المرجع السابق**، ص ص 27-38.

2 منير الجنبيهي، ممدوح الجنبيهي، أمن المعلومات الالكترونية، الإسكندرية: دار الفكر الجامعي، 2005، ص21.

3 محمد نور برهان، عز الدين خطاب، التجارة الالكترونية، القاهرة: الشركة العربية المتحدة للتسويق والتوريدات، 2008، ص 266.

4 يونس عرب، أمن المعلومات، مرجع سبق ذكره، ص56.

ت- الإزعاج والتحرش: هي تهديدات تندرج تحتها أشكال مختلفة من الاعتداءات والأساليب ويجمعها توجيه رسائل الإزعاج والتحرش وربما التهديد والابتزاز.

ث- قرصنة البرمجيات: وهي تتحقق عن طريق نسخ البرامج دون تصريح أو استغلالها على نحو مادي دون تخويل بهذا الاستغلال، أو تقليدها ومحاكاتها والانتفاع المادي بها على نحو يخل بحقوق المؤلف.

- **اختراق حماية الاتصالات: Breaches of communication security** ويمكن تصنيفها كالآتي:

أ- هجمات البيانات، وتكون كالتالي:

- ✓ النسخ غير المصرح به: وهي العملية الشائعة التي تتبع الدخول غير المصرح به للنظام، حيث يمكن الاستيلاء عن طريق النسخ على كافة أنواع المعطيات والتي تشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها.
- ✓ تحليل الاتصالات: الفكرة هنا ببساطة أي هجوم ينصب على دراسة أداء النظام في مرحلة التعامل ومتابعة ما يتم فيه من اتصالات والارتباطات بحيث يستفاد منها في تحديد سلوك المستخدمين، وتحديد نقاط الضعف ووقت الهجوم المناسب، وغير ذلك من مسائل يجمعها فكرة الرقابة على حركة النظام بغرض تسيير الهجوم عليه.
- ✓ القنوات المخفية: وهي عمليا صورة من صور اعتداءات التخزين حيث يحضى المقتحم بمعطيات أو برمجيات مستولى عليها كأرقام بطاقات ائتمان في موضع معين من النظام ويمكن أن تستخدم في هجوم لاحق.[1]

ب- هجمات البرمجيات، وتتنوع هذه الهجمات كالآتي:

- المصائد أو الأبواب الخلفية: وهي عبارة عن ثغرة في برنامج معين يتيح للمخترق إمكانية الوصول إلى النظام.
- سرقة أو اختلاس المعلومات: أي أن يستغل الشخص استخداما مشروعا من قبل غيره لنظام ما، فيسترق النظر أو يستخدم النظام عندما تتاح له الفرصة لانشغال المستخدم دون علمه أو أن يجلس ببساطه مكان مستخدم النظام فيطلع على المعلومات أو يجري أية عملية في النظام، وذلك بغرض الحصول على أية معلومات تساعده في الاختراق لاحقا كأن يراقب المستخدم وهو يكتب كلمة السر.
- الهجمات الوقتية: تتم بطرق تقنية معقدة للوصول غير المصرح به إلى البرنامج أو المعطيات وتقوم جميعها على فكرة استغلال وقت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام.
- الشفرات الخبيثة: برمجيات ضارة تستغل للتدمير سواء تدمير النظام أو البرامج أو المعطيات أو الملفات أو الوظائف أو تستثمر للقيام بمهام غير مشروعة كإنجاز احتيال أو غش في النظام.[2]

1 منير الجنبيهي، ممدوح الجنبيهي، أمن المعلومات الالكترونية، مرجع سبق ذكره، ص 23.

2 أحمد نوري دخيل، سعد عبدالسلام طلحة، اختراقات أمن المعلومات وطرق تفاديها، المجلة الدولية المحكمة للعلوم الهندسية وتقنية المعلومات، المجلد 2، العدد 2، يونيو 2016، ليبيا، ص 22.

اختراق حماية العمليات: Breaches of operation security

هي المخاطر المتصلة بعمليات الحماية والتي تستهدف استراتيجية الدخول، نظام الإدخال أو الإخراج ومعالجة البيانات، وهي متنوعة كالآتي:

أ- العبث بالبيانات: وهو تغيير البيانات أو إنشاء بيانات وهمية في مراحل الإدخال أو الإخراج.

ب- خداع برتوكول الانترنت: وهي وسيلة تقنية بحتة، بحيث يقوم المهاجم عبر هذه الوسيلة بتزوير العنوان المرفق مع حزمة البيانات المرسلة .

ت- تخمين كلمة السر: وتتم عن طريق تخمين كلمات السر مستفيدا من ضعف الكلمات عموما.

ث- المسح: هو برنامج احتمالات يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة ويستخدم تحديدا بشأن احتمالات كلمة السر بدلا من الاعتماد على التخمين البشري.

ج- استغلال المزايا الإضافية: الأصل أن مستخدم النظام وتحديدا داخل المنشأة يكون محدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، لكن ما يحدث في الواقع العملي أن مزايا الاستخدام يجرى زيادتها دون تقدير لمخاطر ذلك، وفي هذه الحالة فإن مخترق النظام سيكون قادرا على تدمير أو التلاعب ببيانات المستخدم الذي دخل عبر نقطة الدخول الخاصة به، وهذا باستثماره للمزايا الإضافية.[1]

ثالثا: وسائل أمننة المعلومات.

تنبع أهمية أمن المعلومات من أنها تستخدم من قبل الجميع بلا استثناء سواء الدول، الشركات أو الأفراد، كما أنها هدف للاختراق من جانب الجميع كذلك وأيضا بلا استثناء، وفي بعض الأحيان تكون المعلومات هي الفاصل بين الربح والخسارة للشركات وتكلف الفرد ثروته وربما حياته في بعض الأحيان.

وفي هذا العصر بالذات انقلبت الآية ولم تعد مشكلة الناس كيفية الحصول على المعلومات وإنما أصبحت مشكلتهم كيف تحمى هذه المعلومات من الأخطار التي تهددها، ويمكن أن نبرز وسائل أمننة المعلومات كالآتي:

1- تشفير البيانات Encoding.

أ- **مفهوم التشفير:** يفرض أنه لدينا رسالة نود إيصالها إلى شخص معين ولكننا نخشى من وقوع رسالتنا هذه في يد طرف ثالث لا ينبغي له أن يطلع عليها، في هذه الحالة نقوم بتشفير الرسالة بحيث لو تم اعتراض طريقها فلا ينكشف مضمونها. هذا باختصار هو التشفير وهو أكثر وسائل الأمن فعالية.

و يعرف **Bowyer** التشفير بأنه:" تغيير مظهر المعلومات بحيث يختفي معناها".[2]

بينما **رأفت رضوان** يعرف التشفير على أنه:" تغيير مضمون الرسالة باستخدام برنامج معين يسمى مفتاح التشفير وذلك قبل إرسال الرسالة على أن يكون لدى مستقبل الرسالة القدرة على استعادة محتوى الرسالة في

1 فايز جمعة، مرجع سبق ذكره، ص243.

2 حسن طاهر داوود، الحاسب وأمن المعلومات، الرياض: منشورات معهد الإدارة العامة، 2000، ص177.

صورتها الأصلية قبل عملية التشفير، وذلك باستخدام عملية عكسية للتشفير تسمى حل الشفرة".[1]

أي أن التشفير يهدف إلى منع الغير من التقاط الرسائل أو المعلومات ومن ثم منع وصولها أو وصولها مشوهة إلى الطرف الآخر في المعاملة، وذلك على نحو يعرقل هذه المعاملة.

وفي كل الأحوال لا بد من حماية الرسالة وضمان وصولها بالشكل المطلوب إلى مستقبلها.

ب- **أهداف التشفير:** يهدف التشفير إلى التغلب على الأخطار التالية:

- ✓ الاطلاع على المعلومات المحظورة.
- ✓ محاولة تعديل البيانات المنقولة.
- ✓ إعادة توجيه البيانات إلى وجهة أخرى.
- ✓ تغيير محتويات الرسائل المتبادلة.
- ✓ إقحام رسائل زائفة ضمن الرسائل المنقولة عبر الخط.
- ✓ تغيير كلمات السر الخاصة بالمستفيدين.
- ✓ انتحال شخصية المستخدم الحقيقي.[2]

2- الجدران النارية Firewall

وهي عبارة عن مجموعة من البرامج والأجهزة تتصل بشبكة المعلومات والأنظمة الداخلية للمنشأة وبين الانترنت، وتقوم بمراقبة كافة التيارات الالكترونية المارة من وإلى الشبكة الداخلية للمنشأة، وذلك لمنع أية محاولة لدخول إلكتروني غير مصرح به إلى الشبكة الداخلية، وكذلك لمنع دخول أية برمجيات مخربة من الفضاء السايبيري الخارجي[3].

وتعمل الجدران النارية ضمن سياسات حماية أشهرها.

- ✓ منع جميع الزوار من الدخول إلى الشبكة المحلية باستثناء الزوار المخولين، حيث يعطى لكل زائر خارجي اسم مستخدم وكلمة مرور تخوله الدخول إلى الشبكة المحلية للمنشأة.
- ✓ السماح للزوار بالدخول إلى الشبكة المحلية باستثناء الزوار المشكوك بهم، حيث يعرفون من خلال تصرفاتهم السابقة ويتم رصد عنوان أجهزتهم على الانترنت أو اسم مجال المستخدم على الانترنت.[4]
- ✓ تستخدم الجدران النارية الحديثة أسلوبا لفلترة وتصفية البيانات الواردة كما تقوم بإنشاء الشبكات الافتراضية الخاصة ورقابة محتوى البيانات الوقائية من الفيروسات حيث يتم تحليل حزم المعلومات

1 رأفت رضوان، مرجع سبق ذكره، ص 32
2 حسن طاهر داوود، مرجع سبق ذكره، ص 178.
3 نادر ألفرد قاحوش، مرجع سبق ذكره، ص42.
4 محمد نور برهان، عز الدين الخطاب، مرجع سبق ذكره، ص42.

الداخلية عبر حاجز العبور قبل السماح لها بالدخول.

إن وضع الجدران النارية المانعة بالنسبة للشبكة يعد أحد العناصر الأساسية في تحديد مستوى التأمين حيث يوجد أكثر من طريقة وأسلوب يمكن استخدامه[1].

3- النسخ الاحتياطي: Back-up

يعتبر النسخ الاحتياطي أحد الأركان الأساسية لأمن المعلومات والمقصود به: أخذ نسخة من البيانات وتخزينها في مكان آمن، وعند الحاجة إليها يتم استرجاعها Restore، بمعنى استعادة محتويات النسخة الاحتياطية لتكون هي النسخة العاملة حتى يتمكن من إعادة تشغيل النظام من النقطة التي تم أخذ النسخة الاحتياطية عندها.

ويعتبر النسخ الاحتياطي إجراء احتياطيا ليس إلا، فلو كان نظام تأمين الحاسب كفؤا بنسبة 100% لما كان هناك داع له، ولكن من المؤكد انه بسبب ضعف إجراءات التأمين وبسبب أخطاء البشر الذين لا يلتزمون بها تأتي لحظة ما يحدث فيها تلف للبيانات أو الملفات وتظهر الحاجة للنسخ الاحتياطية.[2]

هذا ويجب أن يكون النسخ الاحتياطي جزءا من الروتين اليومي لمركز الحاسب، فيتم تنفيذه في أوقات محددة، وكذلك يجب أن يكون دوريا لأنه عند حدوث الخطأ في النظام يلزم معرفة إلى أي مدى يجب الرجوع إلى الوراء لاستعادة البيانات.

3-إجراءات الاستعادة:

يجب لضمان نجاح استرجاع البيانات المفقودة مجموعة من الإجراءات منها ما يلي:

- ✓ أن يتم تخزين النسخ الاحتياطية في مكان آمن ، ويتم استرجاع البيانات المخزنة عند الحاجة بواسطة برامج مساعدة جاهزة.
- ✓ يجب توعية الموظفين بالإجراءات الواجب إتباعها لتنفيذ عمليات الاسترجاع بالشكل الصحيح، فهذه العمليات لا تتم بصفة دورية مثل النسخ الاحتياطي، وإنما تتم عندما تكون هناك الحاجة إليها.
- ✓ يجب إجراء اختبارات من وقت لآخر بهدف التأكد من أن البيانات والبرامج التي تم نسخها احتياطيا يمكن استرجاعها بنجاح.

هذا وهناك طرق أخرى لحماية وأمن المعلومات، ولكن المهم في مسألة الأمن ليس أن نضع الإجراءات المحكمة، وإنما المهم أن تكون الإجراءات عملية وميسرة، فمن السهل أن تبني قلعة مسلحة محكمة التحصينات ولكن من الصعب أن تكون الإقامة في هذه القلعة سهلة وممكنة وممتعة لسكانها.

III. تجربة الحكومة الإلكترونية في الإمارات العربية المتحدة .

إن الحكومة الإلكترونية في الإمارات تعتبر تجربة رائدة على مستوى العالم العربي حيث بدأت عام 2002، إذ تعد دولة الإمارات العربية المتحدة بصورة عامة- لاسيما إمارة دبي- مركزا للتجارة والصناعة في منطقة الشرق الأوسط وهي كذلك سوق عالمية لتجارة الإلكترونيات والحاسوب حيث وضعت الإمارة نوعين من الأهداف ، تبرز في

1 رأفت رضوان، مرجع سبق ذكره، ص 110-111

2 طاهر داوود، مرجع سبق ذكره، ص 241.

الأهداف قصيرة المدى حيث تعمل على تهيئة البنية التحتية اللازمة لتشغيل الخدمات الإلكترونية. فضلا على توفير عدد من خدمات الدائرة الإلكترونية الخاصة بالأفراد والمؤسسات عبر شبكة الأنترنيت. بما في ذلك تحسين الإجراءات الداخلية الخاصة بإنجاز المعاملات... و**الأهداف بعيدة المدى** التي تعمل من خلالها على توفير عدد أكبر من الخدمات عبر الأنترنيت. وربطها عبر قنوات جديدة كالهواتف والأجهزة النقالة، بما في ذلك التركيز المستمر على تحسين الإجراءات والنظم الداخلية المساندة للخدمات الإلكترونية، والعمل على توعية وتهيئة العملاء والموظفين ودفعهم نحو الاستفادة من الخدمات الإلكترونية.[1]

وما يدعم مصداقية ريادتها على مستوى القطر العربي في هذا المجال الإحصائيات المقدمة من طرف منظمة الأمم المتحدة سنة 2018حول مؤشر تنمية الحكومة الإلكترونية ومؤشر المشاركة الإلكترونية كما ورد ضمن الجدول التالي:

جدول رقم (01): مؤشر تنمية الحكومة الإلكترونية والمشاركة الإلكترونية لدى بعض الدول العربية سنة 2018.

	الدولة	مؤشر تنمية الحكومة الإلكترونية E-Government Development Index EGDI	مؤشر المشاركة الإلكترونية E-Participation Index (EPI)
1	الإمارات العربية المتحدة	0.8295	94.57%
2	البحرين	0.8116	80.43%
3	الكويت	0.7388	70.11%
4	قطر	0.7132	72.28%
5	المملكة العربية السعودية	0.7119	72.28%
6	عمان	0.6846	83.70%
7	تونس	0.6254	80.43%
8	الأردن	0.5575	50.00%
9	لبنان	0.5530	46.20%
10	المغرب	0.5214	78.26%
11	مصر	0.4880	55.43%
12	الجزائر	0.4227	22.83%
13	العراق	0.3376	35.87%
14	السودان	0.2394	50.00%
15	اليمن	0.2154	14.67%

Source: UNITED NATIONS، E-GOVERNMENT SURVEY 2018، Department of Economic and Social Affairs، New York، 2018، PP228-249.

1 سعود جايد مشكور و عقيل جابر ،"**إمكانات تطبيق الحكومة الالكترونية في العراق**"، مجلة أبحاث ودراسات التنمية، لعدد الثالث ، ديسمبر 2015، ص ص19-20.

وفق للإحصائيات الواردة في الجدول و المقدمة من طرف منظمة الامم المتحدة في سياق احصائيات الحكومة الإلكترونية فإن الإمارات العربية المتحدة تعتبر الأولى عربيا في مؤشر تنمية الحكومة الإلكترونية E-Government Development Index بما يقدر بـ : 0.8295، كما أنها الأولى عربيا أيضا من حيث مؤشر المشاركة الإلكترونية E-Participation Index والتي تقد بـ: 94.57% .[1]

فبحسب استبيان تنمية الحكومات الإلكترونية E-GOVERNMENT SURVEY ، الصادر في عام 2018 عن إدارة للشؤون الاقتصادية والاجتماعية التابعة للأمم المتحدة، حققت دولة الإمارات قفزة نوعية في المؤشر الكلي لتنمية الحكومة الإلكترونية من المركز 29 في العام 2016 إلى المركز 21 في 2018، متقدمة ثمانية مراكز لتصبح دولة الامارات من الدول الطليعية الخمس والعشرين في هذا المؤشر. ويرصد المؤشر مستوى التقدم في مسار التحول الرقمي للحكومات العالمية[2].

وقد عملت دولة الإمارات على تكريس الحكومة الإلكترونية من خلال عدة خدمات بارزة في ما يلي:

- ✓ **خدمات المواطنين :** من بينها خدمات المنح الإسكانية؛ معادلة الشهادات الدراسية؛ إصدار الوثائق المدنية؛ دفع المخالفات المرورية؛ دفع الزكاة؛ خدمة القروض الإسكانية....
- ✓ **خدمات الزوار**: حجز الفنادق، إذن الدخول سياحة، الاستفسار عن التأشيرات، الحصول على خرائط المترو...
- ✓ **خدمات الأعمال**: إجراءات الرخصة التجارية- استقبال عروض الشركات، إصدار شهادة انجاز مبنى، الاستعلام عن حالة الطلب، إصدار تصريح استزاد شتلات وبذور ومنتجات السمكية، إصدار تصريح بناء فندق...[3]

وقد تم تعزيزها بخدمات أخرى بارزة في ما يلي:

- ✓ **الدخول الذكي(Smart Pass)** : توفر دخول موحد لكافة المواقع والتطبيقات الحكومية من خلال اسم مستخدم واحد وكلمة مرور واحدة.
- ✓ **خدمة الإستبيان الذكي (mSurvey)** تعنى باستطلاع رضى الموطنين حول الخدمات المقدمة،
- ✓ **خدمة مبروك مايك** : توفر باقة استخراج الوثائق للمولود الجديد .
- ✓ **بوابة خدماتي:** وهي عبارة عن نظام لتوثيق كل الخدمات الحكومية وفق تصنيفاتها المعتمدة من مكتب رئاسة الوزراء. وتعمل البوابة كمرجع للخدمات الحكومية.

1 UNITED NATIONS، E-GOVERNMENT SURVEY 2018، Department of Economic and Social Affairs، New York، 2018، PP228-249

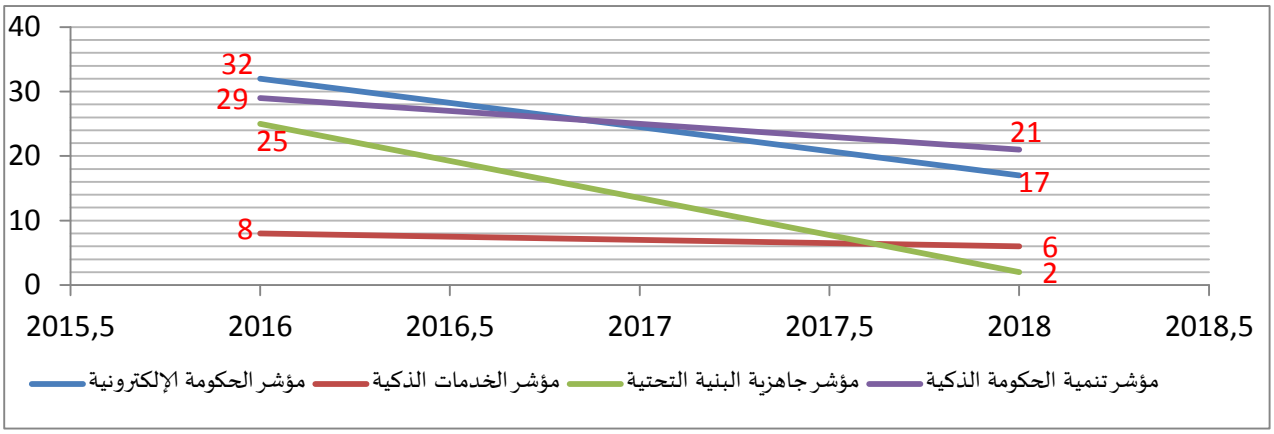
2 البوابة الرسمية لحكومة الإمارات العربية المتحدة،" مؤشر تنمية الحكومة الإلكترونية لدولة الإمارات"، تاريخ الولوج: 2018/11/22، نقلا عن الموقع الإلكتروني: https://www.government.ae/ar-AE/information-and-services/g2g-services/uae-e-government-development-index-egdi

3 سارة بهلولي،الحكومة الإلكترونية آلية لترقية الخدمة العمومية لتجربة الإماراتية نموذجا، مجلة الإقتصاد الصناعي،العدد 12، جوان 2017، ص ص 49-50.

✓ **خدمة الإنترنت المشترك للحكومة:** تؤمّن الشبكة الإلكترونية الاتحادية ربطاً آمناً بالإنترنت لكافة الجهات الحكومية الاتحادية عبر مزود مزدوج لخدمة الإنترنت، مما يسمح بتحقيق إنتاجية أعلى. وتوفر هذه الخدمة اتصالا موحدا بالإنترنت في الجهات الاتحادية[1]

بناء على ما سبق، يمكن القول أن دولة الإمارات العربية المتحدة حققت قفزة نوعية في إرساء الحكومة الإلكترونية، وقد برز هذا جليا في الإحصائيات المقدمة من طرف منظمة الأمم المتحدة حولة ترتيب الدول عالميا، ومن بينها دولة الإمارات وفق عدة مؤشرات على النحو التالي:

الشكل رقم (2): يوضح مقارنة لترتيب دولة الإمارات عالميا ضمن عدة مؤشرات بين سنتي 2016 و2018.



المصدر: من إعداد الباحثين وفقا للمعلومات المتداولة في الموقع الرسمي لحكومة الإمارات عبر الموقع التالي:
https://www.government.ae/ar-AE/information-and-services/g2g-services/uae-e-government-development-index-egdi

وفقا لما ورد في الشكل رقم (2) يتضح جليا أن الإمارات أحرزت تقدما من حيث الترتيب العالمي حسب مؤشر المشاركة الإلكترونية من المرتبة 32 عالميا سنة 2016 إلى المرتبة 17 عالميا سنة 2018، وحققت تقدما حسب مؤشر الخدمات الذكية/الرقمية من المرتبة 8 عالميا سنة 2016 إلى المرتبة 6 عالميا سنة 2018، وبالمقابل أيضا أحرزت قفزة نوعية في مؤشر جاهزية البنية التحتية للاتصالات السلكية واللاسلكية من المرتبة 25 عالميا سنة 2016 إلى المرتبة 2 عالميا سنة 2018، أما بالنسبة لمؤشر تنمية الحكومة الذكية فقد حققت تقدما أيضا من المرتبة 29 عالميا سنة 2016 إلى المرتبة 21 عالميا سنة 2016... بناء على ما سبق، يتضح أن الحكومة الإلكترونية في الإمارات تسير وفق سياسات وخطط ناجعة ما يؤهلها إلى أن تكون مراتب عالمية أولى في هذا المجال.

الأمن المعلوماتي في الإمارات العربية المتحدة:

يمكن القول أن استراتيجية استباب الأمن المعلوماتي في الإمارات العربية المتحدة أخذت اتجاهين بارزين في توليفة التدابير الوقائية و توليفة التدابير العقابية، وهذا ما سنعكف عليه في الآت ذكره.

1حكومة الإمارات، " قائمة خدمات الشبكة الإلكترونية الاتحادية"، تاريخ الولوج: 2018/12/01، نقلا عن الموقع الإلكتروني :
https://www.government.ae/ar-AE/information-and-services/g2g-services/fednet/fednet-service-catalogue

توليفة التدابير الوقائية: تعمل دولة الإمارات على تعزيز الأمن الرقمي لأفراد المجتمع من مواطنين ومقيمين من خلال عدة مبادرات تشمل خدمة الدخول الذكي، مركز الاستجابة الوطني لطوارئ الحاسب الآلي (aeCERT)، ومبادرة سالم*، بطاقة الهوية الصادرة من دولة الإمارات.

خدمة الدخول الذكي : تتيح خدمة الدخول الذكي للمتعامل الوصول إلى كافة الخدمات الإلكترونية لمختلف الجهات الحكومية في دولة الإمارات، وإجراء المعاملات عبر الإنترنت باستخدام حساب موحد، وكلمة مرور موحدة، بحيث لا يحتاج المتعامل لإنشاء عدة حسابات وكلمات مرور للحصول على الخدمات من مختلف الجهات الحكومية، كما توفر الخدمة الكثير من الوقت والجهد فيما يخص تعريف المتعاملين وتمكنها من التعرف على صاحب المعاملة بطريقة ذكية والحصول على بياناته الأساسية دون الحاجة إلى سؤاله عنها كل مرة، فضلاً عن التقليل من نسيان المتعامل لاسم المستخدم وكلمة المرور لكل موقع إلكتروني حكومي في الدولة، حيث باستطاعته الدخول مرة واحدة، باستخدام ملف مستخدم واحد[1] .

مركز الاستجابة الوطني لطوارئ الحاسب الآلي (aeCERT): قامت بإنشائه هيئة تنظيم الاتصالات ، إذ تعد مهمته الرئيسية في دعم البنية التحتية للاتصالات ونظم المعلومات والمحافظة عليها من تهديدات الجرائم الأمنية على الانترنت، وبناء ثقافة آمنة ومحمية من جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة، ولتحقيق ذلك يقدم المركز عدد من الخدمات إلى الجهات المختلفة في الدولة كالإرشاد والتعليم والوعي والإستشارات والمراقبة والاستجابة.[2]

مبادرة سالم: هي مبادرة توعية وقائية كانت نتاج للتعاون بين هيئة تنظيم الاتصالات إذ تعمل على إرشاد وتوجيه جميع مستخدمي الشبكة نحو ثقافة معلوماتية آمنة في دولة الإمارات. ويدعم الموقع الوعي الأمني من خلال الفيديوهات التثقيفية، والمواد، والرسائل التوعوية، والألعاب الهادفة.[3]

مبادرة بطاقة الهوية الصادرة من دولة الإمارات: قامت الهيئة الاتحاديّة للهويّة والجنسيّة المعروفة مُسبقاً بهيئة الإمارات للهوية بتسجيل جميع سكان دولة الإمارات في مشروع السجل السكاني وبطاقة الهوية، إذ تحمل بطاقة الهوية بيانات الشخص البيومترية للتحقق من هويته باستخدام صفاته الفريدة التي لا يمكن نقلها للآخرين، مثل بصمات الأصابع، وهندسة كف اليد، وشبكية العين، وبعض خصائص الوجه وملامحه، وغيرها[4].

توليفة التدابير العقابية : لقد اعتمدت دولة الإمارات العربية مجموعة من القوانين العقابية بخصوص منتهكي الأمن الإلكتروني ومن بينها عقوبات تتعلق بتزوير مستند إلكتروني أو تعطيل الوصول إلى شبكة المعلومات أو الولوج الإلكتروني بغير حق بهدف الحصول على ارقام او بيانات بطاقة ائتمانية أو إلكترونية أو حسابات مصرفية، وبما في

* لمزيد من المعلومات يمكن الولوج إلى الموقع الرسمي للمبادرة عبر الرابط التالي: http://salim.ae/ar

1 المرجع نفسه، الصفحة نفسها.

2 سامر مقدادي، مركز الاستجابة لطوارئ الحاسب الآلي – دولة الامارات ، تاريخ الولوج: 2018/12/01، نقلا عن الموقع الإلكتروني: http://security4arabs.com/2011/12/15/aecert/

3 هيئة تنظيم الإتصالات، سالم مرشدكم لحماية الشبكة الإلكترونية، تاريخ الولوج : 2018/12/01، نقلا عن الموقع الإلكتروني: http://salim.ae/ar

4 البوابة الرسمية لحكومة الإمارات العربية المتحدة، المرجع السابق الذكر، الصفحة نفسها.

ذلك التحايل على العنوان الإلكتروني بقصد ارتكاب جريمة، بحيث أقرت صراحة في التشريعات الاتحادية العقوبات التالية:

1- عقوبة تزوير مستند الكتروني واستعمال السند المزور مع العلم بالتزوير: يعاقب بالسجن المؤقت والغرامة التي لا تقل عن مائة وخمسون الف درهم ولا تجاوز سبعمائة وخمسون الف درهم كل من زور مستنداً الكترونياً من مستندات الحكومة الاتحادية او المحلية او الهيئات او المؤسسات العامة الاتحادية او المحلية(المادة 6)[1].

2- عقوبة تعطيل الوصول الى شبكة معلوماتية او موقع الكتروني او نظام معلومات الكتروني: يعاقب بالحبس والغرامة التي لا تقل عن مائة الف درهم ولا تجاوز ثلاثمائة الف درهم او بإحدى هاتين العقوبتين كل من اعاق او عطل الوصول الى شبكة معلوماتية او موقع الكتروني او نظام معلومات الكتروني(المادة 8).[2]

3- عقوبة استخدام الشبكة المعلوماتية او نظام المعلومات الالكتروني او وسائل تقنية المعلومات بغير حق بهدفالحصول على ارقام او بيانات بطاقة ائتمانية او الكترونية او حسابات مصرفية* يعاقب بالحبس والغرامة او بإحدى هاتين العقوبتين كل من توصل بغير حق، عن طرق استخدم الشبكة المعلوماتية او نظام معلومات الكتروني او احدى وسائل تقنية المعلومات، الى ارقام او بيانات بطاقة ائتمانية او الكترونية او ارقام او بيانات حسابات مصرفية، او اي وسيلة من وسائل الدفع الالكتروني(المادة 12).[3]

4- عقوبة التحايل على العنوان البروتوكولي: بموجب القانون الاتحادي رقم (12) لسنة 2016 ، بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، يُعاقب بالسجن المؤقت والغرامة التي لا تقل عن خمسمئة ألف درهم ،ولا تتجاوز مليوني درهم أو بإحدى هاتين العقوبتين كل من تحايل على العنوان البروتوكولي للشبكة المعلوماتية ،باستخدام عنوان وهمي، أو عنوان عائد للغير أو بأية وسيلة أخرى، وذلك بقصد ارتكاب جريمة، أو الحيلولة دون اكتشافها.[4]

بيد أنه ليس في سبيل الحصر أو القصر أن يتم ذكر هذه العقوبات، إذ أن الزخم الوافي الذي يحوزه قانون مكافحة جرائم تقنية المعلومات في الامارات العربية المتحددة كفيل بالشرح المفصل لكافة الجهود القانونية من أجل استتباب الأمن الإلكتروني في هذه الدولة.

1 دائرة القضاء أبوظبي ، قانون مكافحة جرائم تقنية المعلومات، سلسلة التشريعات الإتحادية، 2013، ص ص 21-22.

2 المرجع نفسه ، ص 22.

3 قصر الرئاسة بأبوظبي، مرسوم بقانون اتحادي رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، تاريخ الولوج : 2018/12/01، نقلا عن الموقع الإلكتروني: https://goo.gl/4TxpnW

4 قصر الرئاسة بأبوظبي، القانون الاتحادي رقم (12) لسنة 2016 ، بتعديل المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، المادة الأولى، 23 ماي 2016، ص20.

الخاتمة:

الحكومة الالكترونية هي نتيجة طبيعية لثورة المعلومات واقتصاد المعرفة، ومشروعها يقوم بالبحث عن أفضل الوسائل التي يمكن بها استفادة الحكومات من تقنيات المعلومات والاتصالات في إدارة مرافقها وتسيير مختلف شؤون المجتمع، وتسعى من خلال نموذجها الجديد أن تساهم في تنمية وتطوير الاقتصاد الوطني وتحسين صورة البلد بشكل عام، بالاضافة إلى تحسين خدمة العنصر الأهم في المجتمع ألا وهو المواطن.

إن مشروع بناء الحكومة الالكترونية يتمحور حول فكرة أساسية مفادها الاستثمار في تقنيات المعلومات والاتصالات، والتحضير اللازم للعنصر البشري وربط المواطن والمؤسسات الحكومية ومؤسسات الأعمال ومؤسسات المجتمع المدني بنسق إلكتروني موحد يتيح إجراء مختلف المعاملات بين هذه الأطراف جميعا بالسهولة والسرعة اللازمة مما يوفر الجهد والوقت والتكاليف، ويوفر قدرا من الثقة، الشفافية، الخصوصية والأمن.

إن التحول إلى الحكومة الالكترونية وعلى خلاف ما يعتقد الكثيرون ليس قضية تقنية وحسب أساسها الحاسبات الآلية وشبكة الانترنت وشبكات الاتصالات وغيرها من الجوانب الفنية على أهميتها، ولكنها وفي الدرجة الأولى قضية إدارية في الأساس تعتمد على فكر إداري متطور وقيادات إدارية واعية تستهدف التطوير وتسانده وتدعمه بكل قوة حتى تحقق مسؤوليتها الرئيسية وهي خدمة المستفيدين وتحقيق رغباتهم مع الالتزام بأعلى مستويات الجودة والاتقان في العمل.

الحكومة الالكترونية تعتبر الوجه الآخر للحكومة الكلاسيكية عبر الفضاء الإلكتروني، هذا الفضاء الذي يشكل تحديا كبيرا للعديد من الدول النامية التي لا تزال تعاني من عقبات للولوج إليه، والتي تواجه في ظل هذا الفضاء عدة تهديدات فيما يخص أمن المعلومات الذي يعتبر من أهم معضلات العمل الالكتروني، بمعنى أن المعلومات والوثائق التي يجري حفظها، وتطبيق إجراءات المعالجة والنقل عليها إلكترونيا لتنفيذ متطلبات العمل يجب الحفاظ على أمنها، حيث أن ضعف الأمن في مجال العمل الالكتروني يعد ضعفا للثقة والتي يجب توفرها ضمن الأنظمة الالكترونية ومستخدميها.

ودولة الإمارات العربية المتحدة قد تجاوزت عقبات التحول إلى الحكومة الالكترونية ، إذ أنها احتلت المرتبة الأولى عربيا في مجال مؤشر الحكومة الإلكترونية سنة 2018 وفقا لما تداولته إحصائيات الأمم المتحدة، فضلا على أنها حققت نجاحا كبيرا في مجال استتباب الأمن المعلوماتي عن طريق مواجهة التهديدات الأمنية من خلال اتخاذ كافة التدابير ووضع السياسات الأمنية المناسبة لها ما أهلها أن تكون تجربة ناجعة تستحق الدراسة للاستفادة منها.

ومن خلال الإطار النظري للحكومة الالكترونية ودراستنا لتجربة دولة الإمارات العربية المتحدة في مجال استتباب الأمن المعلوماتي نخرج بالتوصيات التالية:

- ✓ إن تطبيق الحكومة الالكترونية في الدول النامية لاينبغي أن يكون محاولة لاستعمال التقنيات الحديثة في أتمتة العمليات الروتينية البيروقراطية، ولكن ينبغي أن يكون فرصة لزيادة الكفاءة في أداء الجهات الحكومية على جميع المستويات، مع الحرص على تطوير هذه العمليات وتسهيل وصول المواطن إليها في ظل

الشفافية والخصوصية والموثوقية، وكذا العمل على ضمان حق المواطن في التواصل مع هذه الجهات وإبداء الرأي من خلال خلق فضاءات تفاعلية.

- ✓ ضرورة إعادة هيكلة مختلف الإدارات والهيئات الحكومية بشكل يتماشى مع متطلبات التغيير ويتلاءم مع تطبيقات مشاريع الحكومة الالكترونية وذلك بإعادة هندسة العمليات وتحسينها وتبسيط إجراءات العمل ومراجعة الهياكل التنظيمية للإدارات.
- ✓ ضرورة العمل على زيادة الوعي العام لدى المواطنين والموظفين بأهمية ومزايا تطبيقات الحكومة الالكترونية من خلال وضع برامج إرشادية تحسيسية، مع ضرورة العمل على النهوض بالمواطن الإلكتروني والسعي إلى محو الأمية الالكترونية.
- ✓ يستلزم تحقيق الأمن الالكتروني توفير عددا من المتطلبات أهمها:

- وضع السياسات الأمنية المناسبة لتقنية المعلومات
- تكوين فريق لمتابعة وتطوير المتطلبات الأمنية لبرنامج للحكومة الالكترونية.
- استخدام برامج الحماية وتطبيق أنظمتها في كل المستويات الادارية، مع الاستعانة بالخبراء في المجال التقني والقانوني.
- تطوير أدوات التشفير التي تسمح للأفراد بالدخول على المعلومات والبيانات وكذلك تسمح للادارات بالوصول إلى حسابات الأفراد في التعاملات التي تكون الأنترنت وسيطا لنقلها، مما يمكن المستخدم من الحفاظ على بياناته وحساباته على الأنترنت وتشمل عملية التأمين خصوصية الحكومة والأفراد على حد سواء.