محددات الأمن المعلوماتي

مقدمة

يعد الأمن المعلوماتي خيارا حتميا لجهة الإدارة؛ وبالتالي تنعكس تلك الحتمية على النشاط الفردي. فإن لم تفلح جهة الإدارة في الحفاظ على أمنها المعلوماتي؛ سيترتب على ذلك موجات من الاضطرابات في شبكاتها المعلوماتية، مما يؤثر على دقة ومصداقية البيانات والمعلومات، ويحد من إمكانية تداولها.

لذا إن لم يكن الفضاء الإلكتروني والمعلوماتي وسيلة موثوقة بها للاتصال أو التجارة فسيعرض الأفراد كما الشركات عن الاستثمار بل وسيؤثر ذلك على الصعيد الدولي في جهود تطوير اختراعات وتكنولوجيات حديثة، وبالتالي سيكون ذلك عائقًا عن التعاون بين الدول، ويزيد من احتمالية ذلك الفرض التقاعس الحكومي في دول العالم ـ خاصة العالم الثالث ـ عن توفير وتطبيق الإجراءات الدفاعية اللازمة(٣١٠٢).

أضف إلى ذلك أنه رغم التطور الكبير في علم الحاسبات الإلكترونية إلا أن مسألة الأمن المعلوماتي لم تحظ بعد بالتطور المطلوب، فاعتراض المعلومات والتطفل عليها والعبث بها لم يعد حكراً على الجواسيس والخبراء العسكريين بل أصبح هواية للأشخاص العاديين مما شكل في حد ذاته تهديدًا حقيقيًا للمنظمات الحكومية والخاصة(٣١٠٣).

ومما يزيد الإشكالية تعقيداً "الاستخدام العام للبريد الإلكتروني ووصول الجمهور لمواقع الويب "web sites" عبر الإنترنت، وسهولة الوصول إلى المعلومات في النظم المعلوماتية، مع الإمكانيات اللا محدودة لتبادلها وإرسالها بصرف النظر عن بعد المسافات الجغرافية مما مكن المستخدمون من اصطناع فضاء جديد يسمى **"الفضاء المعلوماتي"** والذي يستعمل أساسًا لأغراض شرعية ولكن يمكن أن يخضع لسوء الاستخدام"(٣١٠٤).

"إن الحديث عن أمن المعلومات يملى ضرورة الحديث كمقدمة ضرورية ولازمة عن فكرة الوجود القانوني لغايات الدولة، ذلك أن بعضاً ينكر هذا الوجود من منظور أن الحديث عن مهام الدولة هو الحديث عن وجهة نظر متجاوزة للقانون"(٣١٠٥).

فالأمن بصفة عامة من بين الغايات الأساسية للدولة، ويستقر الفقه على تعريفه بصفة عامة بأنه عبارة عن "الإجراءات والتدابير الوقائية التي تراعى بقصد الحفاظ على الدولة ورقابة نظامها العام المجتمعي وحماية الأشخاص والممتلكات والأموال، فضلاً عن المنشآت العامة والخاصة ناهيك عن المعلومات المحفوظة بل وأيضًا المتداولة"(٣١٠٦).

(٣١٠٢) تمكن المنتهكون الإلكترونيون من سرقة أسماء العملاء، وكلمات المرور المشفرة، وعناوين البريد الإلكتروني، والحسابات الإلكترونية، وبلغ عددها في "ياهو" فقط أكثر من ٥٠٠ مليون حساب، وتعجز التشريعات الحالية في الدول النامية عن مواجهة تلك الاختراقات.

(٣١٠٣) باستطاعة طفل لا يتجاوز عمره ١٢ عامًا إطلاق هجوم إلكترونى على أي مؤسسة من أي مكان في العالم.

(٣١٠٤) د/ طارق إبراهيم الدسوقي عطية: "الأمن المعلوماتي" (النظام القانوني لحماية المعلومات) دار الجامعة الجديدة ٢٠٠٩، ص١٤.

(٣١٠٥) د/ صلاح الدين فوزي، الإدارة العامة بين علم متغير ومتطلبات التحديث ـ دار النهضة العربية ١٩٩٨، ص٣٨٨.

(٣١٠٦) المرجع السابق، ص٣٨٨.

وفى اعتقادنا بوجود تحول في العقد الاجتماعي قد نتج عن التحول في فلسفة الأمن المعلوماتي، مما ترتب عليه أمران في غاية الأهمية:

أولهما: تحول الأمن العام أو الجماعي من نطاقه المحلي إلى نطاق أكثر رحابة واتساعًا ألا وهو النطاق الدولي ،**وثانيهما:** تحول دور الدولة من الدور الحارس إلى الدور المتدخل.

على الصعيد الأول تحول الأمن العام إلى النطاق الأوسع لتضاؤل فكرة الحدود وللتطورات التكنولوجية الهائلة ،وعلى الصعيد الثاني تشعبت وظائف الدولة الحديثة وتعددت وسائل تدخلها في حياة الفرد بصورة لم يسبق لها مثيل، فالمواطن العصري في كل حركة يبديها يتعرض لاختصاصات الدولة فاختصاصات السلطة استغرقت معظم مساحة النشاط الإنساني، كاختصاصاتها فى الدفاع، والأمن الداخلي، ووضع التشريعات الاجتماعية في مجال التعليم والتأمين ضد المرض والبطالة... الخ.

وقد تجلت أهمية الأمن في سياق الآية القرآنية الكريمة الأخيرة من سورة قريش بقوله تعالى "الذي أطعمهم من جوع وآمنهم من خوف" فالأمن بالمرتبة التالية من احتياجات الإنسان بعد الطعام"[٣١٠٧].

مؤدى ما سبق أن الأمن كأحد مكونات النظام العام لم يقتصر على لون واحد فقط بل تعددت صوره ما بين الأمن العسكري، والأمن الاجتماعي، والأمن السياسي، والأمن الفكري، والأمن الاقتصادي، وأمن الجهاز الإداري الحكومي، والأمن العقائدي والقيمي والأخلاقي[٣١٠٨].

(٣١٠٧) الدولة والأمن دراسة بالموقع الالكترونى -مجلة كلية الملك خالد بن عبد العزيز-آخر تحديث ٢٠١٧/٨/١٥ والرابط كالتالى:

http:/www.KKmaq.gov.sa/Detail.asp?InSectionID=١٦٨٩&InNewsItenID =١٥٩٧٣٠.

(٣١٠٨) للمزيد انظر جمال محمد غيطاس: أمن المعلومات والأمن القومي- مكتبة نهضة مصر بدون سنة نشر، ص٢٨، ٢٩.

فالأمن العسكري هو: قواعد بيانات ونظم المعلومات العسكرية والحربية والمحتوى المعلوماتي الرقمي العسكري . **والأمن الاجتماعي هو:** قواعد بيانات ونظم المعلومات المخصصة للتعامل مع الحالة الاجتماعية للمجتمع كإحصاءات ودراسات السكان، **والأمن السياسي هو:** قواعد بيانات ونظم المعلومات والمحتوى الرقمي للأحزاب والبرلمان ورئاسة الدولة والجماعات السياسية المختلفة وأجهزة الأمن السيادية.

والأمن الفكري هو: قواعد بيانات ونظم المعلومات والمحتوى الخاص بالإنتاج الفكري والفني والثقافي، **والأمن الاقتصادي هو:** قواعد البيانات ونظم المعلومات والمحتوى الرقمي لدى البنوك والبورصة والجمارك والضرائب والمالية وغيرها من المؤسسات الاقتصادية الكبرى.

أضف الى ذلك أن مفهوم الأمن لم يعد يقتصر على تأمين المواطن ضد المخاطر التقليدية المحتملة، أو الوجود المادي للدولة وسيادتها الكاملة على أراضيها[٣١٠٩] لكنه توسع نحو آفاق جديدة أهمها صيانة أمن الفرد والجماعات والدولة، والحفاظ على كيانها ووجودها المادي والافتراضي.

إذن على السلطة في العقد الاجتماعي في ظل التطور التكنولوجي الحالي أن تعمل على توازن معادلات إنفاق الدخل القومي وتوزيع الموارد المتاحة بين التهديدات الخارجية "Threats" والتحديات الداخلية "Challenges" وأن تنفق على مستويات ثلاثة **أولها:** الإنفاق على مرفق الدفاع والأمن الداخلي **وثانيها:** رفع مستوى معيشة الفرد **وثالثها:** تثبيت الحكم الذاتي من خلال تأمين الفضاء المعلوماتي حيث إن جوهر الأمن يقاس بالقدرة العسكرية وإمكانية مواجهة التهديدات الملموسة علاوة على توافر مستوى مقبول من الأمن السيكولوجي.

من جماع ماسبق يجب لمعالجة الأمن المعلوماتي أن نتعرض لذلك كالتالي:

الباب الأول: محددات الأمن المعلوماتي، وتحته فصلان:

الفصل الأول: المحددات العملية للأمن المعلوماتي.

الفصل الثاني:المحددات القانونية للأمن المعلوماتى.

الباب الثاني: أثر المحددات المعلوماتية على مفاهيم الضبط الإداري وأساليبه، وتحته فصلان:

الفصل الأول: أثر المحددات المعلوماتية على مفاهيم الضبط الإداري

الفصل الثانى: أثر المحددات المعلوماتية على أساليب الضبط الإداري.

أما أمن الجهاز الإداري الحكومي فهو: قواعد البيانات ونظم المعلومات والمحتوى الرقمي الخاص بالخدمات الحكومية المقدمة للجماهير خاصة مشروعات الحكومة الإلكترونية، أما الأمن العقائدي والقيمي والأخلاقي فهو قواعد بيانات ونظم المعلومات لدى المؤسسات الدينية كالأزهر والأوقاف والمجلس الأعلى للشئون الإسلامية ... الخ.

(٣١٠٩) "إذا أردت أن تعرف سمات نموذج الأمن القومي الجديد فلا تناقش كبار الجنرالات أو أبرز خبراء الدفاع ولكن ناقش خبراء التكنولوجيا والاتصالات ومنظمة التجارة العالمية وأساتذة الاقتصاد.انظر المرجع السابق ص ١٢ في إشارة إلى المفكر الاستراتيجي الأمريكي (Thomas Barner).

الباب الأول

في

محددات الأمن المعلوماتى

تقتضى دراسة الأمن المعلوماتى عند مناقشة اشكالياته على صعيد الضبط الإدارى التعرض إلى العديد من المحددات العملية والمحددات القانونية للأمن المعلوماتى، حيث نتعرض فى الفصل الأول إلى المحددات العملية للأمن المعلوماتي الذى نتعرض فيه الى تعريف كل من المعلومات ،والأمن المعلوماتى ثم علاقة الأمن المعلوماتي بالأمن الفكري والأمن السياسي فى الفصل الثاني نتناول المحددات القانونية للأمن المعلوماتى نطاقات الأمن المعلوماتى،.

وسوف تتم معالجة الفصل الأول كالتالى:

الفصل الأول : المحددات العملية للأمن المعلوماتى، **وتحته خمسة مباحث:**

المبحث الأول:تعريف المعلومات، وفيه مطلبان:

المطلب الأول:التعريف اللغوي للمعلومات.

المطلب الثانى:التعريف الاصطلاحي للمعلومات

المبحث الثانى:تعريف الأمن المعلوماتي:

المبحث الثالث:علاقة الأمن المعلوماتي بالأمن الفكري والأمن السياسي، وفيه مطلبان:

المطلب الأول :علاقة الأمن المعلوماتي بالأمن الفكري.

المطلب الثانى :علاقة الأمن المعلوماتي بالأمن السياسى.

المبحث الرابع:نطاقات الأمن المعلوماتى، وفيه ثلاثة مطالب:

المطلب الأول:البيئة المعلوماتية.

المطلب الثانى:الجريمة المعلوماتية.

المطلب الثالث: الجرائم المعلوماتية على ميزان الضبط الإدارى.

أما فى الفصل الثانى ستتم معالجته كالتالى:

الفصل الثانى:المحددات القانونية للأمن المعلوماتى، وفيه أربعة مباحث:

المبحث الأول:إشكاليات الأمن المعلوماتي

المبحث الأول:إشكاليات المعلومات بين أمنها وتداولها.

المبحث الثاني: مدى تعارض الأمن المعلوماتي مع الخصوصية

المبحث الثالث:مدى ارتباط الأمن المعلوماتي بمبدأ سيادة الدولة

المبحث الرابع:مدى وجود أطر تشريعية ورقابية معلوماتية.

الفصل الأول

في

المحددات العملية للأمن المعلوماتى

يتحدد الأمن المعلوماتى فى العديد من المحاور ،إذ تشكل المعلومات والبيانات نواة ذلك المفهوم بما تمثله من أهمية على صعيد الوحدات الادارية بصفة خاصة ، ونشاطات الإدارة والأفراد على كافة المستويات ، ثم تتأتى بعد ذلك تعريفات الأمن المعلوماتى ، وعلاقته بالأمن السياسى الذى يشكل أداة استقرار الحكومة ، والأمن الفكرى الذى يعد أمنا وقائيا ضد مد النزعات المتشددة ، ثم نختم ذلك الفصل بنطاقات الأمن المعلوماتى وأهمها البيئة المعلوماتية ، ثم الجريمة المعلوماتية ،وتحديد مفاهيمها من وجهة نظر الضبط الإدارى وعلى ميزان ذلك النوع من أنواع الضبط .

لذا سوف تتم معالجة الفصل الأول كالتالى:

الفصل الأول : المحددات العملية للأمن المعلوماتى، **وتحته خمسة مباحث:**

المبحث الأول:تعريف المعلومات، وفيه مطلبان:

المطلب الأول:التعريف اللغوي للمعلومات.

المطلب الثانى:التعريف الاصطلاحي للمعلومات

المبحث الثانى:تعريف الأمن المعلوماتي

المبحث الثالث:علاقة الأمن المعلوماتي بالأمن الفكري والأمن السياسي، وفيه مطلبان:

المطلب الأول :علاقة الأمن المعلوماتي بالأمن الفكري.

المطلب الثانى :علاقة الأمن المعلوماتي بالأمن السياسى.

المبحث الرابع:نطاقات الأمن المعلوماتى، وفيه ثلاثة مطالب:

المطلب الأول:البيئة المعلوماتية.

المطلب الثانى:الجريمة المعلوماتية.

المطلب الثالث: الجرائم المعلوماتية على ميزان الضبط الإدارى.

المبحث الأول

في

تعريف المعلومات

ستتم معالجة تعريف المعلومات كالتالى :

المطلب الأول:التعريف اللغوي للمعلومات.

المطلب الثانى:التعريف الاصطلاحي للمعلومات

المطلب الأول

في

التعريف اللغوي للمعلومات

يمكن تعريف المعلومات لغويًا من خلال البحث في الأصل الذي اشتقت منه وهو كلمة "علم" ويقال "عَلِمَ" "يَعْلَم" ، كما تأتي المعلومات بمعنى المعرفة، ومن المعاني أيضًا ما يتصل بالعلم، أي إدراك طبيعة الأمور، والمعرفة أي القدرة على التمييز والتعليم والتعلم والدراية ... إلخ(٣١١٠).

والمعلومات في اللغة الإنجليزية Information مشتقة من الكلمة اللاتينية "Informatio" وهي تعني عملية الاتصال أو ما يتم إيصاله أو تلقيه كتلقي المعرفة(٣١١١).

أما مصطلح المعلوماتية فقد اشتق من اللغتين الفرنسية والعربية من الأحرف الأولى لكلمتى معلومات ،وأتوماتيك فى إشارة إلى تكنولوجيا وعلم المعلومات(٣١١٢).

(٣١١٠) المصباح المنير للفيومي، دار الحديث، القاهرة، ١٤٢٤هـ/ ٢٠٠٣م، ص٢٥٤.

(٣١١١) د/ دويب حسين صابر، النظام القانوني لحرية الحصول على المعلومات، دراسة مقارنة- دار النهضة العربية ٢٠١٤/ ٢٠١٥، ص١٣، ١٤.

(٣١١٢) مشار إليه في الجريدة الرسمية الفرنسية -عددها الصادر بتاريخ ١٧ كانون الثاني ١٩٨٢ ، نقلا عن: فهد سلطان محمد أحمد بن سلطان-" مواجهة جرائم الإنترنت"، رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة- دراسة مقارنة- ٢٠٠٤ ص١٧.

"اقترح ذلك المفهوم في العام ١٩٦٦ ونال قبول الأكاديمية الفرنسية وظهر للمرة الأولى في ملحق للقاموس الفرنسي Le Robert خلال العام ١٩٧٠.

علاوة على ما سبق ركزت التعريفات الخاصة بالمعلوماتية على عنصرين، وهما **أولًا:** المعلومة، وهي المادة الأولية للمعلوماتية، ويفهم بها كل مادة مُعرفة قابلة للحفظ أو المعالجة أو البث، **وثانيًا:** المعالجة الآلية للمعلومة بواسطة الوسائل المعلوماتية المتدرجة بمجموعها تحت تسمية الحاسب أو الكمبيوتر(٣١١٣).

ومن أهم تلك التعريفات التعريف الفرنسى الذي اعتبر المعلوماتية علم معالجة العقلانية ، ومثال ذلك القاموس الفرنسي فقد عرفها بمجموعة التقنيات المتعلقة بالمعلومة، كنقلها ومعالجتها (٣١١٤).

المطلب الثانى

في

التعريف الاصطلاحي للمعلومات

قام بعض العلماء بتعريف المعلومات بأنها:" تعبير يستهدف جعل رسالة قابلة للتواصل إلى الغير"(٣١١٥) **ويعرفها آخرون بأنها:** الصورة المحولة للبيانات التى تم تنظيمها ومعالجتها بطريقة تسمح باستخلاص النتائج.

أو هي:"مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلاً للتبادل والإتصال "Communication" والتفسير والتأويل Interpretation أو المعالجة "Processing" بواسطة الأفراد أو الأنظمة الالكترونية"(٣١١٦).

وذهب بعضهم إلى تعريفها بأنها:" البيانات الأولية التي غالبًا ما تكون لها قيمة كبرى بالنظر إلى دائرة بثها"(٣١١٧).

ويذهب الفقه ونؤيده في ذلك، إلى أن المعلومات ما هي إلا بيانات في حالة حركة ونشاط، والبيانات ما هي إلا معلومات في حالة سكون(٣١١٨).

فالمعلومات إذن هي المرحلة التالية لتشغيل البيانات أو تحليلها أو استقراء دلالتها أو استنباطها أو تفسيرها.

(٣١١٣) المرجع السابق ص١٧.

(٣١١٤) المرجع السابق ص١٨.

(٣١١٥) د/ حسام الدين كامل الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، يناير ويوليو ١٩٩٠، العددان الأول والثاني، السنة الثانية والثلاثون، ص٤.

(٣١١٦) د. نائلة محمد فريد قورة:- جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية) منشورات الحلبي الحقوقية - بدون سنة نشر ص٩٧.

(٣١١٧) أيمن عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة سنة ٢٠٠٦ ص٤.

(٣١١٨) المرجع السابق ص٢٣.

ويذهب بعضهم إلى التفرقة بين البيانات الأولية والبيانات المجهزة، حيث يتم الحصول على النوع الأول من البيانات دون تدخل مباشر من الأفراد، أما النوع الثاني وهو البيانات المجهزة فتجرى عليه مجموعة من العمليات قبل المعالجة النهائية للبيانات(٣١١٩).

فالمعلومات إذن حلقة يتم توليدها من حلقة أدنى وهي البيانات، وقد صاغ بعضهم تلك الحلقات كالتالي:- (٣١٢٠)

١) **البيانات:** هي الحقائق المجمعة عن طريق الملاحظة أو القياس بحيث يمكن إعادة استخدامها أو تمثيلها في صورة مفردة أو مجمعة لإنتاج معلومات مفيدة يمكن استخدامها.

٢) **المعلومات:** هي بيانات تمت معالجتها بطريقة حسابية أو منطقية لتستخدم في اتخاذ قرارات فعالة .

علاوة على ما سبق تبنت الاتجاهات الدولية التفرقة بين المعلومات والبيانات بأن البيانات هي مجموعة أرقام وكلمات ورموز أو حقائق أو إحصاءات خام لا علاقة بين بعضها البعض ولم تخضع بعد للتفسير أو التجهيز للاستخدام، أما المعلومات فهي المعنى الذي يتم استخلاصه من تلك البيانات(٣١٢١).

ونحن إذ نؤيد ما سبق من تفرقة بين البيانات والمعلومات نرى أن التفرقة نسبية وأن مسئولية جهة الإدارة عن الحماية المعلوماتية نحو النوعين متساوية لسهولة قيام الأفراد والمؤسسات في اعتقادنا بإجراءات التفسير أو التجهيز للاستخدام أو التأويل أوالمعالجة كي تصبح تلك البيانات معلومات ذات فائدة.

علاوة على ما سبق يفرق الفقه عادة بين المعلومات والأخبار حيث تستخدم الأولى رسميًا، في حين تستخدم الثانية على المستوى الإعلامي(٣١٢٢).

مؤدى ما سبق أن البيانات والمعلومات تتعرض إلى خطر واحد، وهو الخطر المعلوماتي وهذا ما سوف نتناوله فيما يلي.

(٣١١٩) د/ ممدوح فرجاني خطاب: النظام القانوني للاستشعار من بعد من الفضاء الخارجي، دار النهضة العربية ١٩٩٣، ص٤١٦.

(٣١٢٠) د/ سمير مصطفى: منظومة الإدارة بالمعلومات، القاهرة ٢٠٠٢ ص: ١ مشار إليه في مؤلف جمال غيطاس: المرجع السابق ص٢٢.

(٣١٢١) المرجع السابق ص٩٧ ومن الاتجاهات التي فرقت التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية عام ١٩٩٢ الخاصة بحماية أنظمة الحاسبات الآلية وشبكات المعلومات حيث عرفت البيانات بأنها مجموعة من الحقائق أو المفاهيم أو التعليمات التي تتخذ شكلاً محددًا يجعلها قابلة للتبادل والتفسير أو المعالجة بواسطة الأفراد أو بوسائل إلكترونية.

Recommendation of the council concerning Guidelines for the security of Information system, ٢٦ November ١٩٩٢.

(٣١٢٢) د/ محمد عبد اللطيف عبد العال: الحظر والرقابة على النشر في القانون الجنائي المصري (دراسة مقارنة تأصيلية تحليلية)- دار النهضة العربية ١٩٩٨ ص٨٥.

المبحث الثانى

في

تعريف الأمن المعلوماتى

بداءة قبل تعريف الأمن المعلوماتى يجدر بنا أن نقوم بتعريف الخطر المعلوماتى، وقد قام بعض الباحثين بتعريفه بأنه: خطر جديد يواجه المؤسسات وجهات الإدارة ويكون مرتبطا بالتطور التكنولوجي، وتدفقات المعلومات(٣١٢٣).

وفي اعتقادنا أن الخطر المعلوماتي يمكن تعريفه بأنه تهديد إلكتروني محتمل يتعلق بالمعلومات والبيانات الرسمية وغير الرسمية للمؤسسات والأفراد والجهات الإدارية والحكومية، ومجاله احتمال التغيير أو التأثير في صورة أو في نشاط أو في سلوك بإرادة مصدر الخطر.

وتتعدد أشكاله مابين التهديد بالاضطراب في تدفق المعلومات، أوالتهديد باستغلال المعلومات الحساسة، والسرية، والملكية المعلوماتية أو التهديد بانتقاء المعلومات لتحقيق أغراض غير شرعية مختلفة ومتعددة أوالتهديد بتدمير المعلومات، أو تدمير مكونها الأساسي.

إذن فإن جملة المخاطر المعلوماتية تتلخص في عملية جمع المعلومات وتخزينها وتوزيعها(٣١٢٤) وهو ما يتطلب القيام باتخاذ تدابير وإجراءات معينة يطلق عليها الأمن المعلوماتي .

ويذهب البعض أن نشأة المخاوف المعلوماتية جاءت بعد تصميم البروتوكول الاساسى لنقل المعلومات على شبكة الإنترنت والمعروف اختصارا باسم (TCP/IP)، وبعد دخول القطاع التجارى للشبكة(٣١٢٥).

أما الأمن المعلوماتي (أو السيبري) فقد ذهب بعضهم إلى تعريفه بأنه: مجموعة الأطر التنظيمية والإجراءات العملية والتقنيات التي تهدف إلى منع الاستعمال غير المصرح به للمعلومات مع الأخذ في

(٣١٢٣) أ.د/حسام الدين كمال الأهوانى ـ المرجع السابق ص٤، وانظر أيضًا: د /محمد على فارس الزغبى:الحماية القانونية لقواعد البيانات وفقا لقانون حق المؤلف-دراسة مقارنة مابين النظام اللاتينى والنظام الأنجلوأمريكى ص ٨٥.

(٣١٢٤) سامية بوقرة: المخاطر المعلوماتية لنظم المعلومات وآليات مواجهتها، مجلة صوت الجامعة ٢٠١٥ - تصدر عن الجامعة الإسلامية في لبنان ، ص٢٢٩ص٢٢٩.

للمزيد من المراجع انظر:=

= – Jean françois Lemetter, Risque, informaion et organisation, Paris, Éditions L'Harmatlan, ٢٠٠٨.

– Olivier Hassid, La Gestion des Risques, Paris, Éditions Dunod, ٢ed, ٢٠٠٨.

– Stewart Mitchell, Managing Information Risk, a director's guide combs, united kingdom, ٢٠٠٩.

(٣١٢٥) د/إياس بن سمير الهاجرى:مقال بعنوان"أمن المعلومات على شبكة الإنترنت" - منشور بمجلة جامعة نايف للعلوم الأمنية حول أعمال ندوة حقوق الملكية الفكرية المنعقدة بالجامعة سنة ٢٠٠٤ ص ١٤٠.

الاعتبار تأمين استمرارية الخدمة، وخصوصية المعطيات والمعلومات، وكذلك الحرص على إيجاد السبل الكفيلة بحماية المستخدم لتلك التقنيات من كافة المخاطر.[٣١٢٦]

ويذهب الفقه المقارن إلى تعريف مختصر للأمن المعلوماتي بأنه "كيفية حماية البيانات والنظم الإلكترونية من الهجماتattack ، أو الفقد loss، أو التداخل compromise.[٣١٢٧]

لذا يتسع مفهوم الأمن المعلوماتي ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية (الأجهزة والبرمجيات وبيانات الأفراد) من التجاوزات والتداخلات غير المشروعة التي تقع صدفة أو عمدًا عن طريق التسلل أو كنتيجة لإجراءات خاطئة ،لذا تشكل المحاور التالية عماد الأمن المعلوماتي:-

١) الأخطاء العفوية غير المتعمدة أثناء تجهيز البيانات.

٢) سرقة المعلومات أو التقاطها وتغييرها بشكل غير مأذون به.

٣) حوادث فقدان أو تغيير المعلومات بسبب تعطيل الأجهزة أو حصول خلل في البرامج.

٤) فقد قدرات إدارة المعلومات نتيجة لوقوع كوارث طبيعية أو صناعية.[٣١٢٨]

ويرى الفقه أن أتمتة الأنظمة في الحكومة الالكترونية automation هي أحد تطورات الإدارة في العصر الحديث ويعني ذلك المصطلح ربط وتكامل جميع موارد المنشأة لتسيير العمل بشكل آلي منظم وهي بالتالي تشمل الجزء المعرفي المكتسب للموظف[٣١٢٩].

وفي اعتقادنا أنه ر غم محاسن الأتمتة في العصر الحالي إلى أن عدم توفير بيئة معلوماتية وإلكترونية آمنة يهدد الأمن المعلوماتي لجهة الإدارة بصورة خاصة والأمن المعلوماتي للدولة بصورة عامة.

(٣١٢٦) د/ عماد يوسف حب الله: ورشة عمل حول "بناء القدرات في مجال الحماية القانونية على الإنترنت ٤-٥ شباط ٢٠٠٩ - الهيئة المنظمة للاتصالات في لبنان - أمن الفضاء السيبراني ص٢ فى إشارة إلي الجهود في مجال الأمن المعلوماتي من خلال لجنة الاتصالات وتكنولوجيا المعلومات التابعة لجامعة الدول العربية، ومثال تلك الجهود القانون الاتحادي لمكافحة الجرائم المعلوماتية الصادر في الإمارات العربية المتحدة = =في شباط ٢٠٠٦، وقانون سعودى صادر في عام ٢٠٠٦ يجرم التصنت، والاعتراض أو الاستفادة من البيانات الإلكترونية دون مسوغ قانوني .

(٣١٢٧) The Emergence of cyber security law, prepared for the Indiana university –Maurer school of law by Hanover Research, February,٢٠١٥ p. ١١.

(٣١٢٨) د/ دلال صادق الجواد. د/ حميد ناصرالفتال- أمن المعلومات - دار اليازوري العلمية للنشر والتوزيع ص١٢.

(٣١٢٩) ناجح أحمد عبد الوهاب: التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية- رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١١ ص١٧٤.

"والمتصفح للتشريعات العربية التي تأخذ بنظام الحكومة الإلكترونية يتبين أن الإمارات العربية المتحدة من أوائل الدول العربية التي أخذت بذلك المصطلح في القانون رقم ٢ لسنة ٢٠٠٢.

وتأسيسا على ماسبق تعمل جهة الإدارة على حماية أمنها المعلوماتى من خلال بروتوكولات معينة كمثال بروتوكول نقل الملفات عن بعد بخلاف الملفات السرية المحمية.[٣١٣٠]

علاوة على ما سبق تقوم عملية تصنيف المعلومات بدور أساسي في تعزيز الأمن المعلوماتي.[٣١٣١] لذا يجدر التمييز بين المعلومات بصفة عامة، والمعلومات التي تعد من قبيل الأسرار حيث تعد من الطائفة الثانية ما يلي:

أولاً: الأسرار الطبيعية أو الحقيقية: ويقصد بها المعلومات أو الوثائق التي تعد بطبيعتها من الأسرار، ولا يعلمها إلا المنوط بهم حفظها وصيانتها لأن مصلحة الدفاع عن البلاد تقتضي أن تبقى سرًا على من عداهم.

ثانيًا: الأسرار الحكمية أو الاعتبارية :وهي المعلومات أو الوثائق أو غير ذلك من الأشياء والتي لا تتصف بالسرية بطبيعتها وإنما وصفت بالسرية لأن إذاعتها وإفشائها يؤدي إلى الوصول لسر حقيقي أو لأنها في حكم الأسرار بمقتضى أمر السلطات المختصة"[٣١٣٢]

وتجدر الإشارة الي تعدد فروض التطور المستقبلي للأمن المعلوماتي ما بين فروض عدة[٣١٣٣] ولكن أهم تلك الفروض هو أن شبكة الإنترنت ستتحول إلى نطاق للصراعات الإلكترونية "conflict

(٣١٣٠) المرجع السابق ص١٧٧.

"وخير مثال على ذلك بيانات المواطنين لدى مصلحة الأحوال المدنية (ميلاد - وفاة - طلاق - قيد عائلي) وهو ما يعرف بالملفات المشمولة بالحماية.

(٣١٣١) المرجع السابق اص١٨٠

يمكن تصنيف المعلومات حسب مدى إتاحتها للجمهور كالتالي:

١) معلومات متاحة للجميع.

٢) معلومات يمكن الاطلاع عليها لبعض الموظفين.=

=٣) معلومات سرية لا يجوز الاطلاع عليها إلا لأشخاص محددين وبموجب كلمة مرور سرية تمنح بموجب الصفة الوظيفية، وذلك للحد من العبث بها ومثالها: بيانات مصلحة الأحوال المدنية والعسكرية، والمعلومات الخاصة بالمواليد والوفيات.

(٣١٣٢) منى فتحي أحمد عبد الكريم: الجريمة عبر الشبكة الدولية للمعلومات: رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة، ص١١٤.

وانظر كذلك د/ حسين عبد الباقي: النظرية العامة لجريمة إفشاء الأسرار في التشريع الجنائي المقارن - رسالة دكتوراه جامعة عين شمس ١٩٧٨.

(٣١٣٣) مروان صالح:المستقبل الافتراضي: السيناريوهات المحتملة لمستقبل الإنترنت: مقال منشور في مجلة حالة العالم" مجلة تصدر عن المركز الإقليمي للدراسات الإستراتيجية بالقاهرة - العدد ١٦ صدر في أبريل ٢٠١٥ ص١٤ وما بعدها .

" ومن أهم التدابير التي اتخذتها الولايات المتحدة الأمريكية كي تحفظ أمنها المعلوماتي إنشاء قيادة فرعية من القوات المسلحة يشار لها اختصارًا "USC YBERCOM" تعمل كمركز قيادة لتنسيق عمليات الفضاء الإلكتروني، وتنظيم الموارد الإلكترونية، والإشراف على التنسيق بين شبكات الدفاع للولايات المتحدة والتخطيط والتنسيق لكل= =الأنشطة الالكترونية وإدارة العمليات من خلال شبكات وزارة الدفاع المعلوماتية، وإجراء عمليات عسكرية في الفضاء الإلكتروني.

على صعيد آخر تعمد بعض الجهات الإدارية إلى إنشاء ما يسمى "حائط النار" "firewall" لحماية الشبكات والتحكم في تدفق المعلومات والبيانات منها وإليها، مثل الصين وأوروبا كي لا تصبح السيطرة بيد قراصنة جماعات الجريمة المنظمة والجيوش الالكترونية التي يمكن أن تدمر منظومة الاتصال والتجارة."

"Domain إذ ستزيد حالات التجسس واللجوء إلى خطر نشر المعلومات والتحكم بها، وإندلاع صراعات حادة ذات أبعاد سياسية بين الحكومات.

ولكن يثور تساؤل مهم عن المضمون الذي يعالجه الأمن المعلوماتي أو بمعنى آخر ما هي الاتصالات؟ هل هى (المحتوى أم بيانات المرور) content V.S. Traffic data

من الأهمية بمكان التفرقة بين طريقة الاتصالات ذاتها وبين محتواها وذلك كالفرق بين بيانات الخطاب المرسل وعنوانه وبين محتوى ذلك الخطاب وكمثال بين رقم المكالمة والرقم المستقبل ومدة المكالمة ووقتها وبين محتوى المكالمة ذاتها.

فهل ينصب الأمن المعلوماتي على المحتوى والمضمون أم البيانات الخارجية فقط كمثال:
Search terms, Port numbers, web page, IP addresses, email address, URLs

في اعتقادنا أن الأمن المعلوماتي ينصب على كل من المحتوى والمضمون والبيانات الخارجية كذلك فطلبات HTTP مثلاً يمكن أن تحوي معلومات عن الإيميل الموجه email address الخاصة بالمستخدم في الصفحات التي قام بتصفحها.

وينقلنا ذلك إلى تعريف التسريب "Leak" بوصفه أحد المخاطر التي تهدد الأمن المعلوماتي للدولة،والذى يمكن تعريفه بأنه الإفصاح عن المعلومات بطريقة غير مشروعة، ويمكن تعريف التسريب الواقع على جهة الإدارة بأنه الإفصاح عن المعلومات المتعلقة بالحكومة فيما يخص النشاط السياسي من خلال قنوات رسمية أو وسائل غير معتادة.[٣١٣٤]

أضف إلى ذلك أنه غالبًا ما يتم التسريب بالاختراق الإلكتروني بغرض التسريب، ويميز ذلك أن المخترق يكون في موقع جغرافي مختلف، وقد يتم ذلك بالنفاذ لسجلات هامة معينة كسجلات المرضى مثلاً، أو الولوج لأنظمة البنى التحتية[٣١٣٥] أو من خلال استهداف نظم المعلومات الاقتصادية أو أنظمة التحكم بخطوط الملاحة الجوية أو البحرية أو البرية أو باختراق نظم الاتصالات[٣١٣٦] وقد يمتد ذلك إلى تدمير الأنظمة المعلوماتية بهدف تخريب نقطة الاتصال أو النظام[٣١٣٧].

---

(١)-Lawerence k. Grossman: – Reflections on leaks in the United States: the media perspectives, International studies In Human Rights Volume ١٦, p. ٧٨.

"Disclosure of information, usually concerning government political activity, through unofficial channels or what some consider improper means ."

(٣١٣٥) كمثال ضرب مولدات الطاقة الكهربائية في حرب الخليج الثانية مما أدى لموت ١٩٠ ألف مواطن لعدم توافر الطاقة الكهربائية.

(٣١٣٦) محمد محمد صالح الألفي: الجرائم المضرة بأمن الدولة عبر الإنترنت: رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١١ ص١٠٠.

(٣١٣٧) المرجع السابق ص١٠٠.

علاوة على ماسبق نجد أن أهمية المعلومات تتعدى الأمن المعلوماتي إلى الأمن القومي، فإذا كانت الدول النامية من أكثر المستفيدين من الطفرة المعلوماتية إلى أنها تبنت آراء مقيدة لجمع المعلومات أو نشرها لذا تطالب دومًا بالحصول على المعلومات الخاصة بأراضيها حتى لا يمكن استغلال ثرواتها بدون علمها أو باتفاقيات غير متكافئة.

وهذا ما ظهر في المبادئ القانونية التي اعتنقتها سواء من حيث الموافقة المسبقة على جمع المعلومات أو على نشرها أو أسبقيتها في الحصول على المعلومات التي تجمعها أنشطة الاستشعار من بعد قبل أي طرف ثالث". (٣١٣٨)

فالأمن أحد محددات الأمن القومي، وإذا كانت فكرة الأمن القومي أكثر غموضًا فإن الأمن المعلوماتي يعد أكثر تحديدًا لكنه أوسع نطاقًا". (٣١٣٩)

المبحث الثالث

في

علاقة الأمن المعلوماتي بالأمن الفكري والأمن السياسى

يتصل الأمن المعلوماتي بالأمن الفكري إذ إن الإخلال بالنظام العام بصورة عامة يمكن تفاديه بالضبط الإداري، لكن تعزيز الأمن المعلوماتي يحتاج فضلا عن وسائل الضبط الإداري إلى وجود الأمن الفكري، علاوة على ماسبق يتصل الامن المعلوماتى بالامن السياسى حيث ترتكز سلطة الحكم فى ترسيخ دعائمها على تعزيز الأمن المعلوماتى،لذا ستتم معالجة ذلك المبحث كالتالى:

"التدمير هو دخول غير مشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي (server – PC) أو مجموعة نظم مترابطة شبكيًا (Intranet) بهدف تخريب نقطة الاتصال أو النظام.

(٣١٣٨) د/ ممدوح فرجاني، المرجع السابق ص٣٠٣.

"ولا تجدي هذه الدول المطالبات القانونية بل عليها الاشتراك في هذه الأنشطة والتعاون مع برامج الدول المتقدمة إن لم يكن في عمليات جمع المعلومات فعلى الأقل في استقبالها بواسطة المحطات الأرضية، مما يستلزم منها موقفًا أكثر مرونة وصولاً إلى اتفاق دولي يحفظ لها حقوقها من خلال هذا التعاون".

(٣١٣٩) يحيط الأمن القومي تساؤلات وتحديدات عديدة ما بين التحديد السياسي والتحديد القانوني ويسيطر على التحديد الأول ما يعرف بالتحديد العسكري، وترجع إشكالية تحديد مفهوم الأمن القومي إلى ما يلي:-

١) أنه فكرة غامضة. =

= ٢) لم تعد الفكرة حكرًا على الفكر العسكري.

٣) ارتباط ذلك المفهوم بجعل الدولة في حالة جاهزية دائمة.

٤) قرارات الدول في ذلك المفهوم ذات طبيعة استثنائية.

For more: ١- Tuner B. Goron, Classic and modern strategy, national security in the nuclear war – London ١٩٩٠, p. ٥.

٢- Lamaby Frank, strategic disarmament and national security, London ١٩٩٧ p. ٥.

المطلب الأول :علاقة الامن المعلوماتى بالأمن الفكرى.

المطلب الثاني :علاقة الامن المعلوماتى بالأمن السياسى.

المطلب الأول

في

علاقة الأمن المعلوماتي بالأمن الفكري

"يجب على الباحث في الأمن السياسي الإلمام بأساليب النشاط المضاد كنوعيات البناء التنظيمي، وأساليب العمل السري، وعلاقات الأفراد في التنظيم ومستوياتهم ومسئولياتهم"(٣١٤٠)، "ولا تعتمد استراتيجيات المواجهة فقط على القدرات المادية والإمكانيات الهائلة في الأسلحة ووسائل النقل والاتصال، وإنما ترتكز في المقام الأول على اختراق آليات الحركة السرية للتنظيمات المتطرفة بالمعلومات، وامتلاك الأسانيد لرد التسويغات الشرعية لتلك التنظيمات".(٣١٤١)

إذن لا يكتمل الدور الفعال للأمن الفكري دون امتلاك المعلومات التي تخص الأفكار والمعتقدات، فالأمن الفكري هو عملية تأمين خلو أفكار وعقول أفراد المجتمع من كل فكر منحرف ومعتقد خاطئ، مما قد يشكل خطرًا على النظام العام والأمن في المجتمع.(٣١٤٢)

فالأمن الفكري يصعب على سلطة الضبط الإداري وحدها تحقيقه إذ يضم في طياته أمنًا معلوماتيًا وأمنًا سياسيًا، ومن أبرز الأمثلة التي تختلط فيها إشكاليات الأمن السياسي والأمن المعلوماتي قيام سلطات الضبط الإداري بالاعتماد على عنصر الملاءمة الأمنية، ويرى الفقه أن الإدارة تمتلك حرية واسعة في ممارسة نشاطها ولا تكون خاضعة لأي التزام قانوني، حيث إنها لا تلتزم بتحديد المبررات التي مارست اختصاصاتها على أساسها.(٣١٤٣)

لذا يرى الفقه الإنجليزي أن سلطة التقدير التى تتمتع بها جهة الإدارة في المملكة المتحدة تزيد كلما كان التشريع غامضًا.(٣١٤٤)

وتجدر الإشارة إلى أن النظام العام ليس مجرد حالة نفسية أو تصوراً ذهنياً يقوم لدى رجل الضبط، بل هو حالة واقعية تستهدف القضاء على كل ما يتهدد أمن وسلامة المجتمع.(٣١٤٥)

(٣١٤٠) د/ محمد فاضل "محاضرات الجرائم السياسية" - معهد الدراسات العربية العليا، القاهرة ١٩٦٢، ص١٦٧، د/ أحمد جلال عز الدين، الإرهاب والعنف السياسي" دار الحرية، القاهرة، ١٩٨٦ ص ٤ وما بعدها.

(٣١٤١) د/ نبيل عبد الفتاح "الوجه والقناع في الحركة الإسلامية والعنف والتطبيع" - دار سيشات للدراسات والتوزيع - القاهرة - الطبعة الأولى ١٩٩٥ ص٣٠.

(٣١٤٢) حيدر عبد الرحمن الحيدر "الأمن الفكري في مواجهة المؤثرات الفكرية - رسالة دكتوراه مقدمة لكلية الدراسات العليا أكاديمية الشرطة المصرية ٢٠٠١ ص٢١ وما بعدها (غير منشورة) مشار له في المرجع السابق ص٣٩٧.

(٣١٤٣) د/ محمد حسنين عبد العال: فكرة السبب في القرار الإداري ودعوى الإلغاء - رسالة دكتوراه، مقدمة لكلية الحقوق -جامعة القاهرة ١٩٧٢ ص٧٢، ٧٣ .

(٣١٤٤) انظر د/ طارق الجيار، الملاءمة الأمنية ومشروعية قرارات الضبط الإداري، منشأة المعارف - الطبعة الأولى ص٢٠٠٩ ص١٦٦.

إذن فالملاءمة الأمنية المعلوماتية تقاس على فكرة الملاءمة بصورة عامة في مجال الضبط الإداري، حيث تقوم على حرية الإدارة في اتخاذ إجرائها فى ضوء الواقع والظروف المحيطة لكنها حرية غير طليقة من كل قيد بل يجب أن تقاس في ضوء أغراض النظام العام وحماية الحقوق والحريات كى يكون تدخلها لأسباب واقعية.

المطلب الثانى

في

علاقة الأمن المعلوماتي بالأمن السياسى

تقوم المعلومات بدور أساسي في تحقيق سلطات الضبط الإداري للأمن السياسي بصورة خاصة، وحفظ النظام العام بصورة عامة عن طريق تجميع المعلومات في مواجهة الدول والكيانات الأخرى بصورة تُمكن الدولة من التحرك من خلال استراتيجية واضحة لكافة المتغيرات والعوامل.

وفي ضوء ذلك يجب أن نحدد تعريفًا للأمن السياسي، حيث ذهب اتجاه إلى تحديده بأنه "جميع التدابير والإجراءات التي تضعها الدولة وتعمل على تطبيقها بواسطة أجهزتها المشكلة لهذا الغرض، وصولاً إلى تحقيق الأمن الوقائي المتمثل في منع وقوع الجرائم، أو الأمن القمعي والمتمثل في كشف وقائع هدم النظام العام في الداخل، بقصد تقديم مرتكبي الإخلال لجهات المحاكمة".(٣١٤٦)

أما الاتجاه الآخر يُعرفه في ضوء الأمن المعلوماتي بأنه:" جهود مبذولة للحفاظ على أسرار الدولة وسلامتها والعمل على منع ما من شأنه إفساد العلاقة بين السلطة والشعب أو تشويه صورة الدولة".(٣١٤٧)

أما الاتجاه الثالث فإنه يركز على أن الأمن السياسي يخص الجرائم التي تقع على الدولة في علاقتها بالمحكومين بغرض الإطاحة بالهيئات الحاكمة أو استبدال النظام الاجتماعي أو السياسي بغيره.(٣١٤٨)

وإن كانت تلك التعريفات متقاربة إلا أن التعريف الأخير –فى اعتقادنا- أقرب للصحة ولكن ما يهم في ذلك السياق أن نؤكد على أنه قد يختلط الأمن المعلوماتي في بعض صوره بالأمن السياسي، وذلك منذ العصور الأولى لتكوين الدولة ،فالتزام جهة الإدارة بتحقيق الأمن بصفة عامة يبني ركنًا أساسيًا للاعتراف بالدولة، فإن تحقق دانت الجماعة الوطنية بالولاء والانتماء.

(٣١٤٥) د/ محمد حسنين عبد العال - المرجع السابق ص٣٤٢.

(٣١٤٦) عبد الوهاب حومد "الإجرام السياسي" - دار المعارف - القاهرة ١٩٦٣ ص٢٦١ مشار إليه لدى د/ طارق الجيار المرجع السابق ص٣٨٦.

(٣١٤٧) عبد الكريم نافع "الأمن القومي" - مطبوعات دار الشعب - القاهرة ١٩٧٥ ص٦٥ مشار إليه في المرجع الوارد في الهامش السابق ص٣٨٧.

(٣١٤٨) د/محمد عطية راغب "التمهيد لدراسة الجريمة السياسية في التشريع الجنائي العربي المقارن - دار النهضة العربية - القاهرة - الطبعة الأولى ١٩٦٩ ص٢٤ مشار إليه في المرجع السابق ص٣٨٧.

"وتحرص الدولة بشتى الوسائل على الحفاظ على أسرارها وعدم تسربها للدول الأخرى سواء أكانت صديقة أم معادية، وهي في سبيل ذلك تتخذ من القوانين والإجراءات ما يكفل صيانة أمنها ونظامها، ومن ناحية أخرى تحاول الدول اختراق الحواجز السرية وجمع المعلومات من الدول المجاورة، أو التي ترتبط معها بمصالح اقتصادية أو عسكرية سعيًا لتأمين حدودها الداخلية أو الخارجية".(٣١٤٩)

أضف الى ذلك يرتبط مفهوم الأمن المعلوماتي بالأمن القومي والسياسي من خلال عنصريه الأمن الخارجي والأمن الداخلي، إذ يقصد بالأمن السياسي على مستوى الأمن الخارجي تجميع المعلومات في مواجهة الدول الأخرى التي تمكن الدولة من التحرك من خلال وضوح الرؤية لكل العوامل والمتغيرات المؤثرة ويتضح ذلك جليًا في الإرهاب الإلكتروني كمثال يجمع بين الأمن المعلوماتي والأمن السياسي، أما على مستوى الأمن الداخلي يتضح ذلك جليًا في اعتقادنا في المواقع الإلكترونية التي تنشر خطابات التطرف والكراهية بما يهدد السلام الاجتماعي والنظام العام، فالأمن السياسي لا يقتصر على الأسلوب الشرطي وتنفيذ القوانين بل يمتد إلى الضبط الإداري الإلكتروني من خلال متابعة الرأي العام والتفاعل الجماهيري في الواقعين المادي والافتراضي كي تكون هناك تدابير وقائية واضحة ضد ما يُخل بالنظام العام.

" فالأمن السياسي كممارسة يرتكز على مجهود علمي منظم يستهدف تحقيق الاستقرار والتوازن الاجتماعيين، وتخليص المجتمع من معوقات تتخذ مظهرًا انحرافيًا يمس سيادة الدولة وسلطات نظامها في تصريف شئون الجماعة الوطنية".(٣١٥٠)

المبحث الرابع

في

نطاقات الأمن المعلوماتى

يثور التساؤل عن الحيز الذي يمكن من خلاله أن يتحقق أمن المعلومات لكي يتحقق الأمن العام بصورة عامة ، وهو مايطلق عليه البيئة المعلوماتية، ومن ناحية اخرى لابد من معالجة أوجه الاخلال بنطاقات الأمن المعلوماتى والتى تتمثل في الجرائم المعلوماتية، ونظرا لخصوصية تلك الجرائم من الناحية العملية لابد من دراستها فى ضوء وسائل الضبط الإدارى،لذا ستكون معالجة ذلك المبحث كالتالى:

المطلب الأول:البيئة المعلوماتية.

المطلب الثانى:الجريمة المعلوماتية.

المطلب الثالث: الجريمة المعلوماتية على ميزان الضبط الادارى.

(٣١٤٩) د/ طارق الجيار - المرجع السابق ص٣٨٥.

(٣١٥٠) المرجع السابق ص٣٨٧.

المطلب الأول

في

البيئة المعلوماتية

يرى البعض أن مناطق أمن المعلومات تنقسم إلى ما يلي:

١) **أمن الاتصالات:** ويقصد به حماية المعلومات خلال عملية تبادل البيانات.

٢) **أمن النظام المعلوماتي:** ويقصد به حماية المعلومات بكافة أنواعها وأنماطها، كحماية نظام التشغيل، وحماية برامج التطبيقات، وحماية برامج إدارة البيانات وحماية قواعد البيانات بأنواعها المختلفة.

أما من حيث أنماط ومستويات أمن المعلومات فإن الحماية تكون كالتالي:

١) **الحماية المادية:** وتخص تلك الحماية كل الوسائل التي تعيق الوصول إلى نظم المعلومات، كالأقفال والغرف المحصنة.

٢) **الحماية الشخصية:** وتخص تلك الحماية وسائل التعريف والتدريب والتأهيل لعناصر الضبط الإداري المنوط بها تحقيق الأمن المعلوماتي.

٣) **الحماية الإدارية:** وتعني تلك الحماية سيطرة جهة الإدارة على إدارة النظم المعلوماتية كالتحكم بالبرمجيات الخارجية أو الأجنبية عن المنشأة، ومسائل التحقيق بانتهاكات الأمن، ومسائل الإشراف والمتابعة لأنشطة الرقابة.

٤) **الحماية الإعلامية المعرفية** :وتخص تلك الحماية السيطرة على إعادة إنتاج المعلومات وعلى عملية إتلاف مصادر المعلومات الحساسة عند اتخاذ القرار بعدم استخدامها.[٣١٥١]

علاوة على ماسبق يرتكز الأمن المعلوماتي على نجاح آلية التوثيق الإلكتروني والتي تعتمد في الأساس على بيئة تقنية يمكن للعناصر التالية أن تحققها، وهي كالتالي:

١) التوثيق أو التحقق من المستخدم.

(٣١٥١) د/ محمد فهمي طلبة وآخرون : فيروسات الحاسب وأمن البيانات ص٢٢١، مرجع مشار إليه في مؤلف د/ أيمن عبد الله فكري، المرجع السابق ص٥٠٨.

" لذلك يرى الفقه أن الأمن المعلوماتي هو "الإحساس المجتمعي الفعلي والتخيلي بعدم وجود تأثير لتهديدات طبيعية أوافتراضية لبناء المجتمع المعلوماتي، وخاصة الحساسة منها في جوانبها المختلفة، سواء كان مصدرها داخليًا أو خارجيًا، وتستدعى التأهب والفعل الجماعي والرسمي لمواجهتها".

٢) التصديق: أي التأكيد على السماح بالوصول إلى المعلومات الإلكترونية للأشخاص المحددين فقط.

٣) السرية: وتعني تأكيد عدم إفشاء المعلومات إلى الأطراف غير المصرح لها بالاطلاع على تلك المعلومات.

٤) التكامل: ويعني التأكد من عدم وجود تعديل أو تلاعب بالبيانات أثناء نقلها.(٣١٥٢)

المطلب الثانى

في

الجريمة المعلوماتية

تعد الجريمة المعلوماتية أحد فروع الجريمة السيبيرية Cyper Crime أو الجريمة الإلكترونية، فقد كان الأمر يرتبط ذهنيًا أو واقعيًا بالجريمة التي تقع من خلال الكمبيوتر Crime by computer ولكن نتيجة للتطور التكنولوجي الرقمي لم يعد يقتصر الأمر عند ذلك النوع من أنواع الجريمة السيبيرية، بل امتد إلى إضافة مصطلحات أخرى. (٣١٥٣) وتشكل الجرائم المعلوماتية ضد جهة الإدارة أخطر تلك الأنواع حيث يقصد بها الجرائم ضد المصلحة العامة إذ أن الحق المعتدى عليه في تلك الحالة هو المجتمع في مجموع أفراده، ومثالها الإخبار الخاطئ عن جرائم الحاسب، والعبث بالأدلة القضائية والتأثير فيها، وتهديد السلامة العامة، وبث البيانات من مصادر مجهولة، وجرائم تعطيل الأعمال الحكومية، وجرائم تعطيل تنفيذ القانون، والإرهاب الإلكتروني، والأنشطة الثأرية الالكترونية. (٣١٥٤)

مؤدى ما سبق يمكن تصنيف هجمات الأمن المعلوماتي إلى نوعين كالتالي:-

١) **هجمات الأمن المعلوماتي السلبية** ومثالها اعتراض الرسائل بشكل سلبي، ويمكن أن يسمى بالهجوم على السرية، ويكون ذلك من خلال التصنت وغيره.

(٣١٥٢) د/ عبد السلام هابس السويفان:إدارة مرفق الأمن بالوسائل الإلكترونية - دراسة تطبيقية -دار الجامعة الجديدة- ص١٥٠ وما بعدها.

(٢) Jonathan clough: principles of cybercrime–second edition –Cambridge press ٢٠١٠. p.٩ "other variants include "digital" electronic (or, virtual, IT, high tech "and technology – enabled crime.=

= for more see :

S. W. Brenner:cyber crime metrics. Old wine, new bottles? ٢٠٠٤ (٩) Virginia Journal of law and technology p. ٤

(٣١٥٤) محمد محمد صالح الألفي: المرجع السابق ، ص١٠٠.

٢) **هجمات الأمن المعلوماتي النشطة**، ومثالها: مقاطعة الرسائل الإلكترونية أو القيام بتعديل الرسالة الأصلية قبل وصولها، **ومثالها أيضًا:** الهجوم الملفق.(٣١٥٥)

من ناحية أخرى يطلق بعضهم على أوجه الإخلال بالأمن المعلوماتي مصطلح "جرائم تقنية المعلومات وقد عرفوا جرائم تقنية المعلومات بأنها أفعال غير مشروعة يتم إرتكابها بأحد وسائل تقنية المعلومات أو عليها تستهدف إضرارا بحق أو بمصلحة محمية تشريعيًا.(٣١٥٦)

إذن قد تقع الجرائم المعلوماتية على حقوق فردية أو على حقوق تخص جهة الادارة ككل كالجرائم التي تقع على مصلحة عامة كالإتلاف المعلوماتي لأجهزة الحاسوب الحكومية، أو جرائم الإرهاب الإلكتروني، أو جرائم التجسس الإلكتروني.

ولكن كيف تشكل الجرائم المعلوماتية إخلالاً بالأمن المعلوماتي؟

يمكن الإجابة عن ذلك بالتعرض لإشكاليات الضبط الإداري في مثل تلك الجرائم، وما يتعلق بها من المساس بالحريات إذ لا يبدو المجتمع الدولي قادرًا على ضبط ورقابة المعدلات المرتفعة للجرائم الإلكترونية فضلاً عن الوقوف أمام جمعيات الحقوق المدنية المنادية بمزيد من الحريات، وإلغاء الرقابة المسبقة، ".(٣١٥٧)

فإذا كانت الدول قد استطاعت الحد من الاتصال والتبادل في أوقات مضت تحت ستار الحماية لأمنها القومي والاقتصادي وغيره، إلا أنها لم تعد كذلك الآن في ظل عصر السماوات المفتوحة، لدرجة يمكن القول معها أن سيادة الدول الإقليمية قد انحسرت عن الإقليم الفضائي أو الهوائي، واقتصرت على إقليمها الأرضي والمائي فقط.(٣١٥٨)

المطلب الثالث

في

الجرائم المعلوماتية على ميزان الضبط الإدارى

(٣١٥٥) المرجع السابق ص١٢١.

(٣١٥٦) د/ حسين بن سعيد الغافري: منظومة سلطنة عمان التشريعية لمكافحة جرائم تقنية المعلومات ٢٠١١، دار النهضة العربية ص٤.

(٣١٥٧) د/ عبد الرحمن الجيران: اختلاف المفاهيم بين الشرق والغرب - دار إيلاف الدولية للنشر والتوزيع ٢٠١٥ ص٦٤.

"ولا شك أن عالم الاتصالات والشبكة العنكبوتية وما أنتجه من جرائم إلكترونية، هي نتيجة طبيعية للتزاوج بين ثورة المعلومات ومد العولمة الجارف، فتدفق المعلومات وسرعتها وكميتها وتخزينها في مكان واحد مع تيسير التصرف بها، إذا أضفنا إليه تيار العولمة وما نتج من تداخل في المفاهيم، واختلال في القيم واضمحلال كثير من الأخلاق والمبادئ سنصل فعلاً إلى مجتمع مشاع، لا يمكن التحكم في مساراته"

(٣١٥٨) د/ أحمد عبد الكريم سلامة : الانترنت والقانون الدولي الخاص - بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت - مركز الإمارات للدراسات والبحوث - من ١-٣ مايو ٢٠٠٣ - ص١.

تكمن صعوبة مواجهة الإخلال بالأمن المعلوماتي بسبب خصائص الجرائم المعلوماتية التى تتصف بالعديد من الخصائص التي تجعلها عصية على الضبط الإداري بالمفهوم التقليدي ومن تلك الخصائص ما يلي:

١) الطابع الفني الهادئ:-

تتصف تلك الجرائم بأنها جرائم فنية يرتكبها شخص ذو خبرة عالية في مجال التقنية المعلوماتية، علاوة على أنها لا تحتاج إلى العنف كالجرائم التقليدية، كما أنها تنطوي على أساليب غير تقليدية لذا يمكن وصفها بالوباء. (٣١٥٩)

٢) **الطابع المكاني**:-

تتصف تلك الجرائم بأنها لا يحدها مكان إذ يمكن لأي شخص بأى مكان أن يرتكب الجريمة في أي مكان آخر، مما قد يثير مشاكل عدة فيما يخص القانون واجب التطبيق علاوة على احتمالية تعارض وظائف الضبط الإداري على الصعيد الدولي.

٣) **الطابع الاقتصادي**:

علاوة على ماسبق عادة ما تنجم خسائر اقتصادية جراء الجرائم المعلوماتية على الصعيد الحكومي وعلى الصعيد المالي للمؤسسات التجارية والاقتصادية خاصة إذا أخذنا في الاعتبار تدني نسبة الإبلاغ عن تلك الجرائم لعدم زعزعة ثقة العملاء.

وفي اعتقادنا أن نتائج الجريمة المعلوماتية قد تؤدي للتأثير على سمعة الدولة على المستويين المحلي والدولي، حيث قد ترتكب تلك الجرائم بدافع الرغبة في قهر النظام السياسى ،وإحراج جهة الإدارة أكثر من شهوة الحصول على الربح المادي. (٣١٦٠)

من جماع ماسبق يعد الأمن المعلوماتي الحكومي أهم وعاء للأمن المعلوماتي للدولة ككل نظرا لتعلقه بالنظام العام، ولذا تشمل طائفة الجرائم المعلوماتية ضد الأمن المعلوماتي الحكومي كل جرائم تعطيل الأعمال الحكومية وتنفيذ القانون، والإخفاق في الإبلاغ عن جرائم الكمبيوتر، والحصول على معلومات سرية، والإخبار الخاطئ عن جرائم الكمبيوتر، والعبث بالأدلة القضائية، وتهديد السلامة العامة، وبث البيانات من مصادر مجهولة، والإرهاب الالكتروني، والأنشطة الثأرية الإلكترونية أو أنشطة تطبيق القانون بالذات. (٣١٦١)

وهناك العديد من المخاطر الأخرى التي تهدد الأمن المعلوماتي لجهة الإدارة كالتالي:

(٣١٥٩) د/ ذياب البداينة: الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن ٢٠٠٢ ص١٠٣ .

(٣١٦٠) مثال ذلك ما تعرضت له امتحانات الثانوية العامة في مصر من تسريبات هددت سير العملية التعليمية، وأخلت بمفهوم النظام العام." ، حيث يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم ومستوى براعتهم، وتزداد الدوافع لدى الشباب الذي يحاولون كسر حواجز الأمن لأنظمة الحاسب الآلي وشبكات المعلومات"

(٣١٦١) د/ أيمن عبد الله فكري، المرجع السابق ص١٠٠.

١) **اختراق النظم:** ويكون ذلك عن طريق دخول شخص غير مخول له بالدخول حتى وإن لم يؤثر ذلك سلبيًا على النظام.

٢) **زراعة نظم الضعف:** ويكون ذلك باستخدام الشخص غير المخول لـه بالـدخول باستخدام النظـام بزرع مدخل ما يمكنه من اختراق النظام ومن أمثلة ذلك (فيروس حصان طروادة).

٣) **مراقبة الاتصال:** ويكون ذلك عن طريق مراجعة إحدى نقاط الاتصال بدون اختـراق الحواسب الآلية.

٤) اعتراض الاتصالات.

٥) إنكار الخدمة. (٣١٦٢)

لذا تعمل الحكومات على حماية البنية التحتية الحيويـة، وتشمل تلك البنيـة المعلومـات والاتصـالات والبنـوك والمـاء والصـحة العامـة وخـدمات الطـوارئ، والطاقـة، والنقـل، والصـناعات الكيماويـة، والمـواد الخطرة. (٣١٦٣)

ويثور التساؤل عن صور الإخلال بالأمن المعلوماتي لجهة الإدارة بصورة خاصة.

(٣١٦٢) محمد محمد صالح الألفي، المرجع السابق ص ١٢٠

للمزيد انظر:

- محمود الرشيدي: الجرائم الالكترونية والتأمين الالكتروني "قضايا المركز الدولي للدراسات المستقبلية والاستراتيجية العدد ١١ السنة الأولى، نوفمبر ٢٠٠٥، ص٣٠-٣٢.

وكذلك محمد أمين الرومي: جرائم الكمبيوتر والانترنت - دار المطبوعات الجامعية، الإسكندرية ٢٠٠٤.

(٣١٦٣)" ومن أوائل الدول التي عملت على هذا النحو في التشريعات العربية الإمارات العربية المتحدة، حيث جاء القانون الاتحادي الإماراتي لسنة ٢٠٠٦ بوجوب الحفاظ على بيانات الحكومة الاتحادية والحكومات المحلية "

يقصد بالبيانات الحكومية في المادة الأولى من القانون الاتحادي الإماراتي: البيانات الحكومية الاتحادية وبيانات الحكومات المحلية والهيئات والمؤسسات العامة الاتحادية والمحلية، بل عمد المشرع في المادة(٢٢)من القانون إلى توسعة مفهوم البيانات الحكومية بأنها تشمل الدخول بدون وجه حق إلى موقع أو نظام معلوماتي بقصد الحصول على بيانات أو معلومات سرية، والمتتبع لمسارات التجريم في ذلك القانون عند تعلق الأمر بالأمن المعلوماتي لجهة الإدارة يجد التجريم التالي:

- تجريم إيقاف أو تعطيل الشبكة أو تدمير وحذف البيانات (المادة ٦ من القانون).
- التدخل في القطاع الطبي بإتلاف الفحوصات الطبية (المادة ٧ من القانون).
- إعاقة الوصول لبيانات ومعلومات الشبكة المعلوماتية (المادة ٥ من القانون).
- الإضرار بالنظام العام الأخلاقي الآداب العامة (المادة ١٢ من القانون).
- الإضرار بالأمن العام عن طريق ترويج المخدرات والمؤثرات الفعلية (مادة ١٨ من القانون).
- الإضرار بالنظام العام والآداب العامة عن طريق ترويج أفكار وبرامج معينة (مادة ٢٠ من القانون).
- الإضرار بالنظام العام عن طريق الإرهاب الالكتروني (م ٢١ من القانون).

في الواقع يمثل القرصان الإلكتروني السياسي (أو مخترق المعلومات ذات الطابع السياسي) أخطر أنواع المخترقين الإلكترونيين الذين يهددون الأمن المعلوماتي لجهة الإدارة والأمثلة الإلكترونية على ذلك عديدة(٣١٦٤)

ومن أمثلة مخترقي المعلومات السياسية دوليًا ما أعلنته وزارة العدل الأمريكية من إدانة خمسة ضباط اشتركوا في عملية سرقة معلومات وبيانات سرية تخص مجموعة من الشركات الأمريكية. (٣١٦٥)

وعلى الصعيد المقابل ألقت الإدارة الأمريكية بتهمة الهجوم الإلكتروني على شركات صينية لشبكات الهواتف النقالة بغرض سرقة ملايين الرسائل النصية.(٣١٦٦)

ولا يقتصر الأمر على مجال التجارة والاتصالات بل امتد ليشمل الإخلال بالأمن العام بصفة خاصة وتهديد النظام العام المادي بصفة عامة. (٣١٦٧)

علاوة على ماسبق يرى الفقه المقارن أن من أخطر أنواع الهاكرز الذين ينتهكون الأمن المعلوماتي لجهة الإدارة هو النوع الذي يقوم بسرقة المعلومات الحساسة (التجسس).

Net spoinage (theft of confidential information)

فرغم تعدد أنواع القراصنة الإلكترونيين(٣١٦٨) إلا أن ذلك النوع إلى جانب القرصان الإلكتروني السياسي والقرصان الإلكتروني الإرهابي يمثلون أخطر أنواع القراصنة الذين يهددون الأمن المعلوماتي لجهة الإدارة.

---

(١) Steven Philippsohn, Trends in cyber crime – An overview of current financial crimes on the internet, computers & security, ٢٠ (٢٠٠١) p. ٥٤.

تم استغلال الهجمات الإلكترونية داخل إطار الخلافات السياسية كمثال الأزمة بين كوسوفو وصربيا، واكتشاف اليابان وجود هجمات كيميائية من جماعة AUM على محطات المترو هناك، وكذلك الهجمات على مواقع مثال Yahoo, CNN, Amazon, ZD, eBay وكلها مواقع تجارية شهيرة لذا عمد الرئيس الأمريكي "كلينتون" وقتها لاعتماد ٢ بليون دولار أمريكي لتعزيز الأمن المعلوماتي الأمريكي.

(٣١٦٥) مروان صالح، المرجع السابق ص١٥." ، وطالت تلك الهجمات عددا من مقاولي الدفاع والأمم المتحدة، واللجنة الأولمبية الدولية في منتصف عام ٢٠٠٦، بل وطالت الهجمات بيانات مهولة، كمثال سرقة مخططات التصنيع، ونتائج الاختبارات، وخطط العمل، ووثائق التسعير، واتفاقات الشراكة، ورسائل البريد الالكتروني، وقوائم الاتصال"

(٣١٦٦) المرجع السابق ص١٦ "نقلا عن تسريبات ادوارد سنودن مسئول الأنظمة السابق لوكالة الاستخبارات المركية "CIA" حيث قرر أن وكالة الأمن القومي "NSA" تستهدف الشبكات الرئيسية "Network Backbones".

(٣١٦٧) في عام ٢٠١١ ظهر الجيش السوري الإلكتروني SEA والذي قام بتخريب العديد من المواقع عن طريق البرمجيات الخبيثة، ويبدو أن تلك الخلية الإلكترونية لها تسلسل هرمي واضح المعالم، يتكون من قادة وخبراء تقنيين، وأذرع إعلامية ومئات من المتطوعين، ينتمي العديد منهم إلى الجمعية العلمية السورية المعلوماتية حيث كانوا يعملون بنظام القرصنة الجماعية المنظمة حكوميًا.

حيث يعمل ذلك النوع الأول من القرصنة على سرقة المعلومات الحساسة وبيعها لمن يقوم بالدفع بأعلى سعر ويطلق عليه القرصان المتجسس (Net spoinage theft of confidential information) وقد واجهت الجهة الإدارية في الصين ذلك. (٣١٦٩)

أما النوع الثاني وهو الإرهاب الإلكتروني أو السيبري (cyber - terrorism) يتزايد خطره من خلال الأسلحة الإلكترونية على جهة الإدارة والتي تتمثل في القنابل المنطقية logic bombs والقنابل الكهربائية المغناطيسية eletromagnetic bombs، والتي تتاح لدى العصابات الإلكترونية، والتي يمكنها أن تعطل الأجهزة والمراسلات الحكومية وغيرها إذا لم يتحقق تهديدها وابتزازها للمؤسسات أو الهيئات الخاصة والعامة. (٣١٧٠)

(٣١٦٨) Steven Phillippsohn, op. cit., p. ٥٥, ٥٦

"The types of criminal Hackers are:–

١) Hackers A) External Hacker.

B) Hacking to highlight lack of security.

٢) Internet Hackers.

٣) Internet Saboteur.

٤) Net spoinage (theft of condifential Information).

٥) E. Theft.

٦) Credit Card fraud.

٧) Pump & Dump.

٨) Cyber Terrorism.

٩) Cybor privacy.

١٠) Virus.

١١) Fraudulent internet Banking sites.

(٣١٦٩) قامت الجهة الإدارية في الصين بغلق ١٢٧ مقهى إنترنت لقيامها بنشر أسرار الدولة وبث العديد من المعلومات شديدة السرية.
وبمتابعة المواقع الإخبارية والإلكترونية فى ٢٢مايو ٢٠١٧ نجد وجود صدى واسع لهجوم "الفدية الخبيثة" الإلكترونى المعروف باسم "WannaCry" وهو آخر تجليات برمجيات الابتزاز الإلكترونى والذى أصاب ربع مليون مستخدم للدولة فى حوالى ١٥٠ دولة حول العالم مابين الغاء عمليات جراحية،واختراق مواقع إلكترونية جامعية، وتعطيل محطات القطارات فى ألمانيا،وقدر خبراء صناعة الإنترنت الفدية المدفوعة للقراصنة بمبلغ٢٠ألف دولار تم دفعها من خلال "عملة البيكوتين" التى لايمكن تتبع مصدرها.

(٢) Ibid, p. ٦٠

ويتعلق الأمن المعلوماتي بجريمة تمرير المكالمات الدولية، وهي من الجرائم التي تتطلب درجة عالية من الحرفية في رجال الضبط الإداري، ومن تلك الجرائم القضية رقم ٢٠١٠/٥ جنايات عسكرية، والتي قام المتهمون فيها بنقل حركة المكالمات الدولية من داخل وخارج البلاد عبر شبكة المعلومات الدولية لتلك الدولة الأجنبية (إسرائيل) مما أضر بالمركز الاقتصادي للبلاد ومصالحها القومية خاصة أن بعض البيانات والأرقام كانت تحت مسمى (صانعي القرار في مصر) وكذلك العديد من المعلومات السرية سواء اقتصادية أو عسكرية أو سياسية أو دبلوماسية بالإضافة إلى الضرر الاقتصادي المحقق والمتمثل في الخسارة المالية للشركة المصرية للاتصالات، والتي تملك الدولة فيها أكثر من ثمانين في المائة من أسهمها.[٣١٧١]

فالجريمة المعلوماتية قد تكون جريمة مختلطة كجريمة تمرير المكالمات الدولية بحيث تكون جريمة معلوماتية واقتصادية في ذات الوقت لذا يتعين مواءمة أنواع الضبط لتلك الخطورة.[٣١٧٢]

وإذا كانت النظرة الشائعة عن الأمن المعلوماتي تعد أكثر تركيزًا من الناحية السياسية إلا أن تلك النظرة يمكن أن تتسع لتشمل الأمن المعلوماتي الاقتصادي كمثال جريمة الحصول على خدمات اتصال بطرق احتيالية ،ومن الدول التي جرمت ذلك الفعل سلطنة عمان في القانون رقم ٣٠ لسنة ٢٠٠٢ الخاص بالاتصالات حيث جرمت المادة ٥٣ منه إنشاء أو تشغيل نظام الاتصالات أو تقييد خدمات اتصالات بدون الحصول على ترخيص.[٣١٧٣]

ويمكن تحقق تلك الجريمة المعلوماتية من خلال العديد من الوسائل كالتالي:

الوسيلة الأولى: استخدام جهاز هاتف مبرمج[٣١٧٤] مرتبط بشبكة الإنترنت في إجراء مكالمات دولية دون المرور بالشبكة التابعة للشركة حائزة الخدمة.

ويشير الكاتب هنا أن العصابات الالكترونية تبيع تلك الأسلحة كمثال العصابات الروسية وتقوم تلك العصابات بإبتزاز المؤسسات العامة والخاصة وتهديدها إن لم تقم= =بدفع مبلغ مالي مقابل عدم استخدام تلك الأسلحة الإلكترونية، وأبرز مثال لذلك عندما تم استهداف الكمبيوتر الرئيسي لبنك اليابان، ولكن تم إخطار FBI في الوقت المناسب وتم إفشال الهجوم بسرعة، لكن في أغلب الأحيان تفشل المؤسسات في إخطار السلطات المختصة، **ومثال ذلك:** قيام بيت السمسرة البريطاني بدفع فدية قدرها ١٠ مليون جنيه استرليني وقيام البنك البريطاني بدفع ١٢.٥ مليون جنيه استرليني بعد تهديدات.

(٣١٧١) حكم المحكمة العسكرية العليا يوم الثلاثاء ٢٠١١/٥/١٠ في القضية رقم ٢٠١/٥ جنايات عسكرية إدارة المدعى العام العسكري-حكم غير منشور.

(٣١٧٢) من واقع القضية نجد شهادة الرئيس التنفيذي للجهاز القومي لتنظيم الاتصالات تؤكد على ذات المعنى بأن "تغطية شبكات التليفون المحمول في مصر من الواجب ألا تتعدى حدود الدولة ويثبت ذلك في تراخيص الشركات إعطاء الترخيص لها وأنه = =يجب على شركات الاتصالات عند إقامة أو إنشاء أبراج، أن تخطر الجهاز القومي لتنظيم الاتصالات الذي يخاطب بدوره هيئة عمليات القوات المسلحة، علاوة على ما سبق فإن تمرير المكالمات عن طريق دولة معادية يعد خطرًا على الأمن القومي علاوة على الضرر الاقتصادي المحقق.

(٣١٧٣) عاقبت المادة ٥٣ المنشيء أو المشغل لتلك الخدمة غير المشروعة والمهددة للأمن وعاقبت المادة ٥٧ من ذات القانون كذلك كل مستفيد من تلك الخدمة ولم يقتصر عند ذلك الحد بل تم تجريم حائز الأشياء المستخدمة في تلك الخدمة من خلال المادة ٥٨ من القانون وتجريم مورد الأشياء المستخدمة في ذلك.

(٣١٧٤) المرجع السابق، ص٧٠، ٧١.

الوسيلة الثانية: إدخال بطاقات مدفوعة القيمة تستخدم في الاتصال الدولي المباشر بشبكة الإنترنت ومن ثم بيعها نظير مبلغ مالي دون موافقة من الجهة المختصة.

الوسيلة الثالثة: إجراء مكالمات دولية باستخدام المكالمات الدولية المرتدة "International call back".[٣١٧٥]

٤) **الطابع المتصل بالأمن القومي**:

كما ذكرنا سلفًا تتصل الجرائم المعلوماتية بالطابع الأمني القومي والطابع السياسي، ونجد ذلك فيما يعرف بحرب المعلومات والتجسس الإلكتروني، والإرهاب الإلكتروني.[٣١٧٦]

وعادة ما تلجأ الدول تحت الهاجس الأمنى القومى إلى كبت الحريات وإلى وضع قيود إضافية على استخدام الإنترنت، كالقانون الذي أصدرته تركيا، والذي يمنح هيئة الاتصالات التركية الصلاحية والترخيص بإغلاق مواقع الإنترنت في خلال أربع ساعات، ولكن المحكمة الدستورية العليا التركية اشترطت استصدارحكم قضائي قبل إغلاق أي موقع، ورأت المحكمة عدم دستورية النص الذي يتيح للهيئة الحصول على معلومات من خلال رقابتها لبعض المواقع عبر مستخدميه ثم تخزينها.[٣١٧٧]

ويرى الفقه المقارن أنه ولكون مصطلح **"الأمن القومي"** مصطلحًا سياسيًا فإنه من المرونة ما يؤثر على حرية التعبير وتداول المعلومات؛ ولذلك فإنه مصطلح مجرد وغامض ويفترض أن يكون محدد المعنى كي يوازن بين حق المواطن في المعرفة، ومصلحة الإدارة في الحفاظ على الأمن المعلوماتي[٣١٧٨].

"في هذه الطريقة يقوم المتصل بالاتصال بأحد الأرقام الدولية دون إكمال المكالمة حيث يقوم بقطعه قبل أن يقوم الطرف الآخر بالرد، ومن ثم تقوم الجهة الأخرى بالاتصال وربط المتصل بالجهة المطلوبة دون أن تكون هناك بطاقة مدفوعة القيمة ويتم محاسبة المشترك محليًا".

(٣١٧٥) مروان صالح، المرجع السابق ص١٥.

(٣١٧٦) مشار لتلك الأمثلة في مؤلف د/ حسين الغافري، المرجع السابق، ص١٥ نقلاً عن:

- د/ منصور محمد عقيل ود/ علي قاسم، الانترنت والأبعاد الأمنية، مركز البحوث والدراسات الشرطية، دبي، يناير ١٩٩٦، ص١٢-١٣. "ومثال ذلك: سرقة معلومات عسكرية من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية في صيف ١٩٩٤، **ومثال ذلك أيضًا:** ما تعرضت له عدة وزارات وجهات حكومية ومؤسسات مالية من هجوم من جماعات الألوية الحمراء عن طريق تدمير مراكز المعلومات الخاصة"

(٣١٧٧) جريدة الأهرام المصرية الورقية - العدد اليومي بتاريخ ٥ أكتوبر ٢٠١٤.

(٣١٧٨) Shimon shetreet: free speech and national security, International studies in Human Rights – Volume ١٦ p. ٤٤.

"The notion of national security is so abstract and vague that it must be given specific content"

"Right of the public to know, and the Interest of keeping certain Matters secret".

وعلى صعيد الواقع العملي تميل الجهات الإدارية لتفضيل كفة الحفاظ على الأمن القومي، وذلك لتفضيل الحكومة بالمفهوم السياسي الابتعاد عن النقد فيما يخص تصرفاتها وأعمالها، ويتجسد ذلك التفضيل في حجب المعلومات التي تتعلق بعملية صناعة القرارات، أو النشاطات غير المشروعة، أو الفساد.

وعامة يعد الأمن القومي للدولة هدفًا رئيسيًا قبل وجود الدولة ذاتها، ويعد شرطًا لاحقًا لأنشطتها بعد ذلك، لذا من المقبول أن تتبع الإدارة العديد من الإجراءات السرية فيما يخص معاملاتها[٣١٧٩].

ولكن من غير المقبول أن يتسع النشاط السري في أنشطة جهة الإدارة سواء زمنيًا أو موضوعيًا بشكل مطلق بل يعد ذلك محكومًا بأن تعالج السرية بأدوات ضرورية فقط تحدد ذلك الهدف[٣١٨٠]، وتتباين تلك المفاهيم من دولة إلى أخرى بحسب طبيعة النظام السياسي، وفي ذات البلد من وقت لآخر.

ومن أهم تلك المفاهيم "مفهوم الأمن القومي" حيث يعد مفهومًا متلازمًا مع الأمن المعلوماتي، وقد عرف القانون رقم ١٥ لسنة ٢٠٠٣ بتنظيم الاتصالات مفهوم الأمن القومي في المادة الأولى منه[٣١٨١] كما تم تعريف أجهزة الأمن القومي بأنها رئاسة الجمهورية ووزارة الداخلية، وهيئة الأمن القومي، وهيئة الرقابة الإدارية.

ويذهب بعض الباحثين إلى أن ذلك التعريف جاء عامًا شاملاً لكل ما يتعلق بأنشطة تلك الأجهزة.[٣١٨٢]

أما محكمة القضاء الإداري فقد ذهبت في سبيل تعريفها للأمن القومي بأنه "قدرة الدولة على حماية أراضيها وقيمها الأساسية والجوهرية من التهديدات الخارجية، وبخاصة العسكرية منها، انطلاقًا من أن تأمين أراضي الدولة من العدوان الأجنبي، وحماية مواطنيها ضد محاولات إيقاع الضرر بهم وبممتلكاتهم ومعتقداتهم وقيمهم، هو دافع الولاء الذي يمنحه الشعب للدولة بالعقد الاجتماعي المبرم ".[٣١٨٣]

([٣١٧٩]) Ibid, p. ٥٩.

([٣١٨٠]) Ibid, p. ٥٩ "The secrecy is instrumentally necessary for the promotion of a goal"

(٣١٨١) نصت المادة الأولى بند ٢٠ من القانون على أن مفهوم الأمن القومي يشمل كل ما يتعلق بشئون رئاسة الجمهورية، والقوات المسلحة والإنتاج الحربي ووزارة الداخلية، والأمن العام، وهيئة الأمن القومي، وهيئة الرقابة الإدارية والأجهزة التابعة لهذه الجهات يعد من أجهزة الأمن القومي.

(٣١٨٢) أحمد عزت وآخرون: حرية الفكر والتعبير - الطبعة الثانية ٢٠١٣ ص٦٠.

(٣١٨٣) انظر حكم محكمة القضاء الإداري - الدعوى رقم ٢١٨٥٥ لسنة ٦٥ ق - جلسة ٢٠١١/٥/٢٨ -حكم غير منشور،.وقد عددت المحكمة الأبعاد المتعددة للأمن القومي كمثال البعد السياسي داخليًا ويعبر عنه بتماسك الجبهة الداخلية وخارجيًا ويعبر عنه بتقدير أطماع الدول العظمى، أما البعد الاقتصادي يتعلق بالاستخدام الأمثل للموارد وتنمية التبادل التجاري، أما البعد الاجتماعي هو إقامة العدالة الاجتماعية والبعد العسكري هو بناء قوة عسكرية قادرة على تحقيق التوازن الاستراتيجي العسكري والردع الدفاعي.

علاوة على ما سبق يرى الفقه المقارن أن اصطلاح "الأمن القومي" عندما يتعلق الحديث بالأمن المعلوماتي يعد من الغموض بمكان، ولكن من المهم قياس مصطلح السرية "secrecy" عن طريق معرفة قدر التهديد "threat".(٣١٨٤)

وتجدر الاشارة الى أن الاعتماد بشكل كامل على التقنيات الإلكترونية في حفظ الأمن المعلوماتي قد يضر بالأمن القومي، إذ ستكون المعلومات معرضة لتصرف الغير في حين لا تكون التقنيات تحت السيطرة من كل جوانبها، علاوة على ذلك تواجه الدول النامية معضلة الفجوة الرقمية، والتي تمثل الحد الفاصل بين من يملكون وتتاح لهم التقنيات المعلوماتية، وبين الذين لا يتاح لهم ذلك، وعادة ما تكون الفجوة أكثر وضوحًا وأوسع في الدول النامية، نتيجة العوائق التعليمية والاقتصادية والتنظيمية. (٣١٨٥)

ومن أبرز مايهدد الأمن القومى ما يعرف بالإرهاب الإلكتروني وهو استخدام الفضاء الإلكتروني cyper space كأداة لإلحاق الضرر بالبنى التحتية الحرجة كالطاقة، والمواصلات، وعمليات الإدارة أو تعطيلها. (٣١٨٦)

ويؤثر الإرهاب الإلكترونى على نطاقات الأمن المعلوماتى من خلال قيام المنظمات المتطرفة بالإخلال بالنظام العام وخاصة فى عنصر الأمن العام وعن طريق تهديد الفضاء المعلوماتي من أجل أغراض سياسية أو بدوافع دينية من خلال تكنولوجيا الاتصال والمعلومات والهواتف المحمولة والحاسبات الآلية وعبر شبكة الانترنت. (٣١٨٧)

وقد عرفت وكالة المخابرات المركزية الأمريكية مصطلح الإرهاب الإلكتروني بأنه هجوم تحضيري ذو دوافع سياسية موجه ضد نظم معلومات الكمبيوتر وبرامجه.

أما مركز حماية البنية التحتية القومية الأمريكية فقد ذهب إلى أن الإرهاب الإلكتروني عمل إجرائي يتم تحضيره عن طريق أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية ينتج عنه تدمير أو تعطيل الخدمات بهدف إرباك وزرع الشك بهدف التأثير على الحكومة أو السكان. (٣١٨٨)

والتعريف الذي يؤيده الفقه هو:" العدوان أو التخويف أو التهديد ماديًا أو معنويًا باستخدام الوسائل الالكترونية الصادرمن دول أو جماعات أوأفراد عبر الفضاء الإلكتروني، أو أن يكون الفضاء الإلكتروني هدفًا لذلك العدوان بما يؤثر على الاستخدام السلمي له". (٣١٨٩)

(٣١٨٤) Ruth Gavison, Atomic secrets and free speech– International studies in Human Rights volume ١٦ p. ٥٨.

(٣١٨٥) د/ نبيل علي، د/ نادية حجازي: الفجوة الرقمية - رؤية عربية لمجتمع المعرفة، عالم المعرفة - الكون - أغسطس العدد (٣١٨) ٢٠٠٥ ص٧ مشار إليه لدى د/ عبد السلام هابس السويفان المرجع السابق ص١٠٩، ١١٠.

(٣١٨٦)د/ عادل صادق: استخدام الإرهاب الالكتروني في الصراع الدولي - دار الكتاب الحديث بدون سنة نشر. ص١٠٥

(٣١٨٧).من أمثلة ذلك: تطوير تنظيم القاعدة برنامجًا أطلق عليه (أسرار المجاهدين ٢) وهو أول برنامج للتراسل الآمن في ذلك الإطار عبر الشبكات وكان يعد ذلك فى حينها أعلى مستوى تقني في التراسل المشفر (المرجع السابق ص١١٧).

(٣١٨٨) مشار لتلك التعريفات في مؤلف د/ عادل صادق - المرجع السابق ص١٠٦.

(٣١٨٩) المرجع السابق ص١٠٩.

وما نميل إليه هو أن الإرهاب الالكتروني صورة للإخلال بالنظام العام في أى عنصر من عناصره من خلال نشاط أو هجوم متعمد بغرض التأثير على القرارات الحكومية أو الرأي العام أو من خلال التأثير المعنوي والنفسي عبر التحريض على بث خطابات الكراهية الدينية وحرب الأفكار، أو أن يتم في صورة رقمية للإضرار بالأمن المعلوماتي للأفراد أو المؤسسات أو الدولة ككل.(٣١٩٠)

وتجدر الإشارة لدور القانون رقم ٩٤ لسنة ٢٠١٥ الصادر بقانون مكافحة الإرهاب فى تعزيز الأمن المعلوماتي لجهة الإدارة بصورة خاصة ،والدولة بصورة عامة حيث اعتبر القانون بموجب الفقرة الثانية من المادة الثانية أن الإضرار بالنظم المعلوماتية يعد عملاً إرهابيًا، وذلك بالنص على أنه " كل سلوك يرتكب بقصد تحقيق أحد الأغراض المبينة بالفقرة الأولى من هذه المادة، أو الإعداد لها، أو التحريض عليها، إذا كان من شأنه الإضرار بالاتصالات أو بالنظم المعلوماتية...". (٣١٩١)

ويعد ذلك النص تأكيدا على النصوص التي تجرم اختراق النظم الإلكترونية والمعلوماتية الخاصة بجهة الإدارة وخاصة بيانات الأحوال المدنية كمثال ما تناوله المشرع في القانون رقم ١٤٣ لعام ١٩٩٤. (٣١٩٢)

وحسنا ما جاء به المشرع في المادة ٢٩ من قانون مكافحة الإرهاب من تجريم استخدام المواقع الإلكترونية في العمليات الإرهابية للارتباط الوثيق كما أسلفنا بين الجرائم المعلوماتية والإرهاب الإلكترونى، ويتأكد ذلك من خلال قيام المشرع بمضاعفة النص العقابي في حالة تهديد الأمن المعلوماتي لجهة الإدارة(٣١٩٣) حيث نصت الفقرة الثانية من المادة ٢٩ من قانون مكافحة الإرهاب إلى أنه "... ويعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعًا إلكترونيًا تابعًا لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها...". (٣١٩٤)

(٣١٩٠) نستبعد من ذلك التعريف باستخدام الأسلحة التقليدية كالقصف المباشر القذائف على نقاط الإنترنت الرئيسية ومهاجمة كابلات الاتصال أو القيام بهجوم عن طريق استخدام الطاقة الكهرومغناطيسية للقيام بهجوم إلكتروني Electronic Attack ضد أجهزة الكمبيوتر والبيانات بداخلها رغم أنها داخلة في تعريف الإرهاب الالكتروني ولكنها ترتبط بالقانون الدولي العام بصورة أوضح.
ويرى د/ عادل صادق أن هجمات الفضاء الالكتروني تؤثر على الأمن والطابع المدني له والدليل على ذلك الحرب الجورجية الروسية عام ٢٠٠٨ والحرب الروسية الآستونية عام ٢٠٠٧.

(٣١٩١) انظر قرار رئيس جمهورية مصر العربية بالقانون رقم ٩٤ لسنة ٢٠١٥ بإصدار قانون مكافحة الإرهاب الجريدة الرسمية – العدد ٣٣ (مكرر) في ١٥ أغسطس سنة ٢٠١٥.

(٣١٩٢) نصت المادة ٧٦ من قانون الأحوال المدنية رقم ١٤٣ لعام ١٩٩٤ بأن يعاقب بالأشغال الشاقة المؤقتة كل من اخترق أو حاول اختراق سرية البيانات، أو الإحصائيات المجمعة بأي صورة من الصور...".

(٣١٩٣) نصت الفقرة الأولى من المادة ٢٩ من قانون مكافحة الإرهاب على أنه "يعاقب بالسجن المشدد مدة لا تقل عن خمس سنين، كل من أنشأ أو استخدم موقعًا على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن أية جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج".

(٣١٩٤) أنظر الفقرة الثانية من المادة ٢٩ من قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥.

لذا فإن حرب الشبكات تشير إلى الصراعات التي تقودها المعلومات، وهي تعني التركيز على آراء النخبة أو آراء الجماهير أو هما معًا، ومن أبرز أنواع تلك الحروب التسلل إلى شبكات الكمبيوتر وقواعد البيانات لتخريبها، ومحاولة تدعيم الجماعات المنشقة أو المعارضة في بلد ما من خلال شبكات الكمبيوتر. وبالتالي فإن حرب الشبكات تتميز باستهدافها للمعلومات والاتصالات.(٣١٩٥)

ومن أبرز أنواع التأثير على النظام العام في مجال الأمن المعلوماتي هو تغير أشكال التدرج التقليدي في المنظمات الإدارية عامة، والجهات الأمنية خاصة، حيث إن وجود الفضاء المعلوماتي والمجتمع الشبكي سيلغي فكرة التدرج الرئاسي في مجالات الأمن العام والقوات المسلحة.(٣١٩٦)

(٣١٩٥) السيد ياسين: شبكة الحضارة المعرفية من المجتمع الواقعي إلى العالم الافتراضي - الهيئة المصرية العامة للكتاب ،سلسلة العلوم الاجتماعية ، ٢٠٠٩، ص١٠٣.

(٣١٩٦) المرجع السابق ص١٠٤، "يصف مانويل كاستلز" المجتمع الشبكي Net work society بأنه سوف يؤثر تأثيرًا بالغًا على تكوين وإدارة القوات المسلحة من خلال تغيير فكرة التدرج Hierarchy في القيادات والرتب حيث إن القرار في الشكل التقليدي يصدر من القيادة العليا إلى المرؤوس، أما في الشكل الحديث سيكون الأمر عن طريق مجموعات لأعضائها حق التفكير والتخطيط واتخاذ القرار". وفي اعتقادنا أن ذلك التأثير قد يكون محتملاً في الحكومات الإلكترونية والتي قد يتم اختراقها بطريقة أو بأخرى، بما يخل بفكرة سرية الإجراءات والقرارات أو على الأقل إرباك جهات الضبط الإداري وخاصة الجهات الأمنية.

الفصل الثانى

في

المحددات القانونية للأمن المعلوماتى

تمهيد وتقسيم:

يثير تعزيز الأمن المعلوماتى العديد من الاشكاليات التى تشكل تحديدا قانونيا يحد من الفعالية التى يتطلبها ذلك التعزيز،لذا يجدر بأى تشريع لتنظيم الأمن المعلوماتي أن يوازن بين تلك المحددات ،وبين عنصر الفعالية المتطلبة سلفا لذا ستكون معالجة المحددات القانونية للأمن المعلوماتى فى أربعة مباحث كالتالى:

المبحث الأول:إشكاليات المعلومات بين أمنها وتداولها.

المبحث الثاني: مدى تعارض الأمن المعلوماتي مع الخصوصية

المبحث الثالث:مدى ارتباط الأمن المعلوماتي بمبدأ سيادة الدولة

المبحث الرابع:مدى وجود أطر تشريعية ورقابية معلوماتية.

المبحث الأول

في

إشكاليات المعلومات بين أمنها وتداولها

كما ذكرنا سلفًا تثير فكرة الأمن المعلوماتي صعوبة لحداثة الفكرة ومرونتها، فالأمن المعلوماتي أحد مفردات الأمن العام بمفهومه المستحدث، ويتصل بذلك مرونة فكرة النظام العام نفسها وشيوع استخدامها في مجالي القانونين العام والخاص، وقد وسع الفقه من مدلول النظام العام وتعريفه بأنه "مجموعة الشروط اللازمة للأمن والآداب العامة التي لا غنى عنها لقيام علاقات سليمة بين المواطنين وما يناسب علاقاتهم الاقتصادية".(٣١٩٧)

ويعارض الفقه إدراج مفهوم النظام العام ضمن القوالب القانونية الجامدة لمرونته وحركيته، لأن القول بخلاف ذلك يعيق مهمة القضاء، ويشجع السلطة الإدارية على التعسف فى تحديده، حيث إن خاصية المرونة تساعد على تقبل سنة التجديد والتطور وسرعة تقبل المستجدات دون حاجة إلى تعديل في التشريع القائم.(٣١٩٨)

(٣١٩٧) د/ محمد محمد بدران "مضمون فكرة النظام العام ودورها في مجال الضبط الإداري" دراسة مقارنة في القانون المصري والفرنسي، دار النهضة العربية ١٩٩٢، ص٦٩.

(٣١٩٨) د/ طارق الجيار - المرجع السابق ص٢٦٤.

ويؤكد الرأي السابق أن القضاء الفرنسي والمصري حددا النظام العام بشكل لا يحول دون تطور جوهره، ويمنع من افتئات سلطة الإدارة عليه، بل أنه يراقب تقدير الإدارة إذا اضطر إلى فحص عناصر المشروعية، والتي أحيانًا ما تكون من بينها الملاءمة، فتمتد إليها رقابة القضاء لحماية الحقوق والحريات وصون النظام العام.

وفي اعتقادنا أن وجود تشريعات تضبط العلاقة بين الحق في تداول المعلومات وبين الأمن المعلوماتي يقلص من فكرة تغول سلطات الضبط الإداري على الحريات العامة بحجة الملاءمة وسلطة التقدير فالضبط التشريعي في تلك الحالة يوازن بين الأمن المعلوماتي والحريات العامة ولكن من ناحية أخرى نرى أن النظام العام لا بد أن يكون له مرونته كي لا نسلب سلطات الضبط الإداري السلطة التقديرية.

ويؤكد قولنا إن الحق في تداول المعلومات أحد سمات الدولة القانونية لذا فإن الإشكالية الحقيقية تكمن في التوفيق بين ذلك الحق وبين حاجة الإدارة للاحتفاظ بقدر من السرية أو ما يعرف بالأمن المعلوماتي ولا بد أن يملك القضاء القدرة على إقامة ذلك التوازن[٣١٩٩].

لذا يرى الفقه المقارن أن الدول الديمقراطية ـ غالبًا ـ ما تضحى بمسألة حرية تداول المعلومات وحرية التعبير عندما يتعلق الأمر بالأمن القومي، **ومثال ذلك:** ما قررته "تاتشر" في بريطانيا من التقييد المعلوماتي في حرب الفوكلاند" وعدم إذاعة ما يتعلق بها[٣٢٠٠].

مما سبق يتبين لنا أن الفضاء المعلوماتي يعد عنصرًا مهمًا بين السلطة التي تمثلها جهة الإدارة وبين الخاضعين لها، فإذا تأثر ذلك المحيط الوسيط بين السلطة والخاضعين لها خسرت الإدارة كسلطة، حيث لا بد من وجود شبكة من المعلومات والبيانات بين الإدارة والأفراد.

كذلك إذا كانت السلطة غير العادية لجهة الإدارة قد تغيرت بصورة أو بأخرى بالأمن المعلوماتي ومقتضياته، فإن مفهوم الضبط الإداري كذلك قد يتغير من حيث مدى خضوع وسائل التكنولوجيا الحديثة للتنظيم الضبطي،ويرتبط ذلك باعتبارات قانونية من حيث مدى احترام خصوصية المعلومات، وكذلك باعتبارات عملية لوجود معوقات لدى سلطات الضبط الإداري لدى ممارستها لاختصاصها بشأن التقنيات الحديثة، ويكون ذلك بتدريب رجال الضبط الإداري على مكافحة الممارسات غير المشروعة ضد الأمن المعلوماتي. [٣٢٠١]

والسؤال الذي يطرح نفسه هل تؤدي الانتهاكات المتلاحقة على أمن الفضاء المعلوماتي إلى تغير في مفهوم سلطة الإدارة، أو في مفهوم الامتيازات الاستثنائية غير العادية التي تتمتع بها؟

([٣١٩٩]) shetreet,op.cit.p٢٠

"How and where the court might strike a balance between the public's need to know and the government's needs both for administrative workability and reasonable a mounts of secrecy".

([٣٢٠٠]) Ibid,p.٤

(٣٢٠١) راشد محمد راشد حمداني السلحدي الشحي: الرقابة القضائية على قرارات الضبط الإداري في الحكومة الإلكترونية ـ دراسة تطبيقية على دولة الإمارات العربية المتحدة ـ رسالة دكتوراه مقدمة لكلية الحقوق ـ جامعة القاهرة ٢٠١٤، ص٢١٢.

يذهب الفقه المقارن "Castells" إلى أن السلطة هي أكثر العمليات أصولية في المجتمع لأن القيم والمؤسسات تحدد المجتمع، وما هو ذو قيمة وذو طابع مؤسسي تحدده علاقات السلطة، فالسلطة هي القدرة ذات الصلة التي تمكن فاعلاً اجتماعيًا من أن يؤثر بشكل غير مناسب على قرارات الفاعلين الاجتماعيين الآخرين بسبل تحابي إرادة الفاعل المتمتع بالسلطة ومصالحه وقيمة ".[٣٢٠٢] لذا فى اعتقادنا لن يتغير مفهوم سلطة الإدارة بالنسبة لمقتضيات الأمن المعلوماتى سوى بأن جهة الإدارة ملزمة بتطوير وسائلها لتساير التطور التكنولوجي، وذلك لكى يكون الضبط الإدارى فعالا.

وينصح الفقه المقارن أن يتم تداول البيانات والمعلومات في إطار يخدم المجتمع الديمقراطي من خلال أن تقوم الصحافة بنشر الأخبار التي تجعل الأفراد يشاركون في صناعة القرار السياسي لا أن تركز على الأخبار التي يحب الجمهور تداولها[٣٢٠٣]. ويثير ذلك أحد أهم الإشكاليات في الدولة القانونية وهى كيفية التوفيق بين اعتبارات الأمن المعلوماتي وتداول المعلومات.

عالجت محكمة القضاء الإداري في حكم حديث لها تلك الإشكالية، ورسمت خطًا فاصلاً بين الحق في المعرفة وتداول المعلومات ودور جهة الضبط الإداري في حماية وتعزيز الأمن المعلوماتي، حيث ذهبت إلى أنه لا يمكن التضحية بالحق في المعرفة بحجة تهديد النظام العام، واللجوء إلى أسلوب غلق مواقع التواصل الاجتماعي، وأنه إذا تعلق الأمر بانتهاك النظام العام أوالأمن القومي فإنها مهمة الأجهزة الحكومية، والجهاز القومي للاتصالات عن طريق التدخل لحجب وتقييد الصفحات المخالفة وليس عن طريق القيام بالحظر الشامل أو الحجب الكامل للمواقع الإلكترونية.[٣٢٠٤]

---

(٢)Manuel Castells, communication power ١st Edition ٢٠٠٩.p.٥٥

سلطة الاتصال ـ العدد ٢٠٩١ الطبعة الأولى ٢٠١٤ ـ المركز القومي للترجمة ص٣٧.

(٣٢٠٣)Richard S. salant, CBC, and the battle for the soul of Broadcast Journalism: The Memoirs of Richards. Salant ٢٤٨ – ٤٩ (١٩٩٩)= =(discussing the "fundamental and underlying issue of what types of information should have priority in a democracy), available at

"... news should be based on what the public what they would like to know".

(٣٢٠٤) انظر الحكم الصادر عن محكمة القضاء الإداري، الدائرة الثانية في جلسة ٢٠١٥/٨/٢٥ في الدعوى رقم ٥٧٩٣٣ لسنة ٨٦ ق. (حكم غير منشور).

وقد أقام المدعى دعواه ضد مواقع التواصل الاجتماعي وخاصة موقع face book بدعوى تهديد النظام العام والأمن القومي من الناحية المعلوماتية، وأقام دعواه ضد وزارة الداخلية والاتصالات والجهاز القومي لتنظيم الاتصالات.

"ومن حيث إن شبكات التواصل الاجتماعي "social Networking" ... لم تكن سوى وسائل التعبير التي انتزعها المتواصلون اجتماعيًا وسياسيًا تأكيدًا لحقوقهم = =المقررة دستوريًا في الاتصال والمعرفة وتدفق المعلومات وتداولها..." وتطرقت المحكمة إلى خلو التشريعات من حظر وحجب المواقع الالكترونية وضرورة اضطلاع أجهزة الضبط الإداري وبالدور المنوط لها عوضًا عن الحظر الشامل أو الحجب الكامل لمواقع التواصل الاجتماعي كالتالي "... حيث خلت نصوصها من تحديد لثمة= =حالات يمكن أن تستدعي حظر أو حجب المواقع الإلكترونية إلا أنه وفي المقابل إذا ما تناولت بعض الصفحات على مواقع التواصل الاجتماعي أمورًا من شأنها المساس بالأمن الوطني والنظام العام فإنه يتعين على الأجهزة الحكومية والجهاز القومي للاتصالات التدخل لحجب وتقييد تلك الصفحات

علاوة على ما سبق قد يتهدد الأمن المعلوماتي لجهة الإدارة باعتمادها على مصادر معلوماتية غير موثوقة فيما يخص قضايا الأمن القومي قد تؤدي إلى تضارب المواقف فيما بين السلطة التنفيذية أو السلطة القضائية، الأمر الذي يؤثر في النهاية على مصداقية الادارة، وذلك بالقياس على القضية الأمريكية Padilla [٣٢٠٥] حين أصرت الإدارة على ضرورة الاعتقال العسكري الاستثنائي "Extraordinary military detention" مستخدمة في ذلك أدوات سرية مثل السجون العسكرية السرية [٣٢٠٦].

لذا يرى الفقه المقارن أن الرقابة القضائية على القرارات الإدارية المتعلقة بالأمن المعلوماتي خاصة، والأمن القومي عامة، لا بد أن تتطرق إلى مكونات القرار كما تتطرق إلى القرار ذاته عن طريق ما يعرف بالرقابة القضائية "Judical Review" إذ إن ذلك النوع من الرقابة على القرارات الإدارية المتعلقة بالطبيعة الأمنية تعد رقابة مشروعية بالمفهوم التقليدي، بدون تدخل في اعتبارات الملاءمة الأمنية، ويقوم ذلك على اعتبارين **أولهما:** عملي لعدم احترافية القاضي بقدر احترافية رجل الإدارة، **وثانيهما:** نظري وهو اعتبار الفصل بين السلطات "The separation of powers". ولكن على القاضي فحص تسبيب توجهات رجل الإدارة من خلال ما يعرف بالمعقولية "Reasonableness". [٣٢٠٧]

ويلجأ القضاء المقارن في المسائل المعلوماتية إلى وزن الاعتبارات "weighing the considerations" بين احتياجات المجتمع والفرد[٣٢٠٨].

على تلك المواقع استنادًا إلى مالها من سلطة في مجال الضبط الإداري كحماية النظام العام بمفهومه المثلث الأمن العام، والصحة العامة والسكينة العامة...".

([٣٢٠٥]) Rumsfeld V. padilla, ٥٤٢ U. S. ٤٢٦, ٤٦٠ – ٦١ (٢٠٠٤) (Stecens, J., dissenting). Klein op. cit., p.٤

([٣٢٠٦]) "After confining pardilla in the brig" for three and a half years, steadfastly mantaning, that it was imperative in the hinterest of national security that he be so held and without demonstrating the reliability of the information underlying that detention to a single Judge ...".

"The government's motion to transfer padella to civilian custody spurred Judge. Lutting, whose opinion only weeks earlier Judge. Lutting, whose opinion only weeks earlier had upheld the president's authority to detain padilla, to rebuke the government for attempting to moot the case on the eve of possible supreme= =court review. Creating the impression that the government had held padilla mistakenly and Jeopardizing "the government's creadibility before the courts".

([٣٢٠٧]) H.C.J. ٦٨٠ / ٨٨ Schitzer v. Chief Military censol, ٤٢ (٤) P. D. ٦١٧ "the security character of Administrative discretion deterred Judical Review in the past. Judges are not security personnel and may not interfere in security consideration.

([٣٢٠٨]) Shimon shetreet. Op. cit., p. ٤٩.

ويرجع ذلك غالبًا إلى قيام جهة الإدارة بحجب معلومات تخص انتهاكات تتعلق بالأمن القومي لتعلق ذلك بمصداقية شهادة الشهود أو قيمة الدليل هذا من ناحية، ومن ناحية أخرى تلجأ الإدارة لأشكال جديدة من الإجراءات السرية لحماية الأدلة التي تحوزها، ومن البديهى أن تلجأ الجهة الإدارية بإعاقة التقاضي فيما يتعلق بالأمن القومى، كمثال رفض القضايا في آخر لحظة، حتى لا تتم مناقشتها أو لحجب معلومات عن القضاة لغل أيديهم عن الدعوى، ويشمل ذلك المحاكم الاستئنافية أيضًا، لذا تتحمل جهة الإدارة بشكل كبير مسئولية تلك التصرفات غير القانونية(٣٢٠٩).

عامة يرى الفقه المقارن أن حدود الأمن المعلوماتي تتركز حول أربعة محاور بحيث يعد الإفصاح عن المعلومات التي تتعلق بها يقع تحت طائلة القانون **وتلك المحاور هي:** الأمن والاستخبارات، والدفاع، والعلاقات الدولية، وسلطات التحقيق الخاصة وما يتعلق بها(٣٢١٠).

في اعتقادنا فيما يتعلق بنطاق حيازة البيانات والمعلومات التي يمكن لجهة الإدارة أن تسمح بها للقطاع الخاص والأفراد يقتصر نطاقها على المعلومات التي يكون الحصول عليها بطريقة قانونية "lawfully obtained" وتكمن الإشارة في غياب القيود التي ترد على نقل المعلومات والبيانات من القطاع الخاص إلى جهة الإدارة، خاصة عندما يركز برنامج جهة الإدارة لجمع البيانات على أمر جدي كمنع عناصر إرهابية من دخول الطائرات مثلاً.

ولا بد أن يتوافر في النظام القانوني النموذجي لحيازة المعلومات عنصر المحاسبة من ناحية ، وثقة صانعي القرار والسياسات من ناحية أخرى، علاوة على تشجيع القطاع الخاص على مد جهة الإدارة بالبيانات للاستخدامات القانونية في مجال مكافحة الإرهاب(٣٢١١).

وتجدر الإشارة إلى أن الدستور المصري قد جعل من الأنشطة المعلوماتية مقومًا أساسيًا للاقتصاد الوطني، وألزم الدولة بحماية تلك الأنشطة وزيادة تنافسيتها بما مؤداه أن الدولة تحتاج إلى مساهمة القطاع

" In such a situation it was helf that the high court of Justice would examine the Justification for the claim of privilege by carefully weighing the considerations based on security needs on the one hand, and the need to a ssure a fair trial, on the other hand."

(٣٢٠٩) For more see: James klein: Indigent Defendants and Enemy combatants: Developing prototypes for National security cases. Harvard – C. R. – C. L. L. Rev. ٢٠٠٧ p. ٣.

(٣٢١٠) Garaham, J. Zellich:– Spies, suberversive terrorists, and the British Government– free speech and other casualties, International studies in human Rights, Volume١٦ p. ١١٣.

(٣٢١١) see:– James oliphant, phone firms want shield If spy suits come calling, chicago Tribune, Nov ١٥, ٢٠٠٧,p٢٢.

الخاص في الأنشطة المعلوماتية، غير أن الدولة منوط بها حماية تلك الأنشطة من خلال الضبط التشريعي والضبط الإداري كما سيرد بيانه.[٣٢١٢]

علاوة على ما سبق تشكل الوثائق حلقة مهمة من حلقات الأمن المعلوماتي إذ تختلف درجة سرية الوثائق بحسب المعلومة، فمن المعلومات ما هو سري، ومنها ما هو سري جدًا، ومنها ما هو سري للغاية، ومنها ما هو معلومات محظور الاطلاع عليها وذلك على النحو التالي:[٣٢١٣]

أولاً: المعلومات السرية:

تخص تلك المعلومات ما يتعلق بالأشخاص كالبيانات الشخصية والتحقيقات الإدارية، وما يتعلق بمصالح المواطن كالمعلومات البنكية للعميل مثل حساباته وأرصدته وأنشطته التجارية.

ثانيًا: المعلومات السرية جدًا:

تدور تلك المعلومات حول المعلومات المتعلقة بالمؤسسة ككيان وليس كأفراد أو منتفعين بها.

ومثال ذلك: القرارات المتعلقة بتنظيم العمل وطرح مناقصات أو مزايدات لجهة الإدارة.

ثالثًا: المعلومات السرية للغاية:

تدور تلك المعلومات حول ما يتعلق بالمصلحة العامة للدولة كنوعية التسليح وعدد أفراد الجيش، والمعلومات الاستراتيجية المتعلقة بأجهزة المخابرات.[٣٢١٤]

رابعًا: المعلومات المحظور الإطلاع عليها:

تدور تلك المعلومات حول المشروعات القومية أوالخطط الاستراتيجية أو الخطط العسكرية في المفاوضات الدبلوماسية والمنازعات الدولية، ولا يمكن الاطلاع على تلك المعلومات إلا للمكلف بالمهمة.

وعلى نطاق التشريع قد تأكد تعزيز الأمن المعلوماتي المصرى فيما يخص السياسة العليا للدولة أو الأمن القومي بصدور القانون رقم ١٢١ لسنة ١٩٧٥ بشأن المحافظة على الوثائق الرسمية للدولة، وتنظيم أسلوب نشرها وقد خولت المادة الأولى منه سلطة لرئيس الجمهورية في وضع نظام للحفاظ على الوثائق والمستندات الرسمية المتعلقة بالسياسة العليا للدولة أو بالأمن القومي، بل ونص القانون على إمكانية عدم نشر بعض هذه الوثائق لمدة لا تجاوز خمسين عامًا في حالة إذا ما تطلبت المصلحة العامة ذلك.

(٣٢١٢) نصت المادة ٢٨ من الدستور المصري على أن "الأنشطة الاقتصادية الإنتاجية والخدمية والمعلوماتية مقومات أساسية للاقتصاد الوطني، وتلتزم الدولة بحمايتها، وزيادة تنافسيتها...".

(٣٢١٣) د/ صلاح الدين فوزي، المرجع السابق ص٣٨٩.

(٣٢١٤) ينتقد ذلك الرأي فكرة المصلحة العامة لغموضها، ولأنها فكرة نسبية فتارة يمكن أن تكون تابعة لمصلحة المرفق العام، وتارة يمكن أن تكون مجموع المصالح الخاصة.

أما المادة الثانية من ذات القانون فقد حظرت على من اطلع بحكم وظيفته أو مسئوليته أو حصل على وثائق ومستندات غير منشورة من نوعية المستندات المشار إليها بالمادة الأولى، أو على صورة منها أن يقوم بنشرها أو نشر المحتوى الكلي أو الجزئي لها بدون تصريح خاص صادر من مجلس الوزراء بناء على عرض الوزير المختص ،وتأكيدًا على ذلك صدر القرار الجمهوري رقم ٤٧٢ لسنة ١٩٧٩ بشأن نظام المحافظة على الوثائق الرسمية للدولة وأسلوب نشرها واستعمالها.[٣٢١٥]، وفي اعتقادنا أن الأسرار العسكرية وتعزيز سريتها تعد من أساسيات الأمن المعلوماتي، والتي لا يتعارض وجودها مع عناصر الدولة القانونية.

ويذهب الفقه في تعريفه للأسرار العسكرية إلى أنها كافة المعلومات التي تخص تشكيل وتحركات القوات المسلحة وعتادها وأفرادها، وعامة يعد سرًا عسكريًا كل ما له مساس بالشؤون العسكرية والاستراتيجية، ولم يكن قد صدر إذن كتابي من القيادة العامة للقوات المسلحة بنشره أو إذاعته.[٣٢١٦]

أما قانون العقوبات المصري في المادة ٨٥ منه قد نص على أنه يعد من أسرار الدفاع ما يلي:

١) المعلومات الحربية والسياسية والدبلوماسية والاقتصادية والصناعية، التي بحكم طبيعتها لا يعلمها إلا الأشخاص الذين لهم صفة ذلك، ويجب لمراعاة مصلحة الدفاع عن البلاد أن يبقى سرًا على من عداهم.

٢) الأشياء والمكاتبات والمحررات والوثائق والرسوم والخرائط والتصميمات والصور وغيرها من الأشياء التي يجب لمصلحة الدفاع عن البلاد ألا يلم بها إلا من يناط بهم حفظها أو استعمالها، والتي يجب أن تبقى سرًا على من عداهم.

٣) كل ما له مساس بالشؤون العسكرية والاستراتيجية ولم يكن قد صدر إذن كتابي من القيادة العامة للقوات المسلحة بنشره أو إذاعته.

ويذهب الفقه إلى أن مذهب التشريع المصري في ذلك قد قارب التشريع الفرنسي في عدم التحديد الدقيق لما يعد من الأسرار العسكرية المتعلقة بالدفاع الوطني، وبالتالي تتمتع الجهة المختصة بسلطة تقديرية واسعة في تحديد محتوى ونطاق هذا السر وفقًا للاعتبارات السياسية والظروف التي تحيط بالمعلومة، لذا يعد ذلك في اعتقادنا تغليبًا للأمن المعلوماتي على مبدأ تداول المعلومات في ذلك النوع من الأسرار.

ويلمس الفقه ذات المشكلة فيما يخص الأمن المعلوماتي للأسرار العسكرية بعدم وجود معايير لما يعد من قبيل الأسرار العسكرية وتلك السلطة التقديرية الواسعة.[٣٢١٧]

(٣٢١٥) نصت المادة الأولى من هذا القرار على "أن تعتبر الوثائق والمستندات والمكاتبات التي تتعلق بالسياسة العليا للدولة أو بالأمن القومي سرية لا يجوز نشرها أو إذاعتها كلها أو بعضها، كما لا يجوز تداولها أو الإطلاع عليها إلا لمن تستوجب طبيعة عمله ذلك، وذلك كله ما لم تكن مما ينص الدستور أو القانون على نشرها فور صدورها".

ونصت المادة الرابعة من هذا القرار على أن يكون حفظ الوثائق والمستندات والمكاتبات التي تتعلق بالسياسة العليا للدولة أو بالأمن القومي لمدة لا تتجاوز خمسة عشر عامًا تنقل بعدها إلى دار الوثائق القومية، لتحفظ في الأماكن التي تعد لهذا الغرض، وتظل محتفظة بسريتها لمدة خمسة عشرة سنة أخرى.

(٣٢١٦) د/ محمد سعيد حسين أمين، حرية الصحافة ضمان ممارستها وضوابط تنظيمها، دار النهضة العربية، ٢٠٠٥ ص٥٣ .

(٣٢١٧) د/ فاروق عبد البر، دراسات في حرية التعبير واستقلال القضاء وضمانات التقاضي، بدون ناشر سنة ٢٠٠٦ ص١١.

وفي ذات الاتجاه يقرر البعض – ونحن معه – باحتمالية إساءة استخدام تلك السلطة التقديرية الواسعة كستار لتغطية أعمال غير مشروعة على الصعيد القانوني الدولي، كأعمال إرهاب في دولة أجنبية، أو التآمر لقلب نظام الحكم في دولة أخرى.(٣٢١٨) وفي اعتقادنا أن ذات التخوف يمكن أن ينطبق على الصعيد القانوني الداخلي إذا لم تتناسب الأعمال العسكرية في الداخل مع حجبها المعلوماتى.

ومن أمثلة الدساتير التي نصت على جواز تقييد تداول المعلومات بغرض حماية الأمن القومي وبالتالي أحد بنوده الأمن المعلوماتي ما نص عليه الدستور التركي في المادة ٢٦ منه (بالصيغة التي عدلت بها في ١١٧ أكتوبر ٢٠٠١) إذ بعد أن أوردت الحق في حرية التعبير وتداول المعلومات بدون تدخل السلطات الرسمية أوردت جواز خضوع البت لنظام الحصول على التراخيص بغرض حماية الأمن القومي أو النظام العام أو السلامة العامة".(٣٢١٩)

(٣٢١٨) د/ سامي الطوخي، الإدارة بالشفافية للطريق للتنمية والإصلاح الإداري من السرية وتدني الأداء والفساد إلى الشفافية والتسبيب وتطور الأداء البشري والمؤسسي، دار النهضة العربية، ص٢٠٠٦، ص٤٥٧ مشار إليه في مؤلف د/ دويب حسين صابر، المرجع السابق ص٢٠٢.

(٣٢١٩) انظر: دساتير العالم (المجلد السادس) دستور تركيا – ترجمة وتقديم أماني فهمي – المركز القومي للترجمة، ص٣١.

المبحث الثانى

في

مدى تعارض الأمن المعلوماتي مع الخصوصية

من المحددات القانونية المهمة في مجال الأمن المعلوماتي ما يتعلق بمبدأ السرية الإلكترونية للأفراد والاتصالات، حيث يذهب البعض إلى وجود التزام بموجب الدساتير والقوانين بما يلي:

١) عدم جواز رقابة تلك الاتصالات أو المعاملات الإلكترونية إلا لضرورة تتعلق بالأمن القومي أو النظام أو للوقاية من الجرائم أو لحماية حريات وحقوق الغير، وألا يتم الكشف عنها إلا عن طريق القضاء أو الإدارة لأسباب مشروعة قانونًا.

٢) معاقبة أي شخص يراقب تلك الاتصالات مع الأخذ في الاعتبار وجود بعض الاستثناءات في بعض التشريعات الأوروبية، ومنها جواز تدخل مقدم الخدمة المعلوماتية لانتهاك السرية إذا كان تدخله تبرره الضرورة الفنية، ومنها كذلك مراقبة صاحب العمل لمن يعمل معه استنادًا لرضائهم المفترض بسياسة الرقابة الخاصة بمصلحة المشروع.(٣٢٢٠)

وتتعلق السرية الإلكترونية للأفراد بمدى وجود بنوك معلومات وبيانات، وتثور إشكالية بنوك المعلومات والبيانات على صعيدين **أولهما:** كمي، **والثاني:** كيفي وذلك كالتالي:-

١) على الصعيد الكمي: هناك عدد هائل من البيانات والمعلومات تخزنها المؤسسات الكبرى في الشركات الحكومية، وكذلك جهة الإدارة، ومن تلك البيانات ما يتعلق بالوضع المادي، أو التعليمي أو العائلي، أو المهني، أو الصحي، وتعد الحاسبات وشبكات الاتصال هي الوعاء الذي يقوم بتخزين ومعالجة وتحليل تلك البيانات والمعلومات.

٢) على الصعيد الكيفي: يعد شيوع النقل الرقمي للبيانات مشكلة أمنية معلوماتية لسهولة استراق السمع والتجسس الإلكتروني.(٣٢٢١)

ويمكن للأمن المعلوماتي أن يتعارض مع الخصوصية في عدة مفاهيم، وذلك كما ذهب الفقه بأن استثناء الوثائق والسجلات والمعلومات المتعلقة بحرمة الحياة الخاصة ينبغي أن يوضع في إطار محدود تراعى فيه مصلحة الفرد في التمتع بالاستقلال الذاتي والحرية أو السرية أو حتى العزلة، وبين مصلحة المجتمع، خاصة إذا كان هؤلاء الأشخاص من الشخصيات العامة، ويتمتعون بامتيازات عامة كالوزراء والمحافظين أو رؤساء الدول وغيرهم، ومن ثم ينبغي أن تتوافر فيهم شروط معينة.(٣٢٢٢)

(٣٢٢٠) د/ أيمن عبد الله فكري، المرجع السابق ص٤٨٨.

(٣٢٢١) د/ هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ١٩٩٢ ص٨٠.

(٣٢٢٢) د/ دويب حسين صابر، المرجع السابق ص١٩٥، ١٩٦.

وفي ذات الاتجاه يؤكد بعضهم على أنه إذا كانت قوانين المعلومات تفضل احترام الخصوصية ومنح الأمن المعلوماتي للأفراد العاديين إلا أنه لا بد من إقامة توازن بين حق الفرد في الأمن المعلوماتي وبين حق المجتمع في المعرفة من خلال عدم حجب المعلومات التي تضر ضررًا بالغًا بالآخرين أو المجتمع ككل.(٣٢٢٣)

فقد قررت المادة ٢٨ من قانون حماية البيانات لعام ١٩٩٨ في المملكة المتحدة استثناء حماية المعلومات الشخصية من الحماية في الخصوصية طالما تعلق الأمر بأغراض حماية الأمن القومي(٣٢٢٤).

ولكن من ناحية أخرى نصت الفقرة الثانية من ذات المادة من الجدول الأول من مبادئ حماية البيانات The Data protection principles على أن تكون طريقة الحصول على البيانات الشخصية لغرض أو للأغراض المحددة قانونًا وألا يتم معالجتها بطريقة غير متوافقة مع تلك الأغراض، وأكدت الفقرة الثالثة ذلك بأن تكون ذات تلك البيانات متوافقة وذات صلة مع الأغراض التي من أجلها تمت المعالجة(٣٢٢٥).

لذا مؤدى ما سبق أنه يجب اتخاذ جهة الإدارة التدابير التنظيمية اللازمة والإجراءات التقنية ضد عمليات المعالجة غير المشروعة وغير المرخص بها ضد الفقد الفجائي، أو التدمير، أو خسارة تلك البيانات وهذا ما أكدته الفقرة السابعة، بل واتخاذ التدابير اللازمة لعدم نقل تلك المعلومات الشخصية لأي بلد خارج بلدان المنطقة الاقتصادية الأوروبية EEA ما لم تضمن تلك البلد حماية لتلك البيانات.

وعلى الصعيد الأمريكى يرى الفقه المقارن أن حماية الخصوصية تؤدي غالبًا إلى تعزيز الأمن المعلوماتي، وذلك من خلال تقنين الإدارة لأنشطتها في حيازة المعلومات، أو على الأقل تبرير قيامها بنشاط تجميع البيانات والمعلومات على مستوى المسئولين الأعلى، أو من خلال لجنة من الكونجرس أو قضاة فيدراليين أو بمتطلبات الإذن القضائي أو أية إجراءات لحماية الخصوصية وجهود الأمن القومي(٣٢٢٦).

"إن فرص التضليل ملازمة للحماية القانونية "لطلب الأفراد" أو الجماعات بأن تقرر نفسها متى وكيف، وإلى أي مدى يجرى نقل المعلومات عنها للآخرين، لذلك فإن الخصوصية متى وكيف وإلى أي مدى يجرى نقل المعلومات منها للآخرين، لذلك فإن الخصوصية تسهل تقديم معلومات زائفة، مثلاً عندما يكذب طالب الوظيفة بالنسبة لوظيفته السابقة يجعل كشف هذا الزيف أكثر صعوبة أو مستحيلاً".

(٣٢٢٣) عمر محمد سلامة العليوي، حق الحصول على المعلومات في ضوء القانون الأردني رقم ٤٧ لسنة ٢٠٠٧ – دراسة مقارنة – رسالة دكتوراه، كلية الحقوق، جامعة عين شمس سنة ٢٠١١، ص١٨١.

(٣٢٢٤) Data Protection Act ١٩٩٨ Published by TSO, the stationery office p. ٥٠ – Data pretention & Investigatory powers Act ٢٠١٤ chapter ٢٧.

(٣٢٢٥) "Personal data shall be a dequate, relvant and not excessive in relation to the purpose or purposes for which they are processed".

(٣٢٢٦) Fred H. Cate, Government Data Mining:– The need for a legal framework, Hienonline – ٤٣ Harv. C. R. C.L.L. Rev. ٢٠٠٨ p. ٥١.

عامة تكمن الإشكالية في عدم وضوح الرؤية قانونًا عن المدى الذى يمكن أن يمد القطاع الخاص الحكومة بالبيانات الهائلة، وإلى أي مدى يمكن أن تقلق الادارة من البرامج الخاصة بحيازة المعلومات والبيانات لدى القطاع الخاص(٣٢٢٧).

في اعتقادنا أن مسألة التوازن بين الخصوصية والأمن المعلوماتي تحتاج إلى وضوح في فهم المقاصد وضبط الصياغات التشريعية المرتبطة، حيث قد تثير مسألة غموض المصطلحات عبئًا إضافيًا على الجهة القائمة بالتشريع والجهة القائمة بالضبط في مسائل الأمن المعلوماتي، **ومثال ذلك:** أن الدخول Access برز في العام ١٩٩٦ أمام محكمة كانساس العليا في قضية الولاية ضد Allen. (٣٢٢٨) وقد اعتمدت الحكومة الأمريكية على التعريف التشريعي الواسع لعبارة Access وذلك لعموميته بين التشريعات الولائية المبكرة لجرائم الحاسوب، ولكن المحكمة رفضت تفسير عبارة الدخول بأنها مجرد الاقتراب "To approach".

فى ذات السياق ما نص عليه قانون الاتصالات الأمريكي الصادر عام ١٩٧٠، على عدة معايير في مجال مراقبة المحادثات لأغراض أمنية، والتي ينبغي أن يكون قد تم الحصول على ترخيص مسبق، وأن يكون هناك مسوغ يبرز تلك المراقبة حيث يجب أن يكون الغرض من المراقبة الكشف عن الجرائم وضبط الجناة، وأن تكون الأحاديث المراد مراقبتها ذات صلة لجريمة ويجب أن يحدد الترخيص هوية الشخص الذي يستهدف مراقبة أحاديثه، ويحدد المكان الذي تجرى فيه المراقبة، وكذلك نوع الاتصالات التي يعتقد أنها ذات صلة بالجريمة. والمدة اللازمة للمراقبة، وما إذا كانت هذه المراقبة ستنتهي آليًا بعد التقاط الاتصالات المراد مراقبتها أو كيفية انتهاء المراقبة ووقف التقاط أو تسجيل الأحاديث.

وتجدر الاشارة لدور القضاء فى حث المشرع على تحديث التشريعات لتوائم حالات التطور المعلوماتى، **فعلى سبيل المثال:** رأى القضاء الأمريكي أن التشريعات التى تهدف الى مراقبة الاتصالات الهاتفية التقليدية لا تعزز الأمن المعلوماتى ،ولذلك أصدر المشرع الأمريكي عام ١٩٨٦ قانون خصوصية الاتصالات الإلكترونية

Electronic communication privacy Act ١٩٨٦ (ECPA)

(٣٢٢٧) Ibid, p. ٥١.

(٣٢٢٨) نطاق الجريمة الافتراضية (تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب):- أورين كير: بحث منشور في مجلة القانون – جامعة نيويورك – العدد ٧٨/ نوفمبر ٢٠٠٣، ترجمة د/ عمر محمد بن يونس، الأكاديمية الدولية للتجارة الدولية ٢٠٠٨ ص٧٤.

"فقد استخدم Allen حاسوب بشكل مستمر بنظام dial up (الاتصال الهاتفي بالشبكة) للاتصال بحاسوب شركة الهاتف الجنوبية الغربية التي تتحكم في تحويلات الاتصالات البعيدة المدى وتلاعب بها بحيث تسمح للمستخدم بالقيام بمكالمات بعيدة المدى مجانًا، وعندما اتصل Allen بحواسيب الشركة المذكورة واجهته شاشة تطلب منه اسم المستخدم وكلمة العبور. ولقد اتضح للمحققين أن Allen ضمن كلمة العبور بدقة وقام لاحقًا بازالة الدليل على نشاطه بإلغاءه للسجلات Logs، ولقد تمت إدانة Allen بدخوله إلى حواسيب الشركة بدون تصريح انتهاكًا لتشريع جرائم الحاسوب بولاية كانساس.

وبذلك تمتد الحماية وفق هذا القانون اللاحق إلى الاتصالات الإلكترونية علاوة على قانون التخزين الإلكتروني "The stored communications" والخاص بحماية الحق في خصوصية المراسلات الإلكترونية.(٣٢٢٩)

وإذا كانت برامج التصنت الإلكتروني في الولايات المتحدة الأمريكية قد لاقت معارضة من أكثر منظمة معنية بالحريات إلا أن القوانين الأمريكية المتعاقبة كقانون الاتصالات السلكية الصادر في عام ١٩٨٤، وقانون الاتصال عن بعد الصادر عام ١٩٩٦ وقانون خصوصية الاتصالات الصادر عام ١٩٩٧ أباحت مراقبة الاتصالات الإلكترونية أو الهاتفية، واشترطت لذلك صدور إذن من القاضي المختص بناء على طلب من أحد أعضاء النيابة ممن حددهم القانون بالموافقة على طلب المراقبة الذي يقدمه أحد رجال الضبط القضائي، كما حددت القوانين الجرائم التي يجوز فيها استصدار إذن بالمراقبة.(٣٢٣٠)

ومن القوانين الأمريكية التي تعالج إشكاليات الخصوصية والأمن المعلوماتي قانون "مشاركة وحماية المعلومات الرقمية (Cyper Intelligence Sharing and Protection Act) إذ يسمح ذلك القانون بمشاركة المعلومات ما بين الحكومة الأمريكية وشركات التقنية والتصنيع.(٣٢٣١)

وعلى صعيد التشريعات العربية التي وازنت بين الأمن المعلوماتي وتعزيزه، وحماية الخصوصية والبيانات الشخصية من الانتهاك أو التدمير نص القانون الكويتي رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية في المادة ٣٥ منه على التزام الإدارة عند حيازتها وجمعها للمعلومات والبيانات أن تكون في وظيفتها تقوم بذلك في إطار مشروع، وفي الغرض الذي تم جمع المعلومات من أجله بل وألزمها في الفقرة الثانية من التحقق من دقة البيانات والمعلومات المسجلة، وأن تتخذ تدابير حمايتها من القضاء والتلف أو الإفشاء أو الاستبدال ببيانات غير صحيحة أو إدخال معلومات عليها على خلاف الحقيقة.(٣٢٣٢)

ولكن على الصعيد العملي تذهب بعض الآراء في دولة الكويت إلى إغلاق تويتر (الموقع الإلكتروني الاجتماعي الأكثر شهرة هناك).(٣٢٣٣)

(٣٢٢٩) نشوى رأفت إبراهيم أحمد: حماية الحقوق والحريات الشخصية في مواجهة التقنية الحديثة "البيانات الشخصية، المراسلات والمحادثات الشخصية، الحق في الصورة) رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة ٢١٠٢ ص٢٨٣.

حيث أجاز قانون مراقبة الحافلات وأمن الشوارع الصادر عام ١٩٦٨م في الفصل الثالث منه لسلطات الأمن مراقبة الاتصالات الهاتفية بناءً على أمر السلطات القضائية في حالة ما إذا كان هنالك جريمة مرتكبة أو يوشك ارتكابها، مع توافر الاعتقاد بأن اتصالات خاصة تتعلق بالجريمة يمكن إثباتها عن طريق هذه المراقبة، وتكون وسائل التحري والبحث العادية قد أجريت وثبت فشلها.

(٣٢٣٠) في ذلك المعنى – المرجع السابق ص٢٨٤.

(٣٢٣١) تم انتقاد ذلك القانون من دعاة الخصوصية والحريات المدنية الأمريكية لقيوده القليلة في فترة مراقبة الحكومة للمعلومات الشخصية على الإنترنت، ولكن رحبت به مجموعة من الشركات ومجموعات الضغط "كغرفة التجارة الأمريكية وفيسبوك".

(٣٢٣٢) انظر القانون رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية: الكويت اليوم العدد ١١٧٢ السنة الستون ٦٩ بتاريخ ٢٠١٤/٢/٢٣.

(٣٢٣٣) جريدة الشاهد الكويتية الورقية – العدد ٢٧١٦ صدرت الأربعاء ١٣ يوليو ٢٠١٧ الصفحة الثالثة.

انقسمت الآراء التشريعية والبرلمانية هناك إلى أربعة آراء:- الرأي الأول يرى تفعيل القانون الكويتي للجرائم الإلكترونية واللائحة التنفيذية، والرأي الثاني يرى سن تشريعات جديدة بها عقوبات رادعة لمن يضر بالنظام العام المعلوماتي، حيث يجب تنظيم التواصل الاجتماعي بما يتماشى مع الأمن العام والوحدة الوطنية، والرأي الثالث يرى إغلاق تويتر نهائيًا، أما الرأي الرابع والأخير فيرى وجوب التواؤم مع القضاء المعلوماتي بمتطلباته الحديثة. وهو الرأي الوسط الذي يمثل إليه.

ويلقي البعض بالعبء على وسائل الضبط الإداري – وخاصة وزارة الداخلية – في مواجهة اختراقات أمن الفضاء المعلوماتي والأدهى من ذلك الوقوع في فخ المطالبة بحزمة تشريعات جديدة تتيح إمكانية التحكم في مواقع التواصل الاجتماعي، بل وطالب بعضهم بإنشاء محكمة دولية إلكترونية لعلاج الجرائم المعلوماتية المهددة للنظام العام.

أما الرأي الذي نميل إليه هو أن تلك المواقع أصبحت واقعًا لا بد من التعامل معه، فلا بد من الوصول إلى صيغة تجبر كل من يدخل إلى تلك المواقع بتسجيل بياناته الصحيحة والرسمية لإنهاء الحسابات المزيفة أو الحد منها على أقل تقدير.[٣٢٣٤]

وبالنظر للواقع المعلوماتي المصري تثير المدونات الإلكترونية إشكاليات فيما يتعلق بالأمن المعلوماتي لجهة الإدارة خاصة والأمن المعلوماتي بصورة عامة غير أن أحكام مجلس الدولة تميل إلى الإنحياز خاصة في حالة وجود فراغ تشريعي ينظم دواعي الحجب وحدود ذلك الحجب وتوقيتاته، حيث قضت المحكمة الإدارية العليا بأحد أحكامها بأن "الحريات والحقوق العامة التي كفلها الدستور ليست طليقة من كل قيد وإنما يجوز تنظيمها تشريعيًا بما لا ينال من محتواها، ومن ثم فإن القيود التي يفرضها المشرع على تلك الحرية تمثل استثناء من الأصل الدستوري المقرر بكفالة وضمان حرية التعبير، ومن ثم يجب أن تكون في أضيق الحدود، ولما كانت التشريعات المصرية لم تحدد الحالات التي تستدعي حجب المواقع الإلكترونية إلا أن هذا الفراغ التشريعي لا يخل بحق جهة الإدارة في الحجب حينما يكون هناك مساس بالأمن القومي أو المصالح العليا بما لتلك الأجهزة من سلطة في مجال الضبط الإداري لحماية النظام العام بمفهومه المثلث الأمن العام والصحة العامة والسكينة العامة للمواطنين".[٣٢٣٥]

وقد أقر ذلك الحكم الترخيص باستخدام الطيف الترددى كونه أحد الموارد الطبيعية شرط أن يكون ذلك محكومًا بالمصلحة العليا للدولة والأمن القومي للبلاد.[٣٢٣٦]

(٣٢٣٤) تثور تلك المشكلة في دولة الكويت خاصة لأن النسيج الاجتماعي هناك يحتوي على فئات مختلفة اجتماعيًا، فهناك بدو وحضر وشيعة وسنة، ولوجود العديد من الحسابات الوهمية على موقع تويتر تسيء للنظام العام الكويتي المعلوماتي وغير المعلوماتي من خلال العديد من المغردين الذين يخلوا بالأمن العام.

(٣٢٣٥) انظر الطعن رقم ١٠١٧١ لسنة ٥٤ ق. عليا المحكمة الإدارية العليا – الدائرة الثانية -حكم غير منشور- وكانت الدعوى تطالب بحجب المواقع الإلكترونية لارتكابها جرائم جنائية ضد الدولة.=

= "ويتعين التفرقة في هذا الصدد بين التعدي على الحق الفردي للأشخاص وبين التعدي على المجتمع وأمنه وأمانه وإن كانا كلاهما ممقوتاً ومجوجاً تلفظه الشرائع ونصوص الدستور والقانون ، أما حال المساس بأمن المجتمع وأمانه فلا يدرأه إلا أن يوصد منبع هذا الخطر موقعًا على شبكة الإنترنت أو غيره".

(٣٢٣٦) انظر الحكم السابق.

"وقد انتظم القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات مبادئ وقواعد لتنظيم جميع أنواع الاتصالات إلا ما استثنى بنص خاص، وناط بالجهاز القومي لتنظيم الاتصالات وبوزير الاتصالات وتكنولوجيا المعلومات تنظيم وسائل إرسال أو استقبال الرموز أو الإشارات أو الرسائل أو الكتابات أو الصور أو الأصوات، وذلك أيًا كانت طبيعتها سواء كان الاتصال سلكيًا أو لا سلكيًا وخدمة الاتصالات الدولية بين المستخدمين في مصر وبين الدول الأجنبية من خلال المعايير الدولية للاتصالات بما في ذلك الطيف الترددي الذي يمثل الموجات التي يمكن استخدامها في الاتصال اللاسلكي طبقًا لإصدارات الاتحاد الدولي، وضمان الاستخدام الأمثل لهذا الطيف مع مواكبة التقدم العلمي والفني والتكنولوجي ووضع قواعد وشروط منح التراخيص الخاصة باستخدامه ، وإصدار هذه التراخيص وتجديدها وإلغائها ومراقبة تنفيذها، وذلك كله بما لا يخل بالمصلحة العليا للدولة والأمن القومي للبلاد".

ومن القضايا التي أثيرت في فرنسا والتي تخص الأمن المعلوماتي ما قامت به شركة جوجل الأمريكية عندما استخدمت برنامج التصوير الحي للشوارع (street view) إذ انتهكت حينها أحكام قانون حماية المعلوماتية والحريات الفرنسي رقم (١٧-٧٨) وقد اعتبرتها اللجنة القومية للمعلوماتية في فرنسا منتهكة لأحكام القانون العام لعدم إخطارها لأن الخدمة تقدم معلومات تعريفية عن أفراد يمكن تحديدهم بالدمج مع بيانات الموقع ومعالجتها.(٣٢٣٧)

وعلى صعيد التشريعات العربية نصت المادة ٣٧ قانون المعاملات الإلكترونية الكويتي رقم٢٠ لسنة ٢٠١٤ على أنه "فيما عدا ما تختزنه الجهات الحكومية الأمنية بسجلاتها وأنظمتها المعالجة الإلكترونية من بيانات أو معلومات تتعلق بالأشخاص – لاعتبارات تتعلق بالأمن الوطني للبلاد – يجوز للشخص أن يطلب من أي من الجهات المذكورة بالمادة السابقة بإطلاق على البيانات أو المعلومات الشخصية المسجلة لديها....".(٣٢٣٨)

وتأكيدا على امكانية التخلي عن فكرة الخصوصية المعلوماتية إذا تعلق الأمر بالنظام العام للدولة، وذلك كمثال مانص عليه قانون الأمن ومكافحة الإرهاب والجريمة ٢٠٠١ في المملكة المتحدة (الفصل ٢٤)، حيث نصت المادة ١٧ من الجزء الثالث منه على نطاق سلطات الكشف عن المعلومات حيث تحدد الفقرة الأولى بنودًا معينة لتلك السلطة، وأحالت للجدول رقم ٤ المرفق بالقانون ،ونصت الفقرة الثانية من ذات المادة على أن تلك البنود الواردة في ذلك القسم تطبق للكشف عن المعلومات بواسطة أو لمصلحة السلطة العامة إذا كانت أغراض الكشف تلك المعلومات مصرح به بموجب البنود التالية:-

أ) لأغراض أي تحقيق جنائي سواء يجرى بالفعل أو سيتم لاحقًا سواء بالمملكة المتحدة أو أي مكان.

ب) لأغراض أي إجراءات جنائية، سواء تتم بالفعل أو ستبدأ لاحقًا سواء بالمملكة المتحدة أو أي مكان آخر.

بالإضافة إلى ما سبق صدرت العديد من قوانين الخصوصية الأمريكية على مستوى القطاعات sectoral privacy laws كمثال تبنى قسم الصحة والخدمات الإنسانية The department of Health

---

(٣٢٣٧)د/ وليد السيد سليم، ضمانات الخصوصية فى الإنترنت – دار الجامعة الجديدة ٢٠١٢ ص٦٠٠.

وللمزيد انظر أيضًا حقوق الأفراد بشأن المعالجة الآلية للبيانات ومثالها كما نص عليها قانون (١٧-٧٨) للمعلوماتية والحريات للحق فى الاستعلام، والحق في الإطلاع كي يمارس الفرد دوره في حماية الأمن المعلوماتي كرقابة ذاتية إلى جانب الرقابة والحماية الإدارية للأمن المعلوماتي، والجدير بالذكر أن المشرع الفرنسي أقام توازنًا بين الأمن المعلوماتي والحق في تداول المعلومات الهامة والحساسة كالبيانات الخاصة بالأمن العام والشرطة والدرك وأمن الدولة والمخابرات والأمن الخارجي، والبيانات المتعلقة بوزارة العدل وملفات السجناء و، لم يجعل الاطلاع مباشرًا على تلك المعلومات للشخص نفسه بل عن طريق غير مباشر إذ يقوم المواطن بتقديم طلب للجهة الإدارية (اللجنة القومية للمعلوماتية والحريات إذ تقوم بندب قاضي حالي أو سابق يقوم بإجراء تحريات لازمة وإطلاع كافٍ.

(٣٢٣٨) أنظر قانون المعاملات الإلكترونية الكويتي رقم٢٠ لسنة ٢٠١٤ منشور بجريدة الكويت اليوم العدد ١١٧٢ السنة الستون ٦٩ بتاريخ ٢٠١٤/٢/٢٣.

Human Services فى العام ٢٠٠١ قواعد - مصرح بها من الكونجرس – لا تجيز الإفصاح عن المعلومات الشخصية الصحية ما لم يكن ذلك في إطار من القانون(٣٢٣٩).

المبحث الثالث

في

مدى إرتباط الأمن المعلوماتي بمبدأ سيادة الدولة

لا يجب الاعتماد على نظريات قانونية للتأسيس للأمن المعلوماتي "فرغم النص الصريح على المساواة في السيادة بين الدول، إلا أن السيادة المؤسسة على حقوق نظرية فقط تتضاءل إذا ما قورنت بالسيادة التي تؤسس على القوة والسيطرة".(٣٢٤٠)

وتنطلق المواقف القانونية للأمن المعلوماتي على الصعيد الدولي من منطلق براجماتي "فاستشعار الدولة لأراضيها أو للمناطق الخاضعة لولايتها أو لمناطق من أعالي البحار لا يثير أية مشاكل قانونية، بينما يثير استشعار دولة لأراضي دولة أخرى من الفضاء الذي يعلو إقليمها بعض المشاكل القانونية، لتعارض مصالح الدولتين. وباتباع هذا الأسلوب في التحليل ترى بعض الدول أن الاستشعار عن بعد من الفضاء الخارجي، البعيد عن سيادة الدول، عملاً قانونيًا حيث إن هذا النشاط عمل فضائي وليس عملاً أرضيًا، وبالتالي فإن القيود الناتجة من تطبيق مبدأ السيادة الإقليمية لا مكان لها.

وبعض الدول الأخرى ترى: أن الاستشعار من بعد يعد نشاطًا ينتهك سيادة الدولة، وتقف بعض الدول موقفًا وسطًا، حيث ترى شرعية أنشطة الاستشعار، ولكنها ترفض استشعار أراضيها دون موافقتها المسبقة، أو على الأقل دون إعلام مسبق بذلك من الدولة القائمة بالاستشعار"(٣٢٤١).

(٣٢٣٩) While, facially restrictive, in reality, those rules permit broad disclosure of personal health information to the government in response to a warrant, court order, subpoena, discovery request administrative request, investigate demand or even a law enforcement official's "request".

(٣٢٤٠) د/ ممدوح فرجاني: المرجع السابق ص٢٠٧ في إشارة لرأي :

Myers, Davids, Remote sensing and National sovereignty over natural Resources, Assessment of the Mexican view, ١٤ california western international law Journal. (١٩٨٤) p. ٢٤.

(٣٢٤١) Christol, carl Q., Remote sensing and International law– ٥ Annals of Air and space law– (١٩٨٠) p. ٧٣١.

"وهناك من الدول من تقبل بالشرعية العامة لأنشطة الاستشعار من بعد، ولكنها ترى ضرورة تقييد نشر البيانات الناتجة عن ذلك. ومن هنا يظهر أن جميع الدول التي تعارض حرية الاستشعار من بعد من الفضاء الخارجي، أو تلك الدول التي ترى ضرورة وضع قيود معينة عليه، تعتقد أن الحصول على معلومات معينة عن كمية ونوع ومكان المصادر الطبيعية الخاصة، مسألة قومية خاصة تتطلب الاعتبارات الاقتصادية والأمنية للدولة المحافظة عليها".

ويثور تساؤل بخصوص إمكانية ربط السيادة الوطنية بتحقيق الحماية المعلوماتية للدولة، ويمكن الرد على ذلك عمليًا بتعارض أي امتداد للسيادة الأرضية للفضاء الخارجي مع الحقائق العلمية، فالسيادة الأرضية للدولة في الفضاء الخارجي لا يمكن تحديدها لتداخل الحدود السيادية الأفقية للدول علاوة على أنه لا يوجد مكان معين على الأرض يعد ثابتًا" بالنسبة للفضاء الذي يعلو الفضاء الجوي[٣٢٤٢].

مؤدى ما سبق أنه بالمفهوم التقليدى قد تغيرت مفاهيم الحدود فمن السهل تحديد الحدود الطبيعية والبحرية، وإن كان ذلك الأمر من الصعوبة بمكان في تحديد المجال الجوي نظرًا لوجود الأقمار الصناعية والبث الفضائي وعمليات اختراق الأمن المعلوماتي بصورة عامة.

ومن أمثلة انتهاك الأمن المعلوماتي على الصعيد الدولي: القرصنة المعلوماتية على سفن حلف شمال الأطلنطي من خلال قرصنة نظم الحاسبات الآلية الخاصة بالقوات المسلحة الفرنسية عام ١٩٩٤[٣٢٤٣]، وكذلك القرصنة المعلوماتية على نظام المعلومات الخاص بوزارة الدفاع الأمريكية (البنتاجون) وكانت إبادة البشرية على المحك.[٣٢٤٤]

أما في الإمارات العربية المتحدة فقد تعرض الأمن المعلوماتي هناك لخطر وشيك ولم تسعف النصوص العقابية حينها في مجابهة ذلك سوى ببعض النصوص التي تضمنت عقوبات يسيرة في قانون الاتصالات نفسه.[٣٢٤٥]

فإذا كان تهديد الأمن المعلوماتي تتعاظم آثاره على الصعيد الدولي عن طريق اختراق الحواسب الآلية والحصول على آلاف الشفرات، فإن الأمن المعلوماتي العربي أصبح مهددًا كذلك بالاختراق عن طريق التجسس الإلكتروني.

ويذهب رأي – ونؤيده – في أن الأمن المعلوماتي العربي لا يجد تحديه الأكبر في عالم الإنترنت السفلي من المخترقين بقصد غسل الأموال والدعارة والجنس والقمار ولكن في محاولات التجسس الدولي، وتغير مفاهيم التجسس من المفهوم التقليدي إلى عمليات التجسس الإلكترونية.[٣٢٤٦]

وقد فطنت القيادة السياسية الأمريكية مبكرًا لتدعيم الضبط الإداري في تعزيز الأمن المعلوماتي.[٣٢٤٧]

([٣٢٤٢]) Hopkins, Grayl, Legal implications of Remote sensing of Earth Resources by satellites, ٧٨ Military law Review, p. ٧٧.

(١)د/فهد سلطان:المرجع السابق ص٤٧ .

(٣٢٤٤)مقال بمجلة زهرة الخليج – الإمارات – العدد ١٠٢٨ – س٢٠.

(٣٢٤٥) تقرير بعنوان : عمليات تخريب تهدد الأمن القومي على شبكة الإنترنت بتاريخ ٢٠٠٠/٢/١٧م على موقع http:news.bbc.com.U.K مشار إليه في مؤلف د/ فهد سلطان، المرجع السابق ص٦/ وفي تلك القضية تمكن شخص أوروبي من اختراق شبكة اتصالات في عام ٢٠٠٠ وعلى إثر ذلك أصيبت الشبكة بشلل لمدة أسبوعين.

(٣٢٤٦) المرجع السابق ص٧٨، ٧٩.

(٣٢٤٧) مجلة إنترنت الوطن العربي – إعداد فاطمة نعناع – على موقع www.ditent.co.ae مشار إليه في المرجع السابق ص٨١.

ومن الإشكاليات التي تثور بشأن الأمن المعلوماتي في ضوء سيادة الدولة ما يتعلق بتحديد موقع الجاني الذي قد يوجد بإقليم دولة أخرى، لذا يتطلب تعزيز الأمن المعلوماتي وجود تعاون دولي لمكافحة الجريمة المعلوماتية، فضلاً عن توحيد المفاهيم المتعلقة بالأمن المعلوماتي من خلال اتفاقيات دولية بشرط أن تراعى السيادة القومية والإقليمية. (٣٢٤٨)

المبحث الرابع

في

مدى وجود أطر تشريعية ورقابية معلوماتية

يرى الفقه المقارن أن المعالجة التشريعية للأمن المعلوماتي تكون بطريقتين **أولهما:** قوانين التجسس، **وثانيهما:** قوانين الاتصالات. (٣٢٤٩)

غير أنه تجدر الإشارة إلى أن بعض التشريعات تعاني قصورًا تشريعيًا في الأمن المعلوماتي ،ويتمثل القصور التشريعي أحيانًا بالنسبة للأمن المعلوماتي في حداثة الفعل المؤدى لانتهاك الأمن المعلوماتي، **ومثال ذلك:** جريمة الدخول غير المصرح للنظام المعلوماتي، فالمتتبع لتلك الجريمة يجد أنها من الصعوبة بمكان كي تتم معالجتها تشريعيًا بشكل كامل بموجب النصوص العقابية التقليدية. (٣٢٥٠)

قامت بتخصيص ملياري دولار لمواجهة أخطار اختراق شبكات الكمبيوتر الأمريكية، وذلك في عهد الرئيس (بيل كلينتون) وذلك بعد اختراق النظام الأمني لشبكة وكالة الفضاء الأمريكية NASA رغم قوة وتعقيد برامج الأمن المعلوماتي للوكالة وقد قام المخترق بالفعل في تدمير ملفات قدرت قيمتها بحوالي سبعين ألف دولار

ومن الأمثلة الهامة كذلك: اختراق النظم المعلوماتية في المنتدى الاقتصادي العالمي الذي عقد في سويسرا (تقرير بعنوان – قراصنة الكمبيوتر يتسللون -بتاريخ ٢٠٠١/٢/٤م على شبكة إنترنت بالموقع http:newsbbc.co.uk.

(٣٢٤٨) في ذلك المعنى انظر محمد أحمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١٦ ص١٥٤.

وقد أقرت الأمم المتحدة في المادة الرابعة من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة ذلك بأنه "يتعين على الدول الأطراف أن تؤدي التزاماتها بمقتضى هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة والسلامة الإقليمية للدول، ومع مبدأ عدم التدخل في الشئون الداخلية للدول الأخرى" مشار لذلك النص في المرجع سابق الذكر نقلاً عن إتفاقية الأمم المتحدة خلال المؤتمر الدولي الذي عقد في إيطاليا بمدينة باليرمو الإيطالية، الفترة من (١٢ – ١٥) ديسمبر ٢٠٠٠م".

(١) Abraham D. Safaer, National security and leaks, the Government's Authority to Discipline itself. International studies in Human Rights volume ١٦, p. ٦٩.

(٣٢٥٠) أ. د/ عبد الإله محمد النوايسة: جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية "دراسة مقارنة" – المجلة القانونية والقضائية الصادرة من مركز الدراسات القانونية والقضائية وزارة العدل – دولة قطر – العدد الأول – (السنة العاشرة) يونيو ٢٠١٦ ص١٠، ١١.

ويتهدد الأمن المعلوماتي للإدارة بصورة كبيرة لاعتماد الإدارة في الوقت الحالي في إدارتها لمرافقها على نظام الحكومة الإلكترونية، وقد يصل الأمر لانتهاك أمن الدولة الوطني، كالاطلاع على معلومات تمس أمن الدولة، أو الوصول إلى أنظمة التحكم في محطات المفاعلات النووية[٣٢٥١].

وتجدر الإشارة في مجال الضبط التشريعي خاصة فيما يتعلق بقوانين الكمبيوتر أنها تتفرع إلى العديد من التعريفات، وذلك كالتالي:

١) **تشريعات حماية برامج الكمبيوتر:** وهي تعكس الاتجاهات العالمية في إدراج الملكية الفكرية ضمن تنظيمات التجارة الدولية تبعا للاقتصاد الرقمي والاقتصاد المؤسسي على المعرفة.

٢) **تشريعات الأصول الإجرائية الجزائية:** وهي في الواقع تطوير لقواعد الإثبات في الإجراءات لكنها تتصل بالحقوق الجديدة المعترف بها في الميدان التقني المعلوماتي.

٣) **تشريعات المحتوى الضار:** وهي تهدف في المقام الأول إلى الحماية من محتوى المعلومات الضارة.

٤) تشريعات معايير الأمن المعلوماتي وهي تهدف إلى تبادل البيانات والتشفير ويستهدف البعض دراستها ضمن محتوى التجارة الإلكترونية.[٣٢٥٢]

مؤدى ما سبق أن العديد من الدول تلجأ في سبيل حماية أمنها المعلوماتي إلى تطبيق قوانين موضوعية وأخرى إجرائية على العكس من دول أخرى تعتمد على قوانين غير فعالة.[٣٢٥٣]

(٣٢٥١) Brain bridge. D: introduction to computer law, London ٢٠٠٠, fourth edition p. ٣٠٧.

(٣٢٥٢) هناك العديد من تشريعات الأمن المعلوماتي على مستوى العالم نذكر منها على سبيل المثال: في الولايات المتحدة الأمريكية قانون خصوصية الاتصالات الإلكترونية لعام ١٩٨٦، وقانون خصوصية الاتصالات لعام ١٩٩٧، وقانون خصوصية المعطيات لعام ١٩٩٧ – أما في ألمانيا فنجد قانون حماية المعطيات ومشروع قانون حماية البيانات عام ٢٠٠٠ المتوافق مع القانون الأوروبي لعام ١٩٩٥، وفي فرنسا قانون المعالجة الآلية للمعطيات والمعدل في عام ٢٠٠٠، وفي النرويج قانون تسجيل البيانات الشخصية لعام ٢٠٠٠، وفي بلجيكا قانون حماية الحياة الخاصة فيما يتعلق بالتعامل مع المعطيات الشخصية المعدل عام ٢٠٠٠، وقانون حماية البيانات الشخصية والوثائق الإلكترونية = =لعام ٢٠٠٠، وفي بريطانيا قانون حماية المعطيات لعام ١٩٨٤ وقانون حماية البيانات لعام ١٩٩٨ المعدل لقانون ١٩٨٤، وقانون حرية المعلومات لعام ٢٠٠٠، وفي اليابان قانون حماية المعلومات في الشخصية رقم ٩٥ الصادر في ١٩٩٨/١٢/١٦ وفي التشيك قانون حماية البيانات الشخصية في نظم المعلومات لعام ١٩٩٢ وقانون حماية البيانات لعام ٢٠٠٠، وفي هنجاريا قانون حماية البيانات الشخصية ونشر البيانات للمصالح العامة لعام ١٩٩٢، وفي رومانيا قانون حماية البيانات لعام ١٩٩٢، وفي كوريا الجنوبية قانون حرية المعلومات لعام ١٩٩٦، وفي روسيا قانون حماية المعلومات لعام ١٩٩٥، وفي إيطاليا قانون حماية البيانات لعام ١٩٩٦، وفي ليتوانيا قانون الحماية القانونية للبيانات الشخصية لعام ١٩٩٦، وفي الصين نظم حماية وإدارة الشبكات لعام ١٩٩٧، وفي تايلاند قانون حماية البيانات في القطاع العام لعام ١٩٩٨، وفي الهند مشروع قانون حماية البيانات الموصى بإصداره من الفريق الوطني لتقنية المعلومات وتطوير البرمجيات وفي جنوب أفريقيا قانون الوصول إلى المعلومات لعام ٢٠٠٠، وفي تركيا مشروع قانون حماية البيانات الشخصية لعام ٢٠٠٠.

(١)David weissbrodt, cyber – conflict, cyber – crime, and cyber Espionage, Minnesota Journal of Internatinal Law's ٢٠١٣ symposium, p. ٣

وبالنظر إلى التجربة الأمريكية في تعزيز الأمن المعلوماتي نجدها تنقسم إلى شقين أولهما المعايير الفنية Technical standatds والتشريعات والرقابة Legislation and Moitoring ونتناولهما كالتالي:- (٣٢٥٤)

أولاً: المعايير الفنية:

تم إنشاء المعهد القومي للمعايير القياسية والتكنولوجيا كباكورة أولية في عام ١٩٠١ يتتبع وزارة التجارة الأمريكية، علاوة على وحدة المعلومات التابعة لمعمل تكنولوجيا المعلومات حيث تضع سياسات ومعايير تبادل المعلومات. (٣٢٥٥)

ومن أهم اللجان لجنة الحاسب الآلي والاتصالات التابعة للمجلس القومي للبحوث، وترجع أهمية تلك اللجنة إلى أنها تشفر المعلومات والبيانات "cryptography". (٣٢٥٦)

ثانيًا: التشريعات والرقابة:

لن تكتمل منظومة الأمن المعلوماتي إلا بوجود إطار تشريعي كي تطبق معايير الأمن القومى المعلوماتي، لذا صدرت في الولايات المتحدة الأمريكية قوانين تعزز ذلك المفهوم كقانون حرية المعلومات في عام ١٩٦٦، وإذا كان غرض ذلك القانون هو تعزيز الحق في المعرفة وتداول المعلومات إلا أن التعديلات اللاحقة على ذلك القانون كانت تهدف إلى تعزيز السرية والأمن المعلوماتي، والدليل صدور التعديل الذي يقضي مجموعة المعلومات الإلكترونية Electronic freedom of Information Act)) (EFIA) لتعزيز الأمن المعلوماتي حيث يطالب جميع جهات الإدارة (بأتمتة الملفات) أي جعل الملفات الورقية في صورة إلكترونية وإعداد غرف خاصة لإطلاع المواطنين عليها.

ويأتي القانون الفيدرالي لأمن المعلومات الصادر في عام ٢٠٠٢ كأهم التشريعات التي تعزز الأمن المعلوماتي لجهة الإدارة في الولايات المتحدة الأمريكية من خلال إلزام المؤسسات والهيئات بالإجراءات القياسية التي أصدرها المعهد القومي للمعايير القياسية والتكنولوجيا. (٣٢٥٧)

For more: (١) Susan W. Brenner:– cyber crime– criminal threats for cyberspace (٢٠١٠)

(٢) Jonathan clough, principles of cyber crime (٢٠١٠).

(٣) Richard Clarke, threats to U.S. National security: proposed partnership initiatives towards preventing cyber terrorist Attacks, ١٢ Depaul Bus, L. J. (١٩٩٩ – ٢٠٠٠).

(٣٢٥٤) أنظر للمزيد راشد محمد المري: رسالة دكتوراه بعنوان "الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، رسالة مقدمة لكلية الحقوق جامعة القاهرة ٢٠١٣ ص١٨٢.

(٣٢٥٥) يقوم ذلك المعهد بإصدار القواعد والمعايير الفنية لتصنيف نظم المعلومات على أنها نظم قومية من وجهة نظر أمن المعلومات (المرجع السابق ص١٨٢).

(٣٢٥٦) المرجع السابق ص١٨٢ في إشارة إلى المرجع:

- Kasperson (W. K. Henrik) computer crimes and other crimes Against Information Technology in U. S. A., R. I. D. P. ٢٠٠١, P. ٢٧٣.

ـ أما على صعيد الرقابة تم إنشاء فريق الإستعداد في ٢٠٠٣ كجزء رئيسي من وحدة الأمن القومي الافتراضي (National cyper security Division). (٣٢٥٨)

وبالنظر إلى القانون الفيدرالي لإدارة أمن المعلومات نجد أنه يشكل حجر الزاوية للأمن المعلوماتي الأمريكي من الناحية القانونية، إذ يوفر إطارًا عامًا لتأمين نظم تكنولوجيا المعلومات والمحتوى المعلوماتي الرقمي في جميع الوكالات الفيدرالية الأمريكية، وكل الوكالات والمؤسسات الواردة في هذا القانون يتعين عليها تنفيذ الاحتياجات والمتطلبات التي يفرضها القانون،

ويتعين عليها تقديم تقارير سنوية إلى مكتب الإدارة والميزانية والكونجرس عن مدى فعالية وقدرة هذه الوكالات على تنفيذ برامج أمن المعلومات وحماية ما لديها من معلومات. (٣٢٥٩)

ويوفر القانون إطارًا لتأكيد فعالية السيطرة الإدارية على مصادر المعلومات بما فيها حماية المعلومات الفيدرالية ونظم المعلومات مع تحديد الاختصاصات المتعلقة بكل رئيس وكالة فيدرالية(٣٢٦٠) ويهدف ذلك القانون إلى ثلاثة أهداف وهي:-

أولاً: السرية: الاحتفاظ بالقيود المرخص بها على الوصول إلى المعلومات وكشفها بما في ذلك الوسائل الخاصة بحماية الخصوصية الشخصية والمعلومات المملوكة لجهة ما.

ثانيًا: السلامة: منع دخول معلومات غير صحيحة أو إتلاف المعلومات.

ثالثًا: التوفر (الإتاحة): ضمان الوصول الفوري والموثوق به للمعلومات واستخدامها.

(٣٢٥٧) لمزيد من الإيضاح أنظر :راشد محمد المري، المرجع السابق ص١٨٣.

وتتلخص المعايير المذكورة في تعريف نظام المعلومات وتحديد نوع المعلومات من خلال تقسيمها في مجموعات محددة، وعمل توثيق كامل للنظم وعمل قياس للمخاطر التي قد يتعرض لها النظام.

(٣٢٥٨) في اعتقادنا أن أهم ما يميز ذلك الفريق هو شراكة القطاع الخاص مع جهة الإدارة الأمريكية. في إنشائه بغرض تنسيق الرد والتعامل مع مخاطر التأمين، بل يتعاون القطاع العام والقطاع الخاص بتطوير نظم التأمين والإصلاح لأنظمة المعلومات والاتصالات ضد الإختراقات المحتملة.

(٣٢٥٩) جمال غيطاس، المرجع السابق ص٢٣٤.

تم التصديق على هذا القانون كجزء من قانون الأمن الداخلي الذي تم إقراره عام ٢٠٠٢ وقانون الحكومة الإلكترونية ويطلب القانون من كل الوكالات والمؤسسات الحكومية تأمين معلوماتها ونظم المعلومات لديها التي تدعم عملياتها وأصولها بما فيها تلك التي تقدم أو تدار بواسطة وكالات أخرى متعاقدة ومقاولين أو أي مصدر آخر".

(٣٢٦٠) "على كل رئيس وكالة فيدرالية":- ١) تقييم المخاطر واتجاهات الضرر الذي قد يحدث من عمليات الوصول والاستخدام والإفصاح والتوزيع والتعديل والتدمير غير المرخص به للمعلومات أو لنظم المعلومات.

٢) تحديد مستويات أمن المعلومات المناسبة لحماية كل المعلومات ونظم المعلومات بوكالته.

٣) تنفيذ السياسات والإجراءات التي تقلل المخاطر لأدنى حد ممكن

٤) القيام باختيارات دورية وتقييم لأدوات أمن المعلومات.

في ذات السياق يرى الفقه القانوني الأمريكي أن الكونجرس كان عليه أن يرسم استراتيجية واضحة[٣٢٦١] لدور جهة الإدارة في تعزيز الأمن المعلوماتي من خلال الضبط الإداري، ويرتكز ذلك على إصلاح قانون إدارة أمن المعلومات الاتحادية لعام ٢٠٠٢.

Federal Information security Management Act of ٢٠٠٢ (FISAAA) [٣٢٦٢].

علاوة على ما سبق يمكن أن تقوم النظم القانونية الأوروبية بتغليب الأمن المعلوماتي في حالة تهديد الأمن العام، كمثال ما نصت عليه المادة الثالثة من القانون الفرنسي الصادر في ١٠ يوليو ١٩٩١ بالنص على الأسباب القانونية التي يمكن الاستناد إليها لإجراء المراقبة أو التصنت الإداري والتي جاء فيها (يجوز الإذن أو التصريح بالتصنت الذي يكون موضوعه أو محله البحث عن المعلومات التي تهم الأمن القومي، أوالمحافظة على المصالح الاقتصادية والعلمية للمجتمع الفرنسي، أومنع الإرهاب والمجموعات الإجرامية المنظمة وكذلك منع تكوين أو إعادة تكوين المجموعات التي تم حلها وفقًا لقانون ١٠ يناير ١٩٦٣[٣٢٦٣].

أضف إلى ماسبق أنه يمكن لبعض الدول أن تلجأ إلى قانون العقوبات لتعزيز الأمن المعلوماتي عن طريق الضبط التشريعي، كمثال قانون العقوبات الأسترالي في المادة ٤٧٨ منه ذهب إلى تجريم حيازة البيانات أو التحكم فيها بقصد استخدامها سواء بشخصه أو عن طريق شخص آخر ،ويمكن أن تمتد حيازة تلك البيانات إلى:

١) حيازة البيانات عن طريق حاسب آلي أو وحدة تخزين.

٢) حيازتها عن طريق مستند كمثال كتاب سارق لتقنيات أو أكواد في صيغة مكتوبة.

([٣٢٦١]) See office of TECH: Assessment, Electronic Record system anti– individual privacy ٥٧ (١٩٨٦).

([٣٢٦٢]) The Emergence of cypersecurity law, op .cit., p.١٢

ومن تلك المحاور التي أوردها الفقه القانوني الأمريكي:-

١) حماية البنية التحتية الحيوية (وخاصة شبكة الكهرباء والصناعات الكيماوية).

٢) تبادل المعلومات والتنسيق بين القطاعات.

٣) مراعاة انتهاكات السرقة أو التعرض للبيانات الشخصية كالمعلومات المالية.

٤) مراعاة السياسة العقابية لجرائم الإنترنت.

٥) مراعاة الخصوصية في مجال التجارة الإلكترونية.

٦) الجهود الدولية في الأمن المعلوماتي.

٧) البحث والتطوير.

٨) تطوير القوى العاملة في مجال الأمن السيبري

(٣٢٦٣) د/ نشوى رأفت إبراهيم أحمد، المرجع السابق ص٢٧٧.

"واشترطت المادة الرابعة من القانون أن يتم الإذن بالمراقبة بإذن مكتوب ومسبب يصدر من رئيس الوزراء أو من يقوم بتفويضه تفويضًا خاصًا"، وذلك بناء على اقتراح مكتوب ومسبب من وزير الدفاع، ووزير الداخلية والوزير المكلف بأعمال الجمارك" ومن الجدير بالذكر أن شروط وضوابط المراقبة الإدارية تراقبها اللجنة القومية للرقابة.

انظر بالتفصيل ص٢٧٨ من المرجع السابق فيما يخص اللجنة القومية للرقابة وتشكيلها وآليات عملها.

٣) التحكم في بيانات موجودة في حاسب آلي مملوك لشخص آخر سواء داخل أو خارج أستراليا (كمثال معلومات موجودة على موقع إلكتروني لآخرين وقراءاته) (٣٢٦٤).

وبالنظر إلى الحماية الواجبة للبيانات الشخصية الحساسة عند تعزيز الأمن المعلوماتى تضمن دليل حماية البيانات الأوروبي لعام ١٩٩٥ حماية فاعلة ضد استخدام تلك البيانات كالبيانات المتعلقة بالصحة والأمور المالية، وإن كانت ظهرت العديد من الإشكاليات بشأنه جراء قدرة الجهات الخاصة والحكومية على الوصول للبيانات لذا ظهر التوجه الأوروبي نحو إيجاد جهة رقابة تعمل على تنفيذ القانون فيما يعرف في بعض الدول باسم (المفوض) وفي دول أخرى (المراقب)، وفي دول ثالثة (مسجل البيانات)، ويفرض دليل حماية البيانات على الدول الأعضاء التزامات فيما يخص التأكد من الطابع الأمنى للبيانات الشخصية التي ترتبط بالمواطنين الأوروبيين كى تحظى بنفس المستوى من الحماية إذا تم نقلها إلى خارج الحدود ، ويحظر نقل البيانات إلى الدول التي لا توفر قوانينها حماية للخصوصية. (٣٢٦٥)

علاوة على ما سبق أصدرت المفوضية الأوروبية في عام ٢٠٠٠ نموذجًا جديدًا لدليل معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية، وقد وسع ذلك الدليل من نطاق الحماية للأفراد عن طريق حماية البيانات المنقولة عبر الإنترنت ومنع السلوكيات الاتصالية الضارة في السوق التجاري الإلكتروني مثل (SPAM) البريد الإلكتروني. (٣٢٦٦)

أما على صعيد النظام القانوني الفرنسي تعد فرنسا من أوائل الدول التي تدرجت التشريعات فيها بشأن الأمن المعلوماتى وخاصة فيما يتعلق بمبدأ استغلال فضاء الدولة في بث المعلومات. (٣٢٦٧)

(٣٢٦٤) Jonathan clough, op. cit., p. ١٢٤.

والجدير بالذكر أن هناك عدة تشريعات تم إدخالها إلى الكونجرس مؤخرًا تمس الأمن السيبري ومن تلك القوانين قانون خصوصية المعلومات الشخصية وأمنها لعام ٢٠١٤ من شأن ذلك القانون حفاظ الشركات على المعلومات الاستهلاكية في مأمن من قراصنة الكمبيوتر.

وهناك أيضًا قانون أمن البيانات لعام ٢٠١٤ (Data security Act ٢٠١٤) ويلزم ذلك القانون الكيانات بما في ذلك المؤسسات المالية والوكالات الاتحادية بحماية أفضل للمعلومات الحساسة، والتحقق من الخروقات الأمنية المعلوماتية وإخطار المستهلكين بذلك عند وجود خطر كبير من سرقة الهوية والاحتيال.

وثالثًا هناك القانون الوطني للأمن السيبراني وحماية البنية التحتية الحيوية لعام ٢٠١٣.

"The National cyber security and infrastructure protection ٢٠١٣ Act".

ويعمل ذلك القانون على تعاون المؤسسات الخاصة مع جهة الإدارة في تقاسم المخاطر عن السيبرية.

(٣٢٦٥) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، دار الفكر الجامعي ٢٠٠٦ ص٨٤.

(٣٢٦٦) المرجع السابق ص٨٥ "تجدر أن التوجيهات الصادرة عن الاتحاد الأوروبي عمومًا تجيز للدول الأعضاء تقييد وتضييق الأحكام بالاستناد إلى القواعد المقررة بشأن إنفاذ العدالة وتطبيق القانون كلما كان من الممكن حصول التناقض بين ما تقرره الأدلة التوجيهية وبين قواعد النظام العام".

(٣٢٦٧) د/ محمد السعيد رشدي: الإنترنت والجوانب القانونية لنظم المعلومات – مؤسسة دار الكتب للطباعة والنشر والتوزيع ١٩٩٧ ص٥٦. =

= تعرض الرأي السابق إلى أن المشرع الفرنسي تبنى في البداية مبدأ حرية الاتصالات في قانون ٢٩ يوليو ١٩٨٢ ثم أصدر قانون ١٧ يناير ١٩٨٩ بشأن حرية الاتصال، وبعدها صدرت تشريعات لاحقة خاصة عام ١٩٩٠ بشأن تنظيم المرفق العام للبريد والإتصالات عن

علاوة على ماسبق من أطر رقابية في سبيل تعزيز الأمن المعلوماتي يمكن أن تمارس جهة الإدارة رقابتها مسبقًا على بث المعلومات، وتختلف تلك الرقابة بحسب النظام القانوني ففي القانون الإنجليزي تكون الرقابة على بث المعلومات وفقًا للقواعد العامة دون حاجة إلى لجهة الإدارة بصفة عامة وبالتالي تكون تلك الرقابة وفقًا للقواعد العامة دون الحاجة إلى وجود جهة إدارية مستقلة.

علاوة على ما سبق تسلك العديد من التشريعات أسلوبًا مغايرًا في الرقابة وبالتالي تكون الرقابة بين مجالس ولجان وجهات مختصة، فقد عرفت ألمانيا سلطة رقابة المفوض "وهو يعين خصيصًا لنظم المعلومات ويراقب عمليات بنوك المعلومات الشخصية. (٣٢٦٨) وهو ما سوف نتناول بعض ملامحه في الجزئية الخاصة بالضبط الإداري.

وبالنظر إلى الأسلوب الفرنسي في الرقابة نجد أن الدولة أقامت نظامًا نموذجيًا للرقابة على معالجة المعلومات وبثها في القانون رقم (١٧-٧٨) الصادر في يناير ١٩٧٨ بشأن معالجة المعلومات والحريات. (٣٢٦٩) وإلى جانب ذلك هناك لجنة أخرى للرقابة على بث المعلومات باستخدام أجهزة الحاسب الآلي وهي اللجنة الوطنية للاتصالات والحريات (C.N.C.L) وقد خولها المشرع سلطة الرقابة بوسائل متنوعة على موضوع ومضمون البرامج التي يبثها الحاسب الآلي، وأساليب البث وعمليات الإرسال المرخص بها قانونًا. (٣٢٧٠)

بعد ثم مرسوم ٤ فبراير ١٩٩٢ بشأن تحديد معدات الاستقبال= = المعتمدة ومواصفاتها وكل ذلك كشف بوضوح عن نية المشرع الفرنسي في تحرير نظام البث عبر فضاء الدولة.

(٣٢٦٨) المرجع السابق ص٦٤، ٦٥.

(٣٢٦٩) المرجع السابق ص٦٧. =

= ومن مهام اللجنة الرقابة على تنفيذ معالجة المعلومات وحماية النظام العام واحترام حريات الآخرين وإنشاء نظم للمعلومات وتلقي الإخطارات بذلك، والتحقق من احترام نظم المعلومات لأحكام القانون.

(٣٢٧٠) راجع موقف التشريع الفرنسي واتجاهات القضاء فيما يتعلق بحماية المعلومات الشخصية، المجلة الدولية للقانون المقارن، ١٩٨٧، ص٦٢ وما بعدها مشار إليه في المرجع السابق ص٦٦ وما بعدها.

والجدير بالذكر أن تلك اللجنة مستقلة في عملها ولا تخضع للسلطة الرئاسية أو الوصائية للجهاز الإداري في الدولة بل تخضع لرقابة القضاء فقط.

الباب الثانى

في

أثر المحددات المعلوماتية

على مفاهيم الضبط الإداري ووسائله

تمهيد وتقسيم:

توثر المحددات المعلوماتية على مفاهيم الضبط الاداري ووسائله ،وذلك لحداثة المفاهيم القانونية المعلوماتية ،وتثار التساؤلات عما إن كانت تلك المحددات المعلوماتية تؤدى لنشأة مايسمى بمفهوم الضبط الاداري الالكترونى ،أم إن الأمر لا يرقى لذلك ، ومايعد متطلبا هو فقط التحديث فى مفاهيم ووسائل الضبط الاداري ،لذا ستكن معالجة ذلك الباب فى فصلين كالتالي:

الفصل الاول :أثر المحددات المعلوماتية على مفاهيم الضبط الإداري.

الفصل الثاني: أثر المحددات المعلوماتية على وسائل الضبط الإداري.

الفصل الأول

في

أثر المحددات المعلوماتية على

مفاهيم الضبط الإداري

تؤثر المحددات المعلوماتية على مفاهيم الضبط الاداري لكون الإخلال بالأمن المعلوماتى مفهوما متطورا يستلزم تطورا مماثلا فى المفاهيم القانونية عامة، ومفاهيم الضبط الاداري بصورة خاصة،لذا ستكون معالجة ذلك الفصل كالتالي:

المبحث الأول:التعريف اللغوي والاصطلاحى للضبط الادارى.

المبحث الثانى: مدى مواءمة المفهوم الواسع للضبط الإداري مع تعزيز الأمن المعلوماتى.

المبحث الثالث: أهمية وخصائص الضبط الإداري الإلكتروني ومتطلباته.

المطلب الأول:أهمية الضبط الإداري الإلكتروني.

المطلب الثانى:خصائص الضبط الإداري الإلكتروني.

المطلب الثالث:متطلبات الضبط الإداري الإلكتروني.

المبحث الأول

في

التعريف اللغوى والاصطلاحى

للضبط الإدارى

يمكن تعريف "الضبط" لغويًا بأنه "تحديد الأمر على وجه الدقة"[٣٢٧١] أو إعادة الأمور إلى نصابها، ووضعها بالاطار القانوني الصحيح عقب إصابتها بخلل أو إضطراب".[٣٢٧٢]

ويُشتق من كلمة ضبط "الضابطية" ويقصد بها جند الوالي المكلفين بجمع الأموال، والمحافظة على الأمن، والقبض والتعقب، ولإحضار للمجرمين وغيرهم إلى باب الحكومة. ويمكن كذلك أن ترادف كلمة الضبط كلمة بوليس "police".[٣٢٧٣]

أما على مستوى الدول يدل مصطلح البوليس "police" في المملكة المتحدة على ما تقوم به الإدارة من تعامل لرعاياها، من ضبط شؤونهم وخاصة المرتبطة بسياسة الدولة، وبنظامها الداخلي.[٣٢٧٤]

أما في فرنسا فيشير مصطلح البوليس لعدة أسس وأوامر ومبادئ تحقق ما تهدف إليه الجماعة من أهداف سياسية إلا أنه ما لبث أن استخدم مصطلح "letaplice" ومعناه الدولة الأكثر انضباطًا، وانتظامًا، وقانونية أي التي تقف قواعدها القانونية بالمرصاد لاستبداد السلطة الحاكمة.[٣٢٧٥]

وتجدر الإشارة إلى أن الفقه العربي اعتمد في تعريف الضبط الإداري على اتجاهات عدة، فمن الفقه العربي من عرف الضبط الإداري بأنه "حق الإدارة في أن تفرض قيودًا على الأفراد تحد بها من حرياتهم بقصد حماية النظام العام".[٣٢٧٦]

وذهب آخرون إلى التركيز على هدف الضبط الإداري مع تقييده بقيود ولذا يُعرف هذا الرأي الضبط الإداري بأنه "مجموعة ما تفرضه السلطة العامة من أوامر ونواه وتوجيهات ملزمة للأفراد بغرض تنظيم حرياتهم العامة، أو بمناسبة ممارستهم لنشاط معين بهدف صيانة النظام العام في المجتمع".[٣٢٧٧]

وركز بعضهم على المختص بالضبط الإداري وهدفه من خلال تعريف الضبط الإداري بأنه "النشاط الذي تتولاه الهيئات الإدارية، ويتمثل في تحديد النشاط الخاص بهدف صيانة النظام العام".[٣٢٧٨]

(٣٢٧١) انظر "المعجم الوجيز": مجمع اللغة العربية ١٩٨٠م ص٣٧٦-٣٧٧.

(٣٢٧٢) أنظر: المنجد في اللغة والأدب والعلوم، بيروت، الطبعة الأولى – المطبعة الكاثوليكية – بدون سنة نشر ص٤٤٥.

(٣٢٧٣) د/ سعاد الشرقاوي: القانون الإداري – القاهرة، الطبعة الأولى، دار النهضة العربية ١٩٨٣.

(٣٢٧٤) د/ طعيمة الجرف: القانون الإداري، القاهرة الطبعة الأولى، دار النهضة العربية ١٩٧٣ ص٤٢١. .

(٣٢٧٥) المرجع السابق، ص٤٣.

(٣٢٧٦) د/ سليمان محمد الطماوي: الوجيز في القانون الإداري "دراسة مقارنة"، القاهرة – دار الفكر العربي ١٩٧٩ ص٥٧٤.

(٣٢٧٧) د/ طعيمة الجرف: القانون الإداري والمبادئ العامة في تنظيم نشاط السلطات الإدارية. دار النهضة العربية ١٩٧٨ ص٤٨٧.

(٣٢٧٨) د/ محمود عاطف البنا في الوسيط في القانون الإداري – القاهرة – دار الفكر العربي ١٩٨٤ ص٣٧.

ويرى غير هؤلاء التركيز على هدف الضبط الإداري جملة وتفصيلاً، ولذا ذهب هذا الرأي إلى أن الضبط الإداري هو "مجموع الأنشطة التي تنفذها الإدارة منفردة بهدف المحافظة على النظام العام أو إعادة هذا النظام في حالة اضطرابه".(٣٢٧٩)

ومنهم من ذهب إلى التركيز على الجانب الأكثر اتساعًا في تعريف الضبط الإداري ومنح الإدارة سلطة أكثر إيجابية في المحافظة على النظام العام ومنحها ما يشبه التفويض العام في حفظه بتعريفه بأنه "مجموع القواعد والإجراءات التي تتخذها الإدارة، مستخدمة امتيازات السلطة العامة، بقصد تمكين الأفراد من التمتع بحقوقهم وحرياتهم، وبهدف المحافظة على النظام العام داخل الدولة، وتتم مباشرته إما بإجراءات قانونية أو بإجراءات مادية".(٣٢٨٠)

وفي اعتقادنا أن هذا الرأي هو أكثر الآراء اتفاقًا مع ما يتطلبه الأمن المعلوماتي من تدابير وقائية عن طريق اتخاذ قواعد وإجراءات إدارية سواء قانونية أو مادية بقصد الحفاظ على النظام العام داخل الدولة، إذ إن أهمية الضبط الإداري في مجال الأمن المعلوماتي تكمن فاعليته في إجراءاته الاستباقية بقدر أهم من معالجة آثاره اللاحقة.(٣٢٨١)

وعلاوة على ما سبق قام الفقه المقارن بتقسيم أدوار الضبط الإداري المتكامل بين إطارين: أولهما الإطار الضبطي الإداري، وثانيهما: الإطار الضبطي الإداري بالمعنى الفني، ويعني الإطار الأول بأفراد الضبط الإداري المخولين بالسلطات التنفيذية "Excutive powers" ممن لهم حق البحث والتفتيش والتحري، أما الإطار الثاني يتعلق بالفريق التقني من المواطنين العاديين ممن لا يملكون سلطات الضبط الإداري ويطلق عليهم أعضاء الخدمة "the members of the service".

وعلى صعيد الفقه الفرنسى ذهب "LAUBADERE" إلى التركيز على الطابع الوقائي والطابع النهائي للضبط الإداري، حيث يعرفه بأنه:" شكل من أشكال عمل الإدارة ويتمثل في تنظيم نشاط الأفراد من أجل ضمان حفظ النظام العام(٣٢٨٢)، فى حين يؤكد RIVERO على الطابع الغائي في تعريف الضبط الإداري حيث يعرفه بأنه "مجموعة تدخلات الإدارة التي ترمي إلى أن التصرف الحر للأفراد النظام الذي تطالب به الحياة في المجتمع"(٣٢٨٣).

(٣٢٧٩) د/ سعاد الشرقاوي، المرجع السابق ص١٣.

(٣٢٨٠) د/ محمد أنس قاسم جعفر: الوسيط في القانون العام "أسس وأصول القانون الإداري" بدون سنة نشر، بدون دار نشر ص١٦٣.

(٣٢٨١) في اعتقادنا أن الطابع الوقائي للنظام العام يفرض دورًا أكثر إيجابية نحو وظيفة الضبط الإداري والتى لا يجب حصرها في مجال الأمن المعلوماتي في قالب سلبي تقليدي، ولكن لا بد من التوازن بين حاجات الأمن المعلوماتي وتنظيم نشاطات الأفراد بحيث لا يؤدي ذلك إلى تقييدها أو الحد منها أو اختراقها بلا مبرر.

(٣٢٨٢) LAUBADERE (A. de.) et VENEXIA (J.C) et GAVDEMET (Y): Traite de droit Administratif, Paris, L.G.D.J., T. ١. ١٠e ed, ١٩٨٨, p. ٦٤٣.

مشار لذلك المرجع في مؤلف د/ عادل أبو الخير – الضبط الإداري وحدوده: الهيئة المصرية العامة للكتاب ١٩٩٥ ص٨٣.

(٣٢٨٣) RIVERO (J.): droit administrative, Paris, DALLOZ, ٦e ed. ١٩٧٥, p. ٣٩٨.

مشار إليه في المؤلف السابق ص٨٤.

وفي اعتقادنا أن تعريف الفقيه CLAUDEKLEIN هو الأكثر تواؤمًا مع الأمن المعلوماتي، حيث اعتمد على أن السمة الأهم للضبط الإداري هي القابلية للتكيف والتهايئية "ADAPTABILITE" فما دامت سلطة الضبط غايتها الحفاظ على النظام العام فلابد أن تتكيف مع أي سبب مستقبلي يؤدي لاضطراب النظام العام لذا "ليس للضبط الإداري ذلك الطابع السلبي وشبه الرادع، بل له أيضًا طابع إيجابي وواق، ذلك فلم تعد وظيفة الضبط تنحصر في تدارك الاضطرابات، حيث إن للضبط أيضًا وظيفة تنظيمية تتمثل في "ديناميكا" التدخل الاجتماعي، حيث إننا لم نعد ندرك أو نتصور الضبط بدون خطة عامة، وأن علينا أن نتحدث عن النظام العام الاقتصادي والاجتماعي والمالي... إلخ"(٣٢٨٤).

وفي اعتقادنا أن ذلك الرأي من الأهمية بمكان، فهو يؤسس لأبعاد جديدة من النظام العام، فإذا كان هناك نظام عام من الناحية الاجتماعية والمالية والاقتصادية فإذن هناك نظام عام من الناحية المعلوماتية لما تمثله تلك الناحية من خطورة على عنصر الأمن بصورة كأحد أهداف الضبط وباقي العناصر بصورة شبه أولية كالصحة العامة والسكينة العامة.

وينتقد بعضهم ذلك الرأي لأنه يوسع من وظيفة الضبط لدرجة أن الضبط الإداري سوف يتطابق مع وظيفة القانون، حيث إن وظيفة الضبط تمارس داخل حدود معينة تميزها عما سواها، كي لا تحيد عن المصلحة العامة كهدف للنظام العام. (٣٢٨٥)

وفي اعتقادنا أن ذلك الرأي في محله من الناحية النظرية لكن على الصعيد العملي تعمد الحكومات حاليًا إلى التدخل في الأنشطة والعلاقات الخاصة للأفراد عمليا لضمان أمنها المعلوماتي، وبحجة الحفاظ على النظام العام. (٣٢٨٦)

المبحث الثانى

في

مدى مواءمة المفهوم الواسع

للضبط الإدارى مع تعزيزالأمن المعلوماتى

كما أسلفنا فى تعريف الضبط الإدارى تبين أنه وفقا لتعزيز الأمن المعلوماتى يتطلب مفهوم الضبط الإدارى توسعة نطاقه لدرجة تقارب وظيفته مع وظيفة القانون، والدليل أن جهة الادارة قد تعمد إلى التدخل في الأنشطة والعلاقات الخاصة للأفراد عمليا لضمان أمنها المعلوماتي وبحجة الحفاظ على النظام العام، ودليلنا فى ذلك أن موقع "face book" قد أفاد بأن الطلبات الحكومية للاطلاع على بيانات حسابات المستخدم زادت بنسبة ١٣% في النصف الثاني من ٢٠١٥ ،وقد أصبح طلب جهات الإدارة الاطلاع على

(٣٢٨٤) KLEIN (C.) "La Police du domaine Public" Paris, L.G.D.I ٣e ed, ١٩٦٦, p. ٣٧.

مشار إليه في المؤلف السابق ص٨٤

(٣٢٨٥) د/ عادل أبو الخير، المرجع السابق ص٨٤.

(٣٢٨٦) طالعتنا الصحف في أول مارس ٢٠١٦ بإقرار وزيرة الداخلية البريطانية "تبريزاماي" صلاحيًات جديدة لشرطة بريطانيا للتصنت على الاتصالات واختراق أجهزة الكمبيوتر" (الموقع الإلكتروني لجريدة اليوم السابع: الثلاثاء ١ مارس ٢٠١٦. آخر تحديث ٢٢ أغسطس ٢٠١٧)

بيانات شخصية من شركات الهواتف والإنترنت مثار خلاف منذ تسريب "إدوارد سنودن" تفاصيل سرية عن برنامج لجمع بيانات من الهواتف في ٢٠١٣. (٣٢٨٧)

بل إنه قد تردد أن جهة الإدارة في مصر قد لجأت - في تدبير احترازى- لإيقاف خدمة الإنترنت المجاني لموقع "face book" لرفض الشركة الأمريكية تمكين الحكومة المصرية من مراقبة عملائها. (٣٢٨٨)

مؤدى ماسبق أن التعارض بين سلطة الضبط الإدارى، وسياسات الخصوصية التى يتبعها القطاع الخاص تعد أحد أهم اشكاليات الأمن المعلوماتى. (٣٢٨٩)

أما بالنسبة لشركات الإتصالات فالأمر يتشابه كذلك، **ومثال ذلك:** قضية الرسائل المجمعة (Bulk sms) حيث أصدر الجهاز القومي لتنظيم الاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات قرارًا إداريًا ألزم به الشركات التي تقدم خدمة رسائل المحمول المجمعة (Bulk sms) بالحصول على ترخيص، وألزم الشركات التي تقدم خدمة رسائل المحمول الفردية بالحصول على إجازة، وتضمن كلاً من الترخيص والإجازة وجوب موافقة الجهات الحكومية المختصة بما فيها جهات الأمن القومي على محتوى الرسائل، بل والاحتفاظ ببيانات المستخدمين وتفاعلاتهم ومحتوى الرسائل لمدة عام، وتقديمها إلى الجهاز القومي لتنظيم الاتصالات أو من يفوضه في ذلك، أو الأجهزة الأمنية عند طلبها، وأيضًا السماح للجهاز القومي لتنظيم الاتصالات والجهات الأمنية بالدخول لمواقع تلك الشركات لمراقبة عملها.

وقد تم مجابهة ذلك قضائيا بتعارضه مع العديد من المواثيق والإعلانات العالمية لحقوق الإنسان فضلاً عن مخالفته لنصوص الدستور المصري التي تكفل حرية الرأي والتعبير. (٣٢٩٠)

(٣٢٨٧)يمكن مطالعة الموقع الإلكتروني لوكالة الحدث الدولية: آخر تحديث الجمعة ٢٩ أبريل ٢٠١٦،

(٣٢٨٨) كانت تلك الخدمة المجانية تستهدف محدودي الدخل وتم إيقاف تلك الخدمة لعدم تقديم الشركة الأمريكية لجهة الإدارة في مصر ما يتيح مراقبة المستخدمين والالتفاف حول حماية خصوصية المحتوى ولكن الرفض المعلن كان بغرض الإضرار بالشركات ومنافسيها.=
= أنظر: الموقع الإلكتروني لجريدة المصري اليوم: خبر بعنوان "روتيرز". مصر أوقفت "فيسبوك المجاني" بعد رفض الشركة تمكينها من مراقبته" منشور بتاريخ ٢٠١٦/٤/١. : آخر تحديث الجمعة ٢٩ أبريل ٢٠١٦،

(٣٢٨٩)إيقاف جهة الادارة فى مصر لخدمة الإنترنت المجاني التابعة لشركة face book free basics internet جاء بعد رفض الشركة الخضوع لرقابة العملاء، وإدعت الشركة حينها أن جهة الإدارة تسعى للإلتفاف حول حماية خصوصية المحتوى.
الخبر منشور على الموقع الالكتروني لوكالة "رويترز" بتاريخ السبت ٢ أبريل ٢٠١٦. آخر تحديث الجمعة ٢٩ أبريل ٢٠١٧،

(٣٢٩٠) دفعت مؤسسة حرية الفكر والتعبير بمخالفة ذلك التقييد المعلوماتي لنص المادة ١٩ من الإعلان العالمي لحقوق الإنسان، والمادة ١٩ من العهد الدولي للحقوق المدنية والسياسية، والمادة ١٣ من العهد الدولي للحقوق الاقتصادية والاجتماعية، وقرار الجمعية العامة للأمم المتحدة رقم ١/٥٩ لسنة ١٩٤٦ في شأن حرية تداول المعلومات، والمادة ٩٢ من الميثاق الأفريقي لحقوق الإنسان والشعوب.

وقد حالت محكمة القضاء الإداري نحو تغليب الحق في تداول المعلومات وأوقفت تنفيذ قرار الجهاز القومي لتنظيم الاتصالات فيما تضمنه من إخضاع خدمة الرسائل النصية القصيرة المجمعة للرقابة المسبقة أو اللاحقة.[٣٢٩١]

والجدير بالذكر أن الجهاز القومي لتنظيم الاتصالات قد أصدر بتاريخ ٢٠١٠/١٠/١١ قرارًا إداريًا بضرورة حصول الشركات التي تقدم خدمة الرسائل المكتوبة على تصريح من الجهات الإدارية المختصة كوزارة الاتصالات، وكوزارة الإعلام وغيرها قبل أن تقدم تلك الخدمة للشركات والصحف أو المؤسسات الإعلامية، ومن بين ضوابط ذلك القرار تخصيص موظفين لمراقبة محتوى تلك الرسائل.[٣٢٩٢]

ويبدو أن المواقع الإلكترونية العالمية لا تحبذ فكرة الضبط الإداري الإلكتروني الذي تقوم به الجهات الحكومية حيث تعمد لتحذير مستخدميها الذين يتعرضون للإخلال بأمنهم المعلوماتي، بل إن موقع facebook يصدر تقارير تتضمن طلب سلطات الضبط الإداري الكشف عن بيانات المستخدمين، وقد تصدرت الولايات المتحدة قائمة الدول التي طالبت بذلك، إذ قدمت أكثر من ١٧ ألف طلب للحصول على بيانات متعلقة بأكثر من ١٢٦ ألف مستخدم، ويشرح موقع face book على صفحته الرسمية ما يطلبه المسئولون الحكوميون أحيانًا من بيانات عن المستخدمين كجزء من التحقيقات الرسمية المتعلقة [٣٢٩٣]وتتعلق الغالبية العظمى من هذه الطلبات بالقضايا الجنائية وغالبًا ما يتم طلب سلطات الضبط الإداري للاسم ومدة فترة الاشتراك بالموقع والحصول على سجلات عناوين أو محتوى الحساب.

وبالاطلاع على التشريعات المقارنة نجد اختلاف الوضع ،مثلا لا يجرم القانون الياباني إلا الحصول على البيانات الشخصية من جهات إدارية فقط وعلى نفس النسق قانون حماية البيانات الهولندي إذ يعاقب فقط على الإخلال بتسجيل ملفات البيانات، بخلاف القانون الفرنسي يضع قائمة مفصلة للأفعال الإجرامية التي ترجع إلى الكثير من الأنشطة المحظورة من قبل الجهات الإدارية.[٣٢٩٤]

(٣٢٩١) حكمت المحكمة كذلك بوقف تنفيذ النصوص غير المشروعة الواردة بالقرار المطعون فيه في البند ١٠ من القرار التنفيذي لشركات المحمول فيما يتعلق بخدمة الرسائل القصيرة الذي نص على أن "يحق للجهاز أو للمفوضين من قبل الجهات الأمنية الدخول إلى مواقع ومنشآت الشركة بغرض مراقبة كيفية توصيل الشركات المرخص لها بتقديم خدمة الرسائل القصيرة، بشبكات المحمول، وله أن يضع الخطوات التنفيذية والقرارات المناسبة لذلك طبقًا لنصوص هذا الترخيص وقانون الاتصالات رقم ١٠ لسنة ٢٠٠٣ وأي قواعد أو تعليمات أو قرارات سيادية أخرى – للمزيد انظر أحمد عزت وآخرون، المرجع السابق ص٨٩.

(٣٢٩٢) جريدة المصري اليوم، منشور بتاريخ ٢٠١٠/١١. آخر تحديث الجمعة ٢٩ أبريل ٢٠١٧.

ويتعلق ذلك بالحكم الشهير لمحكمة القضاء الإداري، دائرة المنازعات الاقتصادية والاستثمار، الصادرة في الدعوى رقم ١٤٣٠ لسنة ٦٥ ق جلسة ٢٠١٠/١١/٢٧ (حكم غير منشور) والذي يناقش الطيف الترددي كأحد المجالات الخصبة للأمن المعلوماتي.

(٣٢٩٣) شمل التقرير الذي نشر في النصف الأول من عام ٢٠١٥ الهند الذي حلت في المرتبة الثانية بعدد خمسة آلاف طلب للحصول على المعلومات المتعلقة بأكثر من ستة آلاف مستخدم، وجاءت بريطانيا في المرتبة الثالثة، أما في الشرق الأوسط فقد ظهرت مصر والعراق والأردن، حيث قدمت مصر طلبين فقط، وتغييت الدول العربية بشكل ملحوظ عن قائمة الدول التي تقدمت بمطالب تحث فيسبوك على حظر محتويات منشورة على الموقع. وجاءت الهند في المرتبة الأولى لوجود انتهاكات للقانون المحلي في البلد، = =إذ طالبت بحظر أكثر من ١٥ ألف مادة على الموقع، ثم تركيا بأربعة آلاف مادة، ثم فرنسا بثلاثمائة مادة محظورة.

"مشار لذلك في الجريدة الإلكترونية "صحيفة الرأي اليوم بتاريخ الجمعة ١٣ نوفمبر ٢٠١٥". آخر تحديث الجمعة ٢٩ أبريل ٢٠١٧،

(٣٢٩٤) حدد القانون الفرنسي كافة الأنماط الإجرامية التي تستهدف الخصوصية تبعًا لمراحل الجمع والمعالجة والتبادل فالتشريع الفرنسي التقليدي قد جرم التعدي على الأمور التي تدخل في نطاق الحياة الخاصة كالمراسلات والمحادثات أما الفقه والقضاء الفرنسيين حاولا

وفى ذات السياق أكد قانون الخصوصية الأمريكي الصادر عام ١٩٨٤، على وجوب إعلام الأفراد عند القيام بجمع وحفظ سجلات شخصية عنهم ، مع منحهم الحق فى مشاهدة وتصحيح تلك السجلات،ومنع استخدام المعلومات الواردة بتلك السجلات في أي غرض آخر غير الغرض الذى قد حفظت من أجله.

أما في المملكة المتحدة فقد فرض قانون حماية البيانات الصادر عام ١٩٨٤ على كل الوحدات التي تحوز بيانات الأفراد على حواسيبها الآلية أن تقوم بتسجيل تلك البيانات من خلال مسجل حماية البيانات مع تعويض الأفراد فى حالة عدم دقة تلك أو في حالة ضياعها. (٣٢٩٥)

وفى اعتقادنا أن سياسات القطاع الخاص فى تعزيز الأمن المعلوماتى لا تؤتى أكلها وحدها دون تعاون الأفراد، لذا تعمد المواقع العالمية على الإنترنت مثل: Yahoo, Google, facebook إلى بذل الكثير من الجهود لإخبار المستخدمين الذين يقعون ضحايا بعض الهجمات من خلال إعلام المستخدم في حالة استهداف حسابه أو تعرضه للخطر. (٣٢٩٦)

طبيعة وظيفة الضبط الإداري:

يعد الضبط الإداري وظيفة "function" ضرورية ومحايدة، لكونه ضرورة اجتماعية تحفظ النظام العام والمجتمع، وترمي إلى ضبط حدود الحريات العامة التي ينجم عن إطلاقها قيام الفوضى المؤدية إلى انتكاستها. لذا لا يمكن تبرير أي إجراء ضبطى إلا إذا كان ضروريًا لوقاية النظام العام وينطبق ذلك على مجالات الأمن المعلوماتى، بيد أن الضبط الإداري وهو وظيفة في يد السلطات قد يُسخر قصدًا أو عفوًا لغايات سياسية .

علاوة على ما سبق لا يجب أن تهدف وظيفة الضبط الإداري الإلكتروني إلى حماية السلطة في ذاتها باعتبارها أمرًا مستقلاً عن أمن الجماعة ونظامها المادي، لذا يذهب بعضهم إلى أن أمن الدولة يعتبر شقًا من النظام العام، وهو بهذا الوصف يعتبر هدفا لازما للضبط الإداري ،ولا شك في أن كفالة حماية نظام الجماعة يستوجب الدفاع عن السلطة العامة في مبادئها وفي وجودها ما دامت هذه المبادئ معبرة عن القيم الأساسية للمجتمع. (٣٢٩٧)

وضع قائمة بالأمور التي تؤثر على الحياة الخاصة للأفراد لذا تم إصدار قانون يحمي جمع ومعالجة البيانات الشخصية ويجرم مختلف صور الاعتداء عليها من القائمين على عمليات الجمع أوغيرهم.

(٣٢٩٥) للمزيد أنظر: منير محمد، ممدوح محمد: المرجع السابق ص٨٥ وما بعدها.

(٣٢٩٦) ترى Yahoo أن هذه الهجمات أكثر تقدمًا وخطورة، ما يستوجب تنبيهات مخصصة تمكن المستخدمين من اتخاذ إجراءات فورية للحفاظ على أمان الحسابات، وصرحت Yahoo أنها لن تقدم هذه التنبيهات إلا عند وجود مخاطر جدية بنسبة ١٠٠% أي أن هذا الاختراق قد تم تدبيره من حكومة خارجية أو دولة.

(٣٢٩٧) المرجع السابق ص١٢٥.

علاوة على ما سبق تتأتى طبيعة الضبط الإداري الإلكتروني باتصاله بالفروع المستحدثة قانونيًا، وغير المطروقة من الفقه بالفحص والدراسة كمثال "القانون السيبري"، أو "قانون الكمبيوتر، وكذلك لاتصاله بقانون التكنولوجيا والمعلومات "Information & Technology Law". "(٣٢٩٨)

لذا يعمد الفقه لإدخال قانون الكمبيوتر ضمن الإطار الجنائي من خلال الحماية القانونية للمعلومات وتحديدًا الحماية الجنائية، وآخرون يتناولونه ضمن موضوعات حماية الملكية الفكرية لربطهم الوجود القانوني للمعلومات بنظم المعالجة ودورها في إنتاج المعرفة، وذلك لكون المعلومات ذات طبيعة معنوية.

(٣٢٩٨) يتصل ذلك المفهوم بالفضاء السيبري (CYPER SPACE) أو الفضاء التخيلي ويرجع الفضل في ذلك المصطلح للمؤلف وليام جبسون ليشير به إلى الحقيقة التخيلية لشبكات الكمبيوتر، وقد تفرع عن ذلك المصطلحات الآتية:-

Cyper "Cyper cash – Cyper time – Cyper crime"

وغيرها من التعبيرات التي تنطلق في فكرة البيئة التخيلية أو الافتراضية . للمزيد انظر.. منير محمد الجنبيهي، ممدوح محمد الجنبيهي، المرجع السابق ص٧٥، ٧٦.

المبحث الثالث

في

أهمية وخصائص

الضبط الإداري الإلكتروني ومتطلباته

تطرقنا فيما سبق لمدى الحاجة لأن يتواءم الضبط الاداري مع التطورات التكنولوجية الحديثة ،لكي تعزز جهة الادارة أمنها المعلوماتي بصورة خاصة،والأمن القومى المعلوماتى بصورة عامة ،والدليل أن جهة الادارة قد تعمد إلى التدخل في الأنشطة والعلاقات الخاصة للأفراد عمليا لضمان أمنها المعلوماتي بحجة الحفاظ على النظام العام ،لذا يجدر بنا التطرق الى أهمية الضبط الادارى الالكتروني فى تحقيق ذلك ، وبيان خصائص الضبط الاداري الالكتروني، علاوة على متطلبات ذلك الضبط من خلال توفير بيئة معلوماتية آمنة، لذا ستكون معالجة ذلك المبحث فى ثلاثة مطالب كالتالي:

المطلب الاول:أهمية الضبط الاداري الالكتروني.

المطلب الثاني:خصائص الضبط الاداري الالكتروني.

المطلب الثالث:متطلبات الضبط الإداري الإلكتروني(تهيئة البيئة المعلوماتية الآمنة)

المطلب الأول

في

أهمية الضبط الإداري الالكتروني

ترتبط فكرة الدولة بفكرة الضبط الإداري ؛ لأن الضبط يعد وسيلة لصون كيان الجماعة، ويعد عصب السلطة العامة وجوهرها، وكانت مهمته مقدمة نسبيا على وظيفتي التشريع والقضاء.[٣٢٩٩] ، لذا فإن الحاجة إلى الضبط الإداري في مجال الأمن المعلوماتي تستمد وجودها من حفظ كيان الدولة بصفة عامة.

علاوة على ماسبق تزايدت الحاجة للضبط الإدارى لمواجهة الكيانات السرية التي تهدد الأمن العام لتمتع تلك الكيانات بأسس تنظيمية وقدرات تكنولوجية هائلة ، وفى اعتقادنا أن تحديث وسائل الضبط الإدارى يعد أمرا أكثر إلحاحاً من خلال تحديث تلك الوسائل، وتطوير الأوعية المعلوماتية لجهة الإدارة.

(٣٢٩٩) تجدر الإشارة في ذلك إلى رأي الدكتور (بودوهيليمبريفت) مدير المكتب الفيدرالي لأمن المعلومات ومفاده "يعتبر الأمن من الحاجات الإنسانية الأساسية، وبدون الأمن ينهار النظام الإجتماعي، وحاليًا تتزايد الرغبة في الأمن باستمرار خاصة مع تزايد مساحة الإعتماد على تكنولوجيا المعلومات".

للمزيد انظر موقع المكتب الفيدرالي الألماني لأمن المعلومات www.bsi.bund.de

"لهذا فإن القول بأن فكرة الضبط الإداري إنما نشأت أول ما نشأت ضرورة محلية، قبل أن تنشأ ضرورة اجتماعية، لا يظاهره المنطق ولا تزكيه النشأة الأولى للضبط الإداري"

وينصح الفقه المقارن أن تتم معالجة التسريبات في المعلومات الحكومية عن طريق تغيير السياسات الإدارية، والتي تساهم في صناعة القرارات، ويكون ذلك عن طريق سيطرة المؤسسات الإدارية على تدفق المعلومات "The flow of Information" من خلال قصر الحق في المعرفة في القطاع التنفيذي على مجموعات محدودة من الأفراد(٣٣٠٠).

ويؤيد رأينا أنه فى حالة قصور الضبط التشريعي في مواجهة السلوك الإجرامي بصورة قانونية فإنه لن تتمكن الدولة من حفظ أمنها الاجتماعي والسياسي.(٣٣٠١)

علاوة على ماسبق لا تعد الظروف الاستثنائية مبررا للقصور فى مهام الضبط التشريعى أوالضبط الإدارى ، وهذا ما أكد عليه المجلس الدستوري الفرنسي حين قرر أن "المهام الدستورية الأساسية تقع بوجه خاص على السلطة التشريعية وعلى رئيس الدولة وعلى الحكومة – كل في حدود اختصاصه – وعليهم ممارستها مهما كانت الظروف ورغم عدم ملاءمة القواعد الدستورية العادية مع العمل المطلوب لأداء هذه المهام".(٣٣٠٢)

مؤدى ماسبق أنه إذا كان النص التشريعي قاصرًا عن توفير الأمن المعلوماتي فلا بد من وجود سلطة أوسع للضبط الإداري الإلكتروني "فإذا كانت اعتبارات العدالة الجنائية والتشريعية تحول دون ممارسة السلطة التنفيذية بعض الاختصاصات التشريعية، لعدم إحاطة المشرع بالجرائم المستحدثة الناشئة من التطور الاجتماعي والسياسي في المجتمع الا أن اعتبارات حسن الإدارة والملاءمة الوظيفية والأمنية تقتضي تخويل السلطة التنفيذية هذه الولاية باعتبارها المنوط بها مواجهة حالات ضبط إيقاع المجتمع في مختلف ميادينه".(٣٣٠٣)

إذن يمكن منح وحدات الضبط الإداري صلاحيات قانونية ودستورية تلائم الإخلال بالنظام العام لتحقيق دورها في صيانة أمن ونظام المجتمع، سواء أكان على مستوى الجرائم الجنائية أم على مستوى الجرائم السياسية التي تضر بمصالح الدولة الإجرام المنظم العابر للحدود والمعتمد على وسائل تتناسب مع آثار وتداعيات العولمة.(٣٣٠٤)

من جماع ماسبق يتسع مفهوم الأمن المعلوماتي ليشمل الإجراءات والتدابير المستخدمة في مجالي الضبط الإداري، والمجال الفنى فى حماية المعلومات والبيانات من الاعتداءات المادية الظاهرة، كالاعتداء على الأجهزة والبرمجيات كجرائم التسلل والإهمال أو سرقة المعلومات أو التقاطها وتغييرها بشكل غير مسموح به قانونًا، أو حوادث فقدان أو تغيير المعلومات.

أو فقدان السيطرة على إدارة تلك المعلومات لوجود كوارث طبيعية أو كوارث غير طبيعية **ومثال الأولى:** الفيضانات، **ومثال الثانية:** الحرائق وحوادث التفجير.

(٣٣٠٠) Abraham D. Safaer,o p.cit. ٧٦.

(٣٣٠١) المرجع السابق ص١٦٧.

(٣٣٠٢) د/ أحمد فتحي سرور: الحماية الدستورية للحقوق والحريات – دار الشروق، الطبعة الثانية ٢٠٠٠ ص٨٠٨.

(٣٣٠٣) حكم المحكمة الدستورية العليا ١٩٩٨/٢/٧، القضية رقم ٤٠ لسنة ١٥ قضائية دستورية الجريدة الرسمية العدد ٨ -مشار إليه في مؤلف د/ طارق الجيار سالف الذكر ص١٦٩.

(٣٣٠٤) فى ذلك المعنى: د/ إمام حسنين "جرائم التنظيمات الإرهابية" دراسة مقارنة – مجلة مركز بحوث الشرطة العدد ٢٧ يناير ٢٠٠٥ ص٣٥٣ مشار إليه في المرجع السابق ص١٧٠.

علاوة على ماسبق تزداد الحاجة لتنوع وسائل تعزيز الأمن المعلوماتى عندما تمس الخطورة المعلومات الحكومية لحيازة الوحدات الإدارية أوعية معلوماتية وتقارير تمس حياة ومهن. (٣٣٠٥)

ويؤكد البعض فى ذات السياق بأن أبعاد الأمن المعلوماتى للجهة الإدارية تنطلق من ثلاثة محاور: أولهما تأمين سرية المعلومات ،وثانيهما تأمين سلامة المعلومات، وثالثهما تأمين وجود المعلومات حيث يتعلق النطاقان الأول والثالث بالأشخاص المخولين بالتعامل مع المعلومات فى حين يتعلق الالنطاق الثانى بالأوعية المادية الى تحفظ عليها(٣٣٠٦).

المطلب الثانى

في

خصائص الضبط الإداري الإلكتروني

يتسم الضبط الإداري عادة بالعديد من الخصائص، إلا أن اتصال الضبط الإدارى بالنطاق الإلكترونى بصورة عامة والنطاق المعلوماتى بصورة أخص يجعل وصفه بالضبط الإدارى الالكترونى وصفا مفضلا يتميز بخصائص عدة ومنها:

١) الطابع المستحدث المتطور:

إن انتقال النشاط الإنساني للفضاء الإلكتروني يفرض ضرورة بسط الإدارة سلطتها تجاهها، والتدخل بشأنه لتحقيق ذات الغاية والمتمثلة في حماية النظام العام، ويتأسس ذلك أيضًا على أن هذه السلطة تعد ضرورة لا غنى عنها في كل مجتمع قوامه سيادة القانون. (٣٣٠٧)

(٣٣٠٥) د/ دلال صادق الجواد، د/ حميد ناصر الفتاك، المرجع السابق ص٢١.

" لذا ينقسم الأمن المعلوماتي فى تلك الجزئية إلى ما يلي:-

١) أمن الأفراد والإدارة.

٢) أمن المعلومات والوثائق في مراكز الحواسيب الإلكترونية.=

=٣) أمن بناية مراكز الحواسيب الإلكترونية.

٤) أمن الأجهزة البيئية الخاصة بتلك المراكز.

٥) أمن الاتصالات الخاصة بتلك المراكز.

٦) أمن أنظمة التشغيل والبرمجيات.

٧) أمن أجهزة الحواسيب الإلكترونية"

(٣٣٠٦) د/إياس بن سمير الهاجرى:المرجع السابق ، ص ١٤٠

وبذلك يمكن القول بأن تحول نشاط الأفراد جزئيا للفضاء الإلكتروني يستتبعه حتمًا تحول سلطة الضبط الإداري بصورة تؤدي إلى اتساع نطاقها واكسابها طابع جديد لم يكن قائمًا من قبل، ويمكن تدعيم ذلك في ظل ما يشير إليه الفقه من أن التكنولوجيا غير محصنة من المخاطر بل تشكل أرضًا خصبة لها، وهو ما يفرض استحداث سلطة ضبطية جديدة للإدارة تكون بموجبها مسؤولة ومكلفة بالقيام بالإجراءات الوقائية التي تحول دون الإخلال بالنظام العام من خلال تقييد حرية ونشاط الأفراد داخل هذا الواقع.[٣٣٠٨]

ومن الأهمية بمكان أن نلاحظ أن الواقع الافتراضي الجديد يمكن أن يؤدي لتصنيف بعض الأنشطة الفردية كجرائم إلكترونية[٣٣٠٩] فضلاً عن دوره الواضح في تمكين الأفراد للتعبير عن إرادتهم ونشر أفكارهم وتصوراتهم، وهو ما يعني تطور نظرية الضبط الإداري.[٣٣١٠]

وهنا تثور الإشكالية هل نحن أمام سلطة ضبط من نوع جديد مستقل تمامًا من الضبط الإداري بالمفهوم التقليدي أم أننا بصدد تطور واستحداث للطابع التقليدي لسلطة الضبط؟

منهم من يرى إمكانية استحداث عناصر مستحدثة للمفاهيم التقليدية فى الضبط الإداري لتحقق صيانة النظام العام، وهو ما نلاحظه كمثال في استحداث "مباحث المعلومات والإنترنت" التي تتبع وزارة الداخلية ،وبالتالي لايعد الضبط الإلكترونى-بحسب ذلك الرأي- سلطة جديدة أو موازية لسابقتها وإنما تشكل امتدادًا داخل الفضاء الإلكتروني، وتطورا لازما بذات الأطراف والأهداف ولكن بثوب جديد قائم على الطابع الفنى أو البراجماتى.[٣٣١١]

ويؤكد بعضهم أيضا على أن كلا من السلطتين – التقليدية والمستحدثة – تعتبران بمثابة وسيلة آمرة وامتياز قائم بيد جهة الإدارة في مواجهة نشاط الأفراد بكافة صوره ومواطنه، بصورة تؤدي إلى الكشف عن مكان جديد تباشر فيه الإدارة امتيازاتها، لذلك فإنه توجد خشية من تعسفها مجددًا بداخله، الأمر الذي يتوجب معه خضوع السلطة الجديدة كما سابقتها للمشروعية ولرقابة القضاء باستمرار.[٣٣١٢]

وفى ذات السياق يرى آخرون أننا بصدد تطور لازم للسلطة التقليدية للضبط الإدارى ، ولسنا أمام سلطة جديدة أو مستقلة تمامًا ،لأن الانتقال من الضبط الإدارى فى مفهومه التقليدى إلى مفهومه المستحدث يكشف عن مد نطاق السلطة الأصيلة للواقع الجديد، أو اعتبار السلطة الجديدة بمثابة الامتداد الطبيعي لسابقتها في ظل ما يفرضه الواقع الإلكتروني من تحديات ومخاطر، وهو ما يجعل هذا الانتقال مستجيبًا

(٣٣٠٧)فى ذلك المعنى د/ محمد سعيد حسين أمين: مبادئ القانون الإداري: "دراسة في أسس التنظيم الإداري – أساليب العمل الإداري، دار الثقافة الجامعية، ١٩٩٧، ص٦٤٥.

(٣٣٠٨) فى ذلك المعنى:د/ أحمد سعد محمد الحسيني، الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، أطروحة دكتوراه مقدمة لكلية الحقوق جامعة عين شمس ٢٠١٢ ص٩٢.

(٣٣٠٩) فى ذلك المعنى:د/ طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي – النظام القانوني لحماية المعلوماتية،دار الجامعة الجديدة للنشر – الإسكندرية ٢٠٠٩ ص١٠.

(٣٣١٠) فى ذلك المعنى:فاطمة الزهراء عبد الفتاح إبراهيم، العلاقة بين المدونات الإلكترونية والمشاركة السياسية في مصر -رسالة ماجستير في الإعلام، جامعة القاهرة ٢٠١٠ ص٩٧.

(٣٣١١) فى ذلك المعنى : د/ محمد سليمان شبير: الإطار القانوني لسلطة الضبط الإداري الإلكتروني في فلسطين – مجلة جامعة الأزهر – ٢٠١٥، المجلد ١٧، العدد ٢ (ب) ص٩

(٣٣١٢) في ذلك المعنى راجع: بوقريط عمر، الرقابة القضائية على تدابير الضبط الإداري، رسالة ماجستير، كلية الحقوق، جامعة منثوري، الجزائر ٢٠٠٦/٢٠٠٧ ص٥.

لاعتبارات المصلحة العامة التي تعد عماد القانون الإداري ونطاق تطبيقه وميزان مشرعه بإعتبارها الغاية الأساسية من وراء النشاط الإداري. (٣٣١٣)

ويؤسس الرأي السابق كذلك على ضرورة تحديث قواعد الضبط الإداري بالاستناد على نظرية العمل الإداري من منطلق قاعدة وجوب تحديثه ومرونة قواعده وتطورها الدائم. (٣٣١٤)

وعلى خلاف ماذهبت له الآراء السابقة نجد أن الضرورة دائما ماتقدر بقدرها لذا يجب استحداث مفهوم جديد من المسئولية الإدارية وهو مسئوليتها عن الأمن المعلوماتى ، ولن يكون ذلك إلا بوحدات ضبط إدارى مستحدثة كما سلف ذكره ، بل وأن تتمتع تلك الوحدات بوسائل ضبط إداري إلكتروني مستحدثة تساير التطور التكنولوجي بالفضاء الالكترونى ، ولا يجب حصرها في وسائل تقليدية كاللوائح الضبطية والقرارات الإدارية الفردية والتنفيذ المباشر .

٢) الطابع الغائي المتعدد الأهداف:

تتشعب مهام وأهداف سلطات الضبط الإلكتروني في حماية النظام العام ،ودليلنا فى ذلك ما تشهده حاليًا من لجوء الأفراد إلى شبكات التواصل الإجتماعي للإعلان عن القيام بأنشطة جماعية كالمظاهرات والتجمهر في الميادين العامة بصورة قد تخل بالأمن العام والسكينة العامة.

بل تمتد سلطة الضبط الإداري في حماية النظام العام إلى النظام العام الأخلاقي لا سيما في ظل انتشار المواقع الإباحية والأفكار الجنسية الشاذة، وخطابات الكراهية نحو الأديان والأفراد والمؤسسات وغيرها.

وفي اعتقادنا أن الطابع الغائي المتعدد الأهداف سلاح ذو حدين :فهو من ناحية أولى يواكب تطور القانون الإداري ومستقبله الذي يعتمد على صور جديدة من الأطر الإلكترونية الحاكمة كالمرافق العامة الإلكترونية والحكومة الإلكترونية والقرارات والعقود الإلكترونية ،ومن ناحية أخرى قد يؤدي ذلك الطابع الغائي المتعدد الأهداف إلى انحراف جهة الإدارة في التدابير المتخذة عن الأهداف المشروعة والتي حددها القانون.

٣) نشاط محدد بضوابط وغير مخصص الأهداف:

يعد الضبط الإداري نشاطًا محددًا بضوابط معينة أساسها المشروعية ومبدأ سيادة القانون، فالضبط الإداري ليس مقابلاً أو معارضًا للمشروعية كي يتحقق هدف المحافظة في النظام العام، بل يجب أيضًا أن تخضع إجراءات الضبط الإداري الإلكتروني لرقابة قضائية فاعلة.

ومن ناحية تعد أهداف الضبط الإداري الإلكتروني غير مخصصة الأهداف وهذا أحد أهم الاختلافات بين السلطة التقليدية للضبط الإداري وسلطة الضبط الإداري الإلكتروني فالطابع الغائي المرن والمتطور للنظام العام المعلوماتي يمنح فرصة لرجال الضبط في تعقب الأنشطة الإجرامية المستحدثة أيًا

(٣٣١٣) في ذلك المعنى د/ وفاء سيد رجب محمد: مستقبل القانون الإداري، دراسة مقارنة " ٢٠٠٧م ص١١، وص٢٣.

(٣٣١٤) راجع في ذلك المعنى: د/ هدى محمد عبد العال، التطوير الإداري والحكومة الإلكترونية – الطبعة الأولى – دار الكتب المصرية ٢٠٠٦ ص٧٦.

كان مجالها فإذا تم تعقب بريد إلكتروني لشخص ما لتهديده الأمن العام المعلوماتي فإن سلطة الضبط الإداري الإلكتروني قد تتخذ الإجراءات والتدابير الواجبة نحوه في حالة إخلاله بالسكينة العامة أو النظام العام الخُلقي إذا ما أخل به.

٤) نشاط يستند إلى السلطة العامة:

تعتمد سلطة الضبط الإداري على سلطة القهر، فليس من المتصور أن يقدم الأفراد على تحقيق تدابير الأمن المعلوماتي طواعية وعن رضا لذلك تستخدم الإدارة في مواجهة الأفراد أساليب السلطة العامة، وأحيانًا أساليب القسر والقهر، من خلال وسائل قانونية أو مادية قادرة على إنفاذ إرادتها.

أضف إلى ما سبق بأن مهمة سلطات الضبط في منع ارتكاب الجرائم تتطور حتمًا في ظل تطور الجرائم ذاتها وظهور الجرائم الإلكترونية، لذلك فإن نقل الإجراءات الضبطية التي تحول دون ارتكاب الجرائم إلى الواقع الجديد أمر تقتضيه المصلحة العامة وحماية النظام العام مجددًا"، ويترتب على ذلك نتيجة في غاية الأهمية تتمثل في أن القيود التي وضعها المشرع بخصوص الإجراءات الضبطية في القوانين التقليدية تنتقل أيضًا مع هذه الإجراءات إلى داخل الواقع الإلكتروني .[٣٣١٥]

المطلب الثالث

في

متطلبات الضبط الإداري الإلكتروني

(تهيئة البيئة المعلوماتية الآمنة)

لا يمكن لجهة الإدارة تعزيز الأمن المعلوماتي عن طريق الضبط الإداري الإلكتروني سوى بتوفر متطلباته وهي البنية المعلوماتية الآمنة.[٣٣١٦]

(٣٣١٥)د/ محمد سليمان شبير، المرجع السابق ص٢٠.

(٣٣١٦) يحيى محمد أبو مفايض، الحكومة الإلكترونية: خيار إستراتيجي لتعزيز التفاعل بين الأجهزة الأمنية والمجتمع (ندوة المجتمع والأمن)، كلية الملك فهد الأمنية الرياض ٢٠٠٤ ص٦٠ مشار إليه في المرجع السابق ص١٥٣.

" تتداخل عناصر البيئة المعلوماتية فيما يلى:-=

= ١) وضع السياسات الأمنية لتنقية المعلومات.

٢) وضع القوانين والعقوبات المتعلقة بالمخالفات الأمنية في الإدارة الإلكترونية.

٣) توافق أنظمة ولوائح عمل الوحدات الإدارية مع متطلبات العمل إلكترونيًا.

٤) استخدام بعض الوسائل الأمنية الإلكترونية كالبصمة الإلكترونية، والتوقيع الإلكتروني في المعاملات الإلكترونية.

٥) تأسيس واستخدام البنية التحتية للمفاتيح العمومية، وهي عبارة عن مجموعة من هيئات التوثيق التي يوجد بينها توثيق إلكتروني متبادل، وتمثل في مجموعها الطرف الثالث أو الوسيط بين المرسل والمستقبل، وبشكل منفرد تُعرف باسم هيئة التوثيق التي تقوم

علاوة على ماسبق ترتبط البيئة المعلوماتية الآمنة ارتباطًا حتميا بإزالة العديد من المعوقات والتحديات التي تحد من نجاح الضبط الإداري في حماية الأمن المعلوماتي. (٣٣١٧)

وإذا ولينا وجهنا شطر فلسفة الضبط الإداري في مصر نجد أنها أغفلت الأمن المعلوماتى كركيزة من ركائز الأمن العام ، لذا نجد تحديات عديدة-تضاف على ماسبق ذكره من معوقات- ومنها على سبيل المثال ما يلي:-

١) الاستيراد الكامل لكل أوعية التداول المعلوماتي من برمجيات ونظم تشغيل وقواعد بيانات ومعدات بناء شبكات ،وشبكات اتصالات أرضية.. إلخ ،والذي غالبا ما يؤثر على ناحيتين: **أولهما:** فنية إذ تنعدم السيطرة الإدارية على جميع الأسرار المعرفية والصناعية لأوعية تخزين وتداول المحتوى المعلوماتي، **وثانيهما:** اقتصادية إذ سيتحكم القطاع المستورد لتلك الأوعية وما خلفه من شركات عالمية وأجنبية في انسياب حركة استيراد وبيع وتشغيل وصيانة الكثير من الأجهزة والمعدات.

٢) عدم وجود الشفافية الإدارية بوحدات الحكم والإدارة، والتى تعتبر أن الأمن المعلوماتي هو حجب المعلومة ومنع تداولها ومنع الوصول إليها. (٣٣١٨)

وفي اعتقادنا أن الاهتمام بحرية تداول المعلومات يساهم بنسبة كبيرة في الحفاظ على الأمن المعلوماتي إذ سيؤدي لتعزيز الحق في المعرفة والشفافية الإدارية. (٣٣١٩)

بعملية إصدار (مفاتيح التعمية) لتحديد هوية أطراف الاتصال، وبالتالي القدرة على التحقق منها، والحفاظ على سرية المعلومات عن طريق التوقيعات الرقمية"

(٣٣١٧) مشار لتلك العوامل وأكثر في مرجع د/ دلال صادق الجواد، د/ حميد ناصر الفتال، المرجع السابق ص١٣، ١٤.

"ومن تلك المعوقات ما يلي:-

-حفظ الإدارة للمعلومات الحساسة داخل أوعية مركزية دون توزيعها على مواقع جغرافية منفصلة بما يزيد من فرص المخاطر التي تواجه أنظمة الاتصال ويزيد من حوادث الانتهاك المعلوماتى.

- عدم توفر قاعدة كافية من التدابير الاحترازية التي يمكن على أساسها وضع سياسة مناسبة للحماية وتحديد حجم التكاليف المطلوبة لمواجهة مخاطر الانتهاك المعلوماتي.

- جهل المؤسسات الإدارية بالقيمة الحقيقية لمصادرها البيانية ومدى تأثيرها على سياسات وأهداف المنشأة وكيفية إدارة الموارد الأخرى.=

= -نقص التشريعات القانونية في مجال الأمن المعلوماتي ،والذي أدى إلى عجز المتعاملين مع المعلومات عن التمييز بين القيمة الحقيقية للمعلومات والقيمة المادية للأوساط التي استخلصت منها المعلومات"

(٣٣١٨) أغلب القوانين والقرارات الجمهورية التي تخص الأمن المعلوماتي المصري صدرت في أعقاب هزيمة ١٩٦٧ بمعنى أننا نتعامل مع قضية حرية المعلومات بفكر الظروف الاستثنائية لا بفكرة الإدارة المجتمعية الشاملة.

(٣٣١٩) حصلت وزارة المالية على المركز الأول في إتاحة البيانات والمعلومات لعام ٢٠١٥ وذلك في تقرير تقييم مستويات الإفصاح الحكومي الصادر عن مركز تقنية = =المعلومات، إذ تقوم الوزارة بشكل شهري بنشر كل البيانات المالية والاقتصادية من خلال التقرير المالي الشهري، كما تقوم بإصدار عدد من التقارير المالية الأخرى **مثل:** موازنة المواطن، وخطة الحكومة على المدى المتوسط والطويل (مشار لذلك الخبر على الموقع الإلكتروني لصحيفة المصري اليوم بتاريخ الثلاثاء ١٥ ديسمبر ٢٠١٥.

٣) إهمال سياسة تشفير وتكويد المعلومات أثناء النقل والتداول من مكان لآخر، وعدم وضع الحد الأدنى للتشفير ، وعدم تبنى سياسة للنسخ الاحتياطي للبيانات والمعلومات القومية تحسبًا للكوارث الطبيعية أو الصناعية.(٣٣٢٠)

علاوة على ماسبق تتزايد أهمية البنية المعلوماتية الآمنة خاصة في وجود ما يسمى بالحكومة الإلكترونية "Electronic government"، والتى يقصد بها: استخدام تكنولوجيا المعلومات لتحسين كفاءة الخدمات الحكومية التي تقدم للمواطنين والموظفين والشركات، ولا بد من توفير الأمن المعلوماتي خاصة عندما تقدم الحكومة جميع خدماتها على موقع واحد على الويب، بحيث تدمج العديد من الخدمات الحكومية حسب الحاجات والوظائف وتلك هي المرحلة الأخيرة من مراحل الحكومة الإلكترونية.(٣٣٢١)

مؤدى ماسبق يجب على أى سياسة ضبط إدارى تعمل فى ظل الإدارة الإلكترونية وتسعى للتغلب على مخاطر الأمن المعلوماتي أن تعمل على ما يلي:-

١) اتخاذ إجراءات وقائية تأخذ في الاعتبار المسألة الأمنية، وأن تهتم بتلك المسألة عند التخطيط لتلك السياسات.

٢) عدم المبالغة في وصف المخاطر المعلوماتية كي لا تتأثر مرونة الخدمات التي تقدمها المصادر البيانية، فقد تؤدى تلك المبالغة لتجنب النظم الإلكترونية في إدارة المعلومات.

٣) تجنب عدم الاهتمام بما يعلن عن حوادث الاختراق الإلكتروني أو الانتهاك الإلكتروني بدعوى أن الحادث يمس الآخرين.(٣٣٢٢)

(٣٣٢٠) تحتاج البني القانونية لتعديل تشريعات إنتاج ونقل وتداول ونشر واستخدام المحتوى المعلوماتي المجتمعي بشتى صوره كالعسكري، والأمني والسياسي، والفكري والثقافي، والعلمي والاقتصادي، والخدمي.

(٣٣٢١) للمزيد انظر: شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه – جامعة المنصورة ٢٠٠٥ ص١٠٧-١٠٨.

وكذلك:

- William ouko, Yanal Yzing, E. Government in Developing countries– A Dissertation submitted to the faculty of Graduate school of the university of Minnesota ٢٠١٠, p. ٣٢–٣٤ =
- = Alexander Matthew. S. E. Government implementation– A Dissertation submitted o university of Delaware in partial fulfillment of the requirements for the degree of Doctor Philosophy with a major in political science spring ٢٠٠٧.

(٣٣٢٢) د/ دلال صادق، د/ حميد ناصر: المرجع السابق، ص١٤.

الفصل الثانى

في

أثر المحددات المعلوماتية على

أساليب الضبط الإداري

كما أسلفنا فى الفصل الاول ببيان أثر المحددات المعلوماتية على مفاهيم الضبط الاداري ، نتناول في ذلك الفصل بيان أثر تلك المحددات على أساليب الضبط الاداري من خلال بيان أثرها علي جهات الضبط الاداري في مبحث أول ،ثم أثر تلك المحددات على حيازة جهة الادارة للمعلومات وقواعد البيانات فى مبحث ثاني،ثم في مبحث ثالث نتناول دور الشراكة المعلوماتية في تطوير اساليب الضبط الاداري، ثم في مبحث رابع نتناول دور تنظيم الطيف الترددي في تطوير تلك الاساليب،وذلك على النحو التالي:

المبحث الأول: أثر المحددات المعلوماتية على جهات الضبط الإداري.

المبحث الثاني: أساليب جهات الضبط الإدارى فى الرقابة المعلوماتية.

المبحث الثالث:أثر المحددات المعلوماتية على حيازة جهة الادارة للمعلومات وقواعد البيانات.

المبحث الرابع: دور الشراكة المعلوماتية في تطوير أساليب الضبط الاداري.

المبحث الخامس: دور تنظيم الطيف الترددي في تطوير أساليب الضبط الاداري.

المبحث الأول

في

أثر المحددات المعلوماتية على

جهات الضبط الإدارى

كما أسلفنا يتصل الأمن المعلوماتي بالإدارة العامة الإلكترونية بصورة خاصة، وبالحكومة الإلكترونية بصورة عامة، لذا لابد أن تتواءم وحدات ووسائل الضبط الإدارى مع ما يعرف بإدارة الأزمة المعلوماتية، إذ يُفضل تشكيل فريق عمل لدى جهة الإدارة له تفويض التصرف وقت نشوء التهديد المعلوماتي، ويسبق ذلك بالتأكيد وجود وحدات ضبط إدارى تتوافر بها العناصر التدريبية التالية:- (٣٣٢٣)

١) **عنصر تنظيمي:** ويشمل ذلك العنصر العمليات الإدارية اللازمة كالتخطيط والتنظيم والاتصالات والتوجيه والتعاون.

٢) **عنصر معلوماتي:** ويشمل ذلك العنصر الإلمام بكل ما يتعلق بالمعلومات اللازمة لإمكانية مواجهة الأزمة والتعامل معها.

٣) **عنصر فني أو تنفيذي:** ويشمل ذلك العنصر الخطة الوقائية ضد الأزمات المعلوماتية.

٤) **عنصر اقتصادي:** ويشمل ذلك العنصر حساب التكلفة الاقتصادية لتفادي آثار الأزمات المعلوماتية.

٥) **عنصر سياسي:** ويشمل ذلك العنصر قياس البعد السياسي للقرار الأمني المعلوماتي.

٦) **عنصر قيادي:** ويتعلق ذلك العنصر بقيادة فريق حل الأزمة المعلوماتية.

علاوة على ماسبق عادة ماتجد وحدات الضبط الإداري ظهيرا دستوريا،كمثال ما نصت عليه المادة ٢٠٦ من دستور ٢٠١٤ على أن "الشرطة هيئة مدنية نظامية في خدمة الشعب، وولاؤها له، وتكفل للمواطنين الطمأنينة والأمن، وتسهر على حفظ النظام العام، والآداب العامة، وتلتزم بما يفرضه عليها الدستور في القانون من واجبات، واحترام حقوق الإنسان وحرياته الأساسية، وتكفل الدولة أداء أعضاء هيئة الشرطة لواجباتهم، وينظم القانون الضمانات الكفيلة بذلك".

(٣٣٢٣) في ذلك المعنى **انظر:** أيمن عبد الحفيظ عبد الحميد سليمان:- استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي – رسالة دكتوراه مقدمة لأكاديمية الشرطة – كلية الدراسات العليا ص ٣٨١ وما بعدها.

ويلخص ذلك الرأي أسلوب عمل فريق إدارة الأزمة المعلوماتية فيما يلي:-

١) التنسيق والتكامل بين مختلف عناصر الفريق المختلفة.

٢) القدرة على التنبؤ بالمخاطر المعلوماتية المستقبلية وطرح البدائل المتاحة لمواجهتها.

٣) توافر الإمكانيات المادية التكنولوجية لذلك الفريق.

٤) المرونة والقدرة على التغيير السريع لمواجهة الأزمات المعلوماتية السريعة.

ومن المستقر عليه تمتع وحدات الضبط الإدارى بالطابع الوقائى، فقد ذهب الفقه إلى أن الضبط الإداري تصدره السلطة المختصة إما بالحيلولة دون وقوع الجرائم قبل ارتكابها أو مخالفة القوانين واللوائح، بخلاف الضبط القضائي التي تُتخذ إجراءاته بعد وقوع الجرائم للكشف عن مرتكبيها فالضبط الإداري ذو طبيعة وقائية بخلاف الضبط القضائي ذو طبيعة علاجية.(٣٣٢٤)

فالمادة الثالثة من قانون رقم ١٠٩ لسنة ١٩٧١ الصادر بشأن هيئة الشرطة أناطت بهيئة الشرطة الحفاظ على النظام والأمن العام والآداب وبالتالي يعد الأمن المعلوماتى أحد الوظائف والأهداف التي يجب على الشرطة توفيرها.(٣٣٢٥)

ويلخص بعضهم أنواع الإجراءات التي يقوم بها رجال الضبط الإداري للحفاظ على النظام العام بصورة عامة والأمن المعلوماتي بصورة خاصة كالتالي:-

أولاً: فحص نظام الاتصال بالإنترنت: (الحماية الخفية).

ويكون ذلك عن طريق تقنية مراقبة البريد الإلكتروني، وتقنية تتبع المشتبه فيهم على سبيل المثال.(٣٣٢٦)

ثانيًا: فحص مكونات الكمبيوتر: (الحماية الظاهرة)

(٣٣٢٤) د/ محمد فوزي نويجي: الجوانب النظرية والعملية للضبط الإداري – دراسة مقارنة دار الفكر والقانون -٢٠١٦ ص٣٦. =

= تجدر الإشارة إلى أن المادة ٦٩ من القانون رقم ١٠ لسنة ٢٠١٣ أقرت بجواز منح العاملين المحددين من الجهاز القومي التنظيم الإتصالات والقوات المسلحة وأجهزة الأمن القومي صفة مأموري الضبط القضائي بالنسبة إلى الجرائم التي تقع بالمخالفة لأحكام هذا القانون وتتعلق بأعمال وظائفهم".

وفى اعتقادنا أن ذلك الطابع الوقائى تزيد الحاجة اليه عند الرغبة فى تعزيز الأمن المعلوماتى حيث يفترض أن لا ينحصر دور جهاز الشرطة كسلطة ضبط إداري توفر الأمن بالمفهوم التقليدي ،حيث اصطبغ دوره بجوانب أخرى سياسية واجتماعية واقتصادية وفكرية.

(٣٣٢٥) انظر المادة الثالثة من قانون رقم ١٠٩ لسنة ١٩٧١ في شأن هيئة الشرطة "تختص هيئة الشرطة بالمحافظة على النظام والأمن العام والآداب، وبحماية الأرواح والأعراض والأموال وعلى الأخص منع الجرائم وضبطها، كما تختص بكفالة الطمأنينة والأمن للمواطنين في كافة المجالات، وتنفيذ ما تفرضه عليها القوانين واللوائح من واجبات".

(٣٣٢٦) راشد محمد راشد:- المرجع السابق ص٢١٦. =

= أنظر كذلك للمزيد:-

- د/ طاهر محمود: عقد إيواء الموقع الإلكتروني دراسة مقارنة في إطار القانون المصري والإماراتي والفرنسي، مجلة معهد دبي القضائي، العدد ٢٢ السنة الأولى، مارس ٢٠١٣ ص٤٠ وما بعدها.
- د/ مصطفى محمد موسى:- المراقبة الإلكترونية عبر شبكة الإنترنت دراسة مقارنة، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٥ ص٢١٦ وما بعدها:
- د/ وليد سمير فهيم المعداوي: دور الشرطة في حماية الحياة الخاصة من أخطار المعلوماتية، رسالة دكتوراه، كلية الدراسات العليا بأكاديمية الشرطة ٢٠١١، ص٣٦١.

يمكن كذلك بحسب المرجع السابق اللجوء لفحص مسار الإنترنت، وفحص النظام الأمني للشبكات ونظام بروتوكول الإنترنت، وفحص الخادم أو الملقم.

يمكن تعزيز الحماية الظاهرة من خلال فحص القرص الصلب، وفحص البرمجيات، وفحص النظام المعلوماتي.[٣٣٢٧]

ويذهب بعض الباحثين إلى وجوب الإعداد الفنى للمحققين ورجال الضبط ، لأنهم يواجهون أنشطة إجرامية معقدة تنفذ بطريقة دقيقة وذكية، وليس بالضرورة أن يكون رجل الضبط الإداري خبيرًا في الحاسب الآلي بل يمكن أن يلم ببعض المسائل الأولية التي تمكنه من التفاهم مع الخبير الفني في الحاسب الآلي .

علاوة على ماسبق يتعين على الجهات الحكومية إعداد كوادرها في مجال الأمن المعلوماتى بقدر من المعرفة الأولية لاتخاذ التدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة علمية وسليمة.[٣٣٢٨]

وتجدر الإشارة أن أغلب حالات الانتهاك للأمن المعلوماتى لجهة الإدارة تتأتى من خلال موظفين سبق لهم العمل لدى الجهات الإدارية، حيث يرى الفقه المقارن أن الإفصاح عن المعلومات بدون وجود سلطة قانونية معتمدة فيما يتعلق بالأمن والاستخبارات security & Intelligence يعد من أهم حالات انتهاك الأمن المعلوماتي خاصة من خلال الموظفين السابقين في المجالين السابقين[٣٣٢٩].

واذا تطرقنا لوسائل الضبط الإدارى في المملكة المتحدة نجد أنه يمكن لوزير الداخلية إصدار العديد من القرارات فيما يخص الأمن المعلوماتي وأمن الشبكات "Directions in respect of networks spectrum functions" وذلك بموجب Communications act ٢٠٠٣ وخاصة في البند الخامس (functions of COM) (الفصل ٢١) ((The office of communications[٣٣٣٠].

(٣٣٢٧) المرجع السابق ص٢١٧.

(٣٣٢٨) د/ عبد الفتاح بيومي حجازي:- نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، الطبعة الأولى ٢٠٠٩ – بدون دار نشر ص٢٩٢. =

= وللمزيد انظر:-

- د/ محمد الأمين البشري: "التحقيق في جرائم الحاسب الآلي"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة – الفترة من ١-٣ مايو ٢٠٠٠م.

(٣٣٢٩) Graham, op. cit., p. ١١٣.

(٣٣٣٠) The secretary of stat's power to give directions under this section shall be confined to a power to give directions for one or more of the following purposes:–

a) in the interests of national security.

b) in the interests of relations with the government of a country or terriority outside the united kingdoms;

c).....

d).....

المبحث الثاني

في

أساليب جهات الضبط الإدارى

فى الرقابة المعلوماتية

تختلف أساليب الرقابة المعلوماتية بحسب النظام القانونى والبيئة المعلوماتية ومن الأساليب الضبطية الإدارية الحديثة في الولايات المتحدة أسلوب العمل على نحو تكاملي قومي كالمركز المتكامل للتهديد الاستخباراتي والمنشأة في ٢٠١٥ (CTIIC) والذي يعمل عن طريق تبادل المعلومات والتهديدات منها الإستخبارات الإلكترونية[٣٣٣١].

ولكن إذا أمعنا النظر فى جهات الضبط الإداري في الولايات المتحدة الأمريكية والتى تعمل على تعزيز الأمن المعلوماتى نجد أنها تضم العديد من الجهات، كمثال وكالة المخابرات المركزية، ووكالة الأمن القومي، ووكالة مخابرات الدفاع، ومكتب المخابرات والإستطلاع بوزارة الخارجية، ومكتب التحقيقات الفيدرالي، ووزارة الأمن الداخلي وخاصة الإدارة الوطنية للأمن الإلكتروني. [٣٣٣٢]

ومن جهات الضبط الإداري المهمة أيضا في هذا الشأن مكتب المحاسبة والموازنة بالكونجرس حيث إن لمدير هذا المكتب النظر بشكل عام في نظم الأمن القومي وسياسات أمن المعلومات مع الأخذ في الاعتبار ما يلي:-

١) مراجعة توافق محل وكالة مع الاحتياجات والمتطلبات الموصوفة في قانون الأكواد الأمريكي.

٢) تقديم تقارير للكونجرس فيما يخص أوجه القصور في إجراءات وممارسات أمن نظم المعلومات.

علاوة على ما سبق يقوم مركز المعلومات المضادة القومية بدور مهم في تعزيز الأمن المعلوماتي إذ تأسس ذلك المركز في عام ١٩٩٤ لمساعدة الجهات العاملة في الأمن المعلوماتي لتحديد وتقييم وترتيب أولويات مخاطر التجسس والمعلومات المضادة من القوى الخارجية والجماعات الإرهابية وغيرها من الكيانات غير الدولية.

(٣٣٣١) Lawrence J. Trautman: congressional cyper security oversight: who's who and how it works: p. ٢٢.

(٣٣٣٢) **انظر:** جمال غيطاس، المرجع السابق ص٢٤ وما بعدها.

وبالرجوع لدور تلك الإدارة نجد أنها تنفذ برنامج (العواصف الإلكترونية) الذي يعمل كاختبار القدرة على تحمل وصد الهجمات التي تستهدف الأمن المعلوماتي ويقوم بذلك الاختبار خبراء الأمن المعلوماتي في وزارة الأمن الداخلي وجهات أمريكية أخرى، وأبرز تجربة للعواصف الإلكترونية ما كان في الفترة من ٦ إلى ١٠ فبراير ٢٠٠٦ لاختبار كفاءة وقدرة الأجهزة الأمريكية على صد عاصفة إلكترونية شاملة والتعامل= =معها إذا ما كانت تستهدف البيئة المعلوماتية التحتية، حيث تم خلال تلك المحاكاة عمل عمليات قرصنة إلكترونية افتراضية على أكثر من ١٠٠ مواطن بالولايات المتحدة تتضمن وكالات حكومية، وبنوكا، وشركات عالمية كبرى، ومحطات كهرباء، وبعض شركات تكنولوجيا المعلومات **مثل:** مايكروسوفت، وسيكو علاوة على تنفيذ عدة سيناريوهات للهجوم على المواقع المستهدفة تضمنت محاولة إيقاف محطات توليد الكهرباء في عشر ولايات أمريكية.

نخلص مما سبق أن الجهات الإدارية للأمن المعلوماتي في الولايات المتحدة يتحدد إطارها في أسلوب اللارقابة، أو أسلوب التنظيم الذاتي (self-Regulation) فلم تأخذ الولايات المتحدة بأسلوب اللجنة المسئولة عن الأمن المعلوماتي، كما هو الحال في فرنسا.

غير أن الفقه الأمريكي يؤكد على إمكانية وجود أقوى لدور الضبط الإداري في حماية الأمن المعلوماتي من خلال وضع المبادئ، ووضع اللوائح التنظيمية، وإدارة نظم حماية المبيعات والفصل في المنازعات.(٣٣٣٣)

إلى جانب ما سبق هناك بعض المؤسسات الحكومية التي تحمي الأمن المعلوماتي، كمثال: الهيئة القومية للاتصالات والمعلومات، ولجنة التجارة الاتحادية (FTC) والتشريعات كمثال، قانون حماية الأطفال على الإنترنت، وقانون حرية المعلومات (FOIA) التي تحمي حقوق المستخدم حال تواجده (on line) على الشبكة(٣٣٣٤).

ومثال تلك المؤسسات أيضًا: المركز الوطني لحماية البيئة التحتية التابع للمباحث الفيدرالية الأمريكية(٣٣٣٥)، ومكتب رئيس التكنولوجيا وهو مكتب مفوض مباشرة من مدير التحقيقات الفيدرالية الأمريكية، وقسم جرائم الحاسب ومعهد أمن الحاسبات، ووحدة جرائم الإنترنت.(٣٣٣٦)

ومن أمثلة جهات الضبط الإداري التي تعزز الأمن المعلوماتي ما قامت به فرنسا من إنشاء عدة وحدات ومراكز متخصصة كمثال الشرطة الوطنية لمكافحة الجرائم المعلوماتية بكل صورها، ومن أهم تلك الوحدات أيضًا المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات للاتصالات، ومن مهام

(٣٣٣٣) مشار إلى ذلك في المرجع السابق ص١٤٥.

(٣٣٣٤) http://www.frc.gov/privacy/reports.htm Federal Trade commission, self Regulation and online Privacy: A Report to congress (July) ١٩٩٩ (concluding that greater incentives were implementation of the basic privacy principles).

والجدير بالذكر أن أغلب الشركات العالمية التي تعمل في مجال الإنترنت تحرص على الأمن المعلوماتى إلى جانب مبادئ أخرى، كمثال: مبدأ الاختيار، ومبدأ الإخطار، ومبدأ الحق في الوصول والإطلاع.

للمزيد أنظر النظم المختلفة لحماية الخصوصية المعلوماتية باعتبار أحد أركان الأمن المعلوماتي د/ وليد سليم، المرجع السابق ص٦٣٥ حتى ص٦٥٠.

- اتفاقية safe Harbor
- نظام مفوض المعلومات في النظام القانوني الألماني.
- مفوض الخصوصية الكندية في النظام القانوني الكندي.
- مفوض خصوصية المعلومات في أستراليا.

(٣٣٣٥) تم إنشاء هذا المركز بعد الهجمات التي طالت الولايات المتحدة الأمريكية في الإتصالات، والكهرباء والمؤسسات الاقتصادية ... الخ. مشار لذلك في المرجع السابق.

(٣٣٣٦) للمزيد أنظر المرجع السابق ص٢٤٦.

وقد أقامت بريطانيا هيئة جديدة لمكافحة الهجمات الإلكترونية، وبالفعل تصدت تلك الهيئة للهجمات في ١٨٨ مناسبة، وتعد تلك الهيئة جزءًا من وكالة الاستخبارات البريطانية.

ذلك المكتب تنسيق عمليات ملاحقة مرتكبي الجرائم المعلوماتية، علاوة على مشاركة جهات الضبط القضائي في إجراءات التحقيق، ومساعدة الشرطة الوطنية وغيرها من الأجهزة.(٣٣٣٧)، ومن تلك الجهات أيضًا القسم الوطني لقمع جرائم المساس بالأموال والأشخاص. (٣٣٣٨)

ومن المبادئ المهمة التي تكفل الأمن المعلوماتي لجهة الإدارة فى فرنسا وجود تنظيم في معالجة البيانات الشخصية، وجاء النص عليه في قانون المعلوماتية الفرنسي من خلال حظر استخدام وسائل غير شرعية لجمع المعلومات والبيانات وتوضح الغرض من جمع البيانات. (٣٣٣٩)

أما على صعيد التشريعات الفرنسية فقد تم إنشاء لجنة وزارية في فرنسا تخص الدعم التقني من أجل تطوير تكنولوجيا المعلومات والاتصالات في الإدارية (M.T.IC) في عام ١٩٩٨ ومن المهام الرئيسية لتلك اللجنة ضمان التنسيق بين الإدارات والمرافق المختلفة، وتبادل ونقل البيانات وتحويلها، واقتراح تبادل المعلومات والبيانات الممكنة بين المرافق والإدارات. (٣٣٤٠)

مؤدى ما سبق يتبين رفض التشريع الفرنسي انتهاج النهج الأمريكي الذي يكتفي بالرقابة القضائية فيما يخص الأمن المعلوماتي، ولكن عمد التشريع إلى أسلوب الوقاية خير من العلاج، لذا عمد المشرع الفرنسي إلى إنشاء تلك اللجنة التى تقوم بالتحري والنصح والاقتراح والرقابة، وإعلام الجمهور ومساعدة أجهزة الدولة المختلفة. (٣٣٤١)

وتعد تلك اللجنة في اعتقادنا أحد أهم أدوات الضبط الإداري لحماية الأمن المعلوماتي في فرنسا، حيث تعتمد على الصفة الأساسية للضبط الإداري، وهي الطابع الوقائي والرقابة السابقة من خلال اتخاذ وسائل الحماية المسبقة، والرقابة المستمرة للتحقق من قيام الجهة القائمة على الحاسب الآلي في تطبيق الضمانات القانونية ،وما يؤكد ذلك سلطة اللجنة فى اتخاذ القرارات التنظيمية العامة والفردية لتطبيق أحكام القانون إلى جانب تكليف أحد أعضائها بالتحقق واقعيًا من احترام الأمن المعلوماتي عن طريق إجراء الفحص المناسب. (٣٣٤٢)

علاوة على ما سبق تعمل اللجنة القومية للمعلوماتية والحريات في فرنسا على تعزيز الأمن المعلوماتي للأفراد من بيانات ومعلومات بما يتفرع عن ذلك من حقوق كالحق في الأمن والسرية المعلوماتية

(٣٣٣٧) تم إنشاء ذلك المكتب بموجب مرسوم وزاري رقم (٤٠٥ – ٢٠٠٠) المؤرخ في ٢٠٠٠/٥/١٥ على مستوى المديرية المركزية للشرطة القضائية التابعة لوزارة الداخلية ويساعد هذا المكتب في نشاطات كل من وزارة الدفاع، ووزارة الاقتصاد، والمالية، والصناعة، وهو يتمتع باختصاص وطني يتحدد نطاقه في الجرائم المرتبطة بتكنولوجيا المعلومات.

(٣٣٣٨) يتكون هذا القسم من "٦" محققين متخصصين في التحقيق في الجرائم المعلوماتية، ولقد بدأ القسم مهامه عام ١٩٩٧ (مشار لذلك وللهامش رقم ١) رسالة دكتوراه في د/ محمد أحمد عزت المرجع السابق، ص٢٤٤.

(٣٣٣٩) د/ وليد السيد سليم، المرجع السابق، ص٥٧٣.

(٣٣٤٠) د/ داود عبد الرازق الباز، الإدارة العامة، الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام، مجلس النشر العلمي، جامعة الكويت، ٢٠٠٤ ص٢٥٦.

(٣٣٤١) د/ وليد السيد سليم المرجع السابق ص٥٨٦.

نقلا عن :=

= MAISL (H), La maitrise d'une interdependence, commentaire

(٣٣٤٢) المرجع السابق ص٥٨٦.

معتمدة في ذلك العديد من إجراءات الضبط الإداري كمثال التفتيش والمراقبة والإشراف على الأنظمة المعلوماتية، بل تتلقى شكاوى الأفراد والأشخاص المعنوية العامة عند مخالفة القانون وتقوم بالترخيص والتصريح عند ممارسة نشاطات جمع البيانات والمعلومات،والتأكد من توافق النظام المعلوماتي مع القانون.(٣٣٤٣)

مؤدى ماسبق تعمل اللجنة القومية للمعلوماتية والحريات على العديد من المحاور كالتالي:

أولاً: المحور الرقابي:

يتضح الدور الرقابى لتلك اللجنة فيما يلي:

١) منح ترخيص معالجة البيانات، كمثال البيانات الخاصة بالمسائل السياسية والعرقية والبيانات الصحية وهي البيانات الواردة في المادة ٢٥ من قانون رقم (١٧-٧٨) الوارد في المادة ٢٦ من ذات القانون كمثال بيانات إحصاءات الرقم القومي، وعمليات التعداد والإحصاء الوطني، وخدمات الإنترنت العامة.

٢) إبلاغ النائب العام فورًا بحسب ما تنص عليه المادة ٤٠ من قانون الإجراءات الجنائية الفرنسي بشأن ما يصل إلى علمها من جرائم معلوماتية.

٣) يمكن أن تسند اللجنة لأحد أعضائها مهمة تفتيش مواقع نظم المعلومات، بل والتحقق من جميع عمليات المعالجة، وتوثيق ما يتصل بذلك ،ويمكن لها اتخاذ أحد التدابير المنصوص عليها في المادة ٤٥ من الفصل السابع ضد المتحكم في البيانات.

ثانيًا: المحور الخدمي:

يتمثل المحور الخدمي للجنة القومية للمعلوماتية والحريات في العديد من المهام ومثالها ما يلي:

١) تلقي الشكاوى والدعاوى والمطالبات الخاصة بعمليات المعالجة الآلية للبيانات الشخصية.

(٣٣٤٣) نصت المادة رقم ١٣ من قانون (١٧-٧٨) المعدل بموجب قانون (٣٣٤-٢٠١١) الصادر في ٢٩ مارس ٢٠١١ على أن تشكيل اللجنة يتكون من سبعة عشر عضوًا على النحو التالي:-

- أربعة أعضاء من النواب (عضوان من الجمعية وعضوان من مجلس الشيوخ).
- عضوان حاليان أو سابقان من مجلس الدولة على درجة مستشار يتم انتخابهم من الجمعية العامة لمجلس الدولة.=
- = عضوان حاليان أو سابقان من محكمة النقض ويكونان على درجة مساوية لأعضاء اللجنة في الدرجة ويتم انتخابهم من قبل الجمعية العامة لأعضاء محكمة النقض.
- عضوان حاليان أو سابقان من ديوان عام المحاسبة القومي.
- ثلاثة أعضاء من الخبراء المتخصصين في علوم الحاسب أو قضايا الحرية الفردية يتم تعينهم بمرسوم من مجلس الوزراء.
- عضوان يختاران من الخبراء في مجال الحاسب والمعلوماتية.

انظر: المرجع السابق ص٥٧٥ وما بعدها.

٢) الاستجابة لطلبات السلطات العامة والمحاكم عند طلب المشورة والرأي والاستجابة لطلبات الأفراد عند طلب إنشاء نظم معالجة آلية للبيانات الشخصية.

٣) الاستجابة لطلبات الاطلاع للأفراد المتعلقة بالمعالجة الآلية للبيانات الواردة في المادة ٤١ (بيانات أمن الدولة وحماية السلامة والأمن العام) والواردة في المادة ٤٢ (والخاصة ببيانات الجرائم وبيانات الضرائب).

ثالثًا: المحور التنفيذي:

يتمثل المحور التنفيذي للجنة القومية للمعلوماتية والحريات في العديد من المهام ومثالها ما يلي:-

١) وضع وإعلان المعايير والقواعد النموذجية المنظمة لضمان أمن النظام المعلوماتي عند الضرورة.

٢) تقديم اعتماد الجودة لنظم المعالجة الآلية التي تطالب القانون والتي تهدف إلى حماية الأفراد فيما يخص المعالجة الآلية للبيانات الشخصية.

رابعًا: المحور الاستشاري:

يتمثل المحور الاستشاري للجنة القومية للمعلوماتية والحريات في العديد من المهام، ومثالها ما يلي:

١) أخذ رأيها في أي مشروع قانون أو مشروع مرسوم أو قرار يخص معالجة البيانات.

٢) اقتراح التدابير التشريعية أو اللائحية التي يجب على جهة الإدارة اتباعها للتوازن بين الحريات وتطورات الحاسب.

٣) تقديم المساعدة الأمنية المعلوماتية بشأن حماية البيانات إذا طلبت أي من السلطات الإدارية الأخرى المستقلة.

٤) إيضاح موقف فرنسا عند التفاوض الدولي فيما يخص حماية البيانات الشخصية، وذلك بناء على طلب رئيس الوزراء.

علاوة على ما سبق يمكن استحداث بعض المراكز الإدارية كمثال مفوض الاتحاد الأوروبي لحماية الخصوصية، فقد نص التوجيه الأوروبي لحماية البيانات لعام ١٩٩٥ على إلزام الدول الأعضاء في الاتحاد الأوروبي بإنشاء سلطات حكومية وطنية رقابية لتعزيز الحماية الإدارية والأمن المعلوماتي. (٣٣٤٤)

(٣٣٤٤) د/ وليد السيد سليم، المرجع السابق ص٥٦٤.

في إشارة إلى

وتجدر الإشارة إلى أن التوجيه الأوروبي نص على العديد من الصلاحيات لسلطات الضبط الإداري لتعزيز الأمن المعلوماتي كمثال:

- صلاحيات البحث والإطلاع على البيانات، وصلاحيات جمع كل ما هو ضروري من معلومات تفيد في أداء الواجبات الرقابية.

- صلاحيات ضمان النشر المناسب للآراء وحجب أو محو أو إتلاف البيانات، أو فرض حظر مؤقت أو نهائي على المعالجة، أو تحديد المتحكم بالمعلومات وتوجيه اللوم إليه أو إحالة الأمر إلى البرلمانات الوطنية أو المؤسسات السياسية الأخرى.(٣٣٤٥)

وعلى صعيد التشريع المصري فقد لجأ المشرع لأسلوب وحدات الضبط الإداري لحماية الأمن المعلوماتي، ومن اللجان التي أنشأها التشريع المصري اللجنة القومية الدائمة للتنسيق الأمني لمنظومة كاميرات الرصد المرئي بموجب قرار رئيس مجلس الوزراء رقم ١٠٣٢ لسنة ٢٠١٥، والتي يترأسها مساعد وزير الداخلية لقطاع نظم الاتصالات وتكنولوجيا المعلومات، وعضوية ممثلين عن الجهات التالية:-

- وزارة الداخلية (قطاعي الأمن الوطني ونظم الاتصالات وتكنولوجيا المعلومات).

- إدارة المخابرات الحربية والاستطلاع.

- جهاز المخابرات العامة.

وللجنة في سبيل إنجاز اختصاصاتها أن تضم في عضويتها ممثلين عن الوزارات المعنية، وهى (الاتصالات وتكنولوجيا المعلومات – التنمية المحلية – الإسكان والمرافق والمجتمعات العمرانية الجديدة – الكهرباء – النقل – الموارد المائية والري – السياحة – البترول – العدل) في الشركة المصرية للاتصالات، الجهاز القومي لتنظيم الاتصالات، إتحاد الإذاعة والتليفزيون وغيرها من الجهات الأخرى ذات الصلة.(٣٣٤٦)

أما السلطات الإدارية التي تنظم قطاع تكنولوجيا الاتصالات في مصر فنجد أنهما جهاز الاتصالات ويتبع وزارة الاتصالات وهيئة تنمية صناعة تكنولوجيا المعلومات (ITIDA).(٣٣٤٧)

وفي اعتقادنا أن أسلوب عمل اللجان لايتناسب مع أساليب الضبط الإدارى فى تعزيز الأمن المعلوماتى.(٣٣٤٨)

Directive ٩٥/٤٦/EC of the European parliament and of the: council of ٢٤ October ١٩٩٥ on the protection of individual with regard to the processing of personal data and on the free movement of such data.

(٣٣٤٥) للمزيد أنظر المرجع السابق ص٥٦٥.

(٣٣٤٦) الجريدة الرسمية – العدد ١٨ (تابع) في ٣ أبريل سنة ٢٠١٥.

(٣٣٤٧) المرجع السابق ص٥٦٥.

علاوة على ما سبق لا تزال نظرة التشريع المصري نحو الأمن المعلوماتي تقتصر على تأمين الأوعية المادية للمعلومات دون النظر إلى الأمن المعلوماتي ككيان يرتكن على أركان إذا انهار أحدها تداعى الكيان كاملاً.[٣٣٤٩]

علاوة على ما سبق قد تهدف بعض التشريعات إلى عدم إنشاء وحدات ضبط إداري مستحدثة مستقلة وتعمد إلى الاكتفاء بوحدات الضبط الإداري التقليدية مع استحداث وسائلها أو تأهيل تلك الوحدات أو مدها بتكنولوجيا حديثة، ومثال ذلك الإدارة العامة لمباحث الأموال العامة، والإدارة العامة للتوثيق والمعلومات، والإدارة العامة للمصنفات الفنية،[٣٣٥٠] وإدارة مكافحة جرائم الحاسبات وشبكات المعلومات.

وفي اعتقادنا أن إدارة مكافحة جرائم الحاسبات وشبكات المعلومات من أهم وحدات الضبط الإداري التي تعزز الأمن المعلوماتي المصري من خلال النظر في اختصاصات تلك الإدارة وعلى رأسها بحسب القرار الوزاري رقم ١٣٥٠٦ لسنة ٢٠٠٢ ما يلي:[٣٣٥١]

- التخطيط لتأمين ووقاية نظم وشبكات المعلومات لأجهزة وزارة الداخلية وبحث مدى كفاية أساليب التأمين للأهداف المطلوبة.

- إخطار الأجهزة القومية والشرطية المختصة بالبيانات والمعلومات المتعلقة بالجرائم الأخرى، مع التنسيق لإجراءات التحريات وأعمال الضبط.

- تعزيز الأمن المعلوماتي من خلال مكافحة مسببات اختراقه كالفيروسات والاختراقات.

- إعداد أرشيف معلوماتي متكامل لخدمة الإدارة في مجال الحاسبات والنظم المعلوماتية.

(٣٣٤٨) د/ ياسر محمد عبد السلام رجب : الإدارة العامة، دار النهضة العربية ٢٠١٧ ص٥٢ وما بعدها.

" حيث توجه العديد من أوجه النقد لأسلوب عمل اللجان كعيوب التشكيل، وتزييف الإرادة لأن القرار يصدر ظاهريًا من اللجنة، لكنه في الواقع يصدر عن رئيس اللجنة، أو قلة مسيطرة على اللجنة، كما أن اللجان تعجز عن الحسم والسرعة، وهما قواما الأمن المعلوماتي، إلى جانب عيب الوسطية في الحلول في أغلب الأحيان"

(٣٣٤٩)وتفسيرنا لذلك هو حداثة التجربة المصرية بالأمن المعلوماتي، حيث لأول مرة ينص دستور مصري على أمن الفضاء المعلوماتي، وذلك كما ورد بنص المادة ٣١ من الدستور المصري الحالي "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون.=

= وتجدر الإشارة إلى اختصاصات اللجنة القومية الدائمة للتنسيق الأمني الواردة في المادة الثانية من قرار رئيس مجلس الوزراء رقم ١٠٣٢ لسنة ٢٠١٥ ومنها تقييم وضع الجمهورية أمنيًا، والتخطيط لتأمين المحاور المرورية والميادين واقتراح ووضع الخطط والسياسات اللازمة لتفعيل منظومة المراقبة الأمنية باستخدام الكاميرات والتواصل مع الخبراء والجهات المتخصصة في مجال تركيب ووضع نظم الرقابة ... إلخ.

(٣٣٥٠) في اعتقادنا أن الإدارة العامة لمباحث الأموال العامة، والإدارة العامة للمصنفات الفنية تتعلق باختصاصات نوعية ولا تحقق تعزيز الأمن المعلوماتي بالمفهوم الذي يناقشه المبحث أما الإدارة العامة للتوثيق والمعلومات فإنها قد تخدم تعزيز الأمن المعلوماتي بصورة جزئية مكملة.

(٣٣٥١) صدر القرار بتاريخ ٢٠٠٢/٧/٧ ونشر في الأوامر العمومية، وزارة الداخلية المصرية، العدد السابع، القاهرة في ٢٠٠٢/٧/١م، ص١٨.

والجدير بالذكر أن القرار الوزاري رقم ١٣٥٠٧ لسنة ٢٠٠٢ نص على إنشاء أقسام إقليمية لمكافحة الجريمة المعلوماتية.(٣٣٥٢)

وبالتركيز على دور إدارة مكافحة جرائم الحاسبات وشبكات المعلومات نجد أن أهم أقسامها هو قسم التأمين حيث يقوم بما يلي: (٣٣٥٣)

١) معاونة أجهزة الوزارة في تأمين نظمها المعلوماتية.

٢) التخطيط ووضع أساليب تعزيز الأمن المعلوماتي ثم التنفيذ والتنسيق مع الأجهزة المختصة.

٣) متابعة التراخيص التي تصدر للشركات الخاصة في مجال المعلومات وذلك من خلال التنسيق مع الجهات المنوطة بذلك.

ومن اللجان ووحدات الضبط الإداري التي تعزز الأمن المعلوماتي ما نصت عليه المادة ١٨ من القانون رقم ١٠ لسنة ٢٠٠٣ الخاص بتنظيم الاتصالات منه تشكيل لجنة لتنظيم الترددات، حيث تتولى تلك اللجنة تنظيم الطيف الترددي وهو أحد موارد الثرورة الطبيعية والتي تشكل محورًا من محاور الأمن المعلوماتي.(٣٣٥٤)

ويأخذ التشريع المصرى بأسلوب الرقابة المعلوماتية حيث تنص المادة ٢١ من القانون سالف الذكر على عدم جواز إنشاء أو تشغيل شبكات اتصالات أو تقديم خدمات الاتصالات للغير أو تمرير المكالمات التليفونية الدولية أو الإعلان عن شئ من ذلك دون الحصول على ترخيص من الجهاز وفقاً لأحكام هذا القانون وحددت المادة ٢٥ من القانون الأمن القومى -فى مجمله سواء ماديا أو معلوماتيا- هدفا، وذلك بأن تطلبت أن يحدد الترخيص الصادر من التزامات المرخص له، والتى تشمل على الأخص الالتزامات الخاصة بعدم المساس بالأمن القومى .

وهذا ما أكدت عليه المادة ٦٧ من القانون بخضوع أى مشغل أو مقدم خدمة للسلطات المختصة فى الدولة ولنظام إدارتها من خدمات وشبكات اتصالات ، وأن تستدعى العاملين لديه القائمين على تشغيل

(٣٣٥٢) انظر للمزيد مرجع د/ محمد أحمد عزت، المرجع السابق ص٢٥١، ٢٥٢.

يختص ذلك القسم بما يلي:-

١) متابعة البحوث الفنية والتقنية في مجال جرائم الحاسبات وشبكات المعلومات.

٢) التنسيق من الناحية الفنية مع الإدارة العامة للمعلومات والتوثيق فيما يخص أعمال المكافحة وجمع البيانات والمعلومات.

٣) رصد ومكافحة وضبط الجرائم المعلوماتية.

٤) تنفيذ خطة الوزارة في التأمين الوقائي في مجال الأمن المعلوماتي.

٥) أرشفة متكاملة لقاعدة البيانات والمعلومات لتعزيز الأمن المعلوماتي.

لذا صدر القرار الوزاري رقم ٣٥٢١ لسنة ٢٠٠٤ بشأن إنشاء قسم بمديرية أمن القاهرة لمكافحة جرائم الحاسبات وشبكات المعلومات بالإدارة العامة للبحث الجنائي

(٣٣٥٣) نصت الفقرة الثانية من المادة الأولى من القرار الوزاري رقم ١٣٥٠٧ لسنة ٢٠٠٢ على الهيكل التنظيمي للإدارة ومنه قسم التأمين، وقسم العمليات، وقسم البحوث والمساعدات الفنية.

(٣٣٥٤) تشكل تلك اللجنة بقرار من الوزير المختص وتضم ممثلين عن إدارة الاتصالات برئاسة الجمهورية ووزارة الدفاع، ووزارة الاتصالات، ووزارة الداخلية، وهيئة الأمن القومي، واتحاد الإذاعة والتليفزيون، علاوة على ثلاثة أعضاء يرشحهم الوزير المختص.

وصيانة تلك الخدمات والشبكات وذلك فى حالة حدوث كارثة طبيعية أو بيئية، أو فى الحالات التى تعلن فيها التعبئة العامة طبقاً لأحكام القانون رقم ٨٧ لسنة ١٩٦٠ ، وأية حالات أخرى تتعلق بالأمن القومى .

وبالنظر إلى التشريع الكويتي نجد أن هيئة تنظيم قطاع الاتصالات وتقنية المعلومات تختص بإدارة طيف الترددات الراديوية ومراقبة التداخلات وجودة الطيف الترددي واتخاذ الإجراءات اللازمة بهذا الخصوص بما في ذلك إعداد الجدول الوطني لتوزيع الترددات وتحديثه، وإعداد المخطط الوطني لتوزيع الترددات والسجل الوطني لتشخيص الترددات بالإشتراك مع الجهات العسكرية والأمنية.[٣٣٥٥]

وقد أكدت المادة ٢٧ من القانون ذلك في فقرتها الأولى من خلال عدم جواز استخدام أي شخص لأية ترددات راديوية إلا إذا حصل على رخصة بذلك وفقًا للشروط التي يحددها إدارة هيئة الاتصالات وتقنية المعلومات.[٣٣٥٦]

(٣٣٥٥) انظر قانون رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات، منشور بمجلة الكويت اليوم العدد ١١٨٤ السنة الستون هـ - المادة ٢.

- نصت المادة الثانية على أن "تنشأ هيئة عامة ذات شخصية اعتبارية مستقلة تسمى الهيئة العامة للاتصالات وتقنية المعلومات ويشرف عليها الوزير المختص وتتمتع بالشخصية الاعتبارية المستقلة وبالاستقلال المالي...".

ونص القانون في المادة ١٤ منه على أن "تحل الهيئة محل وزارة المواصلات وأي جهات أخرى في حدود ما أوكله القانون للهيئة من اختصاصات...". ويعد ذلك إدراكًا من المشرع الكويتي بأهمية مرفق الاتصالات عامة والأمن المعلوماتي لجهة الإدارة خاصة، مما يتوجب معه وجود هيئة مستقلة لها استقلال مالي تتولى المشاركة في تعزيز الأمن المعلوماتي.

(٣٣٥٦) انظر المادة ٢٧ من القانون، وقد اكتملت منظومة تعزيز أمن الطيف الترددي من خلال المادة ٣٠ والتي منعت اقتناء أو استعمال محطة راديوية على أراضي الدولة أو على سفينة أو على طائرة مسجلة في الدولة ما لم يتم الحصول على رخصة وفقًا لأحكام هذا القانون، وعدم جواز إدخال أية محطة راديوية من خارج الدولة إلا بموافقة الهيئة مع استثناء جاء في المادة "٣١" يخص القوات المسلحة والأجهزة الأمنية وجهات أخرى يجوز لمجلس إدارة هيئة الاتصالات وتقنية المعلومات استثناءها، وهي: السفن والطائرات الأجنبية، وخدمات النقل البري في الأراضي أو الموانيء أو المطارات الكويتية، وكذلك السفارات الأجنبية بشروط المعاملة بالمثل، ووجود تصريح قابل للتجديد.

وتتمتع الهيئة بالاختصاصات المهمة في مجال الأمن المعلوماتي ومنها:-

١) تنظيم خدمات شبكات جميع الاتصالات ووضع لائحة تفصيلية للمصطلحات الفنية المستخدمة في قطاعي الاتصالات وتقنية المعلومات.

٢) وضع لوائح تنظيم قطاعي الاتصالات وتقنية المعلومات بما يتفق مع السياسة العامة المقررة في هذا الشأن.

٣) وضع لائحة بضوابط وشروط منح رخص شبكات وخدمات الاتصالات أو الإنترنت واستخدام الترددات الراديوية وإنشاء وتشغيل بنية إتصالات دولية.

٤) تنظيم الربط البيني بين شبكات الاتصالات العامة المملوكة للقطاع الخاص، أو وزارة المواصلات، أو أي جهة حكومية أخرى عدا الجهات الأمنية.

٥) تعقب مصدر أي موجات راديوية للتحقق من ترخيص ذلك المصدر دون المساس بسرية الرسائل.

المبحث الثالث

في

أثر المحددات المعلوماتية على حيازة

جهة الادارة للمعلومات وقواعد البيانات

يتطلب الأمن المعلوماتى تحقق العديد من المحددات وأهمها احتكار المعلومات، وان كان ذلك من الصعوبة بمكان لاعتبارات(المشروعية) أو حرية تداول المعلومات من ناحية،وللصعوبة التكنولوجية ، أو الآليات المعتادة لرصد وحيازة تلك المعلومات من ناحية ثانية،ولإشكاليات تحديد المقصود بالمعلومات والبيانات محل الحيازة من ناحية ثالثة، **لذا ستكون معالجة ذلك المبحث فى المطالب الآتية:**

المطلب الأول: حيازة المعلومات على ميزان المشروعية

المطلب الثاني:حيازة البيانات الروتينية.

المطلب الثالث:الآليات المعتادة لرصد وحيازة البيانات والمعلومات.

المطلب الرابع:اشكاليات حيازة جهة الإدارة للمعلومات وطرق حلها.

المطلب الخامس:حيازة الإدارة للمعلومات البيومترية.

المطلب الأول

في

حيازة المعلومات على ميزان المشروعية

المعرفة هي القوة "Knowledge is power" لذا قد يغدو احتكار الإدارة للبيانات والمعلومات ذو أثر غير محمود، حيث قد تدفع الأجهزة الرقابية والمخابراتية الأفراد لتغيير سلوكهم ليكون أكثر تواؤمًا مع المعايير الاجتماعية، بمعنى أدق "To make their behavior"، وبالتالي يقل نشاطهم للمشاركة في المجتمع لتجنب المراقبة، لذا يرى الفقه المقارن أننا في عصر التقارير التي تعتبر أداة من أدوات تحصيل البيانات والمعلومة، ولا يقتصر الأمر على شبكة الإنترنت بل على الحواسب الآلية التي تسجل كل دقائق الأمور(٣٣٥٧).

وفى اعتقادنا أن ميزان القوى في معادلة العقد الاجتماعي (الإدارة – الفرد) يميل نحو الإدارة فيما يخص حيازة البيانات حيث إن الفرد قد يعدل سلوكه بعد قيام جهة الإدارة بحيازة تلك المعلومات من ناحية ، علاوة على أن الترخيص الممنوح لجهة الإدارة لجمع تلك المعلومات قد يستغل في جمع معلومات تفوق المطلوب والمرخص به سلفًا من ناحية أخرى.

بل والأكثر من ذلك أن القدرة على إنتقاد الحكومة ومعارضة سياساتها سوف تكون معدومة، لذا غالبا ماتهدد حيازة الإدارة للمعلومات والبيانات الخصوصية والديمقراطية والحريات المدنية كحرية التعبير وحرية الاجتماع والحرية الدينية(٣٣٥٨).

وفى اعتقادنا لايؤخذ الرأى السابق على إطلاقه، حيث تعد مشروعات قواعد البيانات الكاملة من أدوات الضبط الإداري التي تساهم في تعزيز الأمن المعلوماتي لجهة الإدارة، و تعزيز دعم اتخاذ القرار في

(٣٣٥٧) Professor Daniel solovie writes, "we are becoming a society of records, and these records are not held by us, but by third parties".

See:– Daniel solove, Digital Dossiers ad the Dissipation of fourth Amendment privacy, ٧٥ S. CAL, L. REV. ١٠٨٣, ١٠٨٩ (٢٠٠٢).

(٣٣٥٨) Philip B. Heymann, Investigative uses of files of Data about many people collected for other purposes ٩ (٢٠٠٣) (unpublished manuscript).

In the words of professor and former Deputy Autorney General Philip Heymann. "No matter how honest the government was in restricting its uses of the data, many citizens would become more cautious in their activities including being less outspoken in their dissent to government policies. For two hundred years Americans have proudly distrusted their government".

المنظمات الإدارية ويعد ذلك من الأهمية بمكان كي لا يكون الضبط الإداري وأدواته بمعزل عن أدوات الضبط التشريعي.(٣٣٥٩)

ومن النصوص التشريعية التى تساير ما سبق ما نصت عليه المادة السادسة من قانون المخابرات العامة المصري رقم ١٠٠ لسنة ١٩٧١ بأنه لا يجوز لأي فرد أو جهة حكومية أو غير حكومية أن تخفي بيانات يطلبها منها رئيس جهاز المخابرات أو أحد أفراد الجهاز المصرح له بذلك مهما كانت طبيعة تلك البيانات أو ترفض إطلاعه عليها". (٣٣٦٠)

وتأكيدًا لما سبق صدر القرار الجمهوري رقم ٤٧٢ لسنة ١٩٧٩ بشأن نظام المحافظة على الوثائق الرسمية للدولة وأسلوب نشرها واستعمالها. (٣٣٦١)

وقد انتقد البعض استطالة مدة الحظر المعلوماتي عامة إلى ما يقارب خمسين عامًا. (٣٣٦٢)

وتعد الاستثناءات المتعلقة بالأسرار العسكرية أو الأمن القومي من أهم مجالات الأمن المعلوماتي، ويرى الفقه أن كافة المعلومات التي تتعلق بالقوات المسلحة وتشكيلاتها وتحركاتها وعتادها وأفرادها، وبصفة عامة كل ما له مساس بالشؤون العسكرية والاستراتيجية يعد من أهم مجالات الأمن المعلوماتي .(٣٣٦٣) وهذا ما تأكد بموجب المادة ٨٥ من قانون العقوبات المصري(٣٣٦٤)

(٣٣٥٩) من ذلك على سبيل المثال: توجه القيادة الحكومية في مصر نحو تأسيس بنية معلوماتية وتكنولوجية قادرة على استيعاب قواعد البيانات القومية بما يحقق التكامل بين مختلف الجهات الإدارية:- خير منشور على موقع اليوم السابع الإلكتروني بتاريخ ١٤ نوفمبر ٢٠١٦-آخر تحديث ٢٢ أغسطس ٢٠١٧

(٣٣٦٠) انظر المادة الأولى من القانون والتي خولت رئيس الجمهورية وضع نظام للحفاظ على الوثائق والمستندات الرسمية المتعلقة بالسياسة العامة للدولة أو الأمن القومي.

تجدر الإشارة إلى أن حيازة المعلومات فى مصر كانت تتلخص في الوثائق الرسمية المكتوبة- حيث لم تكن الثورة المعلوماتية وطفرة وسائل الإتصالات قد ظهرت -وكانت المعلومات المتعلقة بالسياسة العامة للدولة أو الأمن القومي أو الأمن العام إحدى عناصر الأمن المعلوماتي، ودليلنا في ذلك صدور القانون رقم ١٢١ لسنة ١٩٧٥ بشأن المحافظة على الوثائق الرسمية للدولة وتنظيم أسلوب نشرها

(٣٣٦١) د/ دويب حسين صابر، المرجع السابق ص٢٠٥.

وكان البعض حينها ينتقد وجود عبارات مرنة داخل القانون كعبارة "السياسات العامة للدولة" و"الأمن القومي" لكونها غامضة مطاطة

(٣٣٦٢) د/ فاروق عبد البر، المرجع السابق ص١٤، ولا شك أنها مدة طويلة خاصة في ظل النظم الشمولية وغير الديمقراطية التي لا تعرف المسئولية السياسية لحكامها، كما أنها تعد مدة طويلة في ظل وسائل التكنولوجيا الحديثة ووسائل الاتصالات المتقدمة التي تمكن من الحصول على المعلومات مهما أحاطتها السرية".

(٣٣٦٣) د/ محمد سعيد حسين أمين، المرجع السابق ص٥٣.

(٣٣٦٤) انظر المادة ٨٥ من قانون العقوبات المصري، ويرى البعض أن مشكلة تحديد ما يعد من الأسرار وما لا يعد منها يعد إشكالية لاحقة اعتبرت تلك المادة أن من أسرار الدفاع ما يلي:

١) المعلومات الحربية والسياسية والدبلوماسية والاقتصادية والصناعية التي بحكم طبيعتها لا يعلمها إلا الأشخاص الذين لهم صفة ذلك، ويجب مراعاة لمصلحة الدفاع عن البلاد أن يبقى سرًا على من عداهم.

٢) الأشياء والمكاتبات، والمحررات والوثائق والرسوم، والخرائط والتصميمات والصور وغيرها من الأشخاص التي يجب لمصلحة الدفاع عن البلاد ألا يلم بها إلا من يناط بهم حفظها أو استعمالها، والتي يجب أن تبقى سرًا على من عداهم.

ومن النصوص التي تكرس نفس الفكرة ما جاءت به المادة الثالثة عشرمن قانون الأحوال المدنية رقم ١٤٣ لسنة ١٩٩٤ وذلك عقب قيام قطاع الأحوال المدنية بوزارة الداخلية باستخدام سجلات إلكترونية في حفظ بيانات المواطنين الشخصية ،إذ تضمنت وجوب الحفاظ على سرية البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين والتي يشتمل عليها السجلات، أو الدفاتر أو الحاسبات الآلية، أو وسائط التخزين الملحقة، ولم تتح تلك المادة الإطلاع على البيانات سوى في أحوال نص عليها القانون كأن يكون الإطلاع لمصلحة قومية أو علمية وبإذن كتابي من مدير مصلحة الأحوال المدنية أو من ينيبه وفقًا للأوضاع والشروط التي يحددها القانون واللائحة التنفيذية.

أما المادة ٦٥ من القانون أوجبت على الجهة الإدارية المختصة، وهى مصلحة الأحوال المدنية اتخاذ كافة التدابير اللازمة لتأمين البيانات الشخصية والمجمعة والمخزنة بالحاسبات الآلية أو بوسائط التخزين الملحقة بها ضد أي اختراق، أو عبث، أو إطلاع، أو إفشاء، أو تدمير، أو مساس بها بأية صورة كانت ويقع على عاتق مصلحة الأحوال المدنية اتخاذ تلك التدابير.[٣٣٦٥]

وإذا تطرقنا الى التشريع الأمريكي نجد أن جهة الإدارة هناك تحوز رصيدا هائلا من البيانات حول الأفراد لأغراض عامة ومهمة، وعادة ما تكون عملية جمع المعلومات باهظة التكاليف لما تحتويه من صعوبة التجميع أو التكوين، وقد وصفت المحكمة العليا ذلك التأثير كصعوبة عملية أكثر من كونه خصوصية حيث إنه بقدر بساطته يعد أمرا مكلفا وباهظ الثمن[٣٣٦٦].

---

٣) كل ما له مساس بالشؤون العسكرية والاستراتيجية والحركية، ولم يكن قد صدر إذن كتابي من القيادة العامة للقوات المسلحة بنشره أو إذاعته

للمزيد انظر:

د/ فاروق عبد الله، المرجع السابق ص١١.

(٣٣٦٥) للمزيد انظر د/ محمد أحمد عزت عبد العظيم، المرجع السابق ص٢١٣.

كذلك من النصوص التي تكرس حماية الأمن المعلوماتي لجهة الإدارة ما جاءت به المادة الثالثة من قانون الإحصاء والتعداد الصادر بقرار من رئيس الجمهورية رقم (٣٥ لسنة ١٩٦٠) المعدل بالقانون رقم (٢٨ لسنة ١٩٨٢) حيث أكدت تلك المادة على سرية البيانات الفردية التي تتعلق بأي إحصاء أو تعداد، فحظرت إطلاع أي فرد أو هيئة عامة، أو خاصة عليها، أو إبلاغ شيء منها، كما أوجبت عدم استخدامها لغير الأغراض الإحصائية، كما جاءت المادة الرابعة بتجريم الإخلال بسرية البيانات الإحصائية. أو إفشاء أى بيان من البيانات الفردية، أو سر من أسرار الصناعة أو التجارة، أو غير ذلك من أساليب العمل التي يكون قد اطلع عليها بمناسبة عمله في الإحصاء أو التعداد.

علاوة على ما سبق رغبة من المشرع المصري فى سبيل حفظ الأمن المعلوماتي تطرقت المادة ١٠١ في قانون الضريبة على الدخل رقم ٩١ لسنة ٢٠٠٥ للحفاظ على بيانات الملف الضريبي للممول ويقع ذلك العبء على كل من يتعامل بحكم وظيفته واختصاصاته مع البيانات الضريبية.

(٣٣٦٦) Fred H. Cate, op. cit., p. ١

For more: see:– Kathleen M. Sullivan, under a watchful Eye:

Incursions on personal privacy, in the war on our freedoms: civil liberties in An AGE of TERRORISM ١٢٨, ١٣١ (Richard leone & Greg Anrig, Jr. eds, ٢٠٠٣).

كما قد يلزم المشرع جهة الإدارة بتدابير معينة يتم النص عليها في القانون كاتخاذ التدابير الوقائية اللازمة أمنيًا لحماية أنظمتها المعلوماتية وشبكاتها والبيانات والمعلومات الإلكترونية الخاصة بها.(٣٣٦٧) بل وقد يذهب في صورة أكثر تفصيلاً لإلزام الجهة المختصة باتخاذ االتدابير والإجراءات الكفيلة بالحفاظ على الأدوات والأنظمة المعلوماتية.(٣٣٦٨)

وعادة قد يكون جمع الحكومات للبيانات والمعلومات الشخصية حول الأفراد استجابة لظروف معينة تتعلق بالأمن القومي كمخاوف الحكومة الأمريكية من الهجمات الإرهابية(٣٣٦٩).

مثال ذلك سعى جهة الإدارة في الولايات المتحدة الأمريكية لإمتلاك معلومات أكثر خصوصية بعد الهوس الأمني الناتج عن هجمات سبتمبر ٢٠٠١.(٣٣٧٠)

"In the twenty-first century, Technology and law have combined to erode the protection for personal privacy. Previously afforded by practical obscurity. Advances in digital Technologies have greatly expanded the volume of personal data created as individuals engage in every day activities. "Today, our biographies are etched in the ones and zeros we leave behind in daily digital transactions".

(٣٣٦٧) نص المشرع القطري في المادة ٢٢ في قانون رقم ١٤ لسنة ٢٠١٤ بإصدار قانون مكافحة الجرائم الإلكترونية على أن: "تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي:

١) اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية ومواقعها الإلكترونية وشبكاتها المعلوماتية والبيانات والمعلومات الإلكترونية الخاصة بها.

٢) سرعة إبلاغ الجهة المختصة عن أي جريمة منصوص عليها في هذا القانون فور اكتشافها أو اكتشاف أي محاولة للالتقاط الاعتراض أو التصنت بشكل غير مشروع، وتزويد الجهة المختصة بجميع المعلومات اللازمة لكشف الحقيقة. =

= ٣) الاحتفاظ ببيانات تقنية المعلومات ومعلومات المشترك لمدة لا تقل عن ١٢٠ يومًا وتزويد الجهة المختصة بتلك البيانات.

٤) التعاون مع الجهة المختصة لتنفيذ اختصاصاتها.

(٣٣٦٨) نص المشرع القطري في المادة ١٩ من القانون سالف الذكر على أنه "على الجهة المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على الأجهزة أو الأدوات أو وسائل تقنية المعلومات، أو الأنظمة المعلوماتية أو البيانات أو المعلومات الإلكترونية محل التحفظ لحين صدور قرار من الجهات القضائية المعنية بشأنها".

(٣٣٦٩) federal support for Home land saurity information sharing: Role subcomm. On intelligence Information sharing and Risk Assessment of the H. comm. on Home land security, ١٠٩ th cong. ٢٣ (٢٠٠٥) (statement of lee Humilton, vice chairmanm ٩/١١ public Discourse project).

(٣٣٧٠) يكون ذلك من خلال ضمان أمن الرحلة "secure flight" عن طريق طلب الاسم الكامل للراكب ونوعه وتاريخ ميلاده وإرسال تلك المعلومات مع سجل الحجز وخط سير الرحلة إلى إدارة أمن النقل (TSA) "The Transportation security Administration" لمضاهاتها بقوائم الإرهاب =

= ومن أمثلة أبرز المؤسسات الحكومية الأمريكية التي تحفظ أمن النقل والطيران من خلال تداول المعلومات إدارة الطيران الفيدرالي "the federal Aviation and Transportation security Administration" (FAA).

وعلى صعيد آخر تعمل النظم التكنولوجية للمراقبة على مد الحكومات برصيد كبير من المعلومات الشخصية من خلال القطاع الخاص ومن خلال العديد من النظم(٣٣٧١).

المطلب الثاني

في

حيازة البيانات الروتينية

هناك نوع من البيانات يطلق عليه "البيانات الروتينية" تحصل عليه المؤسسات العامة والخاصة من العملاء يوميًا في قطاعات العمل، والتسوق، والسفر، والاستثمار والدراسة والاتصالات تكون مرفقة بنشاطات تلك المؤسسات، وبالتالي يمكن لجهة الإدارة أن تحصل على تلك البيانات بدون أي قيد دستوري، ولا شك أن طلب جهة الإدارة بالكشف عن بيانات تتعلق بالصحة والأمور المالية، أو الأذواق سيكون من الخصوصية بخلاف أن تطلب الحصول على تلك البيانات لن يكون بدون ضمانة أو تصريح قضائي(٣٣٧٢).

وتجدر الاشارة الى أن لائحة الحق في الخصوصية المالية الصادرة في عام ١٩٧٨ The Right to financial privacy act ١٩٧٨ من أوائل التشريعات الأمريكية التي وضعت قيودًا واسعة على

"In short, the TSA is trying to use the consequences of poordata matching to motivate passengers to provide more complete information necessary for more accurate matching.

For more: U.S. GEN. According office, GAO – ٠٤ – ٣٨٥, Aviation security: computer – lenges ٦–٧ (٢٠٠٤).

فى اعتقادنا أن الترخيص يعد وسيلة ناجعة فى حفظ الأمن المعلوماتى، ومن النصوص التشريعية التى تطرقت لتلك الوسيلة ماورد فى المادة ٢١ من قانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات، والتى نصت على أنه "لا يجوز إنشاء أو تشغيل شبكات اتصالات أو تقديم خدمات الاتصالات للغير أو تمرير المكالمات التليفونية الدولية، أو الإعلان عن شيء من ذلك دون الحصول على ترخيص من الجهاز وفقًا لأحكام هذا القانون والقرارات المنفذة له".

(٣٣٧١) for examples:–

– Radio frequency Identifivation (RFID).

– Global positioning system (FPS).

– Other location sensors.

(٣٣٧٢) H. cate, op. cit., p. ٢٦.

يلاحظ أن أغلب البيانات والمعلومات التي تحصل عليها الإدارة يتم من خلال طرف ثالث – غالبًا يكون قطاعاً خاصاً – ويتم تجميع تلك البيانات عن طريق ذلك الطرف لأغراض إدارية.

تحصيل الحكومة للبيانات بل وألزمت جهة الإدارة بوضع دليل إرشادي واضح لكيفية تحصيل تلك البيانات يوازن بين حماية الخصوصية من ناحية والأمن المعلوماتي من ناحية أخرى.

مؤدى ما سبق إن جمع البيانات لأغراض الأمن القومي من أكثر الأشكال التي تثير العديد من الإشكاليات لوقوعها على تخوم العلاقة بين الفرد (وحقه في الخصوصية) والدولة (وحقها في الأمن القومي)، "فقد طالبت الحكومة الأمريكية المؤسسات المالية بتقارير بيانات واسعة المدى في إطار جهودها في محاربة الإرهاب وذلك من خلال تعديل قانون سرية البنوك The Bank secrecy act في ٢٠٠١ بل طالبت الحكومة بموجب قانون "الباتريوت" "A PATRIOT act" المؤسسات المالية أن تمدها بتقارير حول الصفقات المؤكدة التي قد تفيد في المسائل الجنائية والاستخباراتية والضريبية وفي مجال محاربة الإرهاب، بل وتعدى ذلك إلزام الأفراد المتعاملين مع البنوك بملء تقارير النشاطات المشتبه بها "suspiciais Activity Reports" وتقارير تحويل العملة "Currency Transaction Reports" بالنسبة للتحويلات التي تعادل ١٠ آلاف دولار أو تزيد ويقع ذلك الالتزام على أي جهة تتعامل ماليًا مع تلك التحويلات، **كمثال:** وكالات السفر، والمرتهنين، والفنادق، أو أي شخص يتعامل مع ذلك النوع[٣٣٧٣].

في

الآليات المعتادة لرصد وحيازة البيانات والمعلومات

قد تعمد جهة الإدارة إلى اللجوء إلى آليات أمنية لرصد بعض المخاطر على شبكات التواصل الاجتماعي، **ومثال ذلك:** ما قامت به وزارة الداخلية المصرية من إنشاء مشروع لرصد المخاطر الأمنية لشبكات التواصل الاجتماعي في مصر (منظومة قياس الرأي العام).

وقد ذهبت محكمة القضاء الإداري (الدائرة الثامنة) إلى إقرار ذلك الإجراء الضبطي الإداري كونه لا يعدو إلا أن يكون وسيلة لتمكين وزارة الداخلية من القيام بدورها المنوط بها، واعتبرت أن قيام جهة الإدارة بإنشاء تلك الآلية يعد من قبيل الرقابة والتنظيم وليس التقييد. [٣٣٧٤]

(٣٣٧٣) Fred H. Cate, op. cit., p. ١١

:The USA PAIRIOT act also mandates new rules requiring all financial institutins to: (١) verify the Identity of any person seeking to open an account, (٢) maintain records of the information used to verify the person's identity and (٣) provide the information to the government of matching with terrorist watch lists".

Seem eg., customer Identification programs for Banks, saving Association a credit unions, and certain Non-federally Regulated Banks, ٦٨ fed. Reg. ٢٥, ogo (June ٩, ٢٠٠٣).

(٣٣٧٤) حكم محكمة القضاء الإداري – الدائرة الثامنة عقود في الدعوى رقم ٦٣٠٥٥ لسنة ٦٨ ق بتاريخ أغسطس ٢٠١٥ (حكم غير منشور).

"... فكل من الدستور والقانون قد أوجب على وزارة الداخلية الحفاظ على النظام العام والأمن العام والأرواح والأعراض والأموال ومنع الجرائم وضبطها والبرنامج ليس إلا وسيلة لتمكين وزارة الداخلية من القيام بدورها المنوط بها، فضلاً عن أن هذا البرنامج من شأنه فقط

لذا تتعدد آليات الإدارة فى رصد المخاطر المعلوماتية لكننا سنقتصر على أهم آليتين وهما كالتالى:

أولا: نظام الأرشفة الإلكترونية:

يعد نظام الأرشفة الإلكترونية أحد أقدم وسائل التقليدية لحفظ الأمن المعلوماتي ،ويرى البعض امكانية تفعيله كالتالي:-

١) تشكيل لجان حكومية في كل إدارة لدراسة أفضل طرق حفظ الوثائق المعلومات.

٢) أخذ نسخ للبرامج بغرض تشغيل الدعامات القديمة عند الحاجة إليها.

٣) استخدم دعامات إلكترونية لضمان الحصول على البيانات الإلكترونية في حالة فشل تشغيل أي من الدعامات الأخرى والعمل على القيام بعملية تحويل يومي back up خارج جهاز الحاسوب. (٣٣٧٥)

علاوة على ما سبق تعد معالجة البيانات للأغراض الإدارية أحد أوجه نظام الأرشفة الإلكترونية "Data processing model of administrative control" ويمكن **تعريفها بأنها:** هى الشكل التقليدي لمعالجة البيانات حيث يزداد اعتماد الجهات الإدارية على البيانات الشخصية للاستخدام في الأغراض الإدارية، سواء أكانت للأمن الاجتماعي أو الصحي أو قانون العمل أو الضرائب أو مجال ممارسة الحقوق السياسية في انتخاب وترشيح أو المجال الاجتماعي كحالات الميلاد والطلاق والوفاة.

ويرى الفقه المقارن أن هذا الشكل يقوم على اعتماد جهة الإدارة على موظفيها في جمع تلك البيانات، ثم تحليلها من قبل المتخصصين الذين يقومون بالتقييم والتقدير باستقلالية تامة(٣٣٧٦).

الإطلاع على محتوى متاح للكافة يمكن لأي شخص الإطلاع عليه بمجرد دخوله على شبكة الإنترنت، وليس من شأنه اختراق حسابات الأشخاص، أو الإطلاع على بياناتكم الشخصية...".

(٣٣٧٥) ناجح أحمد عبد الوهاب، المرجع السابق ص١٨١، ١٨٢.

للمزيد انظر:

- عبد العزيز السيد مصطفى – أساسيات الرقابة على نظم التبادل الإلكتروني للبيانات – بحث مقدم لمؤتمر التجارة الإلكتروني – الآفاق والتحدي - المنعقد بتجارة الإسكندرية يوليو ٢٠٠٢ ص٤١٩.
- د/ هدى حامد قشقوش: جرائم الحاسب الإلكتروني في التشريع المقارن – دار النهضة العربية القاهرة ١٩٩٢.

(٣٣٧٦) Paul Schwartz, Data processing and Government Administration: The failure of the American legal Response to the computers HASTINGS LJ. ١٣٢١ (١٩٩٢) (emphasis in original),p٤٣

ومن أشكال معالجة البيانات للأغراض الإدارية

١) Government Benefits and Social service programes.

٢) Taxes.

٣) Employment.

٤) Law Enforcement.

ويمكن أن يقترب مصطلح معالجة البيانات من مصطلح "استخلاص البيانات" "Data Mining" حيث يقوم المصطلح الأخير – بمفهوم واسع – على الأنشطة التي تقوم على البيانات كأبحاث تقوم على دراسة موضوع ما أو الأبحاث التي تقوم على دراسة أشخاص بعينهم أو الأبحاث التي تقوم على دراسة نمط ما أو الأشكال المتنبأ بها بالنسبة للأنشطة والعلاقات، ويتصل اصطلاح استخلاص البيانات بمصطلح آخر وهو اصطلاح توفيق البيانات "Data matching".[٣٣٧٧]

ثانيا: الاستشعار عن بعد:

يعد الاستشعار عن بعد من أدوات جهة الإدارة في استخلاص البيانات ، ويمكن تعريفه بأنه طريقة للحصول على معلومات عن شيء ما من مسافة بعيدة، ويستخدم هذا التعبير في الوقت الحاضر لوصف الطرق التي تُجمع بها البيانات عن الأهداف أو الظواهر الطبيعية التي تحدث على سطح الأرض أو بالقرب منه من مكان مرتفع في الهواء أو في الفضاء الخارجي. وبالتالي لا يوجد فرق بين الاستشعار من بعد من الجو أو من الفضاء الخارجي في كثير من النواحي الفنية"[٣٣٧٨].

أضف الى ماسبق يُعد تدفق البيانات نتاجا لعمليات الاستشعار من بعد عبر أربعة مراحل ثابتة، وهي مرحلة جمع البيانات ثم معالجتها وتفسيرها وأخيرًا توزيعها ونشرها.[٣٣٧٩]

(٣٣٧٧) Fred H. Cote, op. cit., p. ٤

Data Matching:– Between these two ends are “relational” searches, which start with an individual but then reach out to determine who communicates or otherwise interacts with whom and determine who communicates or otherwise interacts with whom and “data maching” which involves combining two or more sets of data looking for matches or discrepancies”. =

= تستخدم المؤسسات الحكومية الدراسات التي تقوم على الموضوع والدراسات العلائقية المتصلة كمثال دراسة المسئولين عن تنفيذ القانون لبصمات شخص ما في مسرح الجريمة، أو سائق السيارة وقد يستخدم أيضًا في مجال الضرائب... إلخ، أما دراسات الشكل أو النمط تتصل بصورة أكبر بالقانون التجاري ودراسات تقوم على المستهلك وتقديرات المخاطر التجارية بل وزاد استخدام دراسات النمط بعد هجمات الحادي عشر من سبتمبر ٢٠٠١، فقد طلب الكونجرس بموجب قانون الأمن الوطني لسنة ٢٠٠٢ من الإدارة الجديدة للأمن الوطني.

Department of Homeland security (DHS)

أن يقوم بإنشاء أدوات متقدمة حول الدخول للبيانات واستلامها وتحليلها لاكتشاف المخاطر الإرهابية التي تواجه الولايات المتحدة.

(٣٣٧٨) Marietta Benko, and others, space law in the united nations, Martinus Nijhoff, Netherlands, ١٩٨٥, p.٣

(٣٣٧٩) د/ ممدوح فرجاني، المرجع السابق ص٢٤٦. =

= تكون تلك الآلية بإنشاء أدوات متقدمة حول الدخول للبيانات واستلامها وتحليلها لاكتشاف المخاطر الإرهابية التي تواجه الولايات المتحدة.

وكما تؤدي أنشطة الاستشعار من بعد مهامها في جمع البيانات من الأرض فإنها تستخدم لتوصيل البيانات التي يتم التحصل عليها بواسطة توابع الاستشعار، إلى الأرض، أو توصيل أوامر السيطرة إلى هذه التوابع، وتكمن الصعوبة العملية في أن التوابع الاصطناعية لا تحدد حدود الدول من الفضاء الخارجي بسهولة ،لذا لا يمكن فصل البيانات الخاصة بدولة ما عن باقي البيانات إلا بصعوبة بالغة قد تكون مستحيلة أو باهظة التكاليف إقتصاديًا(٣٣٨٠).

المطلب الرابع

في

اشكاليات حيازة جهة الإدارة للمعلومات وطرق حلها

تجدر الإشارة إلى أن حيازة جهة الإدارة للمعلومات الشخصية خاصة الواردة من أطراف ثالثة تثير إشكاليتين، **الأولى:** الكفاءة "efficacy" بمعنى هل تضمن عملية حيازة تلك المعلومات المصادر المالية والبشرية التي تتطلبها؟ **والثانية:** التأثير "Impact" بمعنى هل يؤدي احتكار القطاع الخاص للمعلومات لإثارة المخاوف لدى جهة الإدارة حول سلوك مضر بالأفراد أو بطريقة أو بأخرى(٣٣٨١).

فى اعتقادنا أنه فيما يخص الكفاءة يمكن أن تؤتي حيازة المعلومات أُكلها بحسب المقاصد التي تحددها جهة الإدارة – خاصة فيما يتعلق بمسائل الأمن القومي وقانون التنفيذ- حيث لا تستطيع الادارة وحدها مواجهة أو منع الأنشطة الإرهابية بناء على تحليل البيانات أو المعلومات وتزداد تلك الإشكالية خاصة عندما تتعارض حيازة المعلومات بغرض الحفاظ على الأمن القومي مع حيازتها لأهداف تجارية لذا يمكن تلخيص عنصر الكفاءة في ثلاثة بنود:-

البند الأول: جودة البيانات Data Quality

في محاولة لتقييم مصطلح حيازة المعلومات لحماية الأمن القومي، قام المركز البحثي التابع للكونجرس (CRS) بتعريفه على أنه مسألة متعددة الوجوه ويشكل ذلك هو التحدي الأبرز في حيازة المعلومات. (٣٣٨٢)

(٣٣٨٠) Van ligten Hans, Municipal law Regulation of Remote sensing in outer space, loyola of Los Angles International and comparative law Journal (Winter, ١٩٨٤)

مشار إليه في د/ ممدوح فرجاني، المرجع السابق ص٢٤٨.

(٣٣٨١) H. Cate, op. cit., p. ٣٥ "If its harmful impact is very low "oven marginally successful data mining might be appropriate if used as= = an additional layer of protection against a particularly grave threat".

For more:

–Tommy Peters on, Data scrubbing, computer world, Feb. ١٠, ٢٠٠٣, at ٣٢.

(٣٣٨٢) تتضمن حيازة المعلومات من جهة الإدارة عادة إعادة تصميم للمعلومة "repurposing"

وتتأتى الإشكالية الأكبر في بند جودة المعلومة كما ذكر في مجلة "computer world" في ٢٠٠٣ من أن "بياناً واحداً من معلومة سيئة" يعد إشكالية بديهية ، ولكن إذا زادت أجزاء البيانات السيئة لنحو آلاف أو ملايين الأخطاء فإن ذلك سيؤدي لمعلومات غير متناسقة تؤدي إلى الفوضى(٣٣٨٣).

البند الثاني :تناسق البيانات "Data matching"

تواجه جهة الإدارة العديد من الأخطاء في حيازة المعلومات(٣٣٨٤) ومنها تناسق البيانات، وقد يستعان في الولايات المتحدة الأمريكية للتغلب على تلك الأخطاء برقم الضمان الاجتماعي "social security Numbers" وقد واجهت الإدارة في الولايات المتحدة نفس الإشكالية خاصة عند مواجهة الإرهاب.(٣٣٨٥) ويكون ذلك لكي يتم تعريف الأفراد القادمين لحدود الدولة وتقدير مدى الخطر الذي يحوم حولهم من خلال المعلومات الدقيقة عنهم،

"The fact that government data mining almost always involves "repurposing" data – i – e – using data for a purpose different from that for which they were originally collected and stores further exacerbates concerns about the accuracy of the underlying data".

For more:– see: office of Inspector GEN, U.S. DEPT of Just, IMMIEGRATION AND NATURALIZATION SERVICE'S ABILITY TO PROVIDE TIMELY AND ACCURATE ALIEN= =INFORMATION TO THE SOCIAL SECURITY ADMINISTRATION (No. ١.٢٠٠٣-٠٠١) at ٢٥ (٢٠٠٢).

(٣٣٨٣) The accuracy of records raises important practical concerns about the value of national important practical concerns about the value of national security analyses performed on potentially bad data as well"

(٣٣٨٤) مثال تلك الأخطاء كالآتي (طريقة كتابة الأسماء، تغيير النساء لأسمائهن خاصة بعد الزواج، العديد من الأشخاص لهم نفس الأسماء، العديد من الأشخاص يشتركون في نفس العنوان سواء عمل أو مسكن أو صندوق بريدي.

(٣٣٨٥) تضمين رقم الضمان الاجتماعي لم يحل تلك الإشكالية في الولايات المتحدة لأن الحسابات الخاصة بكل عائلة يمكن أن يوجد بها أرقام ضمان اجتماعي مختلفة كالزوج والزوجة والمعيل القاصر علاوة على ذلك البيانات الخاصة بالهجمات الإرهابية المحتملة أرقام الضمان الاجتماعي لا تتضمن أرقام ضمان اجتماعي .

ويعد ذلك أكثر ما تم التركيز عليه في تقرير اللجنة الاستشارية للخصوصية والتكنولوجيا (TAPAC) [٣٣٨٦] حيث يعد التحدي الأكبر هو كيفية ضمان أمن المعلومات خاصة في حالات مواجهة الإرهاب ورصد البيانات أو تجميعها من جهات مختلفة منفصلة عن بعضها البعض، **كمثال:** جهات المخابرات الذي لا يخضع لأي سيطرة.

وفي الواقع – أيضًا – يزداد الأمر صعوبة عند وجود بيانات غير متوافقة وغير منتظمة كمثال كاميرات المراقبة الصوتية وكاميرات الفيديو[٣٣٨٧].

البند الثالث: حيازة أدوات حيازة المعلومات Data Mining Tools

تواجه مسألة حيازة المعلومات بغرض الحفاظ على الأمن القومي وقانون التنفيذ تحديات أكبر من مسألة حيازتها بغرض الأهداف التجارية للعديد من الأسباب ، فمثلاً تعد حيازة جهة الإدارة للمعلومات ذات غرض محدد للأهداف البشرية عن القطاع الخاص، علاوة على ذلك غالبًا ما يعمد مخترقو الأمن المعلوماتى لتضليل جهة الإدارة مقارنة بالقطاع الخاص "Government data mining often is searching for needle not in a haystach, but among millions of other needles.

ومع ذلك تعد المعلومات الواردة من القطاع الخاص مفتاحًا مهمًا للأمن القومي من خلال توقع المسئولين عن الأمن القومي للسلوك المعتاد لعملاء القطاع الخاص[٣٣٨٨].

(٣٣٨٦) This is a substantial challenge, as stressed in the ٢٠٠٤ final report of Technology and privacy Advisory committee (TAPAC) the "blue ribbn" bipartisan independent committee appointed by the secretary of Defense Donald Rusfeld in ٢٠٠٣ to examine privacy and security issues.

For more see: Ronald D. lee & Paul M. Schwartz Beyond the "war" on Terrorism: Towards the New Intelligence Network, ١٠٣ MICH. L. REV ١٤٤٦, ١٤٦٧ (٢٠٠٥).

(٣٣٨٧) See: ١) Emily key, coordinating supply chain Data: To Deliver timely Informantion, companies must overcome Data synchronization Hurdles, frontline solutions, May ١, ٢٠٠٣ at ٢١.

٢) Margo Anderson & Stephen E. Feinberg, who count,? the politics of census – taking in contemporaty America ١١٧–١٨ (Russell stage found – ١٩٩٩).=

="The fact that many government data mining applications unstructured data (e.g. audio and video surveillance records) exacerbates the a for mentioned concerns".

"Government data mining seems similarly likely to fighting yesterday's battles".[٣٣٨٩]

ويتحقق منع الهجمات الإرهابية من خلال إعداد الإدارة لبرامج واضحة مسبقة تحدد الأهداف التي من أجلها يتم جمع تلك المعلومات مع مراعاة الدقة والنفقات[٣٣٩٠].

البند الرابع: تقدير الكفاءة Assessing Efficacy

يذهب الفقه المقارن إلى القول بأهمية تقدير كفاءة نظم حيازة المعلومات، ومن المحاولات الأولى في ذلك ما تتطلبه التشريع الأمريكى عند أية محاولة لحيازة المعلومات من أن يكون هناك إذنًا مكتوبًا من الرئيس الإداري الأعلى للجهة الإدارية حائزة المعلومات[٣٣٩١].

(٣٣٨٨) Jeff Jonas & Jim Harper, cato institute, Effective counter terrorism and the limited role of predictive Data mining ٧-٨ (٢٠٠٦).

"For example, data mining used to predict types of consumer behavior ... may be used on as many as millions of previous instances of the same particular behavior".

لذلك يعد رجال الأمن في الولايات المتحدة أكثر توقعًا للهجمات الإرهابية الخارجية من خلال توقع ضباط الاستخبارات للخطط الإرهابية بناء على النشاط الإرهابي في الماضي بخلاف الهجمات الإرهابية المحلية تتخذ شكلاً مختلفًا كل مرة في التخطيط والتنفيذ بحيث تكون مواجهتها أقل وفرص كشفها غير متوقعة.

(٣٣٨٩) For more see: CRS report on Data mining and Homeland security ٢٠٠٧

Hector Becerra, Jennifer Oldham & Mitchell landsberg, Airline Terrorism Alert: winging it one Again, L.A. Times, Aug. ١١, ٢٠٠٦, At A١.

(٣٣٩٠) Jones & Harper, op. cit., p.٢

One of the bluntest assessments comes from Jeff Jonas, Chief scientist of IBM's Entity Analytic solutions Group, and Jim Harper, director of information policy studies at "the cato institute".

(٣٣٩١) TECH, AND PRIVACY ADVISORY COMM, U.S. DEPT of DEL Safeguarding privacy in the fight Against terrorism (٢٠٠٤) TAPAC, safeguarding privacy.

مؤدى ماسبق يرى البعض وجود حرج في مساءلة جهات الإدارة التي تقوم على حيازة البيانات الشخصية للأفراد على اعتبار أن قراراتها غالبًا ما تكون مدروسة وبناء على ضمير مهني(٣٣٩٢)، وفى اعتقادنا أن صعوبة إثبات المسئولية الإدارية عن الخطأ فى حيازة الإدارة للمعلومات لاتعنى القول بنفى المسئولية عنها.

البند الخامس :تقييم آثار حيازة البيانات "Assessing Impact"

هناك حاجة للتوازن بين حيازة المعلومات والحريات المدنية والخصوصية، **فعلى سبيل المثال:** أوصت اللجنة الاستشارية للخصوصية والتكنولوجيا TAPAC بالعديد من المتطلبات القانونية للحد من الآثار السلبية لحيازة المعلومات، وهي كالتالي:

١- لا بد من وجود إذن مكتوب من رئيس الجهة الإدارية المسئولة عن جمع تلك البيانات.

٢- لا بد أن يحدد ذلك الإذن – بجانب النقاط التي سيتناولها –التدابير التى تم اتخاذها.

٣- لا بد أن يحدد الإذن الآثار التي ستقع على الأفراد موضوع ذلك الإذن أو الفحص.

٤- لا بد أن يخضع الأفراد محل الاستقصاء لفحص إضافي قبل السماح لهم بمغادرة البلاد.

٥- وجود نظام في حالة وجود مؤشرات ضد الشخص محل الاستقصاء ولكنها كانت زائفة فيما يعرف "false positives" كي يسمح ذلك النظام بتصحيح معالجة المعلومات الزائفة كلما كان ذلك ممكنًا(٣٣٩٣).

وفي توصية ثانية تتطلب "TAPAC" عمل قواعد بيانات تحوي حدًا أدنى من البيانات Data minimization وتدقيق خط السير audit trail تتضمن المعلومات الشخصية المميزة لمواطني الولايات

(٣٣٩٢) Privacy and civil liberties in the Hands of Government post-september ٢٢, ٢٠٠١: Recommendations of the ٩/١١ commission and the US. Department of Defense Technology and privacy Advisory committee. Hearing Before the subcomm. On commercial and Administrative law ad subcomm-on the constitution of the H. comm. On the Judiciary, ١٠٨th cong. ٥(٢٠٠٤) (Statement of John O. Marsh, Jr. TAPAC).

"We believed that accountability was absolutely critical To.... ensuring that data mining was conducted efficiently and effectively, ... [and that it] would be enhanced, we believed, first by ensuring that no agency engage in data mining involving personal information without making a conscious, thoughtful decision to do so".

(٣٣٩٣) TAPAC, safeguarding privacy, op. cit., at ٥٠

المتحدة الأمريكية لعمل قاعدة من البيانات التقنية كى تتوافر لاحقا،علاوة على تأمين تلك القاعدة وتسهيل الدخول إليها والتدريب على استخدامها(٣٣٩٤).

وتجدر الإشارة الى أن أحد ضمانات (اللجنة الاستشارية للخصوصية والتكنولوجيا) لغير المواطنين ما جاءت به التوصية الرابعة من وجوب التحصل على ترخيص قضائي من محكمة المراقبة الاستخباراتية للأجانب Foreign Intelligence surveillance court (FISC)

وفى اعتقادنا أن التحديث المستمر للبيانات الشخصية يعد من إعتبارات الفاعلية ، وهذا ما أكدته التوصية الخامسة من تقرير اللجنة سالفة الذكر إذ أوجبت تعديل البيانات الشخصية المميزة عن مواطني الولايات المتحدة سنويًا لضمان توافقها مع تلك المتطلبات(٣٣٩٥).

أما التوصية الأكثر أهمية من وجهة نظرنا فهي توصية الإدارة المسئولة عن حيازة تلك البيانات لتعزيز المحاسبة والشفافية، ويتضمن ذلك التدريب على المتطلبات التقنية "Technical Requirements" وتعيين من هو قادر على فهم سياسة الخصوصية، وكذلك تعيين هيئة استشارية خارجية "a Panel of external advisors" مع وجود آليات إشراف فعالة تتضمن تقريرًا سنويًا إلى الكونجرس لتقييم التوافق مع الأمن القومي والقوانين والتشريعات المطبقة، وبذلك تتوافق اعتبارات الفعالية مع الحياد اللازمين(٣٣٩٦).

مؤدى ماسبق يجب على جهة الإدارة أن تُضمن العديد من الشروط في النظام القانوني لحيازة البيانات والمعلومات، وقياسا على الولايات المتحدة تتضح تلك الشروط كالتالي:-

١) تصريح من الكونجرس أو المسئول الإداري الأعلى بالنسبة للبرامج الجديدة لحيازة المعلومات لضمان كفاءة تلك البرامج وتوافقها مع المتطلبات القانونية، مع تطلب مستوى عال من الإشراف والمحاسبة من الإدارات الفيدرالية.

٢) اتباع التعليمات القانونية عند تقييم تلك البيانات والمعلومات كي لا يتم انتهاك القانون، سواء من الإدارة نفسها أو من الصحافة، أو من الأطراف الثالثة عند حيازة المعلومات.

٣) التقييم الدائم لأثر إنجاز الأهداف المقصودة قبل نشر تلك البيانات والمعلومات.

(٣٣٩٤) Id,at ٥٠

(٣٣٩٥) Id, at ٥٠

(٣٣٩٦) Id, at ٥٥

For more see letter from William J. Haynes II, Gen. counsel, Dept of Def, to carol E. Drinkins, civil Rights and civil Liberties oversight Bd, (Sep. ٢٢, ٢٠٠٦) (on file wih the Harvard civil Rights – civil liberties law Review) attaching a list of TAPAC's recommendations with each of those applicable to the DOD initialed by the Deputy secretary as "approved".

٤) وضع قيود على القائم على استخدام البيانات، والمتعامل معها علاوة على وضع تقييد أغراض استعمال تلك البيانات وأدوات تنفيذ تلك القيود.

٥) وضع نوع من الإذن أو التفويض القضائي Judicial authorization قبل نشر برامج المعلومات أو استخدامها عند نشر بيانات شخصية مميزة تؤثرعند استخدامها على المواطن.

٦) استخدام أدوات الفحص audit tools للتأكد من أن القواعد الخاصة بحيازة البيانات قد تم إتباعها(٣٣٩٧).

علاوة على ماسبق يذهب الفقه المقارن إلى الإقرار بالمسئولية الإدارية للنظام القانوني عن حيازة البيانات والمعلومات، من خلال التأكد من وجود نظام لتعويض الأفراد الذين قد أضيروا من حيازة جهة الإدارة تلك البيانات والمعلومات مع منح الأفراد الفرصة الملائمة لتصحيح البيانات الخاطئة، ويمكن التقليل من آثار تلك المسئولية من خلال إشراف الإدارة على عمليات تجميع البيانات من خلال درجات عالية من المحاسبة accountability تضمن استخدام تلك البيانات بطريقة ملائمة appropriately وقانونية lawfully ومؤثرة effectively، ولا بد أن تحوي تلك الرقابة على مراجعة مسئول أعلى، اومن خلال تدقيقات روتينية وتحقيقات من المفتش العام للإدارة، وتقارير منتظمة إلى الكونجرس إلى المدى الذي يتفق مع سياق تجميع تلك البيانات مع ضمان صراحة ذلك النظام واستقلاليته(٣٣٩٨).

مؤدى ماسبق نؤيد الرأي سالف الذكر فيما ذهب إليه لأنه بدون التنظيم القانونى لأى نظام لحيازة البيانات والمعلومات سيكون لدى جهة الإدارة كم هائل من البيانات أشبه ما يكون إلى الفوضى(٣٣٩٩).

فى ذات السياق عمد المشرع المصري إلى إصدار قرار بتشكيل لجنة عليا لتنقية قواعد البيانات القومية وذلك بموجب قرار رئيس الجمهورية رقم ٥٥٢ لسنة ٢٠١٥. (٣٤٠٠)، ونعتقد أيضا بأن غرض تلك

(٣٣٩٧) For example "the analyst might be asked to specify whether she has a search warrant, and if she does not, the system might not allow her to retrieve certain kinds of information".

(٣٣٩٨) H. Cate, op. cit., p. ٥٥

(٣٣٩٩) "In addition to the government's many domestic data sources, it also receives more than ٦٥٠ million intelligence intercepts everyday"

(٣٤٠٠) انظر المادة الأولى من قرار رئيس الجمهورية رقم ٥٥٢ لسنة ٢٠١٥ الجريدة الرسمية – العدد ٥٢ مكرر (هـ) في ٢٩ ديسمبر سنة ٢٠١٥، حيث نصت على أن تشكل لجنة عليا برئاسة السيد المهندس رئيس مجلس الوزراء وعضوية كل من السادة:-

١) وزير الدفاع والإنتاج الحربي. ٢) وزير الداخلية.

٣) وزير الاتصالات وتكنولوجيا المعلومات. ٤) رئيس المخابرات العامة =

= وللجنة أن تستعين بمن تراه من ذوي الخبرة من وزارات الدولة وهيئاتها ومصالحها ويكون لمندوبي الوزارات والهيئات والمصالح الذين يتم اختيارهم من ذوي الخبرة صلاحية اتخاذ القرارات المناسبة نيابة عن الوزارات التي يمثلونها.

وفى اعتقادنا أنه قد غلب على تشكيل تلك اللجنة الطابع الأمني ولكن خفف من قلة وجود العنصر الفني ما تم النص عليه فى القانون من جواز الاستعانة بذوى الخبرة من وزارات الدولة

اللجنة العليا يميل إلى الطابع التنموي الاقتصادي وليس الطابع الأمني المعلوماتي أو السيبري وذلك بحسب ما نصت عليه المادة الثانية.[٣٤٠١]

المطلب الخامس

في

حيازة الإدارة للمعلومات البيومترية

بالإضافة الى ما سبق ايراده من مكونات لنظم حيازة المعلومات يمكن أن يمتد الأمن المعلوماتي إلى التسجيلات الإلكترونية للمعلومات البيومترية كالحامض النووي DNA لتفعيل آليات الضبط الإداري، ووفقا لذلك نص قانون حماية المعلومات لعام ٢٠١٢ والصادر في المملكة المتحدة فى المادة ٢٣ منه على ما يلي: "بالاستناد إلى القسم (٦٣ أ) من لائحة الإثبات الجنائية والشرطية لعام ١٩٨٤ لا بد أن تضم قاعدة البيانات القومية الملفات الشخصية للحامض النووي DNA" وأشارت الفقرة الثانية من المادة على وجوب تسجيل الملفات الشخصية للحامض النووي على قاعدة البيانات القومية"[٣٤٠٢].

أضف إلى ذلك أن القوانين المقارنة تعمل على حفظ الأمن العام كأحد أركان النظام العام في الدولة عن طريق حيازة "المعلومات البيومترية"، وهي نوع من أنواع المعلومات اللصيقة بالفرد ، بحيث يؤدى وجودها – وفق ضمانات معينة – بحوزة الجهة الإدارية لفعالية الضبط الإداري. ومن أمثلة تلك: البيانات والمعلومات: شكل الجلد، والخصائص الشخصية، وملامح القزحية، وصوت الشخص، وكتابة يده[٣٤٠٣].

(٣٤٠١) نصت المادة الثانية على أن "تتولى اللجنة المشار إليها بالمادة الأولى تنقية قواعد البيانات القومية وتحليلها للتعامل مع اقتصاد الظل، وضبط المنظومة الضريبية، والتأمينية، والتنمية الإقتصادية".

والجدير بالذكر صدور قرار رئيس مجلس الوزراء رقم ٢٣٢٨ لسنة ٢٠١٤ والذي ضم بموجبه ممثل لمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء إلى عضوية المجلس الأعلى للأمن السيبراني".

"منشور بالجريدة الرسمية – العدد ٥٢ مكرر (ا) في ديسمبر سنة ٢٠١٤.

(٣٤٠٢) Protection of freedoms Act ٢٠١٢ Chapter ٩– United Kingdom, p. ١٨ clause ٢٣.

وحماية لتلك البيانات الشخصية أشارت المادة ٢٤ من ذات القانون إلى المجلس الخاص باستراتيجيات البيانات القومية للحامض النووي

(National DNA Datebase strategy Board)

وأشارت المواد اللاحقة إلى التزام ذلك المجلس بوضع دليل استرشادي لكيفية تدمير تلك البيانات، بل وأشارت إلى وجوب التزام الرئيس التنفيذي في الشرطة بذلك الدليل الاسترشادي.

(٣٤٠٣) “Biometric Information” means information about a person’s physical or behavioural characteristics or features which:–

a) is capable of being used in order to establish or verify the identity of the person, and

b) Is obtained or recorded the intention that it be used for purposes of biometric recognition system.

See clause ٢٨, protection of freedoms Act ٢٠١٢ (C٩) part ١– Regulation of biometric data.=

علاوة على ما سبق يمكن لجهة الإدارة تجميع البيانات من خلال امتلاك المعلومات حول التحويلات البنكية الدولية من خلال أدوات أخرى كمثال ماتقوم به جهة الإدارة فى الولايات المتحدة الأمريكية من التجميع عبر أداة"SWIFT"(٣٤٠٤) بل وأيضًا من خلال برنامج مراقبة الإرهاب "Terrorist surveillance program".(٣٤٠٥)

وأيضا يشكل برنامجى المراقبة المحلية "Domestic surveillance programm" والوعي المعلوماتي الكامل "Total Information Awarencess" "TIA".(٣٤٠٦) أحد الأدوات سالفة الذكر.

علاوة على ما سبق سارت أجهزة الضبط الإداري في المملكة المتحدة فى ذات النطاق لتعزيز أمنها المعلوماتى، **ومثال ذلك:** ما جاءت به المادة ٢٤ من قانون حماية الحريات لعام ٢٠١٢ Protection of Freedoms، والتى نصت على إنشاء المجلس الاستراتيجي لقاعدة البيانات المحلية للحامض النووي "National DNA Database strategy Board".

من ناحية يعمل وزير الداخلية فى إنجلترا على إعداد الترتيبات الخاصة بمد ذلك المجلس بالبيانات المحلية للحامض النووي، ويلتزم المسئول التنفيذي في الشرطة المحلية في إنجلترا وويلز بالدليل الاسترشادي الذي يصدر عن ذلك المجلس الاستراتيجي ،ومن ناحية أخرى يقع على وزير الداخلية التزام بأن ينشر القواعد الحاكمة ذلك المجلس، ويضع نسخة من تلك القواعد أمام البرلمان وذلك ضمانة للمحاسبة والمسئولية ويقع على المجلس الاستراتيجي ذاته التزامًا بأن يصدر تقريرًا سنويًا موجهًا إلى وزير الداخلية فيما يتعلق بممارسة مهامه، والذي بدوره يضع نسخة من ذلك التقرير أمام البرلمان(٣٤٠٧).

= وفي اعتقادنا أن تلك المعلومات تتعاظم أهميتها في الآونة الأخيرة خاصة بعد العمليات الإرهابية المتزايدة

(٣٤٠٤) "The society for world wide International financial Telecommunication".

(٣٤٠٥) نشرت صحيفة النيويورك تايمز في ١٦ ديسمبر ٢٠٠٥ عن وكالة الأمن القومي "NSA" أنها تقوم باعتراض الاتصالات على الأقل بمعدل اتصال واحد لكل شخص يوجد داخل حدود الولايات المتحدة الأمريكية بدون الحصول على إذن قضائي وتتم مراجعة أنشطة المراقبة تقريبًا كل ٤٥ يوم.

(٣٤٠٦) "TIA" Later renamed "Terrorism Information Awareness"

يحوي ذلك الفرع فهرسة للمعلومات حول فروع عدة، مثال الاتصالات، الأمور المالية، النقل، الإسكان، التقارير الحكومية، الأمور العلاجية.

وقد ثارت عاصفة احتجاجية في الكونجرس الأمريكي ضد "TIA" في ٢٣ يناير ٢٠٠٣ بواسطة السيناتور "William Safire" بناء على اعتدائه على الخصوصية ونادي بأن يكون اعتراض الاتصالات بالنسبة للمواطن الأمريكي بناء على ترخيص من الكونجرس وبعد ثمانية أشهر امتنع الكونجرس الأمريكي عن تمويل تلك الإدارة= =مع استثناء وحيد وهو إعداد وتكتل وتجميع أدوات المراقبة للأشخاص الإجانب في إطار مكافحة الإرهاب.

(٣٤٠٧) Protection of freedoms Act ٢٠١٢ chapter ٩ united kingdom p. ١٨ clause ٢٤

وتجدر الإشارة إلى أن الحماية القانونية للأمن المعلوماتي في فرنسا - وفقًا للفصل الثاني من قانون (١٧-٧٨) والمعدل وفقًا للتعديلات بموجب القانون رقم (٨٠١ – ٢٠٠٤) الصادر في ٦ أغسطس عام ٢٠٠٤ (Loi n° ٢٠٠٤ – ٨٠١ du ٦ aout ٢٠٠٤)قد نصت على شروط معينة لضمان مشروعية جمع ومعالجة البيانات الشخصية، وهي كما يلي:

١) عدالة ومشروعية طريقة جمع ومعالجة البيانات الشخصية.

٢) وضوح وتحديد أهداف وأغراض جمع المعلومات، وأن يكون هناك توافق بين طريقة جمع المعلومات وغرض جمعها.

٣) أن تكون طريقة جمع المعلومات كافية ومناسبة وذات صلة بالقياس للغرض الذي تم من أجله جمعها ومعالجتها. (٣٤٠٨)

ويذهب بعضهم إلى أن قانون المعلوماتية الفرنسي قد حظر جمع بيانات محددة أو معالجتها وهي ما تعرف بالبيانات الحساسة للأفراد كمثال بيانات الأصل العرقي أو الإثنى أو الآراء السياسية أو الفلسفية أو المعتقدات الدينية أو المتعلقة بالصحة. (٣٤٠٩)، وفى اعتقادنا أن تلك البيانات لا تعد حماية للأمن المعلوماتي الشخصي فحسب بل حماية للأمن المعلوماتي القومي أيضًا .

"After section ٦٣ AA of the police and criminal Evidence Act ١٩٨٤ (for which see section ٢٣) insert –

٦٣ A B National DNA Data base strategy Board.

١) The secretary of state must make arrangements for national DNA Date base strategy Board to oversee the operation of National DNA Data base. =

= ٢) The National DNA Database strategy Board must issue guidance about the destruction of DNA profiles which are, or may be, retained under this part of this act.

٣) A chief officer of police force in England and wales must act in accordance with guidance issued under subsection (٢).

٤) The National DNA Database strategy Board may issue guidance about the circumstances. In which applications may be made to the commissioner of the Retention and use of Biometric Material

٥) .....

(٣٤٠٨) د/ وليد السيد سليم، المرجع السابق ص٥٨٨ وما بعدها.

(٣٤٠٩) ورد ذلك الحظر بالمادة رقم (٨) من قانون المعلوماتية الفرنسي.

أما فيما يخص معالجة البيانات نجدها فى المادة (٩) من الفصل ذاته، وذلك من خلال إمكانية معالجة البيانات المتعلقة بالجرائم والعقوبات والإجراءات الأمنية، حيث تعالج بيانات الجرائم أو الأحكام الجنائية أو الإجراءات الأمنية فقط تحت رقابة السلطة الإدارية[٣٤١٠].

المبحث الرابع

في

دور الشراكة المعلوماتية في تطوير أساليب الضبط الاداري

تعد الشراكة المعلوماتية بين القطاعين العام والخاص أحد أهم وسائل تعزيز الأمن المعلوماتي، فضلاً عن ضرورة التعاون الدولي لتوفير الحلول.[٣٤١١]

فالتقنيات المستعملة في الاختراقات المعلوماتية لا بد أن تواجه بطرق جديدة للتعامل لإدارة تلك الاختراقات من خلال وجود قواعد معلوماتية واستخباراتية تحدد نوع التهديدات فضلاً عن التنسيق بين العديد من القطاعات على مستوى التشريع القانوني والرقابي.[٣٤١٢]

ومن أهم المنظمات التي تولت الاهتمام بالأمن المعلوماتي دوليًا الاتحاد الأوروبي، وحلف الناتو الذى اعتمد في ذلك على الشراكات بين مختلف الأجهزة الحكومية وغير الحكومية ومن الدول الرائدة في ذلك الولايات المتحدة الأمريكية، وألمانيا، وأستونيا[٣٤١٣].

ويرى الفقه المقارن أن هدف نظم الشراكة بين القطاعين العام والخاص في مجال الأمن المعلوماتي يرمى إلى وجود تدابير وقائية وبرامج أمن معلوماتي تقلل المخاطر المعلوماتية[٣٤١٤].

(٣٤١٠) Article g– loi n° ٧٨–١٧ du ٦ Janvier ١٩٧٩. Relative a Informatique, aux fichiers et aux libertes.

(٣٤١١) تطرف المؤتمر السنوي الثالث لأمن المعلومات المنعقد في نوفمبر ٢٠١٦ إلى ذلك وأعرب الرئيس السابق لاسكوتلانديارد "اللورد ستيفنز" إلى أن جميع القطاعات أصبحت معنية بتأمين معطياتها وبياناتها حيث عمد بعض القراصنة إلى الاستحواذ على بيانات وملفات اللاعبين المشاركين في الأولمبياد.

(٣٤١٢) من أمثلة قطاعات البنية التحتية المعلوماتية القطاعات المالية والطاقة والرعاية الصحية والاتصالات والاستخبارات ووزارة الداخلية... الخ.

(١) Cezar PETA: cyber security – current topic of National security Public security studies, volume II, Issue ٣ (٧) / ٢٠١٣, p. ٦٧ "cyber security is challenge that must be tackled through cooperation between various national actors, and institutions, private companies and non–governmental organizations, and international level through cooperation among states, regional and global organizations.

فى اعتقادنا أن الاتفاقيات الدولية ومذكرات التفاهم أحد أنجع الوسائل لتبادل الخبرات ، ومثال ذلك ما نادى به البعض من عقد اتفاقيات دولية رقمية كمثال دعوة شركة MICROSOFT الى عقد "اتفاقية جنيف الرقمية" التى تتطلب من الحكومات الإبلاغ عن ثغرات الأجهزة الحاسوبية للبائعين بدلا من تخزينها أو بيعها أو استغلالها.

ويـر الـبعض أن الاحتمـال الأبـرز بالنسـبة للأمـن المعلومـاتي سـيكون بلجـوء جهـات الإدارة علـى المستوى العالمي لتأسيس شبكات محلية أو إقليمية، والاستغناء عن الشبكة الموحدة للإنترنـت، وذلك كـي يتم الحد من تدفق البيانات والمعلومات، ولكن يعيب ذلك التدبير الاحترازي الإدارى أنـه يطغـى علـى عدة أمـور **أولـها:** حرية تداول المعلومات، **وثانيها:** إزدياد قدرة الحكومات علـى مراقبـة مـا يُنشـر علـى الشبكة، لصـغر حجمها، **وثالثها:** ارتفاع تكلفة البنية التحتية لإنشاء هذه الشبكات، بسبب تكرار بنائها في كل دولـة أو إقليم.(٣٤١٥)

وفـى اعتقادنـا أنـه لـن تفلـح جهـود تعزيـز الأمـن المعلومـاتي سـوى بتوحيـد الجهـود الدوليـة قانونيـا واحترازيا وقضائيا وذلك لوجود فقدان في المركزية الأمنية المعلوماتية ، وعدم وجود آليات ضبطية إداريـة على المستوى الدولى تستطيع السيطرة والتحكم.

يؤيدنا فى ذلك اختلاف القوانين الوطنية المنظمة لحماية حق من حقوق الإنسان مثلاً عن القوانين المنظمة لتعزيز الأمن المعلوماتي.(٣٤١٦)

أمـا الفقـه المقـارن فهـو يفضـل الأسـاليب العمليـة فـي تحقيـق الأمـن المعلومـاتي، وذلـك عـن طريـق التعاون الدولي قانونيًا وقضائيًا كالاتفاق في مجال الاختصاص القضائي، والقانون الواجب التطبيق في بيئـة منازعات الإنترنت، أما الوسائل الافتراضية فلن تفيد، ومثالها: دعوات إنشاء حكومـة الإنترنـت أو بـوليس

(٣٤١٤) Ibid, p. ٧٠

"Dan Tofan, Technical director of CERT – RO stated that, there are situations in which the entity can not manage incident alone,= =and in this case the cooperation between both entities becomes very important".

من وحدات الإدارة المعنية بالأمن المعلوماتي على سبيل المثال: وزارة العدل، ووزارة الداخلية، ووزارة نظم المعلومات، والمخابرات بأنواعها

(٣٤١٥) مجلة حالة العالم، المرجع السابق ص١٧، ١٨ نقلاً عن تقرير "جايسون هيلي" مدير مبادرة "cyber state craft initiative" بمركز (Atlantic council).

من أمثلة ذلك: اتجاه بعض الدول إلى إنشاء ما يسمى (حائط النار) "fire wall" لحماية الشبكات الوطنية والتحكم في تدفق المعلومات والبيانات منها وإليها، ومثال تلك الدول: الصين، وروسيا، وقد تدفع الجهود المبذولة لتقنين الإنترنت تحت إشراف الاتحاد الدولي للاتصالات التابع للأمم المتحدة إلى الدفع نحو ذلك التدبير المستحدث

(٣٤١٦) د/ أيمن عبد الله فكري، المرجع السابق ص٥٠١. "ففي النوع الأول هناك سيطرة وسيادة محلية (عناصر ضبط تشريعي، وإداري، وقضائي) وبالتالي هناك جهة تراقب وتمنع الاعتداء وتتيح التعويض وملاحقة المخالفين، أما في النوع الثاني لا توجد سلطة مركزية ولا جهة سيادية توفر الحماية القانونية"

الانترنت، أو معايير الاستخدام الموحد، أو سياسات التنظيم الذاتي للالتزامات وذلك لأن الانترنت يتصف (باللامركزية) وغياب السلطة التحكمية[٣٤١٧].

ويشكل التعاون الدولي في مجال الأمن المعلوماتي ركنًا أساسيًا لتعزيز الأمن المعلوماتي الداخلي من خلال مد رجال الضبط الإداري بالوسائل المستحدثة والاستراتيجيات الجديدة لمكافحة الإرهاب الإلكتروني بصفة خاصة، وانتهاكات الأمن المعلوماتي بصفة عامة.[٣٤١٨]

يرى الفقه المقارن أن مسألة الأمن المعلوماتي أصبحت مسألة قانونية أكثر منها مسألة تقنية لتعلقها بمجالات الخصوصية Privacy وأمن المعلومات Data security، فلا بد أن تعد المنظمات حزمة القوانين المنظمة للأمن المعلوماتي، وأن يكون للقانونيين دور في تصميم الإجراءات والتدريب وتقديرات المخاطر[٣٤١٩].

علاوة على ماسبق يمكن الاستفادة من خبرات القطاع الخاص في مجال الأمن السيبري، كمثال إطار "NIST" (المعهد الوطني للمعايير والتكنولوجيا)، وذلك لحماية البنية الأساسية الحيوية المحلية Domestic critical Infrastructure وذلك في الولايات المتحدة الأمريكية[٣٤٢٠].

وبالمثل نجد أن الحكومة الألمانية قد اعتمدت كذلك استراتيجية أمنية معلوماتية قائمة على الشراكة بين القطاعين العام والخاص[٣٤٢١].

(٣٤١٧) Sieber Urlich, computer crimes and other crimes related to information technology. I.R.P.. ١٩٩٤. Vol. ٦٢ p. ١٠٣٣ seq..

نقلاً عن المرجع السابق ص٥٠١.

(٣٤١٨) شارك ٧٠٠ خبير أمني أوروبي في تدريبات أمنية على حدوث هجوم افتراضي واسع على الفضاء الإلكتروني كجزء من مشروع دفاعي أوروبي عن الأمن الإلكتروني يحمل اسم "cyper Europe٢٠١٦" ، ويضم المشروع التدريب على العديد من= =السيناريوهات المظلمة لبعض صور الإرهاب الإلكتروني، وتشمل قطع الكهرباء والسيطرة على أنظمة الملاحة الجوية، واستغلال ذلك في تعطيل الطائرات، وطلب الضريبة، وذلك بحسب صحيفة ديلي ميل البريطانية في الفترة من أبريل ٢٠١٦ وحتى ديسمبر ٢٠١٦، نقلاً عن صحيفة الوطن في العدد ٧٧٨٠ السنة ٢٢ بتاريخ السبت ٢١ ديسمبر ٢٠١٦.

(٣٤١٩) The Emergence of cyber security law, prepared for the Indiana university Maurer school of law by Hanover Research, February, ٢٠١٥. oP.cit,٣

"Lawyers must play a role in designing the procedures, training and risk assessments required to implement managerial operational and technical controls needed to protect data".

(٣٤٢٠) Scott J. Shackelford, JD, PhiD, scott Russell, JD & Andreas juehn, Defining cybersecurity Due Diligence under International law: lessons from the private sector. ١٥.

Electronic copy available at: http://ssrn.com/abstract =٢٥٩٤٣٢٣

ويرى الفقه المقارن إمكانية لجوء جهة الإدارة إلى إجراء برامج لتطوير برامج حيازة البيانات من خلال تقنيات أكثر سرعة وبشكل قابل لتحمل التكلفة، وتسمح تلك التقنيات لجهة الإدارة بالتحرك فى الفترة ما بعد الجريمة بالبحث عن بيانات الأفراد موضوعي البحث عن البيانات.(٣٤٢٢)

مؤدى ما سبق يجوز الاستعانة بالقطاع الخاص في حماية الأمن المعلوماتي من خلال توفير أعلى حماية تقنية لجهة الإدارة، بل ويمكن تصنيف المعلومات وفقًا لتلك الاستعانة بحسب درجة سريتها، ويمكن لجهة الإدارة دراسة كل حالة على حدة للقيام بعملية التصنيف(٣٤٢٣).

لذا يؤكد الفقه المقارن على أن الولايات المتحدة الأمريكية في مجال تعزيز الأمن المعلوماتي تستعين بالقطاع الخاص واستثماراته في الوقاية ووضع تدابير احترازية للأمن المعلوماتى، وتستعين بالقطاع العام واستثماراته في العلاج وتلافى آثار الإنتهاكات المعلوماتية(٣٤٢٤).

(٣٤٢١) Ibid, p. ١٧

"Germany's cyber securities due diligence efforts rely on close collaboration between the public and private sectors, nationally and globally (German federal Ministry of the Interior, ٢٠١١).

"Multi – level protection (MLPS)أما الصين فقد أصدرت تشريعات لحماية أمن المعلومات، والتي يرمز لها بالمختصر schem".وذلك في عام ٢٠٠٧ وذلك بغرض حماية أمنها المعلوماتي القومي

(٣٤٢٢) See: task force on national security in the information Age, Markle found creating AA Trasted Network for Homeland security (٢٠٠٣): Task force on National security in the information age, Markle found, Mobilizing information to prevent terrorism (٢٠٠٦); protecting America's freedom in the information age.

ساهمت تلك التقنيات خاصة بعد الهجمات الإرهابية في ١١ سبتمبر، حيث كشفت جهة الإدارة فى الولايات المتحدة الأمريكية بيانات هائلة حول الأفراد مستمدة من القطاع الخاص، وبذلك يكون الكونجرس قد أخفق في الموازنة بين الخصوصية privacy والأمن القومي National security

For more – the Cantigny principles on technology terrorism, and privacy, National security law Report, feb. ٢٠٠٥, at ١٤. =

= "The Cantigny" conference on counter terrorism technology and privacy organized by the standing committee on law and Nation security of the American Bar Association".

(٣٤٢٣) Abraham, op. cit., p. ٧٦

فى اعتقادنا أن البنية الأساسية الحيوية هى الأولى بوضع التدابير الإحترازية لذا سعت الولايات المتحدة إلى "حماية البنية الأساسية الحيوية" "critical infrastructure" والتي تعني بالأساس حماية النظم "system" والأصول "assets" والتي لها تاثير على الأمن بصفة عامة، والأمن الاقتصادي القومي، والصحة العامة والسلامة العامة أو كل ما سبق(٣٤٢٥).

ويساير ماسبق ما يميل إليه الفقه الأمريكي من تعزيز الأمن المعلوماتي بصورة شاملة في كل من القطاعين العام والخاص، ولكن لابد من الأخذ فى الاعتبار أن المؤسسات العامة وشركات الطاقة أقل في القدرة الوقائية في مجال الأمن المعلوماتي من الشركات التجارية التنافسية(٣٤٢٦).

علاوة على ماسبق يمكن تحديد سبل حماية الأمن المعلوماتي في الولايات المتحدة من خلال حماية الأمن المعلوماتي للبنية الأساسية الحيوية عن طريق وصف الموقف الأمني السيبراني لجهة الإدارة ،وتحديد وترتيب أولويات فرص التحسين في إطار عملية مستمرة ومتكررة،والتواصل بين الجهات المعنية بالأمن السيبراني في داخل الدولة وخارجها حول مخاطر الأمن السيبراني(٣٤٢٧).

فى اعتقادنا أن جهة الإدارة لا بد أن تأخذ فى اعتبارها عند إبرام عقودها-خاصة فى عقود نقل التكولوجيا- ما يحميها من نصوص تعاقدية وتدابير احترازية، حيث إن من أهم مجالات حماية البيانات عند تعاقد جهة الإدارة مع شركة تقوم باستبدال تقنية معينة لديها أو معالجة قواعد البيانات لديها أن تتخذ جهة

(٣٤٢٤) Nathan Alexander sales: Regulating cyper security – Northwestern university law Review ٢٠١٣ vol., ١٠٧, No ٤, p. ١٥٠٦ "According to Brace smith, the united states follows a "bifurcated approach to network security prevention and public investment in prosecution".

(٣٤٢٥) Todd A. Brown, legal propriety of protecting Defense Industrial Base Information Infrastructure GAA.F.L.Rev. ٢٠١١, ٢٢٠ (٢٠٠٩)p.٢٢٢

(٣٤٢٦) Bruce P. smith, Hacking, Poaching, and counterattacking: Digital counterstrikes and the contours of self–Help, I J.L Econ, & Pol'Y ١٧١, ١٧٣ (٢٠٠٥),p.٣٢

(٣٤٢٧) Hanover Research, op. cit., p. ١٦

ويمكن الاستعانة في ذلك بإطار (NIST) المعهد الوطني للمعايير والتكنولوجيا الذي يقوم على تحسين الأمن السيبراني للبنية التحتية الحيوية، وذلك الإطار لا يعد تشريعا أو نموذجًا رسميًا.

"Critical infrastructure, the core of the NIST framework's focus, is defined as "systems and assests whether physical or virtual, so= =vital to the united states that the incapacity or destraction of such systems and assets".

For more see: Lynch, S. "Experts urge U.S. caution on additional cyber threat Disclosures "Chicago tribune, March ٢٦, ٢٠١٤.

الإدارة التدابير الاحترازية في مجال التعاقد بإدراج التزام عقدي على تلك الشركات كي تحمي البيانات الحكومية من الدخول لغير المرخص، ويجب على جهة الإدارة من خلال العاملين لديها أن تتخذ إجراءات الحماية اللازمة عند تزويد تابعي الطرف الثاني تعويضات وكلمات المرور للدخول إلى نظمها وبياناتها.(٣٤٢٨)

والجدير بالذكر أن جهة الإدارة-خاصة فى حالة نقص مواردها المالية أو عدم خبرتها بأطر الضبطين التشريعى والإدارى للأمن المعلوماتى- بين خيارين ليسا من السهولة بمكان،حيث يتمثل الخيار الأول فى تعزيز أمنها المعلوماتى ، ويتمثل الخيار الثانى فى شراء التكنولوجيا الأجنبية لتعزيز الأمن المعلوماتى.(٣٤٢٩)

لذا يرى البعض أن التشفير يعد وسيلة مهمة لحماية الإدارة من المخاطر المعلوماتية خاصة في حالة تداول البيانات والمعلومات بين جهات إدارة مختلفة في صورة قرارات أو أوامر أو تعاقدات إدارية.(٣٤٣٠)

قد يكون التشفير حلاً مؤقتا عن طريق تأمين الشبكات المعلوماتية لجهة الإدارة كتغيير طريقة التشفير والمراجعة الدورية لأساليب الحماية ، ويمكننا الإضافة إلى ذلك بمراعاة حصر الاختصاصات للموظفين الذين يتعاملون مع البيانات و المعلومات الحكومية وغيرها.(٣٤٣١)

(٣٤٢٨) ويرتبط بذلك وجوب نقل المعرفة لموظفي جهة الإدارة لإحداث تغييرات في واجهة المستخدم عند التحديث الفني، وترحيل قاعدة البيانات.

(٣٤٢٩) Scott J. shackelford & others, op. cit., p. ٢٢

وفي اعتقادنا أن ذلك يتوجب أن تمتلك الدولة إمكانيات اقتصادية هائلة في مجال تكنولوجيا المعلومات والأمن المعلوماتي، علاوة على توفر الكوادر المدربة والمؤهلة لذلك ،لذا من المبادئ الدولية في حماية الأمن المعلوماتي، والتي تلجأ لها بعض = =الدول مبدأ استبعاد تكنولوجيا الأمن المملوكة للأجانب، وعلى سبيل المثال: الصين، وهي في ذلك تخالف السياسة الأمريكية، والألمانية في حماية وتعزيز الأمن المعلوماتي.

For more: see Amanda N. Craigetal. proactive cybersecurity: A comparative Industry and Regulatory Analysis, – AM. Bus L. J. (forth coming) ٢٠١٥.

وتجدر الاشارة كذلك الى أنه يجب على جهة الادارة أن توازن بين رغبتها فى الحفاظ على عيوب البرمجيات السرية- من أجل اجراء التجسس والحرب الإلكترونية- وبين تقاسم تلك العيوب مع شركات التكنولوجيا لضمان الأمن المعلوماتى،فقد توصل القراصنة الإلكترونيين إلى "فيروس الفدية" الذى انتشر مؤخرا من خلال استغلال الثغرات الصفرية الموجودة فى برامج تشغيل ويندوز للتجسس على الأفراد والحكومات والتى طورتها وكالة الأمن القومى الأمريكية.

(٣٤٣٠) د/ بشير على باز: دور الحكومة الالكترونية في صناعة القرار الإداري والتصويت الإلكتروني، مجلة روح القانون، كلية الحقوق جامعة طنطا ٢٠٠٧ ص٣٥، ٣٦.

(٣٤٣١) د/ عماد يوسف حب الله، المرجع السابق ص٢٧ "على سبيل المثال حماية التطبيقات المهمة عبر استخدام بنى تحتية مزدوجة ذات طبقات حماية متعددة تضمن ألا يحقق الدخلاء أهدافهم من خلال اختراق وإسقاط نظم المعلومات ،وكذلك تعزيز البنى التحتية المعلوماتية باعتماد كلمات سر صعبة الاختراق، وأنظمة حماية متعددة الطبقات،= =ومنهجية النسخ المتطابقة Mirroring ،والأرشيف الاحتياطي

وعامة تشكل العناصر الفنية المعروفة في مجال الأمن المعلوماتي كمثال اختبارات الاختراقات العادية، وبناء شبكة موازية Parallel network construction أحد أهم عناصر تعزيز الأمن المعلوماتي لجهة الإدارة إلى جانب العناية الواجبة "Due Diligence". [٣٤٣٢]

علاوة على ماسبق تشكل التجربة اليابانية في مجال الأمن المعلوماتي أنموذجا للشراكة المعلوماتية إذ نجد أن المجتمع الياباني قد انتقل من الحالة الورقية إلى الحالة الرقمية.[٣٤٣٣]

من هنا لم يكن لجهة الإدارة في اليابان أن تتكل على مجهودات فردية للقيام بالتأمين لذا عمدت إلى بناء جسرين: الأمن المعلوماتي، والأمن القومي،

بل تحقيق الشراكة بين القطاع الحكومي والخاص لتعزيز الأمن المعلوماتي.[٣٤٣٤]

وتجدر الإشارة الى أن المجلس القومي لليابان لسياسات أمن المعلومات يعد من وحدات الضبط الإداري المهمة حيث تم إنشاؤه من خلال توصيات اللجنة التي شكلت لدراسة مشكلات قطاع تكنولوجيا المعلومات والاتصالات في مايو ٢٠٠٥

وفي اعتقادنا أن ذلك المركز من الأهمية بمكان لقيام نظام عمله على الاتصال بالمؤسسات الحكومية ووحدات جهة الإدارة اليابانية هذا من ناحية، ومن ناحية أخرى وجود ثلاثة مستويات للعمل في ذلك المركز، وبالنظر لمهام المركز نجد أنها تتحدد في نشر الإجراءات الشاملة لسياسات الأمن المعلوماتي عن طريق دعم الجهاز الإداري عند وقوع مخاطر تهدد الأمن المعلوماتي علاوة على تقوية الأمن المعلوماتي في كل المرافق والبنية الأساسية الحيوية بالدولة. [٣٤٣٥]

للبيانات، وحماية شبكة المعلوماتية في الشركات والمؤسسات التجارية، والاعتماد على مواقع تكون بمثابة نسخة مطابقة للأصل خارج أراضي الدولة عند وجود بيانات عالية السرية"

"ساعد ذلك جورجيا على تخطي الاختراق الروسي لبواباتها الإلكترونية حيث تم استعمال بوابات بديلة مطابقة للبوابات الأصلية تقع في الأراضي الأمريكية."

([٣٤٣٢]) Ibid, p. ٢٤

(٣٤٣٣) إذ يتعامل ما يقرب من ثلاثة أرباع الشعب الياباني في محتوى رقمي معلوماتي بالكامل ومع تلك الزيادة المطردة في الاعتماد على القضاء المعلوماتي زادت مخاطر الأمن المعلوماتي ،فالغالبية الساحقة من الشركات والمؤسسات اليابانية تنفذ بشدة إجراءات الأمن المعلوماتي، لكن ثلث تلك الشركات والمؤسسات هو فقط من يطبق سياسة الأمن المعلوماتي الشاملة حيث وجد أن الإجراءات الخاصة بمقاومة الفيروسات منفذة في ٩٩.٨ من الشركات والمؤسسات أما إجراءات منع الوصول غير المشروع منفذة في ٨٨.٨% من تلك الشركات والمؤسسات، أما ٣٦.٦% فقط من المؤسسات تنفذ السياسات الأمنية الشاملة.

(٣٤٣٤) تخطو اليابان خطوات محسوبة في مجال الأمن المعلوماتي بدءًا من عام ٢٠٠٠، حيث كانت الخطة التي سارت في مسارين أولهما تعزيز الأمن المعلوماتي في القطاع الإداري وثانيهما تعزيز الأمن المعلوماتي في البيئة القومية الحيوية ثم عام ٢٠٠١ صدرت خطة عمل لمواجهة الإرهاب الإلكتروني الذي يستهدف البيئة الأساسية الحيوية للدولة، ثم في عام ٢٠٠٢ بدأت الشراكة بين القطاع الخاص والحكومي فيما يتعلق بتعزيز الأمن المعلوماتي، وفي عام ٢٠٠٣ تم تنفيذ اختبارات لقياس مدى المخاطر التي يتعرض له الجهاز الإداري للدولة.

(٣٤٣٥) جمال غيطاس – المرجع السابق ص٢٥٩.

" يختص ذلك المجلس بما يلي:

وتميز التجربة اليابانية في مجال الأمن المعلوماتي بالعديد من المميزات الذي يجعلها خير معين لتبني تجارب مماثلة، وذلك كالتالي:-

١) إنشاء نموذج جديد للشراكة بين القطاع الإداري والقطاع الخاص عن طريق هجر حل المشكلات الآنية والتوجه لإنشاء بنية تتميز بالاستغلال الأمثل لتكنولوجيا المعلومات ،علاوة على إشراك شركات ذات صلة بالأمن المعلوماتي تكون مسئولة عن حدوث أي تغيرات في خدماتها ولا تهدف إلى الربح.

٢) إيجاد توازن بين الملاءمة والأمن إذ يمكن لمستخدمي التكنولوجيا استمرار استغلالها مع الشعور الفعلي بالأمن والسلامة.

٣) توازي الجهود الإدارية والتشريعية مع المبادئ العامة والسلوكية من خلال تكوين عرف عام بين الأفراد، كمثال التزام الموظف العام بعدم إفشاء أسرار وظيفية. (٣٤٣٦)

- تطوير الاستراتيجية الأساسية ما بين خطة طويلة الأجل وأخرى متوسطة الأجل وثالثة سنوية).
- التقييم المسبق والتقييم بأثر رجعي لسياسة الأمن المعلوماتي.=
- = قياس الاستجابة لما يطرأ من حوادث معلوماتية.
- تطوير إرشادات لسلامة الأمن المعلوماتي.
- تقييم سياسات الأمن المعلوماتي لكل وزارة واختيار أفضلها.

علاوة على ما سبق تم إنشاء المركز القومي لأمن المعلومات كجهة تنفيذية يرأسه نائب رئيس الوزراء ومعه مدير عام مناوب ومستشار في أمن المعلومات وحوالي ٦٠ موظفًا متخصصًا ، ويمكن نقل بعض تجارب ذلك المركز للاستفادة بعمل المجلس السيبراني المصري. "

ويولى اليابانيون اهتمامًا خاصًا بمرافق الدولة الحيوية وأمنها المعلوماتي إذ ينسق المركز مع وزارات المواصلات والبنى الأساسية والاقتصاد والتجارة والصناعة والقطاع المالي ومرافق الطاقة وشبكات نقل وتوزيع الكهرباء والمنشآت البترولية والسكك الحديدية والنقل الجوي وشبكات المياه والصرف الزراعي والصحي.

"وينقسم ذلك المركز إلى المستويات التالية:-

١) المستوى الأعلى: وهو القيادة الاستراتيجية لتكنولوجيا المعلومات والاتصالات برئاسة رئيس الوزراء وعضوية كل الوزراء، بالإضافة إلى خبراء من القطاع الخاص.

٢) المستوى الثاني: ونجد بذلك المستوى المجلس القومي لسياسات أمن المعلومات إذ ينسق مع مجلس الوزراء."

٣) المستوى الثالث: تمثله إدارة ووحدات أمن المعلومات بالوزارات والمؤسسات والوكالات الحكومية وغير الحكومية التي تتعامل مباشرة مع المركز القومي لأمن المعلومات، وفي اعتقادنا يمكن الاستفادة من تلك المستويات المتدرجة على صعيد اللجان الحكومية الخاصة بالأمن المعلوماتي وتعزيزه

(٣٤٣٦) نصت المادة ٨٦ من الدستور المصري على أن "الحفاظ على الأمن القومي واجب، والتزام الكافة بمراعاته مسئولية وطنية يكفلها القانون...".

٤) تفعيل الشراكة بين الحكومة المركزية والوحدات الإدارية اللامركزية، حيث تتولى الحكومة المركزية في اليابان سياسات الأمن المعلوماتي ، ثم يأتي دور الوحدات اللامركزية التي تنفذ تلك السياسات والخطط المركزية، وبذلك يتم القضاء على الإشكاليات البيروقراطية الفرعية وغير الإستراتيجية.(٣٤٣٧)

وهذا ما تبناه الدستور المصري في المادة رقم ١٧٦ التي نصت على أن "تكفل الدولة دعم اللامركزية الإدارية والمالية والاقتصادية...".

٥) تقسيم المخاطرالتي تهدد الأمن المعلوماتي إلى معلومات الحكومة المركزية ،ومعلومات الوحدات اللامركزية التى تقسم بدورها إلى معلومات عالية السرية ومعلومات شخصية ومعلومات حول الشركات وذلك كالتالي:-

أ) المحتوى المعلوماتي للبنى الأساسية الحيوية: حيث لا بد أن تكون على درجة عالية جدًا من التأمين المعلوماتي لضمان سير المرافق العامة بإنتظام واطراد.

ب) المحتوى المعلوماتي للشركات: حيث لا بد أن تكون على درجة عالية من التأمين المعلوماتي باعتبار تلك الشركات والهيئات توفر المنتجات والخدمات الداعمة للبنية الأساسية لتكنولوجيا المعلومات.

ج) المحتوى المعلوماتي للأفراد: ويعد ذلك المحتوى هو الحلقة الأضعف في مجال أمن الفضاء المعلوماتي.

المبحث الخامس

في

دور تنظيم الطيف الترددي فى تحقيق الأمن المعلوماتي

يعد تنظيم الطيف الترددى من أدوات الضبط الإدارى لتعزيز الأمن المعلوماتى ،ولأهميته وباعتباره أحد الموارد الطبيعية نظمه القانون رقم ١٠ لسنة ٢٠٠٣ بشأن تنظيم الاتصالات ،والذى عرفته المادة الأولى من ذلك القانون بأنه : هو حيز الموجات التى يمكن استخدامها فى الاتصال اللاسلكي طبقاً لإصدارات الاتحاد الدولى للاتصالات، وأفادت المادة ٤٩ من القانون بكون ذلك الطيف موردا طبيعيا محدودا، وبكون الجهاز القومى لتنظيم الاتصالات هو الجهة المسئولة عن تنظيم وإدارة جميع الشئون المتعلقة باستخدامه طبقاً لأحكام هذا القانون.

وتجدر الإشارة إلى التفرقة بين ثلاثة أنواع من الأسرار داخل نطاق العمل الحكومي وهي الأسرار الإدارية، والأسرار الحكومية الخاصة بالمستندات وغيرها، وأسرار الأشخاص داخل العمل وفي اعتقادنا أن الأمن المعلوماتي لجهة الإدارة ينطبق بدرجة أكبر على النوعين الأول والثاني.

(٣٤٣٧) قد تكون التجربة اليابانية في الأمن المعلوماتي هي الأنسب لمصر لحداثة تطبيقها، حيث بدأت عام ٢٠٠١ تقريبًا كما أنها من حيث الحجم والتنوع ليست ضخمة= =كالولايات المتحدة ولكن هناك فارق ضخم ومستوى التعليم والقدرة على إنتاج واستيعاب أدوات ومنهجيات وطرق الأمن المعلوماتي.

ووفقا لحكم المادة (٤٤) من دستور الاتحاد الدولي للاتصالات وإصداراته يمكن تعريف الطيف الترددي بوصفه حيز الموجات التي يمكن استخدامها في الاتصال اللاسلكي طبقاً لتوفير خدمات الاتصالات أياً كانت الوسيلة المستعملة .

فى اعتقادنا أن التنظيم التشريعي للطيف الترددى يحتاج لتنظيم تشريعى أكثر تفصيلا وحداثة ، حيث نصت المادة ٦٦ من القانون سالف الذكر على مشاركة الجهاز القومى لتنظيم الاتصالات بالاتفاق مع القوات المسلحة وأجهزة الأمن القومي فى وضع خطة استخدام الطيف الترددي أو خطة استخدام الترقيم القومي وعند مراجعتهما أو تعديلهما.

وتنص المادة ٥٠ على أن يتولى الجهاز – وبمراعاة إصدارات الاتحاد الدولى للاتصالات – وضع خطة الطيف الترددى بما يحقق أفضل استخدام له، وتعظيم العائد من استخدامه وإتاحة إدخال خدمات الاتصالات اللاسلكية الحديثة ، وعرض هذه الخطة على لجنة تنظيم الترددات لمباشرة اختصاصها طبقاً لأحكام هذا القانون ،وتنص المادة ١٣ على اختصاص مجلس إدارة الجهاز بشئونه وتصريف أموره ، ويختص باعتماد خطة استخدام الطيف الترددى ومراجعتها وتعديلها كلما دعت الضرورة،وذلك بمراعاة قرارات وتوصيات الاتحاد الدولى للاتصالات،علاوة على وضع قواعد وشروط منح التراخيص الخاصة باستخدام الطيف الترددى وتنظيم إجراءات منحه.

ومنهم من يرى أن تعزيز الأمن المعلوماتى اعتمد طويلا على النصوص التقليدية العامة غير المواكبة للتطور كمثال المادة ١٧١ من قانون العقوبات التي توضح الوسائل المختلفة للنشر والإذاعة، وقد جاءت تلك المادة بصورة عامة لتشمل كافة الطرق والوسائل التي تتحول بها المعلومات من الحيازة الفردية إلى الحيازة الجماعية ابتداء من القول والوسائل التقليدية مرورًا بالوسائل الميكانيكية، وانتهاء بالوسائل السلكية واللاسلكية وما قد يستجد في المستقبل.[٣٤٣٨]

أضف إلى ذلك أنه حتى بعد تطور وسائل نقل المعلومات تدخل المشرع المصرى لحماية الأمن المعلوماتي بموجب قرار رئيس الجمهورية رقم ١٥١ لسنة ١٩٩٨ بشأن إنشاء جهاز تنظيم الاتصالات السلكية واللاسلكية والذي يهدف على وجه الخصوص إلى عدة أمور منها (حماية أهداف ومصالح الأمن القومي والحقوق السيادية للدولة).[٣٤٣٩]

ورغم القيود الواردة في ذلك القانون لم يتضمن أية عقوبات لتحقيق الردع اللازم لإلزام الأفراد بالالتزام بأحكامه لذا صدر قانون الاتصالات سالف الذكر والذى انتقده بعضهم من خلال إضفاء الطابع الأمني على تشكيل مجلس إدارة الجهاز القومي دون توضيح مبررات وجود ممثلين لأجهزة الأمن القومي، ودون تحديد لماهية أجهزة الأمن القومي.[٣٤٤٠]

(٣٤٣٨)للمزيد انظر: أحمد عزت وآخرون: المرجع السابق ص٥٥.

(٣٤٣٩) قرار رئيس الجمهورية رقم ١٥١ لسنة ١٩٩٨ – نشر بالجريدة الرسمية ١٩٩٨/٤/٤.

والجدير بالذكر أن القانون غلب الأمن المعلوماتي على حرية تداول المعلومات بدليل أن تشكيل إدارة الجهاز، كما ورد في المادة الرابعة من القانون يتكون من وزير النقل والمواصلات رئيسًا وعضوية مستشار مجلس الدولة، ومدير المعهد القومي للاتصالات، ووكيل أول وزارة المواصلات، ومدير سلاح الإشارة بالقوات المسلحة، وثلاثة أعضاء يمثلون جمهور المستفيدين، وثلاثة آخرين من الخبراء في مجال الاتصالات، والدليل على تغليب الأمن المعلوماتي كثرة عدد المسئولين الحكوميين الإداريين عن عدد الخبراء المتخصصين.

(٣٤٤٠) أحمد عزت، المرجع السابق ص٥٧.

أما فيما يتعلق بأجهزة الاتصالات حظر القانون استيراد أو تصنيع أو تجميع أي معدة من معدات الاتصالات إلا بعد الحصول على تصريح بذلك من الجهاز، وطبقًا للمعايير والمواصفات المعتمدة منه، بل إن القانون ألزم جهاز تنظيم الاتصالات بضرورة الحصول على موافقة من القوات المسلحة وهيئة الأمن القومي ووزارة الداخلية قبل قيامه بالاستيراد أو التصنيع أو التجميع أو الحيازة أو الاستخدام لحسابه، وقبل منحه تصاريح بذلك لوحدات الجهاز الإداري للدولة من وزارات ومصالح وأجهزة ووحدات الإدارة المحلية والهيئات والشركات بكافة أنواعها والأفراد وغيرها.[٣٤٤١]

ويذهب بعضهم في سبيل نقده لذلك القانون بأنه تطرف في العقاب لكل من قام دون الحصول على ترخيص من الجهاز وفقًا لأحكام هذا القانون بإنشاء أو تشغيل شبكات الاتصالات، أو إنشاء بنية أساسية لشبكات الاتصالات أو تقديم خدمات الاتصالات، أو تمرير المكالمات التليفونية الدولية بأية طريقة كانت.[٣٤٤٢]

وفي اعتقادنا أن الرأي السابق جانبه الصواب حيث إن منظومة الأمن المعلوماتي تتطلب ردع خروقات الأمن المعلوماتى للدولة ككل لا مايتعلق بخروقات الأمن المعلوماتى لجهة الإدارة فقط ، وكذلك يجب كى تكتمل تلك المنظومة ألا يتم حصر تهديدات الأمن المعلوماتي في تشفير الاتصالات فقط..[٣٤٤٣]

وتجدر الإشارة إلى أن المشرع المصرى قد أخذ بمركزية الرقابة على بيانات مستخدمى ذلك الطيف من خلال تحديد المسؤولية عن تجميع وتحديث وإدارة قواعد بياناته.[٣٤٤٤]

(٣٤٤١) المرجع السابق ص٥٧.

"وذلك بالنسبة لمعدات الاتصالات التي يصدر بتحديدها قرار من وزير الدفاع بالتنسيق مع أجهزة الأمن القومي. والاستثناء على هذا القيد فقط للمعدات والأجهزة المستخدمة في البث الإذاعي والتليفزيوني الخاص بإتحاد الإذاعة والتليفزيون، مع ضرورة حصول الاتحاد على ذات الموافقة".

(٣٤٤٢) المرجع السابق ص٥٨. =

= "حيث قرر القانون مقابل تلك الافعال في المادة رقم ٧٢ عقوبة الحبس مدة لا تقل عن ستة أشهر ولا تجاوز خمس سنوات وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين"

"ويرى ذلك الرأي أن يقتصر التجريم على التشغيل والاستخدام ذات الطابع الربحي الاستثماري، بهدف حماية تكافؤ الفرص للمشغلين المستثمرين، ويتحول الاحتكار لأغراض اقتصادية". فالرأي هنا باعثه هو الباعث الاقتصادي البحت دون النظر للمعايير الأمنية المعلوماتية."

(٣٤٤٣)وتأكيدا على ذات المعنى نصت المادة ٦٤ من القانون رقم ١٠ لسنة ٢٠٠٣ على التزام مشغلي ومقدمي خدمات الاتصالات والتابعين لهم، وكذلك مستخدمي هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز والقوات المسلحة وأجهزة الأمن القومي، ولا يسري ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني.

انظر المادة (٦٤) من الباب السادس "الأمن القومي والتعبئة العامة من قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ "ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة، كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلائهم المنوط بهم تسويق= =تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة".

وما يؤيد وجهة نظرنا بضرورة وضع تنظيم قانونى أكثر شمولية وحداثة ماذهبت إليه محكمة القضاء الإداري بقولها "وحيث إن هذه الدعوى قد كشفت عن القصور التشريعي الذي شاب نصوص الباب السادس من قانون تنظيم الاتصالات الصادر بالقانون رقم ١٠ لسنة ٢٠٠٣ المنظم لموضوع (الأمن القومي والتعبئة العامة) في المواد من (٦٤) إلى (٦٩)، وهو قصور من شأن استمراره الإضرار بجذب المزيد من الاستثمارات في قطاع الاتصالات ... إذ من شأن بقاء تلك النصوص على حالها التعرض لمخاطر تكرار قطع خدمات الاتصالات وخدمات الإنترنت ، بما يؤدي إلى عزوف المستثمر على المخاطرة برأس ماله في بيئة تشريعية غير محفزة للاستثمار، ومن ثم فإن المحكمة تهيب بالمشرع أن يضع ضمن أولوياته القصوى إلغاء تلك النصوص وإعادة صياغة نصوص جديدة تحدث التوازن بين الحفاظ على الاستثمارات والحفاظ على اعتبارات الأمن ([٣٤٤٥]).

(٣٤٤٤) ودليلنا فى ذلك ما نصت عليه المادة ٥٨ من القانون رقم ١٠ لسنة ٢٠٠٣ بأن "يتولى الجهاز تجميع وإدارة وتحديث قاعدة بيانات مستخدمي الطيف الترددي، ويلتزم الجهاز بالحفاظ على سرية هذه البيانات حماية لحق المستخدمين في الخصوصية"

بل وزيادة في بسط سيطرة الجهاز على بيانات حيزات الترددات نصت المادة رقم ٥٩ من ذات القانون على "... ويلتزم جميع المستخدمين للطيف الترددي في تاريخ العمل بهذا القانون بتقديم بيانات وافية للجهاز عن حيزات الترددات التي يستخدمونها، وذلك خلال ثلاثة أشهر من هذا التاريخ. ويتولى الجهاز الترخيص لهم باستخدام التردد طبقًا للشروط التي يقررها وبما يتناسب مع احتياجاتهم الفعلية وخطة إدارة الطيف الترددي".

ودليلنا أيضا ما ورد فى المادة ٥١من القانون بأنه "لا يجوز استخدام تردد أو حيز ترددات إلا بعد الحصول على ترخيص بذلك من الجهاز، وبأن يلتزم المرخص له باستخدام تردد أو حيز ترددات طبقاً لشروط الترخيص ، وفى حالة مخالفته لهذه الشروط يكون للجهاز الحق فى إلغاء هذا الترخيص ، كما أن للجهاز بموجب المادة ٥٥ من القانون- سلطة استخدام الوسائل التى تمكنه من الكشف عن استخدامات الترددات غير المرخص بها ، والتحقق من التزام المرخص لهم بشروط الترخيص ، كما يكون له التفتيش على الأجهزة اللاسلكية المصرح بها للتحقق من مطابقتها لشروط الترخيص ."

- ومن التشريعات العربية التي عملت على تعزيز الأمن المعلوماتي من خلال الطيف الترددي ما نص عليه القانون الكويتي رقم ٣٧ لسنة ٢٠١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات في المادة ٢٦ من أن "يعتبر طيف الترددات ثروة = =وطنية تتولى الهيئة تنظيم استخدامها بموجب هذا القانون، وإعداد الجداول والمخططات والسجلات اللازمة له...".

([٣٤٤٥]) حكم محكمة القضاءالإدارى-دائرة المنازعات الاقتصادية والاستثمار-الدائرة السابعة- الدعوى رقم ٢١٨٥٥ لسنة ٦٥ قضائية بتاريخ ٢٠١١/٥/٢٨-حكم غير منشور

"وذلك بتقليص الجهات التي يطلق عليها مصطلح "الأمن القومي" ، وإعادة النظر في الالتزامات الملقاة بالمادة (٦٤) على كل مشغل أو مقدم خدمة بأن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات، والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون ، فذلك مما يمس الكثير من الحريات ويتيح لبعض الأجهزة التلصص على شبكات الاتصالات بغير سند دستوري ، وألا يكون من بين مفردات خطة تشغيل شبكات الاتصالات وفقاً للمادة (٦٥) من القانون إمكانية قطع الخدمات عن المواطنين ، وألا يُسمح لأية سلطة بالدولة أن تخضع= =لإدارتها جميع خدمات وشبكات الاتصالات المقررة بالمادة (٦٧) من القانون ، فذلك نوع ممجوج من التأميم للشبكات وحلول للسلطات المختصة محل مشغلي ومقدمي الخدمة بغير سند دستوري ، فضلاً عما في إخضاع خدمات الاتصالات وخدمات الإنترنت لإدارة (السلطات المختصة) كما ورد بالمادة ذاتها من اعتداء جسيم على حقوق الاتصالات والحق في الخصوصية ، ولن يكون حلاً للمشكلة أن يُسند قطع الاتصالات لأي سلطة كانت سواء رئيس الجمهورية، أو رئيس الوزراء، أو وزير الداخلية، أو القوات المسلحة أو غيرها، فحرية الاتصالات وتدفق المعلومات وتداولها وشفافية القرار السياسي وتحقيق العدل الاجتماعي ومكافحة الفساد خير ضمان لتحقيق الأمن القومي ، وأن يُعاد النظر في العقوبات المقررة بالمادة (٨٢) من القانون المتعلقة بمخالفة أحكام المادة (٦٧) منه ، وفي ذلك خير ضمان لجذب الاستثمار وحمايته.

وقد ثارت حماية مورد الطيف الترددى أمام محكمة القضاء الإدارى -دائرة المنازعات الاقتصادية والاستثمار – حيث أقر تقرير مفوض الدولة أن "الحق في الاتصالات هو أحد الموارد الطبيعية المملوكة لمجموع الشعب المصري التي عنيت المادة (١٢٣) من الدستور بتنظيمها "([٣٤٤٦]).

وتجدر الإشارة أن الحكم السابق قد أقام حجته فى ذلك على كون الطيف الترددى من مستلزمات الحق في الاتصال، وأن هذا الحق يعد حاجة إنسانية أساسية وأساسًا لكل مواطن يثبت الحق فيه للأفراد، كما يثبت للمجتمعات التي تتكون منهم ، وهو حق لا يقوم إلا بأدواته المحققة له ،وهو يعني حق الانتفاع والمشاركة لجميع الأفراد والجماعات والتنظيمات.

ومؤدى ما سبق يعد تنظيم الطيف الترددى عنصرا لازما لتحقيق الحق فى تداول المعلومات من ناحية ، ولتعزيز الأمن المعلوماتى من ناحية أخرى.

([٣٤٤٦]) الحكم السابق.

"ومن ثم فإن الحق في استخدام الطيف الترددي مخول لجميع المستخدمين لخدمات الاتصالات وفقاً لتعريف المادة (١) من قانون تنظيم الاتصالات، وهم جميع الأشخاص الطبيعية أو الاعتبارية الذين يستعملون خدمات الاتصالات أو يستفيدون منها ، وبالتالي يكون لكل مستخدم لخدمات الاتصالات الصفة والمصلحة الشخصية المباشرة في التنازع حول شرعية القرارات المتعلقة بتنظيم الحق في استخدام الطيف الترددي شاملاً خدمات الاتصالات ومنها عدم قطعة خدمة الاتصالات والإنترنت دون سابق إنذار وبدون مبرر بالمخالفة للقانون"

""وحيث إن (الحق في استخدام الطيف الترددي) باعتباره أحد الموارد الطبيعية التي عنيت المادة (١٢٣) من الدستور بتنظيمها ، وأكدت عليه بوصفه حقاً المواد (١/البند= =١٥) و ٤٩ من قانون تنظيم الاتصالات الصادر بالقانون رقم ١٠ لسنة ٢٠٠٣ بحسبانه هو حيز الموجات التي يمكن استخدامها في الاتصال اللاسلكي ، ومنه تقديم خدمات الاتصالات، وخدمات الرسائل النصية القصيرة، وخدمات الانترنت، إنما هو مورد طبيعي محدود ومن ثم فهو حق من الحقوق المكفولة دستورياً إذ هو بطبيعته ووفقاً لحكم المادة (٤٤) من دستور الاتحاد الدولي للاتصالات كمورد طبيعي محدود يحكمه مبدأ تقسيم الترددات وتخصيصها ، وبالتالي يخضع لفكرة الترخيص المسبق الذي يعد في مجال خدمات الاتصالات وسيلة رقابة تهدف بالدرجة الأولى إلى المحافظة على النظام العام ، ذلك أن حرية الاتصال عبر خدمات الاتصالات المتعددة تعتبر ـ وبحق ـ حجر الزاوية في الممارسة الديمقراطية مما يستوجب تنظيمها دون تقييدها أو العصف بها ، وحمايتها من عسف الإدارة وسوء استعمال القائمين عليها والممارسين لها وعدم حجب الخدمات أو قطعها أو التلصص عليها ، مع الالتزام بالقيم ومبادئ النظام العام".

التوصيات:

١-يجدر بالمشرع المصري العمل على استصدار قانون للأمن المعلوماتي يتلافى إشكاليات المعلومات بين أمنها وتداولها.

٢-نقترح أن يعمل ذلك القانون على معالجة مدى تعارض الأمن المعلوماتي مع الخصوصية وغيرها من الاشكاليات القانونية التى ورد ذكرها في هذا البحث.

٣- نقترح أن تعمل السلطات التنفيذية علي توفير متطلبات الضبط الإداري الإلكتروني من خلال تهيئة أدوات البيئة المعلوماتية الآمنة،وأولها الإدارة الالكترونية،والحكومة الالكترونية.

٤- نقترح أن تعمل السلطات التنفيذية علي تحديث الآليات المعتادة لرصد وحيازة البيانات والمعلومات ،وتهيئة أدوات حيازة البيانات الروتينية كمثال نظام الأرشفة الإلكترونية.

٥- نقترح أن تعمل الجهات الإدارية على وضع سياسة لتنظيم وحفظ المعلومات البيومترية.

٦-نقترح أن تعمل السلطات التشريعية والتنفيذية على دراسة وتنظيم دور الشراكة المعلوماتية ،والطيف الترددي في تطوير أساليب الضبط الاداري.

٧- نقترح أن تعمل الجهات الإدارية على وضع سياسة أمنية معلوماتية عامة للمواطن العادي،وسياسة أمنية معلوماتية أكثر خصوصية للموظف العام لكون الأمن المعلوماتي الحكومي الأكثر تطلبا،والأكثر حساسية.

٧- نقترح أن تعمل الجهات الإدارية على وضع ادارات أو وحدات ادارية خاصة بنظم المعلومات وأمنها بكل هيكل تنظيمي للوزرات والادارت الحكومية وغيرها .

أولا: المراجع باللغة العربية:

١ـ المؤلفات العامة:

١-المعجم الوجيز: مجمع اللغة العربية ١٩٨٠م

٢- المنجد في اللغة والأدب والعلوم، بيروت، الطبعة الأولى – المطبعة الكاثوليكية – بدون سنة نشر

٣-المصباح المنير للفيومي، دار الحديث، القاهرة، ١٤٢٤هـ/ ٢٠٠٣.

٤-د/ أحمد فتحي سرور: الحماية الدستورية للحقوق والحريات – دار الشروق، الطبعة الثانية ٢٠٠٠ .

٥-د/ سعاد الشرقاوي: القانون الإداري – الطبعة الأولى، دار النهضة العربية ١٩٨٣.

٦-د/ سليمان محمد الطماوي: الوجيز في القانون الإداري "دراسة مقارنة"– دار الفكر العربي ١٩٧٩

٧-د/ صلاح الدين فوزي: الإدارة العامة بين علم متغير ومتطلبات التحديث - دار النهضة العربية ١٩٩٨.

٨-د/ طعيمة الجرف: القانون الإداري، الطبعة الأولى، دار النهضة العربية ١٩٧٣.

٩-د/ طعيمة الجرف: القانون الإداري والمبادئ العامة في تنظيم ونشاط السلطات الإدارية- دار النهضة العربية ١٩٧٨

١٠--د/ عادل أبو الخير :الضبط الإداري وحدوده: الهيئة المصرية العامة للكتاب ١٩٩٥.

١١-د/ فاروق عبد البر: دراسات في حرية التعبير واستقلال القضاء وضمانات التقاضي، بدون دار نشر- ٢٠٠٦

١٢-د/ محمد أنس قاسم جعفر: الوسيط في القانون العام "أسس وأصول القانون الإداري" بدون سنة نشر، بدون دار نشر.

١٣-د/ محمد سعيد حسين أمين: مبادئ القانون الإداري: "دراسة في أسس التنظيم الإداري – أساليب العمل الإداري"، دار الثقافة الجامعية، ١٩٩٧.

١٤-د/ محمود عاطف البنا : الوسيط في القانون الإداري– دار الفكر العربي ١٩٨٤.

١٥-د/ ياسر محمد عبد السلام رجب : الإدارة العامة- دار النهضة العربية ٢٠١٧.

٢-المؤلفات المتخصصة

١-السيد ياسين: شبكة الحضارة المعرفية من المجتمع الواقعي إلى العالم الافتراضي - الهيئة المصرية العامة للكتاب ،سلسلة العلوم الاجتماعية ، ٢٠٠٩.

٢-أحمد عزت وآخرون: حرية الفكر والتعبير - الطبعة الثانية ٢٠١٣

٣-د/ أحمد جلال عز الدين: الإرهاب والعنف السياسي- دار الحرية، القاهرة، ١٩٨٦.

٤-أماني فهمي :دساتير العالم (المجلد السادس) دستور تركيا – ترجمة وتقديم أماني فهمي – المركز القومي للترجمة.

٥-جمال محمد غيطاس: أمن المعلومات والأمن القومي- مكتبة نهضة مصر- بدون سنة نشر.
٦-د/ حسين بن سعيد الغافري: منظومة سلطنة عمان التشريعية لمكافحة جرائم تقنية المعلومات ، دار النهضة العربية-٢٠١١
٧-د/دويب حسين صابر: النظام القانوني لحرية الحصول على المعلومات، دراسة مقارنة- دار النهضة العربية ٢٠١٤/ .٢٠١٥
٨-د/ دلال صادق الجواد، د/ حميد ناصرالفتال: أمن المعلومات - دار اليازوري العلمية للنشر والتوزيع .
٩-د/ ذياب البداينة: الأمن وحرب المعلومات، دار الشروق للنشر والتوزيع، الأردن -٢٠٠٢
١٠-سلطة الاتصال : المركز القومي للترجمة-الطبعة الأولى ٢٠١٤ - العدد ٢٠٩١
١١-د/ سامي الطوخي: الإدارة بالشفافية للتنمية والإصلاح الإداري من السرية وتدني الأداء والفساد إلى الشفافية والتسبيب وتطور الأداء البشري والمؤسسي، دار النهضة العربية، ٢٠٠٦
١٢-د/ طارق الجيار: الملاءمة الأمنية ومشروعية قرارات الضبط الإداري، منشأة المعارف - الطبعة الأولى ٢٠٠٩ .
١٣-د/ طارق إبراهيم الدسوقي عطية: "الأمن المعلوماتي" (النظام القانوني لحماية المعلومات) دار الجامعة الجديدة .٢٠٠٩
١٤-د/ عبد السلام هابس السويفان:إدارة مرفق الأمن بالوسائل الإلكترونية - دراسة تطبيقية -دار الجامعة الجديدة.
١٥-د/عبد الكريم نافع :"الأمن القومي" - مطبوعات دار الشعب - القاهرة ١٩٧٥
١٦-د/ عبد الفتاح بيومي حجازي:- نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، بدون دار نشر- الطبعة الأولى .٢٠٠٩
١٧- د/ عبد الرحمن الجيران: اختلاف المفاهيم بين الشرق والغرب - دار إيلاف الدولية للنشر والتوزيع ٢٠١٥
١٨-د/عبد الوهاب حومد: "الإجرام السياسي" - دار المعارف - القاهرة ١٩٦٣
١٩-د/ عادل صادق: استخدام الإرهاب الالكتروني في الصراع الدولي - دار الكتاب الحديث -بدون سنة نشر
٢٠-د/ ممدوح فرجاني خطاب: النظام القانوني للاستشعار من بعد من الفضاء الخارجي، دار النهضة العربية .١٩٩٣
٢١-د/ محمد عبد اللطيف عبد العال: الحظر والرقابة على النشر في القانون الجنائي المصري (دراسة مقارنة تأصيلية تحليلية) -دار النهضة العربية .١٩٩٨

٢٢-د/ محمد فهمي طلبة وآخرون : فيروسات الحاسب وأمن البيانات -١٩٩٥
٢٣-د/محمد أمين الرومي: جرائم الكمبيوتر والانترنت - دار المطبوعات الجامعية، الإسكندرية .٢٠٠٤
٢٤-د/محمد عطية راغب: التمهيد لدراسة الجريمة السياسية في التشريع الجنائي العربي المقارن - دار النهضة العربية - القاهرة - الطبعة الأولى ١٩٦٩
٢٥-د/ محمد فاضل :محاضرات الجرائم السياسية- معهد الدراسات العربية العليا، القاهرة ١٩٦٢
٢٦-د/ محمد سعيد حسين أمين: حرية الصحافة ضمان ممارستها وضوابط تنظيمها، دار النهضة العربية، ٢٠٠٥ .
٢٧-د/ محمد فوزي نويجي: الجوانب النظرية والعملية للضبط الإداري – دراسة مقارنة- دار الفكر والقانون -٢٠١٦ .
٢٨-د/ محمد محمد بدران :مضمون فكرة النظام العام ودورها في مجال الضبط الإداري- دراسة مقارنة في القانون المصري والفرنسي، دار النهضة العربية ١٩٩٢
٢٩-د/ محمد السعيد رشدي: الإنترنت والجوانب القانونية لنظم المعلومات – مؤسسة دار الكتب للطباعة والنشر والتوزيع .١٩٩٧
٣٠-د/ مصطفى محمد موسى:- المراقبة الإلكترونية عبر شبكة الإنترنت- دراسة مقارنة، دار الكتب القانونية، المحلة الكبرى، ٢٠٠٥
٣١-منير محمد الجنبيهي، ممدوح محمد الجنبيهي: أمن المعلومات الإلكترونية، دار الفكر الجامعي ٢٠٠٦
٣٢-د/ منصور محمد عقيل ود/ علي قاسم: الانترنت والأبعاد الأمنية، مركز البحوث والدراسات الشرطية، دبي، يناير ١٩٩٦
٣٣-د. نائلة محمد فريد قورة:- جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية) منشورات الحلبي الحقوقية - بدون سنة نشر
٣٤- د/ نبيل عبد الفتاح: "الوجه والقناع في الحركة الإسلامية والعنف والتطبيع" - دار سيشات للدراسات والتوزيع - الطبعة الأولى.
٣٥-د/ نبيل علي، د/ نادية حجازي: الفجوة الرقمية - رؤية عربية لمجتمع المعرفة، عالم المعرفة - الكون - أغسطس العدد (٣١٨) ٢٠٠٥
٣٦-د/ هدى محمد عبد العال: التطوير الإداري والحكومة الإلكترونية – الطبعة الأولى – دار الكتب المصرية ٢٠٠٦
٣٧-د/ هدى حامد قشقوش: جرائم الحاسب الإلكتروني في التشريع المقارن – دار النهضة العربية -القاهرة ١٩٩٢

٣٨-د/ هشام محمد فريد رستم : قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ١٩٩٢
٣٩-د/ وفاء سيد رجب محمد: مستقبل القانون الإداري، دراسة مقارنة ـ ٢٠٠٧
٤٠-د/ وليد السيد سليم:ضمانات الخصوصية في الإنترنت – دار الجامعة الجديدة ٢٠١٢

٣-الرسائل العلمية

١- أحمد سعد محمد الحسيني: الجوانب الإجرائية للجرائم الناشئة عن استخدام الشبكات الإلكترونية، رسالة دكتوراه مقدمة لكلية الحقوق جامعة عين شمس .٢٠١٢
٢-أيمن عبد الله فكري: جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة سنة ٢٠٠٦
٣-أيمن عبد الحفيظ عبد الحميد سليمان:- استراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي – رسالة دكتوراه مقدمة لأكاديمية الشرطة – كلية الدراسات العليا.
٤-بوقريط عمر، الرقابة القضائية على تدابير الضبط الإداري، رسالة ماجستير، كلية الحقوق، جامعة منثوري، الجزائر ٢٠٠٦/.٢٠٠٧
٥- حسين عبد الباقي: النظرية العامة لجريمة إفشاء الأسرار في التشريع الجنائي المقارن - رسالة دكتوراه جامعة عين شمس ١٩٧٨
٦-حيدر عبد الرحمن الحيدر :الأمن الفكري في مواجهة المؤثرات الفكرية - رسالة دكتوراه مقدمة لكلية الدراسات العليا أكاديمية الشرطة المصرية ٢٠٠١ (غير منشورة)
٧-راشد محمد المري: رسالة دكتوراه بعنوان "الجرائم الإلكترونية في ظل الفكر الجنائي المعاصر، رسالة مقدمة لكلية الحقوق جامعة القاهرة .٢٠١٣
٨-راشد محمد راشد حمداني السلحدي الشحي: الرقابة القضائية على قرارات الضبط الإداري في الحكومة الإلكترونية - دراسة تطبيقية على دولة الإمارات العربية المتحدة - رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة .٢٠١٤
٩-شيماء عبد الغني محمد عطا الله: الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة ٢٠٠٥ .
١٠-عمر محمد سلامة العليوي: حق الحصول على المعلومات في ضوء القانون الأردني رقم ٤٧ لسنة ٢٠٠٧ – دراسة مقارنة – رسالة دكتوراه مقدمة لكلية الحقوق - جامعة عين شمس سنة .٢٠١١
١١-فاطمة الزهراء عبد الفتاح إبراهيم: العلاقة بين المدونات الإلكترونية والمشاركة السياسية في مصر - رسالة ماجستير في الإعلام، جامعة القاهرة ٢٠١٠
١٢- فهد سلطان محمد أحمد بن سلطان: مواجهة جرائم الإنترنت، رسالة دكتوراه مقدمة لكلية الحقوق

جامعة القاهرة- دراسة مقارنة- ٢٠٠٤

١٣- محمد حسنين عبد العال: فكرة السبب في القرار الإداري ودعوى الإلغاء - رسالة دكتوراه مقدمة لكلية الحقوق -جامعة القاهرة ١٩٧٢

١٤-محمد أحمد عزت عبد العظيم:الجرائم المعلوماتية الماسة بالحياة الخاصة- رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١٦

١٥-محمد محمد صالح الألفي: الجرائم المضرة بأمن الدولة عبر الإنترنت- رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١١.

١٦-منى فتحي أحمد عبد الكريم: الجريمة عبر الشبكة الدولية للمعلومات- رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة٢٠١٥

١٧-ناجح أحمد عبد الوهاب: التطور الحديث للقانون الإداري في ظل نظام الحكومة الإلكترونية -رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١١

١٨-نشوى رأفت إبراهيم أحمد: حماية الحقوق والحريات الشخصية في مواجهة التقنية الحديثة "البيانات الشخصية، المراسلات والمحداثات الشخصية، الحق في الصورة) رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة ٢٠١٢.

١٩- وليد سمير فهيم المعداوي: دور الشرطة في حماية الحياة الخاصة من أخطار المعلوماتية، رسالة دكتوراه، كلية الدراسات العليا بأكاديمية الشرطة ٢٠١١.

٤-أبحاث علمية

١-د/ أحمد عبد الكريم سلامة : الانترنت والقانون الدولي الخاص - بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت - مركز الإمارات للدراسات والبحوث - من ١-٣ مايو ٢٠٠٣

٢-أورين كير:نطاق الجريمة الافتراضية (تفسير الدخول والتصريح به في إطار تشريعات الإساءة إلى الحاسوب) - بحث منشور في مجلة القانون – جامعة نيويورك – العدد ٧٨/ نوفمبر ٢٠٠٣، ترجمة د/ عمر محمد بن يونس، الأكاديمية الدولية للتجارة الدولية ٢٠٠٨

٣- د/ إمام حسنين: "جرائم التنظيمات الإرهابية" دراسة مقارنة – مجلة مركز بحوث الشرطة العدد ٢٧ يناير ٢٠٠٥.

٤- د/إياس بن سمير الهاجرى:مقال بعنوان"أمن المعلومات على شبكة الإنترنت" - منشور بمجلة جامعة نايف للعلوم الأمنية حول أعمال ندوة حقوق الملكية الفكرية المنعقدة بالجامعة سنة ٢٠٠٤

٥-الدولة والأمن دراسة بالموقع الالكترونى -مجلة كلية الملك خالد بن عبد العزيز

٦-د/ بشير على باز: دور الحكومة الالكترونية في صناعة القرار الإداري والتصويت الإلكتروني، مجلة

روح القانون، كلية الحقوق جامعة طنطا ٢٠٠٧

٧-د/ حسام الدين كامل الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، يناير ويوليو ١٩٩٠، العددان الأول والثاني، السنة الثانية والثلاثون

٨-د/ داود عبد الرازق الباز، الإدارة العامة، الحكومة الإلكترونية وأثرها على النظام القانوني للمرفق العام، مجلس النشر العلمي، جامعة الكويت، ٢٠٠٤

٩-سامية بوقرة: المخاطر المعلوماتية لنظم المعلومات وآليات مواجهتها، مجلة صوت الجامعة ٢٠١٥ ـ تصدر عن الجامعة الإسلامية في لبنان

١٠-د/ طاهر محمود: عقد إيواء الموقع الإلكتروني دراسة مقارنة في إطار القانون المصري والإماراتي والفرنسي، مجلة معهد دبي القضائي، العدد ٢٢ السنة الأولى، مارس ٢٠١٣.

١١- د/ عبد الإله محمد النوايسة: جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية "دراسة مقارنة" – المجلة القانونية والقضائية الصادرة من مركز الدراسات القانونية والقضائية وزارة العدل – دولة قطر – العدد الأول – (السنة العاشرة) يونيو ٢٠١٦.

١٢-عبد العزيز السيد مصطفى :أساسيات الرقابة على نظم التبادل الإلكتروني للبيانات – بحث مقدم لمؤتمر التجارة الإلكتروني(الآفاق والتحدي) المنعقد بكلية التجارة جامعة الإسكندرية -يوليو ٢٠٠٢.

١٣- د/ عماد يوسف حب الله: ورشة عمل حول "بناء القدرات في مجال الحماية القانونية على الإنترنت ٤-٥ شباط ٢٠٠٩ ـ الهيئة المنظمة للاتصالات في لبنان ـ أمن الفضاء السيبرانى

١٤- د/ محمد سليمان شبير: الإطار القانوني لسلطة الضبط الإداري الإلكتروني في فلسطين – مجلة جامعة الأزهر – ٢٠١٥، المجلد ١٧، العدد ٢ (ب) ص٩

١٥-د/ محمد الأمين البشري: "التحقيق في جرائم الحاسب الآلي"، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون – جامعة الإمارات العربية المتحدة – الفترة من ١-٣ مايو ٢٠٠٠م.

١٦-محمود الرشيدي: الجرائم الالكترونية والتأمين الالكتروني "قضايا المركز الدولي للدراسات المستقبلية والاستراتيجية العدد ١١ السنة الأولى، نوفمبر ٢٠٠٥

١٧-مروان صالح:المستقبل الافتراضي: السيناريوهات المحتملة لمستقبل الإنترنت: مقال منشور في مجلة حالة العالم" مجلة تصدر عن المركز الإقليمي للدراسات الإستراتيجية بالقاهرة ـ العدد ١٦

١٨-يحيى محمد أبو مفايض، الحكومة الإلكترونية: خيار إستراتيجي لتعزيز التفاعل بين الأجهزة الأمنية والمجتمع (ندوة المجتمع والأمن)، كلية الملك فهد الأمنية الرياض ٢٠٠٤

٥- قوانين وقرارات

١-القانون المصري لتنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣
٢-القانون المصري رقم ١٠٩ لسنة ١٩٧١ في شأن هيئة الشرطة
٣-القانون الكويتي رقم ٣٧ لسنة ٢١٤ بإنشاء هيئة تنظيم الاتصالات وتقنية المعلومات، منشور بمجلة الكويت اليوم العدد ١١٨٤ السنة الستون هـ ـ المادة ٢.
٤-قرار رئيس مجلس الوزراء المصري رقم ١٠٣٢ لسنة ٢٠١٥ باختصاصات اللجنة القومية الدائمة للتنسيق الأمني
٥-قرار رئيس الجمهورية المصري رقم ٥٥٢ لسنة ٢٠١٥ بتشكيل لجنة عليا لتنقية قواعد البيانات القومية -الجريدة الرسمية – العدد ٥٢ مكرر (هـ) في ٢٩ ديسمبر سنة ٢٠١٥
٦-قرار رئيس مجلس الوزراء المصري رقم ٢٣٢٨ لسنة ٢٠١٤ والذي ضم بموجبه ممثل لمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء إلى عضوية المجلس الأعلى للأمن السيبراني". "منشور بالجريدة الرسمية – العدد ٥٢ مكرر (ا) في ديسمبر سنة ٢٠١٤.
٧-القانون الكويتى رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية: الكويت اليوم العدد ١١٧٢ السنة الستون ٦٩ بتاريخ ٢٠١٤/٢/٢٣.
٨-القانون القطري رقم ١٤ لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية
٩-القانون الإتحادي الإماراتي رقم ١ لسنة ٢٠٠٦ في شأن المعاملات والتجارة الالكترونية.
١٠-قرار رئيس جمهورية مصر العربية بالقانون رقم ٩٤ لسنة ٢٠١٥ بإصدار قانون مكافحة الإرهاب - الجريدة الرسمية – العدد ٣٣ (مكرر) في ١٥ أغسطس سنة ٢٠١٥.
١١-قرار رئيس الجمهورية المصري رقم ١٥١ لسنة ١٩٩٨ – نشر بالجريدة الرسمية ١٩٩٨/٤/٤.

٦- مقالات وتقارير

١-مقال بمجلة زهرة الخليج – الإمارات – العدد ١٠٢٨ – س٢٠
٢-تقرير بعنوان : عمليات تخريب تهدد الأمن القومي على شبكة الإنترنت بتاريخ ٢٠٠٠/٢/١٧م على موقع http:news.bbc.com.U.K

٧-أحكام قضائية

١-الطعن رقم ١٠١٧١ لسنة ٥٤ ق. عليا المحكمة الإدارية العليا – الدائرة الثانية -حكم غير منشور
٢-حكم المحكمة العسكرية العليا يوم الثلاثاء ٢٠١١/٥/١٠ في القضية رقم ٢٠١/٥ جنايات عسكرية- إدارة المدعى العام العسكري-(حكم غير منشور).
٣-حكم محكمة القضاء الإداري، دائرة المنازعات الاقتصادية والاستثمار، الصادر في الدعوى رقم ١٤٣٠ لسنة ٦٥ ق جلسة ٢٠١٠/١١/٢٧ (حكم غير منشور)

٤-حكم محكمة القضاء الإداري – الدائرة الثامنة عقود- الدعوى رقم ٦٣٠٥٥ لسنة ٦٨ ق بتاريخ أغسطس ٢٠١٥ (حكم غير منشور).

٥-حكم محكمة القضاءالإدارى-دائرة المنازعات الاقتصادية والاستثمار-الدائرة السابعة- الدعوى رقم ٢١٨٥٥ لسنة ٦٥ قضائية بتاريخ ٢٠١١/٥/٢٨-حكم غير منشور

٦-حكم محكمة القضاء الإداري- الدائرة الثانية في جلسة ٢٠١٥/٨/٢٥ في الدعوى رقم ٥٧٩٣٣ لسنة ٨٦ ق. (حكم غير منشور).

٧-حكم المحكمة الدستورية العليا ١٩٩٨/٢/٧- القضية رقم ٤٠ لسنة ١٥ قضائية دستورية الجريدة الرسمية العدد ٨

٨- وثائق:

١-إتفاقية الأمم المتحدة خلال المؤتمر الدولي الذي عقد في إيطاليا بمدينة باليرمو الإيطالية، الفترة من (١٢ – ١٥) ديسمبر ٢٠٠٠م".

٢-مجلة حالة العالم، تقرير "جايسون هيلي" مدير مبادرة "cyber statecraft initiative" بمركز (Atlantic council).

٩-مواقع الكترونية:

١-الموقع الإلكتروني لجريدة المصري اليوم: خبر بعنوان "روتيرز". مصر أوقفت "فيسبوك المجاني" بعد رفض الشركة تمكينها من مراقبته" منشور بتاريخ ٢٠١٦/٤/١

٢-موقع المكتب الفيدرالي الألماني لأمن المعلومات www.bsi.bund.de

ثانيا:المراجع باللغة الانجليزية:

١- Abraham D. Safaer: - National security and leaks, the Government's Authority to Discipline itself. International studies in Human Rights- volume ١٦

٢- Alexander Matthew. S. E: - Government implementation- A Dissertation submitted to university of Delaware in partial fulfillment of the requirements for the degree of Doctor Philosophy with a major in political science spring ٢٠٠٧.

٣- Amanda N. Craig et al: - proactive cyber security: A comparative Industry and Regulatory Analysis, - AM. Bus L. J. (forth coming) ٢٠١٥.

٤- Brain Bridge: - D: Introduction to computer law, London ٢٠٠٠, fourth edition.

٥-Bruce P. smith: - Hacking, Poaching, and counterattacking: Digital

counterstrikes and the contours of self-Help, I J.L Econ, & Pol'Y ١٧١, ١٧٣ (٢٠٠٥),

٦- CRS report on Data mining and Homeland security ٢٠٠٧

٧- Christol, carl Q. : - Remote sensing and International law- ٥ Annals of Air and space law- (١٩٨٠)

٨- Cezar PETA: - cyber security – current topic of National security (١), Public security studies, volume II, Issue ٣ / ٢٠١٣

٩- Data Protection Act ١٩٩٨ Published by TSO, the stationery office– Data pretention & Investigatory powers Act ٢٠١٤ chapter ٢٧

١٠- David weissbrodt: - cyber conflict, cyber crime, and cyber Espionage, Minnesota Journal of International Law's ٢٠١٣ symposium

١١- Directive ٩٥/٤٦/EC of the European parliament and of the council of ٢٤ October ١٩٩٥ on the protection of individual with regard to the processing of personal data and on the free movement of such data.

١٢- Daniel solove: - Digital Dossiers ad the Dissipation of fourth Amendment privacy, ٧٥ S. CAL, L. REV. ١٠٨٣, ١٠٨٩ (٢٠٠٢).

١٣- Emily key: - coordinating supply chain Data To Deliver timely Information, companies must overcome Data synchronization Hurdles, frontline solutions, May ١, ٢٠٠٣

١٤- Fred H. Cate: - Government Data Mining:- The need for a legal framework, Hienonline – ٤٣ Harv. C. R. C.L.L. Rev. ٢٠٠٨

١٥-Federal support for Home land security information sharing: Role subcomm. On intelligence Information sharing and Risk-Assessment of the H. comm. on Home land security, ١٠٩ th cong. ٢٣ (٢٠٠٥) (statement of lee Humilton, vice chairman ٩/١١ public Discourse project).

١٦-Federal Trade commission, self Regulation and online Privacy: A Report to congress (July) ١٩٩٩ (concluding that greater incentives were implementation of the basic privacy principles). http://www.frc.gov/privacy/reports.htm

١٧- Garaham, J. Zellich:- Spies, suberversive terrorists, and the British Government:- free speech and other casualties, International studies in human Rights, Volume١٦

١٨- Hopkins, Grayl: - Legal implications of Remote sensing of Earth Resources by satellites, ٧٨ Military law Review.

١٩- Hubert H. Humphery, foreword to EDWARD V. long. The intruders, at villi (١٩٦٧).

٢٠- Hector Becerra, Jennifer oldham & Mitchell landsberg: Airline Terrorism Alert- winging it one Again, L.A. Times, Aug. I١, ٢٠٠٦

٢١- James oliphant: - phone firms want shield If spy suits come calling, chicago Tribune, Nov ١٥, ٢٠٠٧.

٢٢- Jeff Jonas & Jim Harper: - Cato institute, Effective counterterrorism and the limited role of predictive Data mining ٧-٨ (٢٠٠٦).

٢٣ - James klein: Indigent Defendants and Enemy combatants: Developing prototypes for National security cases. Harvard – C. R. – C. L. L. Rev. ٢٠٠٧

٢٤- Jonathan clough: principles of cybercrime-second edition -Cambridge press ٢٠١٠

٢٥- Kathleen M. Sullivan:- under a watchful Eye, Incursions on personal privacy in the war on our freedoms: civil liberties in An AGE of TERRORISM ١٢٨, ١٣١ (Richard leone & Greg Anrig, Jr. eds, ٢٠٠٣).

٢٦- Kasperson (W. K. Henrik): computer crimes and other crimes Against Information Technology in U. S. A., R. I. D. P. ٢٠٠١

٢٧- letter from William J. Haynes II, Gen. counsel, Dept of Def, to carol E. Drinkins, civil Rights and civil Liberties oversight Bd, (Sep. ٢٢, ٢٠٠٦)

٢٨- Lawrence J. Trautman: congressional cypersecurity oversight: who's who and How it works

٢٩- Lawerence k. Grossman: - Reflections on leaks in the United States: the media perspectives, International studies In Human Rights Volume ١٦

٣٠- Lamaby Frank, strategic disarmament and national security, London ١٩٩٧

٣١-Margo Anderson & Stephen E. Feinberg: - who count? The politics of census – taking in contemporary America ١١٧-١٨ (Russell stage found – ١٩٩٩).

٣٢- Marietta Benko, and others: - space law in the united nations, Martinus Nijhoff, Netherlands, ١٩٨٥

٣٣-Manuel Castells: - communication power ١st Edition ٢٠٠٩. -

٣٤- Myers, Davids: - Remote sensing and National sovereignty over natural Resources, Assessment of the Mexican view, ١٤ california western international law Journal. (١٩٨٤).

٣٥- Nathan Alexander sales: Regulating cyber security – Northwestern university law Review ٢٠١٣ vol., ١٠٧, No ٤,

٣٦- Office of TECH: Assessment, Electronic Record system anti individual privacy ٥٧ (١٩٨٦).

٣٧- office of Inspector GEN, U.S. DEPT of Just, IMMIERATION AND NATURALIZATION SERVICE'S ABILITY TO PROVIDE TIMELY AND ACCURATE ALIEN INFORMATION TO THE SOCIAL SECURITY ADMINISTRATION (No. ١.٢٠٠٣-٠٠١) at ٢٥ (٢٠٠٢)

٣٨- Protection of freedoms Act ٢٠١٢ Chapter ٩- United Kingdom, p. ١٨ clause ٢٣

٣٩- Paul Schwartz: - Data processing and Government Administration: The failure of the American legal Response to the computers HASTINGS LJ. ١٣٢١ (١٩٩٢) (emphasis in original

٤٠- Philip B. Heymann: - Investigative uses of files of Data about many people collected for other purposes ٩ (٢٠٠٣) (unpublished manuscript).

٤١-Privacy and civil liberties in the Hands of Government post-September ٢٢, ٢٠٠١

٤٢- Rumsfeld V. padilla, ٥٤٢ U. S. ٤٢٦, ٤٦٠ - ٦١ (٢٠٠٤) (Stecens, J., dissenting)

٤٣- Richard S. salant, CBC, and the battle for the soul of Broadcast Journalism: The Memoirs of Richards. Salant ٢٤٨ - ٤٩ (١٩٩٩)

٤٤- Ruth Gavison: - Atomic secrets and free speech- International studies in Human Rights volume ١٦

٤٥-Recommendations of the ٩/١١ commission and the US. Department of Defense Technology and privacy Advisory committee. Hearing Before the subcomm. On commercial and Administrative law ad subcomm-on the constitution of the H. comm. On the Judiciary, ١٠٨th cong. ٥(٢٠٠٤) (Statement of John O. Marsh, Jr. TAPAC).

٤٦-Ronald D. lee & Paul M. Schwartz :-Beyond the "war" on Terrorism, Towards the New Intelligence Network, ١٠٣ MICH. L. REV ١٤٤٦, ١٤٦٧ (٢٠٠٥).

٤٧-Richard Clarke: - Threats to U.S. National security: proposed partnership initiatives towards preventing cyber terrorist Attacks, ١٢ Depaul Bus, L. J. (١٩٩٩ – ٢٠٠٠).

٤٨- Stewart Mitchell: - Managing Information Risk, a director's guide combs, United Kingdom, ٢٠٠٩.

٤٩-Sieber Urlich: - computer crimes and other crimes related to information technology. I.R.P.. ١٩٩٤. Vol. ٦٢ p. ١٠٣٣ seq.

٥٠- Scott J. Shackelford, JD, PhiD, scott Russell, JD & Andreas juehn: - Defining cyber security Due Diligence under International law: lessons from the private sector.

٥١- S. W. Brenner: - cyber crime metrics. Old wine, new bottles? ٢٠٠٤ (٩) Virginia Journal of law and technology

٥٢- Steven Philippsohn: - Trends in cyber crime - An overview of current financial crimes on the internet, computers & security, ٢٠ (٢٠٠١)

٥٣- Shimon shetreet: - free speech and national security , International studies in Human Rights - Volume ١٦

٥٤-Susan W. Brenner, cyber crime:- criminal threats for cyberspace (٢٠١٠)

٥٥-Standards for privacy of Individually Identifiable Health Information, ٦٥ fed. Feg. ٨٢, ٤٦٢ (٢٠٠٠) (codified at ٤٥ C.F. R. pt. ١٦٠, ١٦٤. ٥٠٢, ١٦٤. ٥٠٦).

٥٦-Tuner B. Goron: - Classic and modern strategy, national security in the nuclear war - London ١٩٩٠

٥٧-Todd A. Brown: - legal propriety of protecting Defense Industrial Base Information Infrastructure GAA.F.L.Rev. ٢٠١١, ٢٢٠ (٢٠٠٩)

٥٨- TECH, AND PRIVACY ADVISORY COMM, U.S. DEPT of DEL Safeguarding privacy in the fight Against terrorism (٢٠٠٤) TAPAC, safeguarding privacy –

٥٩-The Cantigny principles on technology terrorism, and privacy, National security law Report, feb. ٢٠٠٥

٦٠-"The Cantigny" conference on counterterrorism technology and privacy organized by the standing committee on law and Nation security of the American Bar Association".

٦١- The Emergence of cyber security law, prepared for the Indiana university - Maurer school of law by Hanover Research, February,٢٠١٥

٦٢-"The National cyber security and infrastructure protection ٢٠١٣ Act".

٦٣- Tommy Peters : - Data scrubbing, computer world, Feb. ١٠, ٢٠٠٣

٦٤-William ouko, Yanal Yzing: -E. Government in Developing countries- A Dissertation submitted to the faculty of Graduate school of the University of Minnesota ٢٠١٠

ثالثا- المراجع باللغة الفرنسية: -

١- Article g- loi no ٧٨-١٧ du ٦ Janvier ١٩٧٩. Relative a Informatique, aux fichiers et aux libertes. Electronic copy available at: http://ssrn.com/abstract =٢٥٩٤٣٢٣

٢- Jean françois Lemetter, Risque, informaion et organisation, Paris, Éditions L'Harmatlan, ٢٠٠٨.

٣- LAUBADERE (A. de.) et VENEXIA (J.C) et GAVDEMET (Y): Traite de droit Administratif, Paris, L.G.D.J., T. ١. ١٠e ed, ١٩٨٨.

٤- Olivier Hassid, La Gestion des Risques, Paris, Éditions Dunod, ٢ed, ٢٠٠٨.

٥-RIVERO (J.): droit administrative, Paris, DALLOZ, ٦e ed. ١٩٧٥,

٦- KLEIN (C.) “La Police du domaine Public” Paris, L.G.D.I ٣e ed, ١٩٦٦,

الفهرس

المبحث الثالث: أهمية وخصائص الضبط الإداري الإلكتروني ومتطلباته.

المطلب الأول:أهمية الضبط الإداري الإلكتروني.

المطلب الثانى:خصائص الضبط الإداري الإلكتروني.

المطلب الثالث:متطلبات الضبط الإداري الإلكتروني. (تهيئة البيئة المعلوماتية الآمنة)

الفصل الثاني: أثر المحددات المعلوماتية على أساليب الضبط الإداري

المبحث الأول: أثر المحددات المعلوماتية على جهات الضبط الإداري.

المبحث الثاني: أساليب جهات الضبط الإدارى فى الرقابة المعلوماتية.

المبحث الثالث:أثر المحددات المعلوماتية على حيازة جهة الادارة للمعلومات وقواعد البيانات. لا

المطلب الأول: حيازة المعلومات على ميزان المشروعية

المطلب الثاني:حيازة البيانات الروتينية.

المطلب الثالث:الآليات المعتادة لرصد وحيازة البيانات والمعلومات.

أولا: نظام الأرشفة الإلكترونية:

ثانيا: الاستشعار عن بعد:

المطلب الرابع:اشكاليات حيازة جهة الإدارة للمعلومات وطرق حلها.

المطلب الخامس:حيازة الإدارة للمعلومات البيومترية.

المبحث الرابع: دور الشراكة المعلوماتية في تطوير أساليب الضبط الاداري.

المبحث الخامس: دور تنظيم الطيف الترددي في تطوير اساليب الضبط الاداري.