الإدارة الإليكترونية وإشكالية الأمن المعلوماتي

الدكتورة سامية بلجراف
أستـــــاذة محاضـــرة "أ"
جامعة بسكرة (الجزائر)

الباحثة كـــلاش خلـــود
طالبة دكتوراه في الحقوق
جامعة خنشلة (الجزائر)

droit_alg@live.fr

ملخص:

إن تطبيق الإدارة الإلكترونية كان له الدور الأكبر في الاتجاه نحو تحسين الخدمات المقدمة للمواطنين وتسهيل الحصول على الوثائق في أقل وقت ممكن و بأقل التكاليف، إلا أن التوجه و الاعتماد الكلي على المنظومة المعلوماتية قد يجعلنا في مواجهة العديد من المخاطر التي من شأنها المساس بسرية و أمن المعلومات المصرح بها، مما يؤثر سلبا على مصالح و خصوصية المواطن و المؤسسات ، وهو ما سنركز عليه في هذه الورقة البحثية .

Résumé:

les applications de gouvernance électronique ont eu un rôle plus important dans la direction en vue d'améliorer les services fournis aux citoyens et que, dans le but de faciliter l'accès aux documents dans les plus brefs délais، Cependant, en raison de cette tendance, la dépendance totale sur le système d'information nous fait avoir à faire face à de nombreux risques pouvant compromettre la sécurité d'information et la confidentialité des informations autorisées، Il est ce que nous allons nous concentrer dans cet article à travers deux approches pour aborder l'e-gouvernance d'une part et la sécurité d'information de l'autre.

مقدمة:

إن تقريب الإدارة من المواطن أصبح ضرورة حتمية من أجل تسهيل تمكينه من الخدمة العمومية، مما فرض تنافسا بين المؤسسات للانتقال إلى الإدارة الإليكترونية، وأصبحت فكرة مشاركة المعلومة أحد محددات النجاح في كل المؤسسات خاصة في ظل التنافس القائم بين هذه المؤسسات والذي يعتبر الوقت عنصرا أساسيا فيه، غير أن التوجه نحو التوسع في استخدام تكنولوجيا المعلومات يطرح تحديات جديدة أهمها على الإطراق ضمان أمن وسلامة المعلومة.

والمحافظة على الأمن المعلوماتي يهدف بصفة عامة إلى توفير ثلاث أهداف أساسية هي الحفاظ على سرية المعلومة وتوافر المعلومات وحماية محتوى المعلومة، إضافة إلى أهداف أخرى نستطيع أن نعتبرها أهداف مكملة للأولى تتمثل في توفير المصداقية والتأكد من مصدر المعلومة وتحديد الجهات التي لها صلاحية للدخول للمعلومة.

ويمكن تصنيف الجهات المكلفة بضمان الأمن المعلوماتي إلى صنفين الأول يتعلق بالتقنيين الذين يقومون بفحص الشبكات والأنظمة وإجراء الإعدادات الخاصة بحمايتها للتأكد من خلوها من ثغرات أمنية مختلفة، والثاني خاص بالجهات التي تقوم بوضع السياسات والإستراتيجيات الأمنية والإشراف على تطبيقها عمليا.

وأيا ما كانت الصعوبات التي تواجه القائمين على حماية أمن المعلومة، فلا بد من التصدي لها بوضع استراتيجيات متكاملة على جميع الأصعدة القانونية والمؤسساتية والتقنية لحماية وتحصين وضمان أمن المعلومات التي كثيرا ما تطالها أيدي العابثين بها متسببين في الكثير من الأضرار على مصالح الأشخاص والمؤسسات.

وسنحاول من خلال هذه الورقة البحثية الإجابة على السؤال التالي: كيف يمكن للإدارة تحقيق الموازنة بين ضرورة تطبيق الإدارة الإليكترونية ومقتضيات تحقيق الأمن المعلوماتي ؟

أهداف الموضوع:

- البحث في مدى نجاعة الإدارة الاليكترونية كمدخل وآلية للرفع من كفاءة مؤسسات القطاع العمومي.

- الوقوف على مهددات الأمن المعلوماتي في ظل التوجه نحو عصرنة الإدارة وتحديثها وسبل مواجهة هذه المهددات.

وستتناول هذه الورقة البحثية الموضوع من خلال محورين أساسيين:

ـ نتناول في المحور الأول أهم المقومات التي ترتكز عليها فكرة التحول الإليكتروني في تقديم الخدمة العمومية من خلال بيان مفهوم الخدمة العمومية الإليكترونية، أهميتها في مجال تحديث الإدارة، خصائصها ومتطلباتها، وقد عنونا هذا المحور بالإدارة الإليكترونية كمدخل لترقية الخدمة العمومية.

بينما نتناول في المحور الثاني: مهددات الأمن المعلوماتي وسبل مواجهتها، وذلك ببيان أهم صور المساس بالأمن المعلوماتي والآليات المساعدة على مواجهتها.

المحور الأول: الإدارة الإليكترونية كمدخل لترقية الخدمة العمومية

فرض التطور التكنولوجي وزيادة تنافسية المؤسسات والمطالب المستمرة بجودة الخدمة العمومية وسلامة المعلومات ضرورة وضع استراتيجيات للتحول نحو الإدارة الإليكترونية، والذي يرتكز أساسا على عنصر الزمن باعتباره عنصرا أساسيا في نجاح المؤسسة، كما يجب العمل على حسن استغلال الموارد وو العمل على تحسين جودة المخرجات.

أولا – السياق المفاهيمي للإدارة الاليكترونية:

بداية وقبل تعريف الإدارة الاليكترونية حريٌّ بنا أن نعرف الخدمة، والخدمة الاليكترونية، ومميزاتها كمدخل ضروري لتحديد مفهوم واضح للإدارة الاليكترونية.

حيث تُعرف الخدمة بأنها عبارة عن " ذلك الفعل أو الأداء المقدم من طرف جهة معينة إلى جهة أخرى، وهو عبارة عن نشاط اقتصادي يخلق القيمة ويوفر فوائد للعملاء".[1]

أما مصطلح الخدمة العمومية فيشير "إلى تلك الرابطة التي تجمع بين الإدارة العامة الحكومية والمواطنين على مستوى تلبية الرغبات، وإشباع الحاجات المختلفة للأفراد من طرف الجهات الإدارية والمنظمات العامة، أما الخدمة الاليكترونية فهي عملية ترجمة الأداء إلى أرقام خوارزمية عبر الشبكات والوسائل الاليكترونية موجهة نحو العملاء، وبناءً على هذا يمكن القول أن الخدمة الاليكترونية العمومية ما هي إلا تقديم للخدمة من قبل الحكومة باستخدام تكنولوجيا المعلومات والاتصالات في مقدمتها شبكة الانترنت".[2]

---

[1] – جلام كريمة، فعالية الحوكمة في ترقية الخدمة العمومية مع الإشارة إلى حالة الجزائر، الملتقى الدولي حول جودة الخدمة العمومية في ظل الحوكمة الإليكترونية – حالة البلدان العربية ـ، يومي 29 – 30 أفريل 2014، جامعة محمد بوقرة بومرداس الجزائر، ص 06

[2] – نفس المرجع، ونفس الصفحة.

كما يمكن تعريفها أيضا بأنها: "التوصيل الاليكتروني لمعلومات الحكومة وبرامجها وخدماتها عن طريق الإنترنت".[1]

وانطلاقا مما تضفيه تطبيقات الإدارة الاليكترونية على الأجهزة البيروقراطية الحكومية وخاصة منها الخدمية حاولت بعض التعريفات الربط بينها وبين الخدمة العمومية المعقلنة إذ يعرفها البعض بأنها: " تمثل تحولا أساسيا في مفهوم الوظيفة العمومية، بحيث ترسخ قيم الخدمة العمومية، ويصبح جمهور المستفيدين من الخدمة محور اهتمام مؤسسات الدولة، كما يتعدى مفهومها تقديم الخدمة إلى التواصل الايجابي مع الجمهور، وتعزيز دوره في المشاركة، والرقابة من خلال تطوير علاقات اتصال أفضل بين المواطن والدولة ".[2]

في حين ركزت بعض التعريفات على سرعة الوصول إلى الخدمة كأهم خصائص الإدارة الاليكترونية فعرفوها بأنها "مجموعة الأنشطة الحكومية التي تعتمد على الانترنت والاتصالات الاليكترونية عبر جميع طبقات ومستويات الحكومة لتقديم جميع الخدمات والمعاملات للأفراد، والحصول على المعلومات في شتى المجالات بيسر وسهولة".[3]

كما عرفها البعض انطلاقا من شكل العلاقة التي أصبحت تحدد طبيعة التواصل بين الفواعل داخل الدولة الوطنية، وكيف أثر التحول نحو توظيف التكنولوجيا الحديثة على صياغة تلك الروابط باختلاف أنواعها، حيث عرفها البنك الدولي بأنها "مفهوم ينطوي على استخدام تكنولوجيا المعلومات والاتصالات، بتغيير الطريقة التي يتفاعل من خلالها المواطنين، والمؤسسات التجارية مع الحكومة للسماح بمشاركة المواطنين في عملية صنع القرار وربط طرق أفضل في الوصول إلى المعلومات وزيادة الشفافية وتعزيز دور المجتمع المدني".[4]

---

[1] – حدة عطا الله، اتجاهات الحكومة الإليكترونية في ظل أسس ومتغيرات الحوكمة الإليكترونية، دراسة حالة الإمارات العربية المتحدة، يومي 29 – 30 أفريل 2014، جامعة محمد بوقرة بومرداس الجزائر، ص 04.

[2] – عاشور عبد الكريم، دور الإدارة الاليكترونية في ترشيد الخدمة العمومية في الولايات المتحدة الأمريكية والجزائر، رسالة ماجستير في العلوم السياسية والعلاقات الدولية تخصص الديموقراطية والرشادة، جامعة منتوري قسطينة، السنة الجامعية 2009 – 2010، ص 05.

[3] – الداوي الشيخ عماد بوقلاشي، نحو عصرنة الخدمة العمومية في ظل الإدارة الاليكترونية بالجزائر " قطاع التعليم العالي نموذجا "، مداخلة مقدمة إلى الملتقى الدولي حول جودة الخدمة العمومية في ظل الحوكمة الاليكترونية – حالة البلدان العربية –، يومي 29 – 30، ص04

[4] – عاشور عبد الكريم، المرجع السابق، ص 06.

كما تعرَّف بأنها "تلك العملية الإدارية القائمة على الإفادة من الإمكانيات المتميزة للإنترنت وشبكات الأعمال في التخطيط والتوجيه والرقابة على الموارد والقدرات الجوهرية للمنظمة والآخرين بدون حدود من أجل تحقيق أهدافها".[1]

أي أنها استخدام وتوظيف تقنية المعلومات لتحسين أداء الإدارة من خلال تحسين تنفيذ الأعمال والتطبيق الأمثل لها وتسهيل انسياب المعلومة ووصولها إلى المواطن.

ومما هو جدير بالذكر أنه ليس معنى أن يكون للمنظمة موقع على شبكة الويب أنها تدير أعمالها إليكترونيا، وإنما يتطلب الأمر أن تعيد التفكير في أساليب الإدارة، كما يجب أن يكون لديها الرغبة والاستعداد الكاملين للسماح باستخدام التقنيات المستحدثة في تحسين وتطوير وتحديث خدماتها وتحويلها إلى خدمات إليكترونية تراعي فيها السرعة والدقة.[2]

ثانيا – أهمية الإدارة الاليكترونية :

مما لا شك فيه أن الإدارة الاليكترونية تؤدي إلى التخفيف من البيروقراطية، إضافة إلى الكفاءة والجودة في الخدمات المقدمة وتمكين المواطن من الوصول إلى المعلومة من خلال البوابات الاليكترونية، وهو ما يؤدي بالضرورة إلى تحسين العلاقة بين الإدارة والمواطن وإضفاء نوع من الشفافية على نشاطها والحد من الفساد الإداري.[3]

وللإدارة الاليكترونية أهمية كبيرة لاسيما من خلال تحقيق ما يلي:[4]

– اختصار الوقت في التنفيذ وتخفيض التكاليف الناتجة عن المعاملات الإدارية التقليدية حيث يتم العمل الاليكتروني بشكل سريع وآني مما يحقق عناصر النجاح الثلاثة تبسيط الإجراءات، السرعة في الإنجاز ورفع مستوى الخدمات ؛

– تبسيط الإجراءات داخل المؤسسات وهذا ينعكس ايجابيا على مستوى الخدمات التي تقدم إلى المواطن كما تمكّن من تقديم المعلومة للمستفيد بصورة فورية؛

[1] – فتيحة بن أم السعد، دور تكنولوجيا المعلومات والاتصال في تحسين نظام الخدمة العامة في ظل الحوكمة الاليكترونية، ملتقى حول جودة الخدمة العمومية في ظل الحوكمة الإليكترونية حالة البلدان العربية يومي 29 – 30 أفريل 2014، جامعة محمد بوقرة بومرداس الجزائر، ص 04.

[2] – يوسف محمد يوسف أبو أمونة، واقع إدارة الموارد البشرية إليكترونيا في الجامعات الفلسطينية الظامية – قطاع غزة –، مذكرة ماجستير، كلية الدراسات العليا، الجامعة الإسلامية غزة، 2009، ص 26.

[3] – جلام كريمة المرجع السابق، ص 06

[4] – الداوي الشيخ، المرجع السابق، ص 04

- تسهيل إجراءات الاتصال بين الدوائر المختلفة للمؤسسة وكذلك مع المؤسسات الأخرى، وسهولة إدارة ومتابعة الإدارات المختلفة للمؤسسات وكأنها وحدة مركزية ؛

- الدقة والموضوعية في إنجاز العمليات المختلفة داخل إدارة أي قطاع والسهولة والكفاءة في متابعة وإدارة كل الموارد المتوفرة؛

- تقليل استخدام الورق بشكل ملحوظ والتحول نحو الأرشيف الإليكتروني مما يؤدي إلى تقليل أوجه الصرف، وهذا ما يؤثر إيجابا على عمل الإدارة وربح أماكن التخزين والأرشيف ومن ثم ترشيد التكاليف المالية بما يعزز الكفاءة الإقتصادية ؛

- تقديم الخدمات للمستفيدين بصورة مرضية وعلى مدار ساعات اليوم وطوال الأسبوع ؛

- دعم وبناء ثقافة إيجابية لدى كل العاملين وتعميق مفهوم الشفافية والبعد عن المحسوبية، وتحقيق السرعة المطلوبة لانجاز العمل، وبتكلفة مالية مناسبة ؛

- إنجاز المعاملات الإدارية المختلفة بسهولة ويسر واعتماد البريد الإليكتروني بدلا من الطرق التقليدية (الصادر والوارد)، والحفاظ على أمن وسرية المعلومات وتقليل مخاطر فقدها.

كما أنها تُسهِّل إمكانية الوصول إلى المعلومة بأقل جهد بوسائل البحث الآلي المتوفرة، كما تُسهِّل عقد الاجتماعات عن بعد بين الإدارات المتباعدة جغرافيا، وسهولة وصول التعليمات والمعاملات الإدارية للموظفين والمراجعين ومن ثمة تقليص معوقات اتخاذ القرار عن طريق توفير البيانات بدون جهد وفي وقت أقل.[1]

ومن هنا تعتبر الإدارة الاليكترونية تحولا أساسيا في مفهوم الخدمة العمومية بما يرسخ قيم الخدمة العامة، ويصبح الجمهور المستفيد من الخدمة محور اهتمام مؤسسات الدولة وتعزيز دوره في المشاركة والرقابة، كما تتضمن تعديلات هيكلية في البناء التنظيمي للإدارة من خلال زيادة الترابط بين الإدارة والإدارة العليا، ومن ثمة فالإدارة الإليكترونية تعمل على تحويل الأيدي العاملة الزائدة عن الحاجة إلى أيدي عاملة لها دور أساسي في تنفيذ مشاريع الإدارة عن طريق إعادة التأهيل لمواكبة التطورات الجديدة التي طرأت على المؤسسة واعتماد سياسة التعلم المستمر وبناء المعرفة، والاستغناء على

[1]- يوسف محمد يوسف أبو أمونة، المرجع السابق، ص 35.

الموظفين غير الأكفاء وغير المكونين وغير القادرين على التكيف مع الوضع الجديد، وتقليل معوقات اتخاذ القرار عن طريق توفير البيانات وربطها بدوائر صنع القرار.[1]

وتقاس جودة الخدمة العمومية الاليكترونية بمدى إشباعها لرغبات المواطنين من حيث زمن ودقة الأداء والمؤثرات السسيولوجية المصاحبة لذلك، ويمكن تحديد جودة الخدمة من خلال مدركات المستفيد من الخدمة نفسه ودرجة رضاه عنها، والتي تقاس معظمها بكفاءة الموقع الاليكتروني من حيث سهولة الوصول إلى الخدمة، وتواجده على الشبكة بشكل مستمر ودائم مع ضمان الخصوصية والأمان في المعاملات الاليكترونية، وضمان قانونية هذه المعاملات وشرعيتها.[2]

كما تعمل الإدارة الإليكترونية على التقليل من العلاقة المباشرة بين مقدم الخدمة وطالبها لضمان عدم تدخل العلاقات الشخصية في تحديد نوع وحجم الخدمة المقدمة.

ثالثا – خصائص الإدارة الإليكترونية:

إن التحول من نمط الإدارة التقليدي إلى نمط تشكل تكنولوجيا الإعلام والاتصال ركيزته الأساسية يجعل الإدارة الاليكترونية تتميز عن الإدارة التقليدية بسمات وخصائص نستطيع أن نجملها فيما يلي:[3]

❖ زيادة الإتقان: إن الإدارة الإليكترونية كآلية عصرية في عملية التطور الإداري والتغير التنظيمي تمثل منعرجا حاسما في شكل المهام والأنشطة الإدارية التقليدية، وتنطوي على مزايا أهمها المعالجة الفورية للطلبات والدقة والوضوح التام في إنجاز المعاملات، ومن ثمة فإن الإدارة الإليكترونية تؤثر بشكل مباشر على جودة الخدمة المقدمة؛

❖ تخفيض التكاليف وإعادة النظر في الموارد البشرية: رغم أن الإدارة الاليكترونية تحتاج في بداية تطبيقها إلى إمكانيات مادية، إلا أن انتهاج هذا النهج سيوفر

[1] – علاوي عبد الفتاح وآخرون، دور الإدارة الاليكترونية في ترشيد الخدمة العمومية- التجربة الجزائرية كنموذج – ملتقى حول جودة الخدمة الإليكترونية في ظل الحوكمة الإليكترونية – حالة البلدان العربية -، يومي 29 – 30 أفريل 2014، جامعة محمد بوقرة بومرداس الجزائر، ص 06.

[2] – ياسع ياسمينة وتومي عبد الرحمان، تكنولوجيا المعلومات والاتصالات كمدخل لعصرنة وترشيد الخدمة العمومية، ملتقى دولي حول جودة الخدمة العمومية في ظل الحوكمة الاليكترونية – حالة البلدان العربية -، يومي 29 – 30، ص 08.

[3] – عاشور عبد الكريم، المرجع السابق، ص ص 18، 19.

مبالغ مالية معتبرة، حيث لم تعد الإدارة بحاجة إلى عدد كبير من اليد العاملة كما أنه من المهم إعادة تأهيلها وتكوينها ؛

❖ تبسيط الإجراءات: أمام الحاجة للتحديث والعصرنة الإدارية عملت الإدارات على إدخال تكنولوجيا المعلومات إلى مصالحها، وحرصت على استخدامها الاستخدام الأمثل لما لها من إمكانيات وقدرات في تلبية حاجيات المواطنين بشكل مبسط وسريع خاصة في ظل تنوع الفئات التي تستهدفها أنشطة المنظمات العامة، كما استيعاب عدد أكبر من المستفيدين في الوقت نفسه مقارنة بالإدارة التقليدية التي لها قدرة إستيعاب محدودة؛

❖ تحقيق الشفافية: فالشفافية هي محصلة لوجود الرقابة الاليكترونية التي تضمن المحاسبة الدورية والمستمرة على كل ما يقدم من خدمات، إذ تُعرَّف الشفافية بأنها الجسر الذي يربط بين المواطن ومؤسسات المجتمع المدني من جهة والسلطات المسئولة عن مهام الخدمة العامة من جهة أخرى فهي تتيح مشاركة المجتمع بأكمله في هذه الرؤية ؛

رابعا – متطلبات التحول إلى الإدارة الاليكترونية:

بالرغم من مزايا تطبيق تكنولوجيا المعلومات والاتصال في أداء وتوصيل الخدمة العمومية للمواطن، وما تحققه من تطوير في نوع العلاقة التي تربط بينه بين أجهزة الخدمة العمومية إلا أن هناك عوامل أخرى شجعت المؤسسات على التوجه نحو الإدارة الإلكترونية كزيادة المنافسة بين المؤسسات المختلفة، إلا أن هذه العملية تحتاج إلى جهود على نطاق واسع، وضرورة توفر متطلبات عديدة ومتكاملة لتقديم الخدمة الإليكترونية بالصورة المنشودة سواء من قبل المواطنين أو من قبل أجهزة الخدمة العمومية:

1 – المتطلبات الإدارية:

وتتمثل المتطلبات الإدارية فيما يلي:

1 – 1 – وضع استراتيجيات وخطط التأسيس: ويتطلب ذلك تشكيل إدارة أو هيئة لتخطيط ومتابعة وتنفيذ ووضع الخطط لمشروع الإدارة الاليكترونية، والاستعانة بالجهات الاستشارية والبحثية لدراسة ووضع المواصفات المناسبة لذلك.[21]

1 – 2 – القيادة والدعم الإداري: إن اهتمام ومساندة الإدارة العليا لتطبيق تكنولوجيا المعلومات في الإدارات الفرعية والمؤسسة كافة يعتبر أحد العوامل المهمة

[1] – الشيخ الداوي، المرجع السابق، ص 04.

[16] – نفس المرجع ونفس الصفحة.

والمساعدة في تحقيق نجاح تطبيق الإدارة الإليكترونية والدافعة إلى تحقيق جودة الخدمة.[1]

1 – 3 – الهيكل التنظيمي: يتطلب تطبيق ووجود الإدارة الاليكترونية إجراء تغيرات في الجوانب الهيكلية والتنظيمية والإجراءات والأساليب التي تتناسب مع مبادئ الإدارة الإليكترونية، وذلك عن طريق استحداث إدارات جديدة وتحديث الإدارات القديمة.

1 – 4 – تعليم وتدريب العاملين وتوعية وتثقيف المتعاملين: تتطلب الإدارة الاليكترونية إحداث تغييرات جذرية في نوعية الموارد البشرية الملائمة لها، وهذا يعني إعادة النظر في نظم التعليم والتدريب الحالية لمواكبة متطلبات التحول الجديد.

1 – 5 – وضع الأطر التشريعية وتحديثها وفقا للمستجدات: أي إصدار القوانين والأنظمة والإجراءات التي تُسهِّل التحول نحو الإدارة الاليكترونية، وتلبي متطلبات التكيف معها، وهذا يتضمن على سبيل المثال وضع القواعد القانونية النَّاظمة للإجراءات المتعلقة بالتوقيع الاليكتروني والدفع الاليكتروني.[2]

حيث أن غياب الإطار القانوني المنظم يضع مرحلة التحول الإلكتروني أمام العديد من الإشكالات التي تتعلق بنوعية المعلومات المتداولة ومحتواها، والحفاظ على عنصري الخصوصية والهوية وعلى وجه التحديد تلك المتعلقة بالأشخاص، مما أدى إلى تحول هذه الإشكالات القانونية إلى حاجز أمام التحول إلى الإدارة والخدمة العمومية الإليكترونية.[3]

2 – المتطلبات البشرية:

حيث يعتبر العنصر البشري من أهم الموارد التي يمكن استثمارها لتحقيق النجاح في أي مشروع وفي أي مؤسسة لإيجاد كوادر متخصصة وعلى درجة عالية من المهارة المرتبطة بالبنية الأساسية لنظم المعلومات، وعليه يتوجب على موظفو وعمال ومدراء الإدارات

---

[1] – موسى عبد الناصر ومحمد قريشي، مساهمة الإدارة الاليكترونية في تطوير العمل الإداري بمؤسسات التعليم العالي " دراسة حالة كلية العلوم والتكنولوجيا بجامعة بسكرة – الجزائر ـ، مجلة الباحث، مجلة صادرة عن جامعة الحاج لخضر، عدد 09، 2011، ص 90.

[2] – محي الدين مكاحلية وبوفلفل سهام، متطلبات إرساء الحوكمة الاليكترونية كضرورة لترشيد الخدمة العمومية في الجزائر، ملتقى الدولي حل جودة الخدمة العمومية في ظل الحوكمة الإليكترونية حالة البلدان العربية يومي 29 – 0 أفريل 2014، جامعة محمد بوقرة بومرداس، الجزائر، ص، ص 05.

[3] – علاوي عبد الفتاح، المرجع السابق، ص 18.

الاليكترونية التمتع بمستوى عالي من المعرفة والفكر في مجال تكنولوجيا المعلومات والاتصال.[1]

ومن هنا تبرز ضرورة تنمية وتأهيل العنصر البشري للتكفل بمجمل القضايا التقنية المتولدة عن الاستخدامات الرقمية ضمن فضاء اليكتروني متميز وتحديد الاحتياجات الحالية والمستقبلية من الأفراد المؤهلين واستقطاب أفضلهم وأحسنهم تكوينا وإيجاد نظم فعالة للمحافظة عليهم وتطويرهم.

3 - المتطلبات التقنية:

وهي تقنيات تحديد وإثبات هوية المستخدم وصلاحياته ومسؤولياته وتتمثل في البنية التحتية الصلبة للأعمال الإليكترونية والتي تشمل مختلف التوصيلات الأرضية والخلوية عن بعد، أجهزة الحاسب، والشبكات، وتكنولوجيا المعلومات المادية الضرورية لممارسة الأعمال الإليكترونية، إضافة إلى مجموعة الخدمات والمعلومات والخبرات وبرمجيات النظم التشغيلية للشبكيات، وبرمجيات التطبيقات التي يتم من خلالها إنجاز وظائف الأعمال الإدارية، ومن هنا فالإدارة الإليكترونية تتطلب أربع عناصر أساسية هي: عتاد الحاسوب، البرمجيات، وشبكة الاتصالات، ويقع في قلب هذه المكونات صناع المعرفة من الخبراء والمتخصصين الذين يمثلون البنية الإنسانية والوظيفية لمنظومة الإدارة الاليكترونية.[2]

كما يجب العمل على تحسين وتعبئة المواطنين بمزايا هذه التقنيات، وتقديم التسهيلات الضرورية لهم بخصوص اقتناء الأجهزة المساعدة على الحصول على الخدمات المطلوبة مما يفرض ضرورة توفير التمويل الكافي للمشروع.

كما ترتبط المتطلبات التقنية بالأمن المعلوماتي حيث لا يكفي وضع الإطار القانوني بدون تهيئة القاعدة التقنية التي تمكن من إنجاز المعاملات الإليكترونية بأمان.

4 - المتطلبات الأمنية:

تعد مسألة أمن المعلومات وخصوصية البيانات من أهم معضلات العمل الاليكتروني، حيث يتطلب نجاح الإدارة الاليكترونية مستوى عال من توفر الأمن الاليكتروني والسرية الاليكترونية لحماية المعلومات الوطنية والشخصية، وصون الأرشيف الاليكتروني من أي

[1] - محي الدين مكاحلية وبوفلفل سهام، المرجع السابق، ص 05.

[2] - موسى بن ناصر ومحمد قريشي، المرجع السابق، ص 89 .

تغيير أو عبث أو تخريب، والتركيز على أمن الدولة والأفراد إما بوضع الأمن في برمجيات البروتوكول للشبكة أو باستخدام التوقيع الاليكتروني أو بكلمة مرور مضمونة.[1]

5 – متطلبات سياسية:

يجب توفر الرعاية المباشرة والشاملة للإدارة العليا حيث تترجمها وجود إرادة سياسية داعمة لإستراتيجية التحول الاليكتروني ومساندة لمشاريع الإدارة الإليكترونية، عن طريق تقديم العون المادي والمعنوي المساعد على اجتياز العقبات وتطوير برامج التحول الاليكتروني والإدارة الاليكترونية.[2]

خامسا – دوافع استخدام تكنولوجيا المعلومات والاتصالات في الإدارة (التوجه نحو الإدارة الاليكترونية)

لا تقل حاجة القطاع العام إلى التقنية عن حاجة القطاع الخاص إليها، فلدى القطاع العام من الصعوبات الإدارية ما يدفعه دائمًا إلى البحث عن حلول لها، وليس أنسب حلا من تغيير نمط الإدارة نفسه من الأسلوب التقليدي البيروقراطي الجامد إلى الأسلوب الإلكتروني المرن، للخروج من أزمات الإدارة الحكومية التقليدية، إضافة إلى أن كثيرًا من الإدارات الحكومية ليست إدارات خدمية فحسب، فهناك إدارة حكومية تدير مواقع إنتاج مصانع أو مزارع أو مشروعات تابعة للدولة، وهذه تسعى إلى المنافسة وتحتاج إلى ما تحتاج إليه إدارات القطاع الخاص من إمكانات الإدارة الإلكترونية وقدراتها ومزاياها لخوض منافساتها داخل الأسواق باقتدار[3].

ويمكن ذكر أهم أسباب حاجة القطاع العام لتطبيق أسلوب الإدارة الإلكترونية فيما يلي:

❖ إن القضاء على البيروقراطية وتحسين جودة الخدمات في إدارات الدول النامية على غرار الجزائر لا يتم إلا بإتاحة استخدام التكنولوجيا بشتى أنواعها في نظمها الإدارية، بل أصبحت تكنولوجيا المعلومات والاتصالات حتمية فرضتها الأوضاع الاقتصادية الراهنة.[4]

---

[1] – نفس المرجع، ص ص 91 – 92.

[2] – عبد الكريم عاشور، المرجع السابق، ص 25.

[3] – العوض أحمد محمد الحسن، الإدارة الاليكترونية المفاهيم السمات والعناصر " دراسة وثائقية "، المؤتمر العالمي الأول للإدارة الالكترونية: تواصل خلاق مع طفرة الاتصال والمعلومات في عالمنا المعاصر، طرابلس 01 إلى 04 – 06 – 2010، ص 08.

[4] – الداوي الشيخ، المرجع السابق، ص 06.

❖ تردِّي مستوى خدمات كثير من تلك الإدارات وتعقيدها إلى الدرجة التي تستدعي الحاجة إلى تبسيط إجراءاتها، وجعلها أكثر سلاسة ومرونة، وتسهيل تقديمها للمواطنين[1]

❖ حاجة الإدارة الحكومية إلى مزيد من الثقة المتبادلة بينها وبين المواطن، ورغبتها في تهيئة أجواء من الشفافية في دوائر العمل الحكومي، مما يدعو تلك الإدارات إلى التوجه إلى الإدارة الإلكترونية بوصفها نمطًا جديدًا، فيه من الحياد والموضوعية والانضباط ما يعين على تغيير وجهة النظر السائدة لدى المواطن، وتعديل الصورة القديمة للإدارة الحكومية في ذهنه.[2]

❖ حرص الدولة على تنمية كوادرها الوطنية، وتأهيلها بعلوم التقنية الحديثة للاعتماد عليها في إدارة برامج التنمية وخططها المستقبلية للدولة التي ينبغي أن تقف على قدم المساواة مع خطط التنمية وبرامجها في دول العالم، ولن يتم ذلك إلا بتوفير البنية الأساسية التقنية لتلك الكوادر الوطنية من شبكات وقواعد معلومات، مما يتيح الفرص أمام المشروعات التقنية التي ينبغي أن تكون بيئة تنشأ فيها تلك الكوادر.[3]

❖ حاجة الاقتصاد الوطني إلى الدعم ومد يد العون إليه، وليس شيء أقدر من التقنية وتعميم تطبيقاتها على دوائر القطاع العام للإسهام بفعالية في حل كثير من الصعوبات التي تعترض حركة كثير من الصادرات في الدولة، بما يتاح لها في ظل الإدارة الإلكترونية من فرص التواصل مع الأسواق العالمية ومعرفة احتياجاتهم في حال التصدير وأيضًا معرفة أهم وأجود منتجاتها في حال الاستيراد، لذا تبقى الإدارة الإلكترونية خيارًا لا بديل عنه أمام الحكومات التي تسعى إلى حجز موطئ قدم لها في الأسواق العالمية وكسر طوق العزلة المحلية والإقليمية، والاستفادة من وجودها بوصفها إحدى قوى السوق العالمية، حتى لا تتحول إلى سوق استهلاكية فقط تباع فيها بضائع الآخرين، ويُروج فيها لمنتجاتهم المادية وإفرازاتهم الفكرية، دون أن تكون لها القدرة على الرفض أو الاختيار بسبب العزلة، وافتقاد القدرة على التمييز في المفاضلة في ظل سعي الإدارة الحكومية أخيرًا إلى الحصول على منتجات الأسواق الخارجية بأسعار معقولة فإنها بحاجة إلى مساعدة التقنية التي تمنح تلك الإدارات القدرة على خوض تجربة التجارة عالميًا، والتعرف إلى معروضات

---

[1] – حسن بن محمد حسن، الإدارة الاليكترونية بين النظرية والتطبيق، المؤتمر الدولي للتنمية الإدارية نحو أداء متميز في القطاع الحكومي، معهد الإدارة العامة، المملكة العربية السعودية، 01 – 04 نوفمبر 2009، ص 17.

[2] – العوض أحمد محمد الحسن، المرجع السابق، ص 08.

[3] – حسن بن محمد حسن، المرجع السابق، ص 17

الأسواق، واختيار الأفضل والأنسب من عروضها وأسعارها، بعيدًا عن هيمنة الوسطاء ومشكلاتهم، وما قد يلحقونه بالمصلحة الوطنية من خسائر، إضافة إلى أن انفتاح الإدارة الوطنية على العالم سيقضي على الاحتكار، ويجعل الخيارات متاحة أمامها لتكون بديلا إذا ما رفع أحد الموردين الأسعار عليها، وخاصة في السلع التي تمس الاحتياجات اليومية للمواطنين كالسلع الاستهلاكية الضرورية.[1]

❖ تحتاج الإدارات الحكومية إلى خوض تجربة الإدارة الإلكترونية لزيادة قدرة المشروعات الصغيرة والمتوسطة على المشاركة في حركة التجارة العالمية، لكون إدارات الدولة الإلكترونية نافذة تطل منها هذه المشروعات الصغيرة التي يصبح بإمكانها الالتقاء بعملائها في الخارج وتوقيع الاتفاقيات معهم عبر نافذة الدولة، وأيضًا تكون الإدارة الحكومية في موقع معلوماتي مميز ولديها من العلاقات خارجيًا ما يمكّنها من عقد صفقات ناجحة في الأسواق العالمية لصغار المستثمرين، لتقديم منتجات تقبلها السوق العالمية، بعد توفير الدولة مواصفاتها لأصحاب المشروعات الصغيرة، مما يفتح باب التصدير أمام تلك المشروعات ويرفع قدرتها على اختراق تلك الأسواق الدولية بكفاءة وفعالية، ويقلل من تكلفة عمليات التسويق والدعاية والإعلان، مما يزيد من نشاط تلك المشروعات ويسهم بدوره في تعزيز الاقتصاد الوطني، بوصف هذا كله في النهاية مكسبًا يصب في خانة هذا الاقتصاد.[2]

❖ تختصر الإدارة الإلكترونية وقت تنفيذ المعاملات الإدارية المختلفة، وتسهِّل الاتصال بين إدارات الأجهزة الحكومية ومنظماتها، وتوفر الدقة والوضوح في العمليات الإدارية، وترشِّد استخدام الأوراق في المعاملات، إضافة إلى دعم الثقافة التنظيمية لدى العاملين كافة وزيادة الترابط بين الإدارة العليا والوسطى والعاملين، وتوفير البيانات للمراجعين والمستفيدين عامة بصورة فورية، والحد من معوقات اتخاذ القرار.[3]

ورغم أهمية اللجوء إلى تكنولوجيا المعلومات لتسهيل توصيل الخدمة إلى المواطن في صورتها المثلى والذي يعتبر التحدي الحقيقي أمام الإدارة، إلا أن هذا التحدي تعترضه العديد من العوائق تدور أغلبها حول توفير أمن المعلومات وسلامتها وعدم المساس بها، وهو ما سنتناوله في المحور الثاني.

[1] – العوض أحمد محمد الحسن، المرجع السابق، ص 10.

[2] – حسن بن محمد حسن، المرجع السابق، ص 18.

[3] – نفس المرجع، ص ص 18 – 19.

المحور الثاني: مهددات الأمن المعلوماتي وسبل مواجهتها

يمكن تعريف المنظومة المعلوماتية عموما بأنها " نظام متصل أو مجموعة من الأنظمة المتصلة ببعضها البعض، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، وقد عرفتها المادة 02 من القانون رقم 04/15 المتعلق بالتوقيع والتصديق الإلكتروني "بأنها بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية تستعمل كوسيلة للتوثيق"[1].

كما تم تعريف نظام المعالجة الآلية للمعطيات من طرف الفقهاء بأنه " كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها تحقق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية الفنية "، وهذا التعريف يعتمد على عنصرين:

العنصر الأول: مركب يتكون من عناصر مادية ومعنوية مختلفة ترتبط نتيجة علاقات توحدها نحو تحقيق هدف محدد.

العنصر الثاني: ضرورة خضوع النظام لحماية فنية [2].

ولقد ظل مجال أمن المعطيات حتى أواخر السبعينات معروفا باسم أمن الاتصالات والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة الأمريكية بأنه "المعايير والإجراءات المتخذة لمنع وصول المعلومات لأيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات".[3]

فالمقصود بالأمن المعلوماتي: "العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها، ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، أما من الناحية القانونية فإن أمن المعلومات هو محل دراسات

---

[1] – محمد خليفة، حماية التوقيع والتصديق الإلكتروني في ضوء الأحكام الخاصة بحماية أنظمة المعالجة الآلية للمعطيات، ملتقى وطني حول الإطار القانوني للتوقيع والتصديق الإلكتروني في الجزائر، يومي 16/17 فيفري 2016، جامعة محمد الشريف مساعدية، سوق أهراس، ص 04.

[2] – أمال قادة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الجزائر: دار هومه للنشر والتوزيع، 2007، ص 102.

[3] – علوطي لمين، (تحديات الأمن الإليكتروني في المؤسسة)، مجلة أبحاث اقتصادية وإدارية، العدد السادس، ديسمبر 2009، ص 161.

وتدابير حماية سرية وسلامة محتوى وتوفر 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 والانترنت)".[1]

وعموما يمكننا تعريف الأمن المعلوماتي بأنه مجموعة من الإجراءات التي يمكن من خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تتهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

أو هي مجموعة من المعايير التي تحول دون وصول المعلومات المخزنة في الشبكات إلى الأشخاص غير المخول لهم الحصول عليها.

أولا – مكونات الأمن المعلوماتي:

عندما نتحدث عن موضوع "أمن المعلومات" وشبكات المعلومات فإن أول ما يتبادر إلى الذهن هو كيفية الحفاظ على سرية المعلومات، والحديث عن ارتكاب جرائم المعلومات يعني أنه قد تم تسريب لها بحيث حدث انتهاك لهذه السرية، ويرى المختصون أن أمن المعلومات هو عملية معقدة تتألف من مكونات ثلاثة كلها على نفس الدرجة من الأهمية والخطورة ولا يُغني توفير أحدها عن ضرورة توفير الأخرى وهي:[2]

❖ سرية المعلومات: حيث يجب اتخاذ التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة والسرية والتي يفترض أن تكون محمية، ومن بين المعلومات التي يشكل تسريبها أو الإطلاع عليها إخلال بالأمن المعلوماتي تسريب المعلومات لشخصية للأفراد، وتلك المتعلقة بالحسابات المالية لشركة قبل إعلانها الرسمي عنها، والمعلومات العسكرية وغيرها.

❖ عدم حرمان مالك المعلومات من الوصول إليها عند الحاجة إلى ذلك: حيث أن حرمان من له الحق في الحصول على المعلومة أو جعل عملية الوصول إلى المعلومة صعبا وشاقا يخل بالأمن المعلوماتي خاصة إذا تعرضت للحذف أو شل الأجهزة التي تخزن بها المعلومة.

[1] – مصطفى يوسف كافي، الإدارة الإليكترونية، سوريا: دار رسلان، طبعة 2012، ص 431.

[2] – خالد بن سليمان الغثبر ومحمد عبد الله القحطاني، أمن المعلومات بلغة ميسرة، الرياض: بدون دار نشر طبعة 2009، ص 23.

❖ سلامة المعلومات: مما يفرض ضرورة وضع أنظمة حماية كفيلة بحماية المعلومات.

ثانيا – مظاهر الإخلال أو المساس بالأمن المعلوماتي:

يعد مبدأ سرية المعلومات الخاصة من أهم المبادئ التي تحرص الدساتير والقوانين على احترامها وتكريسها بموجب النصوص القانونية، ومن ثمة لا يجوز للجهات الحكومية مراقبة المراسلات والاتصالات إلا للضرورة التي تتعلق بالنظام العام أو الأمن القومي أو الوقاية من الجرائم وبشروط نص عليها القانون، ولحماية حقوق وحريات الغير، ولا يتم الكشف عن المعلومة أو الرسالة أو الاتصال إلا عن طريق السلطة القضائية أو السلطة الإدارية لأسباب يحددها القانون[1].

إلا أنه نتيجة للتطور المعلوماتي الحاصل فقد تعددت وتنوعت مظاهر المخاطر المعلوماتية سواء كانت العمدية منها أو غير عمدية، من سرقات واختلاس أموال واعتداء على كيانات ومعلومات وغيرها، الأمر الذي قد يؤثر بشكل سلبي على معاملات الأفراد ومؤسسات الأعمال واستقرار وتبادل المعاملات الإلكترونية، [2] بإعتبارها الأساس الذي تقوم عليه الحكومة الإلكترونية وبناءً عليه سوف نتناول أهم أوجه المساس بهذه المعاملات.

1- الإختراق المعلوماتي:

إن جرائم الاختراق هي أنشطة الاقتحام أو الدخول أو التوصل غير مصرح به إلى نظام الكمبيوتر أو الشبكة ضد البيانات والبرامج والمخرجات، وتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر وإيذائه والمساس بالملكية، وبالتالي يعرَّف الاختراق المعلوماتي بأنه "فعل غير مشروع يوظف المعرفة العلمية السائدة في ميدان تقنية الحاسوب والمعلوماتية لاقتراف إساءة أو هجوم على الغير"[3].

فهو إذن الدخول أو الاستعمال غير المصرح به في النظام المعلوماتي الذي يتم بواسطة برامج متطورة يستخدمها كل من يملك خبرة في استخدامها، وذلك من خلال توجيه هجمات إلى معلومات الكمبيوتر أو خدماته قصد المساس بالسرية أو المساس

[1] – خالد ممدوح إبراهيم، أمن مراسلات البريد الإلكتروني،الإسكندرية: الدار الجامعية للنشر، 2008،ص70.

[2] – خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الإسكندرية: الدار الجامعية للنشر، 2008، ص 56.

[3] – ضياء مصطفى عثمان، السرقة الإلكترونية (دراسة فقهية)، الأردن: دار النفائس للنشر والتوزيع، 2010، ص 40.

بسلامة المحتوى أو تعطيل القدرة أو الكفاءة للأنظمة للقيام بأعمالها، أيضا الوصول إلى المعلومات والبيانات المخزنة داخل نظام الكمبيوتر دون رضا المسئول ودون علمه، فهو بمفهوم عام إساءة استخدام الكمبيوتر ونظامه عن طريق شخص غير مرخص له باستخدامه والدخول إليه للوصول إلى معلومات وبيانات مخزنة بداخله لاستخدامها في غرض ما.[1]

ولا يشترط صفة معينة في من يقوم بالدخول أو البقاء، كما لا يشترط أن يتم الدخول بطريقة معينة، فيستوجب أن يترتب على الدخول أو البقاء غير مصرح به في أنظمة المعالجة الآلية للمعطيات حذف أو تغيير معطيات النظام، وتتمثل جريمة التلاعب بالمعطيات في إدخال أو تعديل أو إزالة المعطيات، ويؤدي ذلك بشكل حتمي إلى تغيير حالة المعطيات[2].

وقد أصدر الإتحاد الأوروبي توجيها عاما سنة 1995 يتعلق بمعالجة البيانات الشخصية وحرية انتقالها، وحدد مسؤولية من يتعرض لسرية هذه المعلومات، كما اهتمت الهيئات الدولية بإصدار توجيهات بشأن حماية السرية[3].

1-1- دوافع الاختراق: تتحدد الدوافع الرئيسية للاختراق في نقاط تظهر على النحو التالي:

1.1.1 - الدافع السياسي والعسكري: مع بروز مناطق جديدة للصراع في العالم، وتغيير الطبيعة المعلوماتية للأنظمة والدول، أصبح الاعتماد كلية على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية، وبالتالي أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة خطيرة.

2.1.1 - الدافع التجاري: في ظل انتشار التجارة الإليكترونية وبما أن تسويق السلع والمنتجات من طرف الشركات التجارية الكبرى أصبح يتم على الشبكة المعلوماتية، هذا الأمر يجعلها أكثر عرضة للاختراق نظرا لمتطلبات المنافسة التجارية[4].

---

[1] - خالد ممدوح إبراهيم، أمن الحكومة الإلكترونية، المرجع السابق، ص 152.

[2] - محمد خليفة، مرجع سابق، ص 10. أيضا للمزيد من التفصيل أنظر المادتين 394و394 مكرر من القانون رقم 06-23 المؤرخ في 29 ذي القعدة 1427 الموافق ل20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18صفر 1386 الموافق ل08يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية، العدد 84.

[3] - خالد ممدوح إبراهيم، أمن مراسلات البريد الإلكتروني، مرجع سابق، ص70.

[4] - نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي،الاسكندرية: منشأة المعارف للنشر، 2008، ص 143.

3.1.1 - الدافع الفردي: يظهر هذا الدافع بشكل أساسي في أنه يوجد بعض الأفراد في بعض الشركات الكبرى كانوا يعملون كمبرمجين ومحللي نظم تم تسريحهم من أعمالهم للفائض الزائد، فصبوا جل غضبهم على أنظمة شركاتهم مقتحمين ومخربين لكل ما تقع أيديهم عليه من معلومات حساسة بقصد الانتقام، كما يمكن لمصلحي الأجهزة تنزيل برامج صغيرة في الجهاز يمكنهم من الدخول لكل مواقع التواصل التي يستخدمها صاحب الجهاز وحتى التجسس عليه ومعرفة مكان تواجده في لحظة معينة عن طريق برامج تحديد موقع حامل الجهاز أو إرسال رسائل نصية بدلا عن صاحب الجهاز [1].

1-2- أشكال اختراق أنظمة المعلومات:

أما فيما يخص أشكال اختراق أنظمة المعلومات فتتمثل في الصور التالية:

1.2.1 - اختراق الأمن المادي: من أبرز صور الاختراقات في هذا المجال الاحتيال بالمخالفات التقنية، الاحتيال بالالتقاط السلكي، الاحتيال باستراق الأمواج، ابتكار أو إلغاء الخدمة.

2.2.1 - اختراق الأمن الشخصي للأفراد: من أبرز صوره انتحال صلاحيات مفوضو الهندسة الاجتماعية والإزعاج والتحرش وقرصنة البرمجيات.

3.2.1 اختراق الحماية الخاصة بالإيصالات وأمن البيانات: أبرزها الاعتداء على البيانات والاعتداء على البرمجيات.

4.2.1 الاعتداءات على عمليات الحماية: كغش البيانات والاحتيال على بروتوكولات الانترنت والتقاط كلمة السر والاعتداء باستغلال المزايا الإضافية [2].

ولا يقتصر الأمر على التهديدات التي يكون مصدرها خارج المنظمة، والتي تكمن خطورتها في عدم أو صعوبة معرفة المخترق ومدى اختراقه للنظام وحدود خبرته في التخريب وهدفه من وراء ذلك، بل يتعدى الأمر إلى التهديدات النابعة من داخل المنظمة، وذلك من خلال العاملين في المنظمة الذين يطلعون على معلومات معينة غير مصرح لهم بالإطلاع عليها لاستخدامها في تحقيق مصالح معينة، فعند معرفة أحد الموظفين غير المخولين بالدخول إلى النظام "كلمة المرور" الخاصة بالنظام أو الجهاز قد تتعرض المنظمة للتهديد وتسريب المعلومات سواءً بقصد أو دون قصد [3].

---

[1] - نفس المرجع، ص144.

[2] - خالد ممدوح إبراهيم، أمن الحكومة الإلكترونية، مرجع سابق، ص 153.

[3] - منصور بن سعد القحطاني، مهددات الأمن المعلوماتي وسبل مواجهتها، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، الرياض، 2008، ص41.

2- التعدي على الحياة الخاصة:

قد يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة، كما لو قام شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه وبغير إذنه، أو أن يكون تجميع هذه المعلومات بموجب موافقة سابقة من صاحبها، لكن قام الشخص المكلف بحفظها بإطلاع الغير عليها بدون إذن صاحبها كما في حالة الأسرار المودعة لدى المحاسبين أو لدى المحامين[1].

ويمكن القول أن خصوصية المعلومات هي حماية البيانات، وذلك في مواجهة الاعتداءات على البيانات الشخصية، أما الخصوصية بمفهوم عام فتنطوي إضافة إلى خصوصية الاتصالات والبيانات خصوصية المكان والمراسلات العادية والإلكترونية [2].

وهناك تحديات جديدة أوجدتها شبكة الانترنت في مواجهة حماية الخصوصية المعلوماتية، فهي زادت من حجم البيانات المجمعة وأتاحت عولمة المعلومات، وبالتالي فقدان المركزية وآليات السيطرة والتحكم، فتكون المعلومات المعالجة إلكترونيا محلا للتجسس والسرقة والتلاعب قصد الحصول على أموال وخدمات غير مستحقة [3].

ويعتبر انتحال الشخصية من أهم أشكال المساس بالأمن المعلوماتي وتتمثل في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما للاستفادة من مكانة تلك الهوية أو لإخفاء هوية شخصية، ويعتبر تأمين توثيق الهوية عن طريق التوقيع الرقمي من أهم وسائل مكافحة مثل هذه الجرائم.[4]

كما أن هناك مخاطر تتعلق بالمعالجة المعلوماتية للبيانات الشخصية كعدم مراعاة الدقة في جمع البيانات وكفالة صحتها وسلامتها وعدم استعمال المعلومات للغرض الذي جمعت من أجله [5].

---

[1]- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، المرجع السابق، ص 72.

[2] - بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين التحديات التقنية وواقع الحماية القانونية، مجلة الفقه والقانون، العدد43، أفريل 2016، ص 75.

[3]- نفس المرجع، ص 77.

[4]- ضياء مصطفى عثمان، مرجع سابق، ص 41.

[5] - ذياب موسى البداينة، الجريمة الإلكترونية " المفهوم والأسباب "، ملتقى علمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية من 4إلى 6 أكتوبر 2014، كلية العلوم الإستراتيجية، عمان (الأردن)، ص 8.

كما يمكن التلاعب في بيانات الإدارة الالكترونية عن طريق الإدخال أو المحو أو التعديل، حيث يقصد بالإدخال إضافة معطيات جديدة على الدعامة الخاصة به سواءً كانت خالية أم يوجد عليها معطيات من قبل، ويقع هذا الفعل غالبا بمعرفة المسئول عن القسم المعلوماتي.

أما فعل المحو فيقصد به إزالة جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام أو تحطيم تلك الدعامة.

كما يمكن للمسئولين عن حفظ البيانات أن يتلفوا المعلومات التي كلفوا بحفظها داخل جهاز الحاسوب، وذلك عن طريق إتلاف المعلومات أو محوها، الأمر الذي يتطلب تعديل المعلومات المتواجدة أو محاولة استرجاع الملفات المتلفة [1].

كما قد يؤدي المساس بالمعلومات الخاصة والتي في الغالب ما تكون سرية إلى نشرها بشكل مظلل وخاطئ سواءً كانت المعلومات المستهدفة تتمحور حول فرد أو مجتمع أو مؤسسة تجارية أو هيئة علمية أو غيرها، الأمر الذي يؤدي إلى التشهير وتشويه السمعة والنصب والاحتيال الذي يظهر في شكل مشاريع استثمارية وهمية واستخدام أسماء شركات عالمية مشهورة للولوج إلى السوق العالمية [2].

3- الفيروسات:

يعد الفيروس بمثابة برنامج يتم تصميمه بهدف الدخول إلى أجهزة الحاسوب وإحداث الأضرار بها، بعرقلة المستخدم من التوصل إلى حاسوبه أو برامجه أو بياناته أو موارد الشبكة، وتصميم برامج التحطيم أو تغيير البيانات والذاكرة والأقراص الصلبة، وبالتالي فإن الفيروس هو برنامج له القدرة على نسخ نفسه أكثر من مرة يمتاز بقدرته على التخفي وله آثار تدميرية على أنظمة تشغيل الحاسوب لأن عملية النسخ والتكرار الدائم للفاته تجعل هذه الملفات تحل محل الملفات الأصلية الموجودة على القرص الصلب للحاسوب [3]، وتتمثل أهم مشكلة يسببها الفيروس المعلوماتي هو قدرته على الاختفاء والقدرة على الإنتشار والتدمير، كما أنه هناك العديد من أنواع الفيروسات "حصان طروادة، الديدان، القنابل الموقوتة، باب المصيدة، فيروسات الشبكة، فيروسات العتاد " لكن

---

[1] - عبد الفتاح بيومي حجازي، الحكومة الإلكترونية بين الواقع والطموح، الإسكندرية: دار الفكر الجامعي، ط1، 2010، ص 210.

[2] - نسرين عبد الحميد نبيه، مرجع السابق، ص 141-142.

[3] - جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات "رؤية جديدة للجريمة الحديثة "، عمان: دار البداية للنشر، ص 183.

رغم ذلك يمكن التعرف على هذه الفيروسات من خلال قرائن وعلامات عديدة كثقل الجهاز نفسه ويمكن لمستخدم الجهاز لمس ذلك خلال الاستخدام لذا يجب تفادي تنزيل الملفات من المواقع غير المحمية والرجوع إلى الشركات المنتجة للبرامج [1].

ومن هنا لابد من التأكد من وضع مضاد الفيروسات والتأكد من المتصفح نفسه عند الإستخدام وعدم الوثوق في روابط مشبهة وتفادي إدخال المعلومات والبيانات الخاصة وتحديدا المالية.

ثالثا – استراتيجيات حماية أمن المعلومات:

إن أصعب ما يواجه أي إستراتيجية حماية يمكن اللجوء إليها من قبل الدولة هو صعوبة تحديد مكان وجود الخطر، فوجوده في الدولة المعتدى على نظامها الاليكتروني يسهل عملية المتابعة، بينما يفرض وجود الهجوم في دولة أخرى ضرورة طلب المساعدة من هذه الأخيرة، أو عقد اتفاقيات أمنية اليكترونية، وتنظيم حملة مشتركة، فعملية الحماية تتطلب جهوزية تامة لحظة حصول الهجوم الاليكتروني وتنظيم محكم لاحق للهجوم، غير أن الوقاية تعتبر هي الحل الأمثل لحماية الأنظمة اليكترونية، مما يفرض ضرورة اتخاذ جملة من التدابير الحمائية المسبقة منها:

❖ نشر الوعي الأمني المعلوماتي:

إن كل سياسة حماية تنتهجها الدول المختلفة لابد وأن تقترن بحملات للتوعية حول مختلف المخاطر الأمنية الإليكترونية وكيفية تفاديها بالنسبة لكل الفئات العمرية خاصة صغار السن، وتفادي تنزيل برامج الألعاب من مواقع غير رسمية وتفادي التنزيل من المنتديات والتأكيد على ضرورة تنزيل مضادات الفيروسات وتفادي هجمات الإصطياد باستخدام الإميلات المشبوهة، ومنح فرصة للأفراد والمؤسسات للتبليغ عنها والترغيب بذلك من خلال وضع أرقام للتبليغ وتحديد الإجراءات التي قامت بها الحكومة في هذا المجال.

❖ الاستراتيجيات التنظيمية والهيكلية وتطوير الاتفاقيات الأمنية الخارجية:

حيث يتعين على الدولة أن تنشئ إدارة متخصصة في الأمن الاليكتروني تكون تابعة لأجهزة الأمن بحيث يكون تطوير الأمن الإليكتروني ورسم سياسات الدفاع والهجوم في صلب مهامها، والعمل على تطوير الاتفاقيات الأمنية الثنائية والجماعية مع الدول

[1] – منصور بن سعد القحطاني، مرجع سابق، ص 40.

الأخرى والاستفادة من تجاربها في مجال الحماية، ومن المفيد أن يتم تطوير تلك الاتفاقيات الأمنية لكي تشمل قضايا ومواضيع الأمن وأوجه التعاون المحتملة.[1]

❖ اعتماد مفاتيح التشفير:

يجب اعتماد تقنيات تشفير عالية واستخدام أنظمة ثنائية التعرف بحيث يتم التعرف على الشخص بأكثر من طريقة ومن خلال إدخال عدة معلومات قبل الكلمة السرية نفسها والتي تحمل حدا أدنى لمواصفات الأمن والسرية.

❖ محاكاة أساليب الهجوم الإليكتروني:

إن التطور المستمر للجريمة الإليكترونية، واعتماد مرتكبيها على الوسائل المتطورة يجعل من أجهزة الحماية أمام تحدي مواكبة هذه التطورات، ورغم صعوبة ذلك عمليا إلا أنه إذا توفرت البنى التحتية والتكوين المستمر والإستفادة من التجارب السابقة يمكن الوصول إلى محاكاة الجريمة الإليكترونية وتطوير برامج للحيلولة دون وقوعها، مما يفرض ضرورة وجود فرق حماية مكونة قادرة على مواجتها.

❖ التخطيط الأمني الإليكتروني:

يعتمد التخطيط الأمني الإليكتروني على أربعة مراحل أساسية تشكل في مجموعها دورة حياة الخطة الأمنية الفرعية في إطار التخطيط الأمني الشامل للبلاد بدءا بوضع نصوص قانونية متكاملة لمراقبة مختلف المعاملات للحد من إحتمالية العبث بالبرامج وتحديد المسؤوليات والأدوار داخل المؤسسات وتحديد ماهو مسموح وماهو غير مسموح به للمتعامل مع المعلومات ومع نظم المعلومات، وينبثق عن كل مرحلة من مراحل الحماية العديد من الإجراءات التي ينبغي القيام بها للتأكد من أن حدود البلاد الاليكترونية محصنة ضد هذه الهجمات، وتبدأ الخطة بمرحلة اتخاذ جميع الإجراءات الوقائية الصادرة عن وحدة الأمن الإليكتروني في الدولة، ومنها تعميم معايير الأمن والسرية المطلوبتين على كافة إدارات الدولة، وتحضير البنية التحتية للحكومة الإليكترونية بطريقة تضمن عدم وجود ثغرات في الجدار الواقي الإليكتروني والبحث عن نقاط الضعف وتعديلها، وفي المرحلة الثانية يتم مراقبة الأعمال المريبة التي تحدث في الشبكات الاليكترونية، ومنها محاولات دخول متكررة وغير ناجحة، ومحاولة إرسال فيروسات إلى أنظمة الحكومة، وإمكانية التلاعب بالبرمجيات والأنظمة من الداخل، وبنتيجة هذه

[1] – عباس بدران، الحكومة الاليكترونية من الإستراتيجية إلى التطبيق، بدون دولة نشر وبدون دار نشر، الطبعة الثانية، 2007، ص 226.

التحاليل يصار إلى تحديد أماكن ومصادر التهديد، كما يجب على وحدة الأمن الإليكتروني القيام بإجراءات دفاعية ومنها التعاون مع أجهزة أمن الدولة للقبض على المهاجمين في حال تم تحديد موقعهم أو إيقاف هجومهم الإليكتروني، وكمرحلة أخيرة يجب العمل الدائم على تحسين معايير الأمن والسرية عبر استطلاع التقنيات الجديدة والاستفادة من الأخطاء السابقة.[1]

ومن هنا نستطيع القول أنه لا يوجد نظام معلومات آمن، كما لا توجد برمجيات كاملة من حيث السلامة أو من حيث قدرتها على مواجهة الأخطار، مما يفرض ضرورة ممارسة الرقابة والتخطيط من أجل الحفاظ على سرية البيانات والمعلومات وسلامتها.

خاتمة:

مما لاشك فيه أن التقنية ووسائلها ومعداتها قد ساهمت وبشكل كبير في التواصل بين المجتمعات إلا أنه ومن جانب آخر ساهمت فيما يمكن تسميته بعولمة الجريمة، وذلك نظرا لإساءة استخدام معطياتها وتزايد معدلات الاختراقات، الأمر ذاته أدى إلى ظهور الحاجة المتزايدة لاتخاذ وسائل الحماية اللازمة للبيانات والمعلومات التي تزداد أهميتها كلما كانت هذه البيانات تتبع هيئات أمنية مع صعوبة إيجاد وسائل حماية دائمة في ظل التطور التقني المتسارع، ولذا فلابد من تواصل عمليات السعي إلى مواجهة هذه المخاطر والاهتمام بتطوير الأساليب والوسائل التقنية اللازمة لمواجهتها.

و في هذا المجال نقدم مجموعة من المقترحات:

- ضرورة وجود آليات تشفير المعلومات المحفوظة تفاديا للمساس بها.
- وجود هوية إليكترونية لدى كل العاملين في مجال حفظ المعلومات والتي تكون غير قابلة للتعديل والنقل والنسخ.
- ضرورة وجود إدارة مستقلة تعنى بالشؤون المعلوماتية.
- ضرورة توفير البنية التحتية والقانونية لتطوير الخدمات الالكترونية وحماية أمن المعلومات، وتنسيق وتبادل المعلومات بين مختلف المؤسسات والقطاعات حول أمن المعلومات من خلال قناة رسمية، والعمل على بناء مواصفات قياسية ومتطلبات في مجال أمن المعلومات لحماية المؤسسات بشكل عام.
- توحيد إجراءات المتابعة الأمنية والقضائية بين الدول، وتوقيع اتفاقيات التعاون الثنائية والجماعية الأمنية والدفاعية بحيث تشمل البعد المعلوماتي سواء لمنع الاعتداء

[1] – نفس المرجع، ص ص 231، 232.

أو لضبط المجرمين ولتبادل تسليمهم وتبادل الخبرات في هذا المجال، ورفع كفاءة الموظفين من خلال التدريب النوعي المتخصص ومحاكاة أساليب الهجمات الإليكترونية.

- تشجيع المواطن والمؤسسات على التبليغ عن مختلف الإعتداءات التي يتعرضون لها وعقد الدورات وورش العمل الخاصة بأمن وسلامة المعلومات لرفع مستوى الوعي لدى الأفراد والمؤسسات.

- العمل على تقويم مدى كفاءة الأجهزة الأمنية، والعمل على إنشاء خدمات متطورة لتسجيل الأثر الاليكتروني لطالبي الخدمات لتتبع تاريخ الدخول ومرات الدخول والطلب لتسهيل عملية الرقابة، مع التأكيد على العمل على إنشاء وحدات أمنية وطنية متخصصة لها من التدريب والتكوين ما يؤهلها للعمل في مجال مكافحة الجرائم الالكترونية، ومحاولة الاستفادة من خبرات المجتمعات المتطورة في هذا المجال.

- التأكيد على كل المؤسسات على ضرورة وضع كلمات مرور معقدة لضرورات الأمن وحفظ المعلومة.

- توفير محاكم لفض المنازعات المترتبة عن ارتكاب الجريمة الإليكترونية وتدريب قضاتها وزيادة كفاءتهم.

- توحيد الجهود بين مختلف العناصر من العاملين في أمن المعلومات في القطاعات الخاصة والحكومية وتطوير التعاون بينهم.

- ضرورة الاحتفاظ بنسخ أصلية ومحدثة للملفات من خلال وضع قواعد بيانات احتياطية لضمان التواجد المستمر للمعلومات على الشبكة، مع ضرورة تحديث المعلومات باستمرار باستخدام المحدث التلقائي والتزود ببرامج مكافحة الفيروسات، ومواصلة الفحوصات الدورية للأنظمة لكشف الثغرات الممكنة.