الدكتور/ ياسر محمد عبد السلام رجب
استاذ القانون العام المساعد بكلية الحقوق جامعة القاهرة

# دور الضبط الإدارى الإلكترونى فى الرقابة السيبرانية وتهيئة البيئة السيبرانية الآمنة

**المراسلة:** د. ياسر محمد عبد السلام رجب
أستاذ القانون العام المساعد، كلية الحقوق جامعة القاهرة

**معرف الوثيقة الرقمي (DOI):** https://doi.org/10.54873/jolets.v2i1.22

**البريد الإلكتروني:** ymar900@hotmail.com

**نسق توثيق البحث:**
ياسر عبد السلام، دور الضبط الإداري الإلكتروني في الرقابة السيبرانية وتهيئة البيئة السيبرانية الآمنة، مجلة القانون والتكنولوجيا، المجلد ٢، العدد ١، أبريل ٢٠٢٢، صفحات ١٣٩– ١٧٦

# دور الضبط الإداري الإلكتروني في الرقابة السيبرانية وتهيئة البيئة السيبرانية الآمنة

الدكتور/ ياسر محمد عبد السلام رجب


## ملخص

يعد الأمن السيبراني خيارا حتميا لجهة الإدارة، وتنعكس تلك الحتمية على النشاط الفردي، حيث إذا لم تفلح جهة الإدارة في الحفاظ على أمنها السيبراني؛ سيترتب على ذلك موجات من الاضطرابات في شبكاتها السيبرانية، مما يؤثر على دقة ومصداقية البيانات والمعلومات، ويحد ذلك من إمكانية تداولها. لذا إن لم يكن الفضاء الإلكتروني والسيبراني 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.

وتلجأ الدول لتعزيز الأمن السيبراني من خلال المعايير الفنية من ناحية أولى كمثال إنشاء معاهد للمعايير القياسية والتكنولوجيا والتشريعات والرقابة من ناحية ثانية.

علاوة على ما تقدم تلعب الشراكة السيبرانية دورا في تطوير أساليب الضبط الإداري في الرقابة السيبرانية فالتقنيات المستعملة في الاختراقات السيبرانية لا بد أن تواجه بطرق جديدة للتعامل لإدارة تلك الاختراقات من خلال وجود قواعد سيبرانية واستخباراتية تحدد نوع التهديدات فضلاً عن التنسيق بين العديد من القطاعات على مستوى التشريع القانوني والرقابي.

وهناك العديد من الآليات المعتادة لرصد وحيازة البيانات والمعلومات تساعد في تهيئة البيئة السيبرانية الآمنة، ومن آليات الإدارة في رصد المخاطر السيبرانية نظام الأرشفة الإلكترونية والاستشعار عن بعد.

ولكن تجدر الإشارة إلى أن الجهة الإدارية تواجه إشكاليات عند تهيئة البيئة السيبرانية تتمثل في إشكاليات حيازتها للمعلومات الشخصية خاصة الواردة من أطراف ثالثة ،إلى جانب إشكاليات أخرى كالفعالية والتأثير.


**الكلمات الرئيسية:** الأمن السيبراني- الضبط الإداري الالكتروني- التهديدات السيبرانية-الجريمة السيبرانية - الخطر والأمن السيبراني

# The Role of Electronic Administrative Control in Cyber Monitoring and Creating a Secure Cyber Environment

Dr. Yasser Abdel Salam

**Abstract**

Cyber security is an inevitable option for the administration which is reflected in individual activity. If the administration does not succeed in maintaining its cyber security, this will result in waves of disruptions in its information networks which affects the accuracy and credibility of data and information, and limits the possibility of its circulation. Therefore, if the cyber space is not a reliable means of communication or commerce, it will deter individuals and companies from investment, and this will affect, on the international level, the efforts to develop modern inventions and technologies; therefore, this will be an obstacle to cooperation between countries.

Thus, countries resort to enhancing cybersecurity through technical standards, for example, establishing institutions for standards and technology and legislation and monitoring.

In addition, the cyber partnership plays a role in developing the methods of administrative control in cyber-monitoring. The techniques used in information breaches must be faced with new ways to deal with the management of those breaches through the existence of information and intelligence bases that determine the type of threats as well as the coordination between many sectors on the level of legal and regulatory legislation

There are many usual mechanisms for monitoring and acquiring data and information that help in creating a secure cyber environment, and management mechanisms in monitoring informational risks which includes electronic archiving and remote sensing.

However, it should be noted that the administrative body faces problems when creating the information environment represented in the problems of its possession of personal information, especially from third parties, in addition to other problems, such as: 'efficacy' and 'impact'.

**Keywords:** Cyber security - information security - electronic administrative enforcement authority - cyber threats - cyber risk and security

## مقدمة

«إن الحديث عن الأمن السيبرانى يملى ضرورة الحديث كمقدمة ضرورية ولازمة عن فكرة الوجود القانونى لغايات الدولة، ذلك أن البعض ينكر هذا الوجود من منظور أن الحديث عن مهام الدولة هو الحديث عن وجهة نظر متجاوزة للقانون»[١].

يعد الأمن السيبرانى خيارًا حتميًا لجهة الإدارة؛ وبالتالى تنعكس تلك الحتمية على النشاط الفردي. فإن لم تفلح جهة الإدارة فى الحفاظ على أمنها السيبراني؛ سيترتب على ذلك موجات من الاضطرابات فى شبكاتها السيبرانية، مما يؤثر على دقة ومصداقية البيانات والمعلومات، ويحد من إمكانية تداولها.

لذا إن لم يكن الفضاء السيبرانى وسيلة موثوقة بها للاتصال أو التجارة، فسيبتعد الأفراد كما الشركات عن الاستثمار بل وسيؤثر ذلك على الصعيد الدولى فى جهود تطوير اختراعات وتكنولوجيات حديثة، وبالتالى سيكون ذلك عائقًا فى سبيل التعاون بين الدول، ويزيد من احتمالية ذلك الفرض التقاعس الحكومى فى دول العالم – خاصة العالم الثالث – عن توفير وتطبيق الإجراءات الدفاعية اللازمة[٢].

أضف إلى ذلك أنه رغم التطور الكبير فى علم الحاسبات الإلكترونية إلا أن مسألة الأمن السيبرانى لم تحظ بعد بالتطور المطلوب، فاعتراض المعلومات والتطفل عليها والعبث بها لم يعد حكراً على الجواسيس والخبراء العسكريين؛ وانما أصبح هواية للأشخاص العاديين مما شكل فى حد ذاته تهديدًا حقيقيًا للمنظمات الحكومية والخاصة[٣].

ومما يزيد الإشكالية تعقيداً «الاستخدام العام للبريد الإلكترونى ووصول الجمهور لمواقع الويب "web sites" عبر الإنترنت، وسهولة الوصول إلى المعلومات فى النظم النظم السيبرانية، مع الإمكانيات اللا محدودة لتبادلها وإرسالها بصرف النظر

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

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

(٣) باستطاعة طفل لا يتجاوز عمره ١٢ عامًا إطلاق هجوم إلكترونى على أى مؤسسة من أى مكان فى العالم.

عن بعد المسافات الجغرافية مما مكن المستخدمون من اصطناع فضاء جديد يسمى «الفضاء السيبرانى» والذى يستعمل أساسًا لأغراض شرعية ولكن يمكن أن يخضع لسوء الاستخدام»[١].

**بناء على ما تقدم سوف تكون معالجة هذا البحث كالتالي:**

- **المبحث التمهيدي: تعريف (الفضاء السيبرانى -الخطر السيبرانى -الأمن السيبرانى).**
- **المطلب الأول: تعريف الفضاء السيبراني.**
- **المطلب الثانى: تعريف الخطر السيبراني.**
- **المطلب الثالث: تعريف الأمن السيبراني.**
- **المبحث الثانى: دور الضبط الإدارى الإلكترونى فى الرقابة السيبرانية.**
- **المبحث الثالث: دور الضبط الإدارى الإلكترونى فى تهيئة البيئة السيبرانية الآمنة.**

(١) د/ طارق إبراهيم الدسوقى عطية: «الأمن المعلوماتى « (النظام القانونى لحماية المعلومات) دار الجامعة الجديدة ٢٠٠٩، ص١٤.

# المبحث التمهيدى

# تعريف (القضاء السيبرانى والخطر السيبرانى والأمن السيبرانى)

## المطلب الأول

## تعريف الفضاء السيبراني

الفضــاء الإلكترونــى أو الفضــاء السيبرانى هو الوســط الذى تتواجــد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني». وبمفهوم أشمل يعرف بأنه «مجال مركَـب مادى وغير مادى يشمـل مجموعة من العناصر هي: أجهـزة الكمبيوتر، أنظمة الشبكات والبرمجيـات، حوسبة المعلومات، نقل وتخزين البيانات، ومستخدمى كل هذه العناصر»[(١)].

ويذهــب البعض إلى أن مصطلــح الفضــاء السيــبراني، أو الفضــاء الإلكــتروني، ظهــر لأول مــرة عام ١٩٨٢، فــى رواية خيال علمــي، للكاتــب William Gibson، باسم Neuromancer، ولا يوجد تعريف واحد، متفق عليه دولياً لمصطلح الفضاء السيبراني، إنمــا بعض التعريفــات، المقبولة، علــى مستويات مختلفة، مثــل الأمن القومــي، وأمن المعلومات. وبعيداً عن رواية William Gibson، فالفضاء السيبرانى لم يعد خيالاً علمياً، بل أصبح واقعاً علمياً، ذا تأثيرات اجتماعية وسياسية واقتصادية[(٢)].

فلغويــاً يشتق لفظ Cyber، مــن الكلمة اللاتينية Kubernts بمعنــى قائد الدفة، فى إشــارة إلى القيادة والإدارة، إلا أن اللفظ التصق لاحقًا، بكل ما يخص الفضاء Space، واستخــدم فى كل ما يتعلق بالإنترنت بعد ظهوره وانتشار استخدامه بشكل كبير. فصار مــن المعلوم أن الفضاء السيــبراني، أو الفضاء الإلكتروني، هــو الوسط الذى توجد به،

(1) https://ar.wikipedia.org/wiki/%D9%81%D8%B6%D8%A7%D8%A1_%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A

اشتهــر المصطلح فى التسعينيات بعدما أصبحــت استخدامات الإنترنت والشبكات والاتصال الرقمى تنمو بشكل كبير وأصبح مصطلح الفضاء الإلكترونى قادرًا على تمثيل العديد من الأفكار والظواهر الجديدة التى ظهرت.

يُعتقــد أن هنــاك قواعــد وأخلاقيات مشتركــة تعود بالنفع المتبــادل على الجميع ليتــم اتباعها، ويشار إليهــا باسم أخلاقيات الإنترنت. يرى الكثيرون أن الحق فى الخصوصية هو الحق الأكثر أهمية فى أخلاقيات الإنترنت.

(٢) د/سمــير فــرج :الفضاء السيبراني-مقال منشور بالموقــع الإلكترونى لجريدة الأهرام المصرية بتاريــخ ٣٠ يوليو ٢٠٢٠ -آخر تحديث ٢٠٢١/٨/٣٠ https://gate.ahram.org.eg/News/2444508.aspx

وتعمل فيه شبكات الحواسيب الإلكترونية، فى العالم كله، بما فى ذلك أجهزة الكمبيوتر، وأنظمة الشبكات، والبرمجيات، وحوسبة المعلومات، ونقلها، وتخزينها، ومستخدميها من البشر والهيئات والمؤسسات[١].

## المطلب الثانى

## تعريف الخطر السيبراني

بداءة قبل تعريف الأمن السيبرانى يجدر بنا أن نقوم بتعريف الخطر السيبراني، وقد قام بعض الباحثين بتعريفه بأنه: خطر جديد يواجه المؤسسات وجهات الإدارة ويكون مرتبطًا بالتطور التكنولوجي، وتدفقات المعلومات[٢].

وفى اعتقادنا أن الخطر السيبرانى يمكن تعريفه بأنه تهديد إلكترونى محتمل يتعلق بالمعلومات والبيانات الرسمية وغير الرسمية للمؤسسات والأفراد والجهات الإدارية والحكومية، ومجاله احتمال التغيير أو التأثير فى صورة أو فى نشاط أو فى سلوك بإرادة مصدر الخطر.

وتتعدد أشكال الخطر السيبرانى ما بين التهديد بالاضطراب فى تدفق المعلومات، أوالتهديد باستغلال المعلومات الحساسة، والسرية، والملكية السيبرانية، أو التهديد بانتقاء المعلومات لتحقيق أغراض غير شرعية مختلفة ومتعددة أوالتهديد بتدمير المعلومات، أو تدمير مكونها الأساسي.

إذن فإن جملة المخاطر السيبرانية تتلخص فى عملية جمع المعلومات وتخزينها

---

(١) د/سمير فرج: المرجع السابق ص ٢ .

ولا شك أن العالم كله أصبح يألف استخدام مصطلح الفضاء السيبراني، الذى أصبح جزءًا من حياتنا، ولغتنا، وتواصلنا، حتى قيل إن حياتنا الجديدة أصبحت حياة الإنترنت تترابط كلها إلكترونيا، وتتواصل مع بعضها، بحيث تتجمع فيها المعلومات، وتكون قاعدة للبيانات، نستخدمها يوميًا، وتشير الإحصاءات إلى وجود نحو ٢٦,٦ بليون جهاز، على مستوى العالم، متصل بالإنترنت، أى أكثر من عدد سكان كوكبنا من البشر، وهو ما يخشى معه العلماء من ازدياد ظاهرة فقد السيطرة على أنفسنا، حيث إهمال استخدام العقل البشري، فى ضوء وجود أجهزة لحفظ المعلومات، ومقارنتها، وتحليلها. وفى ضوء هذا التراكم من المعلومات؛ سواء الشخصية، أو المعلوماتية، فى مختلف مناحى الحياة الاقتصادية، والاجتماعية، والسياسية، والعسكرية، والأمنية... إلخ، أصبح من الضرورى تأمين كل هذه المعلومات، ومن ثم ظهر مصطلح الأمن السيبرانى أو الأمن الإلكتروني.

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

وتوزيعها[١] وهو ما يتطلب القيام باتخاذ تدابير وإجراءات معينة يطلق عليها الأمن السيبراني.

ويذهب البعض الى أن نشأة المخاوف السيبرانية جاءت بعد تصميم البروتوكول الأساسى لنقل المعلومات عبر شبكة الإنترنت والمعروف اختصارًا باسم (TCP/IP) ، وبعد دخول القطاع التجارى للشبكة[٢].

## المطلب الثالث

## تعريف الأمن السيبراني

ذهب البعض إلى تعريف الأمن السيبرانى (أو السيبري) بأنه: مجموعة الأطر التنظيمية والإجراءات العملية والتقنيات التى تهدف إلى منع الاستعمال غير المصرح به للمعلومات مع الأخذ فى الاعتبار تأمين استمرارية الخدمة، وخصوصية المعطيات والمعلومات، وكذلك الحرص على إيجاد السبل الكفيلة بحماية المستخدم لتلك التقنيات من كافة المخاطر[٣].

ويذهب الفقه المقارن إلى تعريف مختصر للأمن السيبرانى بأنه "كيفية حماية البيانات والنظم الإلكترونية من الهجمات attack، أو الفقد loss، أو التداخل compromise."[٤].

لذا يتسع مفهوم الأمن السيبرانى ليشمل الإجراءات والتدابير المستخدمة فى المجالين الإدارى والفنى لحماية المصادر البيانية (الأجهزة والبرمجيات وبيانات الأفراد، ونحوها) من التجاوزات والتداخلات غير المشروعة التى تقع صدفة أو عمدًا

(١) سامية بوقرة: المخاطر السيبرانية لنظم المعلومات وآليات مواجهتها، مجلة صوت الجامعة ٢٠١٥ – تصدر عن الجامعة الإسلامية فى لبنان ، ص٢٢٩.

(٢) 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.

(٣) د/ عماد يوسف حب الله: ورشة عمل حول «بناء القدرات فى مجال الحماية القانونية على الإنترنت ٤-٥ شباط ٢٠٠٩ – الهيئة المنظمة للاتصالات فى لبنان – أمن الفضاء السيبرانى، ص٢ فى إشارة إلى الجهود فى مجال الأمن السيبرانى من خلال لجنة الاتصالات وتكنولوجيا المعلومات التابعة لجامعة الدول العربية، ومثال تلك الجهود القانون الاتحادى لمكافحة الجرائم السيبرانية الصادر فى الإمارات العربية المتحدة فى شباط ٢٠٠٦، وقانون سعودى صادر فى عام ٢٠٠٦ يجرم التنصت، والاعتراض أو الاستفادة من البيانات الإلكترونية دون مسوغ قانونى .

(4) The Emergence of cyber security law, prepared for the Indiana university -Maurer school of law by Hanover Research, February,2015 p. 11.

عـن طريق التسلل أو كنتيجـة لإجراءات خاطئة، لذا تشكل المحـاور التالية عماد الأمن السيبرانى:

١- الأخطاء العفوية غير المتعمدة أثناء تجهيز البيانات.

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

٣- حـوادث فقـدان أو تغيـير المعلومات بسبب تعطيـل الأجهزة أو حصـول خلل فى البرامج.

٤- فقد قدرات إدارة المعلومات لوقوع كوارث طبيعية أو صناعية[١].

(١) د/ دلال صادق الجواد. د/ حميد ناصر الفتال، أمن المعلومات، دار اليازورى العلمية للنشر والتوزيع، ص١٢.

## المبحث الثانى
## دور الضبط الإدارى الإلكتروني
## فى الرقابة السيبرانية

تجدر الإشارة إلى أن بعض التشريعات تعانى قصورًا تشريعية فى الأمن السيبرانى، ويتمثل القصور التشريعى أحيانًا بالنسبة للأمن السيبرانى فى حداثة الفعل المؤدى لانتهاك الأمن السيبرانى ، ومثال ذلك: جريمة الدخول غير المصرح للنظام السيبراني، فالمتتبع لتلك الجريمة يجد أنها من الصعوبة بمكان كى تتم معالجتها تشريعيًا بشكل كامل بموجب النصوص العقابية التقليدية[١].

ويتهدد الأمن السيبرانى للإدارة بصورة كبيرة لاعتماد الإدارة فى الوقت الحالى فى إدارتها لمرافقها على نظام الحكومة الإلكترونية، وقد يصل الأمر لانتهاك أمن الدولة الوطني، كالاطلاع على معلومات تمس أمن الدولة، أو الوصول إلى أنظمة التحكم فى محطات المفاعلات النووية[٢].

مؤدى ما سبق أن العديد من الدول تلجأ فى سبيل حماية أمنها السيبرانى إلى وجود أطر تشريعية ورقابية سيبرانية وتطبيق قوانين موضوعية وأخرى إجرائية على العكس من دول أخرى تعتمد على قوانين غير فعالة[٣].

وبالنظر إلى التجربة الأمريكية فى تعزيز الأمن السيبرانى نجدها تنقسم إلى شقين، أولهما: المعايير الفنية Technical standards وثانيهما: التشريعات والرقابة Legislation and Monitoring ونتناولهما كالتالى [٤]:

---

(١) أ. د/ عبد الإله محمد النوايسة: جريمة الدخول غير المشروع فى 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 ، ص ص١٠، ١١.

(2) Brain bridge. D: introduction to computer law, London 2000, fourth edition p. 307.

(3) David weissbrodt, cyber – conflict, cyber – crime, and cyber Espionage, Minnesota Journal of Internatinal Law's 2013 symposium, p. 3
For more: 1-Susan W. Brenner:- cyber crime- criminal threats for cyberspace (2010)

(2) Jonathan clough, principles of cyber crime (2010).
3- Richard Clarke, threats to U.S. National security: proposed partnership initiatives towards preventing cyber terrorist Attacks, 12 Depaul Bus, L. J. (1999 – 2000).

(٤) انظر للمزيد راشد محمد المري: رسالة دكتوراه بعنوان «الجرائم الإلكترونية فى ظل الفكر الجنائى المعاصر، رسالة مقدمة لكلية الحقوق جامعة القاهرة، ٢٠١٣، ص١٨٢.

## أولا - المعايير الفنية:

تم إنشاء المعهد القومى للمعايير القياسية والتكنولوجيا كباكورة أولية فى عام ١٩٠١ يتتبع وزارة التجارة الأمريكية، علاوة على وحدة المعلومات التابعة لمعمل تكنولوجيا المعلومات حيث تضع سياسات ومعايير تبادل المعلومات [١].

ومن أهم اللجان لجنة الحاسب الآلى والاتصالات التابعة للمجلس القومى للبحوث، وترجع أهمية تلك اللجنة إلى أنها تشفر المعلومات والبيانات "cryptography"[٢].

## ثانيًا - التشريعات والرقابة:

لن تكتمل منظومة الأمن السيبرانى إلا بوجود إطار تشريعى

– فعلى صعيد الرقابة تم إنشاء فريق الاستعداد فى ٢٠٠٣ كجزء رئيسى من وحدة الأمن القومى الافتراضى (National cyper security Division) [٣].

وتختلف أساليب الرقابة السيبرانية بحسب النظام القانونى والبيئة السيبرانية. ومن الأساليب الضبطية الإدارية الحديثة فى الولايات المتحدة أسلوب العمل على نحو تكاملى قومى كالمركز المتكامل للتهديد الاستخباراتى والمنشأة فى ٢٠١٥ (CTIIC) والذى يعمل عن طريق تبادل المعلومات والتهديدات منها الاستخبارات الإلكترونية[٤].

ولكن إذا أمعنا النظر فى جهات الضبط الإدارى فى الولايات المتحدة الأمريكية والتى تعمل على تعزيز الأمن المعلوماتى نجد أنها تضم العديد من الجهات، ومنها وكالة المخابرات المركزية، ووكالة الأمن القومي، ووكالة مخابرات الدفاع، ومكتب المخابرات

---

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

(٢) المرجع السابق ص١٨٢ فى إشارة إلى المرجع:

- Kasperson (W. K. Henrik) computer crimes and other crimes Against Information Technology in U. S. A., R. I. D. P. 2001, P. 273.

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

(4) Lawrence J. Trautman: congressional cyper security oversight: who's who and how it works: p. 22.

والاستطلاع بوزارة الخارجية، ومكتب التحقيقات الفيدرالي، ووزارة الأمن الداخلى وخاصة الإدارة الوطنية للأمن الإلكترونى [١].

**ومن جهات الضبط الإدارى المهمة أيضاً فى هذا الشأن مكتب المحاسبة والموازنة بالكونجرس؛ حيث إن لمدير هذا المكتب النظر بشكل عام فى نظم الأمن القومى وسياسات أمن المعلومات مع الأخذ فى الاعتبار ما يلي:-**

١- مراجعة توافق محل وكالة مع الاحتياجات والمتطلبات الموصوفة فى قانون الأكواد الأمريكي.

٢- تقديم تقارير للكونجرس فيما يخص أوجه القصور فى إجراءات وممارسات أمن نظم المعلومات.

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

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

غير أن الفقه الأمريكى يؤكد على إمكانية وجود أقوى لدور الضبط الإدارى فى حماية الأمن السيبرانى من خلال وضع المبادئ، ووضع اللوائح التنظيمية، وإدارة نظم

---

(١) انظر: جمال محمد غيطاس: أمن المعلومات والأمن القومي- مكتبة نهضة مصر- بدون سنة نشر. ص٢٤ وما بعدها.
وبالرجوع لدور تلك الإدارة نجد أنها تنفذ برنامج (العواصف الإلكترونية) الذى يعمل كاختبار القدرة على تحمل وصد الهجمات التى تستهدف الأمن السيبرانى ويقوم بذلك الاختبار خبراء الأمن السيبرانى فى وزارة الأمن الداخلى وجهات أمريكية أخرى، وأبرز تجربة للعواصف الإلكترونية ما كان فى الفترة من ٦ إلى ١٠ فبراير ٢٠٠٦ لاختبار كفاءة وقدرة الأجهزة الأمريكية على صد عاصفة إلكترونية شاملة والتعامل معها إذا ما كانت تستهدف البيئة السيبرانية التحتية، حيث تم خلال تلك المحاكاة عمل عمليات قرصنة إلكترونية افتراضية على أكثر من ١٠٠ مواطن بالولايات المتحدة تتضمن وكالات حكومية، وبنوكًا، 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 فى عشر ولايات أمريكية.

حماية المبيعات والفصل فى المنازعات[١].

إلى جانب ما سبق هناك بعض المؤسسات الحكومية التى تحمى الأمن السيبراني، كمثال: الهيئة القومية للاتصالات والمعلومات، ولجنة التجارة الاتحادية (FTC) والتشريعات على سبيل المثال، قانون حماية الأطفال على الإنترنت، وقانون حرية المعلومات (FOIA) التى تحمى حقوق المستخدم حال تواجده (on line) على الشبكة[٢].

ومثال تلك المؤسسات أيضًا: المركز الوطنى لحماية البيئة التحتية التابع للمباحث الفيدرالية الأمريكية[٣]، ومكتب رئيس التكنولوجيا وهو مكتب مفوض مباشرة من مدير التحقيقات الفيدرالية الأمريكية، وقسم جرائم الحاسب ومعهد أمن الحاسبات، ووحدة جرائم الإنترنت [٤].

ومن أمثلة جهات الضبط الإدارى التى تعزز الأمن السيبرانى ما قامت به فرنسا من إنشاء عدة وحدات ومراكز متخصصة ومنها الشرطة الوطنية لمكافحة الجرائم السيبرانية بكل صورها. ومن أهم تلك الوحدات أيضًا المكتب المركزى لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات للاتصالات، ومن مهام ذلك المكتب تنسيق عمليات ملاحقة مرتكبى الجرائم السيبرانية، علاوة على مشاركة جهات الضبط القضائى فى إجراءات التحقيق، ومساعدة الشرطة الوطنية وغيرها من الأجهزة[٥]، ومن تلك

---

(١) مشار إلى ذلك فى المرجع السابق ص١٤٥.

(2) http://www.frc.gov/privacy/reports.htm Federal Trade commission, self Regulation and online Privacy: A Report to congress (July) 1999 (concluding that greater incentives were implementation of the basic privacy principles).

والجدير بالذكر أن أغلب الشركات العالمية التى تعمل فى مجال الإنترنت تحرص على الأمن السيبرانى إلى جانب مبادئ أخرى، كمثال: مبدأ الاختيار، ومبدأ الإخطار، ومبدأ الحق فى الوصول والاطلاع.

للمزيد انظر: النظم المختلفة لحماية الخصوصية السيبرانية باعتبار أحد أركان الأمن السيبرانى د/ وليد السيد سليم:ضمانات الخصوصية فى الإنترنت – دار الجامعة الجديدة ٢٠١٢ ص٦٣٥ حتى ص٦٥٠.

- اتفاقية safe Harbor
- نظام مفوض المعلومات فى النظام القانونى الألماني.
- مفوض الخصوصية الكندية فى النظام القانونى الكندي.
- مفوض خصوصية المعلومات فى أستراليا.

(٣) تم إنشاء هذا المركز بعد الهجمات التى طالت الولايات المتحدة الأمريكية فى الاتصالات، والكهرباء والمؤسسات الاقتصادية ... إلخ. مشار لذلك فى المرجع السابق.

(٤) للمزيد انظر: المرجع السابق، ص٢٤٦.

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

(٥) تم إنشاء ذلك المكتب بموجب مرسوم وزارى رقم (٤٠٥ – ٢٠٠٠) المؤرخ فى ٢٠٠٠/٥/١٥ على مستوى المديرية المركزية

الجهات أيضًا القسم الوطنى لقمع جرائم المساس بالأموال والأشخاص[١].

ومن المبادئ المهمة التى تكفل الأمن السيبرانى لجهة الإدارة فى فرنسا وجود تنظيم فـى معالجة البيانات الشخصية، وجاء النصـ عليه فى قانون السيبرانية الفرنسى من خلال حظر استخدام وسائل غير شرعية لجمع المعلومات والبيانات وتوضح الغرض من جمع البيانات[٢].

أمـا على صعيـد التشريعات الفرنسية فقد تم إنشاء لجنـة وزارية فى فرنسا تخص الدعـم التقنـى من أجل تطوير تكنولوجيـا المعلومات والاتصالات فـى المرافق والرقابة الإداريـة (M.T.IC) فى عام ١٩٩٨ ومن المهام الرئيسيـة لتلك اللجنة ضمان التنسيق بين الإدارات والمرافق المختلفة، وتبادل ونقل البيانات وتحويلها، واقتراح تبادل المعلومات والبيانات الممكنة بين المرافق والإدارات[٣].

مـؤدى ما سبق، يؤكـد رفض التشريع الفرنسى انتهاج النهـج الأمريكى الذى يكتفى بالرقابة القضائية فيما يخص الأمن السيبراني، ولكن عمد التشريع إلى أسلوب الوقاية خـير من العلاج، لذا عمـد المشرع الفرنسى إلى إنشاء تلـك اللجنة التى تقوم بالتحرى والنصح والاقتراح والرقابة، وإعلام الجمهور ومساعدة أجهزة الدولة المختلفة[٤].

وتعـد تلك اللجنـة فى اعتقادنـا أهم إحـدى أدوات الضبـط الإدارى لحماية الأمن السيبرانى فى فرنسا، حيث تعتمد على الصفة الأساسية للضبط الإداري، وهى الطابع الوقائـى والرقابة السابقة من خلال اتخـاذ وسائل الحماية المسبقة، والرقابة المستمرة للتحقق من قيام الجهة القائمة على الحاسب الآلى فى تطبيق الضمانات القانونية، وما

---

للشرطـة القضائية التابعة لوزارة الداخلية ويساعد هـذا المكتب فى نشاطات كل من وزارة الدفاع، ووزارة الاقتصاد، والمالية، والصناعة، وهو يتمتع باختصاص وطنى يتحدد نطاقه فى الجرائم المرتبطة بتكنولوجيا المعلومات.

(١) يتكـون هـذا القسم من «٦» محققـين متخصصين فى التحقيق فى الجرائـم السيبرانية، ولقد بدأ القسـم مهامه عام ١٩٩٧ (مشار لذلك وللهامش رقم ١) رسالة دكتوراه فى الجرائم السيبرانية د/ محمد أحمد عزت المرجع السابق، ص٢٤٤.

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

(٣) د/ داود عبـد الـرازق البـاز، الإدارة العامة، الحكومة الإلكترونيـة وأثرها على النظام القانونى للمرفـق العام، مجلس النشر العلمي، جامعة الكويت، ٢٠٠٤ ، ص٢٥٦.

(٤) د/ وليد السيد سليم المرجع السابق، ص٥٨٦.

نقلا عن:

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

يؤكـد ذلك سلطة اللجنة فى اتخاذ القرارات التنظيمية العامة والفردية لتطبيق أحكام القانـون إلى جانب تكليف أحد أعضائها بالتحقق واقعيًـا من احترام الأمن السيبرانى عن طريق إجراء الفحص المناسب[١].

علاوة على ما سبق تعمل اللجنة القومية للمعلومات والحريات فى فرنسا على تعزيز الأمن السيبرانى للأفراد من بيانات ومعلومات بما يتفرع عن ذلك من حقوق كالحق فى الأمـن والسرية السيبرانية، معتمدة فى ذلك على العديد من إجراءات الضبط الإدارى ومنها التفتيش والمراقبة والإشـراف على الأنظمة السيبرانية، بل تتلقى شكاوى الأفراد والأشخاص المعنويـة العامة عند مخالفة القانـون وتقوم بالترخيص والتصريح عند ممارسـة نشاطات جمع البيانـات والمعلومات،والتأكد من توافـق النظام السيبرانى مع القانون[٢].

**مؤدى ماسبق أن اللجنة القومية للمعلومات والحريات تعمل على الدور الرقابى فيما يلي:**

١- منـح ترخيص معالجـة البيانات، كمثـال البيانات الخاصة بالمسائـل السياسية والعرقية والبيانات الصحية وهى البيانات الواردة فى المادة (٢٥) من قانون رقم (١٧-٧٨) الوارد فى المـادة (٢٦) من القانون ذاته، ومنها بيانات إحصاءات الرقم القومي، وعمليات التعداد والإحصاء الوطني، وخدمات الإنترنت العامة.

٢- إبـلاغ النائب العام فورًا بحسب ما تنص عليه المادة (٤٠) من قانون الإجراءات الجنائية الفرنسى بشأن ما يصل إلى علمها من جرائم سيبرانية.

---

(١) المرجع السابق ص٥٨٦.

(٢) نصت المادة رقم (١٣) من قانون (١٧-٧٨) المعدل بموجب قانون (٣٣٤-٢٠١١) الصادر فى 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.
- عضـوان حاليـان أو سابقان من محكمة النقض ويكونان على درجة مساوية لأعضاء اللجنة فى الدرجة ويتم انتخابهم من قبل الجمعية العامة لأعضاء محكمة النقض.
- عضوان حاليان أو سابقان من ديوان عام المحاسبة القومي.
- ثلاثة أعضاء من الخبراء المتخصصين فى علوم الحاسب أو قضايا الحرية الفردية يتم تعينهم بمرسوم من مجلس الوزراء.
- عضوان يختاران من الخبراء فى مجال الحاسب والمعلوماتية.

انظر: المرجع السابق ص٥٧٥ وما بعدها.

٣- يمكـن أن تسنـد اللجنة لأحـد أعضائها مهمة تفتيش مواقع نظـم المعلومات، بل والتحقـق مـن جميع عمليات المعالجـة، وتوثيق ما يتصل بذلك، ويمكـن لها اتخاذ أحد التدابير المنصوص عليها فى المادة (٤٥) من الفصل السابع ضد المتحكم فى البيانات.

**وتجـدر الإشارة إلى أن التوجيه الأوروبى نص على العديد من الصلاحيات لسلطات الضبط الإدارى لتعزيز الأمن السيبرانى ومنها:**

- صلاحيـات البحث والاطلاع علـى البيانات، وصلاحيات جمع كل ما هو ضرورى من معلومات تفيد فى أداء الواجبات الرقابية.
- صلاحيـات ضمان النشـر المناسب لـلآراء وحجب أو محو أو إتـلاف البيانات، أو فرضـ حظـر مؤقـت أو نهائى علـى المعالجـة، أو تحديد المتحكـم بالمعلومات وتوجيـه اللوم إليه أو إحالة الأمـر إلى البرلمانات الوطنية أو المؤسسات السياسية الأخرى[١].

علاوة على ما سبق قد تهدف بعض التشريعات إلى عدم إنشاء وحدات ضبط إدارى مستحدثـة مستقلة وتعمد إلى الاكتفاء بوحدات الضبط الإدارى التقليدية مع استحداث وسائلهـا أو تأهيل تلك الوحـدات أو مدها بتكنولوجيا حديثة، ومثال ذلك الإدارة العامة لمباحث الأموال العامـة، والإدارة العامة للتوثيق والمعلومات، والإدارة العامة للمصنفات الفنية،[٢] وإدارة مكافحة جرائم الحاسبات وشبكات المعلومات.

وفى اعتقادنا أن إدارة مكافحة جرائم الحاسبات وشبكات المعلومات من أهم وحدات الضبط الإدارى التى تعزز الأمن السيبرانى المصرى من خلال النظر فى اختصاصات تلك الإدارة وعلى رأسها بحسب القرار الوزارى رقم ١٣٥٠٦ لسنة ٢٠٠٢ ما يلي[٣]:

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

---

(١) للمزيد انظر: المرجع السابق، ص٥٦٥.

(٢) فـى اعتقادنـا أن الإدارة العامة لمباحث الأموال العامة، والإدارة العامة للمصنفات الفنية تتعلق باختصاصات نوعية ولا تحقق تعزيـز الأمـن السيبرانى بالمفهوم الذى يناقشـه المبحث، أما الإدارة العامـة للتوثيق والمعلومات فإنها قـد تخدم تعزيز الأمن السيبرانى بصورة جزئية مكملة.

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

- إخطار الأجهزة القومية والشرطية المختصة بالبيانات والمعلومات المتعلقة بالجرائم الأخرى، مع التنسيق لإجراءات التحريات وأعمال الضبط.
- تعزيز الأمن السيبرانى من خلال مكافحة مسببات اختراقه كالفيروسات والاختراقات.
- إعداد أرشيف سيبرانى متكامل لخدمة الإدارة فى مجال الحاسبات والنظم السيبرانية.

والجدير بالذكر أن القرار الوزارى رقم ١٣٥٠٧ لسنة ٢٠٠٢ نص على إنشاء أقسام إقليمية لمكافحة الجرائم السيبرانية[١].

**وبالتركيز على دور إدارة مكافحة جرائم الحاسبات وشبكات المعلومات نجد أن أهم أقسامها هو قسم التأمين حيث يقوم بما يلي[٢].**

١- معاونة أجهزة الوزارة فى تأمين نظمها السيبرانية.

٢- التخطيط ووضع أساليب تعزيز الأمن السيبرانى ثم التنفيذ والتنسيق مع الأجهزة المختصة.

٣- متابعة التراخيص التى تصدر للشركات الخاصة فى مجال المعلومات وذلك من خلال التنسيق مع الجهات المنوطة بذلك.

---

(١) انظر للمزيد: محمد أحمد عزت عبد العظيم: الجرائم المعلوماتية الماسة بالحياة الخاصة- رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة، ٢٠١٦ ، ص ص٢٥١، ٢٥٢.

يختص ذلك القسم بما يلي:-

١- متابعة البحوث الفنية والتقنية فى 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 فى التأمين الوقائى فى مجال الأمن السيبراني.

٥- أرشفة متكاملة لقاعدة البيانات والمعلومات لتعزيز الأمن السيبراني.

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

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

عـلاوة على ما تقـدم تلعب الشراكـة السيبرانيـة دوراً فى تطويـر أساليب الضبط الإدارى فى الرقابة السيبرانية فالتقنيات المستعملة فى الاختراقات السيبرانية لا بد أن تواجـه بطرق جديدة للتعامل لإدارة تلك الاختراقات مـن خلال وجود قواعد سيبرانية واستخباراتيـة تحدد نوع التهديـدات فضلاً عن التنسيق بين العديد من القطاعات على مستوى التشريع القانونى والرقابي[١].

ويرى الفقه المقارن أن هدف نظم الشراكة بين القطاعين العام والخاص فى مجال الأمن السيبرانى يرمى إلى وجود تدابير وقائية وبرامج أمن سيبرانى تقلل المخاطر السيبرانية[٢].

ويرى البعض أن الاحتمال الأبرز بالنسبة للأمن السيبرانى سيتحقق من خلال لجوء جهـات الإدارة على المستوى العالمى لتأسيس شبكات محليـة أو إقليمية، والاستغناء عن الشبكـة الموحـدة للإنترنت، وذلك كى يتـم الحد من تدفق البيانـات والمعلومات، ولكن يعيـب ذلـك التدبير الاحـترازى الإدارى أنه يطغى علـى عدة أمور **أولهـا:** حرية تداول المعلومـات، **وثانيها:** ازدياد قدرة الحكومات على مراقبة مـا يُنشر على الشبكة، لصغر حجمهـا، **وثالثها:** ارتفاع تكلفة البنية التحتية لإنشاء هذه الشبكات، بسبب تكرار بنائها فى كل دولة أو إقليم[٣].

وفى اعتقادنا أنه لن تفلح جهود تعزيز الأمن السيبرانى سوى بتوحيد الجهود الدولية قانونيـاً واحترازياً وقضائياً وذلك لوجود فقدان فى المركزية الأمنية السيبرانية، وعدم وجود آليات ضبطية إدارية على المستوى الدولى تستطيع السيطرة والتحكم.

---

(١) مـن أمثلـة قطاعات البنية التحتية السيبرانية القطاعات المالية والطاقة والرعاية الصحية والاتصالات والاستخبارات ووزارة الداخلية... الخ.

(2) "Dan Tofan, Technical director of CERT – RO stated that, there are situations in which the entity cannot manage incident alone, and in this case the cooperation between both entities becomes very important".

مـن وحـدات الإدارة المعنية بالأمن السيبرانى على سبيل المثال: وزارة العـدل، ووزارة الداخلية، ووزارة نظم المعلومات، والمخابرات بأنواعها.

(٣) مجلـة حالة العـالم، تقرير «جايسون هيلي» مدير مبادرة "cyber statecraft initiative" بمركز (Atlantic council). 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 فى تدفق المعلومـات والبيانات منها وإليها، ومثال تلك الدول: الصين، وروسيا، وقد تدفع الجهود المبذولة لتقنين الإنترنت تحت إشراف الاتحاد الدولى للاتصالات التابع للأمم المتحدة إلى الدفع نحو ذلك التدبير المستحدث. =

يؤيدنـا فى ذلك اختـلاف القوانين الوطنية المنظمة لحماية حـق من حقوق الإنسان مثلاً عن القوانين المنظمة لتعزيز الأمن السيبراني[١].

يـرى الفقه المقـارن أن مسألة الأمـن السيبرانى أصبحت مسألـة قانونية أكثر منها مسألـة تقنية لتعلقها بمجـالات الخصوصية Privacy وأمن المعلومـات Data security، فلا بد أن تعد المنظمات حزمة القوانين المنظمة للأمن السيبراني، وأن يكون للقانونيين دور فى تصميم الإجراءات والتدريب وتقديرات المخاطر[٢].

عـلاوة على ماسبـق يمكن الاستفادة مـن خبرات القطاع الخاص فـى مجال الأمن السيبري، كمثال إطار "NIST" (المعهد الوطنى للمعايير والتكنولوجيا)، وذلك لحماية البنية الأساسية الحيوية المحلية Domestic critical Infrastructure وذلك فى الولايات المتحدة الأمريكية[٣].

وبالمثـل نجـد أن الحكومة الألمانية قـد اعتمدت كذلك استراتيجيـة أمنية سيبرانية قائمة على الشراكة بين القطاعين العام والخاص[٤].

ويـرى الفقـه المقارن إمكانيـة لجوء جهـة الإدارة إلى إجراء برامـج لتطوير برامج حيـازة البيانات من خـلال تقنيات أكثر سرعة وبشكل قابل لتحمل التكلفة، وتسمح تلك

---

(١) د. أيمـن عبـد الله فكري: جرائم نظـم المعلومات، دراسة مقارنة، رسالة دكتوراه مقدمة لكليـة الحقوق جامعة المنصورة سنة ٢٠٠٦ صـ٥٠١. «ففى النـوع الأول هناك سيطرة وسيادة محلية (عناصر ضبط تشريعـي، وإداري، وقضائي) وبالتالى هناك جهـة تراقـب وتمنع الاعتداء وتتيح التعويض وملاحقة المخالفين، أما فى النـوع الثانى لا توجد سلطة مركزية ولا جهة سيادية توفر الحماية القانونية»

(2) The Emergence of cyber security law, prepared for the Indiana university Maurer school of law by Hanover Research, February, 2015. oP.cit,3
"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".

(3) Scott J. Shackelford, JD, PhiD, scott Russell, JD & Andreas juehn, Defining cybersecurity Due Diligence under International law: lessons from the private sector. 15.
Electronic copy available at: http://ssrn.com/abstract =2594323

(4) Ibid, p. 17
"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, 2011).
أما الصين فقد أصدرت تشريعات بغرض حماية أمنها السيبرانى القومي.. والتى يرمز لها بالمختصر (MLPS) "Multi – level protection schem" 2007 وذلك فى عام

التقنيات لجهة الإدارة بالتحرك فى الفترة ما بعد الجريمة بالبحث عن بيانات الأفراد المعنيين بالبحث عن البيانات[١].

مـؤدى ما سبق يجـوز الاستعانة بالقطاع الخاصـ فى حماية الأمـن السيبرانى من خـلال توفير أعلى حماية تقنية لجهة الإدارة، بل ويمكـن تصنيف المعلومات وفقًا لتلك الاستعانة بحسـب درجة سريتها، ويمكن لجهة الإدارة دراسة كل حالة على حدة للقيام بعملية التصنيف[٢].

فـى اعتقادنا أن البنية الأساسية الحيوية هى الأولى بوضع التدابير الاحترازية، لذا سعت الولايات المتحدة إلى «حماية البنية الأساسية الحيوية» "critical infrastructure" والتـى تعنـى بالأساس حماية النظـم "system" والأصـول "assets" والتى لها تأثير علـى الأمن بصفة عامة، والأمن الاقتصادى القومي، والصحة العامة والسلامة العامة أو كل ما سبق[٣].

ويساير ماسبق ما يميل إليه الفقه الأمريكى من تعزيز الأمن السيبرانى بصورة شاملة فـى كل من القطاعين العـام والخاص، ولكن لابد من الأخذ فى الاعتبـار أن المؤسسات العامـة وشركات الطاقة أقل من حيث القدرة الوقائية فـى مجال الأمن السيبرانى من الشركات التجارية التنافسية[٤].

(1) See: task force on national security in the information Age, Markle found creating AA Trasted Network for Homeland security (2003): Task force on National security in the information age, Markle found, Mobilizing information to prevent terrorism (2006); protecting America's freedom in the information age.

ساهمـت تلك التقنيـات خاصة بعد الهجمات الإرهابية فـى ١١ سبتمبر، حيث كشفت جهة الإدارة فى الولايـات المتحدة الأمريكية بيانـات هائلـة حـول الأفراد مستمدة مـن القطاع الخاص، وبذلـك يكون الكونجرس قـد أخفق فى الموازنة بـين الخصوصية privacy والأمن القومى National security

For more – the Cantigny principles on technology terrorism, and privacy, National security law Report, feb. 2005, at 14. "The Cantigny" conference on counter terrorism technology and privacy organized by the standing committee on law and Nation security of the American Bar Association".

(2) Abraham D. Safaer: - National security and leaks, the Government's Authority to Discipline itself. International studies in Human Rights- volume 16., p. 76

(3) Todd A. Brown, legal propriety of protecting Defense Industrial Base Information Infrastructure GAA.F.L.Rev. 2011, 220 (2009)p.222

(4) Bruce P. smith, Hacking, Poaching, and counterattacking: Digital counterstrikes and the contours of self-Help, I J.L Econ, & Pol'Y 171, 173 (2005),p.32

عـلاوة على ذلك، يمكـن تحديد سبل حماية الأمن السيبرانـى فى الولايات المتحدة مـن خلال حماية الأمن السيبرانـى للبنية الأساسية الحيوية عـن طريق وصف الموقف الأمنـى السيبرانى لجهـة الإدارة، وتحديد وترتيـب أولويات فرص التحسين فى إطار عمليـة مستمرة ومتكررة، والتواصل بين الجهات المعنية بالأمن السيبرانى داخل الدولة وخارجها حول مخاطر الأمن السيبراني[١].

ومن وجهة نظرنا، لا بد أن تأخذ جهة الإدارة فى اعتبارها عند إبرام عقودها-خاصة فى عقود نقل التكنولوجيا- ما يحميها من نصوص تعاقدية وتدابير احترازية، حيث إن من أهم مجالات حماية البيانات عند تعاقد جهة الإدارة مع شركة تقوم باستبدال تقنية معينـة أو معالجة قواعـد البيانات لديها أن تتخذ جهـة الإدارة التدابير الاحترازية فى مجـال التعاقد بإدراج التـزام عقدى على تلك الشركات كى تحمـى البيانات الحكومية مـن الدخول لغير المرخص، ويجب على جهـة الإدارة من خلال العاملين لديها أن تتخذ إجـراءات الحماية اللازمة عنـد تزويد تابعى الطرف الثانى تعويضـات وكلمات المرور للدخول إلى نظمها وبياناتها[٢].

والجديـر بالذكـر أن جهـة الإدارة - خاصة فى حالة نقص مواردهـا المالية أو عدم خبرتهـا بأطـر الضبطين التشريعى والإدارى للأمن المعلوماتـى - بين خيارين ليسا من السهولـة بمكـان، حيث يتمثل الخيار الأول فـى تعزيز أمنها المعلوماتـى، ويتمثل الخيار

(1) The Emergence of cyber security law, prepared for the Indiana university -Maurer school of law by Hanover Research, February,2015., p. 16

ويمكـن الاستعانة فـى ذلك بإطار (NIST) المعهد الوطنـى للمعايير والتكنولوجيا الذى يقوم على تحسـين الأمن السيبرانى للبنية التحتية الحيوية، وذلك الإطار لا يعد تشريعًا 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 26, 2014.

(٢) ويرتبـط بذلـك وجوب نقل المعرفة لموظفى جهـة الإدارة لإحداث تغييرات فى واجهة المستخدم عنـد التحديث الفني، وترحيل قاعدة البيانات.

الثانى فى شراء التكنولوجيا الأجنبية لتعزيز الأمن السيبراني[١].

لذا يرى البعض أن التشفير يعد وسيلة مهمة لحماية الإدارة من المخاطر السيبرانية خاصــة فى حالة تداول البيانــات والمعلومات بين جهات إدارة مختلفة فى صورة قرارات أو أوامر أو تعاقدات إدارية[٢].

قــد يكون التشفير حــلاً مؤقتًا عن طريق تأمين الشبكــات السيبرانية لجهة الإدارة كتغيــير طريقــة التشفير والمراجعــة الدورية لأساليــب الحماية، ويمكننــا الإضافة إلى ذلك بمراعاة حصر الاختصاصــات للموظفين الذين يتعاملون مع البيانات والمعلومات الحكومية وغيرها[٣].

(1) Scott J. Shackelford, JD, PhiD, scott Russell, JD & Andreas juehn: - Defining cyber security Due Diligence under International law: lessons from the private sector,., p. 22

وفى اعتقادنا أن ذلك يتوجب أن تمتلك الدولة إمكانيات اقتصادية هائلة فى مجال تكنولوجيا المعلومات والأمن السيبراني، علاوة على توفر الكوادر المدربة والمؤهلة لذلك ،لذا من المبادئ الدولية فى حماية الأمن السيبراني، والتى تلجأ لها بعض الدول مبدأ استبعــاد تكنولوجيــا الأمن المملوكة للأجانب، وعلى سبيل المثال: الصين، وهى فى ذلــك تخالف السياسة الأمريكية، والألمانية فى حماية وتعزيز الأمن السيبراني.

For more: see Amanda N. Craigetal. proactive cybersecurity: A comparative Industry and Regulatory Analysis, - AM. Bus L. J. (forth coming) 2015.

وتجدر الاشارة كذلك إلى أنه يجب على جهة الإدارة أن توازن بين رغبتها فى الحفاظ على عيوب البرمجيات السرية- من أجل إجراء التجسس والحرب الإلكترونية- وبين تقاسم تلك العيوب مع شركات التكنولوجيا لضمان الأمن السيبراني، فقد توصل القراصنــة الإلكترونيــين إلى «فيروس الفدية» الــذى انتشر مؤخرًا من خلال استغلال الثغــرات الصفرية الموجودة فى برامج تشغيل ويندوز للتجسس على الأفراد والحكومات والتى طورتها وكالة الأمن القومى الأمريكية.

(٢) د/ بشير على باز: دور الحكومة الإلكترونية فى صناعة القرار الإدارى والتصويت الإلكتروني، مجلة روح القانون، كلية الحقوق جامعة طنطا ٢٠٠٧ ، ص٣٥، ٣٦.

(٣) د/ عماد يوسف حب الله: ورشة عمل حول «بناء القدرات فى مجال الحماية القانونية على الإنترنت ٤-٥ شباط ٢٠٠٩ - الهيئة المنظمة للاتصالات فى لبنان - أمن الفضاء السيبرانى ص٢٧ «على سبيل المثال حماية التطبيقات المهمة عبر استخدام بنى تحتيــة مزدوجــة ذات طبقات حماية متعددة تضمــن ألا يحقق الدخلاء أهدافهم من خلال اخــتراق وإسقاط نظم المعلومات، وكذلك تعزيز البنى التحتية السيبرانية باعتماد كلمات سر صعبة الاختراق، وأنظمة حماية متعددة الطبقات، ومنهجية النسخ المتطابقة Mirroring، والأرشيف الاحتياطى للبيانات، وحماية شبكة السيبرانية فى الشركات والمؤسسات التجارية، والاعتماد علــى مواقــع تكون بمثابة نسخــة مطابقة للأصل خارج أراضى الدولة عند وجود بيانات عاليــة السرية" "ساعد ذلك جورجيا علــى تخطى الاختراق الروسى لبواباتها الإلكترونية حيث تم استعمال بوابات بديلة مطابقة للبوابات الأصلية تقع فى الأراضى الأمريكية."

## المبحث الثالث

## دور الضبط الإدارى الإلكتروني
## فى تهيئة البيئة السيبرانية الآمنة

هنـاك العديد من الآليـات المعتادة لرصد وحيازة البيانـات والمعلومات تكرس لدور الضبـط الإدارى الإلكترونـى فى تهيئة البيئة السيبرانيـة الآمنة، ومن اللجان ووحدات الضبـط الإدارى التى تعمل على ذلك فى سبيل تعزيـز الأمن السيبرانى ما نصت عليه المـادة (١٨) من القانون رقـم ١٠ لسنة ٢٠٠٣ الخاص بتنظيـم الاتصالات منه تشكيل لجنة لتنظيم الترددات، حيث تتولى تلك اللجنة تنظيم الطيف الترددى وهو أحد موارد الثرورة الطبيعية والتى تشكل محورًا من محاور الأمن السيبراني[١].

ويأخـذ التشريع المصرى بأسلـوب الرقابة السيبرانية 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 شيء من ذلك دون الحصـول على ترخيص من الجهـاز وفقا لأحكام هذا القانون وحددت المادة (٢٥) من القانـون الأمـن القومى -فى مجمله سواء ماديًا أو سيبرانيًـا- هدفًا، وذلك بأن تطلبت أن يحـدد الترخيـص الصادر مـن التزامات المرخص لـه، والتى تشمـل على الأخص الالتزامات الخاصة بعدم المساس بالأمن القومى .

وهـذا ما أكـدت عليه المـادة (٦٧) من القانون بخضـوع أى مشغـل أو مقدم خدمة للسلطـات المختصـة فى الدولـة ولنظام إدارتها مـن خدمات وشبكـات اتصالات، وأن تستدعى العاملين لديـه القائمين على تشغيل تلك الخدمات والشبكات وصيانتها وذلك فـى حالة حدوث كارثة طبيعيـة أو بيئية، أو فى الحالات التى تعلـن فيها التعبئة العامة طبقًا لأحكام القانون رقم ٨٧ لسنة ١٩٦٠، وأية حالات أخرى تتعلق بالأمن القومى.

وبالنظر إلى التشريع الكويتى نجد أن هيئة تنظيم قطاع الاتصالات وتقنية المعلومات تختص بـإدارة طيف الترددات الراديوية ومراقبـة التداخلات وجودة الطيف الترددى

(١) تشـكل تلك اللجنـة بقرار من الوزير المختص وتضم ممثلين عن إدارة الاتصالات برئاسـة الجمهورية ووزارة الدفاع، ووزارة الاتصـالات، ووزارة الداخليـة، وهيئة الأمن القومـي، واتحاد الإذاعة والتليفزيون، علاوة على ثلاثـة أعضاء يرشحهم الوزير المختص.

واتخـاذ الإجـراءات اللازمـة بهـذا الخصوص بما فى ذلـك إعداد الجـدول الوطنى لتوزيـع الترددات وتحديثه، وإعداد المخطط الوطنـى لتوزيع الترددات والسجل الوطنى لتشخيص الترددات بالاشتراك مع الجهات العسكرية والأمنية[١].

وقـد أكدت المـادة (٢٧) من القانون ذلك فـى فقرتها الأولى من خـلال عدم جواز استخدام أى شخص لأية ترددات راديوية إلا إذا حصل على رخصة بذلك وفقًا للشروط التى تحددها إدارة هيئة الاتصالات وتقنية المعلومات[٢].

فضـلاً عما تقدم هنـاك العديد من الآليـات الإدارية لرصد المخاطـر السيبرانية، حيـث تعمد جهة الإدارة إلى اللجوء إلى آليـات أمنية لرصد بعض المخاطر على شبكات التواصل الاجتماعي، ومثال ذلك: ما قامت به وزارة الداخلية المصرية من إنشاء مشروع لرصـد المخاطر الأمنية لشبكات التواصـل الاجتماعى فى مصر (منظومة قياس الرأى العام).

---

(١) انظـر قانـون رقم ٣٧ لسنة ٢٠١٤ بإنشـاء هيئة تنظيم الاتصالات وتقنية المعلومات، منشور بمجلـة الكويت اليوم العدد ١١٨٤ السنة الستون هـ - المادة (٢).

- نصـت المـادة الثانية على أن «تنشأ هيئة عامة ذات شخصية اعتبارية مستقلـة تسمى الهيئة العامة للاتصالات وتقنية المعلومات ويشرف عليها الوزير المختص وتتمتع بالشخصية الاعتبارية المستقلة وبالاستقلال المالي...».

ونصـ القانـون فى المادة (١٤) منه على أن "تحل الهيئة محل وزارة المواصلات وأى جهات أخرى فى حدود ما أوكله القانون للهيئة مـن اختصاصـات..." . ويعد ذلك إدراكًا من المشرع الكويتى بأهمية مرفق الاتصـالات عامة والأمن السيبرانى لجهة الإدارة خاصة، مما يتوجب معه وجود هيئة مستقلة لها استقلال مالى تتولى المشاركة فى تعزيز الأمن السيبراني.

(٢) انظـر المـادة (٢٧) من القانون، وقد اكتملت منظومة تعزيز أمن الطيف الترددى من خلال المادة (٣٠) والتى منعت اقتناء أو استعمـال محطـة راديوية على أراضى الدولة أو على سفينة أو علـى طائرة مسجلة فى 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 فى المادة (٣١) يخص القوات المسلحة والأجهزة الأمنية وجهات أخرى يجوز لمجلس إدارة هيئة الاتصالات وتقنية المعلومات استثناءها، وهـي: السفـن والطائرات الأجنبيـة، وخدمات النقل البرى فى الأراضـى أو الموانيء أو المطارات الكويتيـة، وكذلك السفارات الأجنبية بشروط المعاملة بالمثل، ووجود تصريح قابل للتجديد.

وتتمتع الهيئة بالاختصاصات المهمة فى مجال الأمن السيبرانى ومنها:

١- تنظيـم خدمات شبكات جميع الاتصالات ووضع لائحة تفصيلية للمصطلحات الفنية المستخدمة فى قطاعى الاتصالات وتقنية المعلومات.

٢- وضع لوائح تنظيم قطاعى الاتصالات وتقنية المعلومات بما يتفق مع السياسة العامة المقررة فى هذا الشأن.

٣- وضـع لائحـة بضوابـط وشروط منح رخص شبكـات وخدمات الاتصالات أو الإنترنـت واستخدام الـترددات الراديوية وإنشاء وتشغيل بنية اتصالات دولية.

٤- تنظيـم الربـط البينى بين شبكات الاتصـالات العامة المملوكة للقطاع الخاص، أو وزارة المواصـلات، أو أى جهة حكومية أخرى عدا الجهات الأمنية.

٥- تعقب مصدر أى موجات راديوية للتحقق من ترخيص ذلك المصدر دون المساس بسرية الرسائل.

وقد ذهبت محكمة القضاء الإدارى (الدائرة الثامنة) إلى إقرار ذلك الإجراء الضبطى الإدارى كونه وسيلة لتمكين وزارة الداخلية من القيام بدورها المنوط بها، واعتبرت أن قيام جهة الإدارة بإنشاء تلك الآلية يعد من قبيل الرقابة والتنظيم وليس التقييد[١].

**لذا تتعدد آليات الإدارة فى رصد المخاطر السيبرانية لكننا سنقتصر على أهم آليتين وهما:**

## أولاً- نظام الأرشفة الإلكترونية:

يعد نظام الأرشفة الإلكترونية أحد أقدم وسائل التقليدية لحفظ الأمن السيبراني، ويرى البعض إمكانية تفعيله من خلال:

١- تشكيل لجان حكومية فى 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 فى حالة فشل تشغيل أى من الدعامات الأخرى والعمل على القيام بعملية تحويل يومى back up خارج جهاز الحاسوب[٢].

وعلاوة على ما سبق تعد معالجة البيانات للأغراض الإدارية أحد أوجه نظام الأرشفة الإلكترونية "Data processing model of administrative control"، ويمكن تعريفها

---

(١) حكم محكمة القضاء الإدارى – الدائرة الثامنة عقود فى 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 الاطلاع على محتوى متاح للكافة يمكن لأى شخص الإطلاع عليه بمجرد دخوله على شبكة الإنترنت، وليس من شأنه اختراق حسابات الأشخاص، أو الاطلاع على بياناتكم الشخصية...».

(٢) ناجح أحمد عبد الوهاب: التطور الحديث للقانون الإدارى فى ظل نظام الحكومة الإلكترونية –رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة ٢٠١١، ص١٨١، ١٨٢.

للمزيد انظر:

- عبد العزيز السيد مصطفى – أساسيات الرقابة على نظم التبادل الإلكترونى للبيانات – بحث مقدم لمؤتمر التجارة الإلكترونى – الآفاق والتحدى – المنعقد بتجارة الإسكندرية، يوليو ٢٠٠٢ ، ص٤١٩.
- د/ هدى حامد قشقوش: جرائم الحاسب الإلكترونى فى التشريع المقارن – دار النهضة العربية، القاهرة، ١٩٩٢.

بأنهـا: هى الشكل التقليدى لمعالجة البيانات حيث يـزداد اعتماد الجهات الإدارية على البيانـات الشخصية للاستخدام فى الأغراض الإدارية، سواء أكانت للأمن الاجتماعى أو الصحى أو قانون العمل أو الضرائب أو مجال ممارسة الحقوق السياسية فى انتخاب وترشيح أو المجال الاجتماعى كحالات الميلاد والطلاق والوفاة.

ويـرى الفقه المقارن أن هـذا الشكل يقوم على اعتماد جهة الإدارة على موظفيها فى جمـع تلك البيانات، ثم تحليلها من قبـل المتخصصين الذين يقومون بالتقييم والتقدير باستقلالية تامة[١].

ويمكـن أن يقترب مصطلح "معالجة البيانات" من مصطلح "استخلاص البيانات "Data Mining" حيث يقوم المصطلح الأخير – بمفهوم واسع – على الأنشطة التى تقـوم علـى البيانات كأبحـاث تقوم على دراسـة موضوع ما أو الأبحـاث التى تقوم على دراسة أشخاص بعينهم أو الأبحاث التى تقوم على دراسة نمط ما أو الأشكال المتنبأ بها بالنسبة للأنشطة والعلاقات، ويتصل اصطلاح استخلاص البيانات بمصطلح آخر وهو اصطلاح توفيق البيانات "Data matching"[٢].

(1) Paul Schwartz, Data processing and Government Administration: The failure of the American legal Response to the computers HASTINGS LJ. 1321 (1992) (emphasis in original),p43

ومن أشكال معالجة البيانات للأغراض الإدارية:

1) Government Benefits and Social service programes.
2) Taxes.
3) Employment.
4) Law Enforcement.

(2) Fred H. Cate: - Government Data Mining:- The need for a legal framework, Hienonline – 43 Harv. C. R. C.L.L. Rev. 2008., p. 4

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". =

تستخـدم المؤسسات الحكومية الدراسات التـى تقوم على الموضوع والدراسات العلائقية المتصلة كمثال دراسة المسئولين عن تنفيذ القانون لبصمات شخص ما فى مسرح الجريمة، أو سائق السيارة وقد يستخدم أيضًا فى مجال الضرائب... إلخ، أما دراسات الشـكل أو النمـط تتصل بصـورة أكبر بالقانون التجارى ودراسـات تقوم على المستهلك وتقديرات المخاطـر التجارية بل وزاد استخـدام دراسـات النمط بعد هجمات الحادى عشر من سبتمبر ٢٠٠١، فقد طلـب الكونجرس بموجب قانون الأمن الوطنى 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 التى تواجه الولايات المتحدة.

**ثانياً- الاستشعار عن بعد:**

يعـد الاستشعـار عن بعد مـن أدوات جهـة الإدارة فى استخلاص البيانات، ويمكن تعريفـه بأنـه طريقة للحصول على معلومات عن شيء ما مـن مسافة بعيدة، ويستخدم هـذا التعبير فى الوقت الحاضر لوصف الطرق التى تُجمع بها البيانات عن الأهداف أو الظواهـر الطبيعيـة التى تحدث على سطح الأرض أو بالقـرب منه من مكان مرتفع فى الهـواء أو فى الفضاء الخارجي. وبالتالى لا يوجد فرق بين الاستشعار عن بعد من الجو أو من الفضاء الخارجى فى كثير من النواحى الفنية"[١].

أضـف إلى ماسبـق أن تدفـق البيانات يُعد نتاجـاً لعمليات الاستشعـار عن بعد عبر أربع مراحل ثابتة، وهى مرحلة جمع البيانات، ثم معالجتها، وتفسيرها وأخيرًا توزيعها ونشرها[٢].

وكمـا تؤدى أنشطة الاستشعـار عن بعد مهامها فى جمع البيانـات من الأرض فإنها تستخـدم لتوصيـل البيانـات التى يتم التحصـل عليها بواسطـة توابـع الاستشعار إلى الأرضـ، أو توصيل أوامـر السيطرة إلى هـذه التوابع، وتكمن الصعوبـة العملية فى أن التوابـع الاصطناعيـة لا تحدد حدود الدول من الفضـاء الخارجى بسهولة. لذا لا يمكن فصل البيانات الخاصة بدولة ما عن باقى البيانات إلا بصعوبة بالغة قد تكون مستحيلة أو باهظة التكاليف اقتصاديًا[٣].

فضـلاً عما تقدم هنـاك العديد من الآليـات الإدارية لرصد المخاطـر السيبرانية، حيث تجدر الإشارة إلى أن الجهة الإدارية تواجه إشكاليات عند تهيئة البيئة السيبرانية تتمثل فى إشكاليات حيازتها للمعلومات الشخصية خاصة الواردة من أطراف ثالثة تثير إشكاليتين، الأولى: الفعالية "efficacy" بمعنى هل تضمن عملية حيازة تلك المعلومات المصـادر المالية والبشرية التى تتطلبها؟ والثانيـة: التأثير "Impact" بمعنى هل يؤدى

(1) Marietta Benko, and others, space law in the united nations, Martinus Nijhoff, Netherlands, 1985, p.3

(٢) د/ ممدوح فرجانى خطاب: النظام القانونى للاستشعار عن بعد من الفضاء الخارجي، دار النهضة العربية ١٩٩٣ص٢٤٦ .تكون تلك الآلية بإنشاء أدوات متقدمة حول الدخول للبيانات واستلامها وتحليلها لاكتشاف المخاطر الإرهابية التى تواجه الولايات المتحدة

(3) Van ligten Hans, Municipal law Regulation of Remote sensing in outer space, loyola of Los Angles International and comparative law Journal (Winter, 1984)

مشار إليه فى د/ ممدوح فرجاني، المرجع السابق ص٢٤٨.

احتكـار القطاع الخاص للمعلومات لإثارة المخاوف لـدى جهة الإدارة حول سلوك مضر بالأفراد بطريقة أو بأخرى[١].

وفيمـا يخص الكفاءة، يمكـن أن تؤتى حيازة المعلومات أُكُلها بحسب المقاصد التى تحددها جهة الإدارة، وبخاصة فيما يتعلق بمسائل الأمن القومى 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 علـى الأمن القومى مع حيازتها لأهداف تجارية لـذا يمكن تلخيص عنصر الكفاءة فى ثلاثة بنود:

**الأول- جودة البيانات** « Data Quality »

فـى محاولـة لتقييم مصطلح حيـازة المعلومات لحمايـة الأمن القومـي، قام المركز البحثى التابـع للكونجرس (CRS) بتعريفه على أنه مسألة متعددة الوجوه ويشكل ذلك التحدى الأبرز فى حيازة المعلومات[٢].

وتتأتى الإشكالية الأكبر فى بند جودة المعلومة كما ذكر فى مجلة «computer world» فـى ٢٠٠٣ مـن أن «بيانًا واحدًا من معلومة سيئة» يعد إشكاليـة بديهية، ولكن إذا زادت أجـزاء البيانات السيئة لنحو آلاف أو ملايين الأخطـاء؛ فإن ذلك سيؤدى إلى معلومات غير متناسقة تؤدى بدورها إلى الفوضى[٣].

**الثانى- تناسق البيانات** "Data matching"

تواجـه جهـة الإدارة العديـد مـن الأخطاء فـى حيازة المعلومـات[٤] ومنهـا تناسق

(1) H. Cate, op. cit., p. 35 "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".

(٢) تتضمن حيازة المعلومات من جهة الإدارة عادة إعادة تصميم للمعلومة "repurposing"

"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. 1.2003-001) at 25 (2002).

(3) 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"

(٤) مثال تلك الأخطاء كالآتى (طريقة كتابة الأسماء، تغيير النساء لأسمائهن خاصة بعد الزواج، العديد من الأشخاص لهم نفس الأسماء، العديد من الأشخاص يشتركون فى نفس العنوان سواء عمل أو مسكن أو صندوق بريدي.

البيانـات، وقد يستعـان فى الولايات المتحدة الأمريكية للتغلـب على تلك الأخطاء برقم الضمـان الاجتماعـى «social security Numbers» وقـد واجهـت الإدارة فـى الولايات المتحـدة نفس الإشكالية خاصة عند مواجهة الإرهاب.[١] وذلك لكى يتم تعريف الأفراد القادمـين لحدود الدولة وتقدير مـدى الخطر الذى يحوم حولهم مـن خلال المعلومات الدقيقة عنهم.

وهذا أكثر ما تم التركيز عليه فى تقرير اللجنة الاستشارية للخصوصية والتكنولوجيا (TAPAC) [٢] حيـث يتمثل التحدى الأكبر فـى كيفية ضمان أمن المعلومات خاصة فى حـالات مواجهة الإرهاب ورصـد البيانات أو تجميعها من جهـات مختلفة منفصلة عن بعضها البعض، ومنها: جهات المخابرات الذى لا يخضع لأية سيطرة.

وفـى الواقع – أيضًـا – يزداد الأمر صعوبـة عند وجود بيانات غـير متوافقة وغير منتظمة كما فى حالة كاميرات المراقبة الصوتية وكاميرات الفيديو[٣].

**الثالث- أدوات استخلاص البيانات** « Data Mining Tools »

تواجه مسألة حيازة المعلومات بغرض الحفاظ على الأمن القومى وقانون التنفيذ تحديات أكـبر مـن مسألة حيازتها بغرض الأهـداف التجارية للعديد من الأسبـاب، فمثلاً تعد حيازة جهة الإدارة للمعلومات ذات غرض محدد للأهداف البشرية عن القطاع الخاص، علاوة على ذلك غالبًا ما يعمد مخترقو الأمن السيبرانى لتضليل جهة الإدارة مقارنة بالقطاع الخاص

«Government data mining often is searching for needle not in a haystack. but among millions of other needles».

---

(١) تضمين رقم الضمان الاجتماعى لم يحل تلك الإشكالية فى الولايات المتحدة لأن الحسابات الخاصة بكل عائلة يمكن أن يوجد بهـا أرقام ضمـان اجتماعى مختلفة كالزوج والزوجة والمعيل القاصر علاوة على ذلـك البيانات الخاصة بالهجمات الإرهابية المحتملة أرقام الضمان الاجتماعى لا تتضمن أرقام ضمان اجتماعى .

(2) This is a substantial challenge, as stressed in the 2004 final report of Technology and privacy Advisory committee (TAPAC) the "blue ribbn" bipartisan independent committee appointed by the secretary of Defense Donald Rusfeld in 2003 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, 103 MICH. L. REV 1446, 1467 (2005).

(3) See: 1) Emily key, coordinating supply chain Data: To Deliver timely Informantion, companies must overcome Data synchronization Hurdles, frontline solutions, May 1, 2003 at 21.
2) Margo Anderson & Stephen E. Feinberg, who count,? the politics of census – taking in contemporaty America 117-18 (Russell stage found – 1999).=
="The fact that many government data mining applications unstructured data (e.g. audio and video surveillance records) exacerbates the a for mentioned concerns".

ومـع ذلك، تعد المعلومات الـواردة من القطاع الخاص مفتاحًـا مهمًا للأمن القومى من خلال توقع المسئولين عن الأمن القومى للسلوك المعتاد لعملاء القطاع الخاص[١].

- "Government data mining seems similarly likely to fighting yesterday's battles".[2]

## التوصيات:

١- يجـدر بالمشرع المصرى العمـل على استصدار قانون للأمـن السيبرانى يتلافى إشكاليات المعلومات بين أمنها وتداولها فعلى الرغم من أن قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ يعد خطوة طال انتظارها ، كما أنه أحد القوانين المكملة للدستـور المصري الصـادر عـام ٢٠١٤ لكنـه لم يشـرع لأدوات الحماية السيبرانية الكافية[٢].

٢- نقـترح أن يعمل ذلـك القانون على معالجـة مدى تعارض الأمـن السيبرانى مع الخصوصية وغيرها من الإشكاليات القانونية التى ورد ذكرها فى هذا البحث.

٣- نقـترح أن تعمـل السلطـات التنفيذيـة علـى توفـير متطلبات الضبـط الإدارى الإلكترونـى من خـلال تهيئـة أدوات البيئـة السيبرانيـة الآمنة، وأولهـا الإدارة الإلكترونية، والحكومة الإلكترونية.

---

(1) Jeff Jonas & Jim Harper, cato institute, Effective counter terrorism and the limited role of predictive Data mining 7-8 (2006).
"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".

لذلـك يعـد رجال الأمن فى الولايـات المتحدة أكثر توقعًا للهجمـات الإرهابية الخارجية من خلال توقـع ضباط الاستخبارات للخطـط الإرهابية بناء على النشاط الإرهابى فـى الماضى بخلاف الهجمات الإرهابية المحلية تتخذ شكلاً مختلفًا كل مرة فى التخطيط والتنفيذ بحيث تكون مواجهتها أقل وفرص كشفها غير متوقعة.

(2) For more see: CRS report on Data mining and Homeland security 2007
Hector Becerra, Jennifer Oldham & Mitchell landsberg, Airline Terrorism Alert: winging it one Again, L.A. Times, Aug. I1, 2006, At A1.

(٣) . مـريم عـراق: دراسة نقدية لقانـون حماية البيانات الشخصية رقـم ١٥١ لسنة ٢٠٢٠ :مقال منشور علـى الموقع الإلكترونى https://www.mondaq.com/ آخر تحديث ٢٠٢١/٨/٣٠

تعـد الدراسـة النقدية لقانون حماية البيانات الشخصيـة رقم ١٥١ لسنة ٢٠٢٠ الإصدار العلمـى الاول لمركز بحوث القانون والتكنولوجيا بكلية القانون بالجامعة البريطانية فى مصر، والتى أعدت بإشراف الأستاذ الدكتور حسن عبد الحميد عميد كلية القانون بالجامعة البريطانية وبمشاركة كوكبة من رجال القانون فى مصر، قضاة ومحامين، بالإضافة للمتخصصين فـى مجال تقنيـة المعلومات، وغيرهم ممن لهـم علاقة مباشرة بقانـون حماية البيانات الشخصيـة وبالتعاون مع مكتب – اندرسـن مصر.وتأتـى أهمية هذا الكتاب انه قد اجرى دراسة مقارنة بين القانون واللائحة الأوروبية لحماية البيانات (GDPR) باعتبارها القواعد التى استهدى بها المشرع فى إعداده.

٤- نقترح أن تعمل السلطات التنفيذية على تحديث الآليات المعتادة لرصد البيانات والمعلومات وحيازتها، وتهيئة أدوات حيازة البيانات الروتينية كنظام الأرشفة الإلكترونية.

٥- نقترح أن تعمل الجهات الإدارية على وضع سياسة لتنظيم وحفظ المعلومات البيومترية.

**أولاً- المراجع باللغة العربية:**

**١-المؤلفات المتخصصة:**

- **جمال محمد غيطاس:** أمن المعلومات والأمن القومي- مكتبة نهضة مصر- بدون سنة نشر.
- **د/ دلال صادق الجواد، د/ حميد ناصر الفتال:** أمن المعلومات - دار اليازورى العلمية للنشر والتوزيع .
- **د/ طارق إبراهيم الدسوقى عطية:** «الأمن المعلوماتي» (النظام القانونى لحماية المعلومات) دار الجامعة الجديدة، ٢٠٠٩.
- **د/ ممدوح فرجانى خطاب:** النظام القانونى للاستشعار عن بعد من الفضاء الخارجي، دار النهضة العربية، ١٩٩٣.
- **د/ هدى حامد قشقوش:** جرائم الحاسب الإلكترونى فى التشريع المقارن – دار النهضة العربية -القاهرة، ١٩٩٢.
- **د/ وليد السيد سليم:** ضمانات الخصوصية فى الإنترنت – دار الجامعة الجديدة، ٢٠١٢.

**٢- الرسائل العلمية:**

- **أيمن عبد الله فكري:** جرائم نظم المعلومات، دراسة مقارنة، رسالة دكتوراه مقدمة لكلية الحقوق جامعة المنصورة، سنة ٢٠٠٦.
- **راشد محمد المري:** رسالة دكتوراه بعنوان «الجرائم الإلكترونية فى ظل الفكر الجنائى المعاصر»، رسالة مقدمة لكلية الحقوق جامعة القاهرة، ٢٠١٣.
- **محمد أحمد عزت عبد العظيم:** الجرائم المعلوماتية الماسة بالحياة الخاصة- رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة، ٢٠١٦.

- **ناجح أحمد عبد الوهاب:** التطور الحديث للقانون الإدارى فى ظل نظام الحكومة الإلكترونية -رسالة دكتوراه مقدمة لكلية الحقوق جامعة القاهرة، ٢٠١١.

**٣- أبحاث علمية:**

- **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.
- **د/ حسام الدين كامل الأهواني:** الحماية القانونية للحياة الخاصة فى مواجهة الحاسب الإلكتروني، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، يناير ويوليو ١٩٩٠، العددان الأول والثاني، السنة الثانية والثلاثون.
- **د/ داود عبد الرازق الباز:** الإدارة العامة، الحكومة الإلكترونية وأثرها على النظام القانونى للمرفق العام، مجلس النشر العلمي، جامعة الكويت، ٢٠٠٤.
- **سامية بوقرة:** المخاطرة المعلوماتية لنظم المعلومات وآليات مواجهتها، مجلة صوت الجامعة ٢٠١٥ - تصدر عن الجامعة الإسلامية فى لبنان.
- **د/ عبد الإله محمد النوايسة:** جريمة الدخول غير المشروع فى 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.
- **عبد العزيز السيد مصطفى :** أساسيات الرقابة على نظم التبادل الإلكترونى للبيانات – بحث مقدم لمؤتمر التجارة الإلكتروني (الآفاق والتحدى ) المنعقد بكلية التجارة جامعة الإسكندرية -يوليو ٢٠٠٢.
- **د/ عماد يوسف حب الله:** ورشة عمل حول "بناء القدرات فى مجال الحماية القانونية على الإنترنت ٤-٥ شباط ٢٠٠٩ - الهيئة المنظمة للاتصالات فى لبنان - أمن الفضاء السيبرانى.

**٤- قوانين وقرارات:**

١- القانون المصرى لتنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ .

٢- القانون المصرى رقم ١٠٩ لسنة ١٩٧١ فى شأن هيئة الشرطة.

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

٤- قرار رئيس مجلس الوزراء المصرى رقم ١٠٣٢ لسنة ٢٠١٥ باختصاصات اللجنة القومية الدائمة للتنسيق الأمني.

٥- قرار رئيس الجمهورية المصرى رقم ٥٥٢ لسنة ٢٠١٥ بتشكيل لجنة عليا لتنقية قواعد البيانات القومية -الجريدة الرسمية – العدد ٥٢ مكررًا (هـ) فى ٢٩ ديسمبر سنة ٢٠١٥.

٦- قرار رئيس مجلس الوزراء المصرى رقم ٢٣٢٨ لسنة ٢٠١٤ «والذى ضم بموجبه ممثل لمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء إلى عضوية المجلس الأعلى للأمن السيبراني». «منشور بالجريدة الرسمية - العدد ٥٢ مكررًا (ا) فى ديسمبر سنة ٢٠١٤.

٧- القانون الكويتى رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية: الكويت اليوم العدد ١١٧٢، السنة الستون بتاريخ ٢٠١٤/٢/٢٣.

٨-القانون القطرى رقم ١٤ لسنة ٢٠١٤ الخاص بمكافحة الجرائم الإلكترونية.

**٥- 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 فى القضية رقم ٢٠١/٥ جنايات عسكرية- إدارة المدعى العام العسكري-(حكم غير منشور).

٣- حكم محكمة القضاء الإداري، دائرة المنازعات الاقتصادية والاستثمار، الصادر فى الدعوى رقم ١٤٣٠ لسنة ٦٥ ق جلسة ٢٠١٠/١١/٢٧ (حكم غير منشور).

٤- حكـم محكمة القضـاء الإدارى – الدائرة الثامنة عقـود- الدعوى رقم ٦٣٠٥٥ لسنة ٦٨ ق بتاريخ أغسطس ٢٠١٥ (حكم غير منشور).

**٦- وثائق:**

- مجلة حالة العالم، تقرير «جايسون هيلي» مدير مبادرة «initiative» cyber statecraft بمركز (Atlantic council).

**٧-مواقع إلكترونية:**

-موقع المكتب الفيدرالى الألمانى لأمن المعلومات www.bsi.bund.de

موقع ويكيبديا

- https://ar.wikipedia.org/wiki/%D9% 81%D8%B6%D8%A7%D8%A1%D8%A5%D9%84%D9 %83%D8%AA%D8%B 1%D9 %88%D9% 86%D9 %8A

**٨-مقالات:**

- **د/سمـير فـرج** :الفضـاء السيبراني-مقال منشـور بالموقـع الإلكترونى لجريدة الأهرام المصرية بتاريخ ٣٠ يوليو ٢٠٢٠ -آخر تحديث ٢٠٢١/٨/٣٠

- https://gate.ahram.org.eg/News/2444508.aspx

٢- مـريم عـراق: دراسة نقدية لقانون حمايـة البيانات الشخصيـة رقم ١٥١ لسنة ٢٠٢٠ :مقـال منشور على الموقـع الإلكترونـى https://www.mondaq.com/ آخر تحديث ٢٠٢١/٨/٣٠.

**ثانياً- المراجع باللغة الإنجليزية:**

- Abraham D. Safaer: - National security and leaks, the Government's Authority to Discipline itself. International studies in Human Rights- volume 16
- Amanda N. Craig et al: - proactive cyber security: A comparative Industry and Regulatory Analysis, - AM. Bus L. J. (forth coming) 2015.
- Brain Bridge: - D: Introduction to computer law, London 2000, fourth edition.
- Bruce P. smith: - Hacking, Poaching, and counterattacking: Digital counterstrikes and the contours of self-Help, I J.L Econ, & Pol'Y 171, 173 (2005),
- CRS report on Data mining and Homeland security 2007

- David weissbrodt: - cyber conflict, cyber crime, and cyber Espionage, Minnesota Journal of International Law's 2013 symposium
- Emily key: - coordinating supply chain Data To Deliver timely Information, companies must overcome Data synchronization Hurdles, frontline solutions, May 1, 2003
- Fred H. Cate: - Government Data Mining:- The need for a legal framework, Hienonline – 43 Harv. C. R. C.L.L. Rev. 2008
- Hector Becerra, Jennifer oldham & Mitchell landsberg: Airline Terrorism Alert-winging it one Again, L.A. Times, Aug. I1, 2006
- Jeff Jonas & Jim Harper: - Cato institute, Effective counterterrorism and the limited role of predictive Data mining 7 -8 (2006).
- Jonathan clough: principles of cybercrime-second edition -Cambridge press 2010
- Lawrence J. Trautman: congressional cypersecurity oversight: who's who and How it works
- Margo Anderson & Stephen E. Feinberg: - who count? The politics of census – taking in contemporary America 117- 18 (Russell stage found – 1999).
- Marietta Benko, and others: - space law in the united nations, Martinus Nijhoff, Netherlands, 1985
- Paul Schwartz: - Data processing and Government Administration: The failure of the American legal Response to the computers HASTINGS LJ. 1321 (1992) emphasis in original
- Ronald D. lee & Paul M. Schwartz :-Beyond the "war" on Terrorism, Towards the New Intelligence Network, 103 MICH. L. REV 1446, 1467 (2005).
- Richard Clarke: - Threats to U.S. National security: proposed partnership initiatives towards preventing cyber terrorist Attacks, 12 Depaul Bus, L. J. (1999 – 2000).
- Scott J. Shackelford, JD, PhiD, scott Russell, JD & Andreas juehn: - Defining cyber security Due Diligence under International law: lessons from the private sector.
- Susan W. Brenner, cyber crime:- criminal threats for cyberspace (2010)

- The Cantigny principles on technology terrorism, and privacy, National security law Report, feb. 2005
- The Cantigny" conference on counterterrorism technology and privacy organized by the standing committee on law and National security of the American Bar Association".
- The Emergence of cyber security law, prepared for the Indiana university -Maurer school of law by Hanover Research, February,2015